

TITAN

Manual de Usuario Software

Índice

Notas generales.....	5
Información importante	5
Revisiones	5
1.- Introducción.....	6
2.- FAQ. Conceptos básicos.....	7
3.- Configuración paso a paso.....	11
4.- Configuración	12
4.1- Mobile	13
4.1.1- Mobile → Status	13
4.1.2- Mobile → Basic Settings.....	14
4.1.3- Mobile → Keep Online.....	17
4.1.4- Mobile → Basic Settings → FailOver	18
4.1.5- Mobile → Basic Settings → Operators	20
4.1.6- Mobile → Basic Settings → SIM Swapping.....	21
4.2- Ethernet	22
4.2.1- Ethernet → Basic Settings.....	22
4.2.2- Ethernet → DHCP Server.....	25
4.3 Wifi	26
4.3.1- Wifi → Basic Settings	26
4.3.2- Wifi → DHCP Server	29
4.4- Firewall	30
4.4.1 - Firewall → NAT	30
4.4.2 - Firewall → Authorized IPs	32
4.4.3 - Firewall → MAC Filter.....	34
4.4.4 - Firewall → Routes	35
4.5- Serial Settings → Serial portX.....	36
4.5.1.- Serial Settings >> Serial portX	36
4.5.2.- Serial Settings → SSL Certificates	42
4.6- External Devices.....	45
4.6.1- External Devices → Logger configuration	45
4.6.2- External Devices → Temperature Sensor.....	51
4.6.3- External Devices → Modbus Devices	54
Basic Mode	54
Expert Mode.....	56

4.6.4- External Devices → GPS Receiver	64
4.6.5- External Devices → Generic Serial Device	66
4.6.6- External Devices → IEC102 Meter.....	68
4.7- Device Manager → KARE.....	74
4.7.1- KARE.....	74
4.8- Other.....	76
4.8.1- Other → AT Command.....	76
4.8.2- Other → DynDns	77
4.8.3- Other → Private DynDns	79
4.8.4- Other → SMS Control.....	82
4.8.6- Other → Periodic autoreset.....	85
4.8.7- Other → Time Servers (NTP).....	87
4.8.8- Other → Remote console (TCP Server).....	89
4.8.9- Other → SNMP	91
4.8.10- Other >> TACACS+	94
4.8.11- Other >> LDAP	95
4.8.12- Other → MQTT	96
MQTT Broker	96
MQTT Client.....	96
Status and certificates.....	99
4.8.13- Other → HTTP / HTTPS.....	100
4.8.14- Other → User Permissions.....	102
4.8.15- Other → Passwords	103
Authentication Methods	104
Users activity.....	104
4.8.16- Other → CA Certificates	106
4.8.17- Other → Email Configuration.....	107
4.8.18- Other → Modbus Slave	109
Comandos AT mediante protocolo Modbus	110
Recibir SMS por Modbus TCP	112
4.8.19 - Other → TITAN Scripts.....	113
Opciones de configuración de los TITAN Scripts.	115
JSON Transformer Function Script.....	144
MQTT Topic Function Script.....	144
4.8.20 - Other → Connectivity tools.....	146
4.8.21 - Other → Digital I/O	148
Configuración de las entradas digitales.....	149
Configuración de las salidas digitales.....	150
4.8.22- Other → Custom Skin.....	152
4.8.23- Other → Custom Led.....	153

4.8.24- Other → SYSLOG	154
4.8.25- Other → Backup / Factory.	156
4.8.26- Other → Firmware Upgrade	157
4.8.27- Other → Reboot.	159
4.8.28- VPN → OpenVPN Server.....	160
4.8.29- VPN → OpenVPN Client	162
4.8.30- VPN → IPSec	164
4.8.31- VPN → Zerotier	167
5.- Comandos AT.....	169
6.- Novedades en versiones de Firmware.....	188

Notas generales

El destinatario considera que el producto es aceptado y se proporciona sin interfaz para los productos del destinatario. La documentación y/o el producto se proporcionan con fines de prueba, evaluación, integración e información. La documentación y/o productos se proporcionan "tal cual" y pueden contener deficiencias. La documentación y/o productos se proporcionan sin garantía de ningún tipo, expresa o implícita. En la máxima medida permitida por la ley aplicable, Webdyn niega aún más todas las garantías; incluidas, entre otras, cualquier garantía implícita de comerciabilidad, integridad, idoneidad para un propósito particular y no infracción de los derechos de terceros. Todo el riesgo derivado del uso o rendimiento del producto y la documentación queda con el destinatario. Este producto no está diseñado para su uso en dispositivos o sistemas de soporte vital donde se pueda esperar razonablemente que el mal funcionamiento del producto provoque lesiones personales. Las aplicaciones que incorporan el producto descrito deben estar diseñadas de acuerdo con las especificaciones técnicas proporcionadas en estas pautas. El incumplimiento de cualquiera de los procedimientos requeridos puede provocar un mal funcionamiento o serias discrepancias en los resultados.

Además, se deben seguir todas las instrucciones de seguridad relacionadas con el uso de sistemas técnicos móviles, incluidos los productos GSM, que también se aplican a los teléfonos celulares. Webdyn o sus proveedores, independientemente de cualquier teoría legal en la que se base el reclamo, no serán responsables de ningún daño consecuente, incidental, directo, indirecto, punitivo u otro tipo de daños (incluidos, entre otros, daños por pérdida de beneficios comerciales, interrupción del negocio, pérdida de información o datos comerciales, u otra pérdida pecuniaria) que surja del uso o la incapacidad de usar la documentación y/o el producto, incluso si Webdyn ha sido informada de la posibilidad de tales daños. Las limitaciones de responsabilidad anteriores no se aplicarán en caso de responsabilidad obligatoria, por ejemplo, conforme a la Ley de Responsabilidad de Productos de España, en caso de intención, negligencia grave, lesiones de la vida, el cuerpo o la salud, o el incumplimiento de una condición que va a la raíz del contrato. Sin embargo, las reclamaciones por daños y perjuicios derivados del incumplimiento de una condición, que va a la raíz del contrato, se limitarán al daño previsible, que es intrínseco al contrato, a menos que sea causado por negligencia intencional o grave o basado en la responsabilidad por lesiones de vida, cuerpo o salud. La disposición anterior no implica un cambio en la carga de la prueba en detrimento del destinatario. Sujeto a cambios sin previo aviso. La interpretación de esta nota general se regirá e interpretará de acuerdo con la ley española sin referencia a ninguna otra ley sustantiva.

Información importante

Esta descripción técnica contiene información importante para el inicio y uso de los equipos basados en TITAN. Léalo detenidamente antes de comenzar a trabajar con ellos. La garantía será nula si se producen daños debido al incumplimiento de estas instrucciones de uso. No podemos aceptar ninguna responsabilidad por pérdidas consecuentes.

Revisiones

VERSIÓN. 7.02

1.- Introducción.

El firmware TITAN habilita equipos 2G/3G/4G con capacidades avanzadas de Gateway.

Además de las capacidades clásicas de router, los equipos basados en TITAN permiten realizar pasarelas 4G/3G/2G - RS232/485, ejecutar comandos AT por SMS (para chequear coberturas, conmutar relés, leer entradas digitales, etc.), aceptar llamadas GSM de datos (CSD) para acceder a dispositivos como contadores eléctricos, leer de forma autónoma dispositivos Modbus RTU o Modbus TCP, enviar a la nube datos de temperaturas, distancias, y muchas cosas más.

