webdyn

Flexitron group

WebdynEasy LoRaWAN

Manual de usuario

Índice

Glosario

NAME	DESCRIPTION
ABP	Activation By Personalization: la activación ABP requiere disponer del DevAddr, así como de las claves de seguridad del periférico memorizadas en el producto. Esta estrategia puede parecer más simple porque omite el procedimiento de acople, pero tiene inconvenientes de seguridad.
ADR	Adaptive Data Rate: es un mecanismo para optimizar la velocidad de datos (Data Rate) y la potencia de emisión de radio. Esto optimiza el consumo de la batería.
APN	Access Point Name: nombre del punto de acceso que permite a la pasarela conectarse a Internet por conexión móvil.
AppEUI	La Aplicación EUI es un identificador de aplicación único asignado por el organismo IEEE (EUI-64). Se utiliza únicamente en OTAA y permite obtener las claves del servidor durante el JOIN.
AppKEY	La Aplicación Key es específica del producto. Se utiliza únicamente en OTAA y permite obtener las claves del servidor durante el JOIN.
AppSKey	La Aplicación Session Key es específica del producto y proporciona un cifrado de extremo a extremo de los datos de la aplicación. Debe introducirse en modo ABP y calcularse automáticamente durante el JOIN por el servidor en modo OTAA.
Data Rate	Data Rate se define por un dígito de 0 a 5 y fija el tipo de modulación, el factor de dispersión y el ancho de banda utilizado.
DevEUI	Device EUI: identificador único atribuido por el organismo IEEE (EUI-64).
Device Address	Identificador de 32 bits del dispositivo que identifica de forma exclusiva el producto en el servidor LoRaWAN. Debe introducirse en modo ABP y proporcionarse automáticamente durante el JOIN por el servidor en modo OTAA.
FTP	File Transfer Protocol: protocolo de comunicación destinado al intercambio informático de archivos en una red TCP/IP.
HTTP	HyperText Transfer Protocol: protocolo de comunicación cliente-servidor desarrollado para Internet.
IP	Internet Protocol: protocolo de mensajes responsable de direccionar y transmitir paquetes TCP en la red.
JSON	Notación de objetos de JavaScript: JSON es un formato de intercambio de datos fácilmente interpretable.

LoRa	LoRa es una modulación de radio que incluye la conexión física y la capa física del modelo OSI
LoRaWAN	LoRaWAN es un protocolo de transmisión que utiliza la modulación LoRa.
MD5	Message Digest 5: función de direccionamiento criptográfico que permite obtener la huella digital de un archivo.
Modbus	Modbus es un protocolo de comunicación comúnmente utilizado en la industria para comunicarse en una red con equipos industriales.
NTP	Network Time Protocol: protocolo que permite sincronizar, a través de una red informática, el reloj local del concentrador con una referencia horaria.
NwkSKey	Network Session Key es específico del producto y proporciona un cifrado de extremo a extremo de los datos de la red LoRaWAN. Debe introducirse en modo ABP y calcularse automáticamente durante el JOIN por el servidor en modo OTAA.
OTAA	Over The Air Activation: la activación OTAA es la forma prioritaria y más segura de conectarse a la red LoRaWAN. El producto realiza un procedimiento de acople (JOIN) con la red, durante el cual se asigna un DevAddr dinámico y se negocian las claves de seguridad con el producto.
PEM	Estándar de formato de archivo para almacenar certificados y claves privadas en formato de texto codificado en Base64.
DIN rail	Raíl metálico estandarizado de 35 mm utilizado en Europa en equipos industriales de control en racks
RTU	El modo RTU es un bus cableado en RS422/485 para Modbus.
Spreading Factor (SF)	El factor de propagación representa la longitud de las tramas enviadas. Cuanto mayor es la propagación de la señal, menor es el flujo, pero aumenta el alcance del producto.
TCP	Transmission Control Protocol: protocolo orientado a la conexión en Internet que ofrece los servicios de segmentación de datos en paquetes que el protocolo IP transmite a través de la red. Este protocolo proporciona un servicio fiable de transferencia de datos. Ver también IP.
TCP/IP	Transmission Control Protocol/Internet Protocol: conjunto de protocolos de red que aportan servicios de interconexión entre ordenadores de diferentes arquitecturas de hardware y sistemas operativos. TCP/IP incluye normas de comunicación entre ordenadores y convenios para interconectar redes y enrutamiento.

UDP	User Datagram Protocol: protocolo no orientado a la conexión de la capa de transporte del modelo TCP/IP. Este protocolo es muy simple, ya que no proporciona control de errores (no está orientado a la conexión...).
VPN	Red Privada Virtual: conexión segura y encriptada entre el concentrador y una red privada, permitiendo así el aislamiento de las redes públicas de telecomunicaciones.
XML	Extensible Markup Language: metalenguaje informático de etiquetación genérica. El objetivo del XML es facilitar el intercambio automatizado de contenidos complejos entre sistemas de información heterogéneos.
XSD	XML Schema Definition: archivo que permite validar las etiquetas XML y los datos de un archivo XML.

Historia del documento

Versión	Descripción
V0.11	Creación
V1.0	Añadir VPN
V3.12	Añadir MQTT data support Añadir LoRaWAN modo C

1. Observaciones sobre este manual

Esta guía describe el montaje, la instalación y la configuración del concentrador, así como su utilización remota.

1.1 Campo de aplicación

La presente descripción técnica es válida para concentradores WebdynEasy LoRaWAN desde la versión de hardware V1 y la versión de software V1.0.

1.2 Grupo destinatario

Esta guía está destinada a instaladores y usuarios de concentradores WebdynEasy LoRaWAN, pero también a personas que utilizan nuestros sensores Sens'RF LoRaWAN.

1.3 Referencias de productos y accesorios

Concentrador LoRaWAN:

Referencias de productos	Versiones
WG0610-A01	WebdynEasy LoRaWAN

Sensor LoRaWAN Webdyn compatible:

Referencias de productos	Descripción
WG0307-D01-EU	Sens'RF-LoRaWAN-Pulse (sin alimentación externa)
WG0307-D02-EU	Sens'RF-LoRaWAN-Pressure Humidity and Temperature (sin alimentación externa)
WG0307-D03-EU	Sens'RF-LoRaWAN-TIC (sin alimentación externa)
WG0307-D08-EU	Sens'RF-LoRaWAN-Analog (0-10V/4-20mA) (sin alimentación externa)
WG0307-D11-EU	Sens'RF-LoRaWAN-Pulse (con alimentación externa)
WG0307-D12-EU	Sens'RF-LoRaWAN-Pressure Humidity and Temperature (con alimentación externa)

WG0307-D13-EU	Sens'RF-LoRaWAN-TIC (con alimentación externa)
WG0307-D18-EU	Sens'RF-LoRaWAN-Analog (0-10V/4-20mA) (con alimentación externa)

1.3.1 Instrucciones de seguridad

Respete todas las instrucciones de seguridad de este manual.

El incumplimiento de estas instrucciones puede dañar los dispositivos y representar un peligro para las personas.

 Conexión eléctrica:

- Todo el trabajo de cableado debe ser realizado por un electricista especializado cualificado.
- Siga todas las instrucciones de seguridad indicadas en la documentación de los equipos.

 El producto WebdynEasy puede resultar dañado por descargas electrostáticas (ESD). Cuando el equipo esté abierto, no realice operaciones distintas a las previstas en este manual. Evite el contacto con los componentes.

 Equipamiento de clase 3: el dispositivo funciona en muy baja tensión de seguridad (MBTS) (50V máximo). La reducción de tensión debe realizarse mediante un transformador de seguridad que proporcione un aislamiento galvánico seguro entre el primario y el secundario.

 No instale el equipo cerca de una fuente de calor o a una altura superior a 2m.

 Para limpiar el producto, use solo un paño ligeramente húmedo para limpiar y frote suavemente las superficies. No utilice nunca agentes químicos agresivos o disolventes que puedan alterar el material plástico o corroer los elementos metálicos.

 Para optimizar la sensibilidad de la recepción de Radio y celular Modem, es esencial dejar un espacio vacío de 20 cm. alrededor de las antenas.

1.4 Reglamentación

El producto cumple las directivas europeas según la declaración de conformidad UE disponible en Webdyn o en el sitio Internet: www.webdyn.com.

Reciclaje:

Las directivas europeas transpuestas relativas a residuos de baterías y equipos eléctricos y electrónicos integran las acciones necesarias para limitar el impacto negativo del final de la vida útil de los productos.

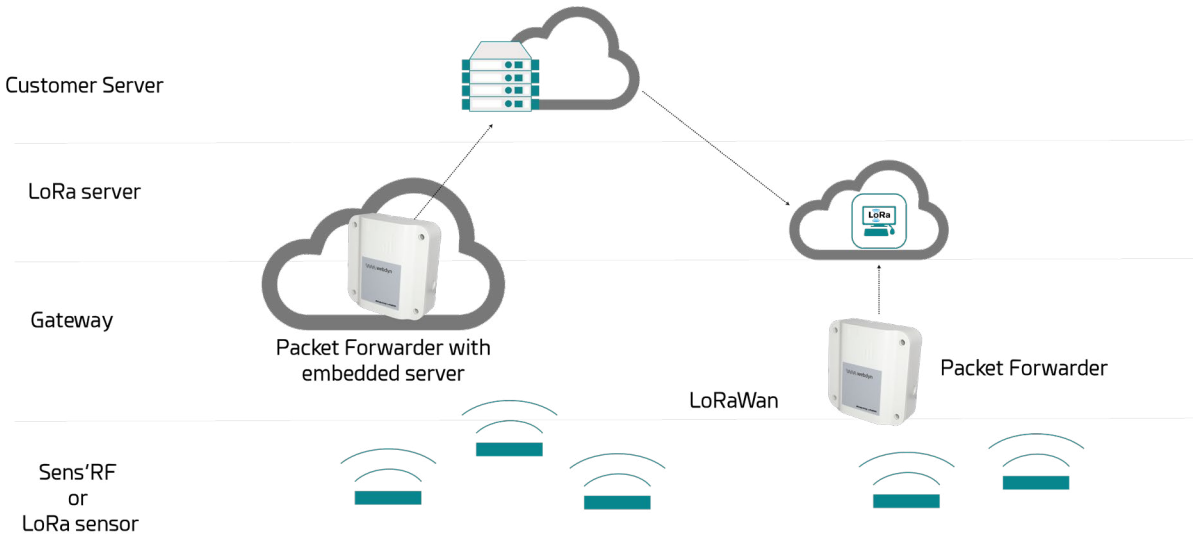
Estos productos deben separarse selectivamente para su reciclaje. Utilice un centro de recogida y tratamiento de baterías autorizado, o contacte con Webdyn.

2. Presentación general

El concentrador WebdynEasy LoRaWAN es parte de una gama de concentradores Webdyn para redes inalámbricas. La funcionalidad principal del concentrador es ser una pasarela LoRaWAN para crear su red LoRaWAN y recuperar datos de los diversos sensores LoRa desplegados en las cercanías. La pasarela LoRaWAN integra 2 modos de funcionamiento:

- Packet Forwarder (reenviador de paquetes)
- Packet Forwarder con servidor LoRaWAN integrado

El concentrador también permite la comunicación con equipos Modbus en modo IP o modo RTU.



Esquema de principio de una solución completa LoRaWAN

2.1 El protocolo LoRaWAN

LoRaWAN es un protocolo de comunicación basado en la modulación LoRa. Este protocolo de

comunicación utiliza varias bandas de radio (ISM) que pueden usarse sin licencia en la gama 868 MHz en Europa.

En una red LoRaWAN, los módulos de radio no están asociados a una sola estación base. Los datos que transmiten son emitidos por múltiples estaciones base. Cada uno transmite la información recibida de un módulo de radio a través de una pasarela al servidor de gestión. La inteligencia y la complejidad son deportadas a este servidor que gestiona la redundancia de información, la verificación de la integridad, la confirmación de recepción, la adaptación del ancho de banda y la potencia de emisión de los sensores.

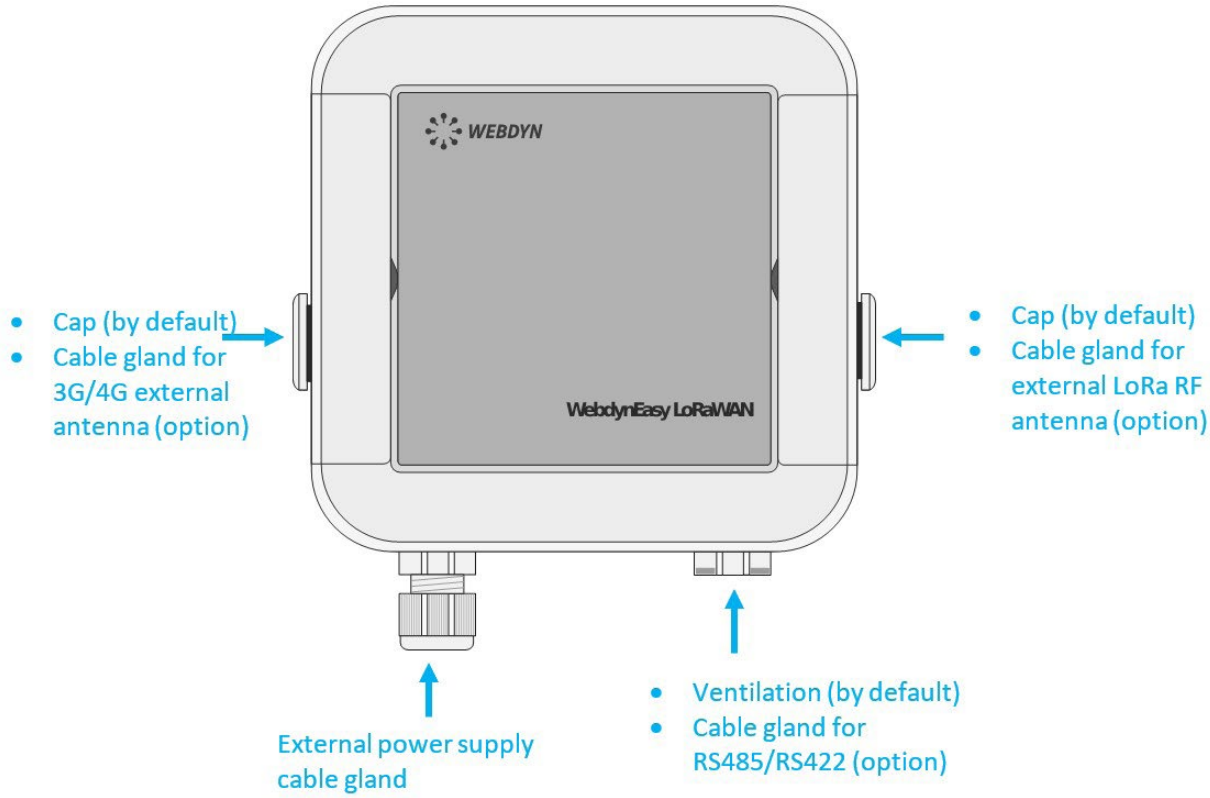
2.2 El concentrador

El objetivo del concentrador es recopilar datos en LoRaWAN y/o en Modbus y transmitirlos periódicamente a un servidor remoto (SI) en Ethernet o 3G/4G.

2.2.1 Descripción general

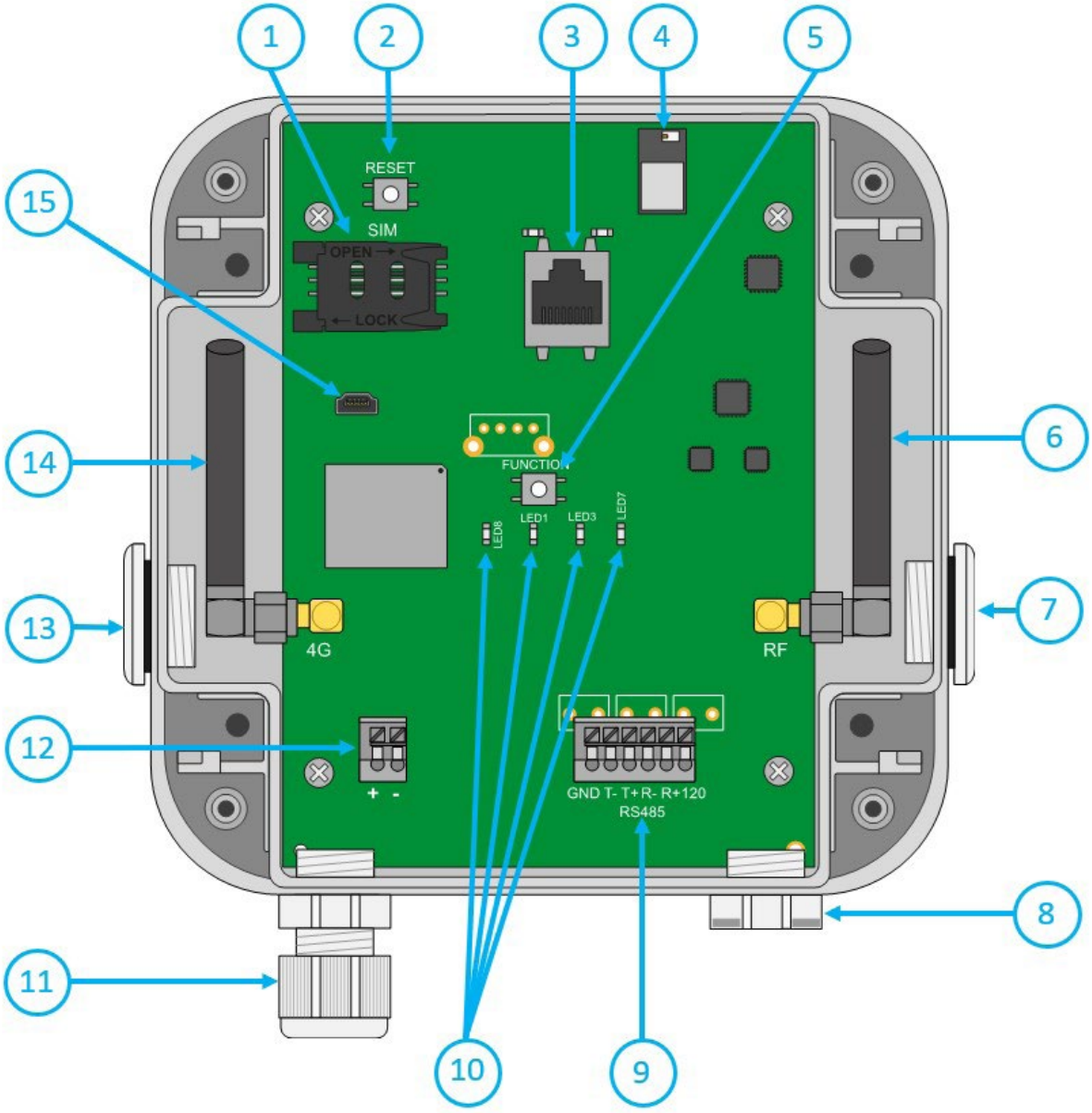
2.2.1.1 Exterior

Frontal de la carcasa:



