



WebdynSunPM

Manuel d'utilisation

Index

Glossaire.....	6
Remarques concernant ce manuel.....	9
1. Présentation.....	11
1.1 Description générale.....	11
1.2 Principe de fonctionnement.....	11
1.3 Les interfaces.....	12
1.4 Équipements supportés.....	13
1.5 Références des produits.....	13
1.6 Spécifications techniques.....	14
1.6.1 Caractéristiques générales.....	14
1.6.2 Caractéristiques techniques.....	15
1.6.3 Caractéristiques logicielles.....	17
1.7 Consignes de sécurité.....	18
1.8 Réglementation.....	19
2. Installation et Maintenance.....	20
2.1 Prérequis.....	20
2.2 Déballage.....	20
2.2.1 Contenu.....	20
2.2.2 Identification.....	20
2.3 Montage.....	23
2.3.1 Ouverture/Fermeture du boîtier.....	23
2.3.2 Fixation murale.....	23
2.4 Description des interfaces.....	24
2.4.1 Alimentation du produit.....	24
2.4.2 Réseau cellulaire.....	25
2.4.3 Les voyants & boutons.....	28
2.4.4 Interface d'extension.....	31
2.4.5 Interface Ethernet.....	33
2.4.6 Interface Série RS485/RS422.....	34
2.4.7 Interface Entrées/Sorties.....	37

3. Configuration.....	42
3.1 FTP/SFTP/WebDAV	42
3.1.1 Principe de fonctionnement.....	43
3.1.2 Fichiers de configuration.....	44
3.1.3 Mises à jour.....	71
3.2 Interface web embarquée	72
3.2.1 Equipements (Devices)	74
3.2.2 Paramètres (Settings)	99
3.2.3 Système (System).....	142
3.3 Carte Micro SD	151
4. Exploitation.....	152
4.1 Le serveur FTP/SFTP/WebDAV.....	153
4.1.1 La configuration « CONFIG »	156
4.1.2 Les définitions « DEF »	157
4.1.3 Les données « DATA ».....	159
4.1.4 Les alarmes « ALARM »	164
4.1.5 Les commandes « CMD »	166
4.1.6 Les scripts « SCRIPT »	167
4.1.7 La mise à jour « BIN »	167
4.1.8 Les Logs « LOG ».....	168
4.1.9 Web Services	174
4.2 Le serveur MQTT/MQTTS	178
4.2.1 Format des données	179
4.3 Carte microSD	187
5. Commandes.....	188
5.1 Principe	188
5.2 Fonctionnement	188
5.2.1 Fichier de commande.....	188
5.2.2 Message de commande MQTT.....	191
5.2.3 SMS	191
5.3 Liste des Commandes	192
5.3.1 « connect » : Déclenchement d'une connexion.....	193

5.3.2 « status » : Récupération du statut du concentrateur	194
5.3.3 « factory » : Retour aux paramètres usines	196
5.3.4 « reboot » : Redémarrage du concentrateur	196
5.3.5 « updateFirmware » : Mise à jour logiciel du concentrateur	197
5.3.6 « apn » : Configuration du modem	198
5.3.7 « ftp » : Configuration du serveur FTP/SFTP.....	198
5.3.8 « sftp » : Configuration du serveur SFTP.....	199
5.3.9 « https » : Configuration du serveur Webdav/HTTPS.....	199
5.3.10 « log » : Activation des log des communications des équipements	199
5.3.11 « setRelay » : Modification de l'état du relais.....	201
5.3.12 « discoverDevices » : Découverte d'équipements	201
5.3.13 « getParameters » : Collecte des paramètres	203
5.3.14 « getData » : Collecte des variables de code action 6 ou 7	203
5.3.15 « writeVariable » : Ecriture de variable sur un équipement.....	204
5.3.16 « setKey » : Ajout des clés pour le déchiffrement des scripts clients	205
5.3.17 « deleteKey » : Suppression des clés pour le déchiffrement des scripts clients.....	206
5.3.18 « startScript » : Démarrage d'un script.....	207
5.3.19 « stopScript » : Arrêt d'un script	207
6. Mise à jour.....	208
6.1 Par Interface web	208
6.2 Par FTP/SFTP/WebDAV.....	208
6.3 Par commande SMS ou MQTT/MQTTS	209
6.4 Par carte micro SD.....	209
7. Outils & diagnostics	210
7.1 Diagnostics.....	210
7.2 Outils	210
8. FAQ.....	211
9. Support.....	216
10. Annexes.....	217
10.1 Annexe A : Fichier de configuration « _config.ini ».....	217
10.2 Annexe B : Liste des zones horaires.....	237
10.3 Annexe C : Onduleurs compatibles.....	239

10.3.1 ABB.....	239
10.3.2 CEFEM.....	239
10.3.3 Fronius	240
10.3.4 GOODWE.....	243
10.3.5 GROWATT	249
10.3.6 Huawei	253
10.3.7 INGETEAM.....	257
10.3.8 KACO	259
10.3.9 Kostal	262
10.3.10 SMA.....	263
10.3.11 Solis.....	264
10.3.12 SUNGROW	267
10.4 Annexe D : Esclave Modbus	272
10.4.1 Fonctionnement général.....	272
10.4.2 Activer l'esclave Modbus	272
10.4.3 Registres utilisateurs	273
10.4.4 Registres Webdyn prédéfinis	274
10.4.5 Lire ou écrire une variable.....	275
10.4.6 Exécuter une commande.....	275
10.4.7 Gestion des erreurs	275
Bureaux et support	277

Glossaire

NAME	DESCRIPTION
2G	Second Generation : standard numérique de seconde génération (2G) pour la téléphonie mobile comprenant le GSM, GPRS et EDGE.
3G	Third Generation : standard numérique de troisième génération (3G) pour la téléphonie mobile comprenant le UMTS, HSPA, HSPA+ et DC-HSPA+.
4G	Fourth Generation: standard numérique de quatrième génération (4G) pour la téléphonie mobile comprenant le LTE-Advanced.
AES	Advanced Encryption Standard : algorithme de chiffrement symétrique.
APN	Access Point Name : nom du point d'accès permettant à la passerelle de se connecter au réseau Internet par liaison mobile.
Broker	Serveur MQTT en charge de la réception des informations publiées afin de les transmettre aux clients abonnés. Le broker a un rôle de relais.
CSV	Comma-separated values : format texte ouvert représentant des données tabulaires sous forme de valeurs séparées par des points virgules. Ce format permet d'exploiter facilement les données avec un tableur comme Excel.
DNS	Domain Name System : service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP.
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.
IMEI	International Mobile Equipment Identity : numéro qui permet d'identifier de manière unique chacun des modems
IMSI	International Mobile Subscriber Identity : numéro unique stocké dans la carte SIM permettant à un réseau mobile d'identifier un usager.
IP	Internet Protocol : protocole de messages responsable de l'adressage et de la transmission de paquets TCP sur le réseau.
Lua	Langage de script. Voir http://www.lua.org/ pour plus de détails.

Modbus	Le Modbus est un protocole de communication couramment utilisé en industrie pour dialoguer en réseau avec des équipements industriels. Voir http://www.Modbus.org/ pour plus de détails.
MQTT	Message Queuing Telemetry Transport : protocole de messagerie publish-subscribe basé sur le protocole TCP/IP.
MQTTS	Protocole de messagerie MQTT sécurisé
NTP	Network Time Protocol : protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale du concentrateur sur une référence d'heure.
DIN rail	Rail métallique standardisé de 35 mm utilisé en Europe dans les équipements industriels de contrôle en racks.
RSSI	Received Signal Strength Indication : mesure du niveau de puissance en réception d'un signal issu d'une antenne radio.
RTU	Le mode RTU est un bus filaire en RS422/485 pour le Modbus.
SO	Impulsion normalisée venant de compteurs (eau, gaz, électricité, ..) suivant la norme NF EN 62053-31
SFTP	SSH File Transfer Protocol : protocole de communication utilisant un protocole de communication sécurisé SSH. Son utilisation est proche du FTP.
IS	Système d'Information : serveur avec lequel le concentrateur échange (configuration, données, alarmes, ...)
Sunspec	Protocole de communication ouvert pour onduleur, basé sur Modbus et conforme aux normes de l'alliance SunSpec (Voir https://sunspec.org/ pour plus de détails.)
TCP	Transmission Control Protocol : protocole orienté connexion sur Internet qui offre services de segmentation des données en paquets que 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.
TIC	Télé-Information Client : sortie d'information numérique des compteurs ERDF qui diffuse en permanence les paramètres contractuels gérés, ainsi que les grandeurs de consommation mesurées par l'appareil.

Topic	Canaux d'informations MQTT qu'utilisent les publieurs (les publishers) pour envoyer les messages. Ces messages peuvent être lus par les abonnés (les subscribers).
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...).
UTF-8	Universal Character Set Transformation Format1 - 8 bits : codage de caractères informatiques conçu pour coder l'ensemble des caractères du « répertoire universel de caractères codés »
WebDAV	Extension au protocole HTTP permettant d'améliorer la gestion des fichiers distants. Dans le cadre de la WebdynSunPM, le protocole WebDAV est utilisé sur HTTPS. On parle donc de WebDAV-HTTPS.

Remarques concernant ce manuel

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

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

Ce manuel comporte six sections distinctes :

- Section 1 : Présentation générale
- Section 2 : Installation
- Section 3 : Configuration
- Section 4 : Exploitation
- Section 5 : Outils & diagnostics
- Section 6 : FAQ

Champ d'application

La présente description technique est valable pour les concentrateurs WebdynSunPM à partir de la version de matériel V1 et de la version logicielle V3.0.0.

Groupe cible

Ce guide s'adresse à toutes personnes impliquées dans la supervision de systèmes photovoltaïques, plus particulièrement aux personnes chargées de la maintenance locale ou à distance des installations, ainsi qu'aux développeurs de portails permettant l'exploitation des données transmises.

Il est recommandé de confier l'installation et la mise en service de la WebdynSunPM aux personnes qualifiés et formés. Les personnes qualifiées doivent avoir les compétences suivantes :

- Connaissance détaillée des services de gestion du réseau.
- Connaissance des protocoles réseau basés sur IP.
- Connaissance des spécifications des protocoles utilisés (Modbus, SunSpec, etc ...) et des équipements reliés au concentrateur.
- Formation à l'installation et à la configuration des systèmes informatiques.
- Connaissance et respect de ce document et de toutes les informations de sécurité.

Veuillez-vous adresser à votre contact commercial (contact@webdyn.com) afin de connaître la liste des portails partenaires.

Historique du document

Version	Contenu	Version du firmware applicable
V2.05	Création du manuel	V2.2 à V2.2.6
V3.00	Gestion de la carte micro SD Ajout du WebDAV Ajout du MQTT Mise en annexe spécifique de la TIC et des protocoles propriétaires Modification de l'édition et création des équipements Ajout de la version WebdynSunPM 4G	V3.0.0 à V4.2.17
V4.2.17	Ajout de variables dans le fichier script SCL Ajout du Webservice Ajout option nombre d'acquisitions dans les fichiers DATA Mise à jour de l'IHM des scripts Ajout des scripts LUA chiffrés client Ajout des scripts Webdyn avec licence Ajout des codes d'écriture forcé dans les fichiers de définition Ajout des codes actions 6, 7 et 9 dans les fichiers de définition Modification du format des données MQTT (métadatas) Ajout de la commande « getData »	V4.2.17
V4.3.2	ActivePowerControl script 1.02 se connecte en mode stop et flat et nouveaux paramètres de script (licence supplémentaire nécessaire) Ajout d'une nouvelle fonction de script pour envoyer une alarme Ajout d'une nouvelle fonction de script pour vérifier un appareil/balise dans la configuration Correction de setKey par SMS Correction dans le script du générateur diesel (délai d'attente) Scripts du générateur diesel : paramétrages distants par FTP	
V4.6	Détection automatique des onduleurs suivants : ABB, Cefem, Goodwe, Growatt, Huawei, Ingeteam, Kaco, Solis, Sungrow, Fronius, Kostal, SMA	V4.6.01

1. Présentation

1.1 Description générale

La WebdynSunPM est un concentrateur qui a pour objectif de monitorer tous types d'installations photovoltaïques. Il permet de collecter, d'analyser, de surveiller et de contrôler les équipements présents sur le site.

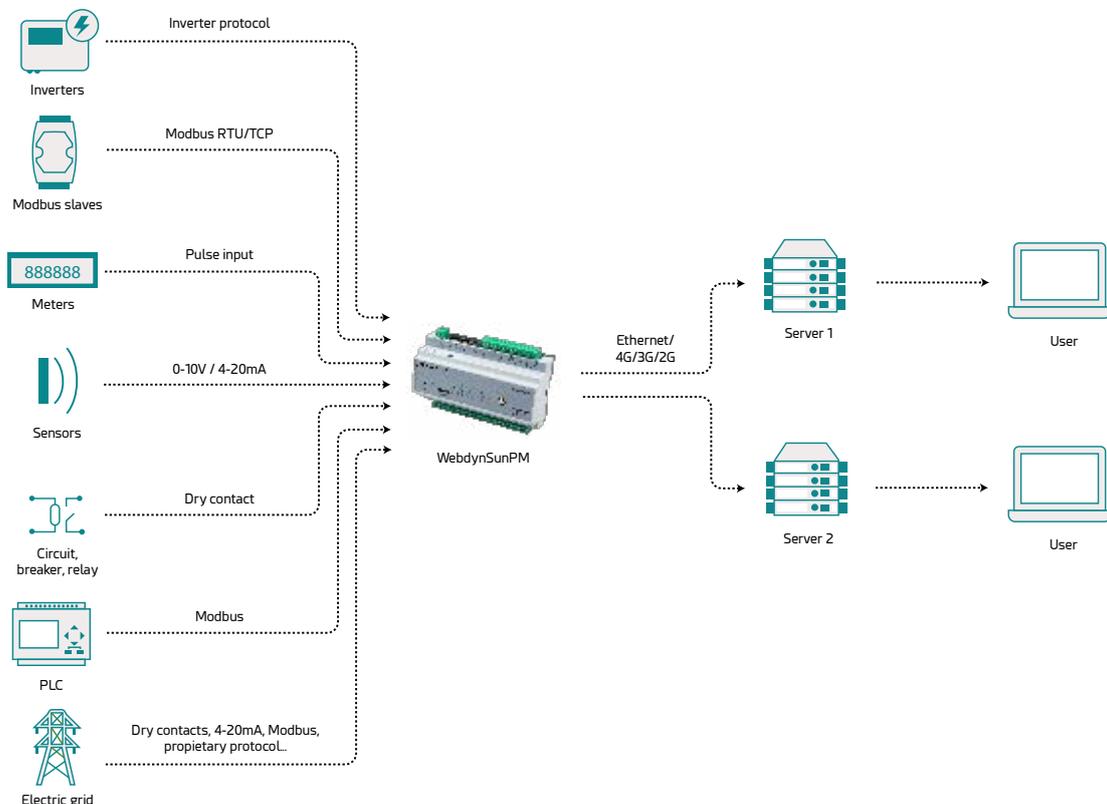
Les informations collectées (données, paramètres, ...) sont mises en forme avant d'être envoyées vers un système d'information (SI). Le concentrateur assure la sécurité et la confidentialité des informations échangées.

L'automatisation de certaines actions locales, par exemple la gestion de l'injection ou de l'autoconsommation, est gérée à l'aide de scripts personnalisables embarqués dans le concentrateur.

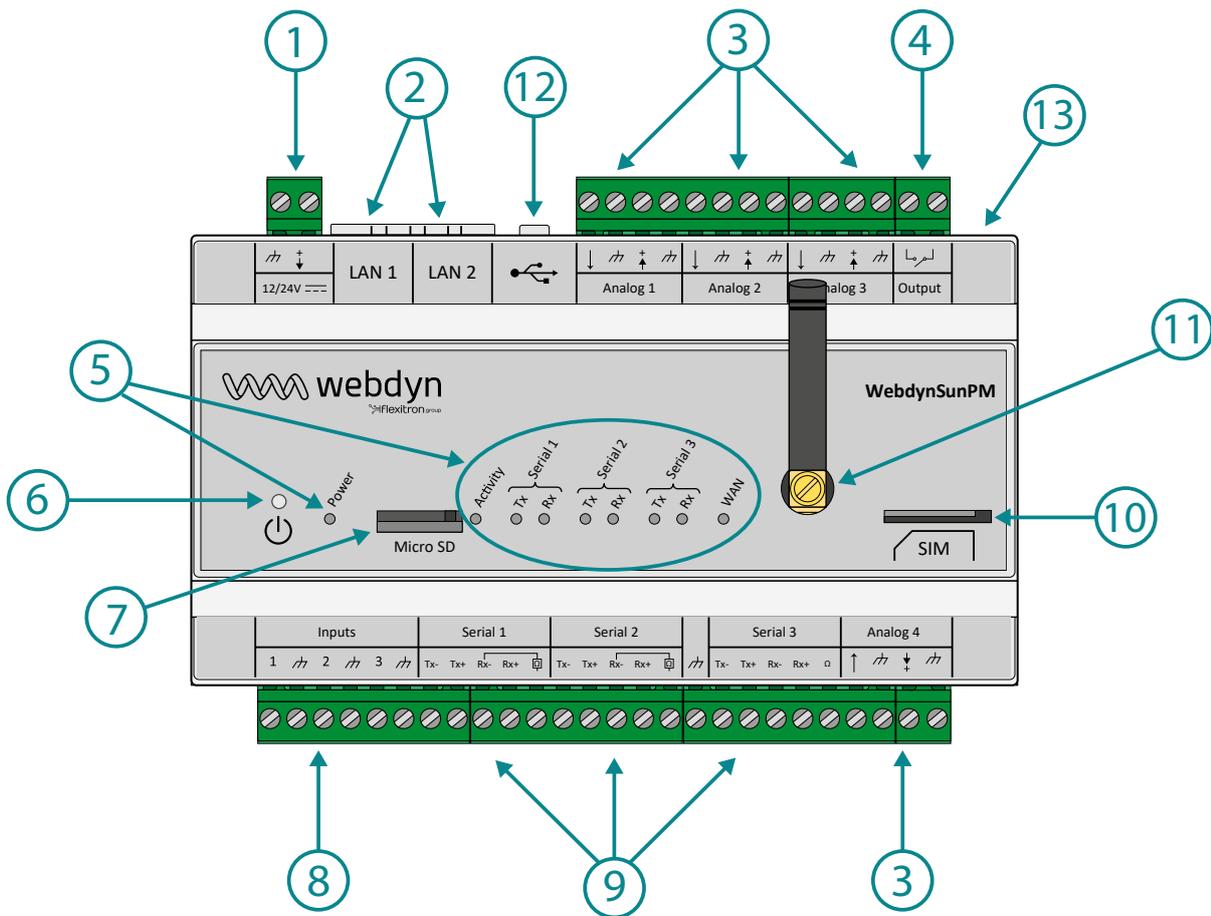
1.2 Principe de fonctionnement

La WebdynSunPM s'intègre complètement dans l'installation photovoltaïque. Les équipements comme des onduleurs, des capteurs (pyranomètre, sonde de température...), des compteurs, des afficheurs, des disjoncteurs ou relais peuvent être raccordés au concentrateur grâce à ses nombreuses interfaces disponibles. La relève des informations ainsi que le pilotage des équipements se font en continu par la WebdynSunPM. Périodiquement, les données seront mises en forme et déposées sur un serveur FTP et/ou envoyée à un serveur MQTT à l'aide du modem ou d'une connexion Ethernet. Afin de sécuriser les échanges avec les serveurs, le concentrateur gère les protocoles SFTP et MQTTS. Il est possible de configurer la WebdynSunPM par un simple envoi de commandes SMS, mais également en utilisant les pages web embarquées.

Pour les installations nécessitant des fonctions particulières, il est possible de créer ses propres scripts.



1.3 Les interfaces



1. Bornier d'alimentation 12-24 V

2. 2 Ports Ethernet (LAN 1 et LAN 2)

3. 4 Entrées analogiques 0-10 V ou 4-20 mA

4. 1 Sortie relais (24V/1A)

5. Voyants :

- Power : Statut de l'alimentation 12-24 V
- Activity : Statut du produit
- Serial1, Serial2, Serial3 :
 - Tx : Données émises sur le port série RS485/RS422
 - Rx : Données reçues sur le port série RS485/RS422
- WAN : Statut de la connexion

6. Bouton Power

7. Emplacement carte Micro SD

8. 3 Entrées digitales (TOR ou SO impulsionnelle)

- 9. 3 Ports RS485/RS422
- 10. Support carte SIM
- 11. Connecteur d'antenne SMA du modem
- 12. Port USB (pour extension)
- 13. Bouton RESET

1.4 Équipements supportés

La WebdynSunPM est compatible avec tous les équipements intégrant l'un des protocoles supportés.

Listes non exhaustives des protocoles supportés :

Protocole Onduleur	Interface physique	Caractéristiques
SMA-net	RS485/RS422 2 fils	100 max
Modbus TCP	Ethernet	254 max
Modbus RTU	RS485/RS422 2 fils ou 4 fils	247 max
Solarmax	RS485/RS422 2 fils	100 max
TIC	USB (câble en option)	1 max
Delta-Solivia	RS485/RS422 2 fils	100 max



Beaucoup d'équipements Onduleur fonctionnent à présent en Modbus. Le concentrateur prend en charge tous les équipements Modbus RTU et TCP.

1.5 Références des produits

Références	Descriptions
WG0517-A01	WebdynSunPM (Version Europe et Inde)
WG0517-A02	WebdynSunPM (Version Monde)
WG0517-A03-DEIE	WebdynSunPM en coffret DEIE (Version Europe et Inde)
WG0517-A04	WebdynSunPM 4G (Version Europe et Inde)

1.6 Spécifications techniques

1.6.1 Caractéristiques générales

Caractéristiques	Descriptions
Alimentation	+12V 700mA (certaines fonctionnalités sont non supportées en 12V ou +24V 350mA)
Batterie	650mAh 3.7V, Lithium-polymère
Consommation	P : 5 W Pmax : 10 W
Dimensions	155x 106 x 58mm 9 modules rail DIN
Boîtier	conforme RoHS DIN EN 60715 TH35 DIN VDE 0470-1 DIN 43880 taille 1 Conforme REACH VBG 4 IEC 529 Non étanche
Fixation	Rail DIN
Poids	0.330 kg
Température de fonctionnement	-5 °C / +40 °C
Température de stockage	Stockage : -20 °C / +85 °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.

1.6.2 Caractéristiques techniques

Caractéristiques	Descriptions
Capacité mémoire pour les données	DDR3 SDRAM : 512 Mo. Flash eMMC : 8 Go au total (50Mo max par équipement défini)
Carte SD	MicroSD MMC/SD/SDIO (jusqu'à 32 Go)
Interface cellulaire Modem	Modem version Europe et Inde : <ul style="list-style-type: none">• 2G (EDGE, GSM, GPRS) : 900MHz et 1800MHz• 3G (HSPA) : B1 et B8 Modem version Monde : <ul style="list-style-type: none">• 2G (EDGE, GSM, GPRS) : 850MHz, 900MHz, 1800MHz, 1900MHz• 3G (HSPA) : B1, B2, B5, B6, B8 et B19 Modem 4G version Europe et Inde: <ul style="list-style-type: none">• 2G (EDGE, GSM, GPRS) : 850MHz, 900MHz, 1800MHz, 1900MHz• 4G (LTE) : B1, B3, B5, B7, B8, B20 et B28 Antenne : SMA externe
Format SIM	SIM standard (mini SIM) format 2FF 1.8V et 3V compatible
Interface Ethernet	2 ports disponibles en 10/100 Mbits/s
Interface USB	1 port USB2.0
Interface Série	3 ports RS485/RS422

Interface Entrées/Sorties 4 entrées analogiques 0/10V ou 4/20mA
3 entrées numériques TOR ou SO impulsionnelle (classe A ou B)
1 sortie Relais (24V/1A)



Webdyn ne fournit aucune carte SIM. Veuillez vous rapprocher d'un opérateur M2M supportant le réseau 2G/3G ou 2G/4G.

Données connectivités version 2G/3G Europe et Inde :

Bande RF	Fréquences Émission	Puissance Max
UMTS B1	1922 MHz - 1978MHz	22,5 dBm(+1,5dB)
UMTS B8	882 MHz - 913 MHz	22,5 dBm(+1,5dB)
E-GSM 900	880 MHz - 915 MHz	33 dBm (+2dB GSM,GPRS)
DCS 1800	1710 MHz - 1785 MHz	30 dBm (+2dB GSM,GPRS)

Données connectivités version 2G/3G Monde :

Bande RF	Fréquences Émission	Puissance Max
UMTS B1	1922 MHz - 1978 MHz	23 dBm(+2dB)
UMTS B2	1852MHz - 1908 MHz	23 dBm(+2dB)
UMTS B5	826 MHz - 847 MHz	23 dBm(+2dB)
UMTS B6	832 MHz - 838 MHz	23 dBm(+2dB)
UMTS B8	882 MHz - 913 MHz	23 dBm(+2dB)
UMTS B19	832.4MHz - 842.6 MHz	23 dBm(+2dB)
GSM 850	824 MHz - 849 MHz	33 dBm (+2dB GSM,GPRS,EDGE)
E-GSM 900	880 MHz - 915 MHz	33 dBm (+2dB GSM,GPRS,EDGE)
DCS 1800	1710 MHz - 1785 MHz	30 dBm (+2dB GSM,GPRS,EDGE)

PCS 1900	1850 MHz – 1910 MHz	30 dBm (+-2dB GSM,GPRS,EDGE)
----------	---------------------	------------------------------

Données connectivités version 2G/4G Europe et Inde :

Bande RF	Fréquences Émission	Puissance Max
GSM 850	824 MHz – 849 MHz	33 dBm (+-2dB)
E-GSM 900	880 MHz - 915 MHz	33 dBm (+-2dB)
DCS 1800	1710 MHz – 1785 MHz	30 dBm (+-2dB)
PCS 1900	1850 MHz – 1910 MHz	30 dBm (+-2dB)
LTE B1	1920 MHz- 1980 MHz	23 dBm (+-2dB)
LTE B3	1710 MHz – 1785 MHz	23 dBm (+-2dB)
LTE B5	824 MHz – 849 MHz	23 dBm (+-2dB)
LTE B7	2500 MHz – 2570 MHz	23 dBm (+-2dB)
LTE B8	880 MHz – 915 MHz	23 dBm (+-2dB)
LTE B20	832 MHz – 862 MHz	23 dBm (+-2dB)
LTE B28	703 MHz – 748 MHz	23 dBm (+-2dB)

1.6.3 Caractéristiques logicielles

Caractéristiques	Protocoles/Formats
Serveur embarqué	HTTP
Protocole de communication serveur (SI)	<ul style="list-style-type: none"> • FTP • SFTP • WebDAV-HTTPS • MQTT • MQTTS (générique et compatible avec AWS IoT, Azure IoT et Google Cloud IoT)

Modbus	<ul style="list-style-type: none"> • RTU • TCP
Synchronisation horloge	NTP
Format de fichier pour le serveur (SI)	<ul style="list-style-type: none"> • CSV en FTP/SFTP/WebDAV-HTTPS • JSON en MQTT/MQTTS

1.7 Consignes de sécurité

Respectez toutes les consignes de sécurité figurant dans ce guide.

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



Raccordement électrique :

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



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



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.



Cet équipement ne convient pas à utilisation dans des lieux pouvant accueillir des enfants.



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 cellulaire Modem, il est impératif de laisser un espace vide de 20 cm autour de l'antenne.

1.8 Réglementation

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

Recyclage :



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

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

2. Installation et Maintenance

2.1 Prérequis

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

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

- Avoir à disposition ce manuel utilisateur.
- Avoir un tournevis approprié aux types de connecteurs disponibles sur le concentrateur WebdynSunPM.
- Connaître les paramètres de connexion au système d'information SI.

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

- Avoir une carte SIM avec un abonnement M2M (data et sms(facultatif)) activé et connaître l'APN du fournisseur. Le numéro d'appel de la carte SIM peut être utile.
- Utiliser une antenne déportée si la réception radio ou cellulaire modem est dégradé.
- Avoir un PC pour la configuration ou mise à jour du produit par l'interface Web du concentrateur.

2.2 Déballage

2.2.1 Contenu

Le concentrateur WebdynSunPM est livré de base avec :

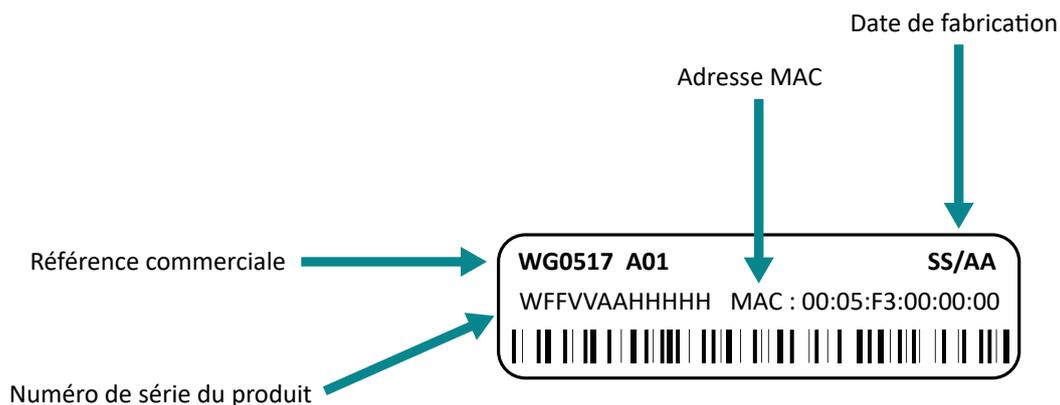
- Une antenne SMA soudée pour le modem (scotchée au dos du produit).
- Une batterie (déjà mise en place dans le produit).

2.2.2 Identification

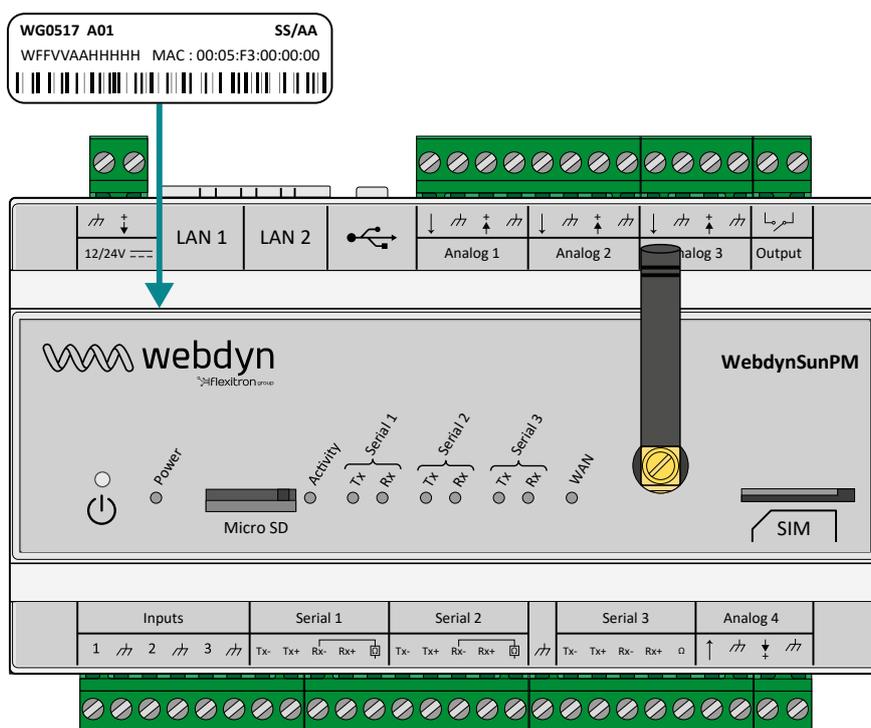
La référence commerciale se compose ainsi :

- **WG0517-A01** : WebdynSunPM en version Europe et Inde
- **WG0517-A02** : WebdynSunPM en version Monde
- **WG0517-A03-DEIE** : WebdynSunPM en version Europe et Inde dans un coffret DEIE
- **WG0517-A04** : WebdynSunPM 4G en version Europe et Inde

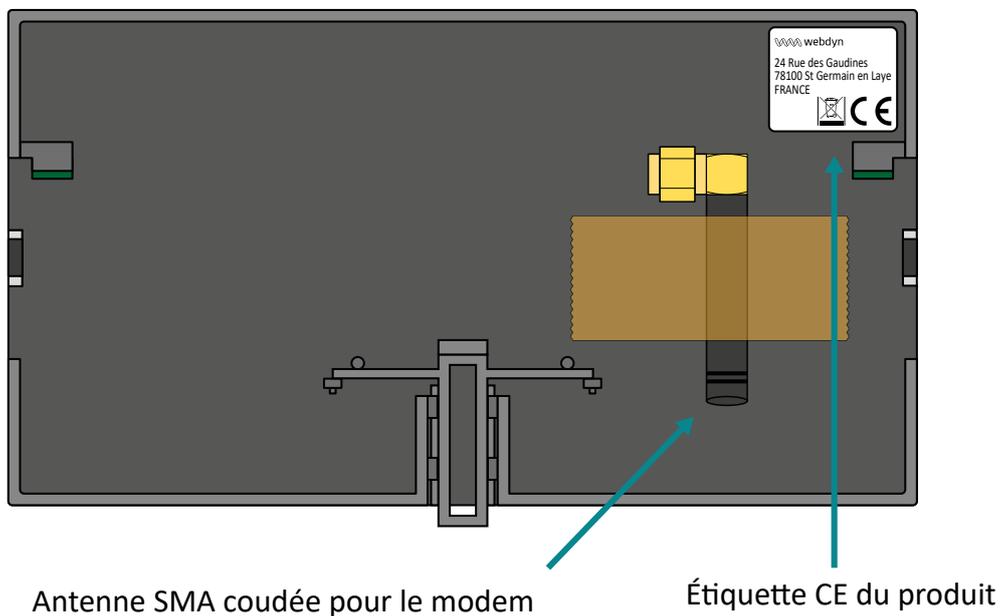
Chaque produit est étiqueté avec les informations suivantes :



Cette étiquette est accessible sur le dessus du produit :



L'étiquette CE du produit se situe sur l'arrière du boîtier :



Version du logiciel :

Vous trouverez la version du logiciel sur l'interface Web du concentrateur. La version du logiciel est indiquée dans l'onglet « Home » (Voir chapitre 3.2 : «Interface web embarquée»).

2.3 Montage

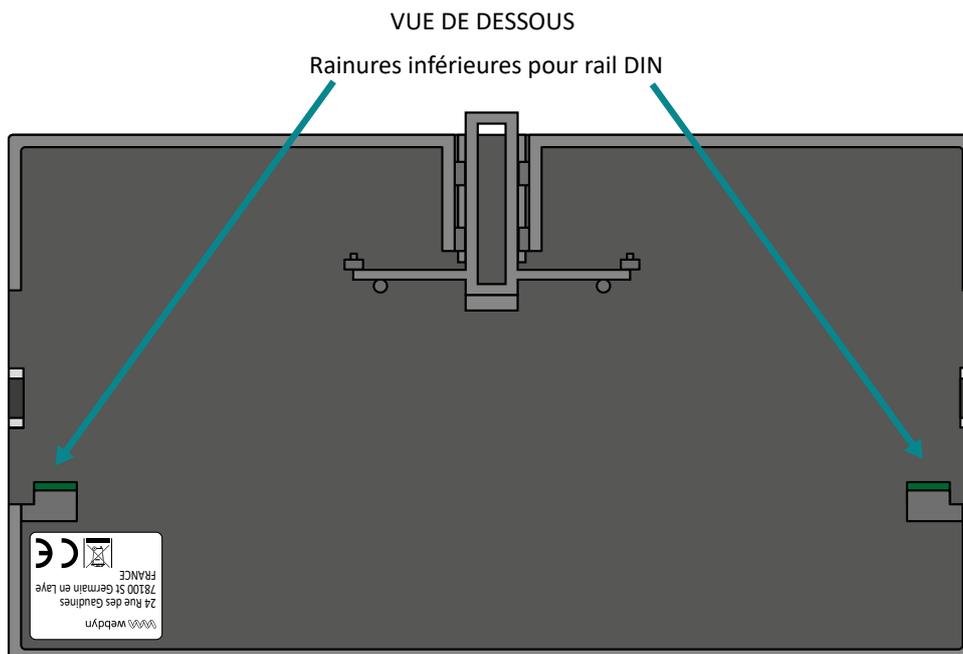
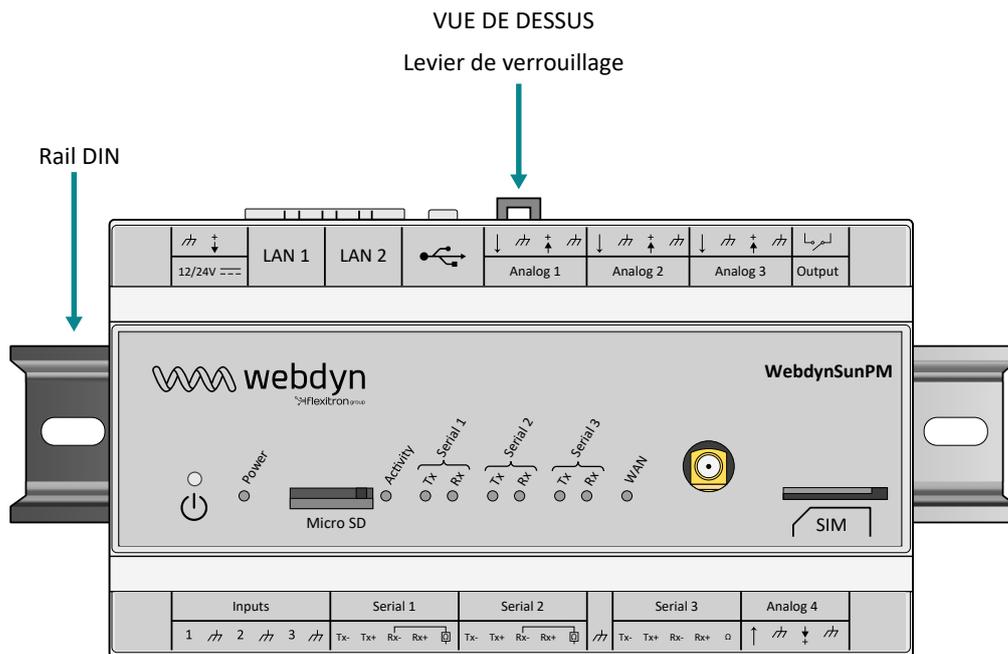
2.3.1 Ouverture/Fermeture du boîtier

Le produit ne doit pas être ouvert par l'utilisateur.

Pour toute intervention, la WebdynSunPM doit être retournée en S.A.V (sav@webdyn.com).

2.3.2 Fixation murale

La WebdynSunPM est prévue pour être fixée sur un rail DIN.



Pour fixer le concentrateur sur un rail DIN, suivre les étapes suivantes :

- Incliner et positionner les rainures inférieures (voir vue de dessous) du concentrateur sur le bas du rail DIN.
- Pousser le concentrateur afin de le faire pivoter vers le haut.
- Appuyer sur le concentrateur jusqu'à entendre le clic.

Pour retirer le concentrateur sur un rail DIN, suivre les étapes suivantes :

- Relever le levier de verrouillage (voir vue de dessus) du concentrateur à retirer jusqu'en haut. Cela ouvre le mécanisme de verrouillage et permet de retirer le concentrateur.
- Faire pivoter vers le bas le concentrateur.



Avant la fixation ou le retrait du concentrateur, veuillez :

- Couper l'alimentation de l'équipement.
- Retirer l'antenne scotchée sur l'arrière du boîtier.

2.4 Description des interfaces

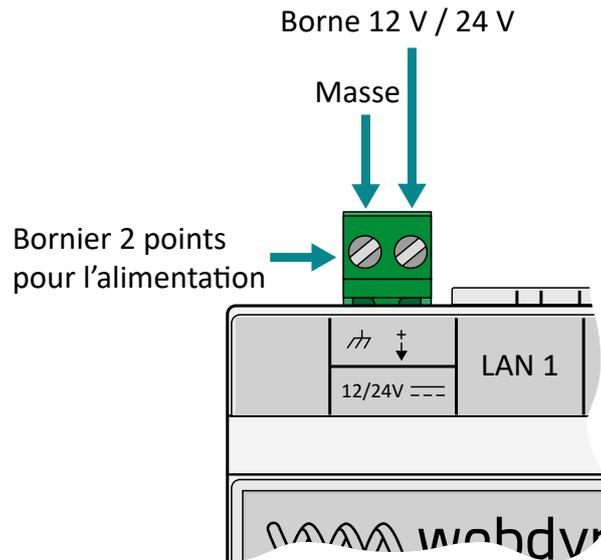
2.4.1 Alimentation du produit

2.4.1.1 Alimentation externe

Le concentrateur WebdynSunPM peut être alimenté en 12V ou 24V continu. L'alimentation est réalisée via le bornier débrochable 2 points identifiés en « 12/24V » et situés en haut à gauche du concentrateur.



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.



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 15 Watts minimum.

2.4.1.2 Batterie

Le concentrateur WebdynSunPM possède une batterie permettant d'envoyer une alarme pour prévenir du défaut de coupure de courant et permettant ensuite de mettre le produit en sécurité jusqu'au retour du courant. La batterie se recharge sur l'alimentation extérieure du concentrateur.



La batterie peut ne pas avoir le temps de se recharger si le concentrateur est soumis à des coupures de courant trop fréquentes ou trop longues.

Si l'état de la batterie ne permet pas d'envoyer immédiatement l'alarme de perte d'alimentation, celle-ci sera envoyée au redémarrage du concentrateur.

2.4.2 Réseau cellulaire

Le concentrateur WebdynSunPM intègre un modem compatible avec les réseaux 2G/3G ou 2G/4G.

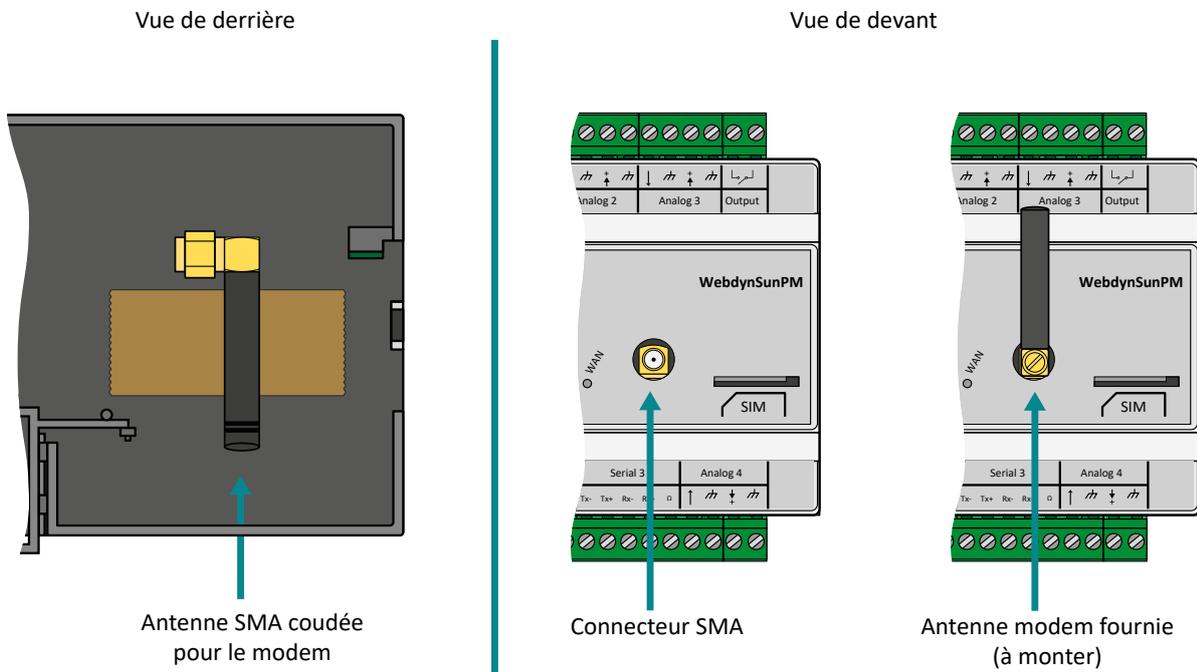
2.4.2.1 Antenne

Le concentrateur possède un connecteur SMA femelle disponible sur la face avant du produit afin de raccorder une antenne pour le modem. Le produit est livré avec une antenne SMA soudée scotchée sur l'arrière du boîtier. Elle peut être remplacée par une autre antenne compatible.



Dans le cas où le concentrateur WebdynSunPM 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.

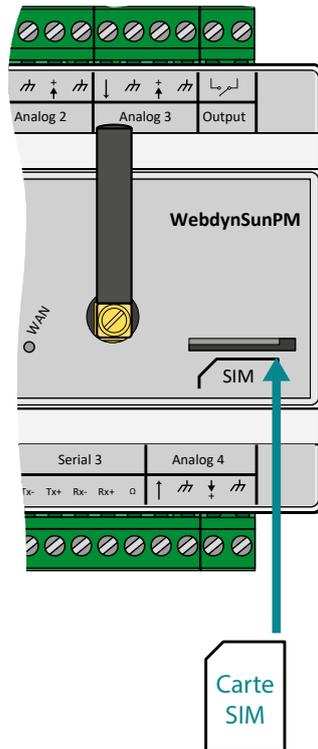
2.4.2.2 Carte SIM

Pour utiliser la liaison Modem 2G/3G ou 2G/4G et permettre au concentrateur de communiquer avec le ou les serveurs distants, il faut insérer une carte SIM au format mini SIM dans le logement de carte SIM présent en face avant 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 WebdynSunPM, vous devez insérer une carte SIM disposant des caractéristiques suivantes :

- Possibilité de recevoir et d'envoyer des SMS (préférable mais pas nécessaire).
- Communication 2G/3G ou 2G/4G inclus.



Il est recommandé d'éteindre le concentrateur avant l'insertion ou le retrait de la carte SIM afin d'éviter toutes décharges électrostatiques.

Pour insérer la carte SIM dans le produit, il faut introduire la carte SIM dans la fente en face avant du concentrateur jusqu'à entendre un clic.

Pour le retrait de la carte SIM du concentrateur, appuyer brièvement sur le bout de carte SIM dépassant du produit jusqu'à entendre un clic puis relâcher la carte. Ensuite vous pouvez récupérer la carte SIM.



Webdyn ne fournit aucune carte SIM. Veuillez vous rapprocher d'un opérateur M2M supportant le réseau 2G/3G ou 2G/4G ou d'un portail partenaire.

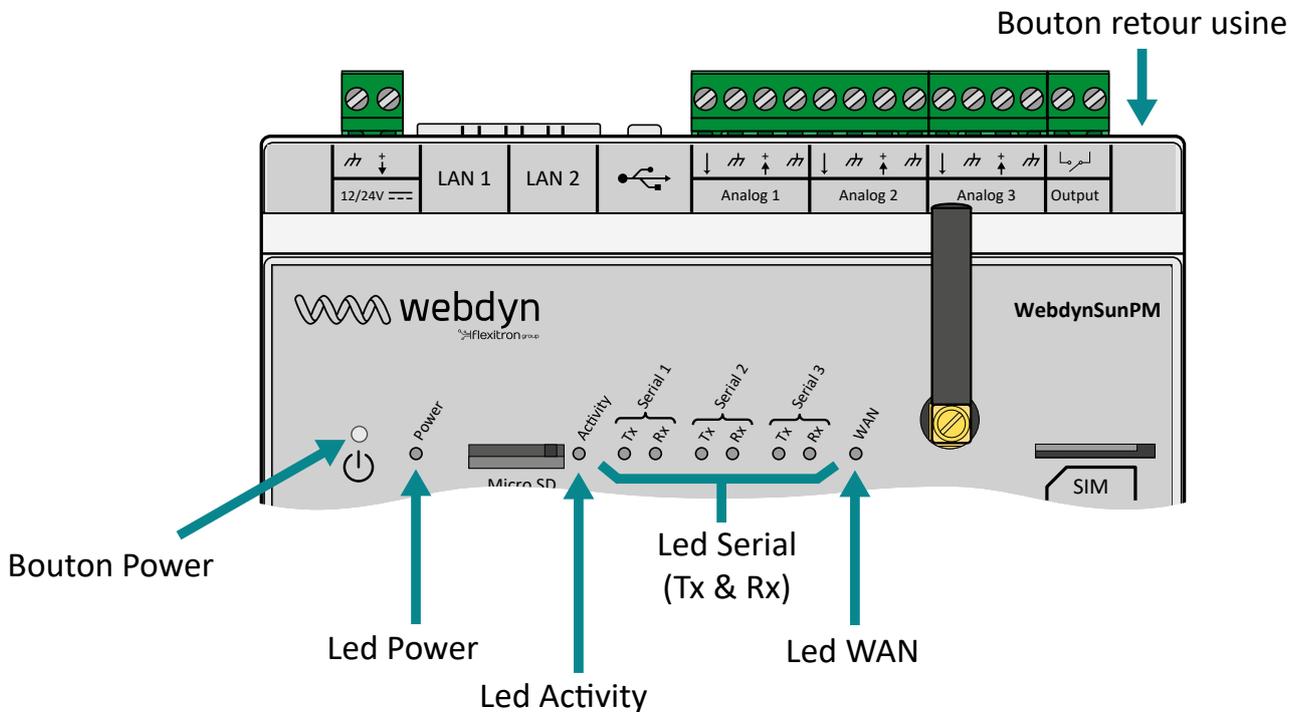


Pour connaître les informations à saisir pour la configuration du modem, veuillez vous rapprocher de votre fournisseur de cartes SIM.

2.4.3 Les voyants & boutons

Le concentrateur est équipé de :

- 2 boutons poussoirs
- 9 voyants



2.4.3.1 Bouton Power

Le bouton Power en face avant du produit permet l'extinction et le redémarrage du concentrateur.

Un appui maintenu sur le bouton Power provoque un clignotement toutes les secondes du voyant « Activity » et permet de déclencher les actions suivantes : Redémarrage du concentrateur : un appui de 2 secondes (2 impulsions de la led Activity).

- Arrêt du concentrateur : un appui supérieur à 5 secondes (5 impulsions minimum de la led Activity).

Lorsque le produit a été arrêté, ce dernier peut être rallumé par un simple appui sur le bouton Power.

2.4.3.3 Bouton Retour Usine (Factory Reset)

Le bouton Retour Usine permet la récupération du produit en toutes circonstances (perte de l'adresse IP, pertes des identifiants et mot de passe, ...).

Un appui maintenu sur le bouton Retour Usine provoque un clignotement toutes les secondes du voyant « Activity » et permet de déclencher les actions suivantes :

- Réinitialiser les paramètres IP : un appui entre 4 et 14 secondes (4 impulsions minimum et 14 impulsions maximum de la led Activity).
- Réinitialiser tous les paramètres et toutes les données : un appui supérieur à 15 secondes (15 impulsions minimum de la led Activity).

2.4.3.3 LED power

Le voyant Power représente la mise sous tension du concentrateur WebdynSunPM. Le voyant est :

- Allumé : le concentrateur fonctionne. Une tension aux bornes de l'alimentation entre 12 et 24 volts est présente.
- Éteint : le concentrateur est arrêté. Absence de tension sur le bornier d'alimentation.

2.4.3.4 LED activity

Le voyant Activity indique l'état de fonctionnement du produit qui es :

- Clignotement rapide : Intervient dans 3 cas qui sont :
 - Un des boutons est enfoncé,
 - Une mise à jour du concentrateur est en cours,
 - La phase de démarrage du concentrateur.
- Clignotement lent : Fonctionnement normal du concentrateur.



L'appui sur le bouton Power modifie le fonctionnement par défaut du voyant Activity. Pendant le maintien appuyé sur le bouton Power, le voyant Activity clignotera toutes les secondes afin d'aider l'utilisateur à réaliser une action.

2.4.3.5 LEDs serial

Le concentrateur possède 3 bus séries RS485/422 et à chaque bus un voyant Tx et un voyant RX lui sont associés.

Le voyant Tx clignotera en fonction du dialogue de transmission série sur le concentrateur (envoi du concentrateur vers un équipement). Si la led Tx ne cligne pas, cela signifie qu'il n'y a pas de transmission sur le bus série.

Le voyant Rx clignotera en fonction du dialogue de réception série sur le concentrateur (envoi d'un équipement vers le concentrateur). Si la led Rx ne cligne pas, cela signifie qu'il n'y a pas de réception sur le bus série.



Dans le cas d'un câblage 2 fils (voir chapitre 2.4.6 : « Interface Série RS485/RS422 »), les données émises par le concentrateur sont reçues en écho. Celles-ci ne provoquent pas le clignotement des voyants « Rx ».

2.4.3.6 LED WAN

Le voyant WAN a pour objectif d'aider l'utilisateur à connaître l'état de la connexion. Le voyant peut prendre 3 couleurs différentes (vert, orange et rouge) et dépend de la configuration du serveur primaire.

Serveur primaire sur interface Ethernet :

Voyant WAN	État	Signification
	Éteint	Aucune tentative de connexion
vert	Clignote lentement	Dernière connexion FTP/WebDAV OK
vert	Clignote rapidement	Connexion FTP/WebDAV en cours
orange	Clignote lentement	Problème de synchronisation NTP
rouge	Clignote lentement	Problème de connexion FTP/WebDAV

Serveur primaire sur interface Modem :

Voyant WAN	État	Signification
	Éteint	Aucune tentative de connexion
vert	X clignotements lents suivis d'une pause de 1 seconde	Indique le signal du modem par clignotement : 1. Instable 2. Limite 3. Correct 4. Bon 5. Excellent
vert	Clignote rapidement	Connexion FTP/WebDAV en cours
orange	Clignote lentement	Problème de synchronisation NTP
rouge	Clignote lentement	Problème de connexion FTP/WebDAV
rouge	Clignote rapidement	Problème d'accroche au réseau mobile ou niveau de signal de réception instable (RSSI < -89 dBm)
rouge	Fixe	Erreur carte SIM (absente, manque le code PIN, code PUK)

Serveur primaire sur interface « SD Card » :

Voyant WAN	État	Signification
	Éteint	Aucune tentative d'utilisation de la carte SD
vert	Clignote lentement	Indique que la configuration est correcte : la carte SD a bien été détectée
rouge	Fixe	Erreur carte SD. La carte SD n'a pas été détectée. Vérifier qu'elle a bien été insérée
rouge	Clignote rapidement	Erreur carte SD. Une erreur d'écriture a été détectée sur la carte SD. Vérifiez qu'elle est bien formatée et que les répertoires ont tous été correctement créés. Le cas échéant, un remplacement de la carte SD est recommandée



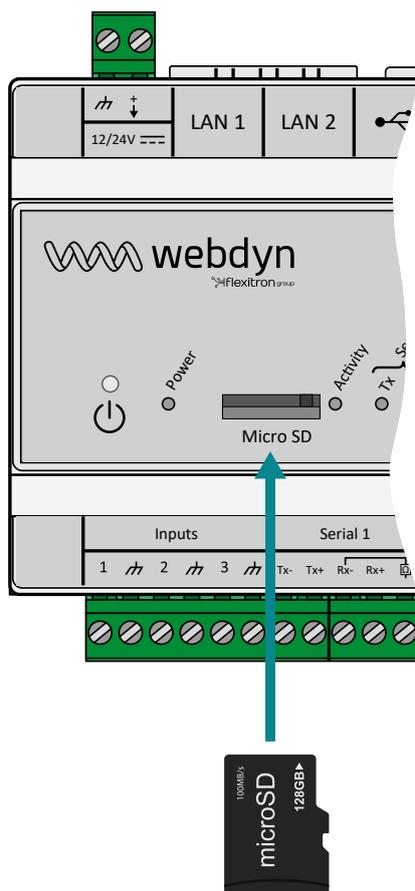
Si une erreur survient, la led WAN reste sur la dernière erreur jusqu'à la prochaine tentative concluante ou que le produit redémarre.

2.4.4 Interface d'extension

2.4.4.1 Support de mémoire externe (MicroSD)

Un emplacement micro SD est disponible en face du concentrateur. La WebdynSunPM est compatible avec les cartes micro SDXC (15 x 11 mm) avec une capacité allant jusqu'à 32 Go.

La carte SD est utilisée pour stocker la configuration, effectuer des mises à jour, ou mémoriser les données relevées des différents équipements localement, permettant ainsi de s'affranchir d'un serveur distant.