Para una mayor comprensión de las posibilidades de estos equipos, se recomienda la lectura del capítulo 2 de este manual, las FAQ. Tras esa lectura tendrá una visión más concreta de lo que realmente puede hacer. Una vez leídas las FAQ, se recomienda dar un vistazo general a las notas de aplicación (documentos PDF externos a este documento). Dichos ejemplos le darán una visión mucho más clara de las posibilidades de estos equipos.

A todos los usuarios de nuestros módems y routers les apoyamos cuando lo necesitan con un soporte técnico gratuito de respuesta rápida y eficaz. Por lo que, si tras la lectura de este manual le quedan dudas, por favor, no deje de comentárnoslas en la dirección de email iotsupport@mtxm2m.com. Lo mismo si tiene la necesidad de alguna característica no incluida en nuestros equipos, o si precisa de una customización, coméntenoslo y lo estudiaremos en profundidad.

2.- FAQ. Conceptos básicos.

■ ¿Qué puedo hacer con los equipos basados en TITAN?

Pues básicamente es posible hacer lo mismo que con un router 4G/3G/2G estándar, pero añadiendo un buen número de prestaciones avanzadas de gateway. Por ejemplo, puede dar conectividad a Internet a dispositivos que estén conectados a su puerto Ethernet, así como hacer NAT para conectar desde Internet a dispositivos que cuelguen de dicho puerto.

■ ¿Es posible dar conectividad a Internet a dispositivos Wifi?

Efectivamente, los equipos basados en TITAN que cuenten con conectividad Wifi pueden trabajar como Access Point Wifi, y por tanto pueden dar conectividad a Internet a dispositivos clientes Wifi que se conecten a él. También pueden configurarse como Cliente Wifi, es decir, el equipo basado en TITAN puede conectarse a un Access Point Wifi existente en su infraestructura y utilizar dicha conexión como acceso a internet.

■ ¿Dispone de pasarelas serie?

Sí, se pueden llegar a tener tantas pasarelas 4G/3G/2G-Serie como puertos serie tenga el equipo que esté utilizando. Estas pasarelas pueden ser de tipo TCP Client o TCP Server y pueden trabajar todas de forma simultánea.

■ ¿Pasarelas serie tipo RS232 o RS485?

Todos los equipos disponen de al menos un puerto serie RS232 y otro RS485 o los dos. Dependiendo del tipo de puerto serie las pasarlas serán de un tipo, de otros o de los dos.

Los equipos basados en TITAN permiten establecer pasarelas IP - RS232/485 ¿pero podrían ser pasarelas seguras SSL/TLS?

Sí, el equipo basado en TITAN permite configurar las pasarelas IP - RS232/485 de tipo Servidor y de tipo Cliente con seguridad SSL/TLS con autenticación mutua por certificado digital (cliente / servidor).

■ ¿El firmware TITAN permite además la gestión de llamada CSD? Es decir, ¿puedo tener una pasarela 4G/3G/2G-Serie funcionando pero que además acepte una llamada de datos GSM/CSD para la lectura de un contador eléctrico).

Sí, pero con condiciones. Si el equipo basado en TITAN está funcionando en modo 2G no habrá ningún problema. El equipo aceptará la llamada CSD cuando la llamada se reciba (para realizar una pasarela CSD-Serie) y al finalizar la llamada retomará la pasarela 2G-Serie. Si el equipo está configurado para trabajar también en modo 3G o 4G la aceptación de la llamada CSD/GSM dependerá de su proveedor de telefonía ya que no todos los operadores lo permiten. Por ejemplo, si utiliza Movistar u Orange y tiene el equipo funcionando en modo "auto 4G/2G" no habrá problema con la aceptación de la llamada CSD independientemente de si el equipo basado en TITAN está trabajando en modo 2G o 4G (en 4G hará el failover sobre 2G), pero con el operador Vodafone no lo hará al no estar soportado.

- **Quiero un router 4G/3G/2G pero necesito poder enviar comandos AT directamente al equipo basado en TITAN, para enviar SMS, consultar coberturas, etc. ¿Lo permiten los equipos basados en TITAN?**

Sí, todos los modelos y de varias maneras. Es posible enviar comandos AT de forma REMOTA desde una conexión "tipo Telnet", o vía SSH, vía Modbus TCP, vía SNMP, vía HTTP/HTTPs, MQTT/MQTTs, por SMS e incluso también comandos embebidos en las propias pasarelas IP-Serie. También es posible enviar comandos AT de forma LOCAL a través del puerto Ethernet vía "Telnet", SSH, Modbus TCP, SNMP, HTTP/HTTPs y a través del puerto serie RS232/RS485 vía comandos AT embebidos, o Modbus RTU.

- **¿Soportan los equipos basados en TITAN una pasarela del tipo Modbus TCP a Modbus RTU?**

Sí, soporta esa conversión de esos protocolos, por lo que si necesita acceder de forma remota a dispositivos Modbus RTU el equipo basado en TITAN se lo permitirá haciendo de pasarela Modbus TCP a Modbus RTU.

- **¿Y el equipo basado en TITAN también puede operar de forma autónoma leyendo dispositivos Modbus RTU o Modbus TCP y enviando las lecturas a la nube?**

También. Los equipos basados en TITAN pueden leer dispositivos Modbus RTU y/o Modbus TCP, incluso combinados, almacenar las lecturas en su interior, y enviarlas a plataformas WEB mediante un objeto JSON vía HTTP/HTTPs, MQTT/MQTTs o FTP.

- **¿Y si el equipo basado en TITAN está leyendo dispositivos Modbus RTU/TCP de forma autónoma, me impide conectarme de forma esporádica y remota a los dispositivos Modbus RTU/TCP desde mi oficina para hacer lecturas puntuales, cambiar el firmware, etc?**

No. Puede tener el equipo basado en TITAN configurado para leer dispositivos Modbus de forma autónoma y establecer una pasarela directa esporádica para acceder a los dispositivos Modbus RTU desde sus instalaciones.

- **¿Los equipos basados en TITAN tienen capacidad de datalogger y pueden almacenar datos?**

Efectivamente. Como se comentaba anteriormente los equipos basados en TITAN pueden almacenar bastantes tipos de datos para su posterior envío a plataformas web, MQTT, FTP. Entre ellos, por ejemplo, las lecturas de dispositivos Modbus RTU/TCP, pero también lecturas de temperaturas, datos serie RS232/RS485 genéricos, lecturas de contadores IEC-102, entradas y salidas digitales, etc

- **¿Cómo se configuran los equipos basados en TITAN?**

Hay varias formas de configurar los Equipos basados en TITAN, pero generalmente toda la configuración de los equipos se puede realizar a través de configuración web, es decir, a través del webserver interno de los equipos.

- **¿Es posible leer / cargar una configuración completa en los equipos? Esto facilita el proceso de producción cuando el número de dispositivos a configurar es significativo.**

Sí, es posible hacer backups / restauraciones de configuración completos (para copiar la configuración de un equipo basado en TITAN en otro equipo basado en TITAN).