2.2.1.2 Interior

Interior de la carcasa:



1. Soporte de tarjeta SIM
2. Botón Reset
3. Conector RJ45 con sus Leds
4. Bluetooth BLE (evolución futura)
5. Botón Request (identificado como FUNCTION en la tarjeta)
6. Antena SMA de la radio RF LoRa
7. Salida de la carcasa para antena externa de radio RF LoRa (opcional)
8. Salida de la carcasa para RS485/422
9. 1 puerto RS485/422

10. Pilotos:
    - LED 8: Power
    - LED 3: Módem
    - LED 1: CPU
    - LED 7: LoRa
11. Salida de la carcasa para alimentación externa
12. Bloque de terminales para alimentación externa 12/24V
13. Salida de la carcasa para antena externa de Módem 3G/4G (opcional)
14. Antena SMA del Módem 3G/4G
15. Conector mini-USB (reservado)

Pilotos:

LED	Descripción
Power	Se ilumina cuando el producto está alimentado
CPU	Se ilumina según la actividad CPU
LoRa	Apagado por defecto y parpadea en tráfico de radio LoRaWAN
Módem	Se ilumina cuando el Módem establece una conexión IP Se ilumina durante 1 segundo al recibir un SMS Al presionar prolongadamente el botón Request, indica el nivel de la señal recibida (RSSI) mediante una serie de parpadeos (de 0 a 5 veces) 0 - intensidad de la señal ≤ -112 dBm 1 - intensidad de la señal entre -111 dBm y -96 dBm 2 - intensidad de la señal entre -96 dBm y -81 dBm 3 - intensidad de la señal entre -81 dBm y -66 dBm 4 - intensidad de la señal entre -66 dBm y -51 dBm 5 - intensidad de la señal ≤ -51 dBm

Botones:

Botón	Descripción
Request	Pulsación corta (menos de 2 segundos) => Solicitud de conexión Pulsación larga (más de 2 segundos) => Muestra el nivel de recepción de la señal del Módem (ver LED Módem) 3 pulsaciones largas sucesivas en 15 segundos => Restablecimiento de los parámetros de fábrica
Reset	Reinicio del concentrador (Hard Reset)

 Nunca presione nunca 7 veces el botón RESET en menos de 30 segundos. De lo contrario el concentrador estará en un modo especial que bloqueará su inicio. Para salir de este modo, deberá realizarse un nuevo RESET del concentrador.

 El usuario final debe asegurarse de que su instalación con antenas remotas cumple las normas CEM vigentes.

2.2.2 Especificaciones técnicas

2.2.2.1 Características generales

Parámetros	Valores
Alimentación externa	+12/24V DC suministrados por una alimentación externa
Consumo	10 vatios máximo
Memoria Flash	50 Mo (compartidos entre los archivos comprimidos y sin comprimir)
Dimensiones	160 x 150 x 55 mm
Carcasa	Carcasa ASA IP67
Peso	0.450 kg
Temperatura de funcionamiento	-20°C/+55°C
Temperatura de almacenamiento	-20°C/+70°C
Humedad	25 - 75 %

Grado de contaminación	2
Certificación	RED ROHS REACH
Reglamentación	 Marcación “CE” creada en el marco de la legislación europea de armonización técnica. Es obligatoria para todos los productos cubiertos por uno o más textos reglamentarios europeos (directivas o reglamentos).
	 Símbolo que indica que los residuos deben recogerse por un canal específico y no deben desecharse en un contenedor convencional.
	 Símbolo que indica que el producto debe reciclarse.

2.2.2.2 Características técnicas

Parámetros	Valores
Interfaz Radio LoRa	863MHz -870MHz
Interfaz Módem	3G: HSPA+, UMTS (B1, B8) 4G: Cat-1, Bands B1, B3, B7, B8, B20, B28
Interfaz serie	1 puerto RS422/RS485 Modbus RTU
Interfaz red Ethernet	10/100 Mbit/s

Banda RF	Frecuencias de Emisión	Potencia Máx.

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

2.2.2.3 Características LoRa

Parámetros	Valores
Canales	8 canales simultáneos: • 863-870 MHz (Europa) • 865-867 MHz (India)
Sensibilidad máx.	-141dBm (125kHz en SF12)
DataRate soportado	DR0-DR5
Ancho de banda soportado	125/250 kHz
Potencia máxima TX	+14dBm
Modo de activación	ABP u OTAA
Frecuencias por defecto	Europa: 867,1 MHz, 867,3 MHz, 867,5 MHz, 867,7 MHz, 867,9 MHz, 868,1 MHz, 868,3 MHz, 868,5 MHz India: 865,0625 MHz, 865,4025 MHz, 865,985MHz

2.2.2.4 Funciones de software

Parámetros	Valores
LoRaWAN server	• Protocolo LoRaWAN V1.0.2 clase A • 1000 sensores LoRaWAN soportados • 10 pasarelas compatibles
Modbus	Supervisión en modo RTU y TCP
OpenVPN	V2.5.4

3. Instalación y Mantenimiento

3.1 Desembalaje

3.1.1 Contenido del producto

Antes de cualquier instalación, comience por verificar el contenido. Si la entrega está incompleta o dañada, contacte con el soporte Webdyn.

Concentrador WebdynEasy LoRaWAN

(Ref.: WG0610-A01)

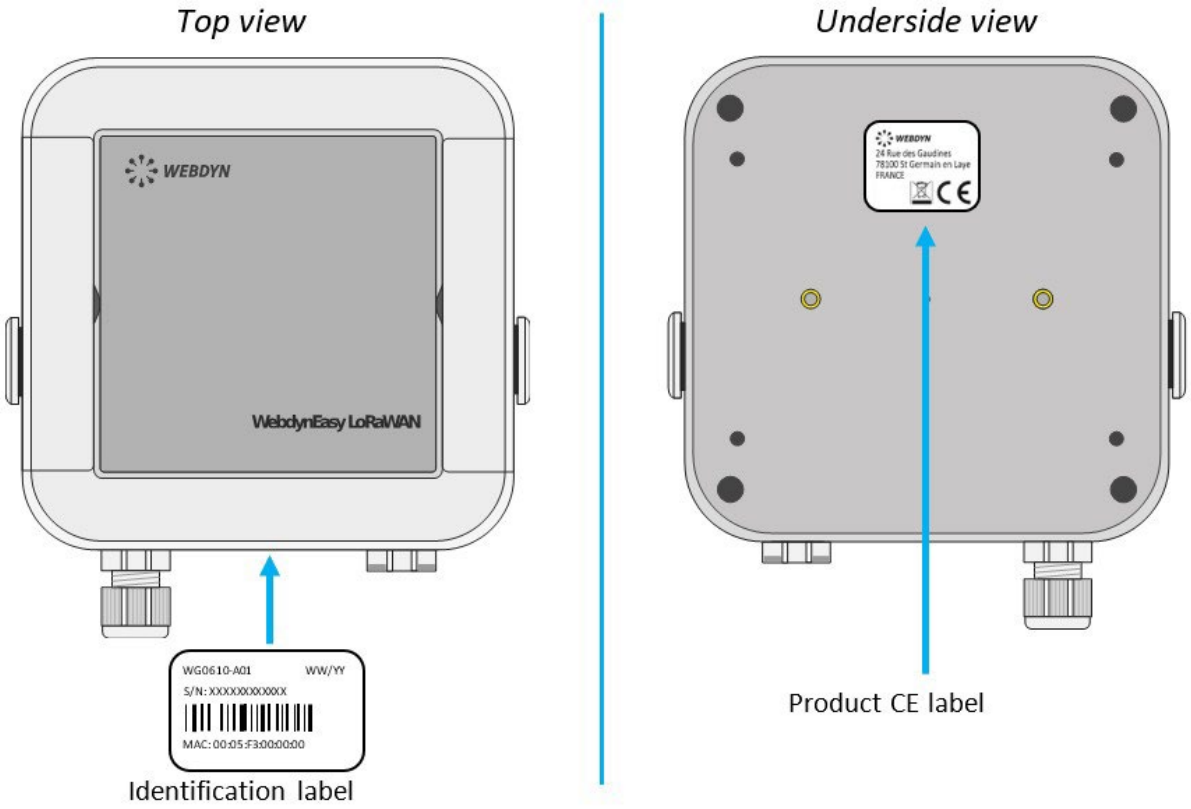
Se entregan con el concentrador:

- una antena SMA acodada para el módem (interna)
- una antena SMA acodada para la radio (interna)

3.1.2 Identificación del concentrador

Etiqueta identificativa:

El concentrador WebdynEasy LoRaWAN puede identificarse por su etiqueta identificativa, que se encuentra sobre la carcasa.



Esta etiqueta contiene:

- El nombre del producto (WG0610-A01).
- La fecha de producción (en forma SS/AA arriba a la derecha).
- El número de serie en formato texto y en código de barras 128.
- La dirección MAC (Ethernet) en formato texto.

Versión del software:

Puede encontrar la versión del software en la interfaz Web del concentrador. La versión del software se indica en la pestaña “Overview” (ver capítulo 4.1.1: “Conectividad del concentrador”).

3.2 Montaje

Antes de cualquier instalación, es importante respetar las condiciones ambientales descritas en el capítulo 2.2.2.1: “Características generales”, además de estas condiciones:

- Proteja el producto del polvo, la humedad, las sustancias agresivas y la condensación.
- La distancia entre el concentrador y los equipos Modbus no debe exceder la distancia máxima autorizada para el tipo de interfaz correspondiente (RS485 o RS422) (ver capítulo 3.2.5.2: “Bus RS485/RS422”).
- En caso de que utilice una conexión por Módem, asegúrese de que la recepción sea óptima durante el montaje. Compruebe el RSSI, accesible en la página web integrada (ver capítulo 4.1.1.1: “Módem”).

 Para optimizar la sensibilidad de la recepción radio Módem y LoRa, es esencial dejar un espacio vacío de 20 cm. alrededor de las antenas.

3.2.1 Apertura/Cierre de la carcasa

Para abrir la carcasa del concentrador, siga las etapas siguientes:

Si la carcasa está fijada a la pared:

- Abra las 2 trampillas de la cara frontal.
- Desatornille los 4 tornillos de fijación mural en las ubicaciones debajo de las trampillas.

Luego siga estas etapas:

- Desatornille los 4 tornillos que están detrás de la carcasa.
- Retire el capó.

Para cerrar la carcasa del concentrador, siga las etapas siguientes:

- Coloque el capó en la base de la carcasa, comprobando que la junta está en su lugar.
- Atornille los 4 tornillos que están detrás de la carcasa.

3.2.2 Fijación mural

El WebdynEasy puede fiarse en una pared. Antes de proceder a la fijación mural, cierre la carcasa (ver capítulo 3.2.1: “Apertura/Cierre de la carcasa”).

 Los tornillos y clavijas no se incluyen en el kit. Debe elegir el tipo correcto de tornillo en función del soporte al que fije el concentrador (tornillo de 4 mm de diámetro y longitud mínima de 25 mm).

Para fijar el concentrador en una pared, siga las etapas siguientes:

- Abra las 2 trampillas de la cara frontal.
- Atornille los 4 tornillos de fijación mural en las ubicaciones debajo de las trampillas.
- Cierre las 2 trampillas de la cara frontal.

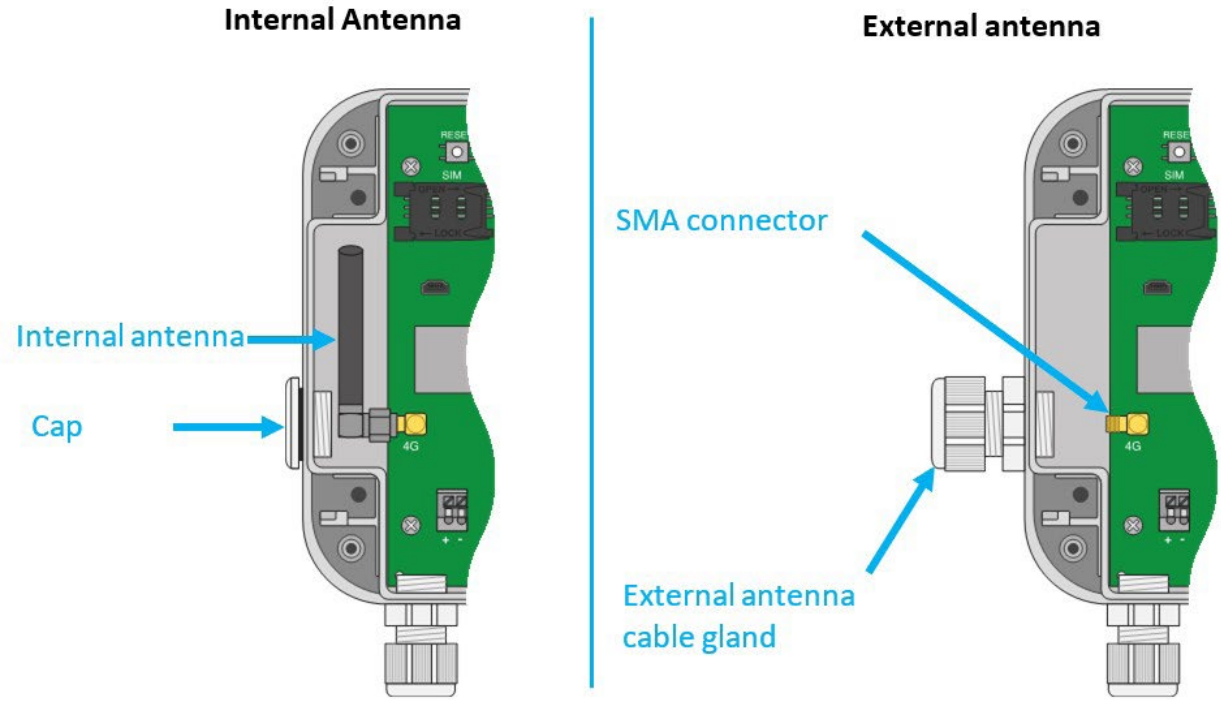
3.2.3 Red celular

El concentrador WebdynEasy integra un módem compatible con redes 3G y 4G.

3.2.3.1 Antena

El concentrador tiene un conector SMA hembra identificado como “4G” en la tarjeta para conectar una antena para el módem. El producto se entrega con una antena interna. Es posible conectar una antena externa al producto. Para ello, debe desatornillar el tapón de la carcasa e instalar un prensaestopas M16*1.5 (no suministrado).

En caso de que el concentrador WebdynEasy se instale en una caja metálica o en una ubicación que no permita una recepción correcta de la señal, se recomienda encarecidamente utilizar una antena remota. Es necesario disponer de una antena compatible con el conector y con las frecuencias utilizadas.



El usuario final debe asegurarse de que su instalación con antenas remotas cumple las normas CEM vigentes.

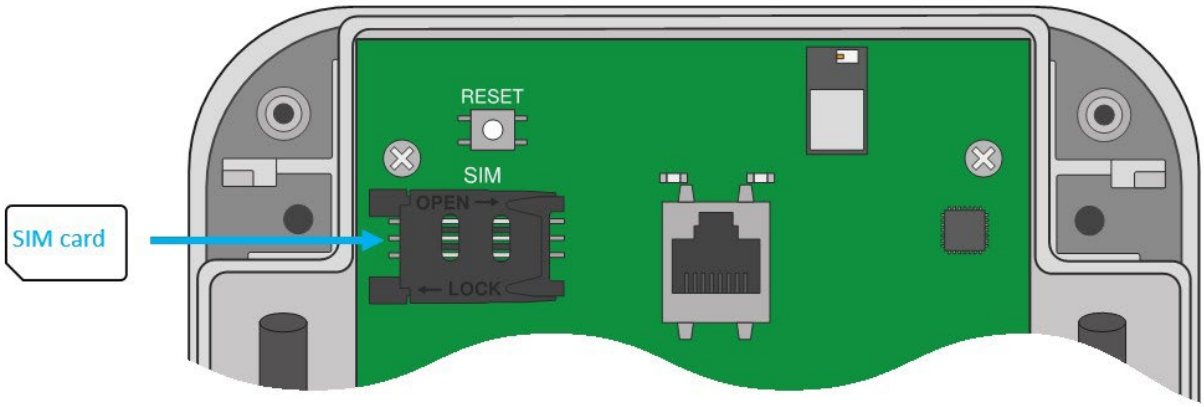
3.2.3.2 Tarjeta SIM

Para utilizar la conexión Módem 3G o 4G y permitir que el concentrador se comunique con el servidor remoto, hay que abrir la carcasa (ver capítulo 3.2.1: “Apertura/Cierre de la carcasa”) e insertar una tarjeta SIM en formato mini-SIM en la ubicación para tarjetas SIM dentro del concentrador.

El concentrador es compatible con todos los operadores del mercado, así como con todas las tarjetas SIM en formato mini-SIM 2FF 25 x 15mm.

Para garantizar el correcto funcionamiento del WebdynEasy, debe insertarse una tarjeta SIM con las siguientes características:

- Posibilidad de recibir y enviar SMS.
- Incluir comunicación 3G y 4G.



Para insertar la tarjeta SIM en el producto, deslice el soporte hacia la derecha (en la dirección OPEN). Inserte la tarjeta SIM en el soporte deslizándola hacia adentro. Luego cierre el soporte deslizándolo hacia la izquierda (en la dirección LOCK).

Webdyn no proporciona ninguna tarjeta SIM. Contacte con un operador M2M que admita la red 3G y LTE-M.

Para conocer la información que debe introducirse para configurar el módem, contacte con el proveedor de su tarjeta SIM.