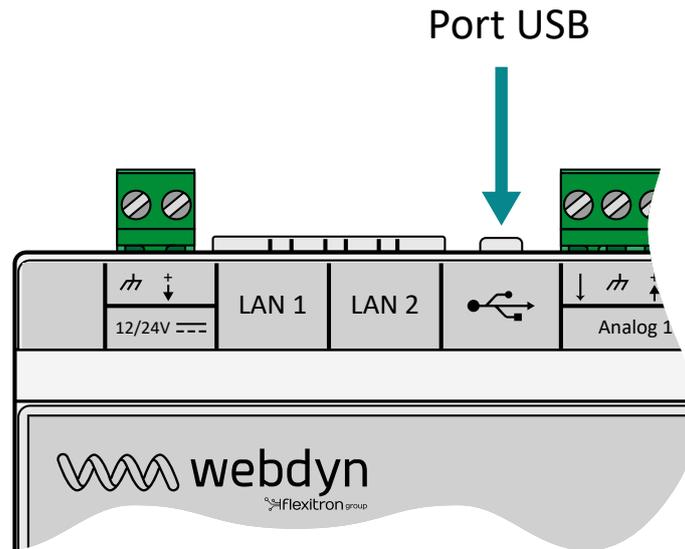
Pour insérer la carte microSD dans le produit, il faut introduire la carte microSD dans la fente en face avant du concentrateur jusqu'à entendre un clic.



Webdyn ne fournit aucune carte SD. Veuillez vous rapprocher d'un revendeur de matériel informatique.

2.4.4.2 Interface USB

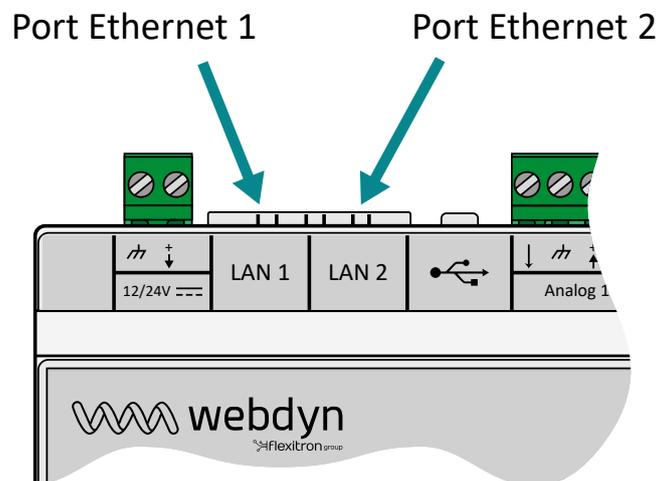
Un port USB est disponible au-dessus du produit à côté des connecteurs LAN et des entrées analogiques. Le port USB est utilisé pour connecter l'accessoire TIC afin de procéder à la télérelève d'information des compteurs électriques.



2.4.5 Interface Ethernet

Le concentrateur WebdynSunPM possède 2 interfaces Ethernet (LAN1 et LAN2) indépendantes l'une de l'autre.

Ces interfaces Ethernet permettent au concentrateur d'appartenir à 2 réseaux Ethernet différents pour communiquer avec des équipements IP locaux appartenant à 2 réseaux distincts ou de communiquer avec le SI en Ethernet.



Paramètres par défauts des ports Ethernet :

Paramètres	LAN1	LAN2
Adresse IP	192.168.1.12	192.168.2.12
Masque de sous-réseau	255.255.255.0	255.255.255.0

Les ports Ethernet supportent et comprennent chacun :

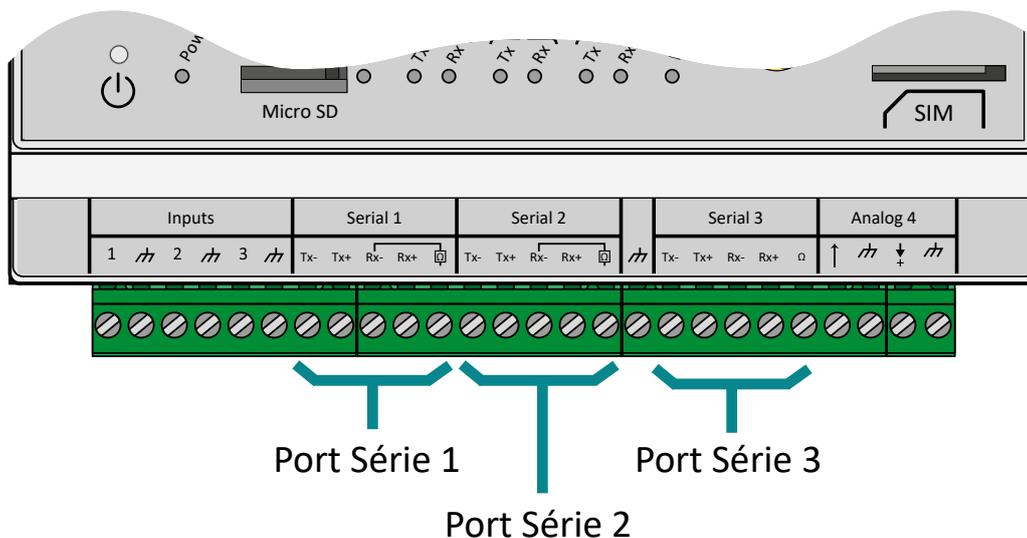
- Une liaison 10Base / 100Base-Tx IEEE 802.3.
- 2 voyants :
 - « Link » (vert) : Permet de contrôler que le lien physique avec un autre équipement réseau est disponible.
 - « Status » (orange) : Permet de visualiser le trafic réseau. Elle clignote en fonction du trafic.
- Une détection et un croisement automatiques du signal,
- Une autonegociation de la vitesse (10/100 Mbps) et du mode (half/full duplex).



Si vous souhaitez raccorder plusieurs équipements IP sur le même réseau, ces équipements doivent avoir des adresses IP différentes mais appartenant toujours au même sous réseau. Ne jamais utiliser 2 fois la même adresse IP.

2.4.6 Interface Série RS485/RS422

Le concentrateur WebdynSunPM possède 3 ports séries RS485/422 identifiés « Serial » sur le bas du produit et qui sont utilisés uniquement pour le Modbus en mode RTU. 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 » appelé également « daisy chain ». 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 WebdynSunPM 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 ci-dessous)

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. (pour 19200 bauds max). Si la longueur est élevée, pensez à réduire la vitesse de transmission des équipements si la communication est difficile.

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 « Serial » en respectant les affectations dans votre bus de communication RS485.

La norme RS485 impose un niveau différentiel d'au moins 200 mV pour la détection du niveau de signal. Pour cela des résistances de polarisation doivent être mises sur une des extrémités du bus, généralement au niveau du maître. Pour vérifier la bonne polarisation, une méthode simple consiste à positionner la source de polarisation au début du bus (côté maître) et de vérifier le niveau de tension à l'autre extrémité du bus. La borne commune (masse) doit être interconnectée aux bornes correspondantes de chaque appareil pour assurer l'équilibre de tension entre elles. Si le conducteur commun n'est pas installé entre tous les appareils, ils doivent être correctement mis à la terre conformément aux recommandations du fabricant de chaque équipement du réseau. Cette exigence entraîne l'utilisation d'un fil supplémentaire, qui, bien que ne participant pas au processus de communication, est essentiel pour assurer l'intégrité électrique des équipements du réseau.



Pour plus d'informations concernant les normes RS485/RS422 et le câblage des équipements, veuillez vous référer aux normes EIA-485 et EIA RS-422-A.

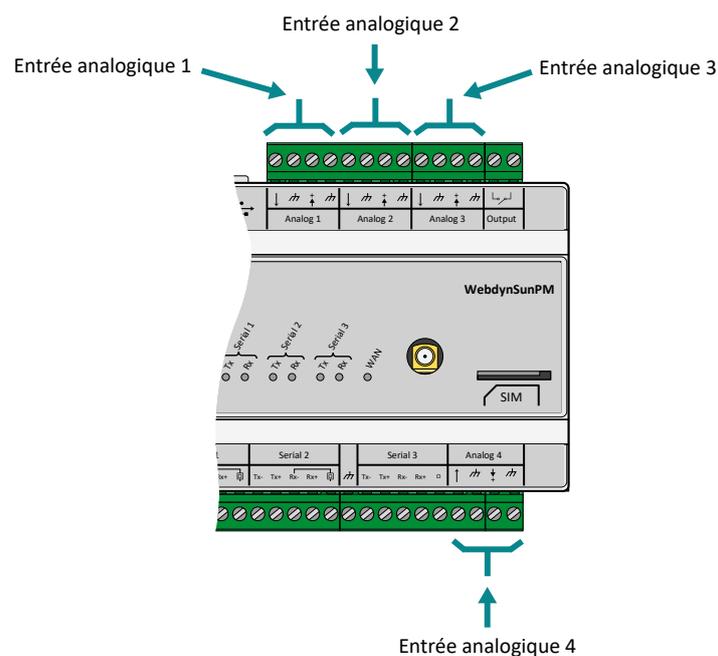
2.4.7 Interface Entrées/Sorties

La WebdynSunPM est équipée de :

- 4 entrées analogiques
- 3 entrées numériques
- 1 sortie relais

2.4.7.1 Entrées analogiques 0-10V ou 4-20mA

La WebdynSunPM possède 4 entrées analogiques identifiées « Analog » permettant mesurer un courant compris entre 4 et 20 mA ou une tension comprise entre 0 et 10 V. Chaque bornier analogique a une sortie alimentation pouvant être utilisée pour alimenter un capteur. La valeur de la tension délivrée par cette sortie alimentation est égale à la tension d'alimentation du concentrateur. Les masses présentes sur chaque bornier analogique sont toutes communes.



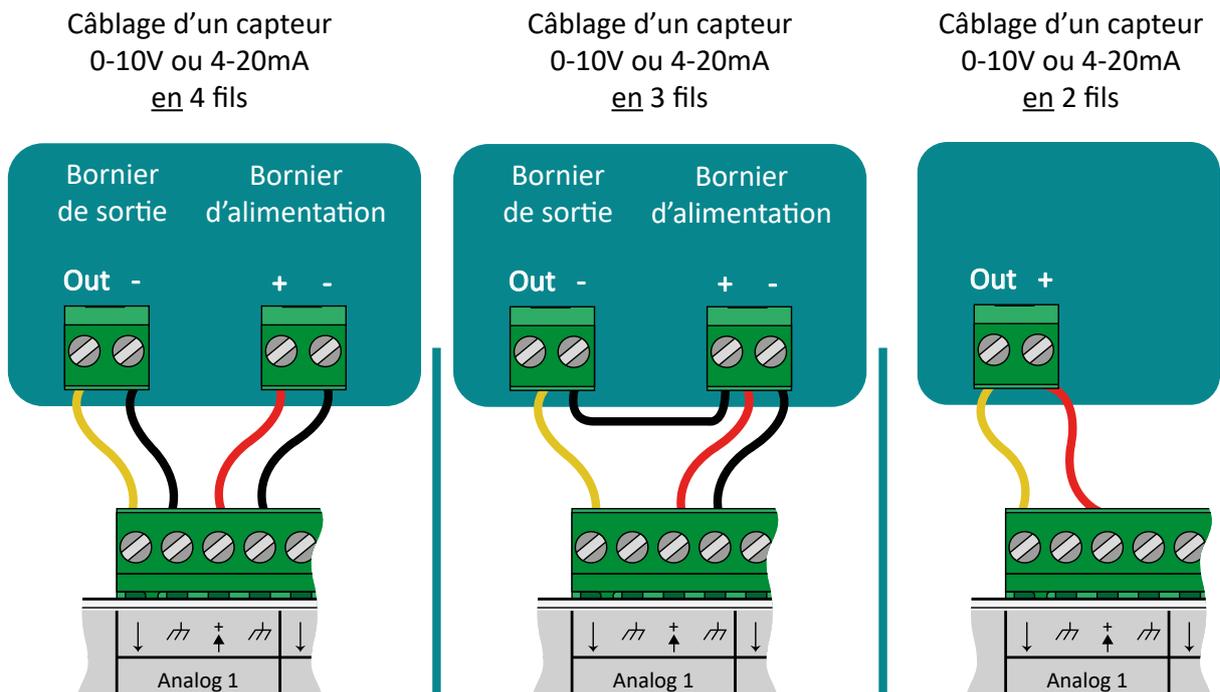
Chaque entrée analogique peut être configurée logiquement en 0-10V ou en 4-20mA.

Les convertisseurs analogiques/numériques (CAN) du concentrateur ont une résolution de 12 bits qui permet d'obtenir en :

- Mode 0-10 V : une résolution de 2,578 mV
- Mode 4-20 mA : une résolution de 5,249 μ A



Pour réaliser le raccordement, veuillez mettre hors tension le concentrateur et le capteur 0-10V ou 4-20mA. Prenez en compte les informations de câblage fournies par le fabricant du capteur.



Ne pas appliquer une tension supérieure à 12V ou un courant supérieur à 24mA sur les entrées analogiques.

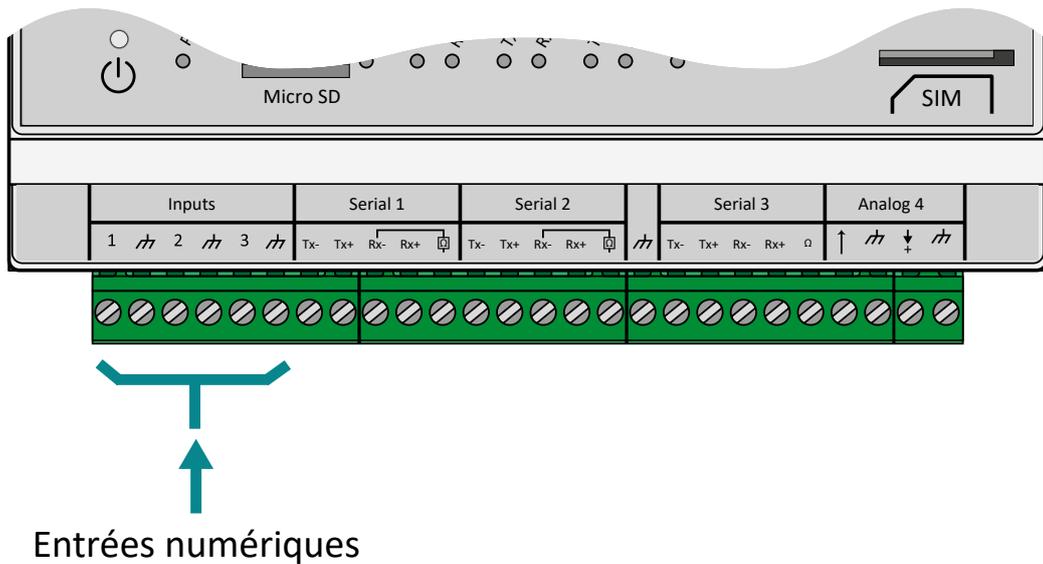


La tension disponible sur le bornier pour les capteurs est identique à celle du bloc alimentation permettant d'alimenter le concentrateur. La puissance maximum disponible pour l'ensemble des capteurs ne doit pas dépasser les 7 watts.

2.4.7.2 Entrées numériques TOR/S0 (impulsionnelle)

Le concentrateur WebdynSunPM possède 3 entrées configurables en mode TOR (Tout Ou Rien) ou en mode S0 impulsionnelle (comptage d'impulsions).

Ces entrées sont situées en bas à gauche du concentrateur WebdynSunPM.



La longueur de câble de ces entrées ne doit pas dépasser les 100m.

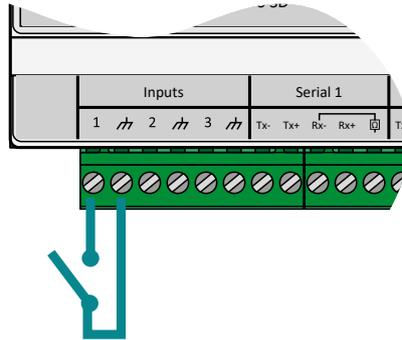


Afin d'éviter toutes détériorations du contracteur, ne pas injecter de courant ou de tension sur les entrées numériques.

En mode TOR : le concentrateur peut détecter les ouvertures et les fermetures de contacts secs pour remonter l'état d'un équipement ou pour déclencher des alarmes sur changement d'état.

Entrées TOR	Entrées numériques
Type	Collecteur ouvert / Drain ouvert / Contact Sec
Tension / Courant Max	4mA @5V
Seuil de commutation inactif « 0 »	> 3.5 V
Seuil de commutation actif « 1 »	< 1 V
Compteurs d'impulsions	> 20 ms

Câblage d'une entrée en TOR

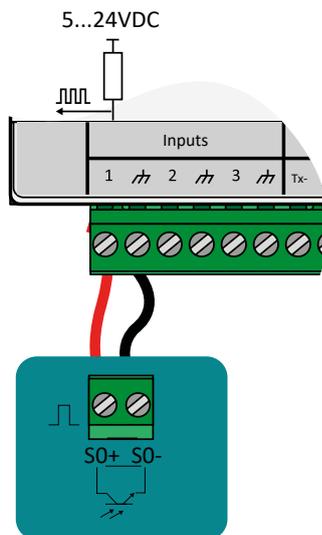


En mode S0 (impulsionnelle) : le concentrateur WebdynSunPM gère des compteurs qui ont des sorties impulsionnelles de classe A (24 V) et B (5 V) selon la norme CEI 62053-31:1998.

Le concentrateur a un fonctionnement de type « Sink », c'est-à-dire qu'une tension est appliquée à borne SO+ du compteur au moyen d'une résistance (interne) de pull-up et une tension de 0V est appliquée à la connexion SO- du compteur.

Entrées S0 impulsions	Classe A (24V) Impulsions de courant	Classe B (5V) Impulsions de courant
Seuil de commutation inactif « LOW »	< 8 mA	< 1 mA
Seuil de commutation actif « HIGH »	> 15 mA	> 2,5 mA
Tension d'alimentation	Interne 24 V	Interne 5 V
Compteurs d'impulsions	> 20ms	> 20ms

Câblage d'une entrée en S0



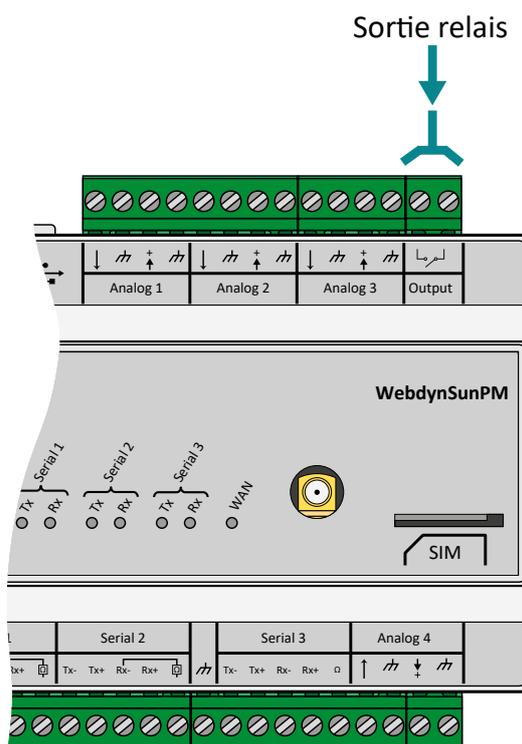
Un compteur avec sortie d'impulsion de classe A doit être utilisé pour les transmissions sur de longues distances. Un compteur avec sortie d'impulsion de classe B peut être utilisée uniquement pour de courtes distances et permet d'avoir une consommation de puissance réduite.



Si le concentrateur n'est pas alimenté en 24V, alors les impulsions en classe A risquent de ne pas fonctionner. La tension pour la classe A sera celle du bloc alimentation connectée au concentrateur.

2.4.7.3 Sortie Relais

Le concentrateur WebdynSunPM possède une sortie relais libre de tout potentiel.



Les caractéristiques de cette sortie sont les suivants :

Caractéristiques	Valeurs MAX
Tension	24 V
Courant	1A



Le relais du concentrateur ne permet pas de piloter directement de forte puissance. Dans ce cas, il est nécessaire d'utiliser un relais externe intermédiaire.

La sortie relais est pilotable par :

- Fichier de commande (FTP, SFTP ou WebDAV), message MQTT/MQTTS et SMS. (Voir chapitre 5.3.9 : « « setRelay » : Modification de l'état du relais »).
- Scripts LUA. (Voir chapitre 3.2.3.1 : « Scripts »).

3. Configuration

La configuration du concentrateur peut se faire de plusieurs manières :

- Par le biais de fichiers de configuration déposés sur un serveur FTP, SFTP ou WebDAV-HTTPS
- Par le biais de fichiers de configuration déposés sur une carte micro SD
- Par le biais de l'interface web du concentrateur
- Par le biais de commandes SMS

L'utilisation d'un serveur a configuration par FTP/SFTP/WebDAV-HTTPS est la solution privilégiée pour la configuration et maintien à distance des équipements afin d'assurer l'entretien du parc. En cas de modification simultanée par l'interface web locale et les fichiers FTP, ce sont ces derniers qui seront prioritaires. Toute modification des fichiers sur le serveur FTP écrasera des modifications éventuelles effectuées en local.

Il est à noter que pour le premier démarrage, il faut au minimum configurer les éléments suivants en utilisant les SMS (voir chapitre 5.2.3 : « SMS »)ou l'interface web locale (voir chapitre 3.2.2.5 : « Serveurs (servers)Serveurs (servers) ») :

- Nom du serveur FTP.
- Identifiants sur le serveur FTP : login et mot de passe.
- Interface à utiliser : modem ou Ethernet configurés correctement pour accéder à des équipements extérieurs.

Les commandes SMS permettent un certain nombre de requêtes basiques afin de lancer la récupération des fichiers de configuration sur le serveur FTP. Elles ne peuvent en aucun cas se substituer à une configuration complète par FTP ou par le web.

3.1 FTP/SFTP/WebDAV

Comme indiqué précédemment, ce mode de configuration est prioritaire sur la configuration locale par le biais de l'interface web.

Ce mode de fonctionnement nécessite un serveur FTP, SFTP ou WebDAV accessible par le concentrateur. Ce serveur est accessible via une adresse, un identifiant de connexion (login) et un mot de passe.

Le serveur peut être hébergé sur n'importe quel type de serveur (Windows, Linux, etc.). L'important est que son adresse soit accessible par le concentrateur en utilisant l'interface réseau qui sera configurée (Ethernet ou modem). Il est à noter que les serveurs FTP sous Windows ne peuvent gérer la casse dans les noms de fichiers. Il est donc conseillé, afin d'éviter tout souci, de n'utiliser que des serveurs FTP sous Linux.

Il est préférable d'utiliser un serveur SFTP ou WebDAV en raison de couches de sécurité supplémentaires par rapport à un serveur FTP classique. En dehors de cela, le fonctionnement des différents types de serveurs est le même. SFTP basé sur login et mot de passe.

3.1.1 Principe de fonctionnement

La gestion de la configuration repose sur une arborescence de répertoires et de fichiers sur un serveur FTP, SFTP ou WebDAV.

Par défaut, l'identifiant du concentrateur (uid) est calculé en fonction de l'adresse MAC du produit., en prenant les 6 derniers caractères de celui-ci préfixés de « WPM ». Ainsi, pour un produit dont l'adresse MAC est « 00:8D:00:00:BD:E4 », l'uid par défaut sera « WPM00BDE4 ».

Cet uid est ensuite utilisé pour préfixer tous les fichiers de configuration déposés sur le serveur. C'est pour cela qu'il est indispensable que cet uid soit unique sur l'ensemble de l'installation.

Les fichiers se décomposent comme suit :

- Fichiers de configuration du concentrateur : ce sont les fichiers qui contiennent les données propres au concentrateur. Par défaut ils sont stockés dans le répertoire « /CONFIG » du serveur.
- Fichiers de définition des équipements : ce sont les fichiers qui vont permettre de configurer/gérer les différents équipements reliés au concentrateur. Par défaut ils sont stockés dans le répertoire « /DEF » du serveur.

Il est à noter que le concentrateur ne crée pas l'arborescence configurée. Il est donc nécessaire de créer manuellement tous les répertoires configurés. Ainsi, par défaut, il faut, au minimum que les répertoires suivants soient présents sur le serveur :

- /CONFIG
- /ALARM
- /LOG
- /BIN
- /CERT
- /DATA
- /CMD
- /DEF
- /SCRIPT

Ces répertoires doivent avoir des droits en lecture et écriture pour l'utilisateur configuré. (Voir chapitre 4.1 : « Le serveur FTP/SFTP /WebDAV ») Pour plus de détails sur les différents droits d'accès requis.

Il est possible de configurer 2 serveurs distincts. Les 2 serveurs sont utilisés pour le dépôt des données et la sauvegarde de la configuration.

Le serveur 1 est appelé serveur principal, le serveur 2 est appelé serveur secondaire.

En revanche, en cas de modification des fichiers sur le serveur, seuls les fichiers du serveur principal sont pris en compte. Il n'y a donc pas de risque de conflit en cas de modification des fichiers de configuration sur les deux serveurs.

Les modifications effectuées sur le serveur principal seront répercutées sur le serveur secondaire à la prochaine connexion.

3.1.2 Fichiers de configuration

Les fichiers de configuration sont de plusieurs sortes.

On retrouve les fichiers pour configurer le fonctionnement du concentrateur (connexion au serveur, gestion NTP, mots de passe, modem, etc.) ainsi que les fichiers de définition des équipements connectés.

Tous ces fichiers sont décrits dans cette section.

Lorsque les fichiers sont modifiés sur le serveur principal, les modifications sont reportées sur le serveur secondaire configuré.

3.1.2.1. Fonctionnement du concentrateur

Les fichiers de configuration du concentrateur se trouvent dans le répertoire de configuration spécifié. Par défaut « /CONFIG ».

Les fichiers sont les suivants :

- <uid>_config.ini : ce fichier contient les éléments de configuration suivants :
 - Configuration de l'arborescence du serveur
 - Configuration du type de serveur : FTP, SFTP, WebDAV, MQTT, etc.
 - Configuration NTP
 - Nom et description du concentrateur
- <uid>_scl.ini : ce fichier contient les paramètres de configuration des scripts installés sur le concentrateur
- <uid>_var.ini : ce fichier contient les paramètres de configuration de la planification des connexions du concentrateur
- <uid>_daq.csv : ce fichier contient la configuration des interfaces de connexion du concentrateur et des équipements supervisés, à savoir :
 - Configuration du modem :
 - Code PIN
 - APN
 - Login/mot de passe/type d'authentification

- Configuration de l'interface Ethernet :
 - Adresse IP
 - Passerelle
 - DNS
- Configuration des ports série :
 - Vitesse
 - Parité
 - Bits de données
 - Type de protocole utilisé : Modbus, etc.
- Déclaration de chaque équipements connectés :
 - Index
 - Nom
 - Interface
 - Adresse
 - Fichier de définition
- `<uid>_licence.ini` : ce fichier contient les licences des scripts Lua Webdyn « .luaw »

Avec `<uid>` l'identifiant du concentrateur.

3.1.2.1.1 Fichier « `<uid>_config.ini` »

A minima, pour assurer la communication avec le concentrateur, il faut prévoir un certain nombre de paramètres dans ce fichier de configuration.

Tout d'abord, définir le nom du fichier de configuration : Il faut prendre l'uid de l'appareil, comme déterminé plus haut, et suffixer de « `_config.ini` ». Ainsi, dans l'exemple ci-dessus, le fichier généré se nommera « `WPM00BDE4_config.ini` ».

Si la configuration de base est faite avec le serveur web embarqué, alors ce fichier est automatiquement créé à la première connexion du concentrateur.

Lors de la connexion au serveur distant, si le fichier est détecté, il est téléchargé et la configuration est immédiatement appliquée, quelle que soit la configuration locale.

Pour un serveur FTP ou SFTP :

- `SERVER_Address=<Adresse ou nom de du serveur FTP/SFTP à utiliser pour la configuration>`
- `SERVER_TYPE=ftp ou sftp`
- Si la connexion se fait par Ethernet :

- SERVER_Interface=Ethernet
- Si la connexion se fait par modem :
 - SERVER_Interface=modem
- FTP_Login=<Nom du login à utiliser pour le serveur>
- FTP_Password=<Mot de passe associé au login>

Pour un serveur WebDAV-HTTPS :

- SERVER_Address=<Adresse ou nom du serveur WebDAV-HTTPS>
- SERVER_TYPE=webdav
- Si la connexion se fait par ethernet :
 - SERVER_Interface=ethernet
- Si la connexion se fait par modem :
 - SERVER_Interface=modem (par défaut)

Le détail des paramètres de configuration pour ce fichier se trouve dans la section 10.1 Annexe A : Fichier de configuration « _config.ini ».

Pour un serveur MQTT :

La WebdynSunPM peut se connecter à un serveur MQTT afin d'y déposer ses données et ses alarmes. Il est également possible de passer des commandes au concentrateur par le serveur MQTT. Pour cela , il faut indiquer les topics souscrits au concentrateur dans son paramétrage.

Le paramétrage du concentrateur ne peut pas être fait par le serveur MQTT, pour cela il faudra soit passer par un serveur FTP ou soit utiliser l'interface web embarquée.

Le concentrateur supporte 5 types différents de serveur MQTT, qui sont :

- MQTT : serveur MQTT sans sécurité.
- MQTTS : serveur MQTT sécurisé.
- MQTTS aws : serveur « AWS IoT » d'Amazon.
- MQTTS gcloud : serveur « Google Cloud IoT » de Google.
- MQTTS azure : serveur « Azure IoT Hub » de Microsoft.

Veuillez-vous rapprocher du gestionnaire du serveur MQTT afin d'obtenir le paramétrage à effectuer ainsi que les certificats et les clés sécurisées à importer sur le concentrateur.

Le détail des paramètres de configuration pour ce fichier se trouve dans la section 10.1 Annexe A :

Fichier de configuration « _config.ini ».



Pour les serveurs MQTTs, des certificats sont à importer dans le concentrateur. Ces certificats ont une durée de vie, il est à votre charge de les renouveler et de les importer avant leur expiration.

3.1.2.1.2 Fichier « <uid>_var.ini »

Le fichier « _var.ini » contient la liste des planifications configurées sur le concentrateur.

Le nom du fichier est défini comme suit : Il faut prendre l'uid de l'appareil, comme déterminé plus haut, et suffixer de « _var.ini ». Ainsi, dans l'exemple ci-dessus, le fichier généré se nommera « WPM00BDE4_var.ini ».

Si la configuration de base est faite avec le serveur web embarqué, alors ce fichier est automatiquement créé à la première connexion du concentrateur.

Lors de la connexion au serveur distant, si le fichier est détecté, il est téléchargé et la configuration est immédiatement appliquée, quelle que soit la configuration locale.

Le fichier comporte une ligne par planification configurée. Chaque ligne contient le numéro de la planification ainsi que les paramètres correspondants.

Le format est le suivant :

Variable	Définition	Valeur par défaut
SCHEDULE_Params[n]	Paramètres de la planification pour la connexion Server 1	
SCHEDULE2_Params[n]	Paramètres de la planification pour la connexion Server 2	

Où « n » est remplacé par le numéro d'index de la planification. Ce numéro commençant à 0.

Les paramètres pour chaque ligne sont au format suivant :

```
SCHEDULE_Params[index]=Id|Type|StartTime|Interval|Count
```

Chaque ligne configurée contient donc les informations de paramétrage suivantes :

Paramètre	Description	Valeur par défaut
Id	L'identifiant de la ligne de la configuration. Cet identifiant doit être unique.	

Type	Indique le type de planification. Les valeurs autorisées sont : <ul style="list-style-type: none"> • everyday : la planification sera exécutée tous les jours • monday : la planification se fera tous les lundis • tuesday : la planification se fera tous les mardis • wednesday : la planification se fera tous les mercredis • thursday : la planification se fera tous les jeudis • friday : la planification se fera tous les vendredis • saturday : la planification se fera tous les samedis • sunday : la planification se fera tous les dimanches • first : la planification se fera tous les 1er du mois • middle : la planification se fera tous les 15 du mois • last : la planification se fera le dernier jour de chaque mois. 	Everyday
StartTime	Indique l'heure de démarrage de la tâche sous la forme suivante : « HH:MM:SS ».	00:00:00
Interval	Indique la fréquence de répétition de la connexion en minutes.	1440
Count	Indique le nombre maximal de connexions à établir dans la journée	1

Ainsi, avec la planification suivante sur la connexion Schedule 1 :

Mode	Start time	Interval	Count			
Everyday	00:00:00	1440	1			
Monday	00:00:00	1440	1			
First day of each m	00:00:00	1440	1			
15th of each m	01:00:00	600	2			
Last day of each m	02:02:00	120	12			

Et la planification suivante pour la connexion Schedule 2 :



Mode	Start time	Interval	Count			
Everyday	00:00:00	1440	1			
Everyday	00:00:00	3600	1			
Everyday	00:00:00	86400	1			

On obtient alors le fichier de configuration suivant :

```
SCHEDULE_Params[0]=1|everyday|00:00:00|1440|1
SCHEDULE_Params[1]=2|monday|00:00:00|1440|1
SCHEDULE_Params[2]=3|first|00:00:00|1440|1
SCHEDULE_Params[3]=4|middle|01:00:00|600|2
SCHEDULE_Params[4]=5|last|02:02:00|120|12
SCHEDULE2_Params[0]=1|everyday|00:00:00|1440|1
SCHEDULE2_Params[1]=2|everyday|00:00:00|3600|1
SCHEDULE2_Params[2]=3|everyday|00:00:00|86400|1
```

Le numéro d'index est calculé automatiquement par le concentrateur en commençant par 0. En cas de modification manuelle de ce fichier, il faut veiller à ce qu'il n'y ait pas de doublon de numéro d'index, sans quoi la configuration sera refusée. Il est à noter que le numéro d'index est indépendant pour « SCHEDULE_Params » et « SCHEDULE2_Params ».

3.1.2.1.3 Fichier « <uid>_daq.csv »

Le fichier « <uid>_daq.ini » contient la liste des équipements configurés sur le concentrateur et le paramétrage de leurs interfaces.

Le nom du fichier est défini comme suit : Il faut prendre l'uid de l'appareil, comme déterminé plus haut, et suffixer de « _daq.csv ». Ainsi, dans l'exemple ci-dessus, le fichier généré se nommera « WPM00BDE4_daq.csv ».

Si la configuration de base est faite avec le serveur web embarqué, alors ce fichier est automatiquement créé à la première connexion du concentrateur.

Lors de la connexion au serveur distant, si le fichier est détecté, il est téléchargé et la configuration est immédiatement appliquée, quelle que soit la configuration locale.

Contrairement aux fichiers précédents, celui-ci est au format CSV (séparateur « ; »), c'est-à-dire éditable directement avec un tableur, comme Microsoft Excel®.

Ce fichier est séparé en 4 parties distinctes :

- Configuration du modem
- Configuration des connexions Ethernet
- Configuration des ports série
- Configuration des équipements connectés

3.1.2.1.3.1 Configuration du modem

La configuration du modem repose sur les paramètres suivants :

Paramètre	Description	Valeur par défaut
Type	Type d'équipement. La seule valeur possible ici est « MODEM »	MODEM
Pin	Permet de préciser la valeur du code PIN du modem s'il a été défini.	
APN	Ce champ contient le nom de l'APN auquel se connecter avec la carte SIM. Cet APN dépend de l'opérateur et de l'abonnement choisi. Pour pouvoir utiliser la connexion modem, ce champ ne peut PAS rester vide.	
Login	Identifiant à utiliser pour s'authentifier lors de l'établissement de la connexion. Cet identifiant est fourni par l'opérateur et dépend de celui-ci et du type d'abonnement. Ce champ peut être vide.	
Password	Mot de passe associé à l'identifiant pour l'authentification lors de l'établissement de la connexion. Ce mot de passe est fourni par l'opérateur et dépend de celui-ci et du type d'abonnement. Ce champ peut être vide.	

Authentification	Type d'authentification à utiliser lors de la connexion. Cette valeur dépend de l'opérateur et du type d'abonnement. Cette information est fournie par l'opérateur. Les valeurs possibles sont : <ul style="list-style-type: none"> • None : Pas d'authentification demandée par le serveur distant • PAP : Authentification de type PAP demandée par le serveur distant 	None
------------------	--	------

Un exemple de configuration du modem est le suivant :

```
type;pin;apn;login;password;authentification
MODEM;;m2minternet;;;None
```

Dans cet exemple, le code PIN est vide, l'APN est fixé à « m2minternet », les login et mot de passe sont vides, et le type d'authentification est défini sur « None ».

En éditant le fichier sous Excel, on obtient l'affichage suivant avec l'utilisation du format CSV :

type	pin	apn	login	password	authentification
MODEM		m2minternet			none



En cas de modifications du fichier avec un tableur type « Excel », il se peut que le format soit modifié et que les séparateurs « ; » soient remplacés par le caractère « , », le rendant inutilisable par le concentrateur. Veillez à toujours bien préciser le format du séparateur lors d'une sauvegarde.

3.1.2.1.3.2 Configuration des connexions Ethernet

La configuration des interfaces Ethernet repose sur les paramètres suivants :

Paramètre	Description	Valeur par défaut
Type	Type d'équipement. Les valeurs possibles sont : <ul style="list-style-type: none"> • LAN1 : pour la configuration de l'interface LAN 1 • LAN2 : pour la configuration de l'interface LAN 2 	LAN1 pour la première ligne LAN2 pour la seconde ligne
Ip	Adresse IP locale affectée à l'interface Ethernet. Cette valeur affecte l'adresse IP locale à laquelle le boîtier pourra être contacté sur l'interface Ethernet en question. Ce champ ne peut pas être laissé vide	192.168.1.12 pour la première ligne 192.168.2.12 pour la seconde ligne

Mask	Ce champ contient la valeur du masque de sous-réseau utilisée conjointement avec l'adresse IP configurée. Ce champ ne peut pas être laissé vide	255.255.255.0
Gateway	Configuration de l'équipement de routage à utiliser pour que le concentrateur puisse communiquer avec des équipements non présents sur son réseau local.	
	Adresse IP d'un serveur DNS à utiliser pour la résolution des noms par le concentrateur.	
DNS1	Adresse IP d'un serveur DNS à utiliser pour la résolution des noms par le concentrateur au cas où le serveur « DNS1 » ne répond pas.	

Un exemple de configuration des interfaces Ethernet est le suivant :

```
type;ip;mask;gateway;dns1;dns2
LAN1;192.93.121.37;255.255.255.0;192.93.121.1;192.93.121.8;
LAN2;192.168.2.12;255.255.255.0;;;
```

Dans cet exemple, la première interface réseau (LAN 1) est configurée à l'adresse IP « 192.93.121.37 », avec un masque de sous-réseau à « 255.255.255.0 » qui lui permet d'accéder à toutes les machines connectées avec l'adresse « 192.93.121.xxx ».

Cette interface utilise également un routeur à l'adresse « 192.93.121.1 » pour communiquer avec les équipements extérieurs et un serveur DNS accessible à l'adresse « 192.93.121.8 ». Il n'y a pas de DNS2 configuré.

De même la seconde interface réseau est laissée avec sa configuration par défaut, à savoir une adresse IP sur « 192.168.2.12 », et un masque de sous-réseau à « 255.255.255.0 ». Tous les autres paramètres sont vides.

Configuration de l'intertrame Ethernet :

Dans le cas d'une utilisation de ces interfaces réseaux pour la collecte de donnée sur un équipement à superviser, il peut être nécessaire d'espacer l'envoi des requêtes pour ne pas saturer l'équipement interrogé. Pour ce faire, on configure le paramètre intertrame ethernet ainsi :

```
tcpInterFrameMs;<value>
```

Paramètre	Description	Valeur par défaut
Valeur	Délai d'attente entre 2 trames en Modbus TCP. Ce délai s'exprime en ms	0

Le principe de fonctionnement est le même que pour les ports série. À chaque fois qu'une trame est émise en ModbusTCP, le concentrateur va laisser un temps de silence correspondant à « tcpInterFrameMs » entre la réponse de l'équipement et la prochaine requête à destination des équipements sur le réseau.



Le paramètre intertrame est global, c'est-à-dire qu'il s'applique à toutes les communications ModbusTCP et peut donc provoquer des ralentissements dans la lecture des données s'il est trop élevé.

Ce paramètre doit être utilisé pour certains équipements ModbusTCP particuliers. Voir « Configuration des ports série » pour plus de détails sur le fonctionnement de ce délai inter trames.

En éditant le fichier sous Excel, on obtient l'affichage suivant avec l'utilisation du format CSV :

type	ip	mask	gateway	dns1	dns2
LAN1	192.93.121.37	255.255.255.0	192.93.121.1	192.93.121.8	0
LAN2	192.168.2.12	255.255.255.0			
tcpInter FrameMs	0				



En cas de modifications du fichier avec un tableur type « Excel », il se peut que le format soit modifié et que les séparateurs ';' soient remplacés par le caractère ',', le rendant inutilisable par le concentrateur. Veillez à toujours bien préciser le format du séparateur lors d'une sauvegarde.

3.1.2.1.3.3 Configuration des ports série

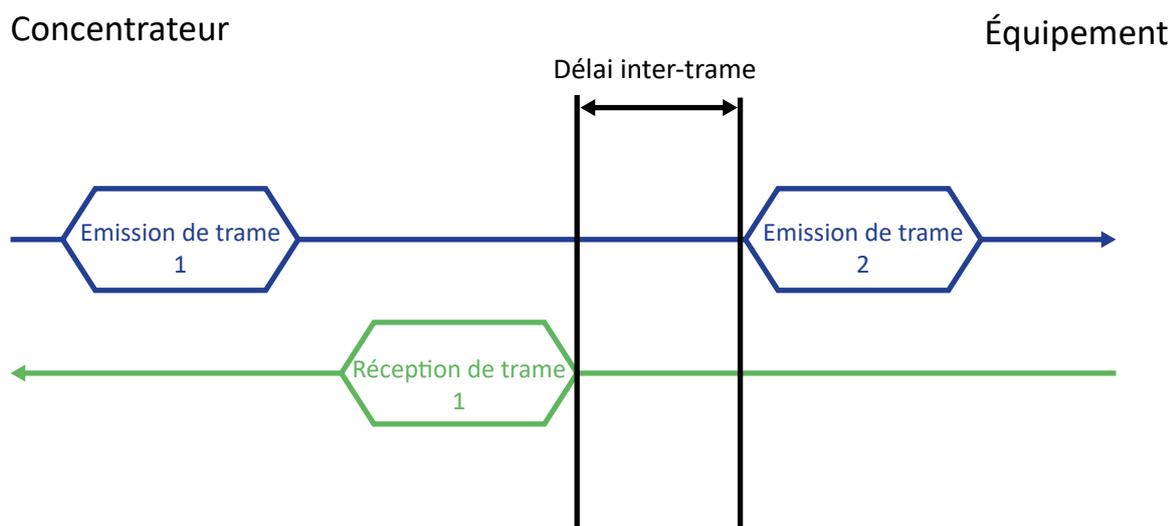
La configuration des ports série repose sur les paramètres suivants :

Paramètre	Description	Valeur par défaut
Type	Type d'équipement. Les valeurs possibles sont <ul style="list-style-type: none">• SERIAL1 : pour la configuration de l'interface « Serial 1 »• SERIAL2 : pour la configuration de l'interface « Serial 2 »• SERIAL3 : pour la configuration de l'interface « Serial 3 »	SERIAL1 pour la première ligne SERIAL2 pour la deuxième ligne SERIAL3 pour la troisième ligne
Baudrate	Vitesse à utiliser en bauds pour la liaison série. Les valeurs possibles sont <ul style="list-style-type: none">• 1200• 2400• 4800• 9600• 19200• 38400• 57600• 115200• 230400• 460800	19200
DataBits	Nombre de bits de données par octet. Les valeurs possibles sont <ul style="list-style-type: none">• 7• 8	8
Parity	Type de parité à appliquer pour la validation des données sur la liaison série. Les valeurs possibles sont <ul style="list-style-type: none">• N : pas de parité• O : parité impaire• E : parité paire	N
StopBits	Nombre de bits d'arrêt entre 2 octets. Les valeurs possibles sont <ul style="list-style-type: none">• 1• 2	1

Wires	<p>Nombre de fils à utiliser sur l'interface série.</p> <p>Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 2 : les mêmes 2 fils servent pour la réception et l'émission de trames de données • 4 : la réception et l'émission de trames de données utilisent des paires de fils séparés 	2
Protocol	<p>Le type de protocole associé à cette interface série. Les valeurs possibles sont</p> <ul style="list-style-type: none"> • ModbusRTU : le port série est dédié à la gestion des communications Modbus RTU • protocole propriétaire (voir annexe spécifique sur les protocoles propriétaires) 	ModbusRTU
InterFrame	<p>Temps d'attente entre 2 trames échangées sur le port série. Ce temps d'attente est exprimé en ms.</p> <p>Voir plus bas pour une explication détaillée du fonctionnement de ce paramètre.</p>	0
Forwarded TCP port	<p>Port Modbus transféré.</p> <p>Si ce champ est renseigné, le concentrateur ouvre un port ModbusTCP sur le numéro de port saisi.</p> <p>Lorsqu'un équipement ModbusTCP se connecte à ce port, toutes les requêtes envoyées sont transférées directement sur le bus ModbusRTU et la réponse est remontée à l'équipement connecté via ce port ModbusTCP.</p> <p>Cette option permet de créer un tunnel de communication entre un équipement ModbusTCP et le réseau ModbusRTU local.</p> <p>Les requêtes sont intercalées entre les requêtes internes de surveillance du concentrateur.</p>	

Le paramètre « InterFrame » permet de définir une période de silence sur le bus série afin de permettre à certains équipements de se remettre en attente de données. Chez certains constructeurs ce délai s'appelle le « délai de retournement ».

Le principe de fonctionnement est le suivant :



Lorsque le concentrateur reçoit une réponse de la part de l'équipement, il va imposer un délai correspondant au paramètre « InterFrame » entre le dernier octet de la dernière trame reçue et le premier octet de la trame suivante qu'il envoie à cet équipement. Ce délai est valable pour le bus complet. Donc, si une nouvelle trame est émise vers un équipement autre que le précédent, le délai sera tout de même respecté.

Un exemple de configuration des interfaces séries est le suivant :

```
type;baudrate;data_bits;parity;stop_
bits;wires;protocol;interframe (ms)

SERIAL1;9600;8;N;1;2;Modbus;0

SERIAL2;1200;8;N;1;4;SMANET;0

SERIAL3;19200;8;N;1;2;PW1;0
```

Dans cet exemple, le premier port série est configuré à 9600 bauds, 8 bits de données, pas de parité, 1 bit d'arrêt, 2 fils de communication, protocole « Modbus » et aucun délai inter-frames.

Le 2ème port série est configuré à 1200 bauds, 4 fils, pour être utilisé avec le protocole SMA-Net.

Le 3ème port série est également configuré à 19200 bauds, 2 fils, pour une utilisation avec le protocole PowerOne.

En éditant le fichier sous Excel, on obtient l’affichage suivant avec l’utilisation du format CSV :

type	br	data_b	parity	stop_bits	wires	protocol	interframe
SERIAL1	9600	8	N	1	2	Modbus	0 ms
SERIAL2	1200	8	N	1	4	SMANET	0 ms
SERIAL3	19200	8	N	1	2	PW1	0



En cas de modifications du fichier avec un tableur type « Excel », il se peut que le format soit modifié et que les séparateurs ‘;’ soient remplacés par le caractère ‘,’, le rendant inutilisable par le concentrateur. Veillez à toujours bien préciser le format du séparateur lors d’une sauvegarde.

3.1.2.1.3.4 Déclaration des équipements connectés

La configuration des interfaces équipements connectées repose sur les paramètres suivants :

Paramètre	Description	Valeur par défaut
Index	<p>Index de l’équipement à définir.</p> <p>Ce champ contient une valeur numérique avec le numéro d’identification de l’appareil à configurer. Chaque numéro doit être unique sous peine de ne pas voir l’équipement dans l’interface web.</p> <p>Les valeurs suivantes sont également acceptées pour l’index :</p> <ul style="list-style-type: none"> • IO : permet de préciser que le fichier de définition concerne les IO du concentrateur • TIC1 : permet de préciser que le fichier de définition concerne un équipement de type TIC. 	
Interface	<p>Dans le cas d’un équipement « IO » ou « TIC » ce champ n’est pas utilisé. Il doit être laissé vide.</p> <p>Dans le cas d’équipements Modbus, il contient les informations suivantes :</p> <ul style="list-style-type: none"> • SERIAL1 : l’équipement est connecté au port série 1 • SERIAL2 : l’équipement est connecté au port série 2 • SERIAL3 : l’équipement est connecté au port série 3 • « adresse IP » : l’équipement est de type Modbus TCP et est accessible à l’adresse IP précisée • « adresse IP:Port » : l’équipement est de type Modbus TCP et est accessible à l’adresse IP précisée au numéro de port TCP spécifié. 	

Name	Ce champ décrit le nom qui sera donné à cet équipement dans l'interface web. Ce nom est également utilisé pour MQTT et les scripts. C'est pourquoi il est indispensable qu'il soit unique dans la configuration.	
Address	Ce champ n'est pas utilisé pour les équipements de type « IO » et « TIC ». Dans le cas des équipements « Modbus » il correspond à l'adresse de l'équipement sur le réseau Modbus. Sa valeur est donc comprise entre 1 et 240. Dans le cas d'équipements « TIC », « IO » et « SMA-Net », ce champ n'est pas utilisé.	
AcqPeriod	Ce champ permet de préciser la période d'enregistrement des données dans le fichier (la collecte des équipements est en continue). Il est exprimé en secondes.	600
Timeout	Configuration du délai de non-réponse de l'équipement. Si l'équipement ne répond pas dans ce délai, le concentrateur estime que la requête a échoué. Ce délai est exprimé en ms. Ce champ n'est pas utilisé par les protocoles « IO », « TIC » et « SMA-Net ». Dans le cas de SMA-Net, la valeur est 3000ms.	1000
SerialNumber	Sur certains équipements, un numéro de série peut être requis. C'est notamment le cas pour les équipements « TIC ». Ce champ permet donc de préciser celui-ci. Il n'est pas utilisé par les protocoles « IO » et « Modbus »	
Parameters	Ce champ ne sert que pour les cas suivants : <ul style="list-style-type: none"> • Equipement ModbusTCP : permet de préciser si on envoie périodiquement des messages « KeepAlive » pour maintenir la connexion ouverte. Si le champ vaut « 1 », un message périodique est envoyé. Si le champ vaut « 0 », aucun message n'est envoyé. La valeur par défaut est 1 • Equipement propriétaire : (voir annexe spécifique sur les protocoles propriétaires). 	
Category	Ce champ permet de préciser la catégorie dont l'équipement fait partie. Il est à noter que ce champ est rempli automatiquement par le concentrateur.	

Model	Ce champ permet de préciser le nom du modèle de l'équipement. Il est à noter que ce champ est rempli automatiquement par le concentrateur.
DefFile	Ce champ permet de préciser le fichier de définition qui décrit exactement toutes les variables et données exposées par l'équipement. Voir la section dédiée aux fichiers de définition (Définition des équipements connectés).

Un exemple de configuration des interfaces équipements connectées est le suivant :

```
index;interface;name;address;acqPeriod(s);timeout(ms);serialNumber;
parameters;category;model;defFile
IO;;;Io;;;36000;;;WebdynSunPM;ioSunPM;WPM00C715_IO.csv
0;SERIAL1;serial1_52224;0;600;0;2000388220;1;Inverter;WR21TL09;
WPM00C715_SMA_Inverter_SMA_WR21TL09.csv
1;192.93.121.23:502;ethernet_192.93.121.23_502_126;126;600;5000;;;1;
Inverter;Solar_Inverter;WPM00BDE4_SunSpec_inverter_SMA_Solar_Inverter
_9301_ModbusTCP.csv
```

Dans cet exemple, on retrouve 3 équipements :

- Un équipement de type « IO » qui correspond aux entrées/sorties du concentrateur
- Un équipement avec un protocole propriétaire sur bus série
- Un équipement Modbus SMA sur Ethernet

Explications des différents équipements :

- IO:
 - Index : IO. La valeur IO indique que l'équipement est de type « IO »
 - Interface : vide. Les entrées/sorties étant intégrées au boîtier, ce champ est ignoré
 - Name : Io. Le nom qui sera affiché sur les pages web locales
 - Address : vide. Les entrées/sorties ne sont pas concernées par cette information
 - AcqPeriod : La période d'acquisition est fixée à 36000 secondes, soit un enregistrement toutes les 10 heures

- Timeout : vide. Les entrées/sorties ne sont pas concernées par cette information
- SerialNumber : vide. Les entrées/sorties ne sont pas concernées par cette information
- Parameters : vide. Les entrées/sorties ne sont pas concernées par cette information
- Category : WebdynSunPM
- Model : ioSunPM
- DefFile : WPM00C715_IO.csv. Le nom du fichier de définitions qui décrit les différentes entrées/sorties configurées
- INV protocole propriétaire (voir annexe spécifique des protocoles propriétaires) :
- Modbus Ethernet:
 - Index : 1. Indice du deuxième équipement Modbus configuré sur le concentrateur
 - Interface : 192.93.121.23:502. Cette valeur indique que l'équipement est de type Ethernet à l'adresse IP 192.93.121.23 en utilisant le numéro de port par défaut, c'est-à-dire 502
 - Name : Ethernet_192.93.121.23_502_126. Le nom qui sera affiché sur les pages web locales
 - Address : 126. Cet équipement répond à l'adresse Modbus 126
 - AcqPeriod : 600. La période d'acquisition est fixée à 600 secondes, soit un enregistrement toutes les 10 minutes
 - Timeout : 5000. Le timeout est fixé à 5000ms
 - SerialNumber : vide. Non applicable
 - Parameters : 1. La connexion est maintenue en vie.
 - Category : Inverter
 - Model : Solar_Inverter
 - DefFile : WPM00C715_SunSpec_inverter_SMA_Solar_Inverter_9301_ModbusTCP.csv. Le nom du fichier de définitions qui décrit les différentes variables configurées pour cet équipement détecté via SunSpec

En éditant le fichier sous Excel, on obtient l’affichage suivant avec l’utilisation du format CSV :

index	interface	name	address	acqPeriod	timeout	serial number	param.	category	model	defFile
IO		lo		36000 s				Webdyn SunPM	ioSunPM	WPM00C715_ IO.csv
0	SERIAL1	Serial1_ 52224	0	600 s	0 ms	20003 88220	1	Inverter	WR21 TL09	WPM00C715_ SMA_Inverter_ SMA_ WR21TL09.csv
1	192.93 .121 .23 :502	Ethernet _192.93 _121.23_ 502_126	126	600 s	5000 ms		1	Inverter	Solar_ Inverter	WPM00C715_ SunSpec_ Inverter_ SMA_Solar_ Inverter_9301_ ModbusTCP.csv



En cas de modifications du fichier avec un tableur type « Excel », il se peut que le format soit modifié et que les séparateurs ‘;’ soient remplacés par le caractère ‘,’, le rendant inutilisable par le concentrateur. Veuillez à toujours bien préciser le format du séparateur lors d’une sauvegarde.

3.1.2.1.4 Fichier « <uid>_scl.ini »

Le fichier « <uid>_scl.ini » contient la liste des scripts configurés dans le concentrateur.

Si la configuration de base est faite avec le serveur web embarqué, alors ce fichier est automatiquement créé à la première connexion du concentrateur.

Lors de la connexion au serveur distant, si le fichier est détecté, il est téléchargé et la configuration est immédiatement appliquée, quelle que soit la configuration locale.

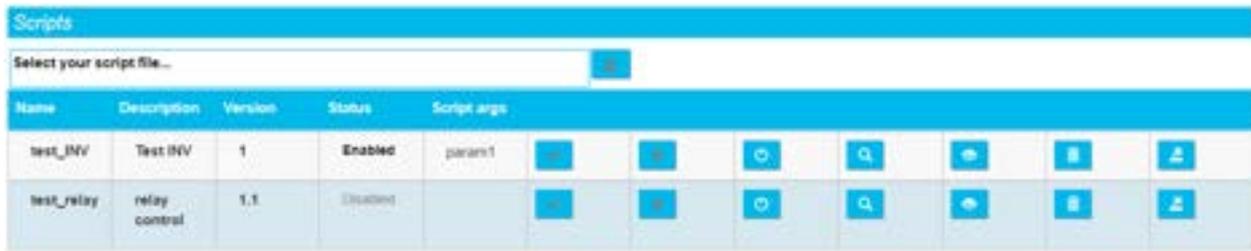
Le fichier comporte trois lignes par script configuré. Chaque ligne contient le numéro du script.

Le format est le suivant :

Variable	Définition	Valeur par défaut
SCRIPT_File[n]	Nom du scénario	Nom du fichier script avec l’extension
SCRIPT_Enable[n]	Activation du script	0
SCRIPT_Args[n]	Paramètre du script	

Où « n » est remplacé par le numéro d’index du script. Ce numéro commençant à 0.