- **¿Es posible pedir a fábrica los equipos basados en TITAN precargados con una configuración?**

Sí, es posible. Pero para volúmenes elevados (>500 unidades). Consulte con su comercial para más información.

- **¿Soportan el servicio DynDNS?**

Por supuesto, siendo compatible también con NO-IP. Además, también tiene la opción adicional de “DNS privado” para enviar su IP actual cada vez que ésta cambie o de forma periódica, a un servidor privado, por ejemplo, el de su empresa. En esta opción adicional, además de enviar la dirección IP actual se adjuntan otros datos, como cobertura, tecnología, IMEI, estado de las entradas y salidas digitales, etc.

- **¿Entonces el equipo basado en TITAN permite la gestión de Entradas y Salidas digitales?**

Sí. Si su modelo de equipo basado en TITAN dispone de entradas o salidas digitales las gestionará. Es posible configurar muy fácilmente el datalogger interno para almacenar y enviar a una plataforma web (vía HTTP/HTTPS, MQTT/MQTTS o FTP) cada vez que se produce un cambio en una entrada digital o bien configurar un periodo de tiempo para la lectura y envío del estado de las mismas. También es posible consultar en cualquier momento el estado de una entrada digital por comando AT (que pueden ser enviados por Telnet, SSH, HTTP/S, SMS, MQTT/S, Modbus, SNMP, RS232, RS485...). Lo mismo para las salidas digitales.

Además, es posible acceder a las entradas/salidas digitales desde la sección del equipo “TITAN Scripts”, desde donde es posible programar un pequeño script (en JavaScript) para que el equipo utilice dichas entradas/salidas digitales a conveniencia del usuario.

- **¿Los equipos basados en TITAN disponen de reloj?**

Sí, disponen de reloj interno. Éste se sincroniza por NTP a través de Internet.

- **¿Se pueden configurar los equipos basados en TITAN por SMS?**

Sí, los equipos basados en TITAN se pueden configurar por comandos AT. Y los comandos AT (además de por Telnet, SSH, HTTP/S, MQTT/S, Modbus, SNMP, RS232, RS485) se pueden enviar al equipo por SMS. Pueden enviarse comandos al equipo para reiniciarlo, cambiar su configuración, averiguar su dirección IP, chequear cobertura, ...

- **¿Es posible personalizar el entorno de configuración Web con logos e imágenes de empresa?**

Sí. Cualquier usuario es libre de customizar el entorno web de configuración con sus logos, pies y título de página, etc. Incluso es posible escoger qué menús su cliente final puede ver o modificar.

- **¿Los equipos basados en TITAN disponen de algún led indicativo?**

Sí, el número de leds depende del modelo. Puede escoger la funcionalidad de los mismos para indicar la cobertura, si el equipo dispone de IP, problemas de SIM, etc. También es posible utilizar los LEDs desde los TITAN Scripts, donde es posible programar un pequeño script JavaScript de usuario para encender o apagar un led del equipo en función de las necesidades particulares (por ejemplo, cuando una entrada digital está activada).

- **¿Es posible utilizar un equipo basado en TITAN como datalogger Serie?**

Sí. Un equipo basado en TITAN puede configurarse para leer todo lo que llega por el puerto serie, almacenarlo en su datalogger interno y enviarlo por HTTP/S, MQTT/S o FTP a una plataforma a través de Internet.

- **¿Y el equipo basado en TITAN tiene la posibilidad de ser utilizado para leer contadores IEC 870-5-102?**

Sí. Con el equipo basado en TITAN podrá hacer lo siguiente en referente a la lectura de contadores eléctricos con protocolo IEC 870-5-102:

- 1.- Leer el contador a través de una pasarela 4G/3G/2G-RS232/485
- 2.- Leer el contador a través de una llamada CSD de datos
- 3.- Configurar el equipo basado en TITAN para que lea el contador de forma autónoma cada periodo de tiempo configurado, enviando los valores instantáneos a una plataforma web (vía HTTP/S, MQTT/S, o FTP) cada periodo de tiempo y también, si lo desea, enviando los cierres fiscales una vez al día. La curva de carga se solicita bajo demanda (no tiene disparo periódico automático en la configuración estándar; ver punto 4)..
- 4.- En la sección “TITAN scripts”, programar un pequeño script en JavaScript para leer el contador eléctrico a voluntad (por ejemplo, supervisar continuamente una determinada variable, obtener valores medios más exactos que los cuarto horarios, etc.).

- **¿Es posible configurar una VPN con un equipo basado en TITAN?**

Sí. El equipo basado en TITAN permite configurar una VPN del tipo IPSEC, OpenVPN o ZeroTier.

- **¿Qué otras características relevantes tienen el equipo basado en TITAN?**

A lo largo de este manual encontrará detalladas las distintas características, pero además de lo ya indicado en los párrafos anteriores, el equipo basado en TITAN permite:

- Configuración de autoreset (autoreset periódico, a una hora determinada, autoresetarse en caso de problemas de conectividad IP, etc)
- Servicio de autenticación por Tacacs+ para HTTP, Telnet y SSH
- Configuración segura a través de HTTPS
- Configuración de permisos de usuario para poder acceder a las distintas funcionalidades del equipo basado en TITAN en función de los roles “admin”, “user”, “guest”.
- Configuración de servicio SMTP para el envío de Emails
- Configuración como SLAVE MODBUS. Esto permite que el equipo basado en TITAN sea configurado y/o leído, por Modbus. Por ejemplo, puede servir para leer vía Modbus el estado de sus entradas digitales, u obtener la hora del equipo, cambiar una salida digital, etc todo desde un equipo Modbus Master como puede ser un PLC.
- TITAN scripts. Esta sección le permite escribir un pequeño script de usuario en JavaScript para, por ejemplo: leer dispositivos serie o enviarles datos personalizados, leer dispositivos Modbus, leer o cambiar una salida digital, enviar SMS, EMAILs, traps SNMP, leer un contador IEC 870-5-102, enviar mensajes MQTT, realizar PINGs, cambiar el estado de los LEDs del equipo, escribir y leer en ficheros, enviar o recibir ficheros por FTP, etc etc

- **¿Soporta el router Titan comunicaciones TLS 1.0, TLS1.1 y TLS1.2?**

Sí, aunque se desaconseja el uso del TLS1.0 y TLS1.1

3.- Configuración paso a paso.