Por defecto, la configuración del concentrador no requiere un código PIN (PIN Mode: Off). Si desea activar el código PIN del concentrador, es preferible configurarlo antes de insertar la tarjeta SIM. (ver capítulo 4.1.1: Conectividad del concentrador)

Son posibles tres casos:

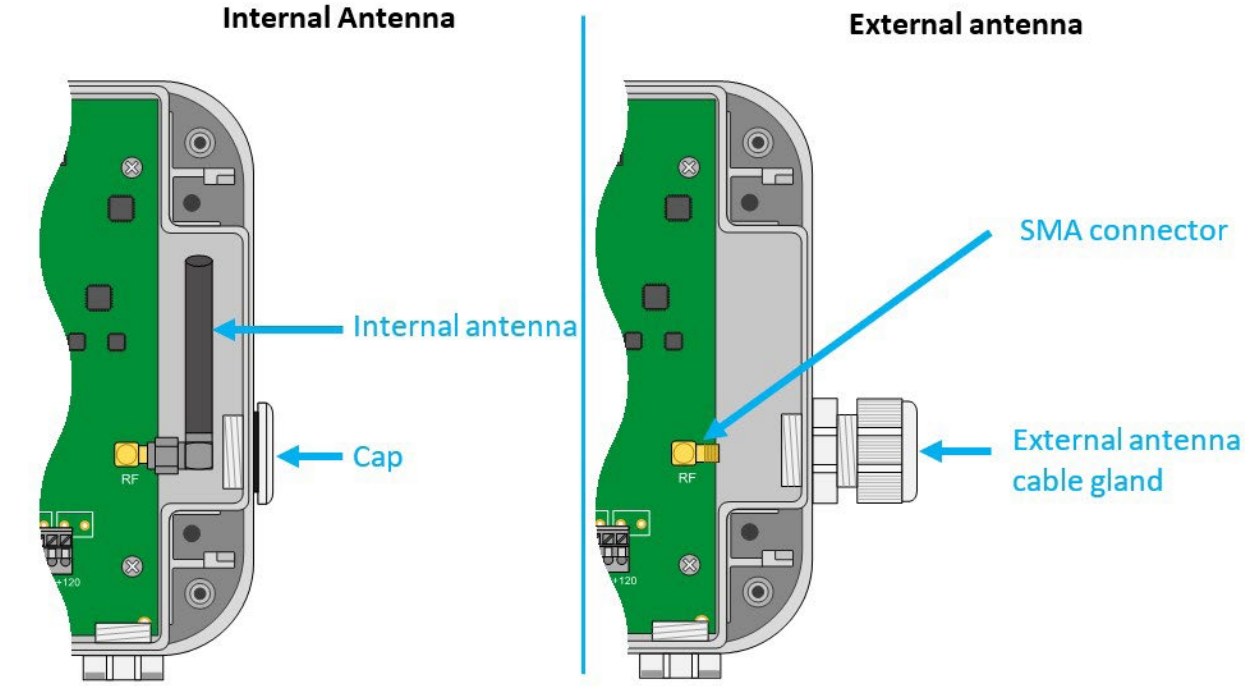
- El código PIN está desactivado: la comunicación módem está activa.
- El código PIN está activado y el código PIN introducido es correcto: la comunicación módem está activa.
- El código PIN está activado y el código PIN introducido es incorrecto: la comunicación módem estará en fallo.

Si la tarjeta SIM tiene un código PIN activado y éste es incorrecto cuando el concentrador se inicia por primera vez, se bloqueará después de 3 intentos. Puede desbloquearla utilizando un teléfono móvil con el código PUK proporcionado por su operador.

3.2.4 LoRa

El concentrador tiene un conector SMA hembra identificado como “RF” en la tarjeta para conectar una antena para la radio. El producto se entrega con una antena interna. Es posible conectar una antena externa al producto. Para ello, debe desatornillar el tapón de la carcasa e instalar un prensaestopas M16*1.5 (no suministrado).

Para optimizar el alcance de radio, es importante instalar la antena de radio lo más alto posible y colocarla con cuidado, evitando los obstáculos en la medida de lo posible. Como prioridad, aléjese de cualquier obstáculo metálico (armario metálico, viguetas, etc.) u hormigón (hormigón armado, muros, etc.), que pueden atenuar significativamente la onda de radio.



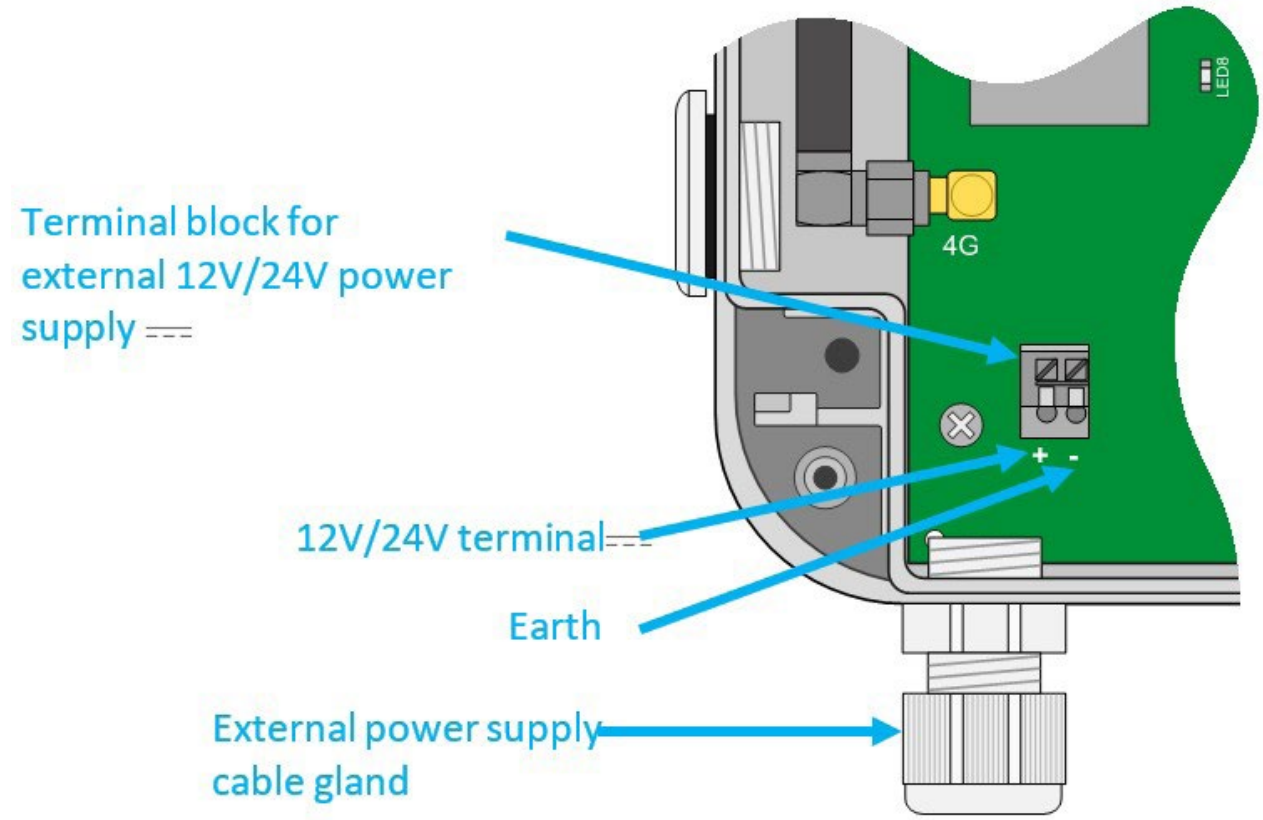
El usuario final debe asegurarse de que su instalación con antenas remotas cumple las normas CEM vigentes.

3.2.5 Conexión

3.2.5.1 Alimentación

El concentrador WebdynEasy debe alimentarse con 12V o 24V DC. La alimentación se realiza a través del bloque de terminales J11 situado en la parte inferior izquierda de la tarjeta.

El usuario final debe utilizar una alimentación certificada CE inferior a 15 vatios. La distancia entre la alimentación y el producto no debe exceder de 3 metros. Es necesario asegurarse de que su instalación cumple los estándares CEM vigentes.



Respete la dirección del cableado de la alimentación.

El consumo del producto es variable en función de su configuración. Asegúrese de que la alimentación utilizada pueda proporcionar una potencia de al menos 10 vatios.

3.2.5.2 Bus RS485/RS422

El bus de comunicación RS485/RS422 se usa solo para modbus en modo RTU, está serigrafiado RS485 en la parte inferior derecha de la tarjeta. Esta interfaz es compatible con Half Duplex (2 cables) y Full Duplex (4 cables).

Si se conectan varios equipos Modbus RTU, debe realizarse un cableado “en serie”. El cable llega a un módulo Modbus y sale hacia el siguiente.

Para garantizar el correcto funcionamiento del bus de datos, un bus RS485 debe terminarse en los dos extremos con un tapón de 120 Ohm. El concentrador WebdynEasy puede encontrarse en el extremo del bus de comunicación RS485 o en el medio del bus. Como el concentrador integra una resistencia de 120 ohmios, dependiendo de la posición del concentrador en el bus puede ser necesario activarlos. (ver cableado)

Para la elección del tipo de cable, hay que considerar 3 casos distintos:

- En instalaciones que requieran longitudes cortas y sin interferencias eléctricas, prever un cable apantallado rígido de 2 pares 6/10.

- En instalaciones mayores con una longitud de cable que no exceda de 500 m, prever un cable apantallado rígido de 2 pares 8/10.
- Cuando la distancia del cable supere los 500 m, y sobre todo en caso de interferencia eléctrica, prever un cable apantallado de 2 pares con una sección de 0,34 mm2.

La longitud máxima del bus RS485 es de 1000 metros.

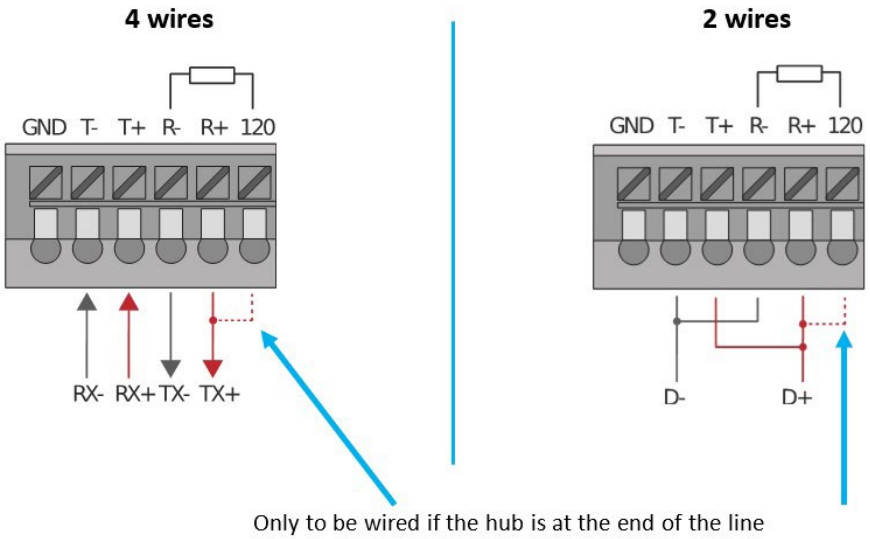
Recomendaciones relativas al cableado del BUS RS485/RS422:

- Los módulos deben conectarse uno tras otro.
- Están prohibidas las conexiones en estrella.
- Los cables deben estar apantallados o blindados, trenzados par a par (ver más arriba: “tipo de cable para la conexión bus RS485”).
- La pantalla o blindaje del cable deben estar conectados al plano de masa de la carcasa del concentrador y no a 0 V (solo conectar un extremo de la pantalla).
- Evite cualquier ida y vuelta en el mismo cable.

Cableado RS485 por el lado del concentrador:

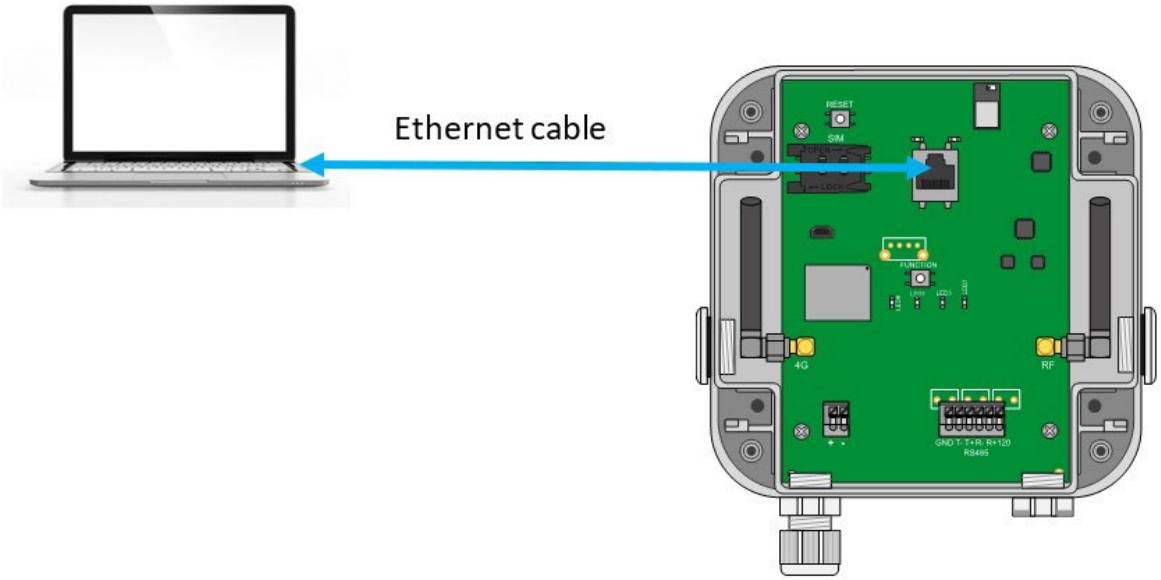
- Pele la funda del cable de comunicación RS485 unos 4 cm.
- Acorte el blindaje hasta la funda del cable.
- Pele los cables unos 6 mm.
- Conecte los conductores al bloque de terminales con la referencia RS485 respetando las asignaciones en su bus de comunicación RS485.

Montaje en RS485/RS422:



3.2.5.3 Ethernet

Para configurar el concentrador, primero hay que abrir la carcasa para poder acceder al conector RJ45 (ver capítulo 3.2.1: “Apertura/Cierre de la carcasa”). Una vez abierto, conectar el concentrador al ordenador con un cable Ethernet.



Es necesario configurar una dirección IP fija en el ordenador en el mismo rango de direcciones IP, y en la misma subred que el concentrador WebdynEasy LoRaWAN.

Los parámetros de configuración IP por defecto del concentrador WebdynEasy LoRaWAN son los siguientes:

Dirección IP: 192.168.1.12

Máscara de subred: 255. 255. 255.0

DHCP: Desactivado

El siguiente paso permite configurar la dirección de red de un PC para acceder al concentrador WebdynEasy LoRaWAN:

Configuración de una segunda dirección IP en el PC:

- En Windows 10, haga clic en Inicio/Configuración/Redes e Internet. Aparece la ventana “Estado de la red”.
- Haga clic en “Ethernet” a la izquierda de la ventana, luego “Centro de redes y recursos compartidos” a la derecha.
- Aparece la ventana “Centro de redes y recursos compartidos”.

- Haga clic en conexiones “Ethernet”. Aparece la ventana “Estado de Ethernet”
- haga clic en “Propiedades”.
- Seleccione “Protocolo de Internet (TCP/IPv4)” y luego haga clic en el botón “Propiedades”.
- Luego haga clic en “Avanzado”.
- En la zona “Dirección IP”, haga clic en “Agregar”.
- Introduzca la dirección IP 192.168.1.xxx (xxx entre 1 y 254 y diferente a 12) y la máscara de subred 255. 255. 255.0.
- Haga clic en “Agregar”.
- Para validar los ajustes, haga clic en Aceptar en cada una de las tres ventanas.
- Cierre la ventana “Conexión de red y acceso remoto”.

Ahora es posible cambiar fácilmente la configuración del concentrador a través de su interfaz web integrada utilizando el navegador web del ordenador. (ver capítulo 5.1.1: “Conectividad del concentrador”).

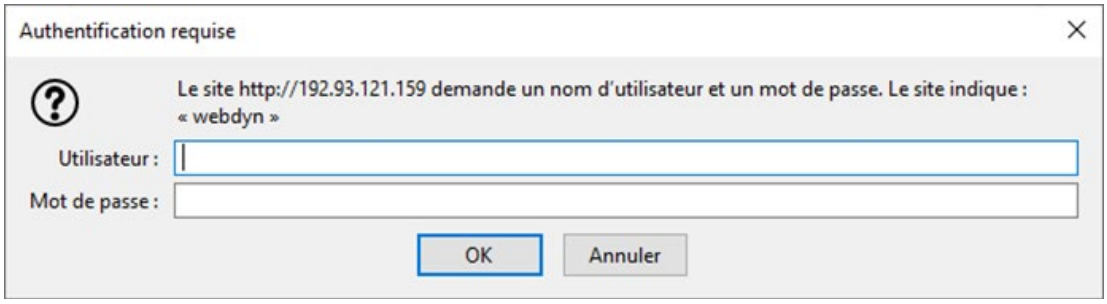
4. Configuración

La primera configuración del concentrador WebdynEasy LoRaWAN se realiza a través de la interfaz web integrada en el producto.