Ainsi, avec la configuration de scripts suivante :



Name	Description	Version	Status	Script args
test_INV	Test INV	1	Enabled	param1
test_relay	relay control	1.1	Disabled	

Le fichier de configuration contiendra les informations suivantes :

```
SCRIPT_File[0]=test_INV.lua
SCRIPT_Enable[0]=1
SCRIPT_Args[0]=param1
SCRIPT_File[1]=test_relay.lua
SCRIPT_Enable[1]=0
SCRIPT_Args[1]=
```

Le numéro d'index est calculé automatiquement par le concentrateur en commençant par 0. En cas de modification manuelle de ce fichier, il faut veiller à ce qu'il n'y ait pas de doublon de numéro d'index, sans quoi la configuration sera refusée.

3.1.2.1.5 Fichier « <uid>_licence.ini »

Le fichier « <uid>_licence.ini » contient les licences des scripts Lua Webdyn « .luaw ». Le fichier de licence doit être placé dans le répertoire CONFIG du serveur distant.

Le fichier de licence permet d'obtenir des scripts spécifiques conçus par Webdyn. Veuillez dans ce cas, vous rapprocher du service commercial Webdyn qui saura vous conseiller et vous rediriger vers les interlocuteurs pertinents : contact@webdyn.com

Lors de la connexion au serveur distant, si le fichier est détecté, il est téléchargé et la licence est immédiatement appliquée. La WebdynSunPM ne déposera pas le fichier de licences si celui-ci est effacé.



Le fichier de licence est propre à une WebdynSunPM. Il n'est pas possible d'utiliser le même fichier sur plusieurs concentrateurs. Il est interdit de modifier le contenu du fichier de licences, sous peine de bloquer la gestion des licences du concentrateur.

3.1.2.2 Définition des équipements connectés

Le fichier de définition est uniformisé pour traiter les différents cas de figure d'équipements. Il gère donc les types suivants : IO, TIC, Modbus RTU, Modbus TCP, etc.

Il faut un fichier de définition par équipement configuré. Un même fichier de définition peut servir à définir plusieurs équipements.

Les fichiers de définition des équipements sont stockés dans le répertoire configuré du serveur. Par défaut, celui-ci est « /DEF ».

Pour que les fichiers de définition soient pris en compte, il faut qu'ils soient référencés dans le fichier « _daq.ini » décrit plus haut (3.1.2.1.3.4 - Déclaration des équipements) dans le champ « DefFile ».

3.1.2.2.1 Nommage des fichiers de définition

Le nommage du fichier est libre et peut être modifié à convenance par le client, la passerelle utilisera le nom fourni dans le fichier daq.csv

Les fichiers générés automatiquement sont préfixés avec l'ID du concentrateur dont la valeur par défaut est composée du trigramme « WPM » suivi des 6 derniers digits de l'adresse MAC de l'équipement qui les a générés.

L'ID du concentrateur peut être modifié par le client, cependant si celui-ci est modifié après la génération d'un fichier cela n'entraîne pas la modification du nom du fichier ni sa déclaration dans le fichier daq.ini.

Le préfix est séparé du reste du nom par un « underscore ». Ceci a pour but d'éviter l'écrasement de fichiers précédemment existant au niveau du SI.

Les fichiers auront une extension csv. Si une autre extension (.ini par exemple) est donnée dans le fichier daq, elle sera acceptée.

Les fichiers générés automatiquement ou créés par le web local seront nommés de la manière suivante :

3.1.2.2.1.1 IO

Le nom des fichiers IO est constitué comme suit :

<uid>_IO.csv

3.1.2.2.1.2 Modbus

Il existe 2 types de fichiers Modbus :

- Les fichiers générés par l'installateur/intégrateur
- Les fichiers générés par l'auto-détection SunSpec

Dans le cas des fichiers générés par l'installateur/intégrateur, il n'y a pas de règle concernant les noms de fichiers. Le choix du nom est laissé libre. Il n'y a aucune contrainte.

Dans le cas des fichiers générés par détection SunSpec, le nom est constitué comme suit :

<uid>_SunSpec_<Category>_<Manufacturer>_<Model>_<Options>_<Protocol>.csv:

- Catégorie : le type d'équipement. A l'heure actuelle seul le type « Inverter » est utilisé.
- Fabricant : nom du fabricant. La valeur est obtenue à partir du champ « Manufacturer » des tables SunSpec
- Modèle : nom du modèle. La valeur est obtenue à partir du champ « Model » des tables SunSpec.
- Options : options détectées sur l'équipement. La valeur est obtenue à partir du champ « Options » des tables SunSpec
- Protocole : le nom du protocole. Les valeurs sont :
 - ModbusRTU : pour un équipement Modbus sur la liaison série
 - ModbusTCP : pour un équipement Modbus sur Ethernet

3.1.2.2.1.3 Protocole propriétaire

Le nom des fichiers des protocoles propriétaire est détaillé dans la note d'application des protocoles propriétaires.

3.1.2.2.2 Contenu du fichier de définition

Le fichier est au format csv, il est constitué de lignes texte elles-mêmes constituées de champs séparés par des « ; ».

La première ligne du fichier contient les informations suivantes :

```
Protocole ; Catégorie ; Fabricant ; Modèle ; Code d'écriture forcé
```

Les champs sont configurés comme suit :

Champ	Description
Protocole	Nom du protocole utilisé pour cet équipement. Les valeurs possibles sont : <ul style="list-style-type: none">• ModbusRTU : l'accès à l'équipement se fait par liaison série via Modbus RTU• ModbusTCP : l'accès à l'équipement se fait par liaison TCP• io : l'équipement est de type IO• tic : l'équipement est de type TIC
Catégorie	Catégorie d'équipement. Ce nom apparaîtra en clair sur le site web local.
Fabricant	Nom du fabricant. Ce nom apparaîtra en clair sur le site web local.

Modèle	Nom du modèle de l'équipement. Ce nom apparaîtra en clair sur le site web local.
Code d'écriture forcé	Indique si le code fonction Modbus utilisé pour l'écriture doit être forcé à 0x10. Les valeurs possibles sont : <ul style="list-style-type: none"> • 0 (valeur par défaut) : l'écriture d'un registre simple se fait avec le code fonction 0x06 tandis que l'écriture de plusieurs registres se fait avec le code fonction 0x10. C'est le comportement classique pour un équipement Modbus. • 1 : l'écriture se fait uniquement avec le code fonction 0x10, même dans le cas d'un registre simple. Ce comportement est nécessaire pour certains onduleurs. Par exemple certains onduleurs de la marque GoodWe.

La Catégorie, le Fabricant et le Modèle permettent de retrouver, depuis les pages web, le fichier de définition à associer à l'équipement.

À la suite de cette première ligne, toutes les lignes suivantes contiendront la définition des différentes variables de l'équipement.

Chaque ligne décrit intégralement une variable.

Chaque ligne aura le format suivant :

```
Index ; Info1 ; Info2 ; Info3 ; Info4 ; Name ; Tag ; CoefA ; CoefB ; Unit ; Action
```

La signification des champs est la suivante :

Champ	Description
Index	Contient l'identifiant unique de la variable dans le fichier. Le choix est libre pour le client à condition qu'il conserve son unicité. Ce champ permet l'identification des variables dans le fichier de données, dans les logs ou dans les fichiers de commande.
Info1	Ce champ contient des informations spécifiques au protocole mis en œuvre sur l'équipement. Se référer à la documentation spécifique au protocole plus bas.
Info2	Ce champ contient des informations spécifiques au protocole mis en œuvre sur l'équipement. Se référer à la documentation spécifique au protocole plus bas.

Info3	<p>Format de la variable. Les formats autorisés sont les suivants :</p> <ul style="list-style-type: none"> • U8 : entier non signé sur 8 bits (1 octet) • U16 : entier non signé sur 16 bits (2 octets, ou 1 registre) • U32 : entier non signé sur 32 bits (4 octets, ou 2 registres) • U64 : entier non signé sur 64 bits (8 octets, ou 4 registres) • I8 : entier signé sur 8 bits (1 octet) • I16 : entier signé sur 16 bits (2 octets, ou 1 registre) • I32 : entier signé sur 32 bits (4 octets, ou 2 registres) • I64 : entier signé sur 64 bits (8 octets, ou 4 registres) • F32 : flottant sur 32 bits (4 octets, ou 2 registres) • F64 : flottant sur 64 bits (8 octets, ou 4 registres) • String : la variable est une chaîne de caractères. Il faut alors utiliser la notation « Adresse_Taille » pour le champ « Info2 » • Bits : la variable est de type champ de bits. Il faut alors utiliser la notation « Adresse_1er bit_Nombre de bits » pour le champ « Info2 » • IP : la variable est de type adresse IP V4 et est donc codée sur 4 octets (2 registres) • IPV6 : la variable est de type adresse IP V6 et est donc codée sur 16 octets (8 registres) • MAC : la variable est de type adresse MAC, au format « EUI48 ». Elle est donc codée sur 6 octets (3 registres) <p>Il est à noter qu'il est possible de modifier les types entiers en rajoutant un suffixe. Les modificateurs autorisés sont :</p> <ul style="list-style-type: none"> • _W : les mots sont échangés, c'est-à-dire que le contenu des registres de la variable est échangé par blocs de 2 octets • _B : les octets sont échangés, c'est-à-dire que le contenu des registres de la variable est échangé au niveau des octets, un par un • _WB : les mots ET les octets sont échangés. Les 2 modificateurs ci-dessus sont appliqués. <p>Ainsi, par exemple, la notation « I32_W » indique qu'il s'agit d'une variable donc les octets 1 et 2 vont être échangés avec les octets 3 et 4.</p> <p>De même, la notation « U16_B » indique que les octets 1 et 2 de la variable seront échangés. Cela correspond à une conversion « Little endian/Big Endian »</p>
Info4	Ce champ contient des informations spécifiques au protocole mis en œuvre sur l'équipement. Se référer à la documentation spécifique au protocole plus bas.
Name	Contient le nom de la variable en question, celui-ci peut être librement choisi à condition d'être unique.
Tag	Contient une identification permettant l'utilisation de la variable en question dans les scripts. (Calcul de cumul, envoi de commande à de multiples équipements, etc...). Ce nom doit donc être unique pour permettre une identification et une utilisation sans équivoque dans les scripts.
CoefA	Contient le coefficient multiplicateur à appliquer à la variable en question afin qu'elle respecte l'unité décrite dans le champ « unit », Ce coefficient est un nombre à virgule flottante, le séparateur décimal est le « . »

CoefB	<p>Contient l'offset à appliquer à la variable en question afin qu'elle respecte l'unité décrite dans le champ « unit ». Ce coefficient est un nombre à virgule flottante, le séparateur décimal est le « . ».</p> <p>Les coefficients A et B seront par défaut renseignés avec la valeur appropriée si elle est connue, sinon A vaut 1 et B vaut 0. Si les valeurs sont absentes, ces valeurs seront considérées comme valant 1 et 0.</p> <p>Ces coefficients sont informatifs à destination de l'utilisateur et ne sont pas appliqués sur les données transmises dans les fichiers de données. Cette opération est à la charge de l'exploitant qui, s'il souhaite convertir la donnée transmise brute, devra effectuer sur une donnée x l'opération « Ax+B » notamment afin d'obtenir une valeur dans l'unité précisée dans le champ « unit ».</p> <p>Ces coefficients sont appliqués sur les valeurs utilisées par les scripts et par le mécanisme de renvoi vers un afficheur afin d'obtenir une valeur dans l'unité précisée dans le champ « unit ».</p>
Unit	<p>Contient l'unité souhaitée. Tout comme pour les coefficients, ce champ est renseigné avec l'information appropriée si elle est connue, sinon le champ est vide. Ce champ est informatif à destination de l'utilisateur et c'est au client de s'assurer de sa correspondance avec les coefficients A et B renseignés.</p>
Action	<p>Contient le code décrivant le traitement à effectuer par le produit sur cette variable lors de la création des fichiers à destination du SI. Les actions possibles sont</p> <ul style="list-style-type: none"> • 0 : variable désactivée. La variable n'apparaîtra pas dans les fichiers de données • 1 : la variable est de type paramètre et en lecture seule. Elle n'apparaîtra donc pas dans les fichiers de données. • 2 : la variable est de type min/max/moy. Dans ce cas, dans les fichiers de données, 3 champs seront occupés par cette variable pour loguer les données de valeur minimum, valeur maximum et valeur moyenne pour cette donnée. • 4 : la variable est de type valeur instantanée. La donnée lue au moment de la collecte sera stockée dans le fichier de données, en n'utilisant qu'un seul champ • 6 : la variable est équivalente à une variable définie avec le code 4 en ce qui concerne l'acquisition. Mais la variable sera également ciblée par une collecte instantanée réalisée via la commande <code>getData</code>. • 7 : la variable est équivalente à une variable définie avec le code 2 en ce qui concerne l'acquisition. Mais la variable sera également ciblée par une collecte instantanée réalisée via la commande <code>getData</code>. • 8 : la variable est de type alarme. Lorsqu'un changement de valeur de cette variable est détecté, une alarme est déclenchée. La donnée lue au moment de la collecte sera stockée dans le fichier d'alarmes, en n'utilisant qu'un seul champ. Une connexion est provoquée immédiatement afin de transmettre ledit fichier. • 9 : la variable est équivalente à une variable définie avec le code 8, il s'agit donc d'une alarme. Mais le fichier d'alarme contenant la nouvelle valeur ne sera déposé que lors de la prochaine connexion au serveur (programmée ou manuelle). Il n'y a pas de connexion automatique dans le cas de ce code action.

Les champs « Info1 », « Info2 », « Info3 » et « Info4 » sont spécifiques à chaque protocole et sont donc configurés comme suit :

3.1.2.2.1 IO

Champ	Description
Info1	Type d'entrée/sortie. Les valeurs autorisées sont : <ul style="list-style-type: none"> • 1 : entrée analogique (0-10V ou 4-20mA) • 2 : entrée numérique • 3 : sortie relais de commutation
Info2	Numéro d'entrée/sortie. Les valeurs autorisées sont : <ul style="list-style-type: none"> • 1 à 3 : si « Info1 » vaut 1 (entrée analogique) • 1 à 4 : si « Info1 » vaut 2 (entrée numérique) • 1 : si « Info1 » vaut 3 (sortie relais de commutation)
Info3	Précision sur le type d'entrée ou de sortie. <ul style="list-style-type: none"> • Si « Info1 » vaut 1 (entrée analogique), les valeurs autorisées sont : <ul style="list-style-type: none"> 1 : entrée analogique de type 4-20ma 2 : entrée analogique de type 0-10V • Si « Info1 » vaut 2 (entrée numérique), les valeurs autorisées sont : <ul style="list-style-type: none"> 1 : entrée TOR 2 : entrée impulsionnelle SO • Si « Info1 » vaut 3 (type relais), ce champ n'est pas utilisé
Info4	Non utilisé

3.1.2.2.2 Modbus

Champ	Description
Info1	Type de registre lu. De ce type découlent les codes fonction qui seront utilisés pour la lecture et l'écriture de la donnée. Les valeurs autorisées sont : <ul style="list-style-type: none"> • 1 : « coil ». Le code fonction de lecture Modbus sera 0x01. Le code fonction écriture sera 0x05 • 2 : « discrete inputs ». Le code fonction de lecture Modbus sera 0x03. Ce type s'adresse à la lecture d'entrées. Il n'y a donc pas d'écriture possible. • 3 : « holding register ». Le code fonction de lecture Modbus sera 0x03. Le code fonction d'écriture sera 0x10 • 4 : « input ». Le code fonction de lecture Modbus sera 0x04. Ce type s'adressant à la lecture d'entrées, il n'y a pas de fonction d'écriture associée.

Info2

Adresse et taille du registre ou de l'entrée à lire. Les formes possibles sont les suivantes :

- Adresse registre. C'est le cas le plus courant. On retrouve donc ici l'adresse du registre dans sa forme classique. Exemple : « 40000 » provoque la lecture du registre à l'adresse 40000
- Adresse registre et taille. Ce format est utilisé pour préciser la taille des données à lire, exprimée en octets. Ce format permet, par exemple, de lire des chaînes de caractères.

Le format est le suivant : Adresse registre_Taille. Ainsi, par exemple, la valeur « 40000_10 » configure une variable dont les données se trouvent au registre 40000, avec une taille de 10 octets.

Si le type est « U8 » ou « I8 », l'information « Taille » correspond à l'offset à appliquer sur le registre pour obtenir l'information.

Ainsi, par exemple, pour un entier sur 8 bits (1 octet), la valeur « 40000_1 » implique qu'on veut lire le 2ème octet au registre Modbus 40000.

- Adresse registre, 1er bit et nombre de bits. Ce format est utilisé pour préciser le registre auquel démarre un champ de bits, ainsi que la taille de ce champ de bits. Il est à noter que si le nombre de bits vaut 1, il est inutile de préciser le nombre de bits.

Le format est le suivant : Adresse registre_1er bit_Nombre de bits. Ainsi, par exemple, la valeur « 40005_4_8 » configure une variable dont les données se trouvent au registre 40005, au 4ème bit de celui-ci et qui s'étend sur 8 bits. De même, la valeur « 40008_1 » configure une variable dont les données se trouvent au registre 40008, au 1er bit de celui-ci et la valeur ne fait qu'un seul bit étant donné que le nombre de bits n'a pas été précisé.

Info3

Type de variable. Les types autorisés sont les suivants :

- U8 : entier non signé sur 8 bits (1 octet)
- U16 : entier non signé sur 16 bits (2 octets, ou 1 registre)
- U32 : entier non signé sur 32 bits (4 octets, ou 2 registres)
- U64 : entier non signé sur 64 bits (8 octets, ou 4 registres)
- I8 : entier signé sur 8 bits (1 octet)
- I16 : entier signé sur 16 bits (2 octets, ou 1 registre)
- I32 : entier signé sur 32 bits (4 octets, ou 2 registres)
- I64 : entier signé sur 64 bits (8 octets, ou 4 registres)
- F32 : flottant sur 32 bits (4 octets, ou 2 registres)
- F64 : flottant sur 64 bits (8 octets, ou 4 registres)
- String : la variable est une chaîne de caractères. Il faut alors utiliser la notation « Adresse_Taille » pour le champ « Info2 »
- Bits : la variable est de type champ de bits. Il faut alors utiliser la notation « Adresse_1er bit_Nombre de bits » pour le champ « Info2 »
- IP : la variable est de type adresse IP V4 et est donc codée sur 4 octets (2 registres)
- IPV6 : la variable est de type adresse IP V6 et est donc codée sur 16 octets (8 registres)
- MAC : la variable est de type adresse MAC, au format « EUI48 ». Elle est donc codée sur 6 octets (3 registres)

Il est à noter qu'il est possible de modifier les types entiers en rajoutant un suffixe.

Les modificateurs autorisés sont :

- _W : les mots sont échangés, c'est-à-dire que le contenu des registres de la variable sont échangés par blocs de 2 octets
- _B : les octets sont échangés, c'est-à-dire que le contenu des registres de la variable sont échangés au niveau des octets, un par un
- _WB : les mots ET les octets sont échangés. Les 2 modificateurs ci-dessus sont appliqués.

Ainsi, par exemple, la notation « I32_W » indique qu'il s'agit d'une variable donc les octets 1 et 2 vont être échangés avec les octets 3 et 4. De même, la notation « U16_B » indique que les octets 1 et 2 de la variable seront échangés. Cela correspond à une conversion « Little endian/Big Endian »

Info4

Scale Factor : lorsque la variable a été générée automatiquement par détection SunSpec, ce champ contient le nom de la variable qui détermine son facteur d'échelle s'il y a lieu.

Lors du calcul de la valeur de la variable configurée, la variable lue verra la position de sa virgule décalée d'autant de chiffres que la valeur de son « scale factor ».

La formule est « var * 10^{sf} » avec « var » la valeur de la variable qu'on lit et « sf » la valeur de la variable indiquée par le « scale factor »

Prenons par exemple une variable « var1 » ayant pour scale factor la variable « sf_var1 ».

Si « var1 » vaut « 1234 » et « sf_var1 » vaut « 3 », la virgule de « var1 » sera décalée de 3 chiffres sur la droite pour obtenir « 1234000 ».

Si « var1 » vaut « 1234 » et « sf_var1 » vaut « -2 », la virgule de « var1 » sera décalée de 2 chiffres sur la gauche pour obtenir « 12,34 »



Trames Modbus : les requêtes Modbus sont regroupées lorsque cela est possible, c'est-à-dire que les variables contiguës sont traitées avec le minimum de requêtes en utilisant au maximum les ressources allouées. En revanche, lorsqu'il y a une zone mémoire libre entre 2 variables, le concentrateur va générer 2 trames et ne cherchera pas à regrouper les 2 variables en une seule requête.

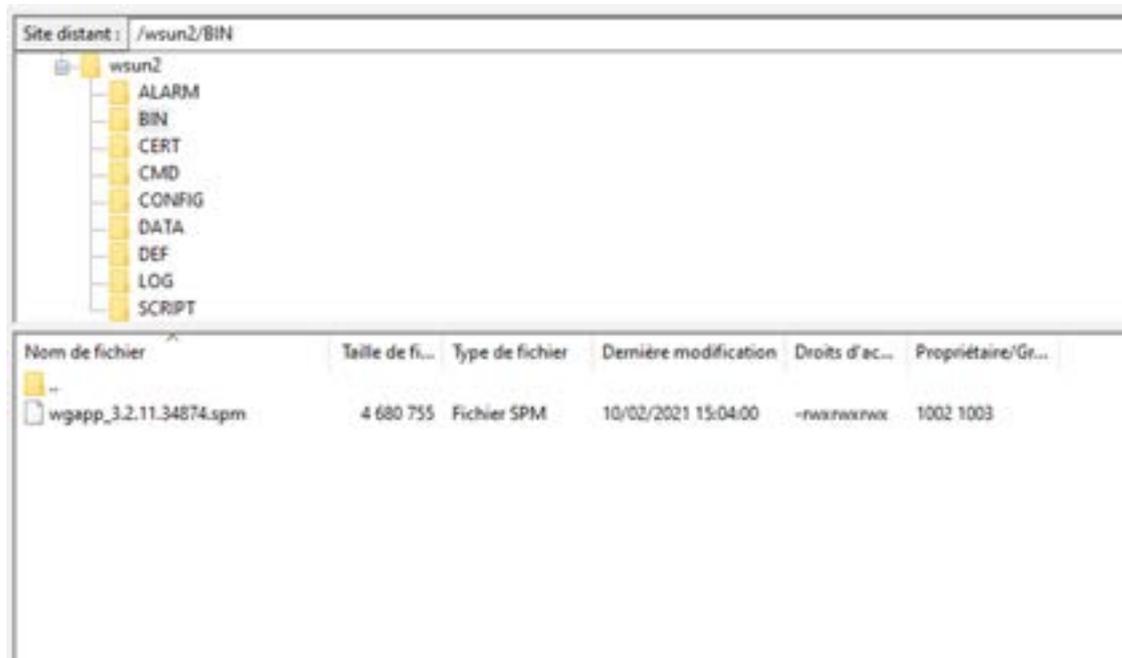
3.1.2.2.3 Protocole propriétaire

Champ	Description
Info1	(voir annexe spécifique des protocoles propriétaires)
Info2	(voir annexe spécifique des protocoles propriétaires)
Info3	(voir annexe spécifique des protocoles propriétaires)
Info4	(voir annexe spécifique des protocoles propriétaires)

3.1.3 Mises à jour

Pour effectuer une mise à jour via le serveur il faut :

- Déposer le nouveau fichier sur le serveur dans le répertoire configuré, comme suit :



- Charger le fichier « _config.ini »
 - Mettre le nom du binaire dans « BIN_FileName ».
 - Mettre le checksum de validation du binaire qui vous a été fourni en même temps que le binaire dans le champ « BIN_Checksum ».
 - Dans l'exemple ci-dessous, les lignes modifiées seront donc :

```
BIN_Checksum=26d00b3496803378cdc8820649cf9535
```

```
BIN_FileName=wgapp_3.2.11.34874.spm
```

3.2 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> pour le LAN1 et <http://192.168.2.12> pour le LAN2) afin d'accéder à la page d'accueil de la WebdynSunPM. (voir chapitre 2.4.5 : « Interface Ethernet »)

Paramètres	LAN1	LAN2
Adresse IP	192.168.1.12	192.168.2.12

- Une fenêtre d'identification s'affiche :



Saisissez votre identifiant et le mot de passe :

Identifiant	Mot de passe
userhigh	high



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 l'interface web (voir chapitre 3.2.2.7 : « Mot de passe (Password) ») ou par fichier de configuration (voir chapitre « Fichier « <uid>_config.ini » »)

- La page d'accueil « Home » s'affiche :

The screenshot displays the 'Home' page of the WebdynGuardPM interface. At the top, there is a navigation bar with 'Home', 'Devices', 'Settings', and 'System' tabs. The main content area is divided into several sections:

- Site's information:** A form showing 'Identifier' as '10746000P'.
- Concentrator's information:** A form showing 'Firmware version' as 'WebdynGuardPM v 1.2.0746', 'Hardware version' as 'V 1.1-4-43-gsm', 'Serial number' as '8000P', and 'Last update' as '2023-01-20 11:07:16'.
- Devices info:** A table with columns for 'Serial / device', 'Status', 'Serial / device', 'Status', 'Serial / device', 'Status', 'Operational status', and 'Status'. It lists three devices: '10746007' (Status: green), '10746008' (Status: orange), and '10746009' (Status: orange). The operational status for these devices is 'SMA SunOpen TCP' (red), 'SMA SunOpen TCP' (orange), and 'SMA SunOpen TCP' (green) respectively.
- Error logs:** A table with columns for 'Error Time', 'Device', and 'Description'. It shows two entries: '2023-01-20 14:27:45' for device '10746008' with description 'TCP error: SMA SunOpen TCP connection has failed 172.20.20.23-8080', and '2023-01-20 14:18:16' for device '10746008' with description 'Exception: msg=10746008: serial=8 - An S2 code=12'.
- Alerts in progress:** A section with a blue header and a table with columns for 'Type', 'Device', 'Severity', and 'Value'.

L'onglet « Home » permet d'obtenir les informations du site et du concentrateur ainsi que l'état général des équipements, les alarmes en cours et les erreurs de communication.

En haut de l'écran se trouvent les informations essentielles du site.

Le panneau « Device info » contient la liste des équipements configurés avec leurs statuts ainsi qu'une liste des erreurs détectées sur les différents équipements configurés.

Seule la première erreur est affichée. Si de nouvelles erreurs arrivent, elles ne sont pas affichées.

Les 4 statuts possibles pour un équipement sont :

-  L'équipement a été trouvé et la configuration actuelle est fonctionnelle
-  L'équipement a été trouvé mais une ou plusieurs variables dans le fichier de définition sont non fonctionnelles
-  L'équipement n'a pas été trouvé ou la configuration actuelle est non fonctionnelle
-  Statut inconnu de l'équipement

Un clic sur un équipement permet d'accéder directement à sa page de paramétrage.

Un clic sur l'icône de corbeille du panneau « Device info » permet de réinitialiser la liste des erreurs détectées. Dans ce cas, toutes les nouvelles erreurs seront affichées.

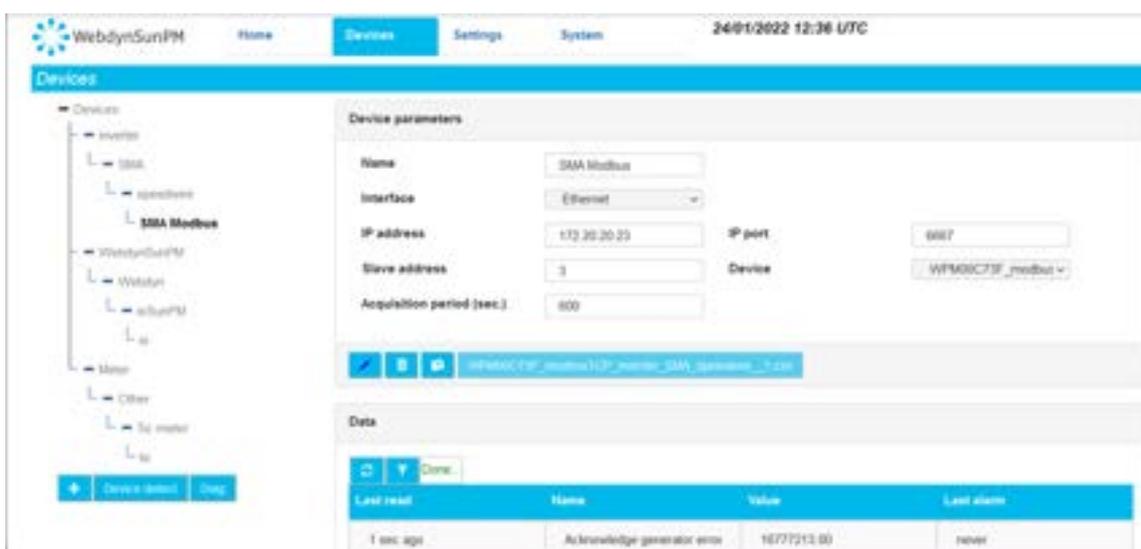
Plus bas, le panneau « Alarms in progress » contient les alarmes en cours.

3.2.1 Equipements (Devices)

Les équipements peuvent être configurés de plusieurs manières :

- En éditant ou important des fichiers existants dans le concentrateur, comme décrit dans la section 3.1.2.1.3 - Fichier « <uid>_daq.csv ».
- En effectuant détection automatique des équipements à partir de l'interface web ou d'un SMS.
- En éditant manuellement la configuration par le biais de l'interface web.

Dans cette section seront détaillées les configurations d'équipements par l'interface web et dont l'accès se fait en cliquant sur l'onglet « Devices » en haut de l'écran.



3.2.1.1 Détection automatique d'équipements

Le concentrateur est capable de détecter automatiquement un certain nombre d'équipements répondant à des normes précises. Ces équipements sont les suivants :

- Onduleurs Modbus pris en charge: ABB, Cefem, Fronius, Goodwe, Growat, Huawei, Ingeteam, Kaco, Kostal, SMA, Solis, Sungrow.
- SunSpec : Les équipements Modbus intégrant des tables répondant aux spécifications de la norme SunSpec (<http://www.sunspec.org/>), peuvent être détectés et configurés automatiquement en utilisant la liaison Ethernet (Modbus TCP) ou série (Modbus RTU).
- Protocole propriétaire : (voir annexe spécifique des protocoles propriétaires).

3.2.1.1.1 Détection d'un équipement SunSpec

La détection automatique d'un équipement SunSpec nécessite les étapes suivantes :

- Brancher l'équipement sur le concentrateur sur une des liaisons série ou sur le réseau Ethernet.
- Vérifier la configuration des équipements : pour une liaison série, vérifier que la configuration est bien la même sur le concentrateur et sur l'équipement. Pour une liaison Ethernet, vérifier que la configuration réseau est compatible entre les deux équipements.
- Aller sur la page des équipements et cliquer sur le bouton « Device detect » :



- La page de détection s'affiche alors :

Launch device detection

Interface: Serial 1 Serial 1 settings: modbusRTU, 9600, 8, none, 1 [Change Serial 1 settings](#)

Brand: SunSpec

Number of devices: 1

[Start detection](#)

- Choisir l'interface sur laquelle on souhaite faire la détection. Dans le champ « Number of devices », saisir le nombre d'équipements à détecter. La valeur par défaut est « 1 ».

Serial 1 ▾

- Serial 1
- Serial 2
- Serial 3
- LAN port 1
- LAN port 2
- TIC 1

Les interfaces sont de type « Série » « LAN » ou TIC (accessoire USB)

Pour chaque type d'interface, les paramètres sont affichés ainsi qu'un lien vers la page WEB permettant de les changer

Serial :

Serial 1 settings: modbusRTU, 9600, 8, none, 1

[Change Serial 1 settings](#)

Ethernet :

IP: 192.168.1.12, mask: 255.255.255.0

[Change Ethernet 1 settings](#)

En fonction de l'interface et du protocole configuré, une liste de marques d'équipement est proposée.

Par exemple :

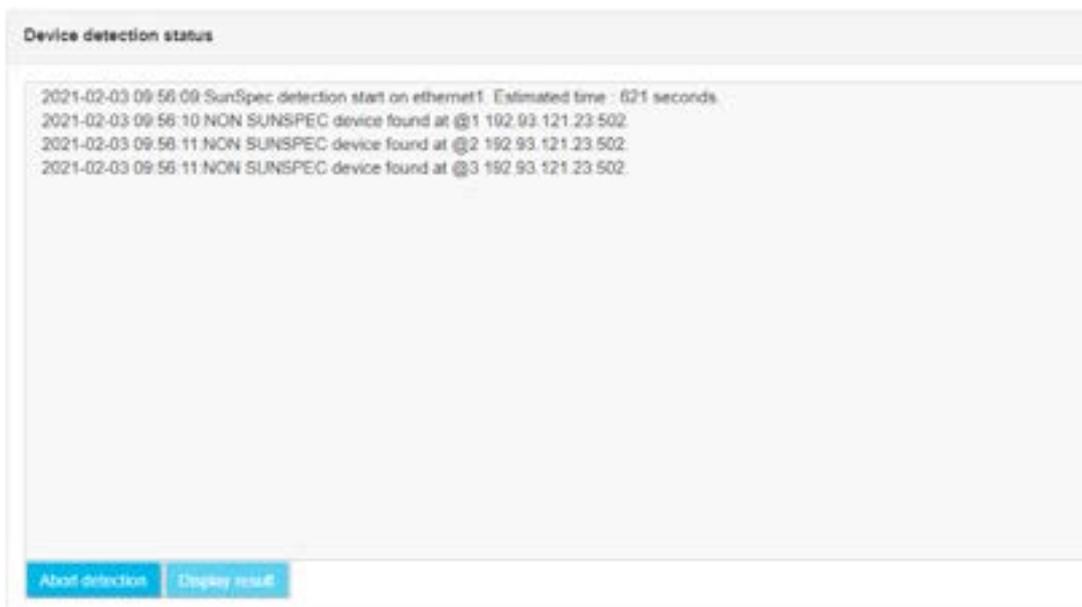


Les onduleurs peuvent être détectés soit par marque (qu'ils soient SunSpec ou non) soit par le protocole SunSpec.

Lorsque la marque de l'onduleur est prise en compte, il est conseillé d'utiliser la détection par marque, ainsi tous les onduleurs de cette marque pourront être détectés, qu'ils soient Sunspec ou non.

Dans le champ « Number of devices », saisir le nombre d'équipements à détecter. La valeur par défaut est « 1 ».

- Cliquer ensuite sur le bouton « Start detection » pour lancer la détection. Une fenêtre de progression s'affiche alors :



La fenêtre de progression indique en première ligne la date et heure du début de la détection ainsi qu'une durée estimée pour la détection.

Les messages affichés permettent de suivre la progression. L'exemple donné ci-dessus concerne la détection SunSpec.

Détection SUNSPEC

Au fur et à mesure de la détection, la progression s'affichera dans la page web. :

- « NON SUNSPEC device found » signifie qu'un équipement Modbus mais non SunSpec a été détecté à l'adresse Modbus précisée :

```
2021-02-03 09:56:10:NON SUNSPEC device found at @1
192.93.121.23:502
```

Signifie qu'un équipement Modbus ne répondant pas aux spécifications SunSpec a été trouvé à l'adresse IP « 192.93.121.23 » avec l'adresse Modbus 1.

- « SunSpec device found » signifie qu'un équipement Modbus répondant aux spécifications SunSpec a été détecté à l'adresse Modbus précisée :

```
2021-02-03 09:56:21:SunSpec device found at @126
192.93.121.23:502
```

Signifie qu'un équipement conforme aux spécifications SunSpec a été détecté à l'adresse IP « 192.93.121.23 », avec l'adresse Modbus « 126 ».

- « Found table » signifie qu'une table SunSpec a été détectée sur l'équipement. La ligne d'information indique ensuite l'identifiant de la table, sa taille revendiquée par l'équipement, ainsi que des informations techniques sur l'équipement et le numéro de registre Modbus de départ de la table :

```
2021-02-03 09:56:21:Found table 1:66 at 40004@126
192.93.121.23:502
```

Signifie que la table d'identifiant « 1 » et de taille « 66 » registres a été détectée sur l'équipement Modbus TCP à l'adresse IP « 192.93.121.23 », au registre « 40004 » et adresse Modbus « 126 ».

- « End of SunSpec detection » signifie que la détection SunSpec est terminée. La ligne indique le nombre d'équipements détectés :

```
2021-02-03 09:56:53:End of SunSpec detection on
ethernet1. 1 devices found.
```

La détection SunSpec s'est terminée avec succès sur l'interface Ethernet. 1 équipement a donc été détecté.

Détection par marque

```
Search for Huawei Modbus devices on ethernet
Estimated time : 2mn 3s
Device found @1 172.20.12.49:502s
Found 1 devices in 2 s
Search terminated
```

- Au cours de la détection il est toujours possible d'interrompre à tout moment en cliquant sur le bouton « Abort detection ». Mais ceci est déconseillé, car certains équipements peuvent être perturbés si la détection est arrêtée au milieu d'une découverte :



- À la fin de la détection SunSpec la dernière page de la détection permet de visualiser tous les équipements qui ont été détectés et, éventuellement, de les ajouter à la configuration.



Manufacturer	Model	Serial number	IP address/modbus	Add
SMA	Solar Inverter	1930159878	192.92.121.23/128	<input checked="" type="checkbox"/>
<input type="button" value="Accept"/>				<input type="button" value="Add"/>

Cet écran affiche donc tous les équipements détectés, ainsi qu'un certain nombre d'informations lues dans les tables équipements SunSpec (modèle, numéro de série, adresse, fabricant) ainsi que le nom du fichier de définition qui lui est associé.

On retrouve également une case à cocher tout à droite qui permet de choisir les équipements à rajouter dans la configuration. Il est à noter que si l'équipement détecté fait déjà partie de la configuration, la case est décochée par défaut. Sinon la case est cochée pour un rajout automatique.

Une fois les équipements sélectionnés, un clic sur le bouton « Accept » importe la nouvelle configuration dans le concentrateur et l'appareil apparaît dans les équipements configurés.

Lorsque la détection est effectuée par marque, le fichier de définition généré est conforme aux variables décrites dans les documentations techniques fournies par les fabricants d'onduleur.

Lorsque la détection est SUNSPEC, il s'agit alors d'un fichier dynamiquement généré en fonction des tables décrites par le consortium SUNSPEC implémentés par le fabricant d'onduleur.

Les variables de ce nouvel équipement seront générées en fonction des tables SunSpec détectées. Ainsi, pour chaque table SunSpec détectée, les variables suivantes seront créées :

- <idTable>_tableId : cette variable va contenir l'identifiant de la table en numérique, sous

forme d'entier sur 16 bits

- <idTable>_tableSize : cette variable contient la taille de la table en nombre de registres, sous forme d'entier sur 16 bits
- <idTable>_<variableName> : pour chaque variable de la table déclarée dans les normes SunSpec, une variable correspondante sera associée à l'équipement. Le nom de la variable sera composée de l'identifiant de table, suivi du nom de la variable
- <idTable>_<repeatBlock>_<variableName> : dans le cas de variables qui proviennent d'un bloc qui se répète, les variables sont créées en utilisant l'identifiant de table, le numéro de la répétition, ainsi que le nom de la variable, de façon à ce que le nom généré soit unique.

Les variables générées sont, par défaut, de type « Paramètre » et auront donc le code « Action » 1, à l'exception des variables des tables 101, 102, 103, 111, 112, 113, 123, 160 et 401 qui seront créées avec le type « Immédiat », c'est-à-dire le code 4.

Il est à noter également que les variables suivantes auront un tag automatiquement appliqué :

- WMaxLimPct de la table 123 reçoit le tag « cmdPwrPercent »
- WMaxLimPct_RmpTms de la table 123 reçoit le tag « WMaxLimPct_RmpTms »
- WMaxLimPct_Ena de la table 123 reçoit le tag « WMaxLimPct_Ena »
- VarPct_Mod de la table 123 reçoit le tag « VArPct_Mod »

Il est à noter que si l'équipement existait déjà dans la configuration et que l'utilisateur force une nouvelle importation, l'équipement précédent n'est pas écrasé. Un nouvel équipement est créé en plus de l'équipement préexistant.

Si l'utilisateur clique sur le bouton « Cancel », cette liste est effacée, et la page affiche à nouveau l'écran de sélection du type de détection.

3.2.1.1.2 Détection d'un équipement Protocole propriétaire

(voir annexe spécifique du protocole propriétaire)

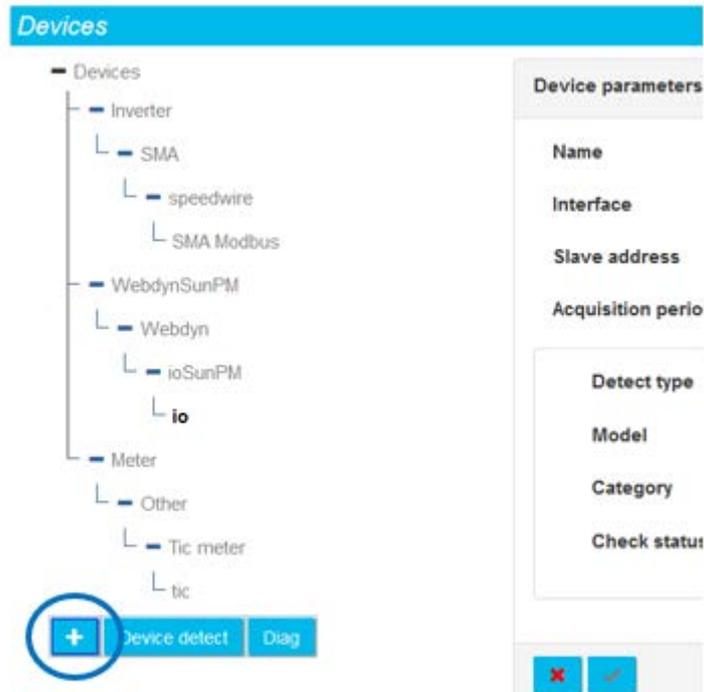
3.2.1.2 Gestion manuelle des équipements

Il est possible de gérer les équipements manuellement sur le site web.

Toute la gestion se fait via l'onglet « Devices » décrit plus haut (voir chapitre 3.2.1 : « Equipements (Devices) »).

3.2.1.2.1 Ajouter un équipement

Pour rajouter un équipement, cliquer tout d'abord sur le bouton « + » :



La page suivante apparaît alors :

Dans ce formulaire, il est possible de sélectionner un équipement par rapport à son fichier de définition correspondant et de choisir son interface, son nom, son adresse ainsi que sa période d'acquisition. Commencer par renseigner un nom à cet équipement. Ce nom doit être unique.

Choisir l'interface où est connecté l'équipement :

- Port Ethernet : si l'équipement est connecté sur le réseau Ethernet (par exemple pour un

équipement qui fait du « Modbus TCP »).

- Port série : si l'équipement est connecté que un des ports série de la WebdynSunPM (par exemple pour un équipement qui fait « Modbus RTU »). Seuls les ports série dont le paramétrage est compatible avec le protocole sélectionné sont affichés.

Dans cet exemple, ce sont donc les équipements de type « Modbus ».

The screenshot shows a configuration form titled 'Device parameters'. The fields are as follows:

Name	<input type="text" value="x96_EAB9FC"/>		
Interface	<input type="text" value="Ethernet"/>		
IP address	<input type="text" value="11.22.33.44"/>	IP port	<input type="text" value="502"/>
Slave address	<input type="text" value="1"/>		
Device	<input type="text" value="x96_EAB9FC_modbusTCP_inverter_SMA_Speedwire.csv"/>	<input type="button" value="+"/>	
Acquisition period (sec.)	<input type="text" value="600"/>		
Timeout (msec.)	<input type="text" value="0"/>		

L'équipement étant de type TCP (dans cet exemple :« ModbusTCP »), les champs suivants sont également apparus :

- *IP address* : saisir l'adresse IP de l'équipement ModbusTCP sur le réseau
- *Port* : saisir le numéro de port pour accéder à l'équipement. Généralement 502
- *Slave address* : adresse Modbus de l'équipement
- *Acquisition period (sec.)* : période d'enregistrement des données dans le fichier (la collecte des équipements est en continu). Il est exprimé en secondes.
- *Timeout (msec.)* : délai de non-réponse de l'équipement. Si l'équipement ne répond pas dans ce délai, le concentrateur estime que la requête a échoué. Ce délai est exprimé en ms.

The screenshot shows a configuration form titled 'Device parameters'. The fields are as follows:

Name	<input type="text"/>	
Interface	<input type="text" value="Serial port 2 - modbusRTU"/>	
Slave address	<input type="text" value="126"/>	
Device	<input type="text" value="Webdyn ABB_10.0 et 12.5 PVL_MODBUS.csv"/>	<input type="button" value="+"/>
Acquisition period (sec.)	<input type="text" value="600"/>	
Timeout (msec.)	<input type="text" value="0"/>	

Lorsque l'équipement est de type série (dans cet exemple :« ModbusRTU »), les champs suivants apparaissent :

- *Slave address* : adresse Modbus de l'équipement

Une fois ces paramètres saisis, il est également possible de saisir la périodicité d'acquisition des données.

Pour le choix de l'équipement dans la liste déroulante du « Device », il est possible de :

- Lancer une détection de l'équipement
- Sélectionner le fichier de définition présent dans la liste déroulante

Il est possible d'importer un nouveau fichier de définition, en cliquant sur le symbole « + ».

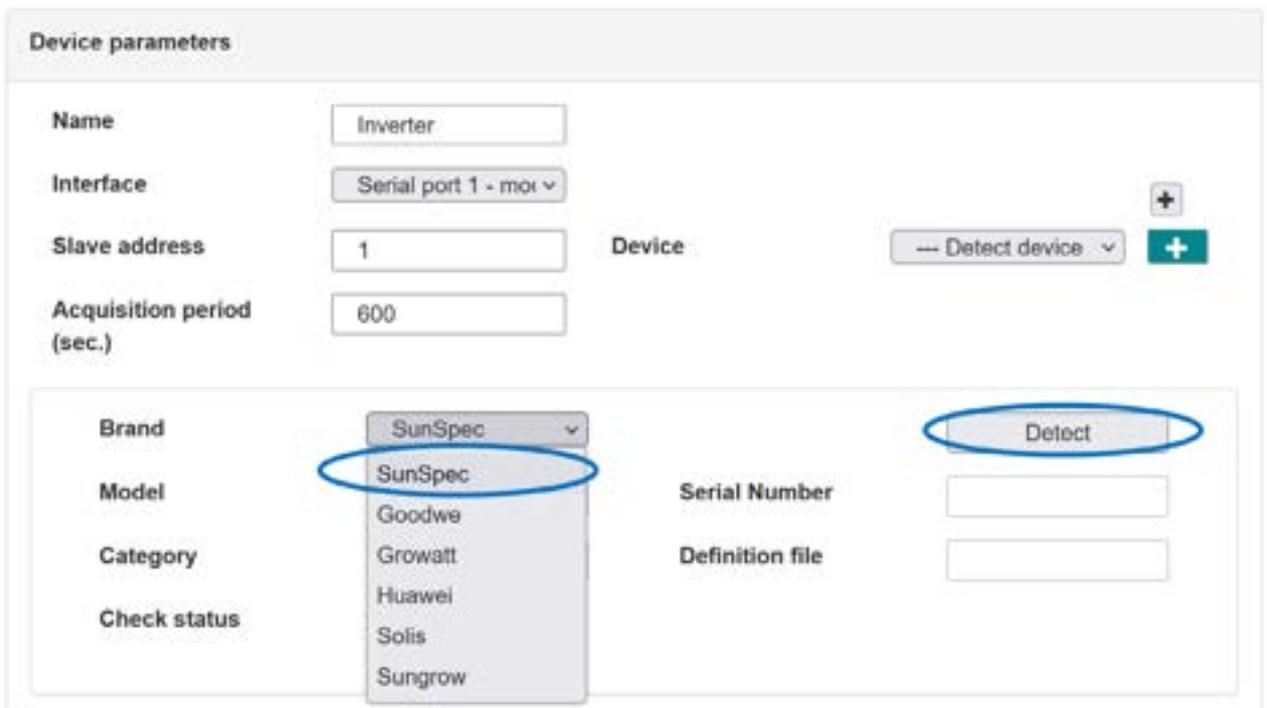
Lancer une détection de l'équipement :

Sélectionner « Detect device » dans « Device » :



The screenshot shows the 'Device parameters' form. The 'Device' dropdown menu is open, displaying options: 'Webdyn ModbusRTU_invert', 'Webdyn ModbusRTU_inverter_Huawei_v3.csv', and '--- Detect device'. The 'Detect device' option is circled in blue. A 'Check' button is visible below the dropdown.

Choisir le type d'équipement à détecter (dans cet exemple « Sunspec »), puis lancer la détection en cliquant sur le bouton « Detect » :



The screenshot shows the 'Device parameters' form with the 'Brand' dropdown menu open, displaying options: 'SunSpec', 'Goodwe', 'Growatt', 'Huawei', 'Solis', and 'Sungrow'. The 'SunSpec' option is circled in blue. The 'Detect' button is also circled in blue. The 'Name' field contains 'Inverter', 'Interface' is 'Serial port 1 - moi', 'Slave address' is '1', and 'Acquisition period (sec.)' is '600'.

Examiner le résultat :

Model: Solar Inverter
Category: Inverter
Serial Number: 1800158078
Definition file: WPM80C73F_SunSpec_
Check status: ●

Buttons: [Close] [Check]

Le modèle, la catégorie, le numéro de série, le fichier de définition ainsi que le statut de l'équipement s'affiche quand l'équipement est trouvé.

Si le « Check status » est :

- L'équipement a été trouvé et la configuration actuelle est fonctionnelle
- L'équipement n'a pas été trouvé ou la configuration actuelle est non fonctionnelle

Valider l'ajout de l'équipement en cliquant sur la coche en bas de la page.

Buttons: [Close] [Check]

Le nouvel équipement apparaît alors dans l'arborescence sur le côté gauche de l'écran :

Devices

- Inverter
 - SMA
 - SMA Sunspec
- ModbusMaster
 - Widom
 - OtherPDI
 - ...
- Other
 - Tu master
 - ...

Device parameters

Name: SMA Sunspec
Interface: Serial port 2 - modbusRTU
Slave address: 125
Acquisition period (sec.): 600
Device: WPM80C73F_SunSpec_ +

Data

Last read	Name	Value	Last alarm
2 sec ago	801_A_SF	-1.00	never

Importer un nouveau fichier de définition :

Si l'équipement souhaité n'est pas trouvé dans les listes déroulantes du « Device », il faut alors importer le fichier de définition correspondant.

Pour cela, dans un premier temps, cliquer sur le bouton :



Device parameters

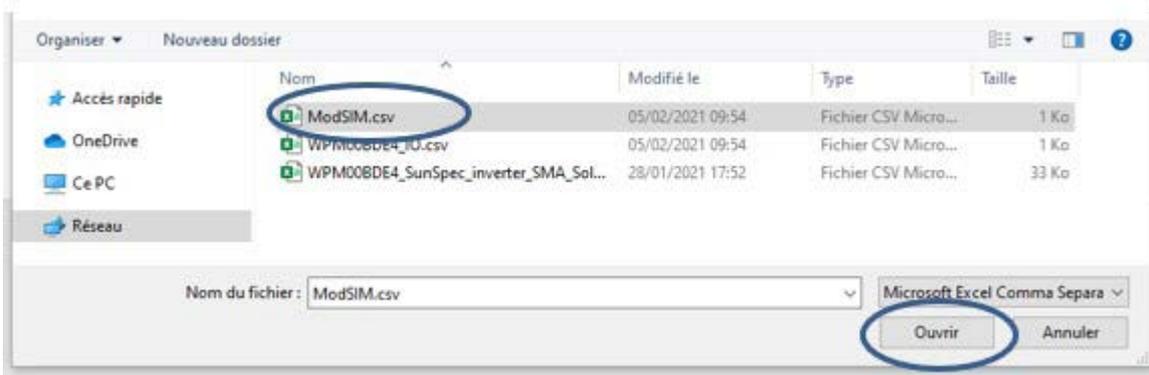
Name

Interface Serial port 2 - modbusRTU

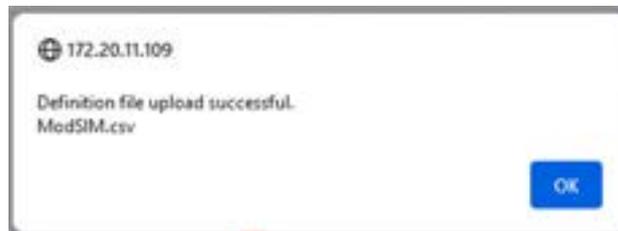
Slave address Device **+**

Acquisition period (sec.)

La fenêtre suivante apparaît ensuite, sélectionner le fichier de définition à importer :



Sélectionner ensuite le fichier à importer puis cliquer sur le bouton « Ouvrir ».



Le message « Definition file upload successful » apparaît alors sur l'interface web pour indiquer le succès de l'opération, cliquer sur le bouton OK pour finaliser l'importation du fichier de définition.



Device parameters

Name

Interface Serial port 2 - modbusRTU

Slave address Device **+**

Acquisition period (sec.)

Webdyn ModbusRTU_Inverter_Huawei_v3.csv

ModSIM.csv

Detect device

Une fois le fichier de définition chargé, il devient possible de sélectionner les caractéristiques de l'équipement souhaité dans les listes déroulantes.

Dans le cas du fichier de test, l'en-tête contient les informations suivantes :

ModbusTCP	modSIM	Webdyn	test_PC1
1	3	2	U16
2	3	3	U16

Sélectionner le fichier de définition présent dans la liste déroulante :

Il est possible de saisir l'équipement correspondant :

The screenshot shows a 'Device parameters' window with the following fields and values:

- Name: [Empty text box]
- Interface: Serial port 2 - modbusRTU
- Slave address: 0
- Acquisition period (sec.): 600
- Device: ModSIM.csv (highlighted with a blue oval)
- Check: [Check button]
- Model: [Empty text box]
- Serial Number: [Empty text box]
- Category: [Empty text box]
- Definition file: [Empty text box]
- Check status: [Empty text box]

Lorsque la configuration est satisfaisante, cliquer sur le bouton « Check » afin de lancer la vérification sur l'équipement :

Device parameters

Name:

Interface:

Slave address: Device:

Acquisition period (sec.):

Model: Serial Number:

Category: Definition file:

Check status: ●

Si le « Check status » est :

- L'équipement a été trouvé et la configuration actuelle est fonctionnelle
- L'équipement n'a pas été trouvé ou la configuration actuelle est non fonctionnelle

Valider l'ajout de l'équipement en cliquant sur la coche en bas de la page.

Device parameters

Name:

Interface:

Slave address: Device:

Acquisition period (sec.):

Model: Serial Number:

Category: Definition file:

Check status: ●

Le nouvel équipement apparaît alors dans l'arborescence sur le côté gauche de l'écran :

Device parameters

Name: INV Modbus
 Interface: Serial port 2 - modbusRTU
 Slave address: 1
 Acquisition period (sec.): 600

Device: ModSM.csv

ModbusRTU

Data

Last read	Name	Value	Last alarm
2 sec ago	101_A_SF	-1.00	never



Tout fichier de définition importé dans la WebdynSunPM qui est non utilisé pendant 24 heures sera automatiquement effacé par le concentrateur lors de sa prochaine connexion distante.

3.2.1.2.2 Supprimer un équipement

Pour supprimer un équipement, sélectionner tout d'abord l'équipement à supprimer :

Device parameters

Name: M
 Category: Inverter
 Acquisition period (s): 600
 Serial port: Serial 1
 Timeout (ms): 5000

Manufacturer: HUANUO
 Model: M
 RTU Slave address: 1

M

Cliquer ensuite sur l'icône de la corbeille sous la description de l'équipement :

Device parameters

Name: M
 Category: Inverter
 Acquisition period (s): 600
 Serial port: Serial 1
 Timeout (ms): 5000

Manufacturer: HUANUO
 Model: M
 RTU Slave address: 1

M

Une boîte de dialogue apparaît alors pour demander confirmation de la suppression.

Après confirmation, l'équipement est supprimé des bases du concentrateur.

La modification sera répercutée sur les fichiers de configuration à la prochaine connexion au serveur.

3.2.1.2.3 Éditer un équipement

Pour éditer un équipement, sélectionner tout d'abord l'équipement à éditer :



Cliquer ensuite sur le bouton d'édition :



Dès l'appui sur le bouton, la page de l'équipement change. La barre de boutons de gestion de l'équipement passe en mode édition :



Il devient alors possible de modifier les différents champs de l'équipement, et donc de modifier le nom, l'interface, la périodicité d'acquisition, le modèle, ainsi que les paramètres spécifiques au protocole : adresse IP et numéro de port pour un équipement IP, adresse d'esclave pour un équipement Modbus, la période d'acquisition, etc.