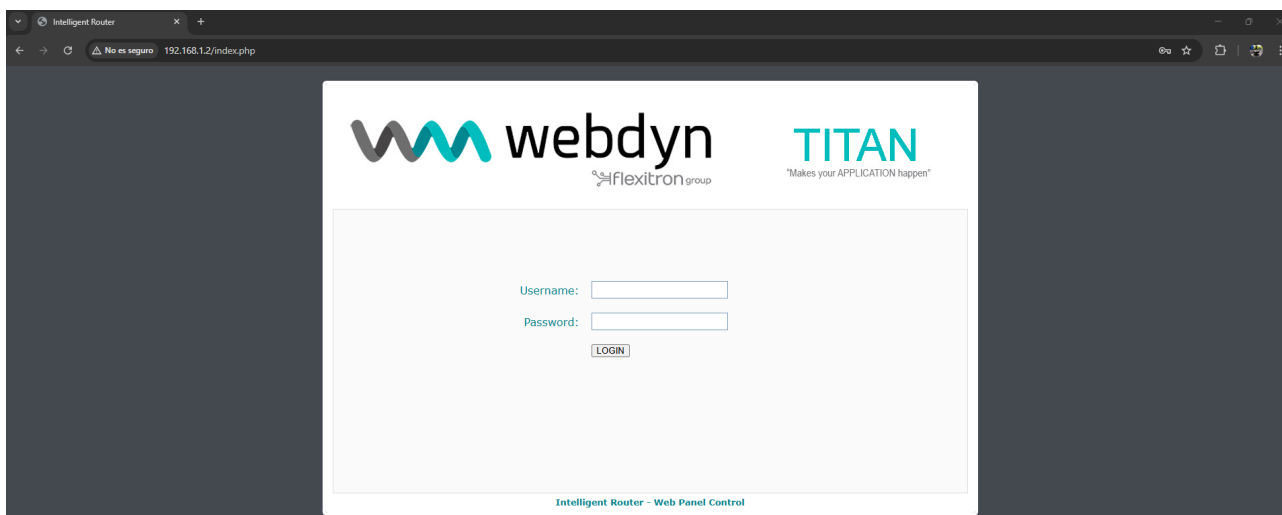
Como se mencionó en apartados anteriores, la configuración de los equipos basados en TITAN se realiza principalmente a través de su entorno web.

¿Qué se necesita?

- Un PC con navegador web (Chrome, Brave, Firefox, ...) y con puerto Ethernet.
- Un cable Ethernet para interconectar el PC con el equipo.

Pasos para acceder al entorno de configuración.

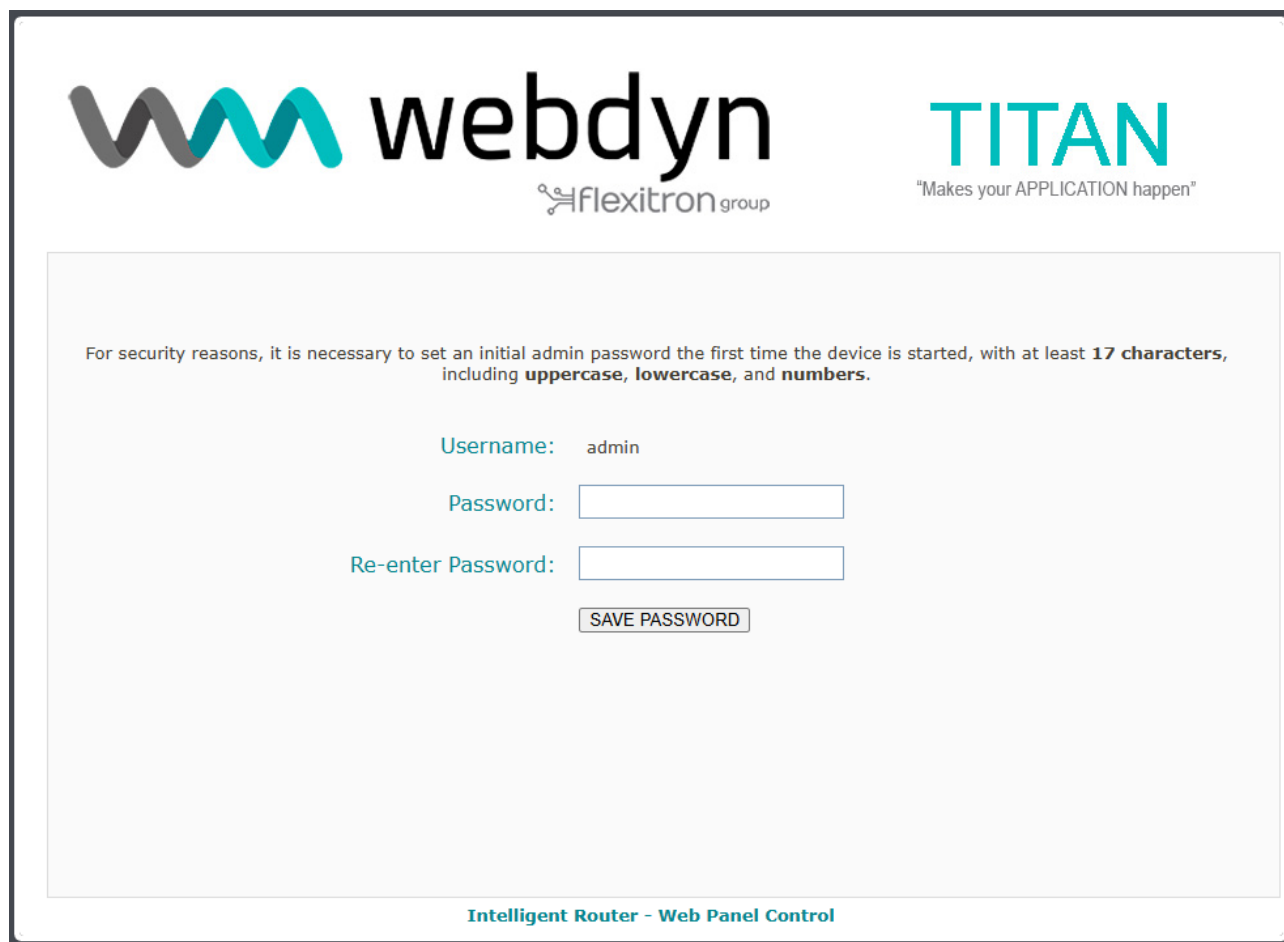
- Conectar un cable Ethernet entre el PC y el equipo.
- El PC tiene que tener una IP fija, dentro del rango 192.168.1.X, pues la dirección IP por es 192.168.1.2
- Abrir un explorador, con la dirección <http://192.168.1.2> . Debería aparecer una ventana como la siguiente:



NOTA

Cuando el equipo viene de fábrica o su configuración se restaura a “*Factory Settings*”, la primera vez será necesario crear una nueva contraseña para iniciar sesión. **Por razones de seguridad**, dicha contraseña debe seguir las recomendaciones de la “European Cybersecurity Certification Group”: **como mínimo 17 caracteres de los cuales se incluya al menos una mayúscula, una minúscula y un número.**

En este caso, la pantalla de inicio de sesión es tal que así:



The image shows a web browser window displaying the login interface for the Webdyn TITAN Intelligent Router. At the top left is the Webdyn logo, which consists of a stylized 'w' made of three overlapping waves in grey and teal, followed by the text 'webdyn' in a bold, sans-serif font, and 'flexitron group' in a smaller font below it. To the right of the Webdyn logo is the TITAN logo, with the word 'TITAN' in a large, bold, teal font, and the tagline '"Makes your APPLICATION happen"' in a smaller font below it. The main content area is a light grey rectangle with a thin border. Inside this rectangle, at the top, is a message: 'For security reasons, it is necessary to set an initial admin password the first time the device is started, with at least **17 characters**, including **uppercase**, **lowercase**, and **numbers**.' Below this message are three labels: 'Username:', 'Password:', and 'Re-enter Password:'. The 'Username:' label is followed by the text 'admin'. The 'Password:' and 'Re-enter Password:' labels are each followed by a white rectangular input field with a thin blue border. Below the 'Re-enter Password:' input field is a button with the text 'SAVE PASSWORD' in a small, bold, sans-serif font. At the bottom of the light grey rectangle, centered, is the text 'Intelligent Router - Web Panel Control' in a small, bold, sans-serif font.