4.1 Interfaz web integrada

Para acceder a la interfaz web integrada del concentrador, siga las etapas siguientes:

- Inicie el navegador web: la interfaz web es compatible con las últimas versiones de navegadores: Firefox, Chrome y Edge. Las versiones anteriores pueden funcionar, pero ya no son compatibles (por ejemplo, IE 7).
- Introduzca la dirección IP del concentrador en su navegador web (por defecto, la dirección es: http://192.168.1.12) para acceder a la página de inicio de WebdynEasy LoRaWAN.
- Debe aparecer una ventana de identificación:

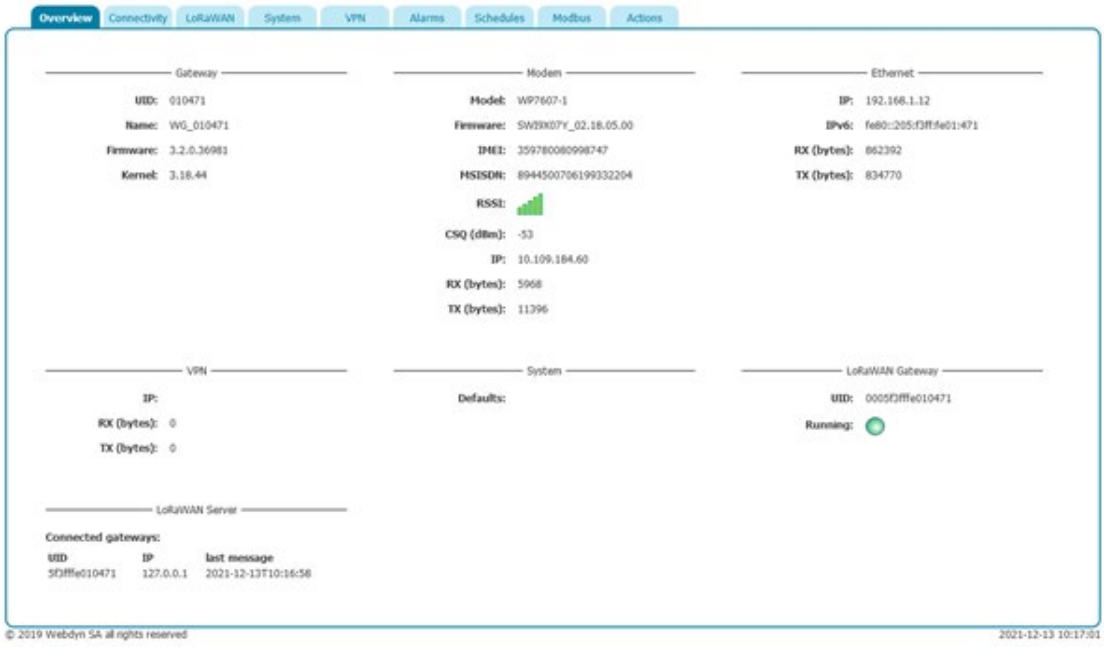


Introduzca su nombre de usuario y contraseña:

Nombre de usuario	Contraseña	Restricciones
admin	high	Ninguna
install	medium	Sistema, LoRaWAN, Modbus, Acciones Schedules en solo lectura
data	low	Solo acciones

Contraseña: para securizar el acceso al concentrador, se recomienda encarecidamente cambiar las contraseñas por defecto después de la primera configuración. Las contraseñas se modifican utilizando el archivo de configuración XML (ver: “Anexo A: Variables “).

- Se muestra la página de inicio:



La pestaña “Overview” proporciona una descripción general del funcionamiento del WebdynEasy LoRawan.

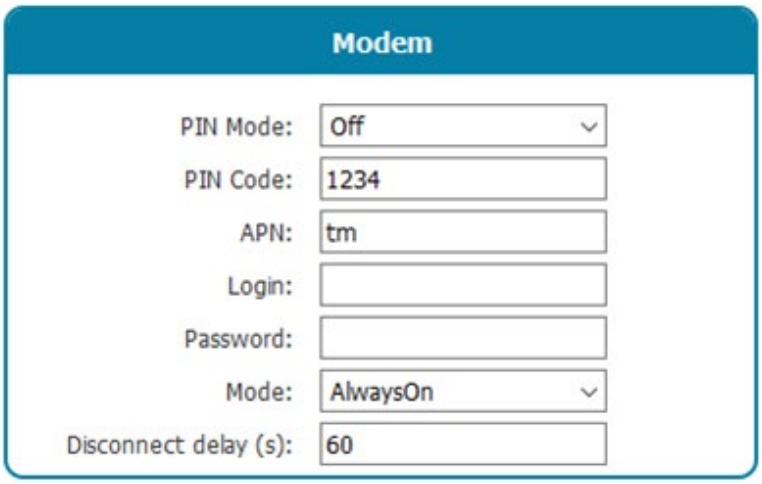
Si se accede a las páginas web durante la fase de inicio del concentrador, se muestra el logotipo 

. Espere a que el concentrador se haya iniciado completamente para acceder a las páginas web.

4.1.1 Conectividad del concentrador

La pestaña “Connectivity” permite configurar el concentrador para que se comunique con el servidor remoto.

4.1.1.1 Módem

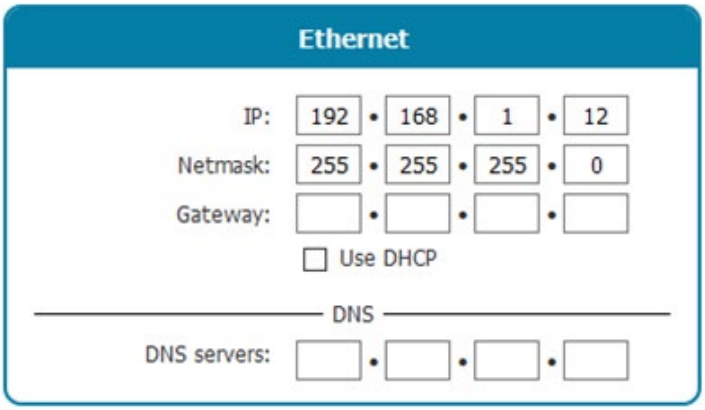


Parámetros	Descripción
Pin Mode	Off : El código PIN de la tarjeta SIM debe estar desactivado
	Manual: El código PIN de la tarjeta SIM debe indicarse en la casilla PIN Code
PIN Code	Código PIN de la tarjeta SIM que se debe indicarse si se selecciona Manual en PIN Mode
APN	Nombre de la APN de su operador de telefonía móvil (necesario para una conexión IP)
Login	Nombre de usuario de su operador de telefonía móvil (opcional según el operador)
Password	Contraseña de su operador de telefonía móvil (opcional según el operador)

Mode	OnDemand: El concentrador solo establece la conexión cuando necesita comunicarse con el servidor remoto. La corta cuando finaliza la transferencia de datos tras un tiempo configurable en Disconnect delay.
	AlwaysOn: El módem está aún conectado. El concentrador utiliza constantemente el módem para todas las comunicaciones IP.
	AlwaysOff: Este modo debe utilizarse en caso de conexión al servidor remoto a través de Ethernet, pero con una tarjeta SIM insertada en el concentrador. La conexión nunca se realiza a través del módem, pero el concentrador puede recibir SMS entrantes y enviar SMS.
Disconnect delay (s)	Valor en segundos del tiempo de espera en modo OnDemand entre el fin de intercambio de datos y el fin de la conexión.

Consulte a su operador de telefonía móvil para obtener la información (APN, inicio de sesión, contraseña) de su tarjeta SIM.

4.1.1.2 Ethernet

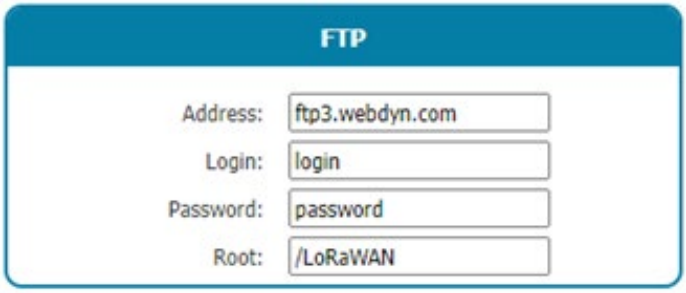


Parámetros	Descripción
IP	Dirección IP a la que puede acceder el concentrador WebdynEasy LoRaWAN a través de la red Ethernet.
Netmask	Máscara de subred de su red Ethernet. Esta máscara limita la red Ethernet a direcciones IP definidas y separa los rangos de red entre sí.
Gateway	Dirección de la pasarela de su red Ethernet. La dirección de la pasarela es la dirección IP del dispositivo que establece la conexión a Internet. En general, la dirección introducida aquí es la de su router ADSL/fibra.

Use DHCP	Tiene la opción de obtener la configuración de Ethernet automáticamente si la infraestructura de red lo permite. En este caso, seleccione el modo dinámico y consulte la configuración de su servidor DHCP para conocer la dirección IP de su concentrador.
DNS servers	Lista de servidores DNS. El servidor DNS (Domain Name System) traduce las direcciones de Internet explícitas (por ejemplo, www.webdyn.com) en las direcciones IP correspondientes. Introduzca aquí las direcciones de los servidores DNS que ha recibido de su proveedor de acceso a Internet (FAI). También puede introducir la dirección IP de su router. También puede utilizar el DNS de Google: "8.8.8.8"

El concentrador solo puede utilizar la conexión Ethernet para acceder al servidor si la conexión a través del módem está desactivada (“off” o “alwaysoff”). De lo contrario, el concentrador intentará conectarse a través de la conexión del módem.

4.1.1.3 FTP



Parámetros	Descripción
Address	Dirección IP o nombre del servidor FTP remoto (puerto por defecto: 21). Posibilidad de modificar el puerto FTP agregando ": ", y luego el número de puerto
Login	Nombre de usuario utilizado por el concentrador para conectarse al servidor FTP remoto
Password	Contraseña utilizada por el concentrador para conectarse al servidor FTP remoto
Root	Carpeta raíz en el servidor FTP remoto

El árbol de carpetas en el servidor FTP remoto debe crearse antes de cualquier conexión FTP. (ver capítulo 6.1.1.1: “El servidor FTP: Configuración”).

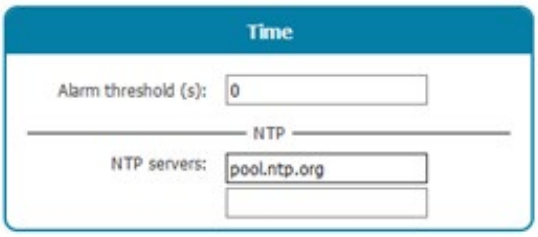
4.1.1.4 Servicios web

Parámetros	Descripción
URL	Dirección IP o nombre del servidor web remoto (Puerto predeterminado: 80). Posibilidad de modificar el puerto del servidor web añadiendo ":" y luego el número de puerto.
Login	Nombre de usuario utilizado por el concentrador para conectarse al servidor web remoto.
Password	Contraseña utilizada por el concentrador para conectarse al servidor web remoto.
Proxy	Dirección IP o nombre de host del proxy (Puerto predeterminado: 1080). Posibilidad de modificar el puerto proxy agregando ":" y luego el número de puerto. El proxy es opcional si no se utiliza, el campo vacío debe estar vacío.
Trust model	Verificación de certificados de autenticación (solo para conexiones HTTPS seguras): • Verify peer: Verificación de certificados de autenticación. • Compañero de confianza: acepta todos los certificados de autenticación (no recomendado).
Upload POST path	Ruta en el servidor web remoto.

4.1.1.5 MQTT

Parametres	Description
Adress	IP address or name of the remote web server (Default port: 1883) Possibility to modify the port of the mqtt server by adding ":" then the port number
Client ID	Client's MQTT identifier
Login	Username used by the hub to connect to the remote MQTT server
Password	Password used by the hub to connect to the remote MQTT server
Keepalive interval (s)	Time in seconds for sending keep-alive frame
Topic	Topic of MQTT messages used
Trust model	Verification of authentication certificates (only for MQTTS secure connections): • Verify peer: Verification of authentication certificates. • Trust peer: Accepts all authentication certificates (not recommended)

4.1.1.6 NTP

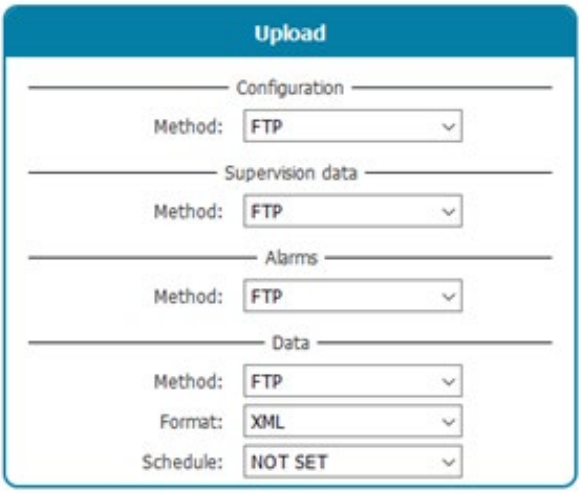


Parámetros	Descripción
Alarm threshold (s)	Diferencia en segundos entre la hora del concentrador y la hora de sincronización NTP más allá del cual se emite una alarma
NTP servers	Direcciones de los servidores NTP utilizados para la sincronización del reloj del concentrador

En la primera conexión se realiza la sincronización NTP y la siguiente sincronización NTP se

realizará en otra conexión tras un tiempo mínimo. El tiempo mínimo entre las sincronizaciones NTP puede configurarse mediante la variable “min_sync_interval.” en segundos.

4.1.1.7 Upload



The concentrator can deposit the following data on the remote server:

Nombres	Descripción	Formato
Configuration	Datos de configuración del concentrador	• XML
Supervision data	Datos de monitoreo del concentrador	• XML
Alarms	alarmas	• XML
Data	Datos LoRaWAN y/o modbus	• XML • JSON

Para cada tipo de datos, el concentrador puede depositar los datos mediante:

- FTP
- Servicio web

Si los comandos son enviados por Web Service, el concentrador responde a los comandos a través de alarmas. En este caso, es necesario configurar las alarmas en Web Service.

La transmisión de datos debe asociarse a un Schedule introduciendo su identificador único configurado (ver capítulo 4.1.5: “Schedules”).

Consulte el capítulo 5.2: “La configuración” para conocer el formato y contenido de los archivos de configuración, supervisión, alarma y datos

El árbol de carpetas en el servidor FTP remoto debe crearse antes de cualquier transmisión de archivos. (ver capítulo 6.1.1.1: “El servidor FTP: Configuración”).

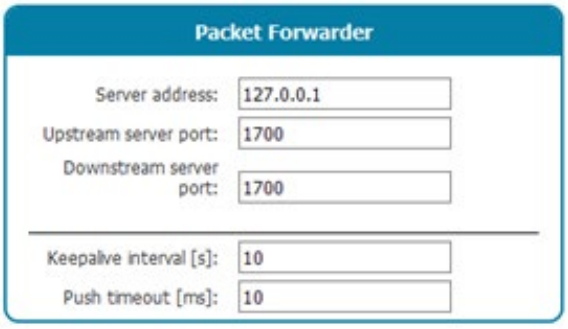
4.1.2 LoRaWAN

La pestaña “LoRaWAN” permite configurar el Packet Forwarder y el servidor LoRaWAN. Estas 2 partes son completamente independientes. El Packet Forwarder puede utilizarse con un servidor remoto, y el servidor LoRaWAN integrado puede utilizar un Packet Forwarder externo.

4.1.2.1 Packet Forwarder

En modo Packet Forwarder, WebdynEasy LoRaWAN adquiere la función de pasarela. La pasarela ésta permanentemente en escucha en la interfaz de radio LoRa y transmite todas las tramas recibidas a través de una conexión IP al servidor LoRaWAN (remoto o integrado).

Para que el Packet Forwarder funcione, debe establecer una conexión IP permanente con el servidor a través de su interfaz Ethernet o Módem en modo AlwaysOn.



Parámetros	Descripción
Server address	Dirección IP o nombre del servidor LoRaWAN. Para utilizar el servidor LoRaWAN integrado del concentrador, debe utilizarse la siguiente dirección: "127.0.0.1"
Upstream server port	Número de puerto UDP saliente del Packet Forwarder
Downstream server port	Número de puerto UDP entrante del Packet Forwarder

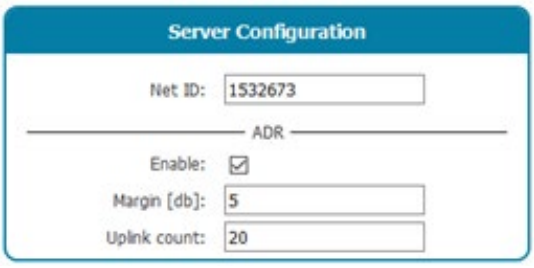
Keepalive interval [s]	Tiempo en segundos para enviar una trama de mantenimiento de conexión
Push timeout [ms]	Tiempo máximo de espera en milisegundos para el reconocimiento de la trama enviada al servidor LoRaWAN.

El Packet Forwarder admitido es el de Semtech.

4.1.2.2 Servidor LoRaWAN

El servidor LoRaWAN gestiona los sensores LoRaWAN como una red privada. Incluye todas las funciones de la red LoRaWAN (pasarela, servidor LoRWAN y servidor de aplicaciones). Todos los datos recibidos se almacenan en archivos, y con cada conexión FTP se descargan todos los datos disponibles.

Para usar el Packet Forwader del concentrador, introduzca en “Server address “ la siguiente dirección IP: “127.0.0.1”. Compruebe igualmente que los puertos del servidor (“Upstream server port “ y “Downstream server portt”) están en 1700.



Parámetros	Descripción
Net ID	Valor hexadecimal de 24 bits utilizado para identificar las redes LoRaWAN. Si introduce el valor 0, cuando se reinicia el concentrador éste utilizará su NetID de fábrica.
Enable	Marque para activar la ADR (Adaptive Data Rate)
Margin [dB]	Margen en dB para calcular la ADR entre 1 y 30
Uplink count	El número de Uplink necesarios para la ADR, comprendido entre 1 y 65535

Para optimizar las pilas de los sensores y el ancho de banda de LoRAWAN, se recomienda encarecidamente dejar activada la ADR y la configuración por defecto del Margin y uplink count.

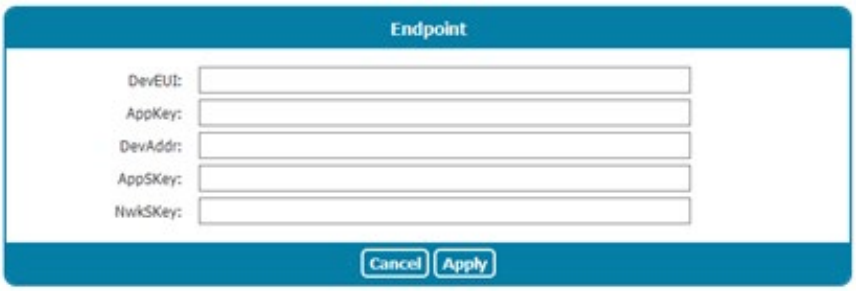
Para el cálculo de la ADR, el concentrador necesita al menos 20 uplinks, es decir, la variable

Uplink Count se utiliza después de los primeros 20 uplinks recibidos por el concentrador antes de enviar comandos ADR al sensor LoRaWAN.

Sensor LoRaWAN:

El servidor soporta los 2 modos de activación:

- ABP (Activation By Personalization): deben introducirse los parámetros DevAddr, NwkSKey y AppSKey.
- OTAA (Over The Air Activación): deben introducirse los parámetros DevEUI y AppKey, las teclas AppSKey y NwkSKey se generan y se guardan en el momento del JOIN.