Un appui sur le bouton de validation permet de valider la nouvelle saisie. Un appui sur le bouton d'annulation ignore toutes les modifications qui ont été faites dans le formulaire de saisie.

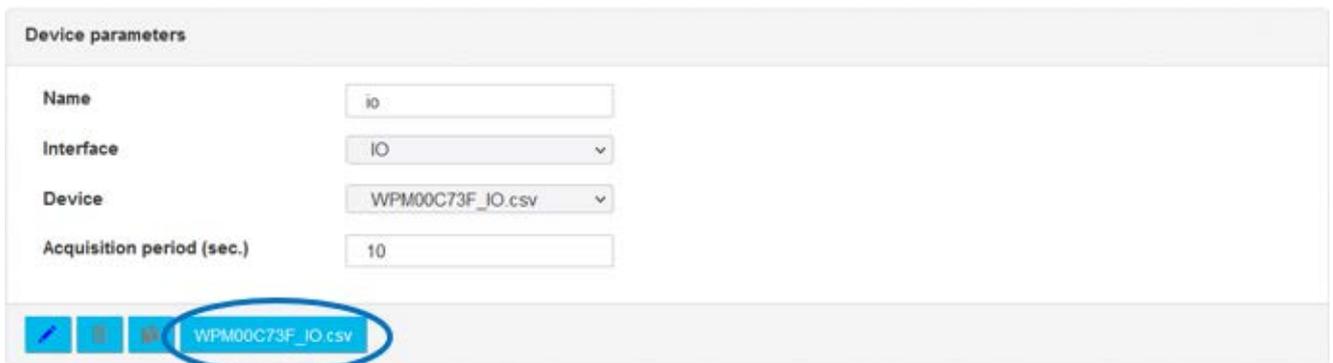
Il est possible également de modifier les variables de l'équipement en important un nouveau fichier de définitions. Pour cela, il suffit de cliquer sur « Import new definition file » dans le menu déroulant « Device » et de sélectionner le nouveau fichier de définitions (Voir le chapitre 3.1.2.1.3.4 : « - Déclaration des

équipements »). Une fois le fichier importé, il faut resélectionner le fichier de définition pour correspondre au nouvel équipement importé afin de recharger les variables, comme lors de l'ajout d'un équipement (voir chapitre 3.2.1.2.1 : « - Ajouter un équipement »).

3.2.1.2.4 Modification de la configuration des entrées/sorties

La configuration des entrées/sorties peut se faire directement à partir de la page de gestion des équipements.

Il suffit de cliquer sur le bouton du fichier de définition des IO du concentrateur :



The screenshot shows a web interface titled "Device parameters". It contains four input fields: "Name" (text input with "io"), "Interface" (dropdown menu with "IO"), "Device" (dropdown menu with "WPM00C73F_IO.csv"), and "Acquisition period (sec.)" (text input with "10"). Below these fields is a row of three buttons: a blue button with a pencil icon, a grey button with a circular arrow icon, and a blue button labeled "WPM00C73F_IO.csv". The blue button is circled in red.

La page d'affichage de l'état des entrées/sorties laisse alors la place à l'affichage suivant :

WPM_D2A0B4_IO.csv

Digital Input

#	Type	name	Action	Contact	tag
1	Pulse B/5V	digital1	Instant value	Normally Open	
2	Pulse B/5V	digital2	Instant value	Normally Open	
3	Pulse B/5V	digital3	Instant value	Normally Open	

Analog Input

#	Type	name	action	Scale	Offset	Unit	tag
1	4-20mA	analog1	Instant va	1	0		
2	4-20mA	analog2	Instant va	1	0		
3	4-20mA	analog3	Instant va	1	0		
4	4-20mA	analog4	Instant va	1	0		

Output

#	Type	name	Action	Contact	tag
1	Dry loop	output	Instant value	Normally Open	

La première partie de l'écran permet de configurer les 3 entrées numériques :

Digital Input

#	Type	name	Action	Contact	tag
1	Pulse B/5V	digital1	Instant value	Normally Open	
2	Pulse B/5V	digital2	Instant value	Normally Open	
3	Pulse B/5V	digital3	Instant value	Normally Open	

Les champs sont :

Champ	Description
Type	Type d'entrée numérique. Les valeurs autorisées sont : <ul style="list-style-type: none">• Dry Loop : boucle sèche (TOR)• Pulse B/5V : SO (voir chapitre 2.4.7.2 : « Entrées numériques TOR/SO (impulsionnelle) »)• Pulse A/24 : SO (voir chapitre 2.4.7.2 : « Entrées numériques TOR/SO (impulsionnelle) »)
Name	Nom à donner à l'entrée. Cette valeur sera utilisée dans les pages web et sur les serveurs MQTT. Le nom doit être unique sur le concentrateur
Action	Action associée à l'entrée. Les valeurs autorisées et les actions possibles sont : <ul style="list-style-type: none">• Ignored : La valeur sera ignorée. La variable est désactivée. Elle n'apparaîtra pas dans les fichiers de données• Instant value : l'entrée est de type valeur instantanée. La donnée lue au moment de la collecte sera stockée dans le fichier de données, en n'utilisant qu'un seul champ• Alarm on change : l'entrée est de type alarme. Lorsqu'un changement d'état est détecté, une alarme est déclenchée. La donnée lue au moment de la collecte sera stockée dans le fichier de données, en n'utilisant qu'un seul champ
Contact	Indique l'état « normal » de cette entrée, c'est-à-dire son état au repos. Les valeurs possibles sont : <ul style="list-style-type: none">• Normally open : l'état au repos de l'entrée est 0. Lorsque l'entrée est active, sa valeur passe à 1.• Normally closed : l'état au repos de l'entrée est 1. Lorsque l'entrée est active, sa valeur passe à 0. <p>Cette distinction est utilisée dans les pages web, pour l'affichage, ainsi que dans les scripts. Elle n'a aucune incidence sur les fichiers de données.</p>
Tag	Contient une identification permettant l'utilisation de la variable en question dans les scripts. (Calcul de cumul, envoi de commande a de multiples équipements, etc...). Ce nom doit donc être unique pour permettre une identification et une utilisation sans équivoque dans les scripts.

La deuxième partie de l'écran d'édition des entrées/sorties est dédiée à la configuration des 4 entrées analogiques :

Analog Input							
#	Type	name	action	Scale	Offset	Unit	tag
1	4-20mA	analog1	Instant va	1	0		
2	4-20mA	analog2	Instant va	1	0		
3	4-20mA	analog3	Instant va	1	0		
4	4-20mA	analog4	Instant va	1	0		

Les champs sont :

Champ	Description
Type	Type d'entrée analogique. Les valeurs autorisées sont : <ul style="list-style-type: none"> •4-20mA •0-10V
Name	Nom à donner à l'entrée. Cette valeur sera utilisée dans les pages web et sur les serveurs MQTT. Le nom doit être unique sur le concentrateur
Action	Action associée à l'entrée. Les valeurs autorisées et les actions possibles sont : <ul style="list-style-type: none"> • Ignored : La valeur sera ignorée. La variable est désactivée. Elle n'apparaîtra pas dans les fichiers de données • Instant value : l'entrée est de type valeur instantanée. La donnée lue au moment de la collecte sera stockée dans le fichier de données, en n'utilisant qu'un seul champ • Min/Max/Average: l'entrée est de type Min/Max/Moyenne. La donnée lue au moment de la collecte sera stockée dans le fichier de données, en utilisant trois champs distincts. Sur la période d'acquisition, le premier champ mémorisera la valeur minimum, le deuxième champ la valeur maximum et le troisième champ sera une moyenne sur l'ensemble des variables acquises sur cette période.
Contact	Contient le coefficient multiplicateur à appliquer à l'entrée en question afin qu'elle respecte l'unité décrite dans le champ « unit », Ce coefficient est un nombre à virgule flottante, le séparateur décimal est le « . » Ce coefficient est informatif à destination de l'utilisateur et n'est pas appliqué sur les données transmises dans les fichiers de données.

Tag	Contient l'offset à appliquer à l'entrée en question afin qu'elle respecte l'unité décrite dans le champ « unit ». Ce coefficient est un nombre à virgule flottante, le séparateur décimal est le « . » Ce coefficient est informatif à destination de l'utilisateur et n'est pas appliqué sur les données transmises dans les fichiers de données.
Contact	Unité pour l'affichage sur le site web local. La valeur n'est pas utilisée ailleurs.
Tag	Contient une identification permettant l'utilisation de la variable en question dans les scripts. (Calcul de cumul, envoi de commande à de multiples équipements, etc...). Ce nom doit donc être unique pour permettre une identification et une utilisation sans équivoque dans les scripts.

La dernière partie de l'écran d'édition des entrées/sorties est dédiée à la configuration de la sortie relais :

#	Type	name	Action	Contact	tag
1	Dry loop	Output 1	Ignored	Normally Open	

Les champs sont :

Champ	Description
Type	Type de sortie. Les valeurs autorisées sont : • Dry loop : contact sec
Name	Nom à donner à l'entrée. Cette valeur sera utilisée dans les pages web et sur les serveurs MQTT. Le nom doit être unique sur le concentrateur.
Action	Action associée à l'entrée. Les valeurs autorisées sont : Les actions possibles sont : • Ignored : La valeur sera ignorée. La variable est désactivée. Elle n'apparaîtra pas dans les fichiers de données. • Instant value : l'entrée est de type valeur instantanée. La donnée lue au moment de la collecte sera stockée dans le fichier de données, en n'utilisant qu'un seul champ. • Alarm on change : l'entrée est de type alarme. Lorsqu'un changement d'état est détecté, une alarme est déclenchée. La donnée lue au moment de la collecte sera stockée dans le fichier de données, en n'utilisant qu'un seul champ.

Contact	Etat du relais au repos : <ul style="list-style-type: none"> • Normally Open : normalement ouvert • Normally Closed : normaleement fermé
Tag	Contient une identification permettant l'utilisation de la variable en question dans les scripts. (Calcul de cumul, envoi de commande a de multiples équipements, etc...). Ce nom doit donc être unique pour permettre une identification et une utilisation sans équivoque dans les scripts.

3.2.1.2.5 Dupliquer un équipement

Pour dupliquer un équipement, sélectionner tout d'abord l'équipement à dupliquer :



Cliquer ensuite sur le bouton de duplication :



À l'appui sur le bouton, l'équipement est dupliqué.

La nouvelle instance utilise le même fichier de définition que l'équipement d'origine. Il est ensuite possible de renommer, changer le fichier de définition en éditant l'équipement. (voir chapitre « Éditer un équipement »).

3.2.1.3 Outils de diagnostics des équipements

Des outils de diagnostics sont mis à disposition pour analyser les trames envoyées aux équipements ainsi que les trames reçues. Ces outils permettent de comprendre ce qui se passe en cas de problèmes de configuration.

3.2.1.3.1 Activation des logs de communication



L'accès aux pages des outils de diagnostics des communications des équipements se fait en cliquant sur le bouton « Diag » dans la page des équipements.

La page suivante apparaît alors :



Le premier paramètre est dédié aux logs des communications avec les équipements, par les ports série ou les IO.

Lorsque les traces de communication sont sélectionnées pour une interface donnée, toutes les communications sur cette interface seront journalisées et envoyées sur le serveur sous forme de log horodaté à la milliseconde près.

Étant donnée la quantité d'informations transmises et reçues, ces logs ne sont activés que pour une

période définie, à configurer dans le champ « Duration ». Cette période est exprimée en minutes. Une fois le délai expiré, l'activation du log rebascule sur « Disabled » automatiquement.

3.2.1.3.2 Exploitation des logs

Lorsque des logs de communication sont disponibles sur le concentrateur ils seront déposés lors de la prochaine connexion au serveur, dans le répertoire configuré pour les logs.

3.2.1.3.2.1 Logs des interfaces série et ethernet

Le nom des fichiers de journalisation des communications avec les équipements est construit selon le même principe que les autres fichiers de logs de la passerelle, à savoir : « uid »_« interface »_« date ».log.gz.

L'interface correspond à celle qui a été choisie pour les logs, à savoir :

- serial1
- serial2
- serial3
- ethernet

Les logs contiennent les informations suivantes :

```
datetime_1;data;
datetime_2;data
...
datetime_Y;data
```

« datetime » est au format DD/MM/YYYY hh:mm:ss.mmm, avec DD le jour dans le mois, MM le numéro du mois, YYYY l'année, hh l'heure de la communication, mm la minute, ss les secondes, et mmm les millisecondes.

Le champ « data » contient les données transmises ainsi que le sens. Pour les communications sortantes, le sens est « => ». Pour les communications entrantes, le sens est « <= ».

Si l'interface de communication est de type « serial », les données en hexadécimal sont ensuite fournies.

Si l'interface de communication est de type « ethernet », l'adresse IP de l'équipement à surveiller est logué, puis les données sont fournies au format hexadécimal, comme pour le protocole série.

Il est à noter que dans le cas de Modbus, la trame Modbus TCP complète est fournie si la liaison est de type ethernet. Sinon c'est la trame Modbus RTU.

Dans le cas d'erreurs Modbus, la trame peut être préfixé des messages suivants :

- « *** CRC *** » : une erreur CRC a été détectée sur la trame entrante. La trame est donc invalide. C'est une erreur de communication matérielle. Trop d'erreurs de CRC est signe d'un problème dans l'installation. La trame est ignorée.
- « *** BAD SLAVE *** » : Un esclave ayant un numéro incorrect a répondu à la requête. Ceci peut provenir d'une erreur de configuration d'un équipement qui peut perturber le bon fonctionnement de l'installation. La trame est ignorée.
- « *** EXCEPTION *** » : L'esclave a répondu une exception à la requête. Ceci signifie que la requête qui a été envoyée est incorrecte pour l'équipement en question.
- « *** INVALID ID *** » : Un esclave a répondu à une requête ModbusTCP avec un identifiant incorrect. La trame a été ignorée.
- « *** INVALID FCT *** » : La réponse contient un code fonction incorrect. La trame est ignorée.

3.2.1.3.2.2 Logs des entrées/sorties

Le nom des fichiers de journalisation des entrées/sorties est construit selon le même principe que les autres fichiers de logs de la passerelle, à savoir : « uid »_IO_« date ».log.gz.

Les logs contiennent les informations suivantes :

```
datetime_1;data
datetime_2;data
...
datetime_Y;data
```

« datetime » est au format DD/MM/YYYY hh:mm:ss.mmm, avec DD le jour dans le mois, MM le numéro du mois, YYYY l'année, hh l'heure de la communication, mm la minute, ss les secondes, et mmm les millisecondes.

Le champ « data » contient les données des entrées sorties.

En premier lieu apparaît le type d'information :

- « In » : indique que c'est une entrée
- « Out » : indique que c'est une sortie

Puis, le nom de l'entrée/sortie impactée, tel que défini dans la configuration

Puis, le nouvel état de l'entrée/sortie :

- 0 : l'entrée/sortie est fermée
- 1 : l'entrée/sortie est ouverte
- Toute autre valeur contient la valeur d'une entrée analogique

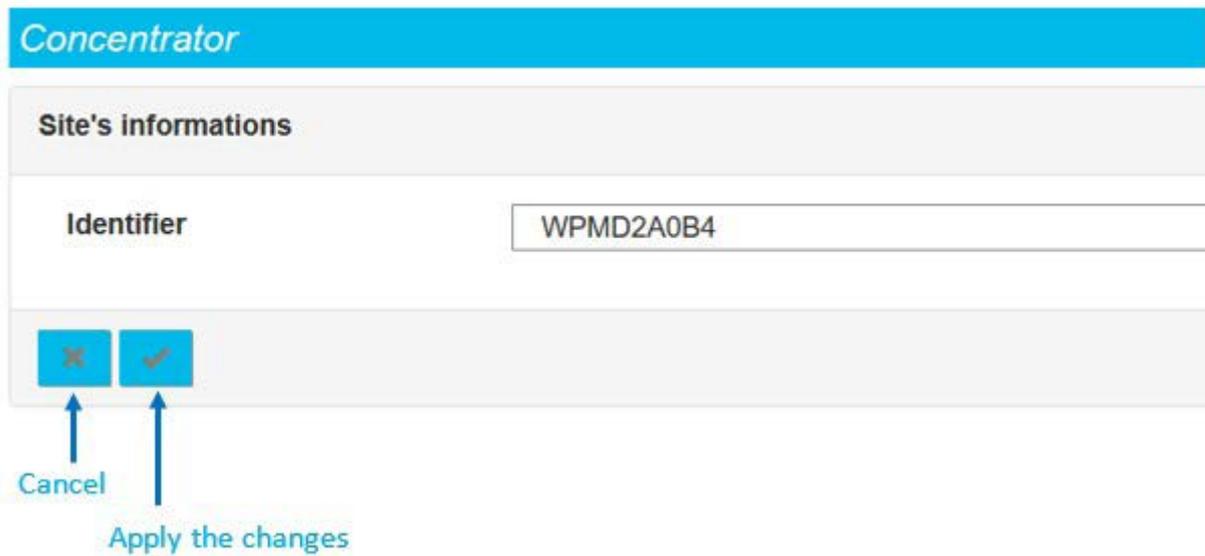
3.2.2 Paramètres (Settings)

L'ensemble des paramètres du concentrateur sont réunis dans l'onglet de paramétrage « Settings ». Les paramètres sont découpés en plusieurs parties dans le menu.



3.2.2.1. Concentrateur (Concentrator)

La partie concentrateur « Concentrator » permet de modifier l'identifiant et la description du concentrateur.



Interface Web	Paramètre dans le fichier de configuration <uid>_config.ini	Description
Identifiant	Concentrator_Identifier	Identifiant du concentrateur

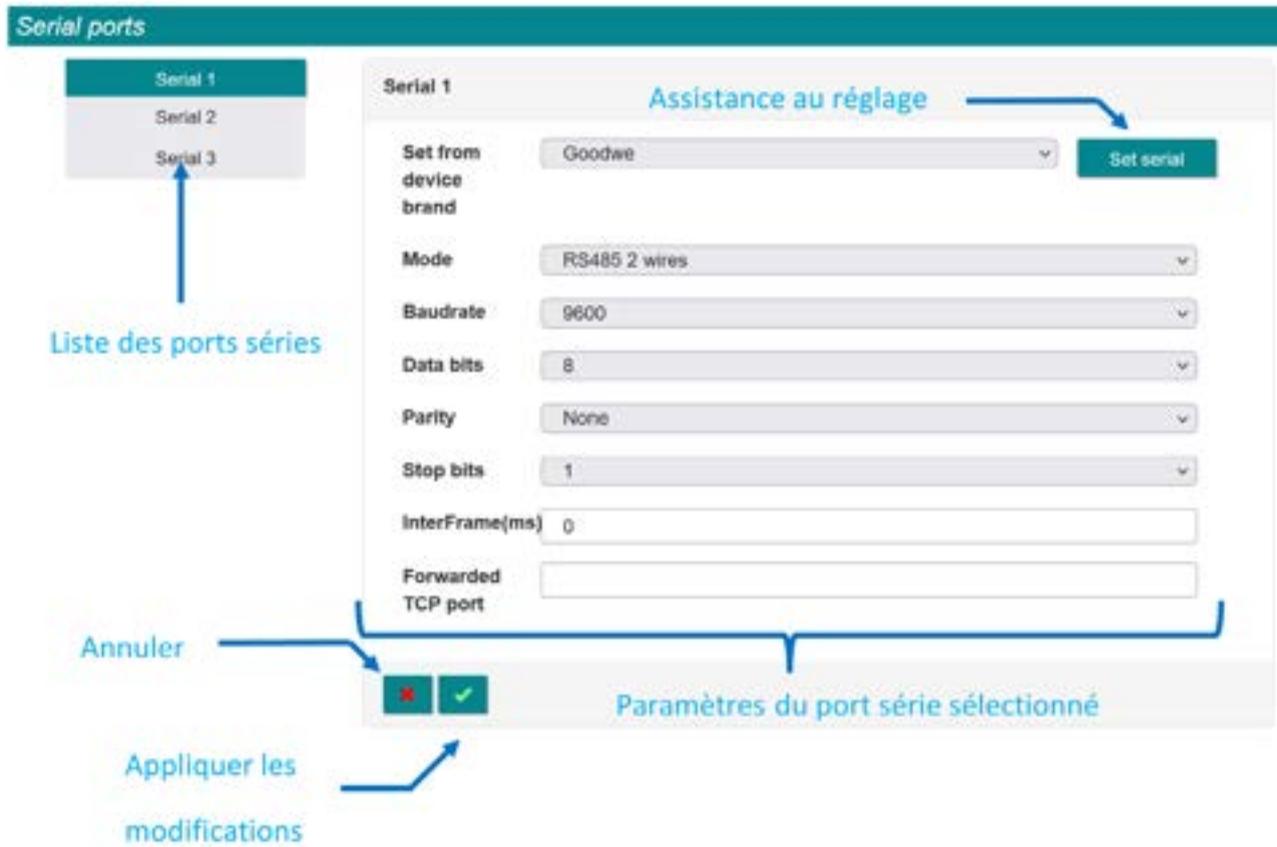
Par défaut, un identifiant unique « WPMxxxxxx » est renseigné. Les « xxxxxx » correspondent aux 6 derniers caractères de l'adresse MAC du concentrateur qui est indiquée sur l'étiquette du produit. (voir chapitre 2.2.2 : « Identification »).



Identifiant : l'identifiant sert dans la création des noms des fichiers qui sont déposés sur le serveur. Il est important que celui-ci soit unique afin de connaître la provenance des fichiers sur le serveur distant. Dans le document, l'identifiant du concentrateur est représenté ainsi : <uid>.

3.2.2.2 Série (Serial)

La partie « serial » permet de configurer les 3 ports série RS485/422 qui possèdent chacun un paramétrage et une sortie qui leur sont propres. (voir chapitre 2.4.6 : « Interface Série RS485/RS422 »).



Les paramètres possibles pour chaque port série sont :

Interface Web	Paramètre dans le fichier de configuration <uid>_daq.csv	Description
Protocol	protocol	Type de protocole associé à l'interface série : <ul style="list-style-type: none"> • Modbus : port série configuré en Modbus RTU • Marque d'onduleurs : ABB, Cefem, Fronius, Goodwe, Growatt, Huawei, Ingeteam, Kaco Modbus, Kostal, Solis, Sungrow • Protocole propriétaire : port série configuré pour le protocole propriétaire (voir annexe spécifique des protocoles propriétaires). • PW1 : port série configuré le protocole PowerOne.

Mode	wires	<p>Mode de l'interface série :</p> <ul style="list-style-type: none"> • RS485 2 fils : liaison série en Half-Duplex (2 fils) en RS485 • RS485 4 fils : liaison série en Full-Duplex (4 fils) en RS485 ou RS422
Baudrate	baudrate	<p>Vitesse de la liaison série en baud :</p> <ul style="list-style-type: none"> • 1200 • 2400 • 4800 • 9600 • 19200 • 38400 • 57600 • 115200 • 230400 • 460800
Data bits	data_bits	<p>Nombre de bits de données :</p> <ul style="list-style-type: none"> • 7 • 8
Parity	parity	<p>Parité de la liaison série :</p> <ul style="list-style-type: none"> • None : pas de parité • Odd : parité impaire • Even : parité paire
Stop bits	stop_bits	<p>Nombre de bits de stop :</p> <ul style="list-style-type: none"> • 1 • 2
InterFrame	interframe	<p>Temps d'attente entre 2 trames échangées sur le port série. Ce temps d'attente est exprimé en ms. Voir l'explication à la section « Configuration des ports série »</p>
Forwarded TCP port	forwarded_port	<p>Port Modbus transféré.</p> <p>Si ce champ est renseigné, le concentrateur ouvre un port ModbusTCP sur le numéro de port saisi. Lorsqu'un équipement ModbusTCP se connecte à ce port, toutes les requêtes envoyées sont transférées directement sur le bus ModbusRTU et la réponse est remontée à l'équipement connecté via ce port ModbusTCP.</p> <p>Cette option permet de créer un tunnel de communication entre un équipement ModbusTCP et le réseau ModbusRTU local.</p> <p>Les requêtes sont intercalées entre les requêtes internes de surveillance du concentrateur.</p>

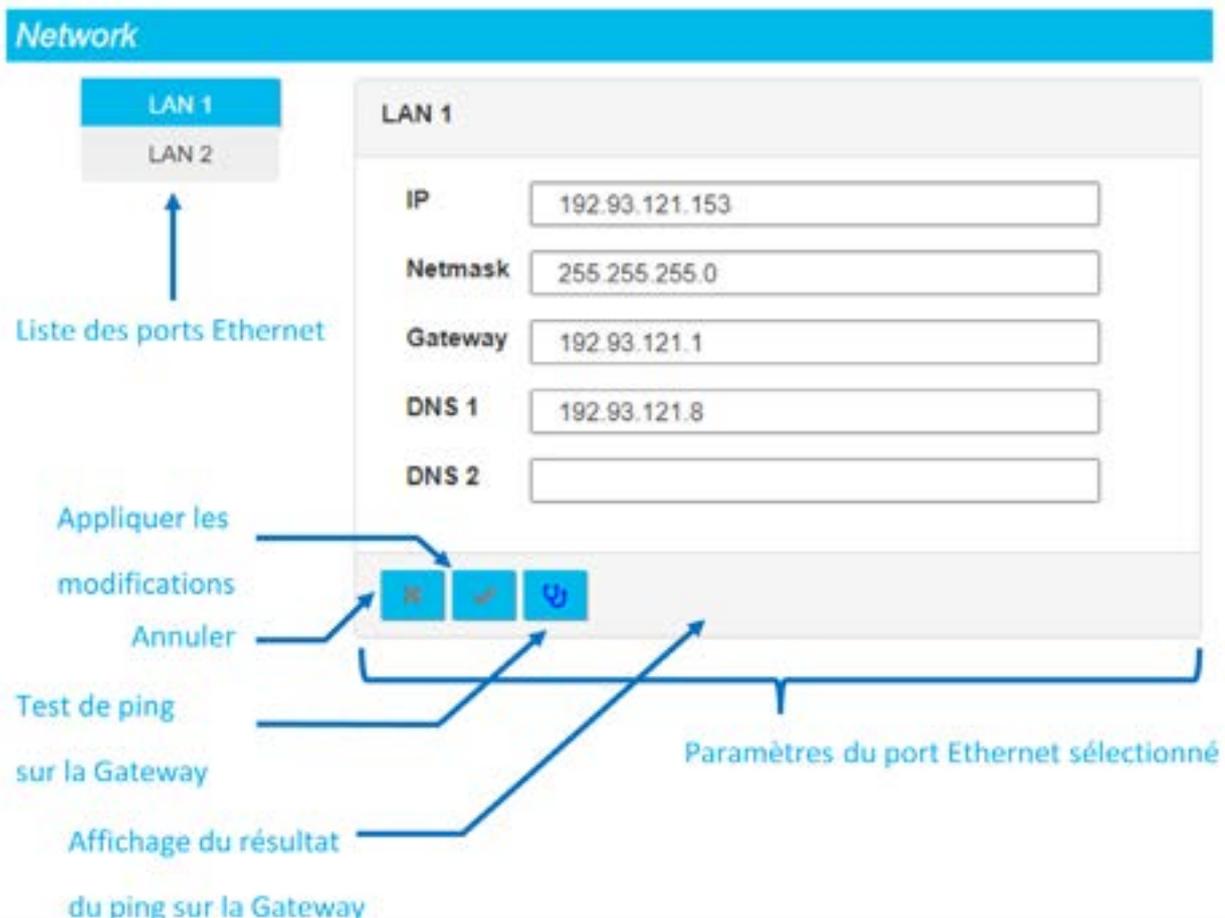
Le bouton « set Serial » permet de renseigner automatiquement les paramètres par défaut d'un fabricant d'équipement.

Dans ce cas, les paramètres sont préremplis avec les paramètres par défaut de la marque d'onduleur sélectionnée.

Si les paramètres des onduleurs n'ont pas été modifiés, il est alors possible de valider la configuration du port série. Dans le cas contraire, il convient d'adapter ses paramètres en fonction de ceux qui ont été réglés dans l'onduleur.

3.2.2.3 Réseaux (Networks)

La partie réseau « Networks » permet de configurer les 2 interfaces Ethernet (LAN1 et LAN2) disponibles sur le concentrateur. Ces interfaces Ethernet permettent au concentrateur d'appartenir à 2 réseaux Ethernet différents.(voir chapitre 2.4.5 : « Interface Ethernet »).



Pour pouvoir effectuer un test de ping sur l'adresse IP de la Gateway, celui-ci doit être renseigné et la configuration doit être appliquée avant de cliquer sur le bouton Test.

Les paramètres des 2 interfaces Ethernet sont :

Interface Web	Paramètre dans le fichier de configuration <uid>_daq.csv	Description
IP	ip	Adresse IP à laquelle le concentrateur est accessible via le réseau Ethernet.
Netmask	mask	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	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.
DNS 1	dns1	Serveur DNS 1. 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 ».
DNS 2	dns2	Serveur DNS 2. Au cas où le serveur DNS1 est en échec.



Si votre réseau local est géré par un administrateur réseau, contactez-le avant d'intégrer la passerelle WebdynSunPM dans votre réseau.

3.2.2.4 Modem

La partie « Modem » permet de configurer le modem et d'obtenir les informations sur les réseaux. Pour utiliser le modem, il faut d'abord procéder à l'insertion de la carte SIM dans le produit (voir chapitre « Carte SIM »).

Modem

The screenshot displays two sections of a web interface for modem configuration. The top section, titled 'PIN code configuration', contains a text input field for 'PIN code' and a status indicator 'PIN code OK' in green. The bottom section, titled 'Modem configuration', includes fields for 'APN' (containing 'TM'), 'Authentication type' (a dropdown menu set to 'None'), 'Connection identification', and 'Connection password'. At the bottom left, there are two buttons: a red 'X' icon labeled 'Annuler' and a green checkmark icon labeled 'Appliquer les modifications'. A blue arrow points from the 'Annuler' button to the 'PIN code OK' status, with the label 'Information sur le code PIN' below it.

Les paramètres du modem sont :

Interface Web	Paramètre dans le fichier de configuration <uid>_daq.csv	Description
PIN code	pin	Code PIN de la carte SIM à renseigner si la carte SIM possède un code
APN	apn	Nom de l'APN de votre opérateur mobile (obligatoire pour une connexion IP)

Authentication type	authentication	Type d'authentification auprès de l'opérateur (facultatif selon l'opérateur) : <ul style="list-style-type: none"> • None : aucune authentification • PAP : authentification de type PAP. Il faut renseigner l'identifiant et le mot de passe ci-dessous.
Connection identification	login	Nom d'utilisateur de votre opérateur mobile (facultatif selon l'opérateur)
Connection password	password	Mot de passe de votre opérateur mobile (facultatif selon l'opérateur)



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

Le PIN code status indique les informations sur le code SIM qui peuvent être :

PIN code status	Description
PIN code OK	Le modem peut accéder à la carte SIM. Soit le code PIN de la carte SIM est correct ou soit la carte SIM n'a pas de code PIN.
PIN code Required	La carte SIM attend un code. Il faut renseigner son code dans le champ « PIN code »
Unknown	Erreurs diverses du modem.
PUK code required	La carte SIM est bloquée, car il y a eu trop d'échecs avec un code erroné.
SIM card not inserted	Il n'y a pas de carte SIM insérée dans le concentrateur.



Si la carte SIM a un code PIN activé et que le code PIN renseigné dans le concentrateur est erroné, la carte SIM peut se bloquer. Vous pouvez la débloquer en utilisant un téléphone portable avec le code PUK fourni par votre opérateur.

Les informations du modem affichées sont :

Modem information	
Model	HL8518
Firmware version	RHL85xx.5.14.0.6.1.20170103.x6255
IMEI number	352948071810273
IMSI number	234500021978798
RSSI	
CSQ	22
dBm	-69
IP Address	10.109.22.156
DNS Address	8.8.8.8

Ces informations correspondent :

Modem information	Description
Model	Modèle du modem intégré dans le concentrateur
Firmware version	Version du logiciel du modèle intégré dans le concentrateur
IMEI number	Numéro unique d'identification internationale du modem intégré dans le concentrateur
IMSI number	Numéro IMSI de la carte SIM insérée, permettant à un réseau mobile d'identifier un usager.
RSSI	Indication du niveau de puissance en réception du modem en nombre de barres
CSQ	Niveau du signal de réception compris entre 0 et 31 retourné par le modem
dBm	Niveau du signal interprété en dBm compris entre -113 dBm et -51 dBm retourné par le modem
IP address	Adresse IP attribuée automatiquement par l'opérateur mobile

DNS address	Adresse DNS fourni automatiquement par l'opérateur mobile
Network type	Le type de réseau sur lequel le modem est connecté (2G/3G/4G.)
Carrier name	Le nom de l'opérateur auquel le modem est actuellement connecté.

Le niveau de signal de réception est très important lors de l'installation du produit. Il permet de connaître l'état de la connexion entre le modem et l'opérateur auquel le concentrateur est rattaché. Cela est très important pour éviter des erreurs de transmission et des temps d'échanges trop importants entre le concentrateur et le serveur distant. Se référer au tableau ci-dessous.

Valeur CSQ	RSSI en dBm	Description
CSQ > 20	RSSI > -73	Niveau Excellent
15 < CSQ < 20	-83 < RSSI < -73	Niveau Bon
12 < CSQ < 14	-89 < RSSI < -85	Niveau limite
CSQ < 11	RSSI < -91	Niveau instable

Dans le cas où le niveau de réception est limite ou instable, il est recommandé d'utiliser une antenne déportée ou de tester un autre opérateur mobile afin d'améliorer la connexion.



Si l'adresse IP et DNS ne sont pas affichés, cela peut provenir de plusieurs choses :

- L'APN n'est pas renseigné ou incorrect.
- Si une authentification est requise, le login et/ou le mot sont incorrects.

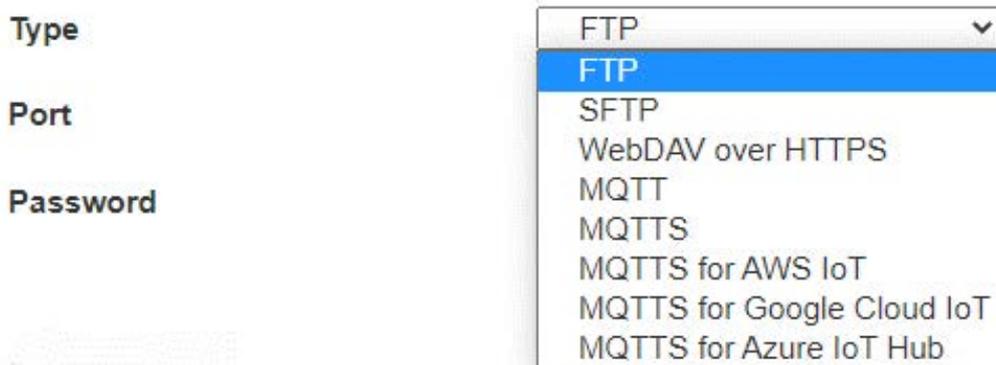
Tant que le problème persiste, le concentrateur ne pourra pas se connecter au serveur distant par le modem. Par contre, les commandes SMS restent fonctionnelles.

3.2.2.5 Serveurs (servers)

La partie « servers » permet de configurer les 2 serveurs disponibles sur le concentrateur et de planifier des horaires de synchronisation. Cette synchronisation peut également se faire localement sur une carte SD.



Le concentrateur supporte 8 types de serveurs distants différents et qui sont :



Le concentrateur peut également stocker les données localement sur une carte SD. Pour cela il faut

sélectionner l'interface « SD card » :

Server 1	
Interface	Ethernet ▼
Address	Ethernet Modem SD card

Le choix du type de serveur ou de l'interface SD Card modifie les paramètres à renseigner. Les paramètres des serveurs restent identiques.



Le serveur 2 n'est utilisé que pour sauvegarder les configurations. Seul le serveur 1 gère la synchronisation des fichiers de configuration. Le MQTT/MQTTS/MQTTS AWS IOT/MQTTS Google Cloud IoT/MQTTS Azure IoT Hub est uniquement disponible sur le serveur 2 (backup).

Pour vérifier que la configuration du serveur est correcte, il est conseillé de cliquer sur le bouton « Connect ». Une fenêtre avec le journal de connexion s'affiche, permettant de voir l'ensemble des fichiers échangés entre le concentrateur et le serveur distant. La dernière ligne permet de savoir rapidement si la connexion s'est bien passée ou si un échec a eu lieu.

L'arrêt de la connexion en cours par l'appui sur le bouton « Abort » n'est pas immédiat. En effet, si une action est en cours, elle devra d'abord se terminer. Une action correspond à chaque ligne décrite dans le journal de connexion.

```
Request Tracking
2021-02-12 18:04:05 Checking WPM00C44F_adb5c74e96.csv
2021-02-12 18:04:05 No change
2021-02-12 18:04:05 Local changes sent WPM00C44F_daq.csv
2021-02-12 18:04:05 Script management...
2021-02-12 18:04:05 Checking WPM00C44F_scl.ini
2021-02-12 18:04:05 No change
2021-02-12 18:04:05 Checking 200922-Script_ZeroInjection.lua
2021-02-12 18:04:05 No change
2021-02-12 18:04:05 Checking 200922-Script_ZeroInjection-v1.0.lua
2021-02-12 18:04:05 No change
2021-02-12 18:04:05 Checking Livrable_GREENYELLOW_02.lua
2021-02-12 18:04:05 No change
2021-02-12 18:04:05 Checking Script_ZeroInjection_v1.0.lua
2021-02-12 18:04:05 No change
2021-02-12 18:04:05 Configuration file summary:
2021-02-12 18:04:05 WPM00C44F_daq.csv: Action=Send local file. Result=Success
2021-02-12 18:04:07 Sending WPM00C44F_SYSTEM_210212_180405.tar.gz
```

En cas d'erreur, vérifier l'ensemble des paramètres du serveur.



Veillez vousVeillez-vous rapprocher de l'administrateur du serveur auquel vous voulez vous connecter afin d'obtenir les paramètres à renseigner sur le concentrateur et si besoin les certificats et la clé pour le chiffage et l'authentification.

3.2.2.5.1 Carte SD (SD Card)

Lorsque l'interface « SD card » est sélectionnée, l'affichage fait disparaître les champs inutiles et la configuration des répertoires n'est pas modifiable dans cette interface. De plus, un cadre apparaît avec les informations actuelles concernant la carte SD :

The screenshot shows a web interface for configuring a server. At the top, there is a 'Connection status' bar with a timestamp '2021-09-27 14:45:06' and the message 'Connection terminated with success'. Below this, the 'Server 1' configuration page is visible. The 'Interface' dropdown is set to 'SD card'. A '2 steps for put file disabled' checkbox is present. The configuration is organized into two columns of text input fields for directories: /CONFIG, /ALARM, /LOG, /BIN, /CERT, /DATA, /CMD, /DEF, and /SCRIPT. There are also checkboxes for 'Synchronise certificates', 'Data file header option enabled', and 'European date format', and a 'Dump gateway logs' checkbox. At the bottom of the configuration area, a 'SD Card status' box is highlighted, containing the following information:

SD Card status	
Status	SD Card OK
Free space	330235904
SD card size	330301440
Free space (%)	99

Cadre d'information sur la carte SD ci-dessus.

Afin de garantir une arborescence compatible sur toutes les cartes SD, la configuration des répertoires est non modifiable.



L'ensemble des paramètres serveur pour l'interface SD card sont uniquement accessibles via l'interface web et non stockés dans le fichier de configuration du concentrateur. Pour utiliser l'interface SD card du concentrateur, vous devez obligatoirement l'activer par l'interface web.

Les paramètres sur les 2 serveurs sont :

Interface Web	Paramètre dans le fichier de configuration <uid>_config.ini	Description
Interface	SERVER_Interface SERVER2_Interface	Choix de l'interface réseau à utiliser par le serveur : Sdcard

Si les répertoires n'existent pas sur la carte SD, ils seront créés automatiquement par le concentrateur.

Le cadre d'informations sur la carte SD contient les informations suivantes :

- Status : Statut de la carte SD, les états possibles sont :
 - Unknown : l'état n'est pas connu car aucun accès à celle-ci n'a été fait jusqu'à présent.
 - SD Card OK : la dernière tentative d'écriture sur la carte SD s'est bien déroulée.
 - Failed to mount SD Card : la carte SD n'a pas été détectée. Vérifier que la carte est correctement insérée et qu'elle est bien formatée (FAT32 ou exFAT).
 - SD Card read error : la carte SD a été détectée mais il y a eu des erreurs de lecture des informations qu'elle contient. Vérifier que la carte est correctement formatée (FAT32 ou exFAT).
- Free space : taille mémoire disponible sur la carte SD (en octet).
- SD card size : capacité de la carte SD (en octet).
- Free space (%) : pourcentage d'occupation de la carte SD. Permet de surveiller facilement et rapidement le remplissage de la carte SD.

À chaque connexion, le concentrateur va déposer les données et récupérer les informations de la carte SD. L'encart « SD Card status » reflète les informations lues à partir de la carte :



Il est bien sûr possible de forcer une connexion en cliquant sur le bouton « Connect » présent sur la page.

3.2.2.5.2 FTP/SFTP

Les serveurs FTP et SFTP ont les mêmes paramètres.

Les paramètres sur les 2 serveurs sont :

Interface Web	Paramètre dans le fichier de configuration <uid>_config.ini	Description
Interface	SERVER_Interface SERVER2_Interface	Choix de l'interface réseau à utiliser par le serveur : • Ethernet (voir chapitre 3.2.2.3 : « Réseaux (Networks) ») • Modem (voir le chapitre 3.2.2.4 : « Modem »)
Type	SERVER_Type SERVER2_Type	Choix du protocole du serveur : • FTP : serveur FTP • SFTP : serveur SFTP
Address	SERVER_Address SERVER2_Address	Adresse IP ou nom du serveur
Port	FTP_Port FTP2_Port	Port du serveur FTP/SFTP
Login	FTP_Login FTP2_Login	Nom d'utilisateur utilisé par le concentrateur pour la connexion au serveur FTP/SFTP distant

Password	FTP_Password FTP2_Password	Mot de passe utilisé par le concentrateur pour la connexion au serveur FTP/SFTP distant
2 steps for put file disabled	FTP_TwoStepsSendingDisabled FTP2_TwoStepsSendingDisabled	Choix du transfert des fichiers en 2 étapes en passant par un fichier temporaire tant que le fichier n'est pas complet sur le serveur distant : <ul style="list-style-type: none"> • Coché : désactivé • Décoché : activé
Configuration directory	FTP_DirConfig FTP2_DirConfig	Répertoire des fichiers de configuration sur le serveur FTP/SFTP
Data directory	FTP_DirData FTP2_DirData	Répertoire des fichiers de données sur le serveur FTP/SFTP
Alarm directory	FTP_DirAlarm FTP2_DirAlarm	Répertoire des fichiers d'alarmes sur le serveur FTP/SFTP
Command directory	FTP_DirCmd FTP2_DirCmd	Répertoire des fichiers de commande sur le serveur FTP/SFTP
Log directory	FTP_DirLog FTP2_DirLog	Répertoire des fichiers de logs sur le serveur FTP/SFTP
Definition directory	FTP_DirDef FTP2_DirDef	Répertoire des fichiers de définitions sur le serveur FTP/SFTP
Binary directory	FTP_DirBin FTP2_DirBin	Répertoire des fichiers de mise à jour sur le serveur FTP/SFTP
Script directory	FTP_DirScript FTP2_DirScript	Répertoire des fichiers scripts sur le serveur FTP/SFTP
Certificate directory	FTP_DirCert FTP2_DirCert	Répertoire des fichiers certificats sur le serveur FTP/SFTP
Synchronise certificates	FTP_SynchroniseCertificates FTP2_SynchroniseCertificates	Choix de synchronisation des certificats : <ul style="list-style-type: none"> • Coché : Active la synchronisation des certificats • Décoché : Aucune synchronisation des certificats

Enable data file header option	FTP_HeaderOption FTP2_HeaderOption	Choix des en-têtes optionnels dans les fichiers de données déposés sur le serveur FTP/SFTP : <ul style="list-style-type: none"> • Coché : Avec les en-têtes optionnels • Décoché : Sans les en-têtes optionnels
Enable advanced data option	FTP_EnableAdvancedData FTP2_EnableAdvancedData	Ajout du nombre de lectures complètes sur cette période d'acquisition dans les fichiers de données déposés sur le serveur FTP/SFTP : <ul style="list-style-type: none"> • Coché : Ajout du nombre de lectures complètes • Décoché : Pas d'ajout du nombre de lectures complètes
Dump gateway logs	FTP_UploadLog FTP2_UploadLog	Choix du dépôt des fichiers des logs systèmes sur le serveur FTP/SFTP : <ul style="list-style-type: none"> • Coché : Dépôt des fichiers logs systèmes sur une planification. • Décoché : Aucun dépôt de fichiers de logs système sur une planification. <p>Les logs système sont systématiquement déposés sur une action manuelle.</p>
European date format	FTP_EuroDateFormat FTP2_EuroDateFormat	Choix du type d'horodatage des données déposé sur le serveur FTP/SFTP : <ul style="list-style-type: none"> • Coché: Format européen (JJ/MM/AA-HH:MM:SS) • Décoché: Format ISO (AA/MM/JJ-HH:MM:SS)
Enable Web Services	FTP_WebServicesEnable FTP2_WebServicesEnable	Activation des services web associés aux actions FTP : <ul style="list-style-type: none"> • Coché : les services web sont activés • Décoché : les services web ne sont pas activés
Web Services URL	FTP_WebServicesUrl FTP2_WebServicesUrl	URL à appeler lorsque des actions FTP ont été effectuées et que les services web sont activés



L'arborescence des répertoires sur le serveur FTP/SFTP distant est à créer avant toute connexion. (voir chapitre 4.1 : « Le serveur FTP/SFTP/ »).

3.2.2.5.3 WebDAV over HTTPS

Le serveur WebDAV over HTTPS est un serveur sécurisé avec une identification avec un identifiant et un mot de passe.

Les paramètres sur les 2 serveurs sont :

Interface Web	Paramètre dans le fichier de configuration <uid>_config.ini	Description
Interface	SERVER_Interface SERVER2_Interface	Choix de l'interface réseau à utiliser par le serveur : <ul style="list-style-type: none"> • Ethernet (voir chapitre 3.2.2.3 : « Réseaux (Networks) ») • Modem (voir le chapitre 3.2.2.4 : « Modem »)
Type	SERVER_Type SERVER2_Type	Choix du protocole du serveur : <ul style="list-style-type: none"> • WebDAV over HTTPS
Address	SERVER_Address SERVER2_Address	Adresse IP ou nom du serveur
Port	HTTP_Port HTTP2_Port	Port du serveur WebDAV
Login	HTTP_Login HTTP2_Login	Nom d'utilisateur utilisé par le concentrateur pour la connexion au serveur WebDAV distant

Password	HTTP_Password HTTP2_Password	Mot de passe utilisé par le concentrateur pour la connexion au serveur WebDAV distant
Configuration directory	HTTP_DirConfig HTTP2_DirConfig	Répertoire des fichiers de configuration sur le serveur WebDAV
Data directory	HTTP_DirData HTTP2_DirData	Répertoire des fichiers de données sur le serveur WebDAV
Alarm directory	HTTP_DirAlarm HTTP2_DirAlarm	Répertoire des fichiers d'alarmes sur le serveur WebDAV
Command directory	HTTP_DirCmd HTTP2_DirCmd	Répertoire des fichiers de commande sur le serveur WebDAV
Log directory	HTTP_DirLog HTTP2_DirLog	Répertoire des fichiers de logs sur le serveur WebDAV
Definition directory	HTTP_DirDef HTTP2_DirDef	Répertoire des fichiers de définitions sur le serveur WebDAV
Binary directory	HTTP_DirBin HTTP2_DirBin	Répertoire des fichiers de mise à jour sur le serveur WebDAV
Script directory	HTTP_DirScript HTTP2_DirScript	Répertoire des fichiers script sur le serveur
Certificate directory	HTTP_DirCert HTTP2_DirCert	Répertoire des fichiers certificats sur le serveur WebDAV
Synchronise certificates	HTTP_SynchroniseCertificates HTTP2_SynchroniseCertificates	Choix de synchronisation des certificats : <ul style="list-style-type: none"> • Coché : Active la synchronisation des certificats • Décoché : Aucune synchronisation des certificats
Data file header option enabled	HTTP_HeaderOption HTTP2_HeaderOption	Choix des en-têtes optionnels dans les fichiers de données déposés sur le serveur WebDAV : <ul style="list-style-type: none"> • Coché : Avec les en-têtes optionnels • Décoché : Sans les en-têtes optionnels

Dump gateway logs	HTTP_UploadLog HTTP2_UploadLog	<p>Choix du dépôt des fichiers des logs système sur le serveur WebDAV :</p> <ul style="list-style-type: none"> • Coché : Dépôt des fichiers logs systèmes sur une planification. • Décoché : Aucun dépôt de fichiers de logs système sur une planification. <p>Les logs système sont systématiquement déposés sur une action manuelle.</p>
European date format	HTTP_EuroDateFormat HTTP2_EuroDateFormat	<p>Choix du type d'horodatage des données déposé sur le serveur WebDAV :</p> <ul style="list-style-type: none"> • Coché: Format européen (JJ/MM/AA-HH:MM:SS) • Décoché: Format ISO (AA/MM/JJ-HH:MM:SS)
Enable Web Services	FTP_WebServicesEnable FTP2_WebServicesEnable	<p>Activation des services web associés aux actions FTP :</p> <ul style="list-style-type: none"> • Coché : les services web sont activés • Décoché : les services web ne sont pas activés <p>Voir la section « Web Services » pour plus de détails sur le fonctionnement.</p>
Web Services URL	FTP_WebServicesUrl FTP2_WebServicesUrl	<p>URL à appeler lorsque des actions FTP ont été effectuées et que les services web sont activés.</p> <p>Voir la section « Web Services » pour plus de détails sur le fonctionnement.</p>



L'arborescence des répertoires sur le serveur distant WebDAV-HTTPS est à créer avant toute connexion. (voir chapitre 4.1 : « Le serveur FTP/SFTP/ »)

3.2.2.5.4 MQTT

Le serveur MQTT est un serveur non sécurisé avec une identification avec un identifiant et un mot de passe.

Server 2

Interface	<input type="text" value="Modem"/>	Type	<input type="text" value="MQTT"/>
Address	<input type="text" value="mqtt.webdyn.com"/>	Port	<input type="text" value="1883"/>
Login	<input type="text" value="login"/>	Password	<input type="text" value="password"/>
Timeout (s)	<input type="text" value="30"/>		
Client Id	<input type="text" value="webdynId"/>	Keepalive (s)	<input type="text" value="10"/>
Data topic	<input type="text" value="data"/>	Data qos	<input type="text" value="1"/>
Command topic	<input type="text" value="cmd"/>	Result topic	<input type="text" value="result"/>
Alarm topic	<input type="text" value="alarm"/>		

Les paramètres du serveur 2 sont :

Interface Web	Paramètre dans le fichier de configuration <uid>_config.ini	Description
Interface	SERVER2_Interface	Choix de l'interface réseau à utiliser par le serveur : <ul style="list-style-type: none">• Ethernet (voir chapitre 3.2.2.3 : « Réseaux (Networks) »)• Modem (voir le chapitre 3.2.2.4 : « Modem »)
Type	SERVER2_Type	Choix du protocole du serveur : <ul style="list-style-type: none">• MQTT : serveur MQTT
Address	SERVER2_Address	Adresse IP ou nom du serveur
Port	MQTT2_Port	Port du serveur MQTT (par défaut 1883)
Login	MQTT2_Login	Nom d'utilisateur utilisé par le concentrateur pour la connexion au serveur MQTT

Password	MQTT2_Password	Mot de passe utilisé par le concentrateur pour la connexion au serveur MQTT
Timeout (s)	MQTT2_Timeout	Délai d'attente maximum en seconde de la réponse du serveur MQTT. Si le serveur n'a pas répondu pendant le temps imparti, l'envoi est arrêté et ressuyé lors de la prochaine planification. Fonctionnel uniquement en QoS 1 ou QoS 2.
Client Id	MQTT2_ClientId	Identifiant personnalisable de l'équipement sur le serveur MQTT. Ce paramètre est à récupérer sur votre serveur MQTT.
Keepalive (s)	MQTT2_KeepAlive	Si aucun échange effectué avec le serveur MQTT pendant le temps défini en seconde, le concentrateur envoie un ping au serveur MQTT afin de vérifier la connexion à celui-ci. Si la valeur est à « 0 », le KeepAlive est désactivé. Si le concentrateur est en mode de connexion permanente avec le serveur MQTT et qu'une déconnexion est détectée après un KeepAlive, le concentrateur se reconnectera automatiquement au serveur MQTT.
Data topic	MQTT2_Topic	Nom du topic pour les données déposées par le concentrateur.

Data qos	MQTT2_QoS	<p>Numéro du service garanti pour l'envoi des messages (Quality Of Service). Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 0 : Le message sera envoyé qu'une fois, c'est-à-dire avec aucune garantie de réception. • 1 : Le message sera envoyé au moins une fois, c'est-à-dire le concentrateur transmettra plusieurs fois s'il le faut jusqu'à ce que le broker lui confirme qu'il a été transmis. • 2 : Le message sera obligatoirement sauvegardé par le concentrateur et le transmettra toujours tant que le broker ne confirme pas son envoi. (évite duplication des messages)
Command topic	MQTT2_ControlTopic	<p>Nom du topic pour les commandes à récupérer par le concentrateur. Le paramètre MQTT2_ResultTopic doit être renseigné pour l'utilisation des commandes. Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTT.</p>
Result topic	MQTT2_ResultTopic	<p>Nom du topic pour les résultats des commandes passées au concentrateur. Le paramètre MQTT2_ControlTopic doit être renseigné pour l'utilisation des commandes. Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTT.</p>
Alarm topic	MQTT2_AlarmTopic	<p>Nom du topic alarme que l'on souhaite publier. Si le champ est vide, aucune alarme ne sera publiée vers le broker. Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTT.</p>

Enable advanced data option

MQTT2_EnableAdvancedData

Publication du nombre de lectures complètes sur cette période d'acquisition dans le topic de données. Les valeurs possibles sont :

- 0 : Désactivé
- 1 : Activé



Le MQTT est uniquement disponible sur le serveur 2 (backup).

3.2.2.5.5 MQTTS

Le serveur MQTTS est un serveur sécurisé avec une identification avec un identifiant et un mot de passe. Il est nécessaire d'importer des certificats et une clé privée afin de sécuriser la connexion entre le concentrateur et le serveur MQTTS.

Server 2

Interface	Modem	Type	MQTTS
Address	mqtt.webdyn.com	Port	8883
Login	login	Password	password
Timeout (s)	30		
TLS version	TLS v1.2	Insecure	<input type="checkbox"/>
SunPM certificate	PM_cert.pem	SunPM Private Key	PM_private.key
CA certificate	PM_ca.pem		
Client Id	webdynId	Keepalive (s)	10
Data topic	data	Data qos	1
Command topic	cmd	Result topic	result
Alarm topic	alarm		

Les paramètres du serveur 2 sont :

Interface Web	Paramètre dans le fichier de configuration <uid>_config.ini	Description
Interface	SERVER2_Interface	Choix de l'interface réseau à utiliser par le serveur : <ul style="list-style-type: none">• Ethernet (voir chapitre 3.2.2.3 : « Réseaux (Networks) »)• Modem (voir le chapitre 3.2.2.4 : « Modem »)
Type	SERVER2_Type	Choix du protocole du serveur : <ul style="list-style-type: none">• MQTTS : serveur MQTT sécurisé
Address	SERVER2_Address	Adresse IP ou nom du serveur
Port	MQTT2_Port	Port du serveur MQTTS (par défaut 8883)
Login	MQTT2_Login	Nom d'utilisateur utilisé par le concentrateur pour la connexion au serveur MQTTS
Password	MQTT2_Password	Mot de passe utilisé par le concentrateur pour la connexion au serveur MQTTS
Timeout (s)	MQTT2_Timeout	Délai d'attente maximum en seconde de la réponse du serveur MQTTS. Si le serveur n'a pas répondu pendant le temps imparti, l'envoi est arrêté et ressayé lors de la prochaine planification.
TLS version	MQTT2_TlsVersion	Version TLS pris en charge par le serveur MQTTS. Les valeurs possibles sont : <ul style="list-style-type: none">• TLS v1.1• TLS v1.2
Insecure	MQTT2_Insecure	Désactiver de la vérification du nom d'hôte spécifié dans les certificats. Les valeurs possibles sont : <ul style="list-style-type: none">• Décoché : Vérification activée• Coché : Vérification désactivée.