Notas adicionales.

- Por razones de seguridad se recomienda configurar el equipo en una red aislada confiable o bien conectando un cable punto a punto entre el PC y el equipo. Se recomienda activar el protocolo HTTPS, pues HTTP conlleva riesgos de seguridad.

4.- Configuración

4.1- Mobile

La sección Mobile hace referencia a todo lo relativo a las configuraciones 4G/3G/2G del equipo, desde el estado de la conexión, parámetros de configuración de red y supervisión de conexión.

4.1.1- Mobile → Status

Esta pantalla muestra el estado general del equipo.

- **Firmware Version:** Versión de FW del equipo
- **WAN Mobile IP:** dirección IP WAN (dirección IP asignada a la conexión 4G/3G/2G) si ésta está disponible.
- **GSM Module:** Indica el fabricante y modelo de módulo GSM interno del equipo.
- **IMEI:** IMEI del dispositivo.
- **SIM:** tarjeta SIM utilizada (SIM1/SIM2) y su estado.
- **Network (2G/3G/4G):** Indica si la conexión WAN actual está usando la red 2G (GPRS), 3G o 4G
- **Signal Strength:** Indica la fuerza de la señal. 0=nula, 31=máxima
- **Extra signal info:** Para conectividad 3G y 4G, indica el RSCP/ECN0 y RSRP/RSRQ
- **Temperature:** Muestra la temperatura interna del procesador.

**webdyn**
flexitron group

TITAN
"Makes your APPLICATION happen"

★ **Mobile**

◆ Status

◆ Basic Settings

◆ Keep Online

★ **Ethernet**

◆ Basic Settings

◆ DHCP Server

★ **Wifi**

◆ Basic Settings

◆ DHCP Server

★ **Firewall**

◆ NAT

◆ Authorized IPs

◆ MAC Filter

◆ Routes

★ **Serial Settings**

◆ Serial Port1-RS232

◆ Serial Port2-RS485

◆ SSL Certificates

★ **External Devices**

◆ Logger configuration

◆ ModBus Devices

◆ Generic Serial Device

◆ Temperature Sensor

▶ **Mobile ▶ Status**

Firmware version:

5.3.7.02.RC.1 (Webdyn EasyRouter)

WAN Mobile IP:

WAN IP (2G/3G/4G) Network

GSM Module:

EC21
Revision: EC21EUGAR06A07M4G

IMEI:

865583047805675

Device identification

SIM:

SIM-1 (SIM READY)

Used SIM and status

Network (2G/3G/4G):

4G (VODAFONE ES)

Used network at this moment

Signal Strength:

(-79dBm)

Signal Strength (0 ... 31)

Extra signal info:

For 3G & 4G Network



Temperature:

Temperature of internal processor (°C)

4.1.2- Mobile → Basic Settings

Esta sección permite configurar los parámetros de la conexión WAN 4G/3G/2G. Deberá conocer algunos datos de su tarjeta SIM, como el APN, login y password. Su proveedor debe proporcionárselos.

- **Mobile WAN:** Si necesita conectividad IP (4G/3G/2G), debe configurar esta opción como “Enabled”. Si no va a utilizar tarjeta SIM, configúrela como “Disabled”. Las opciones son:
 - *Enabled (IP active):* habilita la conectividad IP (4G/3G/2G).
 - *Disabled (only SMS and CSD):* deshabilita la conectividad IP, pero mantiene los SMS y las llamadas CSD.
 - *Disabled (GSM module off):* deshabilita por completo cualquier tipo de conectividad ofrecida por el módulo de comunicaciones.
- **Sim Mode:** dependiendo del modelo de dispositivo se dispone de 1 slot de SIM o 2 slot de SIM. Si dispone de 2 slots de SIM:
 - *SIM1:* el router utilizará la SIM1.
 - *SIM2:* el router utilizará la “SIM2”.
 - *SIM1 + SIM2:* backup. El router utilizará la SIM1 y en caso de problemas utilizará la SIM2.
- **SIM1 APN:** APN del operador de la SIM1. Debe consultarlo con su proveedor GSM
- **SIM1 Username:** Username del operador de la SIM1. Debe consultarlo con su proveedor GSM
- **SIM1 Password:** Password del operador de la SIM 1. Debe consultarlo con su proveedor GSM
- **SIM1 Pin:** si su tarjeta SIM1 tiene PIN debe especificarlo aquí.
- **SIM1 Auth:** método de autenticación “NONE, PAP”, CHAP , AUTO (PAP ó CHAP)”.
- **SIM2 APN:** APN del operador de la SIM2. Debe consultarlo con su proveedor GSM
- **SIM2 Username:** Username del operador de la SIM2. Debe consultarlo con su proveedor GSM
- **SIM2 Password:** Password del operador de la SIM 2. Debe consultarlo con su proveedor GSM
- **SIM2 Pin:** si su tarjeta SIM2 tiene PIN debe especificarlo aquí.
- **SIM2 Auth:** método de autenticación “NONE, PAP, CHAP , AUTO (PAP ó CHAP)”.
- **Network selection:**
 - *Auto (4G/3G/2G):* el equipo usará 4G en caso de haber cobertura, o 3G o 2G en caso contrario.
 - *Auto (4G/2G):* el equipo usará 4G en caso de haber cobertura, o 2G en caso contrario.
 - *4G:* el equipo usará la red 4G en todos los casos. Si no hay cobertura 4G el equipo no cambiará a 2G ni a 3G
 - *3G:* el equipo usará la red 3G en todos los casos. Si no hay cobertura 3G el equipo no cambiará a 2G.
 - *2G:* el equipo usará la red 2g en todos los casos.
- **DNS selection:**
 - *Get DNS from Operator :* Hace que las DNS utilizadas por el equipo sean las asignadas por el operador de telefonía.
 - *Selected DNS Servers (also used for failover if enabled):* Hace que los servidores DNS utilizados sea los especificados en los parámetros DNS1 y DNS2 comentados a continuación.