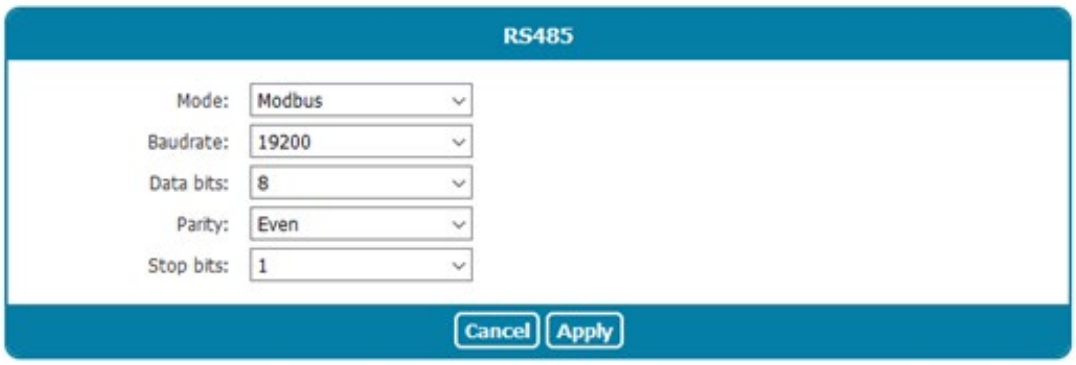


Parámetros	Descripción	ABP	ABP
DevEUI	Identificador único del sensor (EUI64) en hexadecimal de 8 bytes	vacíos	•
AppKEY	Clave de cifrado hexadecimal de 16 bytes que utiliza la red para derivar claves de sesión.	vacíos	•
DevAddr	Dirección del sensor en hexadecimal de 4 bytes	•	auto
AppSKey	Clave de cifrado entre el sensor y el servidor aplicativo en hexadecimal de 16 bytes	•	auto
NwkSKey	Clave de cifrado entre el sensor y el servidor LoRaWAN en hexadecimal de 16 bytes	•	auto

El servidor integrado del concentrador no utiliza la AppEUI.

Los datos de los sensores LoRaWAN se transmiten en formato XML (ver capítulo 5.1.1.5: “Upload) a la carpeta DATA del servidor FTP remoto (ver capítulo 6.3”Los datos”).

4.1.3 Sistema



Cuando el protocolo Modbus está habilitado en el puerto RS485, deben definirse los parámetros del puerto de serie.

Parámetros	Descripción
Mode	Off : RS485 desactivado Modbus: RS485 activado en modo Modbus
Baudrate	4800 9600 **19200** (valor por defecto) 38400 57600 115200
Data bits	5 6 7 **8** (valor por defecto) 9
Parity	None Odd **Even** (valor por defecto)
Stop bits	**1** (valor por defecto) 2

4.1.4 VPN

El concentrador admite VPN desde OpenVPN V2.5.4 (https://openvpn.net/).

Parámetros	Descripción

Enable	Marque para habilitar VPN
Protocol	Protocolo de comunicación utilizado: • tcp • udp
Address	Dirección IP o nombre del servidor VPN
Port	Puerto del servidor VPN (generalmente 1194)
Cipher	Algoritmo de cifrado de paquetes de datos (opcional). Lista disponible en OpenVPN (comando “openvpn --show-ciphers”).
Auth	Algoritmo hash HMAC para autenticar paquetes de datos. Si se ingresa “TLS Auth”, el algoritmo hash también se aplica a los paquetes de control. Si el campo está vacío, el valor utilizado por defecto es “SHA1” (opcional). Lista disponible en OpenVPN (comando “openvpn --show-digests”).
CA	Certificado raíz de CA. En formato de archivo PEM
Cert	Certificado firmado por el cliente local. En formato de archivo PEM
Key	Clave privada del cliente local. En formato de archivo PEM

Seguridad del canal:

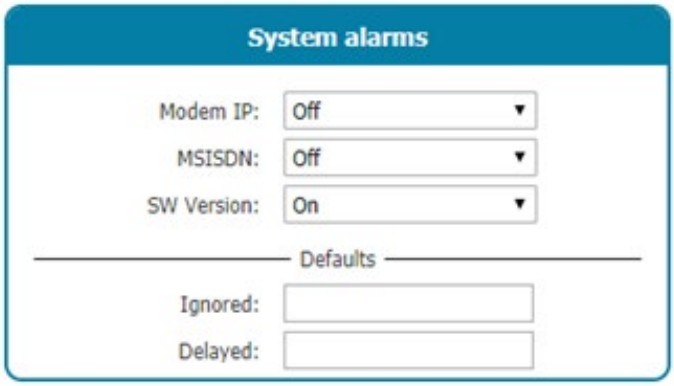
Parámetros	Descripción
Method	Lista de métodos para la seguridad del canal de control: • ninguno Ninguno • tls-auth: clave estática utilizada para el algoritmo hash HMAC en paquetes de control. • tls-crypt: Igual que tls-auth, pero también cifra el canal de control TLS. • tls-crypt-v2: Igual que el anterior, pero usa una clave por cliente en lugar de una clave de grupo compartida.
Key	Clave para la seguridad del canal de control. En formato de archivo PEM.

 Para averiguar qué información ingresar para la configuración de VPN, comuníquese con el administrador de red del servidor VPN.

La configuración de un servidor NTP es obligatoria para el uso de una VPN para verificar la validez de los certificados. (ver capítulo 4.1.1.5: “NTP”).

4.1.5 Alarmas

El concentrador puede generar alarmas de sistema.



Las alarmas de sistema son de 3 tipos:

- Modem IP: alarma generada si la dirección IP obtenida durante una conexión a través del Módem cambia.
- MSISDN: alarma generada si se cambia la tarjeta SIM insertada en el concentrador.
- SW Version: alarma generada si cambia la versión del firmware o del núcleo (tras una actualización).

Cada fuente de alarma puede activarse individualmente y transferirse inmediatamente al servidor remoto (On) o en la siguiente conexión (Delayed).

Las alarmas de disfuncionamiento del concentrador (“Default “) se envían por defecto inmediatamente al servidor remoto. No obstante, es posible desactivarlas (“Ignored”) o posponer su envío (“Delayed “) a la siguiente conexión. Para ello, hay que introducir sus códigos en los campos correspondientes al comportamiento deseado.

A continuación se muestran los códigos y fallos disponibles:

Código	Descripción
D_MODEM	Fallo del módem
D_MODEM_SIM_MISS	Falta la tarjeta SIM
D_MODEM_SIM_CODE_FAIL	Error de código SIM

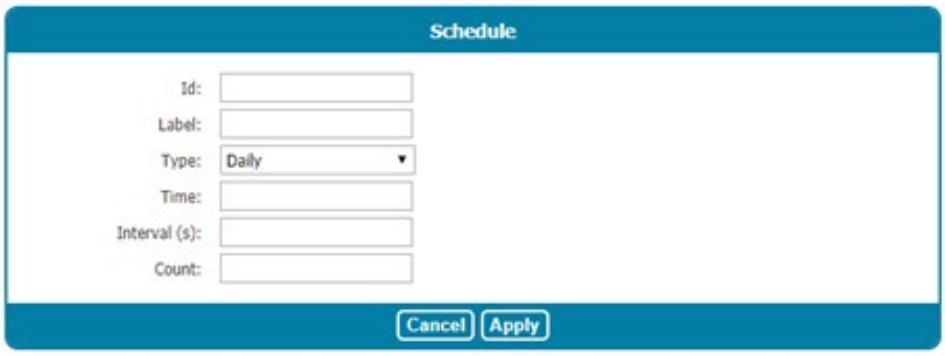
D_MODEM_PUK	Tarjeta SIM bloqueada
D_MODEM_REG_DENIED	Registro de red denegado

En la casilla Ignored pueden enumerarse los códigos de fallo ignorados por el concentrador. Si se introducen varios códigos de fallo, deben estar separados por el carácter ‘,’ (coma).

En la casilla Delayed pueden enumerarse los códigos de fallo transferidos a la siguiente conexión por el concentrador. Si se introducen varios códigos de fallo, deben estar separados por el carácter ‘,’ (coma).

4.1.6 Schedules

El schedule está a cargo de todas las tareas periódicas. La configuración del schedule consta de una lista de programas. Cada uno de estos schedules tiene un identificador único que se utiliza para vincular una o más tareas a un schedule. Se pueden utilizar de forma independiente para activar la recopilación y descarga de datos.



Cada schedule se configura de la siguiente manera:

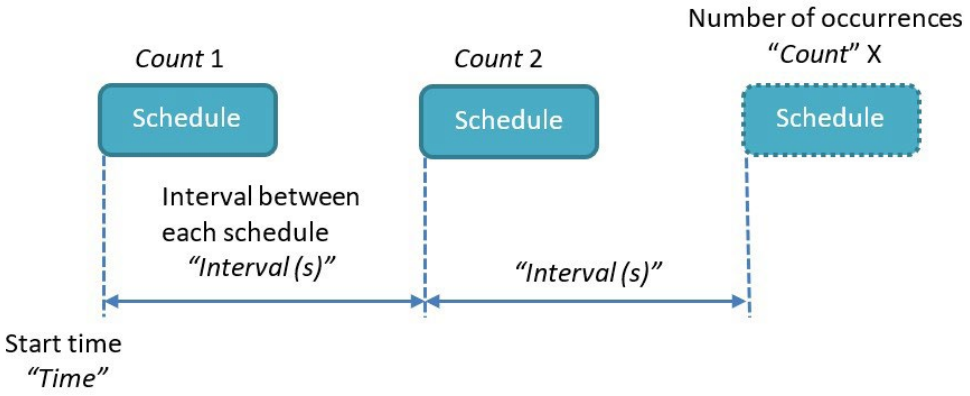
Parámetros	Descripción
Id	Identificador único del schedule. El identificador debe ser un número entero. (entre 1 y 2 147 483 647)
Label	Nombre solo informativo del schedule
Type	Daily, Weekly, Monthly, Yearly o Follower : ver la descripción a continuación
Time	Hora de la primera ocurrencia en formato "HH:MM:SS" (no se utiliza para programas de tipo "Yearly")
Day of Week	Número del día de la semana de la primera ocurrencia (1 = lunes, 7 = domingo) (se utiliza solo para los schedules de tipo "Weekly")

Day of Month	Número del día del mes de la primera ocurrencia (se utiliza solo para los schedules de tipo "Monthly")
Date & Time	Fecha y hora de la primera ocurrencia en un periodo determinado (se usa solo para los schedules de tipo "Yearly")
Interval (s)	Intervalo entre ocurrencias (en segundos)
Count	Número de ocurrencias (mínimo 1)
Parent	Referencia al schedule principal para un schedule de tipo "Follower" .

Configuración de los diferentes tipos de schedules:

- Schedule de tipo “Daily”:

Cada día, la primera ocurrencia viene dada por la hora introducida en el campo “Time”. El número de eventos durante el día viene dado por el campo “Count “ y el intervalo entre cada evento por el campo “Interval “



El formato “Time “ es el siguiente: HH:MM:SS (por ejemplo, 09:30:00)

El valor de “Count “ está entre 1 y 2 147 483 647

El valor de “Interval “ está entre 0 y 2 147 483 647

“Count”: si el schedule debe iniciarse a lo largo de todo el día a intervalos regulares, puede introducirse el valor máximo (es decir, 2 147 483 647) para el “Count “.

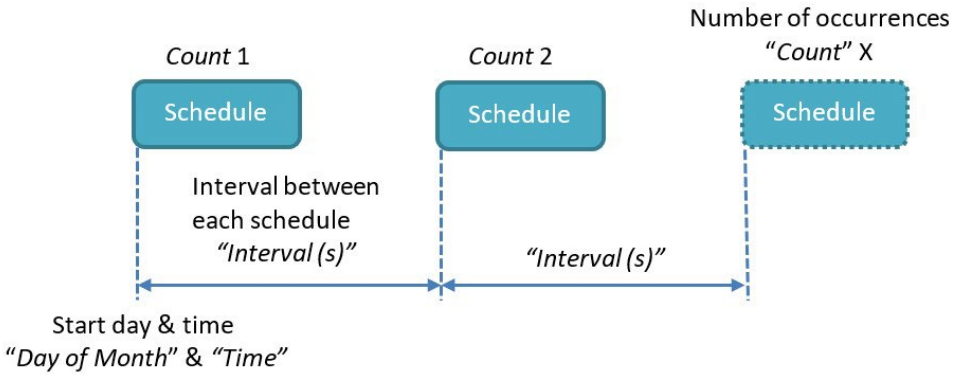
Ejemplo concreto:

Necesidad	Tipo	Time	Day of Week	Day of Month	Date & Time	Interval (s)	Count

Todos los días a las 14:00:00	Daily	14:00:00		0	1

- Schedule de tipo Weekly:

Cada semana, la primera ocurrencia viene dada por el día de la semana introducido en el campo “Day of week” y la hora introducida en el campo “Time” .



El formato “Day of week “ está comprendido entre lunes y domingo.

El formato “Time “ es el siguiente: HH:MM:SS (por ejemplo, 09:30:00)

El valor de “Count “ está entre 1 y 2 147 483 647

El valor de “Interval “ está entre 0 y 2 147 483 647

“Count”: si el schedule debe activarse a lo largo de toda la semana a intervalos regulares, puede introducirse el valor máximo (es decir, 2 147 483 647) para el “Count “.

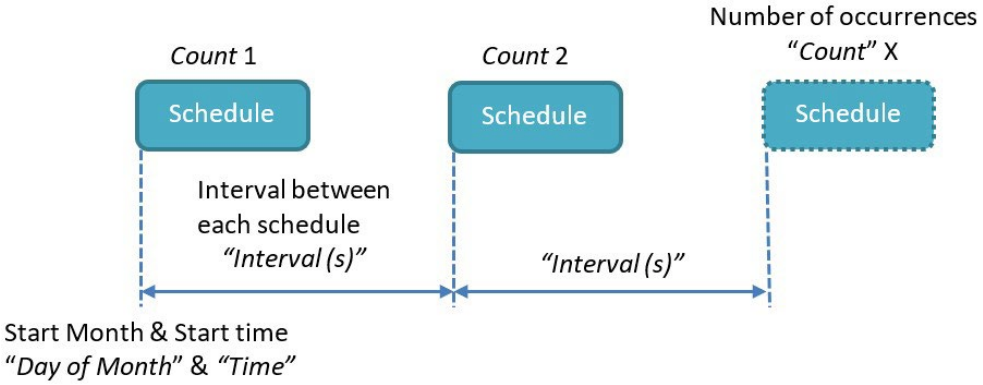
Ejemplo concreto:

Necesidad	Tipo	Time	Day of Week	Day of Month	Date & Time	Interval (s)	Count
Todos los martes a las 15:00:00	Weekly	15:00:00	Tuesday			0	1

Cada hora entre las 8:00 y las 18:00 todos los martes	Weekly	08:00:00	Tuesday		3600	11

- Schedule de tipo Monthly:

Cada mes, la primera ocurrencia viene dada por el número de día del mes introducido en el campo “Day of month” y la hora introducida en el campo “Time”.



El formato “Day of Month “ está comprendido entre 1 y 31

El formato “Time “ es el siguiente: HH:MM:SS (por ejemplo, 09:30:00)

El valor de “Count “ está entre 1 y 2 147 483 647

El valor de “Interval “ está entre 0 y 2 147 483 647

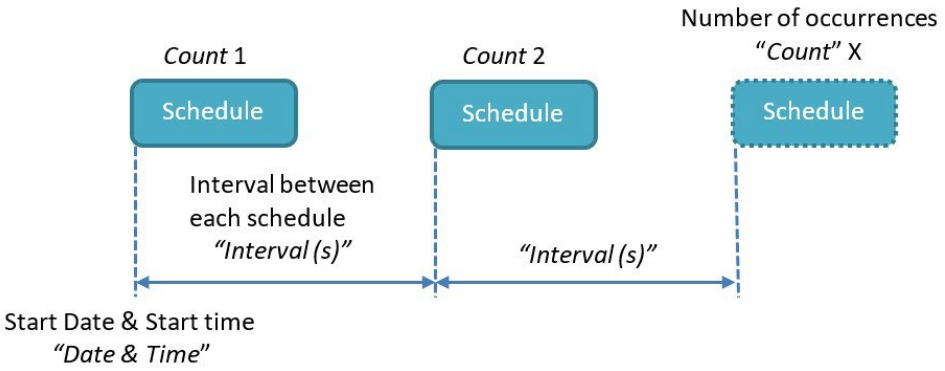
“Count”: si el schedule debe iniciarse a lo largo de todo el mes a intervalos regulares, puede introducirse el valor máximo (es decir, 2 147 483 647) para el “Count “.

Ejemplo concreto:

Necesidad	Tipo	Time	Day of Week	Day of Month	Date & Time	Interval (s)	Count
Todos los 2º días del mes a las 00:00:00	Monthly	00:00:00		2		0	1

- Schedule de tipo Yearly:

Cada año, la primera ocurrencia viene dada por la fecha introducida en el campo “Date & Time”.



El formato “Date & Time” es el siguiente: AAAA-MM-DDTHH:MM:SS (ejemplo, para una primera ocurrencia el 11 de febrero de 2019 a las 13:00: Time = 2019-02-11T13:00:00).

El valor de “Count “ está entre 1 y 2 147 483 647

El valor de “Interval “ está entre 0 y 2 147 483 647

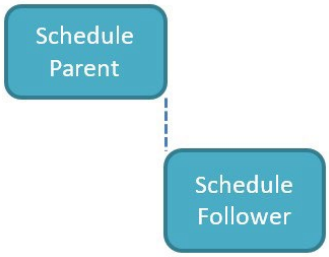
“Count”: si el schedule debe activarse a lo largo de todo el año a intervalos regulares, puede introducirse el valor máximo (es decir, 2 147 483 647) para el “Count “.

Ejemplo concreto:

Necesidad	Tipo	Time	Day of Week	Day of Month	Date & Time	Interval (s)	Count
Cada 2 horas entre las 8:00 y las 20:00 el 31 de diciembre	Yearly				2019-12-31 T08:00:00	7200	7

- Schedule de tipo Follower:

Se activará un schedule de tipo “Follower” después del final de cada ocurrencia del schedule de referencia. El schedule “Parent” no puede ser del tipo “Follower”.



Este tipo permite activar, por ejemplo, una transmisión de datos al servidor remoto tras completar la recopilación de datos prevista.