SunPM certificate	MQTT2_CertFile	Nom du certificat spécifique au concentrateur utilisé pour la connexion. Le certificat est à récupérer sur votre serveur MQTTS et doit être importé sur le concentrateur par FTP ou par l'interface web.
SunPM Private Key	MQTT2_KeyFile	Nom du fichier comprenant la clé privée spécifique au concentrateur utilisé pour la connexion. Le fichier est à récupérer sur votre serveur MQTTS et doit être importé sur le concentrateur par FTP ou par l'interface web.
CA certificate	MQTT2_CaCertFile	Nom du certificat qui permet d'authentifier le serveur MQTTS renseigné. Le certificat est à récupérer sur votre serveur MQTTS et doit être importé sur le concentrateur par FTP ou par l'interface web.
Client Id	MQTT2_ClientId	Identifiant personnalisable de l'équipement sur le serveur MQTTS. Ce paramètre est à récupérer sur votre serveur MQTT.
Keepalive (s)	MQTT2_KeepAlive	Si aucun échange effectué avec le serveur MQTTS pendant le temps défini en seconde, le concentrateur envoie un ping au serveur MQTTS afin de vérifier la connexion à celui-ci. Si la valeur est à « 0 », le KeepAlive est désactivé. Si le concentrateur est en mode de connexion permanente avec le serveur MQTTS et qu'une déconnexion est détectée après un KeepAlive, le concentrateur se reconnectera automatiquement au serveur MQTTS.
Client Id	MQTT2_Topic	Nom du topic pour les données déposées par le concentrateur.

Data qos	MQTT2_QoS	<p>Numéro du service garanti pour l'envoi des messages (Quality Of Service). Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 0 : Le message sera envoyé qu'une fois, c'est-à-dire avec aucune garantie de réception. • 1 : Le message sera envoyé au moins une fois, c'est-à-dire le concentrateur transmettra plusieurs fois s'il le faut jusqu'à ce que le broker lui confirme qu'il a été transmis. • 2 : Le message sera obligatoirement sauvegardé par le concentrateur et le transmettra toujours tant que le broker ne confirme pas son envoi. (évite duplication des messages)
Command topic	MQTT2_ControlTopic	<p>Nom du topic pour les commandes à récupérer par le concentrateur. Le paramètre MQTT2_ResultTopic doit être renseigné pour l'utilisation des commandes. Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTTS.</p>
Result topic	MQTT2_ResultTopic	<p>Nom du topic pour les résultats des commandes passées au concentrateur. Le paramètre MQTT2_ControlTopic doit être renseigné pour l'utilisation des commandes. Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTTS.</p>
Alarm topic	MQTT2_AlarmTopic	<p>Nom du topic alarme que l'on souhaite publier. Si le champ est vide, aucune alarme ne sera publiée vers le broker. Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTTS.</p>



Le MQTTS est uniquement disponible sur le serveur 2 (backup).

3.2.2.5.6 MQTTS AWS IoT

Le serveur MQTTS AWS IoT est un serveur sécurisé d'Amazon avec une identification par certificat. Il est nécessaire d'importer des certificats et une clé privée dans le concentrateur.

Server 2

Interface	Modem	Type	MQTTS for AWS IoT
Address	webdyn.iot.amazonaws.com	Port	8883
Timeout (s)	30		
SunPM certificate	PM_cert.pem	SunPM Private Key	PM_private.key
Amazon root CA certificate	aws_rootca1.pem		
Client Id	webdynId	Keepalive (s)	10
Data topic	data	Data qos	1
Command topic	cmd	Result topic	result
Alarm topic	alarm		

Les paramètres du serveur 2 sont :

Interface Web	Paramètre dans le fichier de configuration <uid>_config.ini	Description
Interface	SERVER2_Interface	Choix de l'interface réseau à utiliser par le serveur : <ul style="list-style-type: none">• Ethernet (voir chapitre 3.2.2.3 : « Réseaux (Networks) »)• Modem (voir le chapitre 3.2.2.4 : « Modem »)
Type	SERVER2_Type	Choix du protocole du serveur : <ul style="list-style-type: none">• MQTTS for AWS IoT : serveur MQTTS sur « AWS IoT »
Address	SERVER2_Address	Adresse IP ou nom du serveur

Port	MQTT2_Port	Port du serveur MQTT (par défaut 8883)
Timeout (s)	MQTT2_Timeout	Délai d'attente maximum en seconde de la réponse du serveur MQTT. Si le serveur n'a pas répondu pendant le temps imparti, l'envoi est arrêté et ressayé lors de la prochaine planification. Fonctionnel uniquement en QoS 1 ou QoS 2.
SunPM certificate	MQTT2_CertFile	Nom du certificat spécifique au concentrateur utilisé pour la connexion. Le certificat est à récupérer sur votre serveur MQTTS et doit être importé sur le concentrateur par FTP ou par l'interface web.
SunPM Private Key	MQTT2_KeyFile	Nom du fichier contenant la clé privée spécifique au concentrateur utilisé pour la connexion. Le fichier est à récupérer sur votre serveur MQTTS et doit être importé sur le concentrateur par FTP ou par l'interface web.
Amazon root CA certificate	MQTT2_CaCertFile	Nom du certificat qui permet d'authentifier le serveur MQTTS renseigné. Le certificat est à récupérer sur votre serveur MQTTS et doit être importé sur le concentrateur par FTP ou par l'interface web.
Client Id	MQTT2_ClientId	Identifiant personnalisable de l'équipement sur le serveur MQTT.
Keepalive (s)	MQTT2_KeepAlive	Si aucun échange effectué avec le serveur MQTT pendant le temps défini en seconde, le concentrateur envoie un ping au serveur MQTT afin de vérifier la connexion à celui-ci. Si la valeur est à « 0 », le KeepAlive est désactivé. Si le concentrateur est en mode de connexion permanente avec le serveur MQTT et qu'une déconnexion est détectée après un KeepAlive, le concentrateur se reconnectera automatiquement au serveur MQTT.

Data topic	MQTT2_Topic	Nom du topic pour les données déposées par le concentrateur.
Data qos	MQTT2_QoS	<p>Numéro du service garanti pour l'envoi des messages (Quality Of Service). Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 0 : Le message sera envoyé qu'une fois, c'est-à-dire avec aucune garantie de réception. • 1 : Le message sera envoyé au moins une fois, c'est-à-dire le concentrateur transmettra plusieurs fois s'il le faut jusqu'à ce que le broker lui confirme qu'il a été transmis. • 2 : Non géré par le serveur MQTTS AWS IoT
Command topic	MQTT2_ControlTopic	<p>Nom du topic pour les commandes à récupérer par le concentrateur. Le paramètre MQTT2_ResultTopic doit être renseigné pour l'utilisation des commandes.</p> <p>Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTTS.</p>
Result topic	MQTT2_ResultTopic	<p>Nom du topic pour les résultats des commandes passées au concentrateur. Le paramètre MQTT2_ControlTopic doit être renseigné pour l'utilisation des commandes.</p> <p>Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTTS.</p>
Alarm topic	MQTT2_AlarmTopic	<p>Nom du topic alarme que l'on souhaite publier. Si le champ est vide, aucune alarme ne sera publiée vers le broker. Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTTS.</p>

Enable advanced data option

MQTT2_EnableAdvancedData

Publication du nombre de lectures complètes sur cette période d'acquisition dans le topic de données. Les valeurs possibles sont :

- 0 : Désactivé
- 1 : Activé



Le MQTTS AWS IoT est uniquement disponible sur le serveur 2 (backup).

3.2.2.5.7 MQTTS Google Cloud IoT

Le serveur MQTTS Google Cloud IoT est un serveur sécurisé de Google avec une identification par certificats. Il est nécessaire d'importer un certificat et une clé privée dans le concentrateur.

Server 2

Interface	Modem	Type	MQTTS for Google Cloud
Address	mqtt.googleapis.com	Port	8883
Timeout (s)	30		
SunPM Private Key	PM_rsa_private.pem		
Google root CA certificate	google_roots.pem	Signing algo	RSA
Cloud project id	WebdynId	Cloud registry	RegistryPM
Cloud region	europa-west1	Cloud device	PM
Keepalive (s)	10		
Data subfolder	SubfolderPM	Data qos	1
Command subfolder	SubfolderCtrlPM	Result subfolder	SubfolderResultPM
Alarm subfolder	SubfolderAlarmPM		

Les paramètres du serveur 2 sont :

Interface Web	Paramètre dans le fichier de configuration <uid>_config.ini	Description
Interface	SERVER2_Interface	Choix de l'interface réseau à utiliser par le serveur : <ul style="list-style-type: none">• Ethernet (voir chapitre 3.2.2.3 : « Réseaux (Networks) »)• Modem (voir le chapitre 3.2.2.4 : « Modem »)
Type	SERVER2_Type	Choix du protocole du serveur : <ul style="list-style-type: none">• MQTTS for Google Cloud IoT : serveur MQTTS sur « Google Cloud IoT »
Address	SERVER2_Address	Adresse IP ou nom du serveur
Port	MQTT2_Port	Port du serveur MQTT (par défaut 8883)
Timeout (s)	MQTT2_Timeout	Délai d'attente maximum en seconde de la réponse du serveur MQTT. Si le serveur n'a pas répondu pendant le temps imparti, l'envoi est arrêté et ressayé lors de la prochaine planification. Fonctionnel uniquement en QoS 1 ou QoS 2.
SunPM Private Key	MQTT2_KeyFile	Nom du fichier comprenant la clé privée spécifique au concentrateur utilisé pour la connexion. Le fichier est à récupérer sur votre serveur MQTTS et doit être importé sur le concentrateur par FTP ou par l'interface web.
Google root CA certificate	MQTT2_CaCertFile	Nom du certificat qui permet d'authentifier le serveur MQTTS renseigné. Le certificat est à récupérer sur votre serveur MQTTS et doit être importé sur le concentrateur par FTP ou par l'interface web.

Signing algo	MQTT2_CloudSigningAlgo	Type de clé utilisé pour vérifier la signature du certificat du serveur MQTTS. Ce paramètre est à récupérer sur votre serveur Google IoT Cloud. Les valeurs possibles sont : <ul style="list-style-type: none"> • « RSA » pour la clé RSA • « Elliptic Curve » pour la clé de courbe elliptique
Cloud project Id	MQTT2_CloudProjectId	Identifiant unique personnalisable du projet défini sur le serveur MQTT. Ce paramètre est à récupérer sur votre serveur MQTT et correspond à « projectId » sur Google Cloud IoT.
Cloud registry	MQTT2_CloudRegistry	Nom du registre personnalisable définie sur le serveur MQTT. Ce paramètre est à récupérer sur votre serveur MQTT et correspond à « deviceRegistryId » sur Google Cloud IoT.
Cloud region	MQTT2_CloudRegion	Région du serveur MQTT du registre des équipements. Ce paramètre est à récupérer sur votre serveur MQTT et correspond à « deviceRegistryLocation » sur Google IoT Cloud. Par exemple : « europe-west1 »
Cloud device	MQTT2_CloudDevice	Identifiant unique personnalisable de l'équipement dans un registre défini sur le serveur MQTT. Ce paramètre est à récupérer sur votre serveur MQTT et correspond à « deviceId » sur Google IoT Cloud.

Keepalive (s)	MQTT2_KeepAlive	<p>Si aucun échange effectué avec le serveur MQTT pendant le temps défini en seconde, le concentrateur envoie un ping au serveur MQTT afin de vérifier la connexion à celui-ci.</p> <p>Si la valeur est à « 0 », le KeepAlive est désactivé.</p> <p>Si le concentrateur est en mode de connexion permanente avec le serveur MQTT et qu'une déconnexion est détectée après un KeepAlive, le concentrateur se reconnectera automatiquement au serveur MQTT.</p>
Data subfolder	MQTT2_Topic	Nom du topic pour les données déposées par le concentrateur.
Data qos	MQTT2_QoS	<p>Numéro du service garanti pour l'envoi des messages (Quality Of Service). Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 0 : Le message sera envoyé qu'une fois, c'est-à-dire avec aucune garantie de réception. • 1 : Le message sera envoyé au moins une fois, c'est-à-dire le concentrateur transmettra plusieurs fois s'il le faut jusqu'à ce que le broker lui confirme qu'il a été transmis. • 2 : Non géré par le serveur MQTTS Google Cloud IoT
Command subfolder	MQTT2_ControlTopic	<p>Nom du topic pour les commandes à récupérer par le concentrateur.</p> <p>Le paramètre MQTT2_ResultTopic doit être renseigné pour l'utilisation des commandes.</p> <p>Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTTS.</p>

Result subfolder	MQTT2_ResultTopic	Nom du topic pour les résultats des commandes passées au concentrateur. Le paramètre MQTT2_ControlTopic doit être renseigné pour l'utilisation des commandes. Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTTS.
Alarm subfolder	MQTT2_AlarmTopic	Nom du topic alarme que l'on souhaite publier. Si le champ est vide, aucune alarme ne sera publiée vers le broker. Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTTS.
Enable advanced data option	MQTT2_EnableAdvancedData	Publication du nombre de lectures complètes sur cette période d'acquisition dans le topic de données. Les valeurs possibles sont : <ul style="list-style-type: none"> • 0 : Désactivé • 1 : Activé



Le MQTTS Google Cloud IoT est uniquement disponible sur le serveur 2 (backup).

3.2.2.5.8 MQTTS Azure IoT Hub

Le serveur MQTTS Azure IoT Hub est un serveur sécurisé de Microsoft avec une identification par certificat. Il est nécessaire d'importer un certificat et une clé privée dans le concentrateur.

Les paramètres du serveur 2 sont :

Interface Web	Paramètre dans le fichier de configuration <uid>_config.ini	Description
Interface	SERVER2_Interface	Choix de l'interface réseau à utiliser par le serveur : <ul style="list-style-type: none"> • Ethernet (voir chapitre 3.2.2.3 : « Réseaux (Networks) ») • Modem (voir le chapitre 3.2.2.4 : « Modem »)
Type	SERVER2_Type	Choix du protocole du serveur : <ul style="list-style-type: none"> • MQTTS for Azure IoT Hub : serveur MQTTS sur « Azure IoT Hub »
Address	SERVER2_Address	Adresse IP ou nom du serveur
Port	MQTT2_Port	Port du serveur MQTT (par défaut 8883)

Timeout (s)	MQTT2_Timeout	Délai d'attente maximum en seconde de la réponse du serveur MQTT. Si le serveur n'a pas répondu pendant le temps imparti, l'envoi est arrêté et ressayé lors de la prochaine planification. Fonctionnel uniquement en QoS 1 ou QoS 2.
SunPM certificate	MQTT2_CertFile	Nom du certificat spécifique au concentrateur utilisé pour la connexion. Le certificat est à récupérer sur votre serveur MQTTS et doit être importé sur le concentrateur par FTP ou par l'interface web.
Private or shared key	MQTT2_KeyFile	Nom du fichier comprenant la clé privée spécifique ou clé partagée au concentrateur utilisé pour la connexion. Le fichier est à récupérer sur votre serveur MQTTS et doit être importé sur le concentrateur par FTP ou par l'interface web.
Azure root CA certificate	MQTT2_CaCertFile	Nom du certificat qui permet d'authentifier le serveur MQTTS renseigné. Le certificat est à récupérer sur votre serveur MQTTS et doit être importé sur le concentrateur par FTP ou par l'interface web.
Cloud IoT Hub	MQTT2_CloudProjectId	Identifiant unique personnalisable du projet défini sur le serveur MQTT. Ce paramètre est à récupérer sur votre serveur MQTT et correspond à « lot Hub » sur Azure IoT Hub.
Cloud device	MQTT2_CloudDevice	Identifiant unique personnalisable de l'équipement dans un registre définie sur le serveur MQTT. Ce paramètre est à récupérer sur votre serveur MQTT et correspond à « device_id » sur Azure IoT Hub.

Keepalive (s)	MQTT2_KeepAlive	<p>Si aucun échange effectué avec le serveur MQTT pendant le temps défini en seconde, le concentrateur envoie un ping au serveur MQTT afin de vérifier la connexion à celui-ci.</p> <p>Si la valeur est à « 0 », le KeepAlive est désactivé.</p> <p>Si le concentrateur est en mode de connexion permanente avec le serveur MQTT et qu'une déconnexion est détectée après un KeepAlive, le concentrateur se reconnectera automatiquement au serveur MQTT.</p>
Data qos	MQTT2_QoS	<p>Numéro du service garanti pour l'envoi des messages (Quality Of Service). Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 0 : Le message sera envoyé qu'une fois, c'est-à-dire avec aucune garantie de réception. • 1 : Le message sera envoyé au moins une fois, c'est-à-dire le concentrateur transmettra plusieurs fois s'il le faut jusqu'à ce que le broker lui confirme qu'il a été transmis. • 2 : Non géré par le serveur MQTTS Azure IoT Hub
Enable invoke method	MQTT2_EnableInvokeMethod	<p>Activer l'appel des méthodes. Permet d'utiliser les topics dédiés. Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • Décoché : Désactive l'appel des méthodes • Coché : Activé de l'appel des méthodes. Le concentrateur reste en mode de connexion permanente avec le serveur MQTTS.
Publish alarms	MQTT2_EnableAlarmPost	<p>Activer la publication des alarmes sur le topic dédié. Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • Décoché : Désactive la publication des alarmes • Coché : Active la publication des alarmes. Le concentrateur reste en mode de connexion permanente avec le serveur MQTTS.

Enable advanced data option

MQTT2_EnableAdvancedData

Publication du nombre de lectures complètes sur cette période d'acquisition dans le topic de données. Les valeurs possibles sont :

- 0 : Désactivé
- 1 : Activé



Le MQTTS Azure IoT Hub est uniquement disponible sur le serveur 2 (backup).

3.2.2.5.9 Schedules :

Sur chaque serveur, configurer un ensemble de planification horaire « Schedules » de connexion.

Mode	Start time	Interval	Count			
Everyday	00:00:00	60	24	[Apply]	[Undo]	[Delete]
Monday	12:30:00	0	0	[Apply]	[Undo]	[Delete]

Ajouter un Schedule

Appliquer les modifications

Supprimer les modifications

Supprimer le Schedule

Les paramètres des « Schedules » sont :

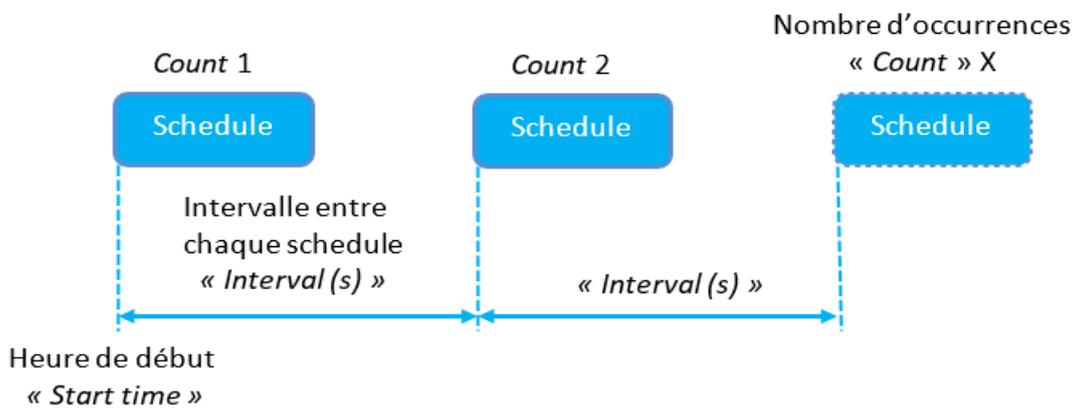
Schedule	Description
Mode	Choix du type de planification : <ul style="list-style-type: none">• Everyday : la planification sera exécutée tous les jours• Monday : la planification se fera tous les lundis• Tuesday : la planification se fera tous les mardis• Wednesday : la planification se fera tous les mercredis• Thursday : la planification se fera tous les jeudis• Friday : la planification se fera tous les vendredis• Saturday : la planification se fera tous les samedis• Sunday : la planification se fera tous les dimanches• First day of each month : la planification se fera tous les 1er du mois• 15th of each month : la planification se fera tous les 15 du mois• Last day of each month : la planification se fera le dernier jour de chaque mois

Start time	Heure de démarrage de la planification (schedule) en : « HH:MM:SS »
Interval	Fréquence de répétition de la planification (schedule) en minutes. Cas particulier la valeur « 0 » est automatiquement modifiée en « 1 »
Count	Nombre maximal de planifications à établir dans la journée. 0 = aucune plan



La planification se fait uniquement sur une journée si les paramètres dépassent la journée alors seulement seront prise en compte les déclenchements ne dépassant pas les 23H59.

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



« Count » : si le schedule doit être déclenché toute la journée à intervalle régulier, vous pouvez renseigner une valeur supérieure à « 1440 » pour le « Count ».

Exemple 1 :

Pour un dépôt période des fichiers toutes les heures, il faudra configurer la planification de cette façon :

Mode	Start time	Interval	Count			
Everyday	00:00:00	60	24			

Exemple 2 :

Pour un dépôt période des fichiers tous les dimanches à midi, il faudra configurer la planification de cette façon :

Mode	Start time	Interval	Count			
Sunday	12:00:00	1	1			

3.2.2.6 Date et heure (Date & Time)

La partie Date et Heure « Date & Time » permet de configurer la date et l'heure du concentrateur ainsi que les serveurs NTP.

Fuseau Horaire (Time zone) :



La liste des zones horaires est disponible en Annexe B : Liste des zones horaires.

Après le choix d'un fuseau horaire, il faut cliquer sur le bouton « Appliquer » pour prendre en compte le nouveau fuseau. La date et l'heure sont mises instantanément à jour et le choix du décalage horaire par rapport à l'UTC est précisé sur l'interface web.

Les changements horaires influent dans le nom des fichiers générés et les données enregistrées qui sont ensuite déposés sur le serveur distant par le concentrateur.

Par exemple, si vous choisissez le fuseau horaire « (GMT+01 :00) Europe : Brussels, Copenhagen, Madrid, Paris » alors le concentrateur indiquera : **15/02/2021 13:00 UTC+1**

Le paramètre date et heure est :

Interface Web	Paramètre dans le fichier de configuration <uid>_config.ini	Description
Time zone	NTP_TimeZone	<p>Choix du fuseau horaire :</p> <p>(GMT-11:00) Midway Island, Samoa (GMT-10:00) Honolulu (GMT-10:00) Tahiti (GMT-09:30) Marquesas (GMT-09:00) Anchorage (GMT-08:00) Pacific Time (US and Canada) (GMT-08:00) Los angeles (GMT-07:00) Denver (GMT-07:00) Chihuahua, La Paz, Mazatlan (GMT-06:00) Guadalajara, Mexico City, Monterrey (GMT-06:00) Chicago, Central America (GMT-05:00) Bogota, Lima, Quito (GMT-05:00) New York (GMT-04:00) Atlantic Time (Canada) (GMT-04:00) Caracas (GMT-04:00) Martinique (GMT-04:00) Guadeloupe (GMT-03:30) Newfoundland, St Johns (GMT-03:00) Antarctica (GMT-03:00) Sao Paulo (GMT-02:00) Brazil (GMT-01:00) Azores UTC (GMT+01:00) Europe: Brussels, Copenhagen, Madrid, Paris (GMT+01:00) Algiers (GMT+02:00) Athens, Bucharest, Istanbul (GMT+02:00) Cairo (GMT+03:00) Moscow, St. Petersburg, Volgograd (GMT+03:00) Kuwait, Riyadh (GMT+04:00) Abu Dhabi, Dubai, Muscat (GMT+04:00) Baku, Tbilisi, Yerevan (GMT+04:30) Kabul (GMT+05:00) Karachi (GMT+05:00) Tashkent (GMT+05:30) Kolkata (GMT+05:45) Katmandu (GMT+06:00) Astana, Dhaka (GMT+06:00) Almaty, Novosibirsk (GMT+06:30) Rangoon, Yangon (GMT+06:30) Cocos (GMT+07:00) Bangkok, Hanoi, Jakarta (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Shanghai (GMT+08:00) Taipei (GMT+09:00) Osaka, Sapporo, Tokyo (GMT+09:00) Seoul (GMT+09:30) Darwin (GMT+10:00) Brisbane, Sydney (GMT+10:00) Guam, Port Moresby (GMT+10:30) Adelaide (GMT+11:00) Noumea (GMT+11:00) Magadan, Solomon Islands (GMT+13:00) Auckland, Wellington</p>



Les décalages horaires des pays ne sont pris en compte par le concentrateur.

NTP:

Les paramètres du NTP sont :

Interface Web	Paramètre dans le fichier de configuration <uid>_config.ini	Description
NTP server 1	NTP_Server1	Adresse du serveur NTP 1 utilisé pour la synchronisation de l'horloge du concentrateur.
NTP server 2	NTP_Server2	Adresse du serveur NTP 2 utilisé pour la synchronisation de l'horloge du concentrateur si le serveur 1 n'a pas répondu.



Si les valeurs des serveurs NTP1 et NTP2 sont vides, alors le concentrateur ne réalisera pas de synchronisation par NTP.



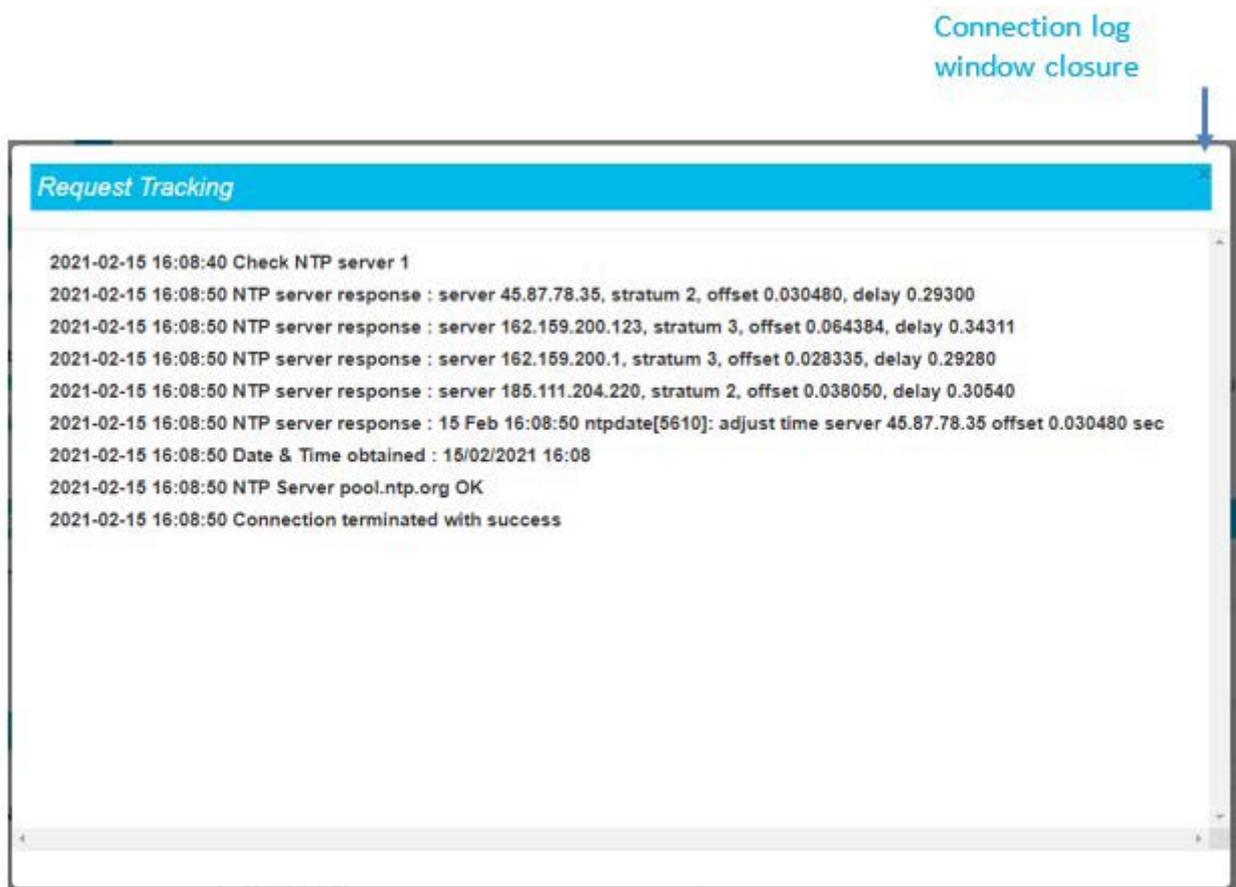
Par défaut, le concentrateur utilise le serveur NTP gratuit « pool.ntp.org », ce serveur ne garantit

pas l'exactitude de la synchronisation horaire et sa robustesse. Il est fortement conseillé d'utiliser un serveur NTP dédié. Rapprochez-vous d'un portail ou d'un fournisseur de serveur NTP.

Après avoir renseigné serveur NTP, il est possible de le tester en cliquant sur un des boutons suivants :

- « Set time from NTP » : lance la synchronisation du serveur NTP1 et si nécessaire sur le serveur NTP2 puis applique sur le concentrateur.
- « Check NTP1 » : Test la synchronisation du serveur NTP1 mais n'applique sur le concentrateur.
- « Check NTP2 » : Test la synchronisation du serveur NTP2 mais n'applique sur le concentrateur.

Une fenêtre s'ouvre affichant le journal de connexion :



La dernière ligne du journal comportant le résultat du test est affichée et mémorisée sur la page principale de la page web. Il est également possible de réafficher le dernier log de connexion en cliquant sur le bouton « Loupe ».

Il est possible de synchroniser l'horaire du concentrateur avec celui du PC en cliquant sur le bouton « Set time from PC ». Le fuseau horaire configuré dans le concentrateur est ensuite appliqué.

3.2.2.7 Mot de passe (Password)

Le champ « password » permet de modifier le mot de passe qui autorise l'accès à l'interface web.

The image shows a web interface for changing a password. It features a blue header with the text 'Password change'. Below the header, there is a form with a grey background. The form has three input fields: 'Old password', 'New Password', and 'Confirm password'. At the bottom of the form, there are two buttons: 'Annuler' (Cancel) and 'Appliquer les modifications' (Apply changes). Blue arrows point from the labels 'Annuler' and 'Appliquer les modifications' to their respective buttons.

Pour changer le mot de passe, il faut suivre les étapes suivantes :

- Indiquer le mot de passe actuel dans le champ « Old password ».
- Entrer le nouveau mot de passe dans le champ « New Password ».
- Saisir à nouveau le nouveau mot de passe dans le champ « Confirm password ».
- Valider en cliquant sur le bouton « Appliquer ».



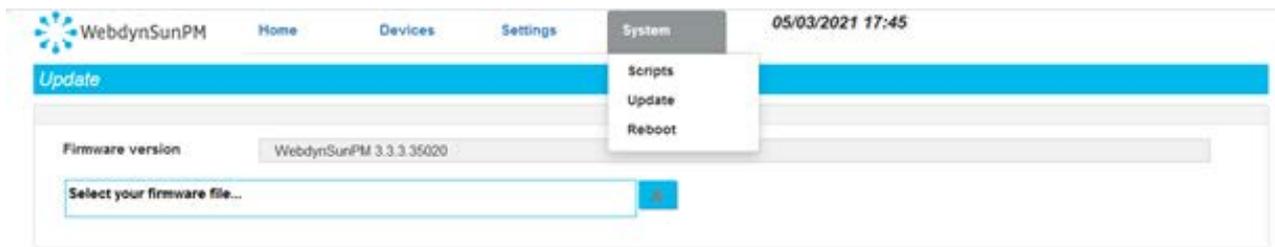
Pour sécuriser l'accès au concentrateur, il est très fortement recommandé de modifier le mot de passe par défaut après la première configuration. La modification du mot de passe peut se faire également par la variable « WEB_Password » du fichier de config « <uid>_config.ini ».



Si vous perdez le mot de passe et qu'aucun serveur n'est configuré, vous devrez réinitialiser entièrement le concentrateur en faisant un retour usine via une commande SMS factory (voir chapitre 5.3.3 : « « factory » : Retour aux paramètres usines »Erreur ! Source du renvoi introuvable.) ou par le bouton « Retour Usine » (voir chapitre 2.4.3.2 : « Bouton Retour Usine (Factory Reset) »).

3.2.3 Système (System)

L'ensemble des paramètres du système sont réunis dans l'onglet système « System ».



3.2.3.1 Scripts

Le concentrateur WebdynSunPM intègre un puissant outil de gestion des équipements et de personnalisation par scripts.

Cet outil s'appuie sur un interpréteur de commandes LUA permettant d'exécuter des tâches en arrière-plan sur le concentrateur.

Un guide technique de référence est à disposition décrivant en détail toutes les commandes et possibilités du langage de script fourni. (« WebdynSunPM LUA User Guide.pdf »)

L'accès à la configuration et gestion des scripts se fait par les pages du site web local :



De cette page il est possible d'importer de nouveaux scripts, les activer, désactiver ou même les supprimer, ou voir le log d'exécution.

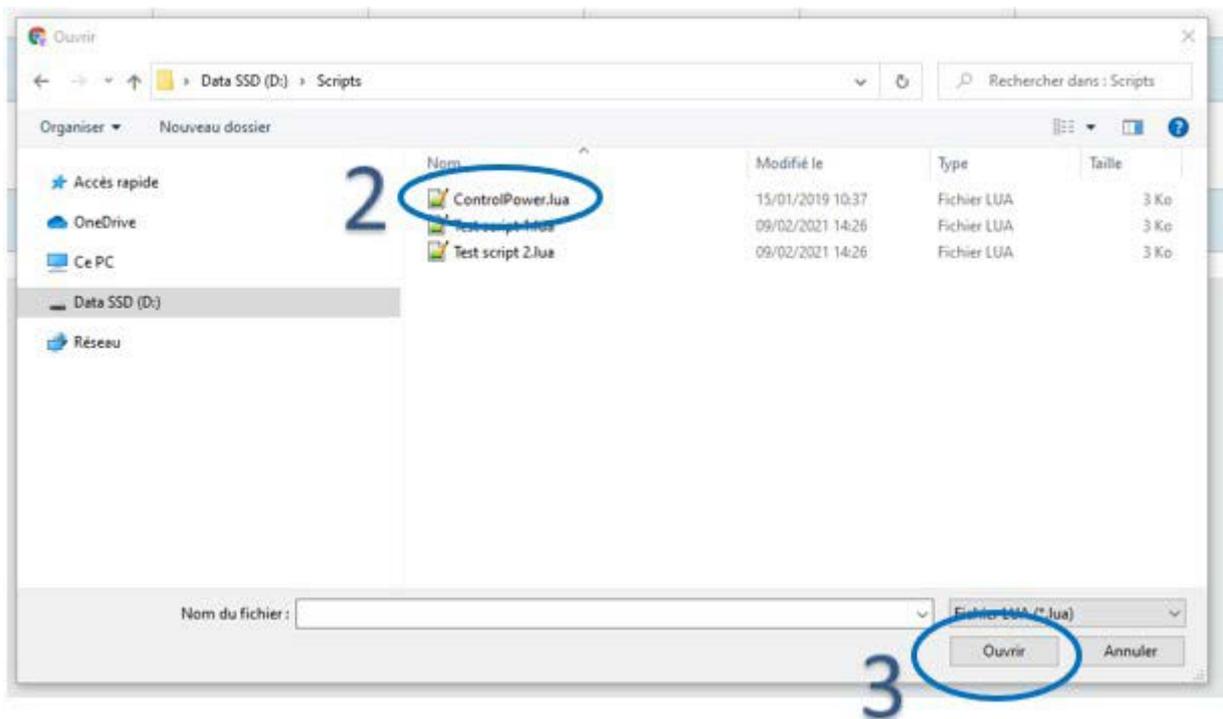
3.2.3.1.1 Importer un script ou une licence

Le seul moyen pour importer un nouveau script dans le concentrateur est de passer par le site web local.

Pour ce faire, il faut cliquer sur la zone « Select your script file » comme ci-dessous.



Une fenêtre de dialogue apparaît alors pour sélectionner le fichier à importer.
Sélectionner alors le fichier à importer et cliquer sur « Ouvrir ».



Enfin, cliquer sur le bouton de transfert pour finaliser l'opération.



Une fois cette 4ème étape franchie, le script va apparaître dans la fenêtre de gestion des scripts.

Name	Description	Version	Status	Script args						
test_INV	Test INV	1	Enabled	param1						
test_relay	relay control	1.1	Disabled							
ControlPower	SandBox	1.0	Disabled							



Lors de l'import d'un script au format « .lua » si le message d'erreur suivant s'affiche « error:Error deciphering test_script.lua : stoul », cela signifie que la WebdynSunPM n'a pas les clés de déchiffrement. Dans ce cas, il faut les envoyer en utilisant la commande « setKey ». (Voir le chapitre 5.3.14 : « « setKey » : Ajout des clés pour le déchiffrement des scripts clients »).

Il est à noter que les scripts sont importés arrêtés, c'est-à-dire qu'ils ne sont pas démarrés automatiquement.

Les informations affichées dans la page web proviennent du script, et, notamment de la section « header ». En effet, le script « ControlPower.lua » démarre par la séquence suivante :

```
header = {  
    version = 1.1,  
    label = "Demo control power"  
}
```

On retrouve donc la description affichée, qui provient de l'information « label » ainsi que le numéro de version qui provient de l'information « version ». Voir le document « WebdynSunPM LUA User Guide.pdf » pour plus de détails.

Name	Description	Version	Status	Script args			
test_INV	Test INV	1	Enabled	param1			

Annotations with arrows pointing to icons in the table above:

- Paramètres du script (points to the 'param1' cell)
- Validation (points to the green checkmark icon)
- Suppression (points to the red X icon)

Il est possible de passer des paramètres au script, il suffit de renseigner le champ « Script args » et de valider en cliquant sur la coche vert « Validation » pour que le script les prenne en compte lors de son activation. Pour supprimer des paramètres, il faut pour cela cliquer sur la coche rouge « Suppression ».

3.2.3.1.2 Activer/Désactiver un script

Activer un script signifie démarrer son exécution au sein du concentrateur. En pratique, la fonction « wslnit() » du script LUA est exécutée :

```
function wsInit()  
    wd.log("Control power initialized")  
end
```

Voir le document « WebdynSunPM LUA User Guide.pdf » pour plus de détails sur ce qu'il est possible de faire.

Désactiver un script signifie arrêter son exécution.



Lorsque la WebdynSunPM est redémarrée, tous les scripts reviennent au même état qu'avant. Par exemple, si le script était démarré, il sera démarré.

L'activation et désactivation se font en appuyant sur le bouton dédié :

Name	Description	Version	Status	Script args							
test_INV	Test INV	1	Enabled	param1							
test_relay	relay control	1.1	Disabled								
ControlPower	SandBee	1.0	Disabled								

Lorsque le script est désactivé, son statut apparaît grisé et affiche « Disabled ».

Lorsque le script est activé, son statut apparaît noir et affiche « Enabled ».

3.2.3.1.3 Visualiser le Log du script

Les scripts ont la possibilité de remonter des informations à l'utilisateur final, par le biais de la fonction « wd.log() ».

Ainsi, le code suivant affichera la chaîne « Control power initialized » dans le fichier log du script au démarrage :

```
function wsInit()  
    wd.log("Control power initialized")  
end
```

L'affichage du fichier de log se fait en appuyant sur le bouton de visualisation :



Name	Description	Version	Status	Script args	Stop	Start	Refresh	View Log	Share	Download	Help
test_INV	Test INV	1	Enabled	param1	⏹	▶	🔄	🔍	📄	📄	👤
test_relay	relay control	1.1	Disabled		⏹	▶	🔄	🔍	📄	📄	👤
ControlPower	SandBox	1.0	Disabled		⏹	▶	🔄	🔍	📄	📄	👤

L'appui sur le bouton affiche alors la page suivante :



La fermeture de la page s'effectue en appuyant sur la croix en haut à droite, indiquée dans le cercle ci-dessus.

3.2.3.1.4 Visualiser le script

Il est possible d'afficher le code source des scripts chargés sur le concentrateur en cliquant sur le bouton d'affichage :



script
X

```

1 header = {
2   version = 1.1,
3   label = "Demo control power"
4 }
5
6 local stateCdeOnOff
7 local stateReqPwr
8 local stateTotalPwr
9
10 --[[
11 Variables objects : Objects used to get or set variables
12 ]]
13 local reqPwrVar          -- int percent : Requested power from CTRL device
14 local totalPwrVar      -- in Watt : Mean pwr from Inverters set to CTRL device
15
16 local cdeOnOffVars -- OnOff command to Inverters
17 local cdePwrVars    -- In percent : requested out power from inverters
18 local pwrVars        -- In watt : measured output power from inverters
19
20
21 --[[
22 wsInit : called once when the script is enabled or Webdyn sun PM starts
23 ]]
24 function wsInit()
25   wd.log("Control power initialized")
26
27   -- current state = -1 so any change to 0 or 1 will be a change and will trigger a change
28   stateCdeOnOff = -1
29   stateReqPwr = -1
30   stateTotalPwr = -1
31
32   -- Get variable object for CTRL device
33   reqPwrVar = wd.getDeviceVar("CTRL", "reqPwr")
34   totalPwrVar = wd.getDeviceVar("CTRL", "totalPwr")
35
36   assert(reqPwrVar, "A device CTRL with reqPwr must exists")

```

Lorsque le code source d'un script est affiché, il faut cliquer sur la croix en haut à droite de la fenêtre pour la faire disparaître.

3.2.3.1.5 Exporter un script

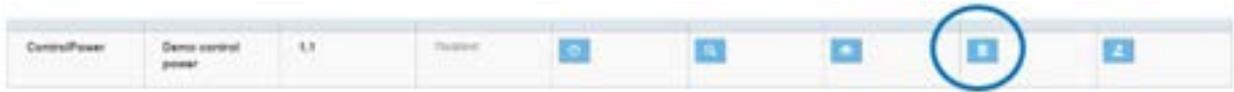
L'appui sur le bouton d'export de script lance un chargement immédiat du script en local par le navigateur.



Lorsque l'utilisateur clique sur ce bouton, le script est directement chargé dans le répertoire de téléchargements du navigateur en utilisant le nom dans le champ « Name », suivi du suffixe « .lua ». Il n'y a pas de message de confirmation.

3.2.3.1.6 Supprimer un script

Le bouton de suppression des scripts permet de supprimer les scripts chargés.



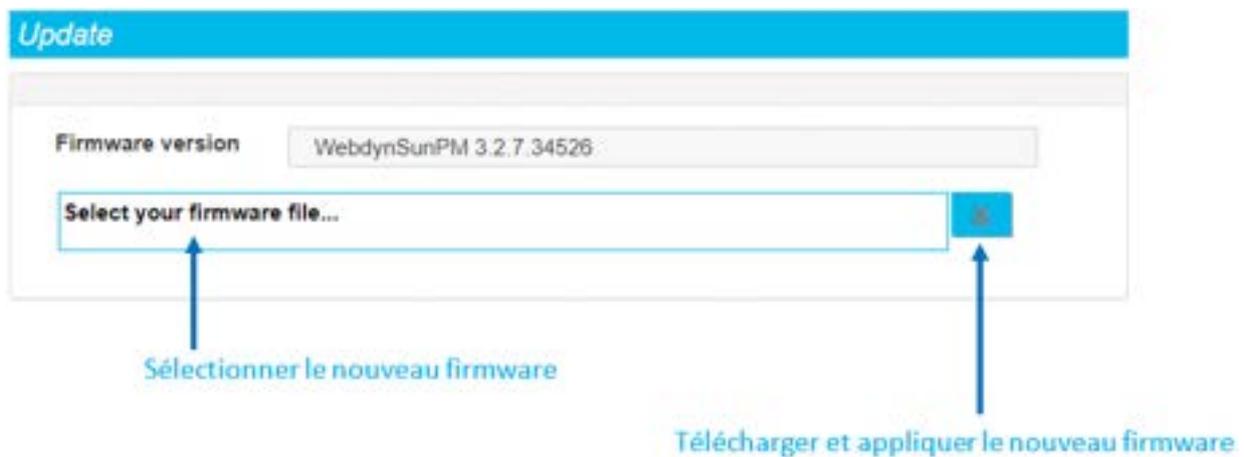
Il n'est pas nécessaire de désactiver les scripts avant de les supprimer.



Il est à noter qu'il n'y a pas de message de confirmation lors de la suppression d'un script.

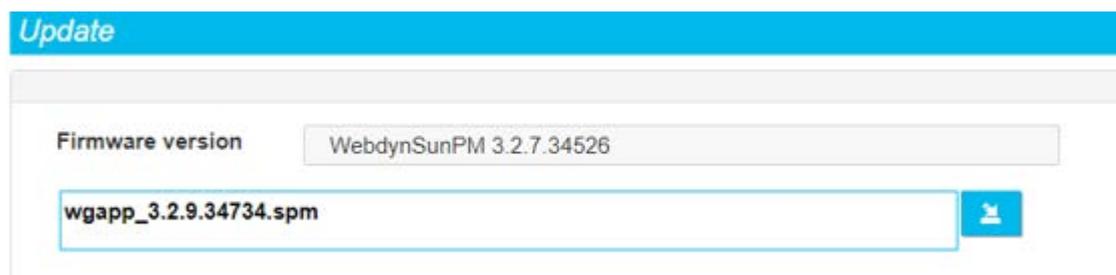
3.2.3.2. Mise à jour (Update)

Le menu Mise à jour « Update » de l'interface web permet de mettre à jour le concentrateur.



Pour procéder à la mise à jour du concentrateur, il faut suivre les étapes suivantes :

- Récupérer le dernier firmware sur le site (voir chapitre 6 : « Mise à jour ») : <https://www.webdyn.com/support/WebdynSunPM/>.
- Dézipper le fichier récupéré.
- Cliquer sur le champ « Select your firmware file ». Une fenêtre s'ouvre permettant de sélectionner le nouveau firmware.
- Sélectionner le firmware « wgapp_x.x.x.xxxxx.spm » qui comprend une extension « .spm ».



- Appuyer sur le bouton « Télécharger et appliquer le nouveau firmware ».
- Suivre l'évolution de la mise à jour dans la fenêtre qui s'ouvre :



- Veuillez patienter pendant l'application de la mise à jour et le redémarrage du concentrateur.
- Actualiser la page web (touche F5 du clavier).
- Connectez-vous à nouveau sur le concentrateur (voir chapitre 3.2 : « Interface web embarquée »).
- Retourner sur le page de mise à jour « Upgrade » du concentrateur.
- Vérifier que la nouvelle version est indiquée dans le champ Firmware version.



- Le concentrateur a été mis à jour.



Ne pas débrancher le concentrateur et éviter toutes manipulations dessus pendant la mise à jour du concentrateur.



Si une erreur survient pendant la mise à jour, le concentrateur conservera son firmware précédemment fonctionnel. Veuillez dans ce cas recommencer scrupuleusement la procédure de mise à jour.

3.2.3.3. Redémarrage de la WebdynSunPM (Reboot)

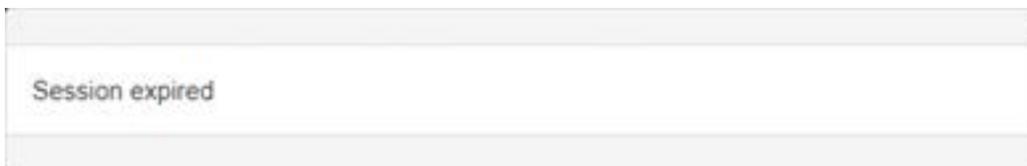
Le menu Redémarrage « Reboot » de l'interface web permet de redémarrer simplement le concentrateur.

Pour procéder au redémarrage du concentrateur, il faut suivre les étapes suivantes :

1. Cliquer le bouton OK de la nouvelle fenêtre.



2. Veuillez patienter pendant le redémarrage du concentrateur. L'écran est alors grisé, pendant le redémarrage puis une fois le concentrateur redémarré, celui-ci affichera l'écran suivant :



3. Actualiser la page web (touche F5 du clavier)

4. Connectez-vous à nouveau sur le concentrateur (voir chapitre 3.2 : « »)

5. Le concentrateur est à nouveau prêt.

3.3 Carte Micro SD

La configuration par carte Micro SD suit le même fonctionnement que décrit précédemment avec le serveur FTP/SFTP/WebDAV (Voir chapitre 3.1 : « FTP/SFTP/WebDAV »).

La seule différence réside dans le fait que le concentrateur n'a pas besoin d'une connexion vers le serveur distant puisque tous les fichiers seront accessibles directement sur la carte SD insérée.

Aussi, les répertoires sur la carte SD n'étant pas configurables, l'arborescence doit respecter le format suivant :

- /CONFIG
- /ALARM
- /LOG
- /BIN
- /CERT
- /DATA

- /CMD
- /DEF
- /SCRIPT

Si les répertoires n'existent pas, ils sont créés sur la carte SD à la prochaine demande de « connexion ».

Si le concentrateur est configuré pour utiliser la carte SD et que l'utilisateur effectue une connexion de test, l'appareil va rechercher les fichiers de configuration éventuellement présents sur la carte et les utiliser.

La carte Micro SD est vue et traitée comme un serveur FTP par le concentrateur.



Il est à noter que les fichiers de commande (CMD) présents sur la carte SD ne sont pas traités sur carte SD par le concentrateur.



Webdyn ne fournit aucune carte SD. Veuillez vous rapprocher d'un revendeur de matériel informatique.

4. Exploitation

Le concentrateur communique avec un ou plusieurs serveurs distants par le protocole FTP/SFTP/WebDAV-HTTPS et/ou par le protocole MQTT/MQTTS. Ces serveurs permettent de gérer le concentrateur à distance.

Un serveur distant à plusieurs rôles :

- Stocker 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 (cas d'un code action 8) ou le déclenchement du schedule de connexion, le concentrateur dépose ses données mémorisées.
- Paramétrer le concentrateur : à chaque connexion, le concentrateur synchronise sa configuration avec le fichier dédié présent sur le serveur. En l'absence de ce fichier, le concentrateur le crée à partir de sa configuration courante.
- Déclencher des actions sur concentrateur : les fichiers de commande doivent être déposés sur le serveur dans un répertoire associé au concentrateur.
- Superviser le concentrateur et aider au diagnostic : le concentrateur peut déposer des fichiers de log pour permettre le diagnostic.



Dans le cas où seul l'un des deux serveurs est un serveur FTP/SFTP/WebDAV-HTTPS, il appartient au client de faire le choix de définir celui-ci en tant que serveur 1 ou serveur 2 selon le comportement souhaité :

- Serveur 1 : il sera considéré comme un serveur principal.
- Serveur 2 : il sera considéré comme un serveur de sauvegarde (backup).

Le serveur principal permet de créer ou modifier la configuration et d'envoyer les commandes, ainsi que de recevoir les alarmes. Le serveur de sauvegarde (backup) sert uniquement comme copie des fichiers déposés sur le serveur principal. Aucune création ou modification de la configuration et aucune action ne peuvent être faites par celui-ci.

4.1 Le serveur FTP/SFTP/WebDAV

Pour la WebdynSunPM, le fonctionnement d'un serveur FTP, SFTP ou WebDAV-HTTPS est identique. Mais il est préférable d'utiliser un serveur SFTP ou WebDAV-HTTPS qui intègre des couches de sécurité contrairement à un FTP classique. La description dans ce chapitre vaut pour les divers types de serveurs.

Paramétrage :

Le serveur est défini par les paramètres suivants :

- Une adresse : Cette adresse peut être une adresse IP ou un nom de domaine.
- Un port de connexion (par défaut 21 en FTP, 22 en SFTP, 443 en WebDAV-HTTPS).
- Un identifiant et un mot de passe : Ces paramètres permettent de définir le compte à utiliser.
- Un répertoire racine : Le répertoire racine peut être la racine du serveur « / » ou une suite de sous-répertoires (par exemple : « /WebdynSunPM/00CF4/ »).

Vous pouvez configurer votre concentrateur à distance depuis votre serveur. Ceci n'est possible que si votre concentrateur WebdynSunPM est correctement configuré pour déposer et synchroniser sa configuration sur celui-ci.

Arborescence du serveur :

Le serveur doit disposer d'une arborescence spécifique au produit WebdynSunPM. Le concentrateur en propose une par défaut, mais il est possible de la personnaliser. Cette architecture doit être présente sur le serveur avant la première connexion, car le concentrateur ne crée pas les répertoires.

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

Nom	Droits	Description
/CONFIG	Lecture/ Écriture	Contient les fichiers de configuration. La configuration du concentrateur déposée par le concentrateur respecte le format suivant : <uid>_config.ini La configuration des interfaces de connexions déposées par le concentrateur respecte le format suivant : <uid>_daq.csv La configuration de la planification des connexions déposée par le concentrateur respecte le format suivant : <uid>_var.ini La configuration de la planification des connexions déposée par le concentrateur respecte le format suivant : <uid>_scl.ini
/DEF	Lecture/ Écriture	Contient les fichiers de définitions. Le fichier de définition respecte le format suivant : <uid>_<interface>_<commentaire>.csv
/SCRIPT	Lecture/ Écriture	Contient les fichiers de scripts. Le fichier de script respecte le format suivant : <commentaire>.lua
/CERT	Lecture/ Écriture	Contient les certificats. Le certificat respecte le format suivant : <commentaire>.pem
/DATA	Écriture	Contient les données collectées. Le nom du fichier de données respecte le format suivant : <uid>_<interface>_<timestamp>.csv.gz
/CMD	Lecture/ Ecriture/ Effacement	Contient les commandes. Le nom du fichier de commande respecte le format suivant : <uid>_cmd.csv
/ALARM	Écriture	Contient les alarmes. Le nom du fichier d'alarme respecte le format suivant : <uid>_AL_<timestamp>.csv.gz
/LOG	Écriture	Contient les fichiers de logs et de debug. Le fichier de log respecte le format suivant : <uid>_LOG_<timestamp>.log.gz Le fichier de debug respecte le format suivant : <uid>_SYSTEME_<timestamp>.tar.gz
/BIN	Lecture	Contient les fichiers de mise à jour. La mise à jour destinée au concentrateur respecte le format suivant : wgapp_<version>.spm

Avec :

- <uid> : Identifiant du concentrateur (du site)
- <timestamp> : Le format d'horodatage est «AAMMJJ_HHMMSS» de sorte qu'un tri alphabétique du répertoire donne l'ordre chronologique
- <interface> : nom de l'interface parmi une liste définie (voir chapitre 3.1.2.1.3.4: « Déclaration des équipements à superviser »)
- <commentaire> : champ libre pour l'utilisateur
- <version> : numéro de la version de la mise à jour.

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

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



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



Tous les fichiers échangés entre le concentrateur et le serveur doivent être encodés au format standard UTF-8.

Fonctionnement :

En FTP ou SFTP, si le paramètre « FTP_TwoStepsSendingDisabled » ou « FTP2_TwoStepsSendingDisabled » est à « 1 », alors le concentrateur dépose les fichiers sur le serveur 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.

Pour un serveur WebDAV-HTTPS, ce mécanisme est inutile.

Format des fichiers :

Le concentrateur gère différents formats de fichier en fonction du type de fichier. On peut les regrouper par rapport à leurs extensions, ceux qui donnent :

Extension	Type de fichiers	Description
.ini	<ul style="list-style-type: none">• Fichier de configuration du concentrateur• Fichier de la planification des connexions• Fichier de donnée (compressé)	Fichier de configuration dans un format de données
.csv	<ul style="list-style-type: none">• Fichier des interfaces de connexion• Fichiers de définitions des équipements• Fichier d'alarme	Fichier avec des données tabulaires sous forme de valeurs séparées par des points virgules. (peut être exploité facilement avec un tableur comme Excel)
.json	<ul style="list-style-type: none">• Fichier de commande	Fichier texte contenant du JSON
.lua	<ul style="list-style-type: none">• Fichier script	Script en langage Lua
.pem	<ul style="list-style-type: none">• Fichier certificat	Certificat au format PEM permettant de se connecter à un serveur sécurisé.
.log	<ul style="list-style-type: none">• Fichier log (compressé)	Fichier texte
.spm	<ul style="list-style-type: none">• Fichier de mise à jour	Package comprenant tous les fichiers de mise à jour

4.11 La configuration « CONFIG »

Le concentrateur peut recevoir des configurations distantes par des fichiers de configuration ou par des commandes SMS.

Fichier de configuration :

Le concentrateur WebdynSunPM a besoin de 4 types de fichiers de configuration qui sont aux formats texte et CSV. Le nom de fichiers sont les suivants :

<uid>_config.ini

<uid>_daq.csv

<uid>_var.ini

<uid>_scl.ini

Avec <uid> l'identifiant du concentrateur.

La configuration courante est disponible sur le serveur distant dans le répertoire « CONFIG ». Que ce soit après une modification locale ou distante de la configuration, le concentrateur envoie sur le serveur distant sa nouvelle configuration dès la prochaine connexion à celui-ci.