- **DNS1 y DNS2:** Servidores de DNS para la resolución de nombres de dominio. Recomendable usar los de Google 8.8.8.8 y 8.8.4.4 o los que le indique su proveedor. Estos DNS serán los usados si se selecciona la característica de FailOver cuando la salida de datos se produzca por la interfaz WAN 4G/3G/2G
- **Remote webserver management:** Si activa la casilla podrá acceder a la configuración web del equipo de forma remota, a través de su dirección IP pública (la indicada en Mobile → Status). Puede cambiar el puerto desde el menú Other→Http / Https




- ★ **Mobile**
 - ◇ Status
 - ◇ Basic Settings
 - ◇ Keep Online
- ★ **Ethernet**
 - ◇ Basic Settings
 - ◇ DHCP Server
- ★ **Wifi**
 - ◇ Basic Settings
 - ◇ DHCP Server
- ★ **Firewall**
 - ◇ NAT
 - ◇ Authorized IPs
 - ◇ MAC Filter
 - ◇ Routes
- ★ **Serial Settings**
 - ◇ Serial Port1-RS232
 - ◇ Serial Port2-RS485
 - ◇ SSL Certificates
- ★ **External Devices**
 - ◇ Logger configuration
 - ◇ ModBus Devices
 - ◇ Generic Serial Device
 - ◇ Temperature Sensor
 - ◇ IEC102 Meter
 - ◇ GPS Receiver
- ★ **VPN**
 - ◇ IPSec
 - ◇ OpenVPN Client
 - ◇ OpenVPN Server
 - ◇ ZeroTier
- ★ **Device Manager**
 - ◇ KARE
- ★ **Other**
 - ◇ AT Command
 - ◇ DynDns
 - ◇ Private DynDns
 - ◇ Sms control
 - ◇ Periodic Autoreset
 - ◇ Time Servers
 - ◇ Remote Console
 - ◇ Snmp
 - ◇ Tacacs+
 - ◇ Ldap
 - ◇ Mqtt / Mqtts
 - ◇ Http / Https
 - ◇ User Permissions
 - ◇ Passwords Web UI
 - ◇ CA Certificates

▶ Mobile ▶ Basic Settings

Mobile WAN	Enabled (IP active)	Enable Wireless WAN interface
Sim Mode	SIM1	Sim selection
SIM1 APN:	airtelwap.es	SIM Card 1 APN
SIM1 Username:		SIM Card 1 username
SIM1 Password:		SIM Card 1 password
SIM1 Pin:		SIM Card 1 PIN
SIM1 Auth:	None	SIM card 1 authentication
SIM2 APN:		SIM Card 2 APN
SIM2 Username:		SIM Card 2 username
SIM2 Password:		SIM Card 2 password
SIM2 Pin:		SIM Card 2 PIN
SIM2 Auth:	None	SIM card 2 authentication
Network selection:	Auto 4G/3G/2G	Network selection
DNS selection:	Get DNS from Operator	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote webserver management:	☐	Enable remote webserver management
SAVE CONFIG		
Failover:	Failover config	4G/3G interface will be activated when Ethernet/Wifi connectivity fails.
Operators:	Operators config	List of operators for automatic apn.
Sim swapping:	SIM swapping config	Sim swapping configuration

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.1.3- Mobile → Keep Online

Desde esta pantalla puede configurar un PING para asegurar la conectividad del equipo. En caso de fallar el PING en las ocasiones configuradas la conexión 4G/3G/2G se reiniciará. Es aconsejable el uso de esta característica.

- **Enabled:** active la casilla para permitir al equipo basado en TITAN enviar un PING periódico para comprobar la conectividad.
- **Ping Server:** indica la dirección IP o DNS del servidor contra el que hacer el PING.
- **Period:** indica cada cuántos minutos se debe realizar un PING de comprobación
- **Timeout:** indica los segundos que debe esperar el equipo respuesta al PING para considerar que el PING falló.
- **Retries:** indica el número de reintentos de PING que deben realizarse antes de considerar problemas de conectividad y reiniciar la sesión 4G/3G/2G.
- **Retry period:** indica los minutos que deben transcurrir entre reintentos.

The screenshot shows the webdyn TITAN configuration interface. The top header features the webdyn logo (a stylized 'w' with a blue and grey wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". Below the header is a sidebar menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), and Firewall (NAT, Authorized IPs, MAC Filter, Routes). The main content area is titled "Mobile ► Keep Online" and contains the following settings:

Setting	Value	Description
Enabled:	☒	Enable PING method for keep Mobile WAN Session
Ping Server:	8.8.8.8	IP or DNS address
Period:	5	Minutes between pings (1 ... 1440)
Timeout:	10	Timeout in seconds (5 ... 20)
Retries:	1	Number of retries (0 ... 9)
Retry period:	1	Minutes between retries (1 ... 1440)

At the bottom of the settings area is a "SAVE CONFIG" button.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.1.4- Mobile → Basic Settings → FailOver

Esta pantalla de configuración es accesible desde el botón situado en la zona inferior de la sección de configuración Mobile → Basic Settings.

Permite configurar la característica failover del equipo. Por ejemplo, para configurar la salida de datos del equipo basado en TITAN a través de su interfaz Wifi o Ethernet y, en caso de caída de ésta, levantar la interfaz 4G/3G/2G para que la salida de datos se produzca por ahí hasta que la interfaz Wifi o Ethernet recuperen la conectividad.

- **Enabled:** active la casilla para activar la funcionalidad failover.
- **IP1:** para comprobar la conectividad de la interfaz de failover utilizada (Ethernet o Wifi) el equipo basado en TITAN realiza un PING sobre esta IP de forma periódica. En caso de fallo, se reintenta el ping sobre la IP2.
- **IP2 (backup):** para comprobar la conectividad de la interfaz de failover utilizada (Ethernet o Wifi) el equipo basado en TITAN realiza un PING sobre esta IP2 si IP1 falla. En caso de fallo, se activa la interfaz WAN (4G/3G/2G) para ser usada mientras dure el fallo de conectividad.
- **Interface:** interfaz de comunicaciones (ethernet o wifi) utilizada como interfaz primaria de salida de datos.
- **Period:** periodo en segundos en los cuales se comprueba el estado de la conectividad.
- **4G/3G/2G interface:** comportamiento de la interfaz de backup 4G/3G/2G. Es posible escoger entre el modo "On when failover" o "Always on". En el modo "On when failover" la interfaz WAN 4G/3G/2G está apagada y sólo cuando la interfaz primaria falla (interfaz wifi o ethernet) se activa y tras ello se utiliza. En modo "Always on" la interfaz WAN 4G/3G/2G está siempre activa y cuando la interfaz primaria falla (Wifi o Ethernet) se utiliza. Al estar la interfaz WAN 4G/3G/2G ya activa el cambio es más rápido.

★ **Mobile**

- ◇ Status
- ◇ Basic Settings
- ◇ Keep Online

★ **Ethernet**

- ◇ Basic Settings
- ◇ DHCP Server

★ **Wifi**

- ◇ Basic Settings
- ◇ DHCP Server

★ **Firewall**

- ◇ NAT
- ◇ Authorized IPs
- ◇ MAC Filter
- ◇ Routes

★ **Serial Settings**

- ◇ Serial Port1-RS232
- ◇ Serial Port2-RS485
- ◇ SSL Certificates

★ **External Devices**

- ◇ Logger configuration
- ◇ ModBus Devices
- ◇ Generic Serial Device
- ◇ Temperature Sensor
- ◇ IEC102 Meter
- ◇ GPS Receiver

★ **VPN**

- ◇ IPsec
- ◇ OpenVPN Client

▶ **Mobile ▶ Basic Settings ▶ WAN Failover**

Enabled:	☐	Enable failover.
IP1:		IP address for check Ethernet/Wifi connection. Mandatory. Example: 8.8.8.8
IP2 (backup):		IP or DNS address for check Ethernet/Wifi connection. Example: 8.8.4.4
Interface:	ETH	Interface for failover
Period:	5 seconds	Connectivity checking period
4G/3G/2G interface:	Always On (fast mode)	Behaviour of 4G/3G/2G interface

SAVE CONFIG

▶ **Mobile ▶ Basic Settings ▶ WAN Failover ▶ Status**

Activated:	---	Failover interface (4G/3G/2G) used
Interface:	---	Current WAN interface

REFRESH

Important note: if failover feature is enabled, the active DNS when 4G/3G/2G connection is used are 'preferred DNS1 and preferred DNS2'

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.1.5- Mobile → Basic Settings → Operators

Esta pantalla de configuración es accesible desde el botón situado en la zona inferior de la sección de configuración Mobile → Basic Settings.