Ejemplo concreto:

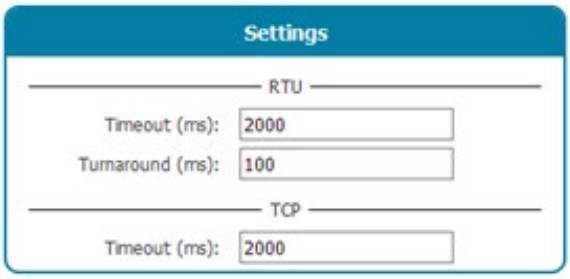
Usted desea recopilar los datos de todos los módulos Modbus una vez al día a medianoche y transmitirlos inmediatamente después. Puede configurar un schedule de tipo “Daily” para la recopilación de datos y otro schedule de tipo “Follower” vinculado al primer schedule para transmitirlos.

4.1.7 Modbus

El concentrador WebdynEasy LoRaWAN es exclusivamente Maestro Modbus RTU y TCP.

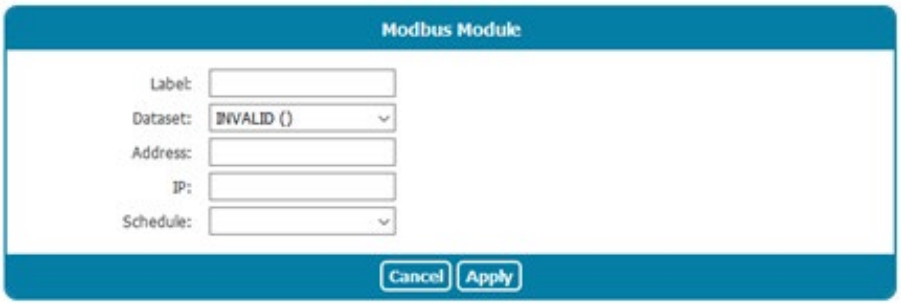
Si se utilizan esclavos Modbus RTU, el protocolo Modbus debe activarse en el puerto RS485/ RS422 (ver capítulo 5.1.3: “Sistema”).

En la pestaña “Modbus” de la interfaz web local, usted puede configurar los tiempos de respuesta máximos para los protocolos Modbus RTU y TCP.



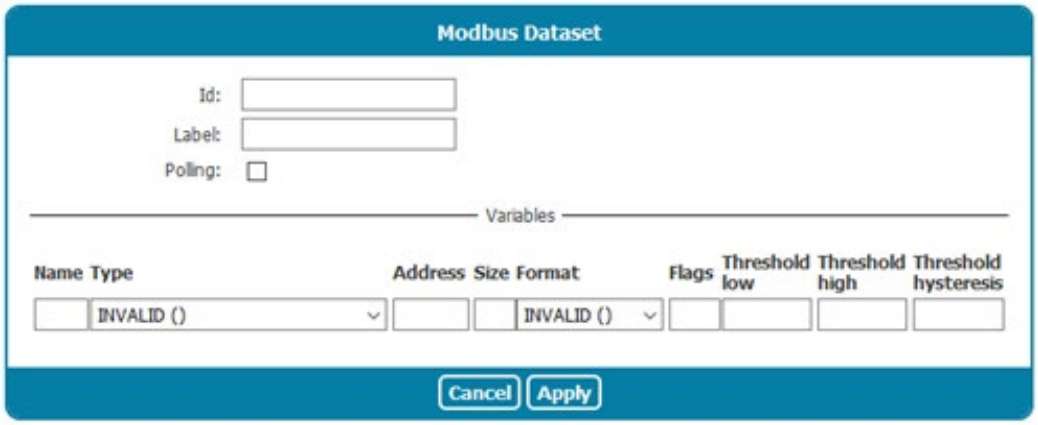
Parámetros	Descripción
RTU	
Timeout (ms)	Tiempo de espera de respuesta Modbus RTU en ms
Turnaround (ms)	Tiempo de respuesta Modbus RTU en ms
TCP	
Timeout (ms)	Tiempo de espera de respuesta Modbus TCP en ms

Un esclavo Modbus se define con una etiqueta, un conjunto de datos (dataset), una dirección Modbus y un schedule. En el caso de un esclavo Modbus TCP, se requiere una dirección IP.



Parámetros	Descripción
Label	Nombre únicamente informativo
Dataset	Identificador del dataset asociado (lista de conjuntos de datos declarada)
Address	Dirección Modbus (de 1 a 247)
IP	Dirección IP (vacía para los equipos RTU)
Schedule	Identificador del schedule (lista de schedules declarada)

Un conjunto de datos define las variables disponibles en un esclavo Modbus y cómo recuperarlas. Configuración de un dataset:



Parámetros	Descripción
Id	Identificador único del conjunto de datos Modbus (entero)
Label	Nombre del conjunto de datos (solo informativo)
Polling	Interrogación de los esclavos Modbus en modo continuo

Configuración de variables, siendo cada variable definida por los siguientes parámetros:

Parámetros	Descripción
Name	Nombre de la variable (solo informativo)
Type	Tipo de variable: • Coil (0x1/0x5,0xF) • Discrete input(0x2) • Holding register (0x3/0x6,0x10) • Input register (0x4)
Address	Dirección de registro extendido de 16 bits
Size	Tamaño en bits para las Discrete inputs y Coils, y en bytes para los Input y Holding registers

Format	Formato de la variable: • Raw (dato bruto) • Boolean (boleano: 0 o 1) • Integer (entero) • Float (cifra con coma) • ASCII (texto)
Flags	Lista de opciones aplicables: (opcional) • cmd_only • little_endian • no_opt • signed • is_status • is_alarm
Threshold low	Nivel de umbral bajo (opcional)
Threshold high	Nivel de umbral alto (opcional)
Threshold hysteresis	Histéresis aplicada a los dos umbrales (opcional)

La variable “Polling” permite activar la interrogación en modo continuo del esclavo Modbus. Cuando está desactivada, solo se interroga al esclavo Modbus cuando se activa el schedule asociado.

El tipo de variable define el código de función que se utilizará para leer o escribir la variable. Ver la tabla siguiente:

Tipo	Descripción	Lectura (múltiple)	Escritura (única)	Escritura (múltiple)
S0	Coil	0x01	0x05	0x0F
S1	Discrete input	0x02	-	-
S3	Input register	0x04	-	-
S4	Holding register	0x05	0x06	0x10

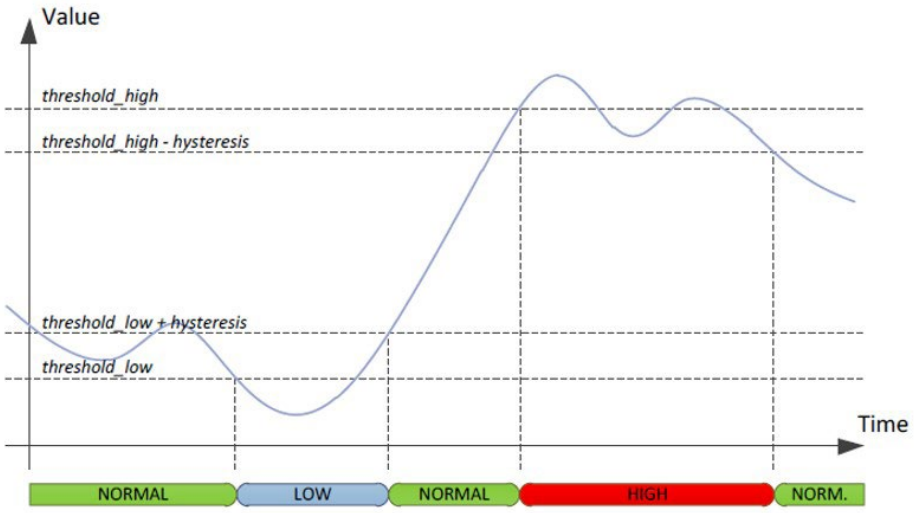
Los formatos disponibles son los siguientes:

Formato	Descripción	Coil	Register
raw	Datos representados como: • cadena binaria para los “Discrete input “ y los “Coils” • cadena hexadecimal para los “registers”	X	X
boolean	Booleano verdadero o falso	X	
integer	Número entero de 8, 16 o 32 bits		X
float	Cifrado de coma flotante de 16 o 32 bits (IEEE 754)		X
ascii	Cadena de caracteres ACSII		X

El campo “Flag” puede completarse con una o más opciones. En caso de opciones múltiples, las opciones deben estar separadas por una coma “,”. A continuación se muestra la lista de opciones disponibles.

Flag	Descripción
cmd_only	El dispositivo Modbus no leerá la variable, pero puede escribirse.
little_endian	Interpreta los registros en little-endian
no_opt	Se utilizará una solicitud Modbus dedicada para leer esta variable
signed	La variable contiene un valor con signo
is_status	Indica que la variable contiene un estado de información
is_alarm	Cualquier modificación de la variable de estado activará una alarma

Cuando se define la opción “is_status”, o se define al menos un umbral, la variable se considera como variable de estado. Es decir, en caso de cambio de estado, el valor de la variable se guarda en el archivo de datos. A continuación se muestra un esquema que describe los cambios de estado en función de los umbrales y la histéresis.



Si la variable es una variable de estado y la opción “is_alarm” está presente, se genera un archivo de alarma en cada cambio de estado. La opción “is_alarm” no tiene ningún efecto si la variable no es una variable de estado (opción “is_status”).

Cuando se utilizan los parámetros de monitorizaciónThreshold low, Threshold high o Threshold hysteresis, debe activarse el modo Polling para permitir que la variable sea monitorizada constantemente.

4.1.8 Acciones ejecutables

La pestaña “Actions” de la interfaz web permite ejecutar ciertas acciones localmente.

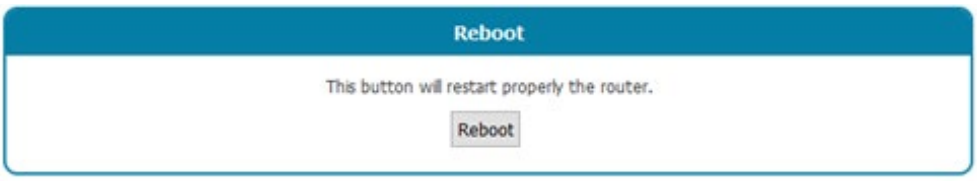
4.1.8.1 Solicitud de conexión al servidor remoto: Request

El botón “Request” tiene el mismo efecto que el botón físico en la parte frontal del producto.

Cuando se presiona este botón, aparece una ventana emergente que muestra todas las etapas de conexión, principalmente la sincronización NTP, la verificación de la carpeta INBOX y la indicación de todos los archivos descargados.

4.1.8.2 Solicitud de reinicio: Reboot

Este botón reinicia el concentrador.



4.1.8.3 Descarga de logs: Download logs

Este botón se utiliza para recuperar los logs (registros) de las últimas acciones ejecutadas en el concentrador.

4.1.8.4 Ajuste manual de la hora: Set time

Este formulario permite actualizar el concentrador en caso de no disponibilidad de una conexión Internet o de un servidor NTP no indicado.

Al hacer clic en el botón “Update”, la fecha y la hora del ordenador se copian en el formulario en formato correcto.

Si desea introducir manualmente la fecha y la hora, el formato debe ser el siguiente: YEAR-MM-DDThh:mm:ss

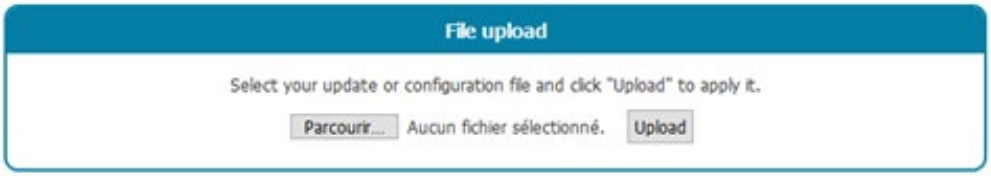
Con:

- AAAA: Año en 4 dígitos
- MM: Mes del año en 2 dígitos
- DD: Día del mes en 2 dígitos
- hh: Hora en 2 dígitos
- mm: Minutos en 2 dígitos
- ss: Segundos en 2 dígitos

La nueva fecha solo se tiene en cuenta tras validar el formulario pulsando el botón “Submit”.

4.1.8.5 Transmisión de archivos de sistema: File upload

Este formulario permite la transmisión local del archivo al concentrador.



Solo se aceptan archivos de configuración y actualizaciones a través de este formulario.

5. Explotación

5.1 El servidor remoto

El concentrador se comunica con un servidor remoto mediante el protocolo FTP. Este servidor permite gestionar el concentrador de forma remota.

El servidor remoto tiene varias funciones:

- Transmitir los datos y alarmas recopilados localmente por el concentrador: en cada conexión al servidor, ya sea siguiendo una solicitud manual, activando una alarma o activando el schedule de conexión, el concentrador aprovecha la conexión al servidor para enviar sus datos almacenados.
- Guardar una copia de la configuración: la carpeta “CONFIG/” del servidor guarda las copias de la configuración del concentrador. Cada vez que se cambie la configuración del concentrador (de forma local o remota), el concentrador envía una copia de su configuración a dicha carpeta.
- Reconfigurar el concentrador o activar acciones en él: los archivos de configuración o de comando deben enviarse al servidor en una carpeta INBOX asociada al concentrador.
- Supervisar el concentrador y ayudar al diagnóstico: el concentrador puede enviar archivos de estado del concentrador, así como logs para permitir el diagnóstico.

5.1.1 El servidor FTP

5.1.1.1 Configuración

El servidor FTP se define mediante los siguientes parámetros:

- Una dirección: Esta dirección puede ser una dirección IP o un nombre de dominio. En el caso de que se utilice un nombre de dominio con una conexión Ethernet, debe configurarse un servidor DNS en el concentrador para permitir la resolución del nombre de dominio en dirección IP.
- Es posible modificar el puerto de conexión FTP (por defecto 21) agregando al final de la dirección el puerto que se utilizará después del carácter ‘:’. El formato que debe utilizarse es el siguiente: “adresse:port” (por ejemplo, “192.168.1.2:8021”).
- Un nombre de usuario y una contraseña: Estos parámetros permiten definir la cuenta FTP que se utilizará.
- Una carpeta raíz: La carpeta raíz puede ser la raíz del servidor FTP “/” o una serie de subcarpetas (por ejemplo, “WebdynEasy_LoRaWAN/00C8B5/”).

En la carpeta raíz, el servidor FTP debe contener las siguientes carpetas:

Nombre	Derechos	Descripción
CONFIG/	Escritura	Contiene la imagen de la configuración. La configuración se guarda en un archivo llamado: “<uid>.xml”
DATA/	Escritura	Contiene los datos recopilados. El nombre del archivo de datos sigue el siguiente formato: “<uid>-<timestamp>.xml. gz” or “<uid>-<timestamp>.json.gz”
ALARM/	Escritura	Contiene las alarmas. El nombre del archivo de alarma sigue el siguiente formato: “<uid>-<timestamp>.xml.gz”
SUPERVISION/	Escritura	Contiene los archivos de estado, así como los logs. Los nombres de los archivos siguen el siguiente formato: “<uid>-<timestamp>.json.gz”
INBOX/<uid>/	Lectura/ Escritura	Buzón para enviar una configuración o un comando al concentrador
BIN/	Lectura	Contiene los archivos de actualización

Con:

- <uid>: Identificador del concentrador.
- <timestamp>: El formato de la marca de tiempo es “AAAAMMDD-HHMMSS”, de modo que la clasificación alfabética de la carpeta proporciona un orden cronológico.

Los archivos de datos, alarmas y supervisión están comprimidos en formato Gzip “.gz”.

Los derechos de acceso mínimos en las diferentes carpetas deben definirse como se indica en la tabla anterior.

 El concentrador no crea carpetas si no existen. Si las carpetas no existen o los derechos son insuficientes, contacte con el administrador del servidor.

5.1.1.2 Funcionamiento

El concentrador siempre envía archivos al servidor FTP mediante un proceso de 2 etapas:

- Al comienzo de la transferencia, el archivo tiene una extensión adicional “.tmp”.
- Cuando el archivo termina de transferirse, se le renombra eliminando la extensión “.tmp”.

Este proceso permite que el servidor remoto distinga fácilmente los archivos que se están transmitiendo de los que ya se han transmitido por completo.


Los archivos intercambiados con el servidor remoto respetan los formatos descritos por los archivos esquema (archivos XSD). Cada versión del firmware se entrega con sus archivos esquema asociados, disponible en nuestro sitio web.


Los esquemas XML que especifican el formato de los diversos archivos XML utilizados por el concentrador pueden cambiar en versiones futuras a medida que se añadan nuevas funciones. Estos cambios se realizarán para que los archivos XML antiguos sigan siendo compatibles con los nuevos esquemas XML. Asimismo, como los archivos XML generados por el concentrador pueden contener elementos adicionales, deben procesarse para que se ignoren los nuevos elementos.

5.1.1.3 Formato de los archivos

Los archivos de datos, alarmas, comandos y configuración intercambiados con el servidor están en formato XML.

5.1.2 Servicio web

5.1.2.1 Configuración

El Servicio Web está definido por los siguientes parámetros:

- Una URL: la URL puede ser una dirección IP o el nombre del servidor web remoto. Cuando se utiliza un nombre de dominio con una conexión Ethernet, se debe configurar un servidor DNS en el concentrador para permitir la resolución del nombre de dominio en una dirección IP.
- Es posible modificar el puerto del servidor web (por defecto el 80) añadiendo al final de la URL, el puerto a utilizar tras el carácter ':'. El formato a utilizar es: "url:puerto" (por ejemplo: "192.168.1.2:5000").
- Un identificador y una contraseña: estos parámetros se utilizan para definir la cuenta del Servicio Web a utilizar.
- Una ruta: la ruta en el servidor web.

El servidor web debe contener las siguientes subrutas:

Nombres	Derechos	Descripción
CONFIG/	Escritura	Contiene la imagen de configuración. La configuración se guarda en un archivo llamado: "<uid>.xml"
DATA/	Escritura	Contiene datos recopilados. El nombre del archivo de datos respeta el siguiente formato: "<uid>-<timestamp>.xml.gz" o "<uid>-<timestamp>.json.gz"

ALARM/	Escritura	Contiene las alarmas. El nombre del archivo de alarma tiene el siguiente formato: “<uid>-<timestamp>.xml.gz”
SUPERVISION/	Escritura	Contiene los archivos de estado y los registros. Los nombres de los archivos tienen el siguiente formato: “<uid>-<timestamp>.json.gz”
INBOX/<uid>/	Lectura/ escritura	Buzón para enviar una configuración o un comando al concentrador.
BIN/	Lectura	Contiene los archivos de actualización.

Con:

- <uid>: ID del concentrador
- <marca de tiempo>: el formato de la marca de tiempo es “AAAAMMDD-HHMMSS”, por lo que una clasificación alfabética del directorio da el orden cronológico

Los archivos de datos, alarmas y supervisión están comprimidos en formato Gzip “.gz”.