L'envoi des fichiers de configuration peut être réalisé à distance via le répertoire « CONFIG ». Il faut déposer ou modifier les fichiers de configuration dans ce répertoire. Lors de la prochaine connexion au serveur, le concentrateur réalise 2 étapes :

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



Nom de fichier	Taille de F...	Type de fichier	Dernière modification	Droits d'accès
WM800C4F_daq.csv	317	Fichier CSV	21/01/2021 17:40:00	-rwxrwxrwx
WM800C4F_var.ini	93	Paramètres de co...	12/01/2021 12:09:00	-rwxrwxrwx
WM800C4F_scl.ini	187	Paramètres de co...	12/01/2021 12:09:00	-rwxrwxrwx
WM800C4F_config.ini	1.241	Paramètres de co...	12/01/2021 12:09:00	-rwxrwxrwx

Il est nécessaire de respecter les noms des fichiers de configuration comme indiqué ci-dessus.

Après application de la nouvelle configuration, le résultat est indiqué dans le fichier de LOG du concentrateur.

En cas d'erreur dans le fichier de configuration comme une valeur incorrecte, le concentrateur ne la prendra pas en compte et utilisera sa valeur par défaut si elle existe sinon le fichier sera rejeté. Le fichier de LOG remontera l'erreur et la valeur appliquée par défaut.



Veillez vous référer au chapitre « Fonctionnement du concentrateur » ou à l'«Annexe A : Fichier de configuration « _config.ini » » pour connaître la liste des variables et leurs valeurs possibles.

4.1.2 Les définitions « DEF »

Les équipements déclarés dans le fichier « <uid>_daq.csv » utilisent un fichier de définition décrivant l'ensemble des variables disponibles sur l'équipement. Les équipements disponibles sur le concentrateur sont :

- Les entrées/sorties : IO
- La téléinformation client : TIC
- Modbus RTU/TCP

- Protocole onduleurs propriétaires

Les fichiers de définition que la WebdynSunPM peut générer automatiquement sont :

- Le fichier IO
- Les fichiers SunSpec
- Les fichiers des protocoles onduleurs propriétaires.

Pour créer des fichiers de définitions Modbus, voir le chapitre 3.1.2.2.2.2 « Modbus ».

Le lancement d'une découverte d'un équipement permet de générer automatique le fichier de définition de celui-ci et de le déposer dans le répertoire « DEF » du serveur. Il est également possible de construire son propre fichier ou de modifier le fichier généré automatiquement.

Un nouveau fichier de définition ou une modification sur l'un des fichiers de définition sera automatiquement récupéré par le concentrateur lors de la prochaine connexion au serveur.

Le nom du fichier de définition peut être personnalisé, par défaut il respecte le format suivant:

`<uid>_<interface>_<comment>.csv`

Avec :

- `<uid>` : Identifiant du concentrateur
- `<interface>` : nom de l'interface parmi une liste définie (voir chapitre 3.1.2.1.3.4 « Déclaration des équipements à superviser »)
- `<commentaire>` : champ libre pour l'utilisateur

Exemples :

`WPM00C44F_SunSpec_inverter_SMA_Solar_Inverter_9301_ModbusTCP.csv`

`WPM00C44F_IO.csv`

`custom.csv`



Veuillez vous référer au chapitre « Définition des équipements connectés » pour connaître la structure des fichiers de définition.

4.13 Les données « DATA »

Les données sont remontées dans le répertoire « DATA » du serveur FTP, sous la forme de fichiers au format CSV, et compressés au format Gzip « .gz ».

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

<uid>_<interface>_<timestamp>.csv.gz

Avec :

- <uid> : Identifiant du concentrateur
- <interface> : nom de l'interface parmi la liste suivante :
 - TIC
 - IO
 - Modbus
- <timestamp> : Le format d'horodatage est «AAMMJJ_HHMMSS» de sorte qu'un tri alphabétique du répertoire donne l'ordre chronologique.

Exemples :

WPM00C44F_Modbus_210112_105947.csv.gz

WPM00C44F_IO_210202_084443.csv.gz

WPM00C44F_TIC_210202_095243.csv.gz

Chaque équipement déclaré et configuré acquiert ses données sur une période définie (voir chapitre 3.2.1 : « Equipements (Devices) ») et les dépose régulièrement sur un serveur (voir chapitre « Serveurs (servers) ») dans le répertoire « DATA ».

Les données resteront mémorisées par le concentrateur tant qu'elles n'ont pas été déposées sur le serveur. Ceci dans le but d'être renvoyées en cas d'échec de transfert.



Quand la mémoire du concentrateur est saturée, les nouvelles données ne seront plus mémorisées tant que celle-ci ne sera pas vidée par un dépôt des fichiers sur un serveur. Le concentrateur mémorise au maximum 50Mo de données non compressés par équipement défini.

La WebdynSunPM collecte en permanence les données des équipements et interfaces puis les sauvegarde. Les valeurs remontées sont toujours brutes et doivent être liées au fichier de définitions de l'équipement. Le contenu d'un fichier de donnée est composé de 2 parties qui sont :

- Un en-tête (header) : qui est différent selon l'équipement ou l'interface.
- Des données : qui ont un formatage identique entre tous les équipements et interfaces.

4.1.3.1 En-tête Entrées/Sortie (IO)

L'en-tête (header) du fichier de données IO est le suivant :

```
TypeIO;fileDefinitionName
```

Code couleur :

- En noir : texte fixe.
- En bleu : informations ou données qui dépendent de l'équipement.

Avec :

- `fileDefinitionName` : nom du fichier de définition associé aux Entrées/Sorties.

4.1.3.2 En-tête Equipements (Modbus, onduleurs)

L'en-tête (header) du fichier de données des équipements est le suivant :

```
DEVICEINDEX;NumDevice_1  
Protocol_1;fileDefinitionName_1  
...  
...  
DEVICEINDEX;NumDevice_N  
Protocol_N;fileDefinitionName_N
```

Code couleur :

- En noir : texte fixe.
- En bleu : informations ou données qui dépendent de l'équipement.

Avec :

- `NumDevice_N` : index de l'équipement « index » dans le fichier de configuration des interfaces de connexions de l'équipement N (voir chapitre « Contenu du fichier de définition »).
- `fileDefinitionName_N` : nom du fichier de définition associé à l'équipement N.

4.1.3.3 Données

Le formatage des données est identique, peu importe l'équipement ou l'interface.

Les valeurs remontées sont brutes et doivent être liées au paramétrage effectué sur l'équipement ou l'interface dans son fichier de définition. Le SI doit interpréter les données en se servant du fichier de données brutes et du fichier de définition afin de pouvoir appliquer les coefficients A et B ainsi que l'unité pour chaque variable. (voir chapitre 3.1.2.2.2 : « Contenu du fichier de définition »)

Le champ « action » associé à chaque variable dans le fichier de définition permet de sélectionner un type de valeur :

"ACTION" CODE	DESCRIPTION
0	Aucune valeur n'est remontée.
1	La valeur du paramètre est remontée.
2	Les valeurs min, max et moyenne sont remontés.
4 ou 6	La valeur instantanée est remontée.
7	Les valeurs min, max et moyenne sont remontées dans le fichier d'acquisition ; la valeur instantanée est remontée dans le fichier créé par la commande getData.
8 ou 9	La valeur instantanée est remontée et une alarme sera générée à chaque changement de valeur.

Les données du fichier de données de l'équipement ou de l'interface sont le suivant :

```
nbVariableDevice_N;indexVariable_1_Device_N;indexVariable_A_Device_N;val_of_EnAdvData(=1)

datetime_1;variable_1_value_1_Device_N;variable_x_value_1_Device_N;nb_refreshes_during_1

datetime_2;variable_1_value_2_Device_N;variable_x_value_2_Device_N;nb_refreshes_during_2

...

datetime_Y;variable_1_value_B_Device_N;variable_A_value_B_Device_N;nb_refreshes_during_B
```

Code couleur :

- En vert : en-tête (header) optionnel, activable ou désactivable par le paramètre « FTP_HeaderOption » pour le serveur 1 et « FTP2_HeaderOption » pour le serveur 2 dans le fichier de configuration <uid>_config.ini).
- En bleu : informations ou données qui dépendent de l'équipement.

Avec :

- nbVariableDevice_N : nombre total de variables collectées de l'équipement N.
- indexVariable_X_Device_N : index X de la variable collectée de l'équipement N.
- datetime_Y : horodatage des données au point d'acquisition Y. Pour le format, voir les variables FTP_EuroDateFormat, FTP2_EuroDateFormat, HTTP_EuroDateFormat et HTTP2_EuroDateFormat dans le chapitre 3.2.2.5 : « Serveurs (servers) ».
- variable_A_value_B_Device_N : valeur A de la Variable B correspondant à l'Index A collectée au point d'acquisition Y et à l'action définie dans le fichier de définition de l'équipement N.
- nb_refreshes_during_B : nombre de lectures complètes sur cette période d'acquisition de la variable B. Cette information est affichée uniquement si le paramètre « FTP_EnableAdvancedData » ou « HTTP_EnableAdvancedData » du serveur 1 ou « FTP2_EnableAdvancedData » ou « HTTP2_EnableAdvancedData » du serveur 2 est à 1. Cette donnée peut être utile uniquement pour les équipements Modbus et Onduleurs. Pour les IO, TIC, périphériques virtuels et pour le fichier de collecte de paramètres, le nombre de rafraîchissements est toujours à 0.



Afin d'éviter l'envoi de donnée inutile sur le serveur et permettant ainsi d'optimiser la connexion, il est conseillé d'activer uniquement les variables que l'on souhaite remonter.

Entrées/Sortie (IO) :

Exemple d'un fichier de donnée IO avec une période d'acquisition toutes les 10 secondes :

- Paramétrage des entrées/sortie :

Entrées/Sortie	Code « Action »	Affichage
1	4	Valeur instantanée
2	0	Aucun
3	4	Valeur instantanée
4	4	Valeur instantanée
5	4	Valeur instantanée

6	2	Valeurs min, max et moyenne
7	8	Valeur instantanée
8	4	Valeur instantanée

- Fichier de données CSV (édité sous Excel) :

TypeID	WPM00C44F_IO.csv									
9	1	3	4	5	6 (min)	6 (max)	6 (avg)	7	8	9
21/02/02-15:41:10	0	0	5	1	130	170	150	5	0	0
21/02/02-15:41:20	0	1	2	2	130	170	120	3	0	0
21/02/02-15:41:30	1	0	3	1	120	160	140	2	0	0
21/02/02-15:41:40	1	0	6	5	120	170	140	3	1	0
21/02/02-15:41:50	0	0	6	4	130	180	150	5	0	0
21/02/02-15:42:00	0	0	6	5	130	200	160	6	0	0

Equipements (Modbus, onduleurs) :

Exemple d'un fichier de donnée équipement avec une période d'acquisition toutes les 10 minutes :

- Paramétrage des index du device 1 :

Index	Code « Action »	Affichage
1	1	Valeur du paramètre
2	0	Aucun
3-11	4	Valeur instantanée
12	8	Valeur instantanée

- Paramétrage des index du device 2 :

Index	Code « Action »	Affichage
1-2	2	Valeurs min, max et moyenne

- Fichier de données CSV (édité sous Excel) :

DEVICEINDEX	1											
ModbusTCP	WPM00C44F_SunSpec_inverter_SMA_Solar_Inverter_9301_ModbusTCP.csv											
11	1	3	4	5	6	7	8	9	10	11	12	1
21/02/05-09:50:00	32	52	5	102	1	0	1	0	0	0	0	5
21/02/05-10:00:00	35	57	5	108	1	10	0	0	0	0	1	6
DEVICEINDEX	2											
SMANET	WPM00C44F_SMA_Inverter_SMA_WR21TL09.csv											
7	1 (min)	1 (max)	1 (avg)	2 (min)	2 (max)	2 (avg)	1					
21/02/05-09:50:00	16	32	26.00	52	58	51.00	12					
21/02/05-10:00:00	4	6	05:50	102	105	103.00	12					

4.1.4 Les alarmes « ALARM »

Les alarmes sont remontées sous la forme de fichiers au format CSV, et compressées au format Gzip «.gz ». Elles sont déposées dans le répertoire « ALARM » des serveurs distants. Aucun autre fichier à part les fichiers d’alarmes n’est déposé sur les serveurs et le concentrateur ne déclenchera pas de synchronisation NTP. La liste des alarmes pouvant être générées est :

Source Alarme	Info	Description
GATEWAY	Power ON	Démarrage du concentrateur
	Power OFF	Extinction du concentrateur
	Perte accessoire TIC	Accessoire TIC retiré
	Retour accessoire TIC	Accessoire TIC reconnecté
IO	Nom du Fichier de définition + Index + Valeur	Valeur d’une entrée de type alarme a changé
Modbus	Nom du Fichier de définition + Index + Valeur	Valeur d’un index de type alarme à changer

Une alarme « Power OFF » est envoyée après une coupure de secteur d’au moins 10 secondes et une alarme « Power ON » est envoyée après le retour de l’alimentation pendant au moins 1 minute. Les autres alarmes ne sont pas temporisées et sont envoyées dès la détection par le concentrateur.

Le fichier d'alarme sur le serveur respecte le format suivant :

`<uid>_AL_<timestamp>.csv.gz`

Avec :

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

Le format du fichier d'alarmes de type GATEWAY est le suivant :

```
datetime_1;GATEWAY;info_1
datetime_2;GATEWAY;info_2
...
datetime_Y;GATEWAY;info_X
```

Code couleur :

- En noir : texte fixe.
- En bleu : informations ou données qui dépendent de l'équipement.

Avec :

- `datetime_Y` : horodatage de l'alarme au point de déclenchement Y. Pour le format, voir les variables `FTP_EuroDateFormat`, `FTP2_EuroDateFormat`, `HTTP_EuroDateFormat` et `HTTP2_EuroDateFormat` dans le chapitre 3.2.2.5 « Serveurs (servers) »
- `info_X` : information sur l'alarme X.

Le format du fichier d'alarmes de type IO et Modbus est le suivant :

```
datetime_1;AlarmSource_1;fileDefinitionName_1;nameEquipment_1;
indexVariable_1;value_1
datetime_2;AlarmSource_2;fileDefinitionName_2;nameEquipment_2
indexVariable_2;
value_2
...
datetime_Y;AlarmSource_X;fileDefinitionName_N;nameEquipment_N;
indexVariable_A;variable_A_value_B
```

Code couleur :

- En bleu : informations ou données qui dépendent de l'équipement.

Avec :

- **datetime_Y** : horodatage de l'alarme au point de déclenchement Y. Pour le format, voir les variables FTP_EuroDateFormat, FTP2_EuroDateFormat, HTTP_EuroDateFormat et HTTP2_EuroDateFormat dans le chapitre 3.2.2.5 « Serveurs (servers) ».
- **AlarmSource** : source qui a déclenché l'alarme (IO, Modbus).
- **fileDefinitionName_N** : nom du fichier de définition associé à l'équipement.
- **nameEquipment_N** : nom de l'équipement. Champ « name » dans le fichier « <uid>_daq.csv » (voir chapitre 3.1.2.1.3.4 « Déclaration des équipements »).
- **indexVariable_A** : index A de la variable en alarme.
- **variable_A_value_B** : valeur B de la Variable A correspondant à l'Index A en alarme.

Les valeurs remontées des alarmes IO et Modbus sont brutes et doivent être liées au paramétrage effectué sur les index dans le fichier de définition de l'équipement. Le SI doit interpréter les données en se servant du fichier de données brutes et du fichier de définition afin de pouvoir appliquer les coefficients A et B définis ainsi que l'unité définie pour chaque entrée ou index. (voir chapitre « Contenu du fichier de définition »)

Exemple d'un fichier d'alarme Modbus :

21/02/12-07:00:19	Modbus	Modbus_DELTA_M88H-COM1.20-Sunspec.csv	OndA	48	0.000000
21/02/12-07:00:49	Modbus	Modbus_DELTA_M88H-COM1.20-Sunspec.csv	OndA	48	3.000000

4.15 Les commandes « CMD »

Les fichiers de commande permettent d'exécuter des tâches à distance sur le concentrateur. Il est ainsi possible ainsi de demander au concentrateur de lancer une recherche d'équipements, d'obtenir la configuration, et ainsi de suite. La liste des possibilités est illimitée.

Les fichiers de commande ne sont pas gérés lorsque la carte SD est utilisée.

Le fonctionnement du fichier de commande (format et traitement) est décrit au chapitre 5 : « Commandes ». Les commandes disponibles sont détaillées au chapitre 5.3 : « Liste des Commandes ».

4.16 Les scripts « SCRIPT »

Le répertoire « SCRIPT » du serveur permet de fournir ou de récupérer les scripts Lua du concentrateur.

Les fichiers scripts Lua peuvent avoir l'extension suivante :

- « .lua » : un script LUA non chiffré
- « .luax » : un script LUA chiffré avec des clés clients
- « .luaw » : un script LUA chiffré avec une licence Webdyn

Ci-dessous le format du nom du fichier script :

<comment>_lua
<commentaire>_luax
<scriptwebdyn>_luaw

Avec :

- <commentaire> : champ libre pour l'utilisateur
- <scriptwebdyn> : script propriétaire Webdyn

Exemples :

ControlPower.lua
Injection.luax
Deie.luaw

Pour plus de détails sur l'utilisation des scripts, voir le document « WebdynSunPM LUA User Guide.pdf » disponible sur le site : <https://www.webdyn.com/support/WebdynSunPM/>



Les scripts propriétaires Webdyn « .luaw » ne sont pas redéposés par le concentrateur en cas de suppression sur le serveur distant.

4.17 La mise à jour « BIN »

Le répertoire « BIN » du serveur permet de stocker le firmware pour la mise à jour du concentrateur.

Ci-dessous le format du nom du fichier de mise à jour :

<uid>_wgapp_x.x.x.xxxxx.spm

Avec :

- <uid>: Concentrator identifier.
- x.x.x.xxxxx: is the firmware version number.

Exemples : wgapp_3.2.9.34734.spm

Pour effectuer la mise à jour, suivre la procédure décrite au chapitre 6.2 : « Par FTP/SFTP/WebDAV »). Après l'application de la mise à jour, il est possible de supprimer le fichier firmware.

4.1.8 Les Logs « LOG »

Les fichiers de logs sont les fichiers qui permettent de surveiller les actions du concentrateur et analyser si les choses ne se passent pas comme elles devraient.

En cas de contact avec le support, il est indispensable de pouvoir fournir les fichiers de log correspondants au problème rencontré.

Il existe 4 types de fichiers de log :

- Les logs de connexion : « uid »_LOG_« date ».log.gz.
- Les logs d'exécution de scripts LUA : « uid »_LUA_« nom du script »_« date ».log.gz.
- Les logs de détection SunSpec : « uid »_SUNSPEC_« date ».log.gz.
- Les logs système : « uid »_SYSTEM_« date ».log.gz.

4.1.8.1. Les logs de connexion

À chaque fois que le concentrateur se connecte à un serveur, par modem ou par Ethernet, toutes les opérations sont enregistrées afin d'être consultées ultérieurement.

Lorsque la connexion est forcée par l'interface web locale, une fenêtre apparaît indiquant toutes les opérations en cours d'exécution comme suit :



```
Request Tracking
2021-02-01 14:28:17 No change
2021-02-01 14:28:17 Checking WPM000004_SunSpec_inverter_0001_Solar_Inverter_0001_middlewareTCP
2021-02-01 14:28:17 Getting remote strings
2021-02-01 14:28:21 Failed to parse http open parameter () for device 192.168.101.20-002: show: 130, use default value true
2021-02-01 14:28:21 Local changes saved WPM000004_spm.lua
2021-02-01 14:28:21 Script management
2021-02-01 14:28:21 Checking WPM000004_spm.lua
2021-02-01 14:28:21 Getting remote strings
2021-02-01 14:28:21 Checking local script.lua
2021-02-01 14:28:21 No change
2021-02-01 14:28:21 No change
2021-02-01 14:28:21 Checking local script.lua
2021-02-01 14:28:21 No change
2021-02-01 14:28:21 Configuration file summary
2021-02-01 14:28:21 WPM000004_SunSpec_inverter_0001_Solar_Inverter_0001_middlewareTCP: Authorize remote file Result:Success
2021-02-01 14:28:21 WPM000004_SunSpec_Authorize local file Result:Success
2021-02-01 14:28:21 WPM000004_spm.lua: Authorize remote file Result:Success
2021-02-01 14:28:21 Sending WPM000004_SUNSPEC_0001_0001.spm
2021-02-01 14:28:21 Sending WPM000004_LOG_210201_142821.log.gz
2021-02-01 14:28:21 Connection terminated with success
```

Pour cette même connexion, le fichier de log déposé sur le serveur contient les données suivantes :

```
2021-02-11 14:25:03:Firmware version : WebdynSunPM 3.2.11.34874
2021-02-11 14:25:03:Connection 1 wait for exclusive...
2021-02-11 14:25:03:Connection requested
2021-02-11 14:25:16:Ntp synchronisation success
2021-02-11 14:25:16:Connection to 192.168.2.13:test server in
progress ...
2021-02-11 14:25:16:Alarms management...
2021-02-11 14:25:16>Data acquisition management...
2021-02-11 14:25:16:Sending WPM00BDE4_Modbus_210211_142503.csv.gz
2021-02-11 14:25:16>Data acquisition management...
2021-02-11 14:25:16:Sending WPM00BDE4_IO_210211_142507.csv.gz
2021-02-11 14:25:16:Sending WPM00BDE4_SUNSPEC_210211_142507.log.gz
2021-02-11 14:25:16:Configuration management...
2021-02-11 14:25:16:Checking WPM00BDE4_config.ini
2021-02-11 14:25:16:No change
2021-02-11 14:25:16:Checking WPM00BDE4_daq.csv
2021-02-11 14:25:16:Sending local changes
2021-02-11 14:25:16:Remove file
2021-02-11 14:25:17:Checking WPM00BDE4_var.ini
2021-02-11 14:25:17:No change
2021-02-11 14:25:17:Checking WPM00BDE4_IO.csv
2021-02-11 14:25:17:No change
2021-02-11 14:25:17:Checking WPM00BDE4_SunSpec_inverter_SMA_Solar_
Inverter_9301_ModbusTCP.csv
2021-02-11 14:25:17:Getting remote changes
2021-02-11 14:25:21:Failed to parse keep open parameter () for device
192.93.121.23:502, slave: 126, use default value true
2021-02-11 14:25:21:Local changes sent WPM00BDE4_daq.csv
2021-02-11 14:25:21:Script management...
2021-02-11 14:25:21:Checking WPM00BDE4_scl.ini
2021-02-11 14:25:21:Getting remote changes
2021-02-11 14:25:21:Checking Test script 1.lua
2021-02-11 14:25:21:No change
2021-02-11 14:25:21:Checking Test script 2.lua
2021-02-11 14:25:21:No change
2021-02-11 14:25:21:Configuration file summary:
2021-02-11 14:25:21:WPM00BDE4_SunSpec_inverter_SMA_Solar_
Inverter_9301_ModbusTCP.csv: Action=Get remote file. Result=Success
2021-02-11 14:25:21:WPM00BDE4_daq.csv: Action=Send local file.
Result=Success
2021-02-11 14:25:21:WPM00BDE4_scl.ini: Action=Get remote file.
Result=Success
2021-02-11 14:25:24:Sending WPM00BDE4_SYSTEM_210211_142521.tar.gz
```

En tout premier lieu on retrouve les informations sur la version logicielle du concentrateur, puis la connexion au serveur NTP pour la synchronisation de l'heure.

Vient ensuite la connexion proprement dite au serveur en commençant par la synchronisation des alarmes s'il y a lieu :

```
2021-02-11 14:25:16:Alarms management...
```

Une fois cette étape terminée, les fichiers de données sont transférés sur le serveur :

```
2021-02-11 14:25:16:Data acquisition management...
2021-02-11 14:25:16:Sending WPM00BDE4_Modbus_210211_142503.csv.gz
2021-02-11 14:25:16:Data acquisition management...
2021-02-11 14:25:16:Sending WPM00BDE4_IO_210211_142507.csv.gz
2021-02-11 14:25:16:Sending WPM00BDE4_SUNSPEC_210211_142507.log.gz
```

Vient ensuite le traitement des fichiers de configuration à envoyer ou recevoir :

```
2021-02-11 14:25:16:Configuration management...
2021-02-11 14:25:16:Checking WPM00BDE4_config.ini
2021-02-11 14:25:16:No change
2021-02-11 14:25:16:Checking WPM00BDE4_daq.csv
2021-02-11 14:25:16:Sending local changes
2021-02-11 14:25:16:Remove file
2021-02-11 14:25:17:Checking WPM00BDE4_var.ini
2021-02-11 14:25:17:No change
2021-02-11 14:25:17:Checking WPM00BDE4_IO.csv
2021-02-11 14:25:17:No change
2021-02-11 14:25:17:Checking WPM00BDE4_SunSpec_inverter_SMA_Solar_
Inverter_9301_ModbusTCP.csv
2021-02-11 14:25:17:Getting remote changes
2021-02-11 14:25:21:Failed to parse keep open parameter () for device
192.93.121.23:502, slave: 126, use default value true
2021-02-11 14:25:21:Local changes sent WPM00BDE4_daq.csv
```

Le fichier de log indique qu'un certain nombre de fichiers ont été vérifiés et qu'aucune modification n'a été détectée.

Il est ensuite indiqué que le fichier « WPM00BDE4_SunSpec_inverter_SMA_Solar_Inverter_9301_ModbusTCP.csv » a été modifié sur le serveur distant. Il est alors rapatrié, lu et importé localement :

```
2021-02-11 14:25:17:Checking WPM00BDE4_SunSpec_inverter_SMA_Solar_
Inverter_9301_ModbusTCP.csv
2021-02-11 14:25:17:Getting remote changes
```

Des modifications ont également été détectées dans les équipements et le fichier « _daq » est envoyé vers le serveur :

```
2021-02-11 14:25:21:Local changes sent WPM00BDE4_daq.csv
```

Le traitement se termine avec la gestion des fichiers de script :

```
2021-02-11 14:25:21:Script management...
2021-02-11 14:25:21:Checking WPM00BDE4_scl.ini
2021-02-11 14:25:21:Getting remote changes
2021-02-11 14:25:21:Checking Test script 1.lua
2021-02-11 14:25:21:No change
2021-02-11 14:25:21:Checking Test script 2.lua
2021-02-11 14:25:21:No change
```

Tous les scripts sont vérifiés sur le serveur. Ici, il n'y a pas eu de changement comme indiqué dans le log.

Une fois tous les traitements terminés, un récapitulatif donne un résumé de toutes les opérations qui ont eu lieu :

```
2021-02-11 14:25:21:Configuration file summary:
2021-02-11 14:25:21:WPM00BDE4_SunSpec_inverter_SMA_Solar_
Inverter_9301_ModbusTCP.csv: Action=Get remote file. Result=Success
2021-02-11 14:25:21:WPM00BDE4_daq.csv: Action=Send local file.
Result=Success
2021-02-11 14:25:21:WPM00BDE4_scl.ini: Action=Get remote file.
Result=Success
```

On y lit donc que les fichiers : WPM00BDE4_SunSpec_inverter_SMA_Solar_Inverter_9301_ModbusTCP.csv » et « WPM00BDE4_scl.ini » ont été rapatriés avec succès du serveur.

On y lit également que le fichier « WPM00BDE4_daq.csv » a été envoyé vers le serveur.

Le fichier de log se termine avec l'indication de l'envoi des logs système :

```
2021-02-11 14:25:24:Sending WPM00BDE4_SYSTEM_210211_142521.tar.gz
```


4.1.8.3 Les logs de détection SunSpec

Lors d'une détection SunSpec, le résultat de la détection est affiché au fur et à mesure sur la web locale :



Ce log peut également se retrouver à la prochaine connexion au serveur dans le répertoire « LOGS ». Le nom du fichier est composé de l'uid du concentrateur, suivi de « SUNSPEC » et de la date et heure du dépôt du fichier sur le serveur : « WPM00BDE4_SUNSPEC_210211_181543.log.gz »

Le fichier de log contient exactement la même chose que ce qui a été affiché à l'écran :

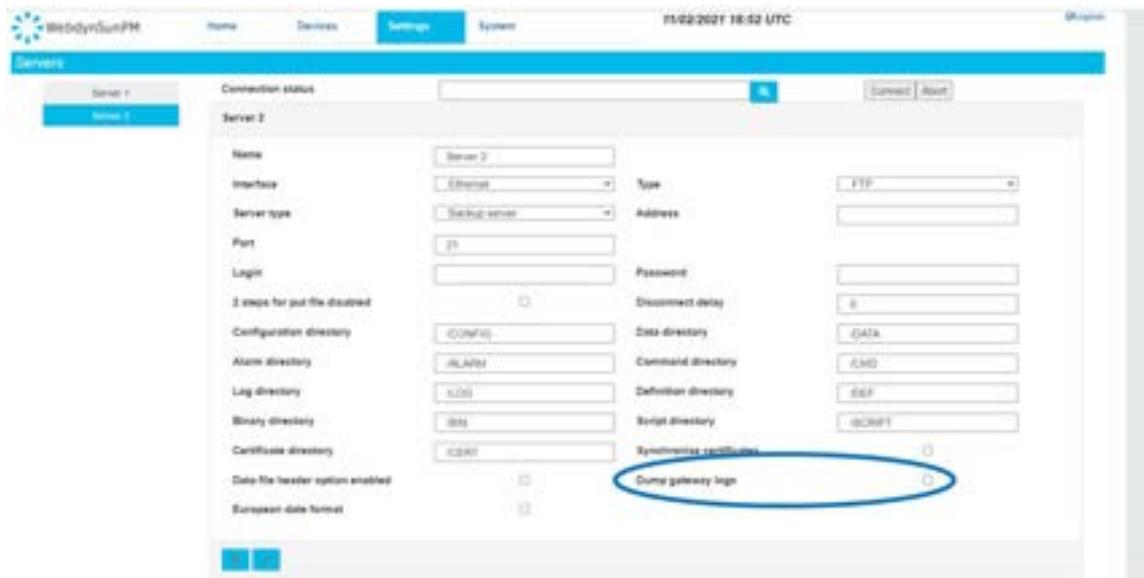
```
21/02/11-17:27:28;SunSpec detection start on ethernet1. Estimated
time : 621 seconds.
21/02/11-17:27:30;NON SUNSPEC device found at @1 192.93.121.23:502.
21/02/11-17:27:31;NON SUNSPEC device found at @2 192.93.121.23:502.
21/02/11-17:27:32;NON SUNSPEC device found at @3 192.93.121.23:502.
21/02/11-17:27:47;SunSpec device found at @126 192.93.121.23:502.
21/02/11-17:27:48;Found table 1:66 at 40004@126 192.93.121.23:502
21/02/11-17:27:49;Found table 11:13 at 40072@126 192.93.121.23:502
21/02/11-17:27:50;Found table 12:98 at 40087@126 192.93.121.23:502
21/02/11-17:27:51;Found table 101:50 at 40187@126 192.93.121.23:502
21/02/11-17:27:52;Found table 120:26 at 40239@126 192.93.121.23:502
21/02/11-17:27:53;Found table 121:30 at 40267@126 192.93.121.23:502
21/02/11-17:27:54;Found table 122:44 at 40299@126 192.93.121.23:502
21/02/11-17:27:55;Found table 123:24 at 40345@126 192.93.121.23:502
21/02/11-17:27:56;Found table 124:24 at 40371@126 192.93.121.23:502
21/02/11-17:27:57;Found table 126:64 at 40397@126 192.93.121.23:502
21/02/11-17:27:58;Found table 127:10 at 40463@126 192.93.121.23:502
21/02/11-17:27:59;Found table 128:14 at 40475@126 192.93.121.23:502
21/02/11-17:28:00;Found table 131:64 at 40491@126 192.93.121.23:502
21/02/11-17:28:01;Found table 132:64 at 40557@126 192.93.121.23:502
21/02/11-17:28:02;Found table 160:128 at 40623@126 192.93.121.23:502
21/02/11-17:28:03;Table 160. Type count not supported.
21/02/11-17:28:04;Found table 129:60 at 40753@126 192.93.121.23:502
21/02/11-17:28:05;Found table 130:60 at 40815@126 192.93.121.23:502
21/02/11-17:28:07;End of SunSpec detection on ethernet1. 1 devices
found.
```

Il est à noter que les fichiers de log de la détection SunSpec sont au format « CSV » afin d'être importés facilement dans un tableur.

4.1.8.4 Les logs système

Les logs système sont les logs de fonctionnement interne du concentrateur. Ils contiennent des informations de débogage internes qui peuvent être réclamées par le support.

Par défaut les logs système ne sont pas transférés vers le serveur. Pour qu'ils le soient il faut activer l'option « Dump gateway logs » dans la page de configuration des serveurs :



Les fichiers de log système sont également transférés automatiquement lorsqu'une connexion est forcée via la page de configuration des serveurs, en cliquant sur le bouton « Connect » ou via la commande SMS « connect ».

Le nom du fichier est composé de l'uid du concentrateur, suivi de « SYSTEM » et de la date et heure du dépôt du fichier sur le serveur : « WPM00BDE4_SYSTEM_210211_181543.log.gz ».

4.19 Web Services

Il existe 2 paramètres pour configurer les web services :

- **WebServiceEnable** : 0 pour désactiver et 1 pour activer les web services.
- **WebServiceUrl** : lorsque les web services sont activés, ce paramètre contient l'adresse réseau qui sera appelée sous certaines conditions décrites dans cette section.

Les actions suivantes peuvent déclencher l'appel à un web service :

- Démarrage du produit
- Dépôt de fichiers de données sur le serveur FTP

- Modification de la configuration (chargement ou dépôt de configuration)
- Exécution d'un fichier de commandes
- Chargement d'un nouveau fichier binaire

Les appels aux web services se font selon le format suivant :

```
URL/confirm.php;NSITE=IDsite&ACTION=action&ACTION-COMP=données complémentaires&RC=0&RC-COMP=
```

La page « confirm.php » est appelée à l'URL configurée. Cette page recevra les différentes informations des actions et devra les traiter.

Les informations sont :

- *NSITE* : identifiant du concentrateur. C'est l'identifiant qui a été configuré lors de la mise en service
- *Action* : identifiant de l'action qui a déclenché l'appel au web service. La liste des actions est décrite plus bas
- *ACTION-COMP* : pour certaines actions, des informations complémentaires sont précisées. La liste complète est décrite plus bas
- *RC* : vaut toujours 0
- *RC-COMP* : toujours vide

Action	Données web service
<p>Première connexion FTP depuis le démarrage du concentrateur.</p> <p>Lorsque la passerelle se connecte la première fois depuis son démarrage (mise sous tension, mise à jour logicielle, ...), le numéro de version logicielle est envoyé.</p>	<p>NSITE=IDsite&ACTION=VERSION&ACTION-COMP=version firmware&RC=0&RC-COMP=</p>
<p>Envoi de données des onduleurs ou des IO vers le serveur FTP.</p> <p>Lorsque la passerelle se connecte au serveur FTP pour déposer les fichiers de données des différents équipements, ce web service est appelé.</p>	<p>NSITE=IDsite&ACTION=UPLOADDATA&RC=0&RC-COMP=</p>

<p>Envoi d'alarmes vers le serveur FTP.</p> <p>Lorsqu'une alarme a été détectée, un fichier d'alarmes est déposé sur le serveur FTP et ce web service est appelé.</p>	<p>NSITE=IDsite&ACTION=UPLOADALARM&RC=0&RC-COMP=</p>
<p>Envoi des fichiers de configuration de la passerelle vers le serveur FTP.</p> <p>Lorsqu'une modification de configuration est apportée localement sur la passerelle, à la prochaine connexion, les fichiers de configuration impactés sont transférés vers le serveur FTP et ce service web est appelé</p>	<p>NSITE=IDsite&ACTION=UPLOADGLOBAL&ACTION-COMP=liste de fichiers de configuration&RC=0&RC-COMP=</p> <p>Les noms des fichiers de configuration sont séparés par le caractère « ; ».</p> <p>Les fichiers concernés sont « _config.ini », « _var.ini » et « _daq.ini »</p>
<p>Chargement de fichiers de configuration du serveur FTP vers la passerelle.</p> <p>Lorsque des modifications des fichiers de configuration distants sont effectuées, la passerelle charge ces fichiers à la prochaine connexion et ce service web est appelé.</p>	<p>NSITE=IDsite&ACTION=CONFIGGLOBAL&ACTION-COMP=liste de fichiers de configuration&RC=0&RC-COMP=</p> <p>Les noms des fichiers de configuration sont séparés par le caractère « ; ».</p> <p>Les fichiers concernés sont « _config.ini », « _var.ini » et « _daq.ini »</p>
<p>Envoi d'un ou plusieurs fichiers de définition.</p> <p>Lorsque la passerelle modifie des fichiers de définition (création par détection par exemple), ces fichiers de définition sont envoyés vers le serveur FTP distant à la prochaine connexion et ce service web est appelé.</p>	<p>NSITE=IDsite&ACTION=UPLOADDEF&ACTION-COMP=liste de fichiers de définition&RC=0&RC-COMP=</p> <p>Les noms des fichiers de définition sont séparés par le caractère « ; ».</p>
<p>Réception d'un ou plusieurs fichiers de définition.</p> <p>Lorsque des fichiers de définition sont modifiés sur le serveur FTP distant, la passerelle les charge lors de la prochaine connexion. Ce service web est alors appelé.</p>	<p>NSITE=IDsite&ACTION=CONFIGDEF&ACTION-COMP=liste de fichiers de définition&RC=0&RC-COMP=</p> <p>Les noms des fichiers de définition sont séparés par le caractère « ; ».</p>
<p>Exécution d'un fichier de commande.</p> <p>Lorsque la passerelle détecte un fichier de commande à charger et exécuter sur le serveur FTP, elle appelle ce service web.</p>	<p>NSITE=IDsite&ACTION=CMD&RC=0&RC-COMP=</p>

Chargement d'un nouveau firmware.
Lorsque la passerelle détecte et charge un fichier de firmware valide (CRC correct) sur le serveur FTP, elle appelle ce service web.

```
NSITE=IDsite&ACTION=CONFIGBIN&RC=0&RC-COMP=
```

Le web service doit retourner une des valeurs suivantes :

Code	Description
00	OK
10	ID site inconnu
11	Code action inconnu
12	RC reçu inconnu
13	Adresse MAC absente
-1	Erreur interne de serveur

Exemples de requêtes web service :

Chargement d'une nouvelle version de firmware :

```
URL/confirm.php;NSITE=IDsite&ACTION=CONFIGBIN&RC=0&RC=
```

Première connexion depuis le dernier démarrage :

```
URL/confirm.php;NSITE=IDsite&ACTION=VERSION&ACTION-COMP=WebdynSunPM  
4.2.3.38295&RC=0&RC-COMP=
```

Chargement des fichiers de configuration IDSite_config.ini et IDsite_var.ini :

```
URL/confirm.php;NSITE=IDsite&ACTION=CONFIGGLOBAL&ACTION-COMP=IDsite_  
config.ini;IDsite_var.ini&RC=0&RC-COMP=
```

4.2 Le serveur MQTT/MQTTS

Le fonctionnement d'un serveur MQTT ou MQTTS est identique. Mais il est préférable d'utiliser un serveur MQTTS qui intègre des couches de sécurité contrairement à un serveur MQTT. La description dans ce chapitre vaut aussi bien pour tous les types de serveurs MQTT.

Paramétrage :

Le serveur MQTT est défini par les paramètres suivants :

- Une adresse : Cette adresse peut être une adresse IP ou un nom de domaine.
- Un port de connexion MQTT (par défaut 1883 pour MQTT et 8883 pour MQTTS).
- Une identification serveur : dépend du type de serveur MQTT choisi. L'identification peut être faite soit par un simple identifiant et mot de passe ou soit par des certificats et une clé à importer dans le concentrateur.
- Une identification applicatif : Identifiant unique du serveur permettant d'avoir son propre espace applicatif.
- Des topics : Nom des canaux d'informations sur le serveur pour le dépôt des données et des alarmes.

Depuis un serveur MQTT/MQTTS, le concentrateur supporte les actions suivantes :

- Dépôt des données,
- Dépôt des alarmes,
- Réception de commande,
- Mettre à jour le concentrateur.

Depuis un serveur MQTT/MQTTS, vous ne pouvez pas :

- Configurer le concentrateur,
- Créer, ajouter ou modifier un fichier de définitions,
- Créer, ajouter ou modifier un script,
- Ajouter ou remplacer un certificat,
- Déposer les logs.

Pour réaliser ces actions, vous devez configurer le deuxième serveur du concentrateur avec un serveur FTP/SFTP.

Arborescence du serveur :

Un serveur MQTT/MQTTS dispose de canaux d'informations appelés topics. Vous devez renseigner le même nom de topic entre le serveur MQTT/MQTTS et le concentrateur.

Un topic doit être renseigné pour les données afin que le concentrateur puisse déposer ces données.

Si vous désirez envoyer les alarmes sur le serveur MQTT/MQTTS, vous devez renseigner un topic pour les alarmes.

Si vous voulez recevoir des commandes à partir du serveur MQTT/MQTTS, vous devez renseigner un topic pour les commandes et un autre topic pour le résultat des commandes.

Fonctionnement :

Le concentrateur se connecte et dépose les données sur le serveur MQTT/MQTTS à chaque planification (schedule) prévue. (Voir chapitre 3.2.2.5.9 : « Schedules »)

Si un nom de topic Alarme et/ou Commande sont renseignés, alors le concentrateur est connecté en permanence avec le serveur MQTT/MQTTS afin de réaliser les actions immédiatement.

Contrairement au serveur FTP/SFTP, les données déposées sur le serveur MQTT/MQTTS sont mise en forme et tiennent compte des coefficients A et B définis ainsi que de l'unité définie pour chaque variable. (voir chapitre 3.1.2.2.2 : « Contenu du fichier de définition »).

4.2.1 Format des données

Le formatage des données est identique, peu importe l'équipement ou l'interface.

Les valeurs remontées sont interprétées et utilisent les coefficients A et B définis pour chaque variable dans le fichier de définition de l'équipement ou de l'interface. (voir chapitre 3.1.2.2.2 : « Contenu du fichier de définition »).

La valeur du champ « action » de l'équipement ou l'interface définie dans son fichier de définition permet l'action suivante :

Code « Action »	Description
0	aucune valeur n'est remontée.
1	la valeur du paramètre est remontée.
2	les valeurs min, max et moyenne sont remontées.
4 ou 6	la valeur instantanée est remontée.
7	les valeurs min, max et moyenne sont remontées dans le fichier d'acquisition ; la valeur instantanée est remontée dans le fichier créée par la commande getData.

Les données du fichier de données de l'équipement ou de l'interface sont au format JSON suivant :

```
{
  "__MetaData__":{
    "id":"concentrator_id"
  },
  "DAQ_Name_eqp_1":[
    {
      "DEF_Name_var_1_eqp_1":var_1_value_1_eqp_1,
      "DEF_Name_var_2_eqp_1":var_2_value_1_eqp_1,
      "DEF_Name_var_X_eqp_1":var_X_value_1_eqp_1,
      "date":"YY/MM/DD-hh:mm:ss",
      "timestamp":value_timestamp_1_eqp_1,
      "nbOfRefreshes":value_nbOfRefreshes_1_eqp_1
    },
    {
      "DEF_Name_var_1_eqp_1":var_1_value_Z_eqp_1,
      "DEF_Name_var_2_eqp_1":var_2_value_Z_eqp_1,
      "DEF_Name_var_X_eqp_1":var_X_value_Z_eqp_1,
      "date":"YY/MM/DD-hh:mm:ss",
      "timestamp":value_timestamp_Y_eqp_1,
      "nbOfRefreshes":value_nbOfRefreshes_Y_eqp_1
    }
  ],
  "DAQ_Name_eqp_N":[
    {
      "DEF_Name_var_1_eqp_N":var_1_value_1_eqp_N,
      "DEF_Name_var_2_eqp_N":var_2_value_1_eqp_N,
      "DEF_Name_var_X_eqp_N":var_X_value_1_eqp_N,
      "date":"YY/MM/DD-hh:mm:ss",
      "timestamp":value_timestamp_1_eqp_N,
      "nbOfRefreshes":value_nbOfRefreshes_1_eqp_N
    },
    {
      "DEF_Name_var_1_eqp_N":var_1_value_Z_eqp_N,
      "DEF_Name_var_2_eqp_N":var_2_value_Z_eqp_N,
      "DEF_Name_var_X_eqp_N":var_X_value_Z_eqp_N,
      "date":"YY/MM/DD-hh:mm:ss",
      "timestamp":value_timestamp_Y_eqp_N,
      "nbOfRefreshes":value_nbOfRefreshes_Y_eqp_N
    }
  ]
}
```

Code couleur :

- En vert : Nom ou variable de l'équipement ou de l'interface.
- En bleu : Données qui dépendent de l'équipement ou de l'interface.
- En noir : Texte fixe.

Avec :

- **DAQ_Name_eqp_N** : Nom de l'équipement N, champ « Name » de l'équipement dans le fichier de <uid>_daq.csv (voir chapitre 3.1.2.1.3.4 : « Déclaration des équipements »)
- **DEF_Name_var_X_eqp_N** : Nom de variable X de l'équipement N, champ « Name » de la variable dans le fichier de définition (voir chapitre 3.1.2.2.2 : « Contenu du fichier de définition »)
- **var_X_value_Z_eqp_N** : Valeur Z de la variable X de l'équipement N collecté au point d'acquisition Y et à l'action définie dans le fichier de définition de l'équipement N.
- **date** : Horodatage des données au point d'acquisition Y en UTC+timezone (voir le paramètre « NTP_TimeZone » en annexe A). Au Format : « YY/MM/DD-hh:mm:ss » pour « Année/Mois/Jours-Heures:Minutes:Secondes »
- **timestamp** : Horodatage des données au point d'acquisition Y en UTC+0. Nombre de millisecondes écoulées depuis le 1 janvier 1970.
- **nbOfRefreshes**: Nombre de lectures complètes sur cette période d'acquisition. Cette information est affichée uniquement si le paramètre « MQTT_EnableAdvancedData » est à 1. Cette donnée peut être utile uniquement pour les équipements Modbus et Onduleurs. Pour les IO, TIC, périphériques virtuels et pour le fichier de collecte de paramètres, le nombre de rafraichissements est toujours à 0.
- **__MetaData__** : Métadonnées sur le contexte des équipements présents dans le fichier. Actuellement la seule information transmise est l'identifiant de la WebdynSunPM dans l'item "id".



Afin d'éviter l'envoi de donnée inutile sur le serveur et permettant ainsi d'optimiser la connexion, il est conseillé d'activer uniquement les variables que l'on souhaite remonter.

Equipements (Modbus, onduleurs) :

Exemple d'un fichier de donnée équipement avec une période d'acquisition toutes les 10 minutes :

- Paramétrage des index du device 1 (ModbusTCP) :

Index	Code « Action »	Affichage
1	1	Valeur du paramètre
2	0	Aucun
3-11	4	Valeur instantanée
12	8	Valeur instantanée

- Paramétrage des index du device 2 (SMANET) :

Index	Code « Action »	Affichage
1-2	2	Valeurs min, max et moyenne

- Fichier de données MQTT au format JSON :

```
{
  "_MetaData_":{
    "id":"WPxxxxxx"
  },
  "modbusTCP":[
    {
      "var_1":32,
      "var_3":52,
      "var_4":5,
      "var_5":102,
      "var_6":1,
      "var_7":0,
      "var_8":1,
      "var_9":0,
      "var_10":0,
      "var_11":0,
      "var_12":0,
      "date":"21/02/05-09:50:00",
      "timestamp":1612515000000,
      "nbOfRefreshes":12
    },
    {
      "var_1":35,
      "var_3":57,
      "var_4":5,
      "var_5":108,
      "var_6":1,
      "var_7":10,
      "var_8":0,
      "var_9":0,
      "var_10":0,
      "var_11":0,
      "var_12":1,
      "date":"21/02/05-10:00:00",
      "timestamp":1612515600000,
      "nbOfRefreshes":12
    }
  ],
  "SMANET":[
    {
      "var_1":[16,32,26.00],
      "var_2":[52,58,51.00],
      "date":"21/02/05-09:50:00",
      "timestamp":1612515000000,
      "nbOfRefreshes":2
    },
    {
      "var_1":[4,6,5.50],
      "var_2":[102,105,103.00],
      "date":"21/02/05-10:00:00",
      "timestamp":1612515600000,
      "nbOfRefreshes":2
    }
  ]
}
```

Entrées/Sortie (IO) :

Exemple d'un fichier de donnée IO avec une période d'acquisition toutes les 10 secondes :

- Paramétrage des entrées/sortie :

Entrées/Sortie	Code « Action »	Affichage
1	2	Valeur instantanée
2	0	Aucun
3	2	Valeur instantanée
4	2	Valeur instantanée
5	2	Valeur instantanée
6	4	Valeurs min, max et moyenne
7	8	Valeur instantanée
8	2	Valeur instantanée

- Fichier de données MQTT au format JSON :

```
{
  "_MetaData_": {
    "id": "WPxxxxxx"
  },
  "IO": [
    {
      "var_1": 0,
      "var_3": 0,
      "var_4": 5,
      "var_5": 1,
      "var_6": [130, 170, 150],
      "var_7": 5,
      "var_8": 0,
      "date": "21/02/05-09:50:00",
      "timestamp": 1612515000000,
      "nbOfRefreshes": 0
    },
    {
      "var_1": 0,
      "var_3": 1,
      "var_4": 2,
      "var_5": 2,
      "var_6": [120, 160, 140],
      "var_7": 3,
      "var_8": 0,
      "date": "21/02/05-10:00:00",
      "timestamp": 1612515600000,
      "nbOfRefreshes": 0
    }
  ]
}
```

4.2.2 Alarmes

Pour que le concentrateur dépose les alarmes sur le serveur MQTT/MQTTS, il faut que le topic Alarme soit renseigné. Le concentrateur reste en connexion permanente avec le serveur MQTT/MQTTS afin de réaliser l'action immédiatement.

Au moment d'une alarme, aucune autre donnée à part celles de l'alarme ne sont déposées sur le serveur. La liste des alarmes pouvant être générées est :

Source Alarme	Info	Description
GATEWAY	Power ON	Démarrage du concentrateur
	Power OFF	Extinction du concentrateur
	Perte accessoire TIC	Accessoire TIC retiré
	Retour accessoire TIC	Accessoire TIC reconnecté
IO	Nom du Fichier de définition + Index + Valeur	Valeur d'une entrée de type alarme a changé
Modbus	Nom du Fichier de définition + Index + Valeur	Valeur d'un index de type alarme à changer

Une alarme « Power OFF » est envoyée après une coupure de secteur d'au moins 10 secondes et une alarme « Power ON » est envoyée après le retour de l'alimentation pendant au moins 1 minute. Les autres alarmes ne sont pas temporisées et sont envoyées dès la détection par le concentrateur.

Le format des données d'alarmes au format JSON est le suivant :

```
{
  "__MetaData__":{
    "id":"concentrator_id"
  },
  "alarms":[
    {
      "defName":defName_alarms,
      "deviceName":deviceName_alarms,
      "source":source_alarms,
      "value":value_alarms,
      "variableIndex":variableIndex_alarms,
      "date":"YY/MM/DD-hh:mm:ss",
      "timestamp":value_timestamp_alarms
    }
  ],
  "alarmsDevice":[
    {
      "type":type_alarmsDevice,
      "info":info_alarmsDevice,
      "date":"YY/MM/DD-hh:mm:ss",
      "timestamp":value_timestamp_alarmsDevice
    }
  ]
}
```

Code couleur :

- En bleu : Données qui dépendent de la source de l'alarme.
- En noir : Texte fixe.

Avec :

- alarms : Alarme ayant pour source IO ou Modbus.
- alarmsDevice : Alarme ayant pour source GATEWAY.
- defName_alarms : Nom du fichier de Définition de l'équipement ou de l'interface qui a déclenché l'alarme. (Voir chapitre 4.1.4 : « Les alarmes « ALARM » »)
- deviceName_alarms: Nom de l'équipement ou de l'interface qui a déclenché l'alarme, champ « Name » de l'équipement dans le fichier de <uid>_daq.csv (Voir le chapitre 3.1.2.1.3.4 : « Déclaration des équipements »)
- source_alarms : Source de l'alarme (IO ou Modbus)
- value_alarms : Valeur de la variable qui a déclenché l'alarme.
- variableIndex_alarms : Index de la variable qui a déclenché l'alarme.
- type_alarmsDevice : Type de l'alarme (GATEWAY).
- info_alarmsDevice : Information sur l'alarme (voir la colonne « Info » du tableau ci-dessus)
- date : Horodatage de l'alarme en UTC+timezone (voir le paramètre « NTP_TimeZone » en annexe A). Au Format : « YY/MM/DD-hh:mm:ss » pour « Année/Mois/Jours-Heures:Minutes:Secondes »
- timestamp : Horodatage de l'alarme en UTC+0. Nombre de millisecondes écoulées depuis le 1 janvier 1970.
- __MetaData__ : Metadata on the context of the devices present in the file. Currently the only information transmitted is the identifier of the WebdynSunPM in the "id" item.

Exemple d'une alarme sur un équipement :

```
{
  "__MetaData__":{
    "id":"WPxxxxxx"
  },
  "alarms":[
    {
      "defName":"WPM00C44F_SunSpec_inverter_SMA_Solar_Inverter_9301_ModbusTCP.csv",
      "deviceName":"ModbusTCP",
      "source":"Modbus",
      "value":"106",
      "variableIndex":3,
      "date":"21/02/05-09:50:00",
      "timestamp":161251500000
    }
  ],
  "alarmsDevice":null
}
```

Exemple d'une alarme interne au concentrateur :

```
{
  " __MetaData__ ": {
    "id": "WPxxxxxx"
  },
  "alarms": null,
  "alarmsDevice": [
    {
      "type": "POWER OFF",
      "info": "GATEWAY",
      "date": "21/02/05-09:50:00",
      "timestamp": 1612515000000
    }
  ]
}
```

4.2.3 Commandes

Il est possible d'envoyer des commandes par le serveur MQTT/MQTTS au concentrateur WebdynSunPM.

Pour cela, les topics « command » et « Result » doivent être renseignés dans la configuration du concentrateur (Voir chapitre 3.2.2.5.4 : « MQTT »).

Quand une commande est publiée sur le topic « Command » sur le serveur MQTT/MQTTS, celle-ci est récupérée par le concentrateur. La commande est exécutée par le concentrateur et le résultat de la commande est publié sur le topic « Result ».

4.2.3.1 Commande de Mise à jour

La commande de Mise à jour permet de récupérer un firmware sur un serveur HTTP/HTTPS ou FTP/SFTP.

Le fichier de commande de Mise à jour est au format JSON suivant :

```
{
  "url": url_value,
  "login": login_value,
  "password": password_value,
  "checksum": checksum_value,
  "interface": interface_value,
}
```

Code couleur :

- En bleu : Informations sur le firmware ou le serveur.
- En noir : Texte fixe.

Avec :

- `url_value` : Adresse IP ou nom de domaine du serveur HTTP/HTTPS ou FTP/SFTP.
- `login_value` : Identifiant pour le serveur FTP/SFTP. Le champ doit être « null » pour un serveur FTP/SFTP.

- **password_value** : Mot de passe pour le serveur FTP/SFTP. Le champ doit être « null » pour un serveur FTP/SFTP.
- **checksum_value** : Checksum du nouveau firmware au format MD5 permettant de vérifier son intégrité.
- **interface_value** : nom de l'interface réseau à utiliser pour accéder au serveur distant afin de récupérer le nouveau firmware. Les valeurs possibles sont « ethernet » ou « modem ».

Exemple de mise à jour par rapport à un serveur HTTPS :

```
{
  "rpcName": "sunpm.updateFirmware",
  "parameters":
  {
    "url": "https://www.webdyn.com/download/wgapp_3.3.666.35005.spm",
    "checksum": "78a37fa7f6714876be7d08d0c39a067b",
    "interface": "modem",
  },
  "callerId": "667"
}
```

Exemple de mise à jour par rapport à un serveur SFTP :

```
{
  "rpcName": "sunpm.updateFirmware",
  "parameters":
  {
    "url": "sftp://192.168.1.66:8081/download/wgapp_3.3.666.35005.spm",
    "login": "login",
    "password": "password",
    "checksum": "78a37fa7f6714876be7d08d0c39a067b",
    "interface": "ethernet",
  },
  "callerId": "668"
}
```

4.3 Carte microSD

L'utilisation de la carte SD répond aux mêmes règles de fonctionnement que pour le serveur FTP.

Les seules différences sont :

- Répertoires non configurables. Les répertoires par défaut sont utilisés et ce sont les mêmes sur toutes les installations.