Permite configurar el APN, user y password a utilizar en caso de APN automático. Puede usar el APN en modo automático especificando el texto “auto” (sin comillas) en los campos APN de la sección Mobile → Basic Settings.

El fichero “operators.mtx” debe tener el formato:

<ID_Operator>:<apn>,<username>,<password> (donde <username>,<password> son opcionales)

The screenshot displays the webdyn interface for configuring mobile operators. The sidebar on the left contains a tree view with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor, IEC102 Meter, GPS Receiver), and VPN (IPSec, OpenVPN Client). The main panel is titled 'Mobile > Operators' and includes an 'Operator List' section with a note: 'Operator List (used only when Mobile > BASIC SETTINGS > APN is set to "auto"). Format: idOperator:<apn>,<username>,<password>'. Below this is a text area labeled 'File: 'operators.mtx'' containing a list of operator configurations, such as '20205:internet.vodafone.gr', '20209:gint.b-online.gr', '20210:gint.b-online.gr', '20402:internet.tele2.nl', '20404:web.vodafone.nl', '20408:basicinternet', '20601:internet.proximus.be', '20610:internet.be,mobistar,mobistar', '20620:orangeinternet', '20800:orange.fr', '20801:orange.fr', '20810:websfr', '20811:websfr', '20820:ebouygtel.com', '20821:b2bouygtel.com', '21401:airtelnet.es', '21403:internet', '21406:airtelnet.es', '21407:movistar.es', '21408:internet.euskaltel.mobi', '21416:internet.telecable.es', '21417:internet.mundo-r.com', '21418:internet.ono.com', '21419:gprs-service.com', '21601:net', '21670:internet.vodafone.net', '21890:mms.bhmobile.ba', '21901:web.htgprs', '21902:mobileinternet.tele2.hr', '21910:data.vip.hr', '22003:gprsinternet', '22004:gprs.monetcg.com', and '22005:vipmobile'. At the bottom of the main panel are two buttons: 'UPDATE' and 'BACK TO MOBILE SETTINGS'.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.1.6- Mobile → Basic Settings → SIM Swapping

Esta pantalla de configuración es accesible desde el botón situado en la zona inferior de la sección de configuración Mobile → Basic Settings (haciendo click sobre el botón con texto “SIM swapping config”). Esta configuración únicamente estará disponible en aquellos dispositivos que dispongan de DUAL SIM.

The screenshot shows the Webdyn TITAN configuration interface. At the top, the Webdyn logo and 'flexitron group' are on the left, and the TITAN logo with the tagline 'Makes your APPLICATION happen' is on the right. A left sidebar contains a menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), and Firewall (NAT, Authorized IPs, MAC Filter). The main content area is titled 'Mobile > Basic Settings > SIM Swapping'. It features four configuration options: 'Main SIM' (a dropdown menu set to 'SIM1'), 'Swap by network' (a text input set to '30'), 'Swap by IP' (a text input set to '90'), and 'Swap by coverage' (a text input set to '0'). There is also an unchecked checkbox for 'Swap by keepalive'. To the right of these inputs, explanatory text is provided: 'Select main SIM after reboot' for the Main SIM dropdown; '(Seconds) Registration fails. (0, 30 ... 1800). Default 30 seconds. 0 = disabled' for Swap by network; '(Seconds) No IP (0, 90 ... 1800). Default 90 seconds. 0 = disabled' for Swap by IP; and '(Seconds) Low coverage (0, 600 ... 86400). Default 0. 0 = disabled' for Swap by coverage. A 'SAVE CONFIG' button is located at the bottom left of the configuration area.

- **Main SIM:** En caso de tener seleccionada una configuración de Dual SIM en el menú “Mobile → Basic settings”, es decir, una configuración “SIM1 + SIM2” este menú permite seleccionar la SIM principal, es decir, la SIM que entrará primero en funcionamiento tras un reset del router Titan.
- **Swap by network:** permite seleccionar un tiempo en segundos en el que, si el router Titan no es capaz de registrarse en la red en los segundos indicados, se iniciará el proceso de cambio de SIM. Un valor “0” indica que esta característica no será usada. El valor mínimo (valor usado por defecto) es “30” segundos y el valor máximo “1800” segundos.
- **Swap by IP:** permite seleccionar un tiempo en segundos en el que, si el router Titan no es capaz de obtener una dirección IP de la red en los segundos indicados, se iniciará el proceso de cambio de SIM. Un valor “0” indica que esta característica no será usada. El valor mínimo (valor usado por defecto) es “90” segundos y el valor máximo “1800” segundos.
- **Swap by coverage:** permite seleccionar un tiempo en segundos en el que, si el router Titan de forma continuada se encuentra en una situación de registro en la red, pero con cobertura crítica, se inicia el proceso de cambio de tarjeta SIM. El valor es “600” segundos y el valor máximo “86400” segundos. El valor por defecto es “0”, deshabilitada.
- **Swap by keep alive:** en caso de estar seleccionada esta opción, si el router Titan reinicia la conexión IP ante un fallo del ping de conectividad de la función keep online (activable desde el menú “Mobile → Keep online”) se producirá un cambio de la tarjeta SIM. Por defecto esta opción está deshabilitada.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