Los derechos de acceso mínimos a las diferentes vías de acceso deben definirse como se especifica en la tabla anterior.

5.1.2.2 Funcionamiento

El concentrador carga los archivos en el servidor web mediante una solicitud HTTP POST en el siguiente formato:

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

El concentrador recupera archivos del servidor web mediante una solicitud HTTP GET en el siguiente formato:

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


Los archivos intercambiados con el servidor remoto cumplen con los formatos descritos por los archivos de esquema (archivos XSD). Cada versión de firmware se entrega con sus archivos de esquema asociados y está disponible en nuestro sitio web.


Los esquemas XML que especifican el formato de los diversos archivos XML utilizados por el concentrador pueden cambiar en futuras versiones cuando se agreguen nuevas funciones. Estos cambios se realizarán para que los archivos XML antiguos sigan siendo compatibles con los nuevos esquemas XML. Además, dado que los archivos XML generados por el concentrador pueden contener elementos adicionales, se debe implementar su procesamiento para que se ignoren los nuevos elementos.

5.1.2.3 Formato de archivo

Los archivos de alarma, comando y configuración intercambiados con el servidor están en formato XML. Los archivos de datos están en formato XML o en formato JSON.

5.1.3 Servicio Web

5.1.3.1 Ajustes

- El servidor MQTT se define mediante los siguientes parámetros:

- Una dirección: Esta dirección puede ser una dirección IP o el nombre del servidor web remoto. Cuando se utiliza un nombre de dominio con una conexión Ethernet, se debe configurar un servidor DNS en el concentrador para permitir la resolución del nombre de dominio en una dirección IP.

- Es posible modificar el puerto del servidor MQTT (por defecto 1883) añadiendo al final de la dirección, el puerto a utilizar después del carácter ':'. El formato a utilizar es: url:port (por ejemplo: "192.168.1.2:5000").

- Un identificador y una contraseña: Estos parámetros se utilizan para definir la cuenta del servidor MQTT que se va a utilizar.

- El tema: El tema de los mensajes MQTT que se van a utilizar

With :

<uid>: Concentrator ID

5.1.3.2 Operación

El hub envía los datos al servidor MQTT en el formato especificado en la sección de carga. No hay gestión de configuración en MQTT. No hay ningún comando en MQTT.

5.1.3.3 Data Format

Las alarmas, los datos y la supervisión están en formato XML o en formato JSON.

En cuanto al formato XML:

Los datos intercambiados con el servidor remoto respetan los formatos descritos por los archivos de esquema (archivos XSD). Cada versión de firmware se entrega con sus archivos esquemáticos asociados y está disponible en nuestro sitio web (consulte el capítulo 7: “Soporte”)

Los esquemas XML que especifican el formato de los distintos archivos XML utilizados por el concentrador pueden cambiar en versiones futuras cuando se agreguen nuevas características. Los archivos XML generados por el concentrador pueden contener elementos adicionales, su procesamiento debe implementarse para que los nuevos elementos sean ignorados.

5.2 La configuración

El concentrador permite configuraciones remotas mediante un archivo de configuración o por SMS

Archivo de configuración:

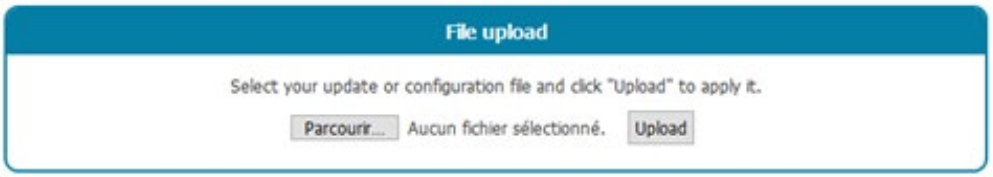
El archivo de configuración del concentrador WebdynEasy LoRaWAN está en formato XML. Consulte el archivo XSD de configuración relativo a su versión de firmware para conocer los detalles sobre el formato de los archivos de configuración.

En anexo a este manual (“Anexo A - Lista de variables”) se presenta la lista de variables y sus significados.

Una copia de la configuración actual está disponible en el servidor remoto, en el carpeta “CONFIG/”. Ya sea tras una modificación local o remota de la configuración, el concentrador envía su nueva configuración al servidor remoto.

El envío de un archivo de configuración puede realizarse de forma local a través de la interfaz web o de forma remota a través del carpeta FTP “INBOX”.

- Localmente: en la pestaña “Actions”, seleccione el archivo de configuración deseado a través del formulario “File upload”, luego confirme su elección haciendo clic en el botón “Upload”. El archivo se enviará al concentrador y se aplicará.



- De forma remota: guarde el archivo de configuración en el carpeta FTP “INBOX” de su concentrador (“INBOX/<uid>/”, con <uid> el identificador de su concentrador). En la próxima conexión al servidor FTP, el concentrador realizará 3 etapas:
  - Transmitir el archivo de configuración disponible al servidor.
  - Eliminar el archivo de configuración del servidor.
  - Aplicar la nueva configuración.

No es necesario utilizar un formato de nombre predefinido en el archivo de configuración.

En caso de error en el archivo de configuración (archivo corrupto, valor incorrecto, etc.), el archivo no se aplicará y se generará una alarma en el servidor. Compruebe la consistencia de su archivo de configuración respecto al archivo XSD correspondiente a su versión de firmware antes de enviarlo a su concentrador.

No es necesario enviar toda la configuración a su concentrador. Un archivo de configuración puede ser completo o parcial. Por lo tanto, puede enviarse un archivo de configuración que contenga una sola variable.

Por defecto, la configuración enviada al concentrador sobrescribe la configuración actual. Solo se sobrescribirán las variables presentes en el archivo de configuración. No obstante, es posible aplicar los valores por defecto a todas las variables antes de aplicar los nuevos valores. Para ello, en la etiqueta principal “config”, agregue el atributo “factory=true”. (Ver ejemplo a continuación) .

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

Consulte el anexo “Anexo A” para ver la lista de variables y sus posibles valores.

5.3 Los datos

Los datos se cargan envían a la carpeta “DATA/” del servidor FTP en forma de archivos en formato XML, y se comprimen en formato Gzip “.gz”.

A continuación, se muestra el formato del nombre de los archivos de datos: <uid>-<timestamp>.xml.gz or <uid>-<timestamp>.json.gz.

Con:

- <uid>: Identificador del concentrador
- <timestamp>: El formato de la marca de tiempo es “AAAAMMDD-HHMMSS”, de modo que una clasificación alfabética de la carpeta proporciona el orden cronológico

Ejemplo:

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

El formato de los archivos de datos se describe en el archivo de datos XSD. Los archivos XSD pueden evolucionar según las versiones de firmware. Se entregan con cada actualización.

La frecuencia de envío de archivos al servidor remoto puede definirse por un schedule. (ver capítulo 4.1.5: “Schedules” y capítulo 4.1.1.5: “Upload”) No obstante, durante una conexión al servidor tras una solicitud manual o la generación de una alarma, el concentrador aprovecha la conexión para almacenar los datos en la memoria.

5.4 Las alarmas

Las alarmas se generan en forma de archivos en formato XML y se comprimen en formato Gzip “.gz”. Se guardan en la carpeta “ALARM/” del servidor remoto.

El formato del nombre de los archivos de alarmas es idéntico al de los archivos de datos. A continuación, se muestra el formato del nombre de los archivos de alarmas: <uid>-<timestamp>.xml.gz

Con:

- <uid>: Identificador del concentrador.
- <timestamp>: El formato de la marca de tiempo es “AAAAMMDD-HHMMSS”, de modo que una clasificación alfabética de la carpeta proporciona el orden cronológico.

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

El formato de los archivos de alarmas se describe en el archivo de alarmas XSD. Los archivos XSD pueden evolucionar según las versiones de firmware. Se entregan con cada actualización.

Las alarmas pueden configurarse para que se envíen inmediatamente tras activarse (On), en la siguiente conexión (Delayed) o desactivarse (Off). (ver capítulo 4.1.4: “Alarmas”).

5.5 Los comandos

Es posible realizar acciones en el concentrador de forma remota. Para ello, debe enviarse un comando (orden) al concentrador. Este comando puede enviarse a través de un archivo de comandos en formato XML o por SMS.

- Archivo de comandos XML: el archivo de comandos debe enviarse al servidor remoto a la carpeta “INBOX” asociada al concentrador (“INBOX/<uid>/”, con<uid>/ , el identificador del concentrador). De igual forma que para los archivos de configuración. Todos los archivos de esta carpeta se enviarán antes de eliminarse y ejecutarse. El formato de los archivos de comandos se describe en el archivo de comandos XSD. Los archivos XSD pueden evolucionar según las versiones de firmware. Se entregan con cada actualización.
- SMS: el formato del SMS debe ser el siguiente:

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

o

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

Con:

- command: comando para enviar
- param1, param2,..., parami: parámetros del comando
- value1, value2, ..., valuei: valores de los parámetros

- comando: comando para enviar
- param1, param2, ..., parami: parámetros de comando
- valor1, valor2, ..., valori: valores de parámetros

Todos los comandos aceptan dos parámetros opcionales “uid” y “cid”:

- uid: identificador único del concentrador
- cid: identificador de comando

Se rechazará un comando si el parámetro uid incluido no coincide con el uid del concentrador.

El cid puede ser elegido libremente por el emisor del comando. Se incluirá con cualquier transmisión asociada.

A continuación se muestra la lista de comandos disponibles en el concentrador:

Comando	Subcomando	Descripción	Retorno
reboot		Reinicio del producto	Ninguno
factory		Retorno a la configuración de fábrica	Ninguno
update		Actualización del software del concentrador	Alarma
connect		Conexión inmediata al servidor remoto	Conexión
status		Recuperación del estado del concentrador	Supervisión + SMS
log		Recuperación del libro de registro	Supervisión
settime		Ajuste del tiempo del concentrador	Alarma
modbus	write	Escritura en un esclavo modbus	Alarma
lorawan	send	Envío de tramas LoRaWAN de enlace descendente	Alarma
lorawan	add	Agregar un sensor	Alarma
lorawan	delete	Eliminación de un sensor	Alarma

 En el caso de enviar varios comandos simultáneos, los comandos “reboot”, “factory” y “update” pueden perder los siguientes comandos.

5.5.1 Comando “reboot”

El comando “reboot” permite activar un reinicio inmediato del producto. No hay retorno/acuse tras el envío de este comando.

No se necesitan subcomandos ni parámetros para este comando.

Ejemplo:

- Por archivo XML:

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

- Por SMS:

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

5.5.2 Comando "factory"

El comando "factory" restaura la configuración de fábrica en el concentrador. No hay retorno/acuse tras el envío de este comando.

No se necesitan subcomandos ni parámetros para este comando.

Ejemplo:

- Por archivo XML:

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

- Por SMS:

```
cmd=factory
```

5.5.3 Comando "update"

(Ver capítulo 6.2: "Actualización Remota".)

5.5.4 Comando "connect"

El comando "connect" permite activar una conexión inmediata del producto con el servidor remoto. No

hay retorno/acuse tras el envío de este comando.

No se necesitan subcomandos ni parámetros para este comando.

Ejemplo:

- Por SMS:

```
cmd=connect
```

5.5.5 Comando "status"

El comando "status" permite obtener información sobre el estado del producto. Cuando la solicitud se realiza a través de un archivo, se envía un archivo de estado al servidor remoto, a la carpeta "SUPERVISION/". Cuando la solicitud se realiza por SMS, la respuesta se envía por SMS al emisor del comando.

No se necesitan subcomandos ni parámetros para este comando.

Ejemplo:

- Por archivo XML:

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

- Por SMS:

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

5.5.6 Comando "log"

El comando "log" permite recuperar el libro de registro del concentrador. El libro de registro se envía al servidor remoto, a la carpeta "SUPERVISION/".

No se necesitan subcomandos ni parámetros para este comando.

Ejemplo:

- Por archivo XML:

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

- Por SMS:

```
cmd=log
```

5.5.7 Comando "settime"

El comando "settime" le permite actualizar la fecha y la hora del concentrador con la hora deseada.

Para ello, en el atributo "hora", debe indicar la fecha y hora deseada en el siguiente formato: AAAA-MM-DDThh:mm:ss.

Con:

- AAAA: año de 4 dígitos
- MM: Mes del año en 2 dígitos
- DD: Día del mes en 2 dígitos
- hh: Hora en 2 dígitos
- mm: Minutos en 2 dígitos
- ss: segundos de 2 dígitos

 Si se configura un servidor NTP, la fecha y la hora del concentrador se actualizarán automáticamente al conectarse al servidor remoto.

Ejemplo:

- Por archivo XML:

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

- Por SMS:

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

5.5.8 Comando "modbus"

El comando "modbus" permite escribir valores en los registros de esclavos Modbus configurados en el concentrador.

Para ello, es necesario especificar el subcomando "write", los datos a escribir en el atributo "data" y la lista de esclavos y registros en los que debe escribirse este valor.

El comando se guarda en las acciones de supervisión y se envía al servidor remoto a la carpeta "SUPERVISION/".

Las direcciones de los esclavos deben respetar el siguiente formato:

- Modbus RTU:

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

  Ejemplo: 45/S3@0x0056

- Modbus TCP:

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

  Ejemplo: 192.168.0.17:223/S3@0x0F52

Ejemplo:

- Por archivo XML:

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

- Por SMS:

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

5.5.9 Comando "lorawan"

El comando "lorawan" se utiliza para enviar comandos al concentrador. Hay varios subcomandos que son:

- "send": envía tramas "downlink" al sensor.
- "añadir": permite añadir un sensor al concentrador.
- "borrar": permite borrar un sensor del concentrador.

Siguiendo el comando, se genera una alarma y se coloca en el directorio "ALARM/" especificando el resultado del comando.

5.5.9.1 Subcomando "send"

El subcomando "enviar" envía marcos de "enlace descendente" al sensor.

Para ello, es necesario rellenar los siguientes atributos:

- "devaddr": el DEVADDR del sensor que identifica al sensor (en formato hexadecimal).
- "Deveui": el DEVEUI del sensor que identifica al sensor (en formato hexadecimal).

- “fport”: el número de puerto del sensor para usar el sensor (en formato decimal).
- “datos”: los datos a enviar en formato hexadecimal.

En la clase A, el concentrador envía tramas de “enlace descendente” justo después de una trama de “enlace ascendente” desde el sensor. El concentrador prepara el mensaje y lo almacena durante un máximo de 48 horas. Pasado este tiempo, se enviará una alarma para avisar que se supera el tiempo. También se envía una alarma para señalar el envío de la trama al sensor.

Ejemplo:

- Por archivo XML:

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

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

- Por SMS:

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

Ejemplo de alarmas en caso de éxito:

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

Ejemplo de alarma en caso de superación de tiempos:

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

5.5.9.2 Subcomando “add”

El subcomando “add” agrega un sensor al concentrador.

Para ello, es necesario rellenar los siguientes atributos:

- “Deveui”: el DEVEUI del sensor que identifica al sensor (en formato hexadecimal).
- “appskey”: la APPSKEY del sensor si el sensor está en modo PAA (en formato hexadecimal).
- “nwkskey”: la NWKSKEY del sensor si el sensor está en modo PAA (en formato hexadecimal).
- “appkey”: la APPKEY del sensor si el sensor está en modo OTAA (en formato hexadecimal).

Ejemplo de adición de un sensor en modo OTAA:

- Por archivo XML:

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

- Por SMS:

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

Ejemplo de adición de un sensor en modo PAA:

- Por archivo XML:

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

- Por SMS:

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

5.5.9.3 Subcomando”borrar”

El subcomando “eliminar” le permite eliminar un sensor del concentrador.

Para ello, es necesario rellenar los siguientes atributos:

- “devaddr”: el DEVADDR del sensor que identifica al sensor (en formato hexadecimal).
- “Deveui”: el DEVEUI del sensor que identifica al sensor (en formato hexadecimal).

Ejemplo:

- Por archivo XML:

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

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

- Por SMS:

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

6. Actualización

El concentrador WebdynEasy LoRaWAN puede actualizarse de forma local o remota. La última versión de firmware (“GatewayLoRaWAN_x.x.x.cwe”) está disponible para descarga desde nuestro sitio web, en la siguiente dirección: https://www.webdyn.com/support/lorawan/.

6.1 Local

Para actualizar el concentrador localmente, hay que pasar por su interfaz web e ir a la pestaña “Actions”, y luego seguir el procedimiento de transmisión de archivos de sistema “File upload” (ver capítulo 4.1.7.5: “Transmisión de archivos de sistema: File upload”).

6.2 Remoto

Para una actualización remota, el archivo que contiene la actualización debe enviarse a la carpeta “BIN” del servidor remoto, así como un comando de actualización (“update”) al concentrador.

El comando de actualización puede enviarse por un archivo de comando o por SMS. El comando debe incluir el nombre del archivo que contiene la actualización (campo “firmware”), así como su código MD5 asociado (campo “checksum”).

 Se recomienda encarecidamente utilizar un archivo de comando (XML).

Ejemplo

- Por archivo XML:

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

- Por SMS:

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

7. Anexo A: Variables del archivo de configuración XML

Todos los “nombres + árbol” resaltados en azul son listas y pueden crearse varias veces.