La carte SD n'est lue que lorsque le concentrateur a besoin d'y accéder. Cela signifie que tout le reste du temps elle peut être retirée sans aucune conséquence. Les informations sont écrites au fur et à mesure de façon sécurisée pour permettre un retrait de la carte en toute sécurité à tout moment.

Le niveau d'utilisation de la carte SD peut être consulté à tout moment sur la page de configuration des serveurs dans l'encart dédié à la carte SD :



Webdyn ne fournit aucune carte SD. Veuillez vous rapprocher d'un revendeur de matériel informatique.

5. Commandes

5.1 Principe

Il est possible d'envoyer des commandes à la WebdynSunPM. Elles permettent d'exécuter des tâches à distance à des fins de configuration, de pilotage ou de surveillance. Par exemple : lancer une recherche d'équipements, obtenir la configuration courante, déclencher une connexion au SI, etc... Le même mécanisme permet également d'invoquer une fonction d'un script installé sur le concentrateur.

5.2 Fonctionnement

Une commande peut être envoyée via trois méthodes distinctes :

- Un fichier de commande déposé sur le serveur (FTP, SFTP ou WebDAV) qui sera récupéré par le concentrateur lors de la connexion SI.
- Un message MQTT posté sur le topic de contrôle de la WebdynSunPM.
- Un SMS envoyé à la carte SIM de la WebdynSunPM.

5.2.1 Fichier de commande

Lors d'une connexion FTP, SFTP ou WebDAV, la WebdynSunPM vérifie la présence d'un fichier de commande dans le répertoire configuré à cet effet (/CMD par défaut). Ce fichier doit être nommé <uid>_cmd.json où <uid> est l'identifiant de la passerelle.

Les commandes incluses dans celui-ci sont au format JSON décrit ci-dessous et sont exécutées dans l'ordre. L'invocation des fonctions de script est également prise en charge. Le fichier est supprimé après import de façon à ne pas traiter deux fois une même commande.

Les résultats de commandes sont également écrits dans des fichiers qui seront déposés lors de la connexion SI suivante. Un fichier peut contenir un ou plusieurs résultats. Ceux-ci sont nommés selon le modèle <uid>_ACK_<timestamp>.json.



Pour une connexion FTP, SFTP ou WebDAV, les commandes fonctionnent uniquement sur le serveur 1 ; les commandes déposées dans le répertoire « /CMD » sur un serveur 2 (backup) ne sont pas prises en compte par le concentrateur.

5.2.1.1 Format JSON du fichier de commande

Le format utilisé pour les commandes et invocations de fonctions de scripts est le suivant :

```
[{
  "rpcName": "<nom du script>.<nom de la fonction>",
  "parameters": { <paramètres de la fonction au format json> },
  "callerId": "<identifiant commande 1>"
},
{
  "rpcName": "<nom du script>.<nom de la fonction>",
  "parameters": { <paramètres de la fonction au format json> },
  "callerId": "<identifiant commande 2>"
},
...
]
```

Propriétés :

- **rpcName** : Nom du script et de la fonction à exécuter sous la forme <nom du script>.<nom de la fonction>. Pour une commande, on utilisera pour le nom de script sunpm qui est réservé pour les commandes internes de la WebdynSunPM.
- **parameters** : Certaines fonctions et commandes nécessitent des paramètres supplémentaires. Lorsque ce n'est pas le cas, ce champ est facultatif.
- **callerId** : Un identifiant associé à cette requête.

Chaque entrée du tableau correspond à une commande différente. À noter que si le fichier ne contient qu'une seule commande, les crochets sont facultatifs. Le format du fichier de résultats est le suivant :

```
[{
  "result": { <éléments retournés par la fonction au format JSON> },
  "error": "<description de l'erreur en cas d'échec>",
  "callerId": "<identifiant commande 1>"
},
{
  "result": { <éléments retournés par la fonction au format JSON> },
  "error": "<description de l'erreur en cas d'échec>",
  "callerId": "<identifiant commande 2>"
},
...
]
```

Propriétés :

- **result** : En cas de succès de la fonction ou de la commande, celle-ci retourne un résultat au format JSON contenu dans ce champ. En cas d'erreur ce champ est absent.
- **error** : En cas d'erreur, ce champ contient un descriptif du problème rencontré. En cas de succès de la fonction ou de la commande, ce champ est absent.
- **callerId** : Le même identifiant que dans la requête. Ainsi vous pouvez associer cette réponse à sa requête d'origine.

Chaque entrée du tableau correspond à un résultat de commande différent.

5.2.1.2 Exemple

Partons du script suivant pour illustrer l'invocation de fonction :

```
header = {
  version = 1.1,
  label = "Test",
  name = "test"
}
--[[
Test function
]]
function testFunction(parameters)
  wd.log("question is " .. parameters.text)
  local result = {
    value = 42 = 42
  }
  return result
end
```

Fichier de commande permettant d'invoquer la fonction :

```
[{
  "rpcName": "test.testFunction",
  "parameters": {
    "text": "what is the answer ?" "is the answer ?"
  },
  "callerId": "3d9311ed-0076-4f28-ac59-a2debfa35b86"
}]
```

Fichier de résultat obtenu :

```
[{
  "result": {
    "value": 42
  },
  "callerId": "3d9311ed-0076-4f28-ac59-a2debfa35b86"
}]
```

5.2.2 Message de commande MQTT

La WebdynSunPM peut recevoir des messages de commande en MQTT. Bien entendu, pour cela il faut qu'un serveur MQTT soit configuré (Voir chapitre 3.2.2.5.4 : « MQTT »). En particulier les topics de commandes et de résultats doivent être renseignés. La WebdynSunPM s'inscrit au topic de commande de sorte que tout message envoyé sur celui-ci est reçu et exécuté. Le résultat d'une commande ou d'une invocation de fonction est publié sur le topic de résultat.

Le format JSON utilisé pour ces messages est le format JSON décrit au chapitre 5.2.1.1 : « Format JSON du fichier de commande ».



Un message MQTT ne peut contenir qu'une seule commande ou résultat. En conséquence, les crochets ouvrant et fermant ne sont pas autorisés.

5.2.2.1 Utilisation avec Azure IoT

Azure possède son propre mécanisme d'invocation de fonctions. Le format JSON utilisé est donc le suivant :

```
{
  "methodName":"<nom du script>.<nom de la fonction>",
  "responseTimeoutInSeconds":<délai avant timeout>,
  "payload":{
    "parameters":{ <paramètres de la fonction au format json> }
  }
}
```

Propriétés :

- methodName remplace rpcName.
- parameters est contenu dans le champ payload du message Azure.
- callerId est ignoré.

5.2.3 SMS

Il est possible d'envoyer des commandes SMS au modem de la WebdynSunPM. Pour cela, vérifier que le modem soit correctement configuré (Voir chapitre 3.2.2.4 : « Modem »).

Les commandes SMS n'utilisent pas le format JSON. À la place le format accepté est le suivant :

```
<commande 1>=<paramètre 1>:<paramètre 2>:<paramètre 3>... ;
<commande 2>=<paramètre 1>:<paramètre 2>:<paramètre 3>... ;
...
```

5.3 Liste des Commandes

Liste des commandes disponibles sur le concentrateur :

Commandes	Descriptions	SMS	MQTT/ MQTTS	Fichier de commande
connect	Déclenchement d'une connexion	x	X	
status	Récupération du statut du concentrateur	X	X	X
factory	Retour aux paramètres usines	X	X	X
reboot	Redémarrage du concentrateur	X	X	X
updateFirmware	Mise à jour logiciel du concentrateur	X	X	X
apn	Configuration du modem	X	X	X
ftp	Configuration du serveur FTP	X	X	X
sftp	Configuration du serveur SFTP	X	X	X
https	Configuration du serveur Webdav/ HTTPS	X	X	X
log	Activation des logs des communications des équipements	X	X	X
setRelay	Modification de l'état du relais	X	X	X
discoverDevices	Découverte d'équipements	X	X	X
getParameters	Collecte des paramètres c'est-à-dire des variables définies avec le code action 1	X	X	X
getData	Collecte des variables définies avec un code action 6 ou 7	X	X	X
writeVariable	Écriture de variable sur un équipement	X	X	X

setKey	Ajout des clés pour le déchiffrement des scripts clients	X	X	X
deleteKey	Suppression des clés pour le déchiffrement des scripts clients	X	X	X
startScript	Démarrage d'un script	X	X	X
stopScript	Arrêt d'un script	X	X	X



Dans le cas d'envoi de plusieurs commandes simultanées, les commandes « factory » et « update » peuvent faire perdre les commandes qui suivent. En cas d'erreur sur une commande précédente, les suivantes seront exécutées.

Les commandes disponibles sont décrites ci-dessous avec les paramètres attendus et les résultats retournés.

5.3.1 « connect » : Déclenchement d'une connexion

Demande à la WebdynSunPM de démarrer une connexion vers le serveur. Cela force alors une synchronisation des paramètres avec le serveur ainsi que le dépôt de tous les fichiers de journalisation. La connexion est lancée immédiatement.

Disponible via SMS uniquement.

```
connect=<connexion>
```

Paramètres :

- connexion : Numéro de la connexion à établir. En l'absence de paramètre, la connexion se fera sur le serveur 1. Les valeurs possibles sont :
 - 1 : Utilisation du serveur 1.
 - 2 : Utilisation du serveur 2.

Retourne :

- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

Exemples SMS :

```
connect
```

ou

```
connect=2
```

Exemple commande MQTT :

```
{  
  "rpcName": "sunpm.connect",  
  "callerId": "1"  
}
```

Et réponse :

```
{  
  "callerId": "1",  
  "result": "OK"  
}
```

5.3.2 « status » : Récupération du statut du concentrateur

Retourne des informations sur la configuration actuelle.

```
status
```

Pas de paramètres par SMS.

Exemple de SMS :

.

```
status
```

Par fichier de commande, le paramètre suivant est pris en compte :

- **number** : Numéro de téléphone qui recevra les SMS de statut envoyé par la passerelle. Il est préférable de renseigner le numéro avec l'indicatif international.

Un fichier d'acquittement de la commande est envoyé sur le serveur (FTP, SFTP, WebDAV, MQTT/MQTTS) qui a envoyé la commande. Les informations de la commande sont quant à eux envoyés sur le numéro de téléphone renseigné.

La commande « status » envoyé par fichier de commande (FTP, SFTP, WebDAV) ou par MQTT/MQTTS permet de récupérer le numéro de la carte SIM du concentrateur.

Exemple de fichier commande (FTP/SFTP/WebDav) :

```
{
  "rpcName": "sunpm.status",
  "parameters": {
    "number": "+33700000000"
  },
  "callerId": "1"
}
```

- Les informations de la commande sont retournées sous la forme de SMS dont voici le détail :

```
type=WebdynSunPM 3G
idSite=WPM01194D
FW=WebdynSunPM 4.2.12.39124
ModeServ1=modem
apn=tm
csq=26,99
network=3G
ip=192.168.1.12
mask=255.255.255.0
gw=
dns=
srv1:
type=ftp
addr=user@ftpserver.com:21
last=12/10 12:53 success
```

- *type* : Nom du produit
- *idSite* : Correspond au nom du site, c'est-à-dire l'identifiant de la WebdynSunPM.
- *FW* : Numéro de version du firmware actuellement chargé sur le concentrateur.
- *ModeServ1* : Mode de connexion serveur (ethernet ou modem).
- *apn* : Nom de l'apn configuré pour le modem.
- *csq* : Force du signal modem.
- *network* : Type de réseau utilisé.
- *ip* : Adresse IP configurée sur l'interface Ethernet 1.
- *mask* : Masque de sous-réseau configuré sur l'interface Ethernet 1.
- *gateway* : Adresse de la passerelle permettant au concentrateur de se connecter à un réseau extérieur sur l'interface Ethernet 1.
- *dns* : Liste des serveurs DNS utilisés pour la résolution de noms pour l'interface Ethernet 1. Si plusieurs serveurs DNS sont configurés, ils sont séparés par le caractère '/'.
- *type* : Type du serveur 1. Les valeurs possibles sont :
 - *ftp* : Le serveur est de type FTP.
 - *sftp* : Le serveur est de type SFTP.
 - *webdav* : Le serveur est de type WebDAV-HTTPS.
 - *mqtt* : Le serveur est de type MQTT.
 - *mqttts* : Le serveur est de type MQTTS.
- *addr* : Adresse du serveur au format login@server-address:server-port.

- *last* : Dernière date et heure à laquelle la WebdynSunPM s'est connectée au serveur 1 ainsi que le résultat de cette connexion au format suivant : « JJ/MM HH :MM <résultat de la connexion> ».

5.3.3 « factory » : Retour aux paramètres usines

Réinitialisation de la WebdynSunPM. Les fichiers de configuration ainsi que les données d'acquisition des équipements sont supprimés et le produit est redémarré immédiatement.

```
factory
```

Pas de paramètres.

Retourne :

- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

Exemple SMS :

```
factory
```

5.3.4 « reboot » : Redémarrage du concentrateur

Redémarrage de la WebdynSunPM. Cette commande s'exécute immédiatement.

```
reboot
```

Pas de paramètres.

Retourne :

- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

Exemple SMS :

```
reboot
```

5.3.5 « updateFirmware » : Mise à jour logiciel du concentrateur

Récupère un firmware à une URL spécifiée, le valide grâce à un checksum et l'installe. La commande retourne un résultat succès juste avant de procéder à l'installation. Le résultat de l'installation proprement dit doit être vérifié par les moyens habituels de contrôle de la version.

```
updatefirmware=<url>:<login>:<password>:<checksum>:<interface>
```

Paramètres :

- url : URL du fichier à récupérer. Les protocoles acceptés sont HTTP, HTTPS, FTP, SFTP. Le port peut être précisé via le format address:port.
- login : Identifiant du serveur.
- password : Mot de passe du serveur.
- checksum : Checksum MD5 du fichier pour vérification de validité.
- interface : Interface utilisée pour la connexion : ethernet ou modem.

Retourne :

- En cas de succès : le message "Firmware downloaded successfully. System will restart...".
- Si une erreur est rencontrée : un message explicatif.

Exemple, commande MQTT :

```
{
  "rpcName": "sunpm.updateFirmware",
  "parameters": {
    "url": "https://www.webdyn.com/download/wgapp_new_fw.spm",
    "checksum": "78a37fa7f6714876be7d08d0c39a067b",
    "interface": "modem"
  },
  "callerId": "674"
}
```

Et réponse :

```
{
  "callerId": "674",
  "result": "Firmware downloaded successfully. System will restart..."
}
```

Exemple SMS :

```
updatefirmware=ftp://ftp3.webdyn.com/wgapp_4.1.0.37427.  
spm:login:webdyn:70a0eeeeae295a7e16d3811b66bee9b66:modem
```

5.3.6 « apn » : Configuration du modem

Configuration de l'APN du modem. Cet APN est nécessaire pour établir une connexion mobile en 2G/3G. Voir la configuration du modem au chapitre 3.2.2.4 : « Modem » pour plus de précisions.

```
apn=<apn>:<login>:<password>
```

Paramètres :

- aapn : Nom de l'APN à utiliser pour la connexion modem.
- login : Utilisateur nécessaire pour l'authentification sur certains APN.
- password : Mot de passe nécessaire pour l'authentification sur certains APN.

Retourne :

- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

Exemples SMS :

```
apn=m
```

ou

```
apn=m2minternet
```

5.3.7 « ftp » : Configuration du serveur FTP/SFTP

Configuration du serveur FTP/SFTP « Serveur 1 ».

```
ftp=<server>:<login>:<password>:<port>:<interface>
```

5.3.8 « sftp » : Configuration du serveur SFTP

Cette commande est similaire à la commande « ftp » hormis qu'elle permet de paramétrer un serveur SFTP.

5.3.9 « https » : Configuration du serveur Webdav/HTTPS

Cette commande est similaire à la commande « ftp » hormis qu'elle permet de paramétrer un serveur Webdav/HTTPS.

Paramètres :

- server : Nom du serveur FTP auquel se connecter. Ce paramètre peut être un nom ou une adresse IP.
- login : Nom de l'utilisateur sur le serveur FTP indiqué.
- password : Mot de passe associé à l'utilisateur ci-dessus.
- port : Numéro de port du serveur FTP. Par défaut les serveurs FTP utilisent le port 21.
- interface : Type de connexion à utiliser. Les valeurs autorisées sont :
 - ethernet : Utilise la liaison Ethernet RJ45 pour établir la connexion avec le serveur FTP. Il faut que l'interface Ethernet ait été préalablement configurée pour que la connexion fonctionne (Voir chapitre 3.2.2.3 : « Réseaux (Networks) »).
 - modem : Utilise le modem pour établir la connexion avec le serveur FTP. Il faut que le modem ait été configuré au préalable. Sinon, il est possible d'utiliser la commande apn pour le configurer par SMS (Voir chapitre 5.3.6 : « apn » : Configuration du modem »).

Retourne :

- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

Exemple SMS :

```
ftp=ftp3.webdyn.com:login:webdyn:70a0eeeeae295a7e16d3811b66bee9b6621
```

5.3.10 « log » : Activation des log des communications des équipements

Cette commande permet d'activer le système de log des communications des équipements.

```
log=<interface>:<duration>
```

Paramètres :

- interface : Le nom de l'interface sur laquelle démarrer les logs : ethernet, serial1, serial2 ou serial3.
- duration : Durée en minutes pendant laquelle les logs seront activés.

Retourne :

- En cas de succès pour une commande JSON : "OK".
- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

Exemple, fichier de commande :

```
[{
  "rpcName": "sunpm.log",
  "parameters": {
    "interface": "ethernet",
    "duration": 2
  },
  "callerId": "672"
},
{
  "rpcName": "sunpm.log",
  "parameters": {
    "interface": "ethernet",
    "duration": 1
  },
  "callerId": "673"
}]
```

Et réponse :

```
[
  {"callerId": "672", "result": "OK"},
  {"callerId": "673", "error": "Invalid interface: ethernet"}
]
```

Exemple SMS :

```
log=serial1:5
```

5.3.11 « setRelay » : Modification de l'état du relais

Modifie l'état du relais : ouverture, fermeture ou impulsion de 1s.

Disponible via fichier de commande (FTP, SFTP ou WebDAV), message MQTT/MQTTS et SMS.

```
setrelay=<action>
```

Paramètres :

- *action* : Action à exécuter : open, close ou pulse.

Retourne :

- En cas de succès pour une commande JSON : "OK".
- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

Exemple SMS :

```
setrelay=pulse
```

5.3.12 « discoverDevices » : Découverte d'équipements

Déclenche une découverte d'équipements.

Disponible via fichier de commande (FTP, SFTP ou WebDAV), message MQTT/MQTTS et SMS.

```
discoverdevices=<protocol>:<maxDevices>:<interface>:<timeout>:<port>
```

Paramètres :

- *protocol* : Les codes ci-dessous permettent de lancer la découverte de divers types d'équipements.
- *sunspec* : SunSpec
- *tic* : TIC
- *abbpvi* : ABB PVI
- *abb2* : ABB autres onduleurs
- *cefem* : Cefem
- *fronius* : Fronius

- *goodwe* : Goodwe
- *growatt* : Growatt
- *huawei* : Huawei
- *3play* : Ingeteam 3Play
- *1playhf* : Ingeteam 1Play HF
- *1playtlm* : Ingeteam 1Play TLM
- *powerblock* : Ingeteam Power Block
- *powermax* : Ingeteam Powe Max
- *kacomodbus* : Kaco Modbus
- *kostal* : Kostal
- *smamodbus* : SMA Modbus
- *solis* : Solis
- *sungrow* : Sungrow
- Certains équipements utilisant un protocole propriétaire peuvent également être détectés via cette commande (voir annexe spécifique des protocoles propriétaires).
- *maxDevices* : Nombre maximum d'équipements à découvrir. Lorsque ce nombre est atteint, la découverte cesse. Ce paramètre est ignoré dans le cas du protocole TIC.
- *interface* : Interface utilisée pour la découverte : serial1, serial2, serial3, ethernet1 ou ethernet2. Ce paramètre est ignoré dans le cas du protocole TIC. Seul le protocole SunSpec est compatible avec les valeurs ethernet1 et ethernet2.
- *timeout* : Durée maximum (en millisecondes) pour la découverte d'un équipement. Ce paramètre est ignoré dans le cas du protocole TIC.
- *port* : Port utilisé pour une découverte réseau. Ce paramètre n'a de sens que pour une découverte SunSpec sur Ethernet. Il est ignoré dans les autres cas.

Retourne :

- En cas de succès : le nombre d'équipements découverts.
- Si une erreur est rencontrée : un message explicatif.

En SMS, la commande detect est également disponible mais elle est limitée à une détection SunSpec (cf. supra).

Exemple SMS :

```
discoverdevices
```

5.3.13 « getParameters » : Collecte des paramètres

Lorsque cette commande est reçue par la WebdynSunPM, les variables définies avec un code d'action 1 (ACTION_PARAMETER) sont collectées. À la connexion SI suivante, les données seront déposées dans un fichier nommé <uid>_<interface>_P_<timestamp>.csv.gz.

```
getparameters
```

Pas de paramètres.

Retourne :

- En cas de succès pour une commande JSON : “OK”.
- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

Exemple SMS :

```
getparameters
```

5.3.14 « getData » : Collecte des variables de code action 6 ou 7

Lorsque cette commande est reçue par la WebdynSunPM, les variables définies avec un code action 6 ou 7 sont collectées. La valeur relevée ici pour chaque variable est la dernière lue, même pour un code action 7. Les valeurs de type min, max, moyenne ne sont calculées que dans le fichier d'acquisition. À la connexion SI suivante, les données instantanées seront déposées dans un fichier nommé <uid>_<interface>_I_<timestamp>.csv.gz.

De plus si un serveur MQTT est configuré, la connexion sur celui-ci est réalisée automatiquement de sorte que ces données sont déposées immédiatement.

Si des données sont disponibles en plus des données instantanées, elles seront également déposées sur le serveur distant avec le nommage habituel.

```
getdata
```

Pas de paramètres.

Retourne :

- En cas de succès pour une commande JSON : “OK”.
- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

Exemple, fichier de commande :

```
[{
  "rpcName": "sunpm.getData",
  "callerId": "1"
}]
```

Et réponse :

```
[
  {"callerId": "1", "result": "OK"}
]
```

5.3.15 « writeVariable » : Ecriture de variable sur un équipement

Écriture d'une variable déclarée dans un fichier de définition.

```
writevariable=<deviceName>:<tagName>:<value>
```

Paramètres :

- deviceName : Nom de l'équipement ciblé.
- tagName : Tag ciblé.
- value : Valeur à écrire. Il peut s'agir d'un nombre ou d'une chaîne de caractères. À noter qu'en SMS la valeur sera interprétée comme un nombre si cela est possible. Pour forcer l'interprétation en chaîne de caractères, il est possible d'encadrer la valeur entre "".

Retourne :

- En cas de succès pour une commande JSON : "OK".
- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

Exemple SMS :

```
writevariable=INV1:setLimit:30
```

5.3.16 « setKey » : Ajout des clés pour le déchiffrement des scripts clients

Cette commande permet d'ajouter les clés pour le déchiffrement des scripts Lua clients. Les clés doivent être dans un format spécifique et contenu dans un fichier. Le fichier contenant les clés doit être mis à disposition sur un serveur afin d'être téléchargeable par la commande. Pour plus de détails sur le format des clés pour les scripts Lua, voir le document « WebdynSunPM LUA User Guide.pdf ».

```
setkey=<url>:<login>:<password>:<interface>
```

Paramètres :

- url : URL du fichier à récupérer. Les protocoles acceptés sont HTTP, HTTPS, FTP, SFTP. Le port peut être précisé via le format address:port
- interface : Interface utilisée pour la connexion : ethernet ou modem
- login : Identifiant du serveur
- password : Mot de passe du serveur

Retourne :

- En cas de succès pour une commande JSON : "OK".
- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

Exemple, fichier de commande :

```
[{
  "rpcName": "sunpm.setKey",
  "parameters": {
    "url": "ftp://ftp.webdyn.com/script_key.json",
    "interface": "ethernet",
    "login": "login",
    "password": "pwd"
  },
  "callerId": "203"
}]
```

Réponse OK :

```
[
  {"callerId": "203", "result": "OK"}
]
```

Ou réponse avec une erreur :

```
[
  {"callerId": "203", "error": "Invalid interface: ethernet"}
]
```

Exemple SMS :

```
setkey=ftp://ftp.webdyn.com/script_key.json:ethernet:login:pwd5
```

5.3.17 « deleteKey » : Suppression des clés pour le déchiffrement des scripts clients

Cette commande permet de supprimer des clés pour le déchiffrement des scripts Lua clients.



Si des scripts au format « .luax » sont présents après la suppression des clés de déchiffrement, ils continueront de fonctionner tant que le script reste actif et que le concentrateur n'est pas redémarré. Il est vivement recommandé de supprimer les scripts « .luax » après une suppression des clés.

```
deletekey
```

Retourne :

- En cas de succès pour une commande JSON : "OK".
- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

Exemple, fichier de commande :

```
[{  
  "rpcName":"sunpm.deleteKey",  
  "callerId":"117"  
}]
```

Réponse OK :

```
[  
  {"callerId":"117", "result":"OK"}  
]
```

Exemple SMS :

```
deletekey
```

5.3.18 « startScript » : Démarrage d'un script

Démarre le script spécifié.

```
startscript=<name>
```

Paramètres :

- name : Nom du script à démarrer.

Retourne :

- En cas de succès pour une commande JSON : "OK".
- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

5.3.19 « stopScript » : Arrêt d'un script

Arrête le script spécifié.

```
stopscript=<name>
```

Paramètres :

- name : Nom du script à démarrer.

Retourne :

- En cas de succès pour une commande JSON : "OK".
- En cas de succès pour une commande SMS : pas de retour.
- Si une erreur est rencontrée : un message explicatif.

6. Mise à jour

Le concentrateur WebdynSunPM peut être mis à jour localement par l'interface web ou à distance par FTP, SFTP ou WebDAV-HTTPS. La dernière version du firmware (« WebdynSunPM_x.x.x.zip») est disponible au téléchargement sur notre site à l'adresse suivante : <https://www.webdyn.com/support/WebdynSunPM/>

Après le téléchargement, décompresser le fichier (Zip) qui comprend 2 fichiers :

- « wgapp_x.x.x.xxxx.spm » qui correspond au firmware du concentrateur.
- « CheckSumx.x.x.txt » qui comprend le checksum du firmware.

6.1 Par Interface web

Pour mettre à jour le concentrateur localement, il faut passer par son interface web et aller dans l'onglet « System » puis « Update » et suivre la procédure de mise à jour par l'interface web (voir chapitre 3.2.3.2 « Mise à jour (Update) »).

6.2 Par FTP/SFTP/WebDAV

Pour une mise à jour à distance, il faut suivre les étapes suivantes :

- Mettre le fichier « wgapp_x.x.x.xxxx.spm » contenant la mise à jour doit être déposé dans le répertoire « BIN » du serveur distant.
- Éditer le fichier « <uid>_config_.ini » (<uid> : Identifiant du concentrateur) qui se trouve dans le répertoire « CONFIG » du serveur. Et mettre le nom du fichier qui vient d'être déposé dans le répertoire « BIN » dans la variable « BIN_FileName » et renseigner le checksum indiqué dans le fichier « CheckSumx.x.x.txt » dans la variable « BIN_Checksum ».

Le concentrateur récupérera son fichier de configuration puis son nouveau firmware à la prochaine connexion au serveur.



La mise à jour par FTP, SFTP ou WebDAV-HTTPS est réalisable uniquement par le serveur primaire.

L'application de la mise à jour peut se voir dans les fichiers de LOG déposés dans le répertoire « LOG » du serveur.

Après l'application de la mise à jour, il est possible de supprimer le fichier firmware et de mettre le champ vide des variables « BIN_FileName » et « BIN_Checksum » du fichier de configuration « <uid>_config_.ini ».

Si une erreur survient lors de la mise à jour, celle-ci ne sera pas retentée.



Le non-respect de l'ordre des étapes décrites dans la procédure entraîne un échec de la mise à jour du concentrateur.

6.3 Par commande SMS ou MQTT/MQTTS

La commande « updateFirmware » permet la mise à jour de la WebdynSunPM en spécifiant une URL ou trouver le nouveau firmware. Pour les détails de la procédure, voir le chapitre 5.3.5 : « « updateFirmware » : Mise à jour logiciel du concentrateur ».

6.4 Par carte micro SD

Pour une mise à jour via la carte SD, il faut suivre les étapes suivantes :

- Mettre le fichier « wgapp_x.x.x.xxxx.spm » contenant la mise à jour dans le répertoire « \BIN » de la carte SD.
- Éditer le fichier « <uid>_config_.ini » (<uid> : Identifiant du concentrateur) qui se trouve dans le répertoire « CONFIG » de la carte SD.

Mettre le nom du fichier qui vient d'être déposé dans le répertoire « BIN » dans la variable « BIN_FileName » et renseigner le checksum indiqué dans le fichier « CheckSumx.x.x.txt » dans la variable « BIN_Checksum ».

Le concentrateur récupérera son fichier de configuration puis son nouveau firmware à la prochaine « connexion » sur la carte SD.



La mise à jour n'est réalisable de cette manière que si la carte SD est configurée comme support principal

L'application de la mise à jour peut se voir dans les fichiers de LOG déposés dans le répertoire « LOG » de la carte SD.

Après l'application de la mise à jour, il est possible de supprimer le fichier firmware et de mettre le champ vide des variables « BIN_FileName » et « BIN_Checksum » du fichier de configuration « <uid>_config_.ini ».

Si une erreur survient lors de la mise à jour, celle-ci ne sera pas retentée.



Le non-respect de l'ordre des étapes décrites dans la procédure entraîne un échec de la mise à jour du concentrateur.



Webdyn ne fournit aucune carte SD. Veuillez vous rapprocher d'un revendeur de matériel informatique.

7. Outils & diagnostics

7.1 Diagnostics

En cas de dysfonctionnement du produit, il existe plusieurs moyens de diagnostiquer les défauts.

- Tout d'abord si le concentrateur est connecté par le modem avec une carte SIM, il est possible de demander un statut au produit en lui envoyant la commande « status ». (Voir chapitre 5.3.5 : « « updateFirmware » : Mise à jour logiciel du concentrateur »)
- Les fichiers de log décrits au chapitre 4.1.8 : « Les Logs « LOG » permettent de visualiser les différentes erreurs et d'en comprendre les causes. Il existe des fichiers de log pour chaque fonctionnalité du concentrateur afin de mieux isoler les problèmes.
- Il est également possible de diagnostiquer les erreurs de communication Ethernet ou série en utilisant les outils intégrés. Ces outils peuvent être activés par FTP (Voir chapitre 5.3.8 : « « log » : Activation des log des communications des équipements »), par SMS (Voir chapitre 5.3.8 : « « log » : Activation des log des communications des équipements ») ou par l'interface WEB (Voir chapitre 3.2.1.3 : « Outils de diagnostics des équipements »).
- Sur la page « Home » de l'interface WEB, la partie « Device info » permet de voir l'ensemble des équipements et de détecter rapidement ceux en anomalie. (voir chapitre 3.2 : « Interface web embarquée »)

En cas de besoin, la WebdynSunPM peut être redémarrée à distance en utilisant la commande SMS « reboot » (Voir chapitre 5.3.4 : « « reboot » : Redémarrage du concentrateur »).

Enfin, il est possible de procéder à une réinitialisation totale du produit en envoyant la commande SMS « factory » (Voir chapitre 5.3.3 : « « factory » : Retour aux paramètres usines »).

7.2 Outils

Definition File Converter

Le format des fichiers ayant évolué entre ces deux produits, un outil est mis à disposition pour la conversion des fichiers de définition de la WebdynSun vers la WebdynSunPM.

Cet outil peut être téléchargé sur le serveur web Webdyn à l'adresse suivante : www.webdyn.com/download/DefFileConverter.zip

Pour toute question, contacter le support : support@webdyn.com

8. FAQ

Configuration de la passerelle :

Comment accéder à la configuration de la passerelle ?

Commencer par vérifier que les paramètres IP de l'ordinateur sont compatibles avec l'adresse IP de la WebdynSunPM (par défaut 192.168.1.12)

Lancer un navigateur Web (Chrome, Firefox, Edge, Safari, ...) et saisir l'adresse IP du concentrateur WebdynSunPM dans la barre d'adresse. Une page d'authentification va s'afficher :



Les accès par défaut sont :

Identifiant	Mot de passe
userhigh	high

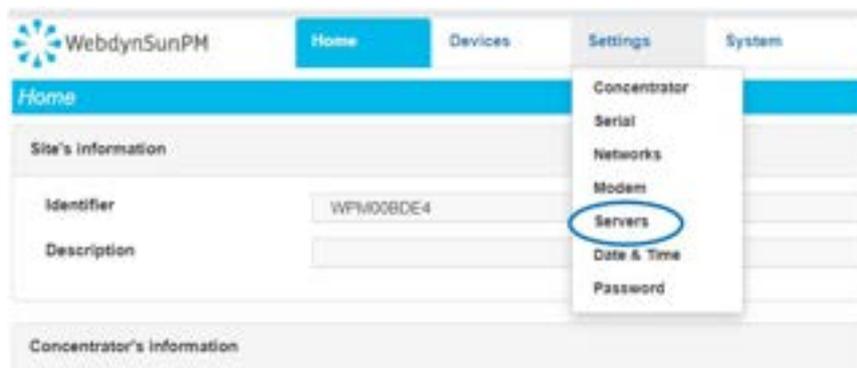
Cliquer sur « Login ».

Comment configurer le concentrateur WebdynSunPM pour qu'il accède au serveur FTP distant ?

Il existe deux solutions de configuration, via l'interface web et via SMS :

- Configuration via l'interface web :

Établir tout d'abord une connexion au concentrateur en se connectant dessus pour accéder à la configuration des serveurs :



Saisir le mode de connexion « Ethernet » ou « modem » :

Connection status: 2021-02-15 11:00:25 Connection term

Server 1

Name: FTP local

Interface: Ethernet (dropdown menu open showing Ethernet and Modem)

Server type: (empty)

Dans le cas d'une configuration par Ethernet, veiller à ce que les paramètres IP soient compatibles avec l'accès au serveur d'après la configuration du réseau local du concentrateur. Dans le cas d'une connexion par Ethernet, la configuration doit être compatible avec la topologie du réseau local du concentrateur afin qu'il puisse accéder aux serveurs. Cette configuration se fait via la page de configuration « Networks » (voir chapitre « Réseaux (Networks) »). Dans le cas d'une connexion par modem, la configuration du modem doit être correcte avant de pouvoir effectuer une connexion. Cette configuration se fait dans la page de configuration « Modem » (voir chapitre « Modem »).

Les paramètres des serveurs à configurer au minimum sont les suivants :

Server 1

Name: FTP local

Interface: Ethernet

Server type: Primary server

Port: 21

Login: (empty)

Type: FTP

Address: 192.00.1.13

Password: (empty)

Il faut donc configurer les champs : « Interface », « Type », « Server type », « Address », « Port », « Login » et « Password ». Les autres champs peuvent être laissés aux valeurs par défaut à condition que les répertoires aient été créés correctement auparavant. Voir chapitre 3.1.2 : « Fichiers de configuration » pour plus de détails.

- Configuration par SMS : la configuration par SMS nécessite l'envoi des commandes suivantes :
 - apn : pour configurer l'APN de la carte SIM. (voir chapitre 5.3.6 : « apn » : Configuration du modem. Erreur ! Source du renvoi introuvable).

```
apn <apn> <utilisateur> <mot de passe>
```

- ftp : pour configuration le serveur FTP qui va contenir la configuration du concentrateur (voir chapitre 5.3.7 : « ftp » : Configuration du serveur FTP/SFTP ». Erreur ! Source du renvoi introuvable).

```
ftp <serveur> <utilisateur> <mot de passe> <port> <interface>
```

- connect : pour lancer la connexion au serveur FTP et charger la configuration (voir chapitre 5.3.1 : « connect » : Déclenchement d'une connexion »).

```
connect <connexion>
```



Pour la configuration par SMS, il ne faut pas rajouter d'espaces entre les paramètres. La syntaxe doit être strictement identique.

Quels sont les identifiants d'accès au serveur FTP ?

L'accès au serveur FTP dépend de la solution adoptée.

Si vous avez choisi un portail, les identifiants d'accès au serveur FTP vous sont communiqués par celui-ci.

Si vous voulez utiliser votre propre serveur FTP, veuillez vous rapprocher de votre administrateur réseau.

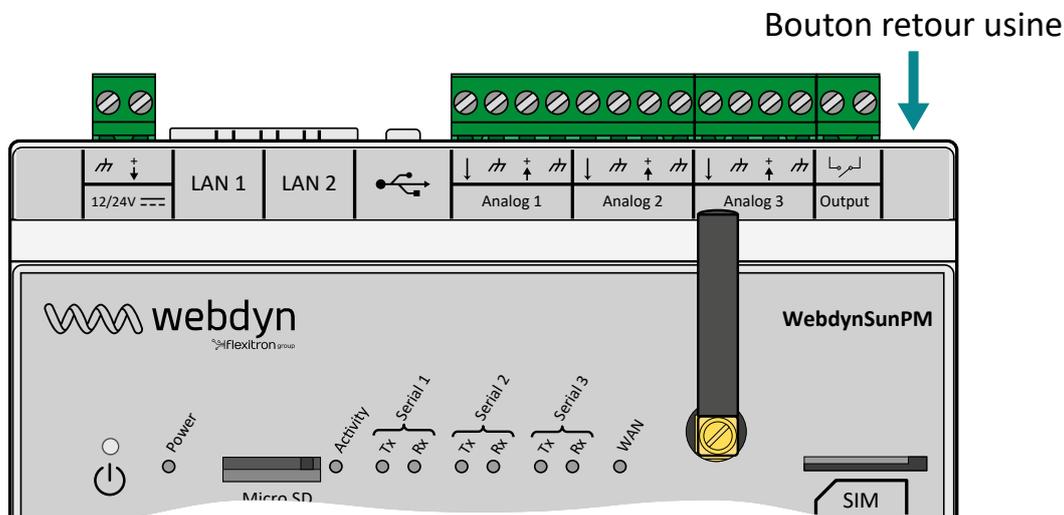
Pour toutes autres configurations et pour déterminer la solution qui convient le mieux, il faut se rapprocher du service commercial Webdyn qui saura conseiller et rediriger vers les interlocuteurs pertinents : contact@webdyn.com.

Utilisation générale de la passerelle

Comment réinitialiser le concentrateur ?

Il existe 2 méthodes pour forcer un retour aux paramètres usine du concentrateur :

- Appuyer sur le bouton Retour Usine du concentrateur pendant 20 secondes :



Attendre. Le concentrateur va redémarrer avec sa configuration usine.

- Si une carte SIM est installée et configurée, un SMS « factory » permet également d'effectuer un retour usine. Il suffit de l'envoyer au numéro de téléphone de la carte SIM (voir chapitre 5.3.3 : « « factory » : Retour aux paramètres usines ». Erreur ! Source du renvoi introuvable).



Le retour à la configuration usine restaure la configuration à son état d'origine. Les données ne seront pas conservées.

La passerelle peut-elle envoyer des commandes aux équipements connectés ?

Il est possible d'envoyer des commandes aux équipements connectés si celui-ci les accepte.

Combien de temps les data peuvent-elles être sauvegardées ?

La WebdynSunPM mémorise jusqu'à 50Mo de données non compressées par équipement déclaré.

En cas de non-accès au serveur distant, le concentrateur WebdynSunPM peut donc stocker les données pendant plusieurs mois.

Le temps maximum de stockage de données varie en fonction du nombre de données à collecter et de la fréquence de la collecte configurée.

La durée moyenne de sauvegarde varie entre 3 et 4 mois.

Quelle est la durée de vie de la batterie ?

La durée de vie moyenne de la batterie est de 5 ans.

Elle peut varier selon l'environnement de l'installation.

Quelles sont les conditions de garantie ?

Tous nos produits sont garantis 2 ans.

Pour plus d'information, consultez nos conditions générales de vente.

Quel est le volume de données échangé par le modem ?

Le volume de données dépend des fichiers échangés.

La moyenne est de l'ordre de 5 Mo par mois et varie pour chaque installation.

Compatibilité des onduleurs

Quels sont les onduleurs compatibles ?

Voir chapitre 1.4 : « Équipements supportés ».

Compatibilité des équipements Modbus

Puis-je connecter différents équipements Modbus sur le même port série ?

Oui, il est possible de connecter différents équipements Modbus sur le même port série.

Compatibilité des équipements :

- Même type de liaison RS485 2 fils ou 4 fils.
- Tous les équipements doivent pouvoir être configurés avec des caractéristiques de bus identique. Même vitesse, même parité, même nombre de stop bits et de data bits sur tous les équipements et dans la WebdynSunPM.
- Chaque équipement doit se voir attribuer une adresse Modbus unique (entre 1 et 247) sur le bus. (UnitID).

9. Support

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

Webdyn SA

26 Rue des Gaudines

78100 Saint-Germain-en-Laye

Tel.: +33 1 39 04 29 40

Mail : support@webdyn.com

<https://www.webdyn.com>

Munissez-vous des éléments suivants :

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

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

10. Annexes

10.1 Annexe A : Fichier de configuration « `_config.ini` »

Les paramètres de configuration autorisés dans le fichier de configuration « `<uid>_config.ini` » sont les suivants :

Paramètre	Description	Valeur par défaut
<code>BIN_Checksum</code>	Indique le nom du firmware à utiliser pour effectuer une mise à jour du logiciel de la passerelle. Ce paramètre ne peut pas être vide si <code>BIN_FileName</code> contient une valeur. Le firmware ainsi désigné doit se trouver dans le répertoire des binaires configuré. Voir la section sur la configuration des mises à jour pour le mode d'emploi des mises à jour.	
<code>BIN_FileName</code>	Indique le checksum du firmware indiqué dans le champ <code>BIN_FileName</code> . Ce paramètre ne peut pas être vide si <code>BIN_Checksum</code> contient une valeur. Voir la section sur la configuration des mises à jour pour le mode d'emploi des mises à jour.	
<code>Concentrator_Identifier</code>	Identifiant de la passerelle (uid). Si le champ est laissé vide, l'identifiant par défaut est utilisé.	WPMABCDEF (où ABCDEF correspond aux derniers caractères du numéro de série.)
<code>FTP_DirAlarm</code>	Répertoire du serveur FTP/SFTP 1 dans lequel seront stockées les alarmes en provenance du concentrateur. Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.	/ALARM
<code>FTP_DirBin</code>	Répertoire du serveur FTP/SFTP 1 dans lequel le concentrateur recherchera les fichiers de mise à jour lorsque demandé. Voir la section sur la configuration des mises à jour pour le mode d'emploi des mises à jour.	/BIN

FTP_DirCert	<p>Répertoire du serveur FTP/SFTP 1 dans lequel le concentrateur recherchera les certificats à utiliser pour les connexions MQTT.</p> <p>Voir la section sur la configuration du serveur MQTT pour plus de détails.</p>	/CERT
FTP_DirCmd	<p>Répertoire du serveur FTP/SFTP 1 dans lequel le concentrateur recherchera les fichiers de commande qui seront exploités par la suite.</p> <p>Voir la section sur l'utilisation des fichiers de commande pour plus de détails</p>	/CMD
FTP_DirConfig	<p>Répertoire du serveur FTP/SFTP 1 dans lequel le concentrateur dépose ses fichiers de configuration.</p> <p>Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.</p> <p>Le concentrateur relira également les fichiers de configuration pour détecter les mises à jour à télécharger et appliquer.</p> <p>Voir la section consacrée à la configuration du concentrateur par les fichiers de configuration pour le principe de fonctionnement (voir chapitre 3.1.2 : « Fonctionnement du concentrateur »)</p>	/CONFIG
FTP_DirData	<p>Répertoire du serveur FTP/SFTP 1 dans lequel le concentrateur va déposer les fichiers de données récoltées lors de l'exploitation.</p> <p>Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.</p>	/DATA
FTP_DirDef	<p>Répertoire du serveur FTP/SFTP 1 dans lequel le concentrateur va déposer les fichiers de définition créés par lui-même.</p> <p>Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.</p> <p>Le concentrateur relira également les fichiers de configuration pour détecter les mises à jour à télécharger et appliquer.</p> <p>Voir la section consacrée à la configuration des fichiers de définition pour le principe de fonctionnement (voir chapitre 3.1.2.2 : « Définition des équipements connectés »)</p>	/DEF

FTP_DirLog	<p>Répertoire du serveur FTP/SFTP 1 dans lequel le concentrateur va déposer les fichiers de log générés.</p> <p>Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.</p> <p>Voir la section consacrée aux logs pour les différents fichiers disponibles (voir chapitre 4.1.8 : « Les Logs « LOG » »).</p>	/LOG
FTP_DirScript	<p>Répertoire du serveur FTP/SFTP 1 dans lequel le concentrateur va déposer et relire les fichiers de scripts actuellement en cours d'exploitation.</p> <p>Si un fichier est chargé sur le concentrateur, il sera transféré lors de la prochaine connexion sur le serveur.</p> <p>Si un fichier est modifié sur le serveur, il est chargé vers le concentrateur à la prochaine connexion.</p> <p>Si un fichier est rajouté sur le serveur, il est ignoré.</p>	/SCRIPT
FTP_DisconnectDelay	<p>Temps de maintien de la connexion au serveur FTP/SFTP 1.</p> <p>Cette valeur est exprimée en secondes.</p> <p>Une valeur de 0 indique que la connexion est coupée dès la fin des traitements.</p>	0
FTP_EnableAdvancedData	<p>Ajout du nombre de lectures complètes sur cette période d'acquisition dans les fichiers de données déposés sur le serveur FTP/SFTP :</p> <ul style="list-style-type: none"> • 0 : Pas d'ajout du nombre de lectures complètes • 1 : Ajout du nombre de lectures complètes 	0
FTP_EuroDateFormat	<p>Indique le format à utiliser pour l'horodatage des données envoyées au serveur FTP/SFTP 1. Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 0 : le format ISO est utilisé (AA/MM/JJ-HH:MM:SS) • 1 : le format européen est utilisé (JJ/MM/AA-HH:MM:SS) 	0

FTP_HeaderOption	Indique si la passerelle doit rajouter les en-têtes optionnels dans les fichiers de données déposés sur le serveur FTP/SFTP 1. Les valeurs possibles sont : • 0 : pas d'en-tête optionnel • 1 : en-têtes optionnels générés	0
FTP_Login	Le login à utiliser pour se connecter au serveur FTP/SFTP 1. Cette valeur est obligatoire.	
FTP_Password	Le mot de passe associé au login « FTP_Login » pour se connecter au serveur FTP/SFTP 1.	
FTP_Port	Port réseau à utiliser pour se connecter au serveur FTP/SFTP 1	21
FTP_SynchroniseCertificates	(Evolution future)	0
FTP_TwoStepsSendingDisabled	Permet de transférer les fichiers en 2 étapes en passant par un fichier temporaire tant que le fichier n'est pas complet sur le serveur FTP/SFTP 1. Les valeurs possibles sont : • 0 : le fichier temporaire est utilisé • 1 : le fichier temporaire n'est pas utilisé	0
FTP_UploadLog	Indique si la passerelle doit également déposer les journaux de fonctionnement internes aux connexions programmées dans le répertoire de dépôt des logs du serveur FTP/SFTP 1. Les valeurs possibles sont : • 0 : pas de dépôt des fichiers • 1 : dépôt des fichiers	0
FTP_WebServicesEnable	Indique si les web services sont activés sur l'interface FTP. Voir la section dédiée aux web services pour plus d'informations sur l'utilisation de cette fonctionnalité. Les valeurs possibles sont : • 0 : web services désactivés • 1 : web services activés	0

FTP_WebServicesUrl	<p>URL qui sera appelée en réponse à certaines actions FTP si les web services sont activés. Voir la section dédiée aux web services pour plus d'informations sur l'utilisation de cette fonctionnalité. L'URL doit avoir le format suivant :</p> <ul style="list-style-type: none"> • http://adresse/page/ 	
FTP2_DirAlarm	<p>Répertoire du serveur FTP/SFTP 2 dans lequel seront stockées les alarmes en provenance du concentrateur.</p> <p>Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.</p>	/ALARM
FTP2_DirBin	<p>Répertoire du serveur FTP/SFTP 2 dans lequel le concentrateur recherchera les fichiers de mise à jour lorsque demandé.</p> <p>Voir la section sur la configuration des mises à jour pour le mode d'emploi des mises à jour.</p>	/BIN
FTP2_DirCert	<p>Répertoire du serveur FTP/SFTP 2 dans lequel le concentrateur recherchera les certificats à utiliser pour les connexions MQTT.</p> <p>Voir la section sur la configuration du serveur MQTT pour plus de détails.</p>	/CERT
FTP2_DirCmd	<p>Répertoire du serveur FTP 2/SFTP dans lequel le concentrateur recherchera les fichiers de commande qui seront exploités par la suite.</p> <p>Voir la section sur l'utilisation des fichiers de commande pour plus de détails</p>	/CMD
FTP2_DirConfig	<p>Répertoire du serveur FTP/SFTP 2 dans lequel le concentrateur dépose ses fichiers de configuration.</p> <p>Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.</p> <p>Voir la section consacrée à la configuration du concentrateur par les fichiers de configuration pour le principe de fonctionnement (voir chapitre 3.1.2 : « Fonctionnement du concentrateur »)</p>	/CONFIG

FTP2_DirData	Répertoire du serveur FTP/SFTP 2 dans lequel le concentrateur va déposer les fichiers de données récoltées lors de l'exploitation. Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.	/DATA
FTP2_DirDef	Répertoire du serveur FTP/SFTP 2 dans lequel le concentrateur va déposer les fichiers de définition créés par lui-même. Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers. Voir la section consacrée à la configuration des fichiers de définition pour le principe de fonctionnement (voir chapitre « Définition des équipements connectés »)	/DEF
FTP2_DirLog	Répertoire du serveur FTP/SFTP 2 dans lequel le concentrateur va déposer les fichiers de log générés. Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers. Voir la section consacrée aux logs pour les différents fichiers disponibles (voir chapitre 4.1.8 : « Les Logs « LOG » »)	/LOG
FTP2_DirScript	Répertoire du serveur FTP/SFTP 2 dans lequel le concentrateur va déposer et relire les fichiers de scripts en cours d'exploitation. Si un fichier est chargé sur le concentrateur, il sera transféré lors de la prochaine connexion sur le serveur. Si un fichier est modifié sur le serveur, il est chargé vers le concentrateur à la prochaine connexion. Si un fichier est rajouté sur le serveur, il est ignoré.	/SCRIPT
FTP2_EuroDateFormat	Indique le format à utiliser pour l'horodatage des données envoyées au serveur FTP/SFTP 2. Les valeurs possibles sont : <ul style="list-style-type: none"> • 0 : le format ISO est utilisé (AA/MM/JJ-HH:MM:SS) • 1 : le format européen est utilisé (JJ/MM/AA-HH:MM:SS) 	0

FTP2_HeaderOption	Indique si la passerelle doit rajouter les en-têtes optionnels dans les fichiers de données déposés sur le serveur FTP/SFTP 2. Les valeurs possibles sont : • 0 : pas d'en-tête optionnel • 1 : en-têtes optionnels générés	0
FTP2_EnableAdvancedData	Ajout du nombre de lectures complètes sur cette période d'acquisition dans les fichiers de données déposés sur le serveur FTP/SFTP 2 : • 0 : Pas d'ajout du nombre de lectures complètes • 1 : ajout du nombre de lectures complètes	0
FTP2_Login	Le login à utiliser pour se connecter au serveur FTP/SFTP 2. Cette valeur est obligatoire.	
FTP2_Password	Le mot de passe associé au login « FTP2_Login » pour se connecter au serveur FTP/SFTP 2.	
FTP2_Port	Port réseau à utiliser pour se connecter au serveur FTP/SFTP 2	21
FTP2_SynchroniseCertificates	(Evolution future)	0
FTP2_TwoStepsSendingDisabled	Permet de transférer les fichiers en 2 étapes en passant par un fichier temporaire tant que le fichier n'est pas complet sur le serveur FTP/SFTP 2. Les valeurs possibles sont : • 0 : le fichier temporaire est utilisé • 1 : le fichier temporaire n'est pas utilisé	0
FTP2_UploadLog	Indique si la passerelle doit également déposer les journaux de fonctionnement internes aux connexions programmées dans le répertoire de dépôt des logs du serveur FTP/SFTP 2. Les valeurs possibles sont : • 0 : pas de dépôt des fichiers • 1 : dépôt des fichiers	0

FTP2_WebServicesEnable	Indique si les web services sont activés sur l'interface FTP 2. Voir la section dédiée aux web services pour plus d'informations sur l'utilisation de cette fonctionnalité. Les valeurs possibles sont : <ul style="list-style-type: none"> • 0 : web services désactivés • 1 : web services activés 	0
FTP2_WebServicesUrl	URL qui sera appelée en réponse à certaines actions FTP 2 si les web services sont activés. Voir la section dédiée aux web services pour plus d'informations sur l'utilisation de cette fonctionnalité. L'URL doit avoir le format suivant : <ul style="list-style-type: none"> • http://adresse/page/ 	
MQTT2_AlarmTopic	Nom du topic alarme que l'on souhaite publier. Si le champ est vide, aucune alarme ne sera publiée vers le broker. Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTT. Fonctionnel pour tous les types MQTT sauf le « mqttps_azure »	
MQTT2_CaCertFile	Nom du certificat qui permet d'authentifier le serveur MQTTS renseigné. Le certificat est à récupérer sur votre serveur MQTT et doit être importé sur le concentrateur par FTP ou par l'interface web. Fonctionnel pour tous les types MQTT sauf le « mqtt »	
MQTT2_CertFile	Nom du certificat spécifique au concentrateur utilisé pour la connexion. Le certificat est à récupérer sur votre serveur MQTT et doit être importé sur le concentrateur par FTP ou par l'interface web. Fonctionnel pour tous les types MQTT sauf le « mqtt » et le « mqttps_gcloud »	

MQTT2_CloudDevice	<p>Identifiant unique personnalisable de l'équipement dans un registre défini sur le serveur MQTT.</p> <p>Ce paramètre est à récupérer sur votre serveur MQTT et correspond à :</p> <ul style="list-style-type: none"> • « deviceId » sur Google IoT Cloud. • « device_id » sur Azure IoT Hub. <p>Fonctionnel uniquement pour les types « mqttp_gcloud » et « mqttp_azure »</p>
MQTT2_CloudProjectId	<p>Identifiant unique personnalisable du projet défini sur le serveur MQTT.</p> <p>Ce paramètre est à récupérer sur votre serveur MQTT et correspond à :</p> <ul style="list-style-type: none"> • « projectId » sur Google IoT Cloud. • Le nom du « IoT Hub » sur Azure IoT Hub. <p>Fonctionnel uniquement pour les types « mqttp_gcloud » et « mqttp_azure »</p>
MQTT2_CloudRegion	<p>Région du serveur MQTT du registre des équipements.</p> <p>Ce paramètre est à récupérer sur votre serveur MQTT et correspond à :</p> <ul style="list-style-type: none"> • « deviceRegistryLocation » sur Google IoT Cloud. <p>Par exemple : « europe-west1 »</p> <p>Fonctionnel uniquement pour le type « mqttp_gcloud »</p>
MQTT2_CloudRegistry	<p>Nom du registre personnalisable définie sur le serveur MQTT.</p> <p>Ce paramètre est à récupérer sur votre serveur MQTT et correspond à :</p> <ul style="list-style-type: none"> • « deviceRegistryId » sur Google IoT Cloud. <p>Fonctionnel uniquement pour le type « mqttp_gcloud »</p>

MQTT2_CloudSigningAlgo	<p>Type de clé utilisé pour vérifier la signature du certificat du serveur MQTT. Ce paramètre est à récupérer sur votre serveur Google IoT Cloud. Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • « RS256 » pour la clé RSA • « ES256 » pour la clé de courbe elliptique <p>Fonctionnel uniquement pour le type « mqttp_gcloud »</p>	
MQTT2_ClientId	<p>Identifiant personnalisable de l'équipement sur le serveur MQTT. Ce paramètre est à récupérer sur votre serveur MQTT. Fonctionnel uniquement pour les types « mqtt » et « mqttps »</p>	
MQTT2_ControlTopic	<p>Nom du topic pour les commandes à récupérer par le concentrateur. Le paramètre MQTT2_ResultTopic doit être renseigné pour l'utilisation des commandes. Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTT. Fonctionnel pour tous les types MQTT sauf le « mqttps_azure »</p>	
MQTT2_EnableAdvancedData	<p>Publication du nombre de lectures complètes sur cette période d'acquisition dans le topic de données. Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 0 : Désactivé • 1 : Activé 	0
MQTT2_EnableAlarmPost	<p>Activer la publication des alarmes sur le topic dédié. Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 0 : La publication des alarmes est désactivée • 1 : La publication des alarmes est activée et le concentrateur reste en mode de connexion permanente avec le serveur MQTT. <p>Fonctionnel uniquement pour le type « mqttps_azure »</p>	