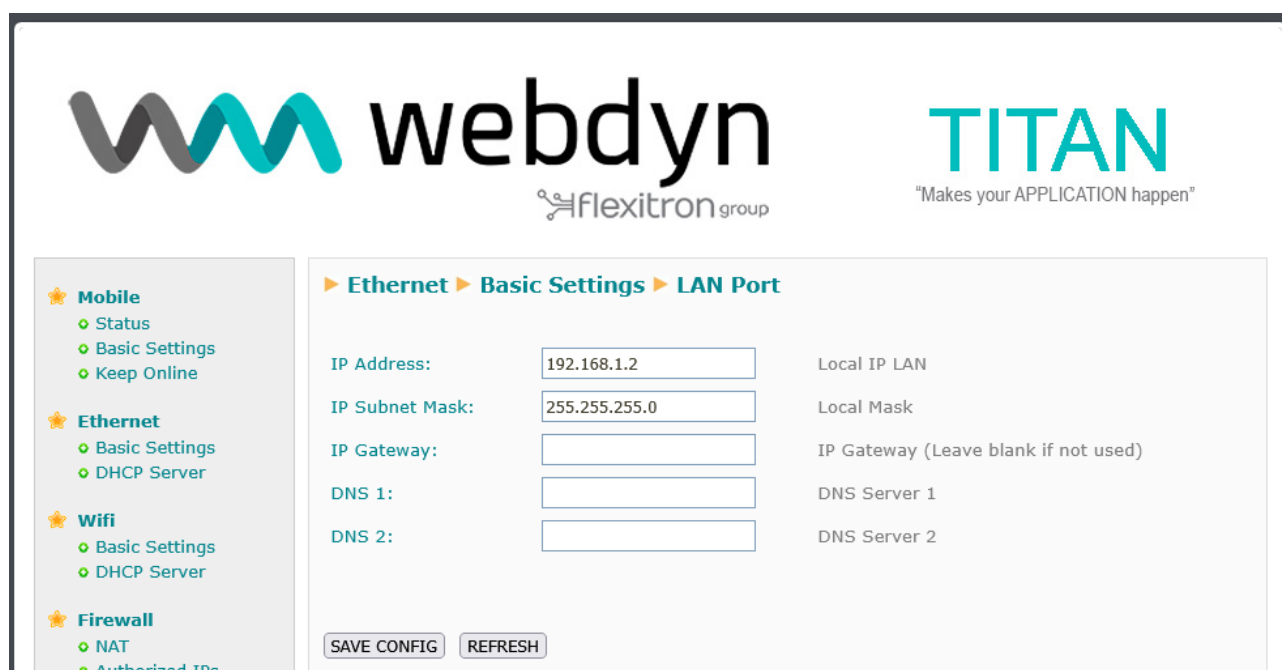
4.2- Ethernet

La sección de configuración “Ethernet” hace referencia a la parte de configuración de los puertos Ethernet del equipo basado en TITAN.

4.2.1- Ethernet → Basic Settings

Esta sección permite configurar los parámetros básicos de red de la conexión Ethernet. Este menú es ligeramente diferente en función de si el equipo basado en TITAN cuenta con uno o varios puertos Ethernet.

Equipos basados en TITAN con 1 puerto Ethernet:



The screenshot displays the webdyn TITAN configuration interface. At the top, the webdyn logo (a stylized 'w' with a blue and grey wave) and the TITAN logo (in blue) are visible, along with the Flexitron group logo. The interface is divided into a left sidebar and a main content area. The sidebar contains a menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), and Firewall (NAT, Authorized IPs). The main content area is titled 'Ethernet > Basic Settings > LAN Port'. It contains a form with the following fields: IP Address (192.168.1.2), IP Subnet Mask (255.255.255.0), IP Gateway (blank), DNS 1 (blank), and DNS 2 (blank). To the right of each input field is a label: 'Local IP LAN', 'Local Mask', 'IP Gateway (Leave blank if not used)', 'DNS Server 1', and 'DNS Server 2'. At the bottom of the form are two buttons: 'SAVE CONFIG' and 'REFRESH'.

- **IP Address:** dirección IP local estática de la interfaz Ethernet (por defecto 192.168.1.2)
- **IP Subnet Mask:** máscara de subred (por defecto 255.255.255.0)
- **IP Gateway:** dirección IP de Gateway de salida. Dejar en blanco si no a a utilizarse un gateway.
- **DNS1:** servidor de DNS principal
- **DNS2:** servidor de DNS secundario

Equipos basados en TITAN con varios puertos Ethernet:

The screenshot displays the webdyn TITAN configuration interface. At the top, the webdyn logo (a stylized 'w' with a blue wave) and the TITAN logo (in blue) are visible, along with the Flexitron group logo and the tagline "Makes your APPLICATION happen".

On the left, a sidebar menu lists various configuration categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), Serial Settings (Serial Port1-RS232, Serial Port2-RS232, Serial Port3-RS485, Serial Port4-TTL, SSL Certificates), and External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor, IEC103 Master).

The main content area is divided into two sections:

- Ethernet > Basic Settings > WAN Port:** This section contains fields for IP mode (static), IP Address (192.168.10.2), IP Subnet Mask (255.255.255.0), IP Gateway, DNS 1, DNS 2, and a checkbox for Remote webserver management. To the right of these fields are labels: "Static or dynamic IP (dhcp)", "Local IP LAN", "Local Mask", "IP WAN for Ethernet", "DNS Server 1", "DNS Server 2", and "Enable remote webserver management".
- Ethernet > Basic Settings > LAN Ports:** This section contains fields for IP Address (192.168.1.2) and IP Subnet Mask (255.255.255.0). To the right are labels: "Local IP LAN" and "Local Mask".

At the bottom of the LAN Ports section, there are two buttons: "SAVE CONFIG" and "REFRESH".

En los equipos con más de un puerto Ethernet siempre se dispondrá de 1 puerto WAN y el resto serán LAN.

Configuración WAN port:

- **IP Mode:** permite utilizar una configuración IP estática o dinámica (DHCP) para el puerto WAN.
- **IP Address:** dirección IP local estática de la interfaz Ethernet WAN (por defecto 192.168.1.2)
- **IP Subnet Mask:** máscara de subred de la interfaz Ethernet WAN (por defecto 255.255.255.0)
- **DNS1:** servidor de DNS principal
- **DNS2:** servidor de DNS secundario
- **IP Gateway:** dirección IP de Gateway de salida

Configuración LAN ports:

- **IP Address:** dirección IP local estática de la interfaz Ethernet LAN (por defecto 192.168.10.2)
- **IP Subnet Mask:** máscara de subred de la interfaz Ethernet LAN (por defecto 255.255.255.0)

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.2.2- Ethernet → DHCP Server

Esta sección permite habilitar y configurar el servidor DHCP asignado en la interfaz Ethernet del equipo basado en TITAN.

- **Enabled:** si activa la casilla se activará el servidor DHCP de la interfaz Ethernet.
- **Starting IP Address:** indica la primera dirección IP que asignará el servidor DHCP
- **Ending IP Address:** indica la última dirección IP que asignará el servidor DHCP
- **MAC Address / IP Address:** estos dos parámetros permiten que el servidor DHCP asigne siempre la misma IP a una determinada dirección MAC.

The screenshot shows the webdyn TITAN web interface for configuring the DHCP Server. The interface includes a sidebar menu with categories like Mobile, Ethernet, Wifi, Firewall, and Serial Settings. The main content area is titled 'Ethernet → DHCP Server' and contains the following configuration options:

- Enabled:** A checkbox to enable or disable the DHCP Server.
- Starting IP Address:** A text input field for the first IP address for DHCP (e.g., 192.168.1.100).
- Ending IP Address:** A text input field for the last IP address for DHCP (e.g., 192.168.1.110).
- SAVE CONFIG:** A button to save the DHCP server configuration.
- MAC Address / IP Address Table:** A table with two columns: 'MAC Address' and 'IP Address'. It contains two rows for configuring static IP assignments. Each row has input fields for the MAC Address and IP Address, and a 'SAVE RULE' button.

Important note: This IP must be **outside** the previous range of automatic assignment.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Pulse el botón “SAVE RULE” por cada pareja MAC / IP que quiera crear. Puede crear hasta 10.
- Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios

4.3 Wifi

La sección de configuración “Wifi” hace referencia a la parte de configuración de la interfaz Wifi. Mediante una configuración Wifi en modo “Access Point” puede, por ejemplo, dar acceso a Internet a dispositivos Wifi cliente o configurar el propio equipo basado en TITAN. Mediante una configuración en modo “Wifi Client” puede hacer que el equipo basado en TITAN utilice como salida a Internet a otro Access Point Wifi que exista en sus instalaciones.

4.3.1- Wifi → Basic Settings

Esta sección permite configurar los parámetros básicos de red de la interfaz Wifi.

- **Enabled:** Si