Nombre + árbol	Descripción	Tipo	Valor por defecto	No usado (evolución futura)
/uid	Identificador del concentrador	Hexadecimal de 3 bytes	3 últimos bytes de la dirección MAC	
/name	Nombre opcional del producto	Texto	"WG_" + 3 últimos bytes de la dirección MAC	
/enable_local_config	Activación/Desactivación del acceso a la configuración local	Booleano (true, false)	false	
/com/modem/pin/mode	Activación/Desactivación del PIN	Lista: •Off •manual	off	
/com/modem/pin/code	Código PIN	Número entero de 4 a 6 dígitos		
/com/modem/apn	APN	Texto		
/com/modem/login	Identificador de APN	Texto		
/com/modem/password	Contraseña APN	Texto		
/com/modem/mode	Modo de conexión del módem	Lista: •ondemand •alwaysOn •alwaysOff	alwaysOff	
/com/modem/delay	Tiempo antes de desconexión en segundos	Número entero (mín. 0 máx. 65 535)	60	
/com/ethernet/use_dhcp	Activación/Desactivación del cliente DHCP	Booleano (false, true)	false	
/com/ethernet/ip	Dirección IP	Formato IP: "xxx.xxx.xxx.xxx"	192.168.1.12	
/com/ethernet/netmask	Máscara de subred	Formato IP: "xxx.xxx.xxx.xxx"	255.255.255.0	
/com/ethernet/gateway	Pasarela de red local	Formato IP: "xxx.xxx.xxx.xxx"		
/com/ethernet/dns/server	Lista de servidores DNS	Formato IP: "xxx.xxx.xxx.xxx"		
/com/ftp/address	Dirección del servidor FTP + puerto (opcional). Si no se especifica el puerto, por defecto el FTP utilizará el 21	Formato IP: "xxx.xxx.xxx.xxx" o nombre de dominio: “xxxxxxxxx.xxx” + puerto (opcional): “:xxxx”		
/com/ftp/login	Identificador de la cuenta FTP	Texto		
/com/ftp/password	Contraseña de la cuenta FTP	Texto		

/com/ftp/mode	Modo de conexión FTP pasivo o activo	Lista: •pasivo •activo	passive
/com/ftp/secured	Activación/Desactivación del modo seguro (FTPS)	Booleano (true, false)	false
/com/ftp/trust_model	Modo de funcionamiento del modo seguro	Lista:	verify_peer
/com/ftp/root_path	Carpeta raíz en el servidor FTP	Texto	
/com/ftp/ws_notification	Activación/Desactivación del envío de notificaciones	Lista: •none •put •get •both	none
/com/ws/address	Dirección del servidor de Web Services		
/com/ws/login	Identificador del servidor de Web Services		
/com/ws/password	Contraseña del servidor Web Services		
/com/ws/webservice_proxy	Dirección del servidor proxy (opcional)		
/com/ws/trust_model	Modo de funcionamiento del modo seguro: •Trust peer Verify peer		
/com/ws/upload_path	Carpeta raíz del servidor de Web Services		
/com/mqtt/address	Dirección del servidor MQTT + puerto (opcional) Si el puerto está vacío, por defecto el MQTT utilizará el 1883	IP format: “xxx.xxx.xxx.xxx” Or Domain name: “xxxxxxxxxx.xxx” + port (optional): “:xxxx”	
/com/mqtt/client_id	Identificador de cliente en el protocolo MQTT Text	Text	
/com/mqtt/login	MQTT Account ID	Text	
/com/mqtt/password	MQTT account password	Text	
/com/mqtt/keepalive	Tiempo en segundos para enviar fotogramas keepalive	Integer (min 0, max 65535)	60
/com/mqtt/topic	El tema del mensaje MQTT comienza con esta cadena		
/com/mqtt/trust_model	Modo seguro Modo de operación	List: • verify peer • trust peer	verify peer
/com/mqtt/ca	Certificado raíz de CA	PEM File Format	
/com/mqtt/cert	Certificado firmado por el cliente local	PEM File Format	

/com/mqtt/key	Clave privada del cliente local	PEM File Format		
/com/keepalive/file	Tipo de archivos a enviar	Lista: •"log" •"supervision" •empty: keepalive au format "[UID]-[TIME %Y%m%d-%H%M%S]-keepalive"		•
/com/keepalive/ Schedule	Identificador del schedule para el envío periódico del keepalive			•
/com/request/upload	Activación/Desactivación de la conexión al servidor tras pulsar el botón "REQUEST"			•
/com/request/include_status	Enviar un archivo de supervisión al servidor tras pulsar el botón "REQUEST"			•
/com/request/sms_status_recipient	Número de teléfono del destinatario del SMS de estado tras pulsar el botón "REQUEST". Número en formato internacional			•
/com/time/ntp/server	Lista de direcciones de servidores NTP	Formato IP: "xxx.xxx.xxx.xxx" o nombre de dominio: "xxxxxxxxx.xxx"		
/com/time/timezone	Zona horaria en formato tz	Lista: (ver en http://en.wikipedia.org/wiki/Zone.tab)		•
/com/time/alarm_threshold	Umbral de activación de alarma en segundos	Número entero (mín. 0 máx. 65 535)	0	
/com/time/min_sync_interval	Tiempo mínimo entre 2 sincronizaciones NTP (en segundos)	Número entero (mín. 0 máx. 4 294 967 295)	86400	
/com/vpn/openvpn/enable	Habilitar cliente OpenVPN	Lista: •true •false	false	•
/com/vpn/openvpn/protocol	Protocolo de comunicación VPN utilizado	Lista: •tcp •udp		•
/com/vpn/openvpn/server/address	Nombre o dirección IP del servidor VPN	Formato IP: "xxx.xxx.xxx.xxx" o nombre de dominio: "xxxxxxxxx.xxx"		•
/com/vpn/openvpn/server/port	Puerto del servidor VPN (generalmente 1194)	Número entero (mín. 1 máx. 65535)		•
/com/vpn/openvpn/server/cipher	Algoritmo de cifrado de paquetes de datos (opcional)	Lista: (ver lista en OpenVPN "openvpn –show-ciphers")		•

/com/vpn/openvpn/server/auth	Autenticación del VPN	Lista: (ver lista en OpenVPN “openvpn --show-digests”)	SHA1	•
/com/vpn/openvpn/server/ca	Certificado raíz de CA	PEM		•
/com/vpn/openvpn/server/cert	Certificado firmado por el cliente local	PEM		•
/com/vpn/openvpn/server/key	Clave privada del cliente local	PEM		•
/com/vpn/openvpn/server/tls_auth (Obsoleto)	Clave estática utilizada para el algoritmo hash HMAC en paquetes de control (Obsoleta, consulte Variable clave a continuación)	PEM		
/com/vpn/openvpn/server/control_channel_security/method	Lista de métodos para la seguridad del canal de control	Lista: •none •tls-auth •tls-crypt •tls-crypt-v2	none	
/com/vpn/openvpn/server/control_channel_security/key	Clave para la seguridad del canal de control	PEM		
/com/firewall	Cortafuegos			•
/com/mdns/enable	Activación del protocolo mDNS destinado a resolver el nombre del concentrador “UID” en una dirección IP.	Lista: •true •false	true	•
/upload/config/method	Protocolo de comunicación para la gestión de archivos de configuración	Lista: •none •ftp •ws	ftp	ws
/upload/config/omit_password	Ocultar las etiquetas "password" del archivo XML	Booleano (true, false)	false	
/upload/supervision/method	Protocolo de comunicación para el envío de archivos de supervisión	Lista: •none •ftp •ws	ftp	ws
/upload/alarm/method	Protocolo de comunicación para el envío de archivos de alarmas	Lista: •none •ftp •ws	ftp	
/upload/data/method	Protocolo de comunicación para la gestión de archivos de datos	Lista: •none •ftp •ws	ftp	
/upload/data/format	Formato de los archivos de datos para los datos	Lista: •xml •json	xml	
/upload/data/schedule	Identificador del schedule vinculado al envío de datos	Número entero (mín. 1 máx. 65535)		
/upload/commun/size_limit	Tamaño máximo de un archivo de datos sin comprimir en Mo	Número entero (mín. 0 máx. 30)	10	
/alarm/sources/modem_ip	Configuración de la alarma de cambio de dirección IP módem	Lista: •on •off •delayed	off	

/alarm/sources/msisdn	Configuración de la alarma de cambio de tarjeta SIM • on: activada y envío inmediato • off: desactiva delayed: activada y envío en la siguiente conexión	Lista: • on • off • delayed	off
/alarm/sources/sw_version	Configuración de la alarma de actualización de software (firmware o núcleo) • on: activada y envío inmediato • off: desactiva delayed: activada y envío en la siguiente conexión	Lista: • on • off • delayed	on
/alarm/sources/defaults/ignored	Lista de fallos que deben ignorarse: • D_MODEM • D_MODEM_SIM_MISS • D_MODEM_SIM_CODE_FAIL • D_MODEM_PUK • D_MODEM_REG_DENIED	Texto (lista de fallos separados por una coma ",")	
/alarm/sources/defaults/delayed	Lista de fallos que no deben enviarse inmediatamente, sino solo en la siguiente conexión: • D_MODEM • D_MODEM_SIM_MISS • D_MODEM_SIM_CODE_FAIL • D_MODEM_PUK • D_MODEM_REG_DENIED	Texto (lista de fallos separados por una coma ",")	
/scheduler/schedules/schedule/	Lista de schedules		
/scheduler/schedules/schedule/id	Identificador del schedule	Número entero (mín. 1 máx. 2 147 483 647)	
/scheduler/schedules/schedule/label	Nombre del schedule	Texto	
/scheduler/schedules/schedule/type	Tipo de schedule	Lista: • Daily • Weekly • Monthly • Yearly • Follower	Daily
/scheduler/schedules/schedule/parent	Identificador del schedule principal en el caso de un schedule de tipo "follow"	Número entero (mín. 1 máx. 65535)	
/scheduler/schedules/schedule/start/time	Hora de activación de la primera iteración del schedule en el caso de un schedule de tipo “day”, “week” o “month”	Hora en formato: “hh:mm:ss”	
/scheduler/schedules/schedule/start/datetime	Fecha y hora de activación de la primera iteración del schedule en el caso de un programa de tipo "year"	Fecha y hora en formato: “aaaa-mm-ddThh:mm:ss”	
/scheduler/schedules/schedule/start/dayofweek	Día de activación en la semana de la primera iteración del schedule en el caso de un programa de tipo "week"	Lista: • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday	

/scheduler/schedules/schedule/start/dayofmonth	Día de activación en el mes de la primera iteración del schedule en el caso de un programa de tipo "month"	Número entero (mín. 1 máx. 31)	
/scheduler/schedules/schedule/interval	Intervalo entre ocurrencias (en segundos)	Número entero (mín. 0 máx. 4,294,967,295)	
/scheduler/schedules/schedule/count	Numero de ocurrencia	Número entero (mín. 1 máx. 65535)	
/modbus/tcp/timeout	Tiempo máximo sin respuesta de los esclavos Modbus/TCP (en ms)	Número entero (mín. 0 máx. 65535)	2000
/modbus/rtu/timeout	Tiempo máximo sin respuesta de los esclavos Modbus RTU (en ms)	Número entero (mín. 0 máx. 65535)	2000
/modbus/rtu/turnaround	Tiempo de respuesta Modbus RTU (en ms)	Número entero (mín. 0 máx. 65535)	100
/modbus/datasets/dataset/	Lista de Dataset Modbus	Número entero (mín. 1 máx. 65535)	
/modbus/datasets/dataset/id	Identificador del dataset	Número entero (mín. 1 máx. 65535)	
/modbus/datasets/dataset/label	Nombre del dataset	Texto	
/modbus/datasets/dataset/vars/var/	Lista de variables del Dataset		
/modbus/datasets/dataset/vars/var/name	Nombre de la variable	Texto	
/modbus/datasets/dataset/vars/var/type	Tipo de variable	Lista: •S0: Coil (0X1/0X5,0XF) •S1: Discrete input (0X) •S3: Holding register (0x3/0x6,0x10) •S4: Input register (0x4)	
/modbus/datasets/dataset/vars/var/address	Dirección del 1er registro de la variable	Hexadecimal de 2 bytes	
/modbus/datasets/dataset/vars/var/size	Tamaño de la variable	Entero sin signo	
/modbus/datasets/dataset/vars/var/format	Formato de la variable	Lista: •raw •boolean •integer •float •ascii	
/modbus/datasets/dataset/vars/var/flags	Opciones de la variable (opcional)	Lista: •cmd_only •little_endian •no_opt •signed •is_status •is_alarm	
/modbus/datasets/dataset/vars/var/threshold/low	Umbral bajo (opcional)	Número (doble)	

/modbus/datasets/dataset/vars/var/threshold/high	Umbral alto (opcional)	Número (doble)	
/modbus/datasets/dataset/vars/var/threshold/hysteresis	Histéresis (opcional)	Número (doble)	
/modbus/datasets/dataset/boundaries			•
/modbus/datasets/dataset/polling	Activación de la interrogación permanente	Booleano (true, false)	false
/modbus/modules/module/	Lista de módulos Modbus		
/modbus/modules/module/label	Nombre del esclavo Modbus	Texto	
/modbus/modules/module/dataset	Identificador del dataset a utilizar	Número entero (mín. 1 máx. 65535)	
/modbus/modules/module/address	Dirección Modbus del esclavo Modbus	Número entero (mín. 1 máx. 247)	
/modbus/modules/module/ip	Dirección IP del esclavo Modbus/TCP	Formato IP: "xxx.xxx.xxx.xxx" o nombre de dominio: "xxxxxxxxx.xxx"	
/modbus/modules/module/schedule	Identificador del schedule de recopilación del esclavo Modbus	Número entero (mín. 1 máx. 65535)	
/system/log/level	Nivel de registros en el libro de registro. Solo para depuración (contactar al soporte)	Nivel de 1 (alto) a 5 (bajo)	5
/system/password/admin	Contraseña de administrador	Texto	high
/system/password/install	Contraseña de instalador	Texto	medium
/system/password/data	Contraseña de usuario	Texto	low
/system/ports/rs485/mode	Configuración del puerto RS485	Lista: •Off •Modbus	Off
/system/ports/rs485/baudrate	Velocidad del puerto RS485 (en baudios)	Lista: •4800 •9600 •19200 •38400 •57600 •115200	19200
/system/ports/rs485/data	Número de bits de datos del puerto RS485	Lista: •5 •6 •7 • •9	8
/system/ports/rs485/parity	Paridad de puerto RS485	Lista: •None •Odd •Even	Even
/system/ports/rs485/stop_bit	Número de bits de stop del puerto RS485	Lista: •1 •2	1

/lorawan/region	Nombre de la región para los parámetros LoRaWAN	Lista: •EU868 •IN865	EU868
/lorawan/channels/channel	Frecuencia del canal 4 (en Hz)	Número entero (mín. 863,000,000 máx. 870,000,0000)	867100000
/lorawan/channels/channel	Frecuencia del canal 5 (en Hz)	Número entero (mín. 863,000,000 máx. 870,000,0000)	867300000
/lorawan/channels/channel	Frecuencia del canal 6 (en Hz)	Número entero (mín. 863,000,000 máx. 870,000,0000)	867500000
/lorawan/channels/channel	Frecuencia del canal 7 (en Hz)	Número entero (mín. 863,000,000 máx. 870,000,0000)	867700000
/lorawan/channels/channel	Frecuencia del canal 8 (en Hz)	Número entero (mín. 863,000,000 máx. 870,000,0000)	867900000
/lorawan/packet_forwarder/server/address	Dirección del servidor LoRaWAN (servidor integrado: 127.0.0.1)	Formato IP: “xxx.xxx.xxx.xxx” o nombre de dominio: “xxxxxxxxx.xxx”	127.0.0.1
/lorawan/packet_forwarder/server/port_up	Número de puerto UDP saliente del Packet Forwarder	Número entero (mín. 1 máx. 65535)	1700
/lorawan/packet_forwarder/server/port_down	Número de puerto UDP entrante del Packet Forwarder	Número entero (mín. 1 máx. 65535)	1700
/lorawan/packet_forwarder/keepalive_interval_s	Tiempo en segundos para enviar una trama de mantenimiento de conexión	Número entero (mín. 0 máx. 65535)	10
/lorawan/packet_forwarder/push_timeout_ms	Tiempo máximo de espera en milisegundos para el reconocimiento de la trama enviada al servidor LoRaWAN.	Número entero (mín. 0 máx. 65535)	10
/lorawan/packet_forwarder/forwarder_crc_valid	Procesamiento de paquetes LoRaWAN con un CRC válido (no modificar, solo se usa para test)	Booleano (true, false)	true
/lorawan/packet_forwarder/forwarder_crc_error	Procesamiento de paquetes LoRaWAN con un CRC erróneo (no modificar, solo se usa para test)	Booleano (true, false)	false
/lorawan/packet_forwarder/forwarder_crc_none	Procesamiento de paquetes LoRaWAN sin CRC (no modificar, solo se usa para test)	Booleano (true, false)	false

/lorawan/packet_forwarder/public	Tipo de preámbulo de la red pública LoRaWAN (public: 0x34, private: 0x12) (no modificar, solo se usa para test)	Booleano (true, false)	true
/lorawan/server/netid	Identificador de la red LoRaWAN (ver especificación LoRaWAN). Si se introduce el valor 0, cuando se reinicie el concentrador se utilizará su NetID de fábrica.	Hexadecimal de 3 bytes	Calculado automáticamente a partir de su dirección MAC
/lorawan/server/adr/enable	Activación de la ADR	Booleano (true, false)	true
/lorawan/server/adr/margin_db	Margen en dB para calcular la ADR	Número entero (mín. 1 máx. 30)	5
/lorawan/server/adr/uplink_count	Número de Uplink necesario para la ADR	Número entero (mín. 1 máx. 65535)	20
/lorawan/server/udp_port	Puerto UDP del servidor LoRaWAN	Número entero (mín. 1 máx. 65535)	1700
/lorawan/server/backup_interval	Intervalo de registro automático de la configuración con los contadores Fcntup y Fcntdown. (en segundos)	Número entero (mín. 1 máx. 4,294,967,295)	86400
/lorawan/server/modules/module/	Lista de módulos LoRaWAN		
/lorawan/server/modules/module/deveui	Identificador único del sensor (EUI64)	Hexadecimal de 8 bytes	
/lorawan/server/modules/module/appkey	Clave de cifrado que utiliza la red para derivar claves de sesión.	Hexadecimal de 16 bytes	
/lorawan/server/modules/module/devaddr	Dirección del sensor	Hexadecimal de 4 bytes	
/lorawan/server/modules/module/appskey	Clave de cifrado entre el sensor y el servidor aplicativo	Hexadecimal de 16 bytes	
/lorawan/server/modules/module/nwkskey	Clave de cifrado entre el sensor y el servidor LoRaWAN	Hexadecimal de 16 bytes	
/lorawan/server/modules/module/fcntup	Contador de tramas Uplink (al servidor)	Número entero (mín. 0 máx. 4,294,967,295)	
/lorawan/server/modules/module/fcntdown	Contador de tramas Downlink (al sensor)	Número entero (mín. 0 máx. 4,294,967,295)	

Contacto de oficinas y soporte

ESPAÑA

C/ Alejandro Sánchez 109
28019 Madrid

Teléfono: +34.915602737
Email: contact@webdyn.com

FRANCIA

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

Teléfono: +33.139042940
Email: contact@webdyn.com

INDIA

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

Teléfono: +91.1141519011
Email: contact@webdyn.com

PORTUGAL

Av. Coronel Eduardo Galhardo 7-1ºC
1170-105 Lisboa

Teléfono: +351.218162625
Email: comercial@lusomatrix.pt

TAIWAN

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

Teléfono: +886.965333367
Email: contact@webdyn.com