MQTT2_EnableInvokeMethod	<p>Activer l'appel des méthodes. Permet d'utiliser les topics dédiés.</p> <p>Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 0 : Appel des méthodes désactivé • 1 : Appel des méthodes activé et le concentrateur reste en mode de connexion permanente avec le serveur MQTT. <p>Fonctionnel uniquement pour le type « mqttps_azure »</p>	
MQTT2_Insecure	<p>Désactiver de la vérification du nom d'hôte spécifié dans les certificats.</p> <p>Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 0 : Vérification activée • 1 : Vérification désactivée. <p>Fonctionnel uniquement pour le type « mqttps »</p>	
MQTT2_KeepAlive	<p>Si aucun échange effectué avec le serveur MQTT pendant le temps défini en seconde, le concentrateur envoie un ping au serveur MQTT afin de vérifier la connexion à celui-ci.</p> <p>Si la valeur est à « 0 », le KeepAlive est désactivé.</p> <p>Si le concentrateur est en mode de connexion permanente avec le serveur MQTT et qu'une déconnexion est détectée après un KeepAlive, le concentrateur se reconnectera automatiquement au serveur MQTT.</p>	10
MQTT2_KeyFile	<p>Nom du fichier comprenant la clé privée spécifique au concentrateur utilisé pour la connexion. Le fichier est à récupérer sur votre serveur MQTT et doit être importé sur le concentrateur par FTP ou par l'interface web.</p> <p>Fonctionnel pour tous les types MQTT sauf le « mqtt »</p>	
MQTT2_Login	<p>Nom d'utilisateur pour accéder au serveur MQTT.</p> <p>Fonctionnel uniquement pour les types « mqtt » et « mqttps »</p>	
MQTT2_Password	<p>Mot de passe pour accéder au serveur MQTT.</p> <p>Fonctionnel uniquement pour les types « mqtt » et « mqttps »</p>	

MQTT2_Port	Port du serveur MQTT. Pour un serveur MQTT, le port par défaut est le 1883. Pour un serveur sécurisé MQTTS, le port par défaut est le 8883.	8883
MQTT2_QoS	Numéro du service garanti pour l'envoi des messages (Quality Of Service). Les valeurs possibles sont : <ul style="list-style-type: none"> • 0 : Le message sera envoyé qu'une fois, c'est-à-dire avec aucune garantie de réception. • 1 : Le message sera envoyé au moins une fois, c'est-à-dire le concentrateur transmettra plusieurs fois s'il le faut jusqu'à ce que le broker lui confirme qu'il a été transmis. • 2 : Le message sera obligatoirement sauvegardé par le concentrateur et le transmettra toujours tant que le broker ne confirme pas son envoi. (évite duplication des messages) <p>Pour les types « mqtts_gcloud », « mqtts_azure » et « mqtts_aws », le QoS 2 n'est pas pris en charge.</p>	1
MQTT2_ResultTopic	Nom du topic pour les résultats des commandes passées au concentrateur. Le paramètre MQTT2_ControlTopic doit être renseigné pour l'utilisation des commandes. Si un nom de topic est renseigné, le concentrateur reste en mode de connexion permanente avec le serveur MQTT. Fonctionnel pour tous les types MQTT sauf le « mqtts_azure »	
MQTT2_Timeout	Délai d'attente maximum en seconde de la réponse du serveur MQTT. Si le serveur n'a pas répondu pendant le temps imparti, l'envoi est arrêté et ressayé lors de la prochaine planification. Fonctionnel uniquement en QoS 1 ou QoS 2.	30
MQTT2_TlsVersion	Version TLS pris en charge par le serveur MQTT. Les valeurs possibles sont : <ul style="list-style-type: none"> • tlsv1.1 : TLS en V1.1 • tlsv1.2 : TLS en V1.2 <p>Fonctionnel uniquement pour le type « mqtts »</p>	tlsv1.2

MQTT2_Topic	Nom du topic pour les données déposées par le concentrateur. Fonctionnel pour tous les types MQTT sauf le « mqttps_azure »	
HTTP_DirAlarm	Répertoire du serveur WebDAV-HTTPS 1 dans lequel seront stockées les alarmes en provenance du concentrateur. Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.	/ALARM
HTTP_DirBin	Répertoire du serveur WebDAV-HTTPS 1 dans lequel le concentrateur recherchera les fichiers de mise à jour lorsque demandé. Voir la section sur la configuration des mises à jour pour le mode d'emploi des mises à jour. (3.1.2.1)	/BIN
HTTP_DirCert	Répertoire du serveur WebDAV-HTTPS 1 dans lequel le concentrateur recherchera les certificats à utiliser pour les connexions MQTT. Voir la section sur la configuration du serveur WebDAV pour plus de détails.	/CERT
HTTP_DirCmd	Répertoire du serveur WebDAV-HTTPS 1 dans lequel le concentrateur recherchera les fichiers de commande qui seront exploités par la suite. Voir la section sur l'utilisation des fichiers de commande pour plus de détails	/CMD
HTTP_DirConfig	Répertoire du serveur WebDAV-HTTPS 1 dans lequel le concentrateur dépose ses fichiers de configuration. Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers. Le concentrateur relira également les fichiers de configuration pour détecter les mises à jour à télécharger et appliquer. Voir la section consacrée à la configuration du concentrateur par les fichiers de configuration pour le principe de fonctionnement (voir chapitre 3.1.2 : « Fonctionnement du concentrateur »)	/CONFIG

HTTP_DirData	Répertoire du serveur WebDAV-HTTPS 1 dans lequel le concentrateur va déposer les fichiers de données récoltées lors de l'exploitation. Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.	/DATA
HTTP_DirDef	Répertoire du serveur WebDAV-HTTPS 1 dans lequel le concentrateur va déposer les fichiers de définition créés par lui-même. Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers. Le concentrateur relira également les fichiers de configuration pour détecter les mises à jour à télécharger et appliquer. Voir la section consacrée à la configuration des fichiers de définition pour le principe de fonctionnement (voir chapitre 3.1.2.2 : « Définition des équipements connectés »)	/DEF
HTTP_DirLog	Répertoire du serveur WebDAV-HTTPS 1 dans lequel le concentrateur va déposer les fichiers de log générés. Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers. Voir la section consacrée aux logs pour les différents fichiers disponibles (voir chapitre 4.1.8 : « Les Logs « LOG » »)	/LOG
HTTP_DirScript	Répertoire du serveur WebDAV-HTTPS 1 dans lequel le concentrateur va déposer et relire les fichiers de scripts actuellement en cours d'exploitation. Si un fichier est chargé sur le concentrateur, il sera transféré lors de la prochaine connexion sur le serveur. Si un fichier est modifié sur le serveur, il est chargé vers le concentrateur à la prochaine connexion. Si un fichier est rajouté sur le serveur, il est ignoré.	/SCRIPT

FTP_DisconnectDelay	Temps de maintien de la connexion au serveur FTP 1. Cette valeur est exprimée en secondes. Une valeur de 0 indique que la connexion est coupée dès la fin des traitements.	0
HTTP_EuroDateFormat	Indique le format à utiliser pour l'horodatage des données envoyées au serveur WebDAV-HTTPS 1. Les valeurs possibles sont : • 0 : le format ISO est utilisé (AA/MM/JJ-HH:MM:SS) • 1 : le format européen est utilisé (JJ/MM/AA-HH:MM:SS)	0
HTTP_HeaderOption	Indique si la passerelle doit rajouter les en-têtes optionnels dans les fichiers de données déposés sur le serveur WebDAV-HTTPS 1 Les valeurs possibles sont : • 0 : pas d'en-tête optionnel • 1 : en-têtes optionnels générés	0
HTTP_Login	Le login à utiliser pour se connecter au serveur WebDAV-HTTPS 1. Cette valeur est obligatoire.	
HTTP_Password	Le mot de passe associé au login « HTTP_Login » pour se connecter au serveur WebDAV-HTTPS 1.	
HTTP_Port	Port réseau à utiliser pour se connecter au serveur WebDAV-HTTPS 1	443
HTTP_SynchroniseCertificates	(Evolution future)	0
HTTP_UploadLog	Indique si la passerelle doit également déposer les journaux de fonctionnement internes aux connexions programmées dans le répertoire de dépôt des logs du serveur WebDAV-HTTPS 1. Les valeurs possibles sont : • 0 : pas de dépôt des fichiers • 1 : dépôt des fichiers	0

HTTP2_DirAlarm	Répertoire du serveur WebDAV-HTTPS 2 dans lequel seront stockées les alarmes en provenance du concentrateur. Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.	/ALARM
HTTP2_DirBin	Répertoire du serveur WebDAV-HTTPS 2 dans lequel le concentrateur recherchera les fichiers de mise à jour lorsque demandé. Voir la section sur la configuration des mises à jour pour le mode d'emploi des mises à jour. (3.1.2.1)	/BIN
HTTP2_DirCert	Répertoire du serveur WebDAV-HTTPS 2 dans lequel le concentrateur recherchera les certificats à utiliser pour les connexions MQTT. Voir la section sur la configuration du serveur WebDAV pour plus de détails.	/CERT
HTTP2_DirCmd	Répertoire du serveur WebDAV-HTTPS 2 dans lequel le concentrateur recherchera les fichiers de commande qui seront exploités par la suite. Voir la section sur l'utilisation des fichiers de commande pour plus de détails	/CMD
HTTP2_DirConfig	Répertoire du serveur WebDAV-HTTPS 2 dans lequel le concentrateur dépose ses fichiers de configuration. Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers. Voir la section consacrée à la configuration du concentrateur par les fichiers de configuration pour le principe de fonctionnement (voir chapitre 3.1.2 : « Fonctionnement du concentrateur »)	/CONFIG
HTTP2_DirData	Répertoire du serveur WebDAV-HTTPS 2 dans lequel le concentrateur va déposer les fichiers de données récoltées lors de l'exploitation. Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.	/DATA

HTTP2_DirDef	<p>Répertoire du serveur WebDAV-HTTPS 2 dans lequel le concentrateur va déposer les fichiers de définition créés par lui-même.</p> <p>Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.</p> <p>Voir la section consacrée à la configuration des fichiers de définition pour le principe de fonctionnement (voir chapitre 3.1.2.2 : « Définition des équipements connectés »)</p>	/DEF
HTTP2_DirLog	<p>Répertoire du serveur WebDAV-HTTPS 2 dans lequel le concentrateur va déposer les fichiers de log générés.</p> <p>Il est à noter que le répertoire DOIT exister. Il ne sera pas créé par le concentrateur lors des dépôts de fichiers.</p> <p>Voir la section consacrée aux logs pour les différents fichiers disponibles (voir chapitre 4.1.8 : « Les Logs « LOG » »)</p>	/LOG
HTTP2_DirScript	<p>Répertoire du serveur WebDAV-HTTPS 2 dans lequel le concentrateur va déposer et relire les fichiers de scripts en cours d'exploitation</p> <p>Si un fichier est chargé sur le concentrateur, il sera transféré lors de la prochaine connexion sur le serveur.</p> <p>Si un fichier est modifié sur le serveur, il est chargé vers le concentrateur à la prochaine connexion.</p> <p>Si un fichier est rajouté sur le serveur, il est ignoré.</p>	/SCRIPT
HTTP2_EuroDateFormat	<p>Indique le format à utiliser pour l'horodatage des données envoyées au serveur WebDAV-HTTPS 2.</p> <p>Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 0 : le format ISO est utilisé (AA/MM/JJ-HH:MM:SS) • 1 : le format européen est utilisé (JJ/MM/AA-HH:MM:SS) 	0
HTTP2_HeaderOption	<p>Indique si la passerelle doit rajouter les en-têtes optionnels dans les fichiers de données déposés sur le serveur WebDAV-HTTPS 2</p> <p>Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • 0 : pas d'en-tête optionnel • 1 : en-têtes optionnels générés 	0

HTTP2_Login	Le login à utiliser pour se connecter au serveur WebDAV-HTTPS 2. Cette valeur est obligatoire.	
HTTP2_Password	Le mot de passe associé au login configuré au paramètre « HTTP2_Login » pour se connecter au serveur WebDAV-HTTPS 2.	
HTTP2_Port	Port réseau à utiliser pour se connecter au serveur WebDAV-HTTPS 2	443
HTTP2_SynchroniseCertificates	(Evolution future)	0
HTTP2_UploadLog	Indique si la passerelle doit également déposer les journaux de fonctionnement internes aux connexions programmées dans le répertoire de dépôt des logs du serveur WebDAV-HTTPS 2. Les valeurs possibles sont : • 0 : pas de dépôt des fichiers • 1 : dépôt des fichiers	0
LOG_Level	Niveau de log du concentrateur reporté dans les fichiers système. Utilisé pour le mode debug du boîtier. Ce paramètre impacte le niveau de détails du fichier de log système (voir chapitre 4.1.8.4 « Les logs système ») Les valeurs seront communiqués par le support Webdyn en cas de besoin.	3
NTP_Server1	1er serveur à interroger pour régler la date/heure. (valeur usine : pool.ntp.org)	
NTP_Server2	2ème serveur à interroger pour régler la date/heure. Ce serveur est utilisé si le 1er serveur ne répond pas.	
NTP_TimeZone	Zone horaire à appliquer. Cette valeur est utilisée conjointement avec les données d'heure remontées par les serveurs NTP configurés. Voir l'annexe « Annexe B : Liste des zones horaires » pour la liste des valeurs autorisées	UTC

SERVER_Address	<p>Adresse du serveur distant à utiliser pour la connexion Server 1.</p> <p>Cette adresse peut être un nom si les DNS sont correctement configurés ou une adresse IP.</p> <p>Cette valeur est obligatoire.</p>	
SERVER_Interface	<p>Interface réseau à utiliser pour accéder au serveur distant pour la connexion Server 1. Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • ethernet : utilise la connexion Ethernet • modem : utilise l'interface 2G/3G/4G avec la carte SIM embarquée • sdcard : utilise la carte microSD insérée dans le concentrateur <p>Ce paramètre ne peut pas être laissé vide</p>	ethernet
SERVER_Type	<p>Type de serveur sur lequel le concentrateur va devoir se connecter pour la connexion Server 1. Il existe plusieurs sortes de serveurs différents. Il est donc important de sélectionner le type de serveur correct. Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • ftp : serveur FTP • sftp : serveur SFTP • webdav : serveur WebDAV-HTTPS <p>Ce paramètre ne peut pas être laissé vide</p>	ftp
SERVER2_Address	<p>Adresse du serveur distant à utiliser pour la connexion Server 2.</p> <p>Cette adresse peut être un nom si les DNS sont correctement configurés ou une adresse IP.</p> <p>Cette valeur est obligatoire.</p>	
SERVER2_Interface	<p>Interface réseau à utiliser pour accéder au serveur distant pour la connexion server 2. Les valeurs possibles sont :</p> <ul style="list-style-type: none"> • ethernet : utilise la connexion Ethernet • modem : utilise l'interface 2G/3G/4G avec la carte SIM embarquée • sdcard : utilise la carte microSD insérée dans le concentrateur <p>Ce paramètre ne peut pas être laissé vide</p>	modem

SERVER2_Type	Type de serveur sur lequel le concentrateur va devoir se connecter pour la connexion Server 2. Il existe plusieurs sortes de serveurs différents. Il est donc important de sélectionner le type de serveur correct. Les valeurs possibles sont : <ul style="list-style-type: none"> • ftp : serveur FTP • sftp : serveur SFTP • webdav : serveur WebDAV-HTTPS • mqtt : serveur MQTT • mqttps : serveur MQTT sécurisé • mqttps_aws : serveur MQTTS sur « AWS IoT » • mqttps_azure : serveur MQTTS sur « Azure IoT » • mqttps_gcloud : serveur MQTTS sur « Google Cloud IoT » <p>Ce paramètre ne peut pas être laissé vide</p>	ftp
WEB_Password	Mot de passe pour accéder à la configuration par le site web du concentrateur.	high

Sauf indication contraire, les paramètres peuvent être omis dans le fichier de configuration. La valeur par défaut sera alors utilisée par le concentrateur comme indiqué lors de l'import du fichier.

Lorsque le concentrateur écrit le fichier et le renvoie vers le serveur, tous les paramètres sont remis en place.

10.2 Annexe B : Liste des zones horaires

La liste des valeurs autorisées pour le paramètre « NTP_TimeZone » est la suivante :

- (GMT-11:00) Midway Island, Samoa
- (GMT-10:00) Honolulu
- (GMT-10:00) Tahiti
- (GMT-09:30) Marquesas
- (GMT-09:00) Anchorage
- (GMT-08:00) Pacific Time (US and Canada)
- (GMT-08:00) Los angeles
- (GMT-07:00) Denver
- (GMT-07:00) Chihuahua, La Paz, Mazatlan
- (GMT-06:00) Guadalajara, Mexico City, Monterrey
- (GMT-06:00) Chicago, Central America
- (GMT-05:00) Bogota, Lima, Quito
- (GMT-05:00) New York
- (GMT-04:00) Atlantic Time (Canada)
- (GMT-04:00) Caracas
- (GMT-04:00) Martinique
- (GMT-04:00) Guadeloupe
- (GMT-03:30) Newfoundland, St Johns
- (GMT-03:00) Antarctica
- (GMT-03:00) Sao Paulo
- (GMT-02:00) Brazil
- (GMT-01:00) Azores
- UTC
- (GMT+01:00) Europe: Brussels, Copenhagen, Madrid, Paris
- (GMT+01:00) Algiers
- (GMT+02:00) Athens, Bucharest, Istanbul
- (GMT+02:00) Cairo
- (GMT+03:00) Moscow, St. Petersburg, Volgograd
- (GMT+03:00) Kuwait, Riyadh
- (GMT+04:00) Abu Dhabi, Dubai, Muscat

(GMT+04:00) Baku, Tbilisi, Yerevan
(GMT+04:30) Kabul
(GMT+05:00) Karachi
(GMT+05:00) Tashkent
(GMT+05:30) Kolkata
(GMT+05:45) Katmandu
(GMT+06:00) Astana, Dhaka
(GMT+06:00) Almaty, Novosibirsk
(GMT+06:30) Rangoon, Yangon
(GMT+06:30) Cocos
(GMT+07:00) Bangkok, Hanoi, Jakarta
(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Shanghai
(GMT+08:00) Taipei
(GMT+09:00) Osaka, Sapporo, Tokyo
(GMT+09:00) Seoul
(GMT+09:30) Darwin
(GMT+10:00) Brisbane, Sydney
(GMT+10:00) Guam, Port Moresby
(GMT+10:30) Adelaide
(GMT+11:00) Noumea
(GMT+11:00) Magadan, Solomon Islands
(GMT+13:00) Auckland, Wellington

10.3 Annexe C : Onduleurs compatibles

La WebdynSunPM est compatible avec tous les onduleurs MODBUS et MODBUS SUNSPEC ainsi que les onduleurs compatibles avec les protocoles propriétaires suivants :

- DELTA
- KACO
- SMANET
- SOLARMAX

Elle permet également la détection automatique des onduleurs suivants :

10.3.1 ABB

- PVI-10.0-TL-OUTD
- PVI-12.5-TL-OUTD
- TRIO-20.0-TL-OUTD
- TRIO-27.6-TL-OUTD
- ULTRA 700.0-TL
- ULTRA 750-TL-OUTD-X-US-690
- ULTRA 1050.0-TL
- ULTRA 1100-TL-OUTD-X-US-690
- ULTRA 1400.0-TL
- ULTRA 1500-TL-OUTD-X-US-690

10.3.2 CEFEM

Série TRIO-TOP :

- 9 TR RO (HF)
- 10K TR (HF)
- 12K TR (HF)
- 15K TR (HF)
- 18K TR (HF)

Série TRIO-SUN :

- 18 kVA
- 20 kVA
- 25 kVA

- 30 kVA
- 33 kVA
- 36 kVA

10.3.3 Fronius

Série IG :

- IG 15
- IG 20
- IG 30
- IG 40
- IG 60
- IG 60 HV
- IG 300
- IG 400
- IG 500
- IG 2000
- IG 3000
- IG 4000
- IG 5100

Série IG LV :

- IG 2500-LV
- IG 4500-LV

Série IG TL :

- IG-TL 3.0
- IG-TL 3.6
- IG-TL 4.0
- IG-TL 5.0

Série IG PLUS :

- IG Plus 35-1
- IG Plus 35V-1
- IG Plus 50-1
- IG Plus 50V-1

- IG Plus 70-1
- IG Plus 70-2
- IG Plus 70V-1
- IG Plus 70V-2
- IG Plus 100-1
- IG Plus 100-2
- IG Plus 100V-1
- IG Plus 100V-2
- IG Plus 120-3
- IG Plus 120V-3
- IG Plus 150-3
- IG Plus 150V-3
- IG Plus 3.0-1 UNI
- IG Plus 3.8-1 UNI
- IG Plus 5.0-1 UNI
- IG Plus 6.0-1 UNI
- IG Plus 7.5-1 UNI
- IG Plus 10.0-1 UNI
- IG Plus 11.4-1 UNI
- IG Plus 11.4-3-Delta
- IG Plus 12.0-3 WYE277

Série CL :

- CL 36.0
- CL 48.0
- CL 60.0
- CL 36.0 WYE277
- CL 48.0 WYE277
- CL 60.0 WYE277
- CL 33.3 Delta
- CL 44.4 Delta
- CL 55.5 Delta

Série GALVO :

- GALVO 1.5-1
- GALVO 2.0-1
- GALVO 2.5-1
- GALVO 3.0-1
- GALVO 3.1-1

Série SYMO :

- SYMO 3.0-3-S
- SYMO 3.7-3-S
- SYMO 4.5-3-S
- SYMO 3.0-3-M
- SYMO 3.7-3-M
- SYMO 4.5-3-M
- SYMO 5.0-3-M
- SYMO 6.0-3-M
- SYMO 7.0-3-M
- SYMO 8.2-3-M
- SYMO 10.0-3-M
- SYMO 12.5-3-M
- SYMO 15.0-3-M
- SYMO 17.5-3-M
- SYMO 20.0-3-M

Série PRIMO :

- PRIMO 3.0-1
- PRIMO 3.5-1
- PRIMO 3.6-1
- PRIMO 4.0-1
- PRIMO 4.6-1
- PRIMO 5.0-1
- PRIMO 6.0-1
- PRIMO 8.2-1

Série PRIMO GEN24 :

- PRIMO GEN24 3.0 PLUS
- PRIMO GEN24 3.6 PLUS
- PRIMO GEN24 4.0 PLUS
- PRIMO GEN24 4.6 PLUS
- PRIMO GEN24 5.0 PLUS
- PRIMO GEN24 6.0 PLUS

Série TAURO :

- TAURO 50-3-D
- TAURO 50-3-P

Série TAURO ECO :

- TAURO ECO 50-3-D
- TAURO ECO 99-3-D
- TAURO ECO 100-3-D
- TAURO ECO 50-3-P
- TAURO ECO 99-3-P
- TAURO ECO 100-3-P

Série ECO :

- FRONIUS ECO 25.0-3-S
- FRONIUS ECO 27.0-3-S

10.3.4 GOODWE

Série ES :

- GW3648D-ES
- GW5048D-ES

Série ES G2 :

- GW3000-ES-20
- GW3600-ES-20
- GW3600M-ES-20
- GW5000-ES-20
- GW5000M-ES-20
- GW6000-ES-20
- GW6000M-ES-20

Série ESA :

- GW5048-ESA

Série EM :

- GW3048-EM
- GW3648-EM
- GW5048-EM

Série BP :

- GW2500-BP
- GW3600S-BP
- GW5000S-BP

Série SBP G2 :

- GW3600-SBP-20
- GW5000-SBP-20
- GW6000-SBP-20

Série ET :

- GW5KL-ET
- GW6KL-ET
- GW8KL-ET
- GW10KL-ET
- GW5K-ET
- GW6.5K-ET
- GW8K-ET
- GW10K-ET
- GW15K-ET
- GW20K-ET
- GW25K-ET
- GW29.9K-ET
- GW30K-ET
- GW5KN-ET
- GW6.5KN-ET
- GW8KN-ET
- GW10KN-ET

- GW50K-ETC

Série BT :

- GW5K-BT
- GW6K-BT
- GW8K-BT
- GW10K-BT
- GW50K-BTC

Série EH :

- GW3600-EH
- GW5000-EH
- GW6000-EH

Série EH+ :

- GW3600N-EH
- GW5000N-EH
- GW6000N-EH

Série BH :

- GW3K-BH
- GW3600-BH
- GW5000-BH
- GW6000-BH

Série XS :

- GW700-XS
- GW1000-XS
- GW1500-XS
- GW2000-XS
- GW2500-XS
- GW3000-XS
- GW2500N-XS
- GW3000N-XS

Série XS+ :

- GW700-XS-11
- GW1000-XS-11

- GW1500-XS-11
- GW2000-XS-11
- GW2500-XS-11
- GW3000-XS-11

Série DNS :

- GW2900D-NS
- GW3000D-NS
- GW3600D-NS
- GW4200D-NS
- GW5000D-NS
- GW6000D-NS
- GW3000T-DS
- GW3600T-DS
- GW4200T-DS
- GW5000T-DS
- GW6000T-DS

Série DNS G3 :

- GW3000-DNS-30
- GW3600-DNS-30
- GW4200-DNS-30
- GW5000-DNS-30
- GW6000-DNS-30

Série SDT-G2 :

- GW17KT-DT
- GW20KT-DT
- GW25KT-DT
- GW4K-DT
- GW5K-DT
- GW6K-DT
- GW8K-DT
- GW10KT-DT
- GW12KT-DT

- GW15KT-DT
- GW17KT-DT
- GW20KT-DT
- GW25KT-DT

Série SDT-G2+ :

- GW4000-SDT-20
- GW5000-SDT-20
- GW6000-SDT-20
- GW8000-SDT-20
- GW10K-SDT-20
- GW12K-SDT-20
- GW12KLV-SDT-20
- GW15K-SDT-20
- GW17K-SDT-20
- GW20K-SDT-20

Série SDT/LV SDT :

- GW12KN-DT
- GW15KN-DT
- GW17KN-DT
- GW20KN-DT
- GW12KLN-DT

Série SMT :

- GW25K
- GW29.9K-MT
- GW30K-MT
- GW36K-MT
- GW50KS-MT
- GW60KS-MT

Série LV SMT :

- GW12KLV-MT
- GW15KLV-MT
- GW20KLV-MT

- GW30KLS-MT
- GW35KLS-MT

Série MT :

- GW50KN-MT
- GW60KN-MT
- GW50KBF-MT
- GW60KBF-MT
- GW75KBF-MT
- GW80KBF-MT
- GW70KHV-MT
- GW80KHV-MT
- GW75K-MT
- GW80K-MT

Série LV-MT :

- GW30KLV-MT
- GW35KLV-MT
- GW50KLV-MT

Série HT :

- GW73KLV-HT
- GW75K-HT
- GW80K-HT
- GW100K-HT
- GW110K-HT
- GW120K-HT
- GW136K-HTH
- GW225K-HT
- GW250K-HT
- GW225KN-HT
- GW250KN-HT

Série MS :

- GW5000-MS
- GW6000-MS

- GW7000-MS
- GW8500-MS
- GW9000-MS
- GW10K-MS

10.3.5 GROWATT

Série MAC :

- MAC 15KTL3-XL
- MAC 20KTL3-XL
- MAC 22KTL3-XL
- MAC 25KTL3-XL
- MAC 30KTL3-XL
- MAC 36KTL3-XL
- MAC 30KTL3-X-LV
- MAC 40KTL3-X-LV
- MAC 50KTL3-X-LV
- MAC 60KTL3-X-LV
- MAC 50KTL3-X-MV
- MAC 60KTL3-X-MV
- MAC 70KTL3-X-MV

Série MAX :

- MAX 50KTL3-LV
- MAX 60KTL3-LV
- MAX 70KTL3-LV
- MAX 80KTL3-LV
- MAX 100KTL3-X-LV
- MAX 110KTL3-X-LV
- MAX 120KTL3-X-LV
- MAX 125KTL3-X-LV
- MAX 185KTL3-X-HV
- MAX 216KTL3-X-HV
- MAX 250KTL3-X-HV

- MAX 253KTL3-X-HV

Série MIC :

- MIC-750TL-X
- MIC-1000TL-X
- MIC-1500TL-X
- MIC-2000TL-X
- MIC-2500TL-X
- MIC-3000TL-X
- MIC-3300TL-X

Série MID :

- MID-15KTL3-X
- MID-17KTL3-X
- MID-20KTL3-X
- MID-22KTL3-X
- MID-25KTL3-X
- MID-25KTL3-X1
- MID-30KTL3-X
- MID-33KTL3-X
- MID-36KTL3-X
- MID-40KTL3-X

Série MIN :

- MIN 2500TL-X
- MIN 3000TL-X
- MIN 3600TL-X
- MIN 4200TL-X
- MIN 4600TL-X
- MIN 5000TL-X
- MIN 6000TL-X

Série S :

- 750-S
- 1000-S
- 1500-S

- 2000-S
- 3000-S

Série SPA TL-BL :

- SPA 1000TL-BL
- SPA 2000TL-BL
- SPA 3000TL-BL

Série SPA TL3-BH :

- SPA 4000TL3-BH
- SPA 5000TL3-BH
- SPA 6000TL3-BH
- SPA 7000TL3-BH
- SPA 8000TL3-BH
- SPA 10000TL3-BH

Série SPH TL3 BH-UP :

- SPH 4000TL3 BH-UP
- SPH 5000TL3 BH-UP
- SPH 6000TL3 BH-UP
- SPH7000TL3 BH-UP
- SPH8000TL3 BH-UP
- SPH10000TL3 BH-UP

Série SPH :

- SPH3000
- SPH3600
- SPH4000
- SPH4600
- SPH5000
- SPH6000

Série TL3-S :

- 3000TL3-S
- 4000TL3-S
- 5000TL3-S
- 6000TL3-S

- 7000TL3-S
- 8000TL3-S
- 9000TL3-S
- 10000TL3-S
- 11000TL3-S
- 12000TL3-S
- 13000TL3-S
- 15000TL3-S
- 17000TL3-S
- 20000TL3-S
- 25000TL3-S
- 30000TL3-S
- 33000TL3-S
- 50000TL3-S

Série TL3-NS :

- 40000TL3-NS

Série MLT-S :

- 2500MTL-S
- 3000MTL-S
- 3600MTL-S
- 4200MTL-S
- 5000MTL-S
- 5500MTL-S

Série MTLP-S :

- 8000MTLP-S
- 9000MTLP-S
- 10500MTLP-S

Série UE :

- 4000UE
- 5000UE
- 6000UE
- 7000UE

- 8000UE
- 9000UE
- 10000UE
- 12000UE
- 18000UE
- 20000UE

10.3.6 Huawei

- SUN2000-100KTL-H0
- SUN2000-100KTL-H1
- SUN2000-100KTL-H2
- SUN2000-100KTL-INM0
- SUN2000-100KTL-M0
- SUN2000-100KTL-M1
- SUN2000-100KTL-USH0
- SUN2000-105KTL-H1
- SUN2000-10KTL
- SUN2000-10KTL-M0
- SUN2000-10KTL-M1
- SUN2000-10KTL-M2
- SUN2000-10KTL-USL0
- SUN2000-11.4KTL-USL0
- SUN2000-110KTL-M0
- SUN2000-111KTL-NHM0
- SUN2000-125KTL-JPH0
- SUN2000-125KTL-M0
- SUN2000-12KTL
- SUN2000-12KTL-M0
- SUN2000-12KTL-M1
- SUN2000-12KTL-M2
- SUN2000-15KTL-M0
- SUN2000-15KTL-M2

- SUN2000-15KTL-M3
- SUN2000-168KTL-H1
- SUN2000-175KTL-H0
- SUN2000-17KTL-M0
- SUN2000-17KTL-M2
- SUN2000-17KTL-M3
- SUN2000-185KTL-H1
- SUN2000-185KTL-INH0
- SUN2000-193KTL-H0
- SUN2000-196KTL-H0
- SUN2000-196KTL-H3
- SUN2000-200KTL-H2
- SUN2000-200KTL-H3
- SUN2000-20KTL-M0
- SUN2000-20KTL-M2
- SUN2000-20KTL-M3
- SUN2000-215KTL-H0
- SUN2000-215KTL-H3
- SUN2000-22KTLUS
- SUN2000-23KTL
- SUN2000-23KTL-M3
- SUN2000-24.5KTL
- SUN2000-24.7KTL-JP
- SUN2000-25KTL-NAM3
- SUN2000-25KTLUS
- SUN2000-28KTL
- SUN2000-28KTL-M3
- SUN2000-29.9KTL
- SUN2000-29.9KTL-M3
- SUN2000-2KTL-L0
- SUN2000-3.8KTL-USLO
- SUN2000-30KTLA

- SUN2000-30KTL-M3
- SUN2000-30KTL-NAM3
- SUN2000-30KTLUS
- SUN2000-33KTL
- SUN2000-33KTLA
- SUN2000-33KTLE001
- SUN2000-33KTL-JP
- SUN2000-33KTL-NAM3
- SUN2000-33KTLUS
- SUN2000-36KTL
- SUN2000-36KTL-M3
- SUN2000-36KTL-NAM3
- SUN2000-36KTLUS
- SUN2000-3KTL-CNLO
- SUN2000-3KTL-LO
- SUN2000-3KTL-M0
- SUN2000-3KTL-M1
- SUN2000-4.95KTL-JPLO
- SUN2000-40KTL
- SUN2000-40KTL-JP
- SUN2000-40KTL-M3
- SUN2000-40KTL-NAM3
- SUN2000-40KTLUS
- SUN2000-42KTL
- SUN2000-42KTL-M3
- SUN2000-43KTL-IN-C1
- SUN2000-43KTL-INM3
- SUN2000-44KTL-M3
- SUN2000-45KTLUS-HV-D0
- SUN2000-4KTL-CNLO
- SUN2000-4KTL-LO
- SUN2000-4KTL-M0

- SUN2000-4KTL-M1
- SUN2000-50KTL
- SUN2000-50KTLC1
- SUN2000-50KTL-JPM0
- SUN2000-50KTL-JPM1
- SUN2000-50KTL-M0
- SUN2000-50KTL-M3
- SUN2000-55KTLHV-D1
- SUN2000-55KTLHV-D1-001
- SUN2000-55KTLIN-HV-D1
- SUN2000-5KTL-CNLO
- SUN2000-5KTL-L0
- SUN2000-5KTL-M0
- SUN2000-5KTL-M1
- SUN2000-5KTL-USLO
- SUN2000-60KTLHV-D1
- SUN2000-60KTLHV-D1-001
- SUN2000-60KTL-M0
- SUN2000-63KTL-JPH0
- SUN2000-63KTL-JPM0
- SUN2000-65KTL-M0
- SUN2000-6KTL-CNLO
- SUN2000-6KTL-M0
- SUN2000-6KTL-M1
- SUN2000-7.6KTL-USLO
- SUN2000-70KTL-C1
- SUN2000-70KTL-INM0
- SUN2000-75KTL-C1
- SUN2000-8KTL
- SUN2000-8KTL-M0
- SUN2000-8KTL-M1
- SUN2000-8KTL-M2

- SUN2000-90KTL-H0
- SUN2000-90KTL-H1
- SUN2000-90KTL-H2
- SUN2000-95KTL-INH0
- SUN2000-95KTL-INH1
- SUN2000-9KTL-USLO
- SUN2000L-2KTL
- SUN2000L-3.68KTL
- SUN2000L-3KTL
- SUN2000L-3KTL-CN
- SUN2000L-3KTL-CN-4G
- SUN2000L-4.125KTL-JP
- SUN2000L-4.6KTL
- SUN2000L-4.95KTL-JP
- SUN2000L-4KTL
- SUN2000L-4KTL-CN
- SUN2000L-4KTL-CN-4G
- SUN2000L-5KTL
- SUN2000L-5KTL-CN
- SUN2000L-5KTL-CN-4G

10.3.7 INGETEAM

Série 1Play HF :

- SUN 1Play 2.5HF
- SUN 1Play 2.7HF
- SUN 1Play 3HF
- SUN 1Play 3.3HF
- SUN 1Play 3.68HF
- SUN 1Play 4.6HF
- SUN 1Play 5HF
- SUN 1Play 5.5HF
- SUN 1Play 6HF

Série 1Play TL-M :

- SUN 1Play 2.5TL M
- SUN 1Play 2.7TL M
- SUN 1Play 3TL M
- SUN 1Play 3.3TL M
- SUN 1Play 3.68TL M
- SUN 1Play 4.6TL M
- SUN 1Play 5TL M
- SUN 1Play 5.5TL M
- SUN 1Play 6TL M

Série 3Play :

- SUN 20TL
- SUN 33TL
- SUN 20TL M
- SUN 33TL M
- SUN 40TL M480
- SUN 100TL
- SUN 160TL

Série Power Block :

- SUN 830TL B300
- SUN 1000TL B360
- SUN 1070TL B385
- SUN 1110TL B400
- SUN 1140TL B410
- SUN 1165TL B420
- SUN 1190TL B430
- SUN 1220TL B440
- SUN 1250TL B450
- SUN 1275TL B460
- SUN 1170TL B450
- SUN 1400TL B540
- SUN 1500TL B578

- SUN 1560TL B600
- SUN 1600TL B615
- SUN 1640TL B630
- SUN 1665TL B640
- SUN 1690TL B650
- SUN 1740TL B670
- SUN 1800TL B690

Série Power Max :

- SUN 250 TL
- SUN 315HE TL
- SUN 365HE TL
- SUN 375 TL
- SUN 400HE TL
- SUN 420HE TL
- SUN 500 TL
- SUN 500HE TL
- SUN 550HE TL
- SUN 600HE TL
- SUN 625HE TL
- SUN 630HE TL
- SUN 730HE TL
- SUN 800HE TL
- SUN 840HE TL

10.3.8 KACO

Série Powador :

- Powador 2500XI
- Powador 3600XI
- Powador 4000XI
- Powador 4500XI
- Powador 5000XI
- Powador 4000 Supreme

- Powador 2002
- Powador 3002
- Powador 4202
- Powador 5002
- Powador 6002
- Powador 6400XI
- Powador 6650XI
- Powador 7200XI
- Powador 8000XI
- Powador 6400
- Powador 6650
- Powador 7200
- Powador 8000 Supreme
- Powador 25000XI
- Powador 30000XI
- Powador 33000XI
- Powador Park
- Powador 10.0 TL3
- Powador 12.0 TL3
- Powador 14.0 TL3
- Powador 30.0 TL3
- Powador 37.5 TL3
- Powador 39.0 TL3
- Powador 72.0 TL3
- Powador 12.0 TR3
- Powador 14.0 TR3
- Powador 18.0 TR3
- Powador XP100-HV
- Powador XP200-HV
- Powador XP 250-HV
- Powador XP200-HV-TL
- Powador XP250-HV-TL

- Powador XP350-HV-TL

Série BluePlanet TL3 :

- Blueplanet 3.0 TL3
- Blueplanet 4.0 TL3
- Blueplanet 5.0 TL3
- Blueplanet 6.5 TL3
- Blueplanet 7.5 TL3
- Blueplanet 8.6 TL3
- Blueplanet 9.0 TL3
- Blueplanet 10.0 TL3
- Blueplanet 15.0 TL3
- Blueplanet 20.0 TL3
- Blueplanet 50.0 TL3
- Blueplanet 50.0 TL3 RP only
- Blueplanet 87.0 TL3
- Blueplanet 92.0 TL3
- Blueplanet 105 TL3
- Blueplanet 110TL3-US
- Blueplanet 125 TL3
- Blueplanet 125TL3-US
- Blueplanet 137 TL3
- Blueplanet 150 TL3
- Blueplanet 155 TL3
- Blueplanet 165 TL3

Série BluePlanet Gridsave :

- Gridsave 50.0 TL3-S
- Gridsave 92.0 TL3-S
- Gridsave 110 TL3-S
- Gridsave 137 TL3-S

Série NX1 :

- 3.0 NX1 M2
- 3.7 NX1 M2

- 4.0 NX1 M2
- 5.0 NX1 M2

Série NX3 :

- 3.0 NX3 M2
- 5.0 NX3 M2
- 8.0 NX3 M2
- 10.0 NX3 M2
- 15.0 NX3 M2
- 20.0 NX3 M2
- 25 NX3 M3
- 30 NX3 M3
- 33 NX3 M3
- 100 NX3 M8
- 125 NX3 M8

10.3.9 Kostal

Série PIKO 3.0-20 :

- PIKO 3.0
- PIKO 4.2
- PIKO 4.6
- PIKO 5.5
- PIKO 7
- PIKO 8.5
- PIKO 10
- PIKO 12
- PIKO 15
- PIKO 17
- PIKO 20

Série PIKO MP PLUS :

- PIKO MP PLUS 1.5-1
- PIKO MP PLUS 2.0-1
- PIKO MP PLUS 2.5-1

- PIKO MP PLUS 3.0-1
- PIKO MP PLUS 3.0-2
- PIKO MP PLUS 3.6-1
- PIKO MP PLUS 3.6-2
- PIKO MP PLUS 4.6-2
- PIKO MP PLUS 5.0-2

Série PIKO CI :

- PIKO CI 30 kW
- PIKO CI 50 kW
- PIKO CI 60 kW

Série PIKO IQ :

- PIKO IQ 3.0 kW
- PIKO IQ 4.2 kW
- PIKO IQ 5.5 kW
- PIKO IQ 7.0 kW
- PIKO IQ 8.5 kW
- PIKO IQ 10.0 kW

Série PIKO PLENTICORE PLUS :

- PIKO PLENTICORE PLUS 3.0
- PIKO PLENTICORE PLUS 4.2
- PIKO PLENTICORE PLUS 5.5
- PIKO PLENTICORE PLUS 7.0
- PIKO PLENTICORE PLUS 8.5
- PIKO PLENTICORE PLUS 10

10.3.10 SMA

Série SUNNY BOY

Série SUNNNY TRI POWER

Série SUNNY MINI central

10.3.11 Solis

Série single phase :

- S6-GR1P2.5K
- S6-GR1P3K
- S6-GR1P3.6K
- S6-GR1P4K
- S6-GR1P4.6K
- S6-GR1P5K
- S6-GR1P6K

Série three phases :

- Solis-15K-LV
- Solis-20K-LV
- Solis-40K
- Solis-50K
- Solis-50K-HV
- Solis-60K-HV

Série Energy Storage Inverters RHI / RAI :

- RHI-3K-48ES
- RHI-3.6K-48ES
- RHI-4.6K-48ES
- RHI-5K-48ES
- RAI-3K-48ES-5G
- RHI-3K-48ES-5G
- RHI-3.6K-48ES-5G
- RHI-4.6K-48ES-5G
- RHI-5K-48ES-5G
- RHI-6K-48ES-5G

Série single phase US 4G :

- Solis-1P6K-4G-US
- Solis-1P7K-4G-US
- Solis-1P7.6K-4G-US
- Solis-1P8K-4G-US

- Solis-1P8.6K-4G-US
- Solis-1P9K-4G-US
- Solis-1P10K-4G-US

Série three phases US 5G :

- Solis-75K-5G-US
- Solis-80K-5G-US
- Solis-90K-5G-US
- Solis-100K-5G-US

Série Mini Inverter 4G :

- Solis-mini-700-4G
- Solis-mini-1000-4G
- Solis-mini-1500-4G
- Solis-mini-2000-4G
- Solis-mini-2500-4G
- Solis-mini-3000-4G
- Solis-mini-3600-4G

Série single phase K-4G :

- Solis-1P2.5K-4G
- Solis-1P3K-4G
- Solis-1P3.6K-4G
- Solis-1P4K-4G
- Solis-1P4.6K-4G
- Solis-1P5K-4G
- Solis-1P6K-4G
- Solis-1P9K-4G
- Solis-1P10K-4G

Série three phases K-4G :

- Solis-60K-4G
- Solis-3P3K-4G
- Solis-3P4K-4G
- Solis-3P5K-4G
- Solis-3P6K-4G

- Solis-3P8K-4G
- Solis-3P9K-4G
- Solis-3P10K-4G
- Solis-3P12K-4G
- Solis-3P15K-4G
- Solis-3P17K-4G
- Solis-3P20K-4G
- Solis-70K-HV-4G

Série single phase K-5G :

- Solis-1P7K-5G
- Solis-1P8K-5G

Série three phases 5G :

- Solis-25K-5G
- Solis-30K-5G
- Solis-33K-5G
- Solis-36K-5G
- Solis-40K-5G
- Solis-80K-5G
- Solis-100K-5G
- Solis-40K-HV-5G
- Solis-50K-HV-5G
- Solis-100K-HV-5G
- Solis-110K-HV-5
- Solis-125K-EHV-5G
- Solis-136K-EHV-5G
- Solis-250K-EHV-5G

Série US :

- Solis-25K-US
- Solis-30K-US
- Solis-36K-US
- Solis-40K-US
- Solis-50K-US

- Solis-36K-US-F
- Solis-40K-US-F
- Solis-50K-US-F
- Solis-60K-US-F
- Solis-66K-US-F
- Solis-25K-US-SW
- Solis-25K-US-F-SW
- Solis-30K-US-SW
- Solis-30K-US-F-SW
- Solis-36K-US-SW
- Solis-36K-US-F-SW
- Solis-40K-US-SW
- Solis-40K-US-F-SW
- Solis-50K-US-SW
- Solis-50K-US-F-SW
- Solis-60K-US-F-SW
- Solis-66K-US-F-SW

10.3.12 SUNGROW

- SG5.5RS-JP
- SG0.7RS-S
- SG1.0RS-S
- SG1.5RS-S
- SG2.0RS-S
- SG2.5RS-S
- SG3.0RS-S
- SG3.0RS
- SG3.6RS
- SG4.0RS
- SG5.0RS
- SG6.0RS
- SG8.0RS
- SG9.0RS

- SG10RS
- SG5.0RS-ADA
- SG3.0RT
- SG4.0RT
- SG5.0RT
- SG6.0RT
- SG7.0RT
- SG8.0RT
- SG10RT
- SG12RT
- SG15RT
- SG17RT
- SG20RT
- SG3.0 RT-P2
- SG4.0 RT-P2
- SG5.0 RT-P2
- SG6.0 RT-P2
- SG7.0 RT-P2
- SG8.0 RT-P2
- SG10 RT-P2
- SG12 RT-P2
- SG15 RT-P2
- SG17 RT-P2
- SG20RT-P2
- SG 25CX-P2
- SG 30CX-P2
- SG 33CX-P2
- SG 36CX-P2
- SG 40CX-P2
- SG 50CX-P2
- SG 75CX-P2
- SG 110CX-P2

- SG 125CX-P2
- SG30KTL-M
- SG30KTL-M-V31
- SG33KTL-M
- SG36KTL-M
- SG33K3J
- SG49K5J
- SG34KJ
- LP_P34KSG
- SG49.5CX-JP
- SG50KTL-M-20
- SG60KTL
- SG80KTL
- SG80KTL-20
- SG60KU-M
- SG5KTL-MT
- SG6KTL-MT
- SG8KTL-M
- SG10KTL-M
- SG10KTL-MT
- SG12KTL-M
- SG15KTL-M
- SG17KTL-M
- SG20KTL-M
- SG80KTL-M
- SG85BF
- SG80HV
- SG80BF
- SG110HV-M
- SG111HV
- SG125HV
- SG125HV-20

- SG25CX-SA
- SG30CX
- SG33CX
- SG40CX
- SG50CX
- SG36CX-US
- SG60CX-US
- SG75CX
- SG100CX
- SG100CX-JP
- SG110CX
- SG136TX
- SG225HX
- SG250HX
- SG250HX-IN
- SG250HX-US
- SG285HX
- SG350HX
- SG125HX
- SG125HX-JP
- SG333HX
- SG320HX
- SG30KTL
- SG10KTL
- SG12KTL
- SG15KTL
- SG20KTL
- SG30KU
- SG36KTL
- SG36KU
- SG40KTL
- SG40KTL-M

- SG50KTL-M
- SG60KTL-M
- SG60KU

10.4 Annexe D : Esclave Modbus

La WebdynSunPM possède une fonctionnalité d'esclave Modbus TCP permet:

- d'accéder aux variables des équipements gérés par la WebdynSunPM,
- d'accéder aux variables créées par les scripts,
- d'accéder à certaines informations prédéfinies propres à la WebdynSunPM (numéro de série, version de firmware, etc.),
- d'exécuter des commandes.

10.4.1 Fonctionnement général

L'esclave Modbus est accessible uniquement en TCP. Son adresse esclave est 1..Un client connecté à l'esclave peut accéder aux 65536 registres (holding registers) de 16 bits, adressés de 0x0 à 0xFFFF. Chaque registre peut être lu via la fonction 0x3 (Read Holding Registers) et écrit via les fonctions 0x10 (Write Multiple Registers) ou 0x6 (Write Single Register).

Un groupe d'un ou plusieurs registres adjacents associé à une variable. Certains registres sont prédéfinis, d'autres peuvent être configurés librement par l'utilisateur.

Lorsqu'on accède à un registre le comportement de base est le suivant :

- Lecture d'un groupe de registres associé à une variable : la WebdynSunPM retourne la dernière valeur lue pour cette variable. Il peut s'agir d'une variable classique (liée à un équipement physique) ou d'une variable virtuelle (créée par un script).
- Écriture d'un groupe de registres associé à une variable : la WebdynSunPM modifie la valeur de la variable. Bien entendu, dans le cas d'une variable classique, cette action nécessite une requête vers son équipement physique.

Enfin il faut noter que toutes les valeurs retournées par la WebdynSunPM sont des valeurs brutes (sans mise à l'échelle), formatées en big-endian. De même les valeurs attendues en écriture sont des valeurs brutes en big-endian.

10.4.2 Activer l'esclave Modbus

L'esclave Modbus se configure grâce à une entrée dans le fichier DAQ :

```
ModbusSlave;<enabled>;<port>:<mapping file>
```

Où :

- enabled : 0 → service désactivé, 1 → service activé
- port : port TCP utilisé par le serveur. Par défaut le port 502 est utilisé
- mapping file : nom du fichier décrivant les associations entre registres et variables. Le fichier est attendu dans le répertoire FTP_DirDef. Par défaut le nom de fichier utilisé est <ConcentratorId>_ModbusSlave.csv. Le paragraphe suivant donne plus de détails sur ce fichier.

10.4.3 Registres utilisateurs

Les registres adressés de 0x0 à 0x7FFF (0-32767) sont libres d'usage et peuvent être configurés via un fichier de définition décrivant les associations entre registres et variables. Cf. § Voir paragraphe 3.1.2.2.2 « Contenu du fichier de définition pour des détails sur le format d'un fichier de définition.

Pour la configuration de l'esclave Modbus, le « protocole » utilisé est ModbusSlave, qui doit apparaître en première ligne du fichier de configuration, et la signification des champs est la suivante :

Champ	Description
Index	Contient l'identifiant unique de l'association dans le fichier. Le choix est libre pour le client à condition qu'il conserve son unicité.
Info1	Non utilisé.
Info2	Adresse du premier registre pour cette association et taille en octets). L'adresse du premier registre et la taille en octets sont séparés par un underscore “_”. (par défaut la taille est de deux octets, i.e. un registre)
Info3	Non utilisé.
Info4	Nom de l'équipement ciblé par cette association (variable classique), nom du script (variable virtuelle) ou io pour une entrée/sortie.
Name	Nom de la variable ciblée par cette association. Ce champ n'est pas nécessaire si Tag est utilisé.
Tag	Tag de la variable ciblée par cette association. Ce champ n'est pas nécessaire si Name est utilisé.
CoedA	Non utilisé.
CoefB	Non utilisé.
Unit	Non utilisé.
Action	Les actions possibles sont : <ul style="list-style-type: none">• 0 : association désactivée et donc non utilisée.• 1 : la variable ciblée est en lecture seule. Il n'est pas permis d'y accéder en écriture (par défaut la valeur est 1).• 4 : la variable ciblée est accessible en lecture et écriture.

Comme pour les autres fichiers, ModbusSlave.csv est récupéré lors d'une connexion SI. Sa cohérence est alors vérifiée et il peut être rejeté en cas d'erreur. Notamment les groupes de registres ne peuvent pas se superposer.

Exemple de fichier de configuration :

```

ModbusSlave
# Ici nous ciblons une variable U16, donc un seul registre suffit
1;;0;;the_purple_inverter;Temperature;;;;

# Ici nous ciblons une variable F32, donc 2 registres (4 octets) sont
nécessaires
2;;1_4;;the_purple_inverter;E-Total-Sell;;;;

# Ici nous ciblons une variable String et nous autorisons 20 octets (10
registres)
3;;3_20;;the_purple_inverter;Firmware Version;;;;

# De même ici, mais nous ciblons un tag plutôt qu'un nom de variable
4;;13_20;;the_purple_inverter;;DisplaySerialNumber;;;;

```

10.4.4 Registres Webdyn prédéfinis

Les registres adressés de 0x8000 à 0xFFFF (32768-65535) sont réservés et ne peuvent pas être configurés librement. Ils permettent d'accéder à certaines informations de la WebdynSunPM.

Registres prédéfinis :

Adresse et nombre de registres	Type de donnée	Accès	
33000 / 15	String	RO	Version du firmware
33015 / 15	String	RO	Version du kernel
33030 / 15	String	RO	Numéro de série
33045 / 15	String	RO	Identifiant
33060 / 2	time_t	RO	Date de dernière mise à jour
33200 / 2	U32	RO	Entrée digitale 1
33202 / 2	U32	RO	Entrée digitale 2
33204 / 2	U32	RO	Entrée digitale 3
33206 / 2	U32	RO	Entrée analogique 1
33208 / 2	U32	RO	Entrée analogique 2
33210 / 2	U32	RO	Entrée analogique 3
33212 / 2	U32	RO	Entrée analogique 4
33214 / 2	U32	RW	Sortie relais

34000 / 120	String	WO	<p>Commandes</p> <p>Ce groupe de registre est spécial : il n'est pas associé à une variable ou une information, mais permet d'exécuter des commandes. Voir paragraphe 5.3 « Liste des Commandes » pour plus de détails sur l'exécution d'une commande via Modbus.</p>
-------------	--------	----	---

10.4.5 Lire ou écrire une variable

Lorsqu'un groupe de registres associé à une variable est lu, la dernière valeur connue de cette variable est retournée dans une réponse standard Modbus.

Lorsqu'un groupe de registres associé à une variable est écrit, la WebdynSunPM procède à l'écriture de la nouvelle valeur sur l'équipement. La réponse n'est retournée au client que lorsque cette opération est terminée.

Attention, comme pour la commande writeVariable, l'écriture d'une seule variable à la fois est autorisée.

10.4.6 Exécuter une commande

Pour exécuter une commande, il suffit d'écrire une chaîne de caractères à l'adresse de registre 34000 avec la même syntaxe que pour une commande SMS.

10.4.7 Gestion des erreurs

En cas d'erreur la WebdynSunPM retourne un code d'exception Modbus. Les cas d'erreur sont les suivants :

Code	Nom	Que se passe-t-il ?
0x1	Illegal Function	Code fonction non pris en charge, i.e. différent de 0x3, 0x6 ou 0x10.

0x2	Illegal Data Address	<p>Problème de cohérence entre la requête et les registres accédés :</p> <ul style="list-style-type: none"> • Un registre est non configuré. • Un registre est ignoré (code action 0). • Un groupe de registre est incomplet, i.e. on demande moins de registres que le groupe n'en contient. • Tentative d'écriture sur plus d'une variable. • Tentative d'écriture sur une variable en lecture seule (code action 1). • Tentative de lecture sur le registre de commande.
0x3	Illegal Data Value	
0x4	Server Device Failure	Adresse Modbus invalide, i.e. différente de 1.
0xA	Gateway Path Unavailable	Lors d'une écriture, impossible de se connecter à un équipement en TCP. La configuration réseau est peut-être en cause.
0xB	Gateway Target Device Failed to Respond	<p>Lors d'une écriture :</p> <ul style="list-style-type: none"> • Un équipement n'a pas répondu (timeout). • Un équipement a répondu avec une trame invalide (erreur CRC, malformée, etc.). • Un équipement a fermé sa socket TCP de manière inattendue.
0x70	Invalid Mapping	Une variable à une taille incompatible avec le nombre de registres lus ou écrits.
0x71	No Such a Variable	Un équipement ou une variable ne sont pas connus de la WebdynSunPM.
0x72	Invalid Action	L'écriture pour la variable ciblée n'est pas supportée (Input Register, U8, etc.).
> 0x80		Lors d'une écriture, si un équipement répond avec une exception Modbus, celle-ci est transférée au client en y mettant le bit de poids fort à 1, i.e. en réalisant la transformation 0x80 code.

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@matrix.es

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@matrix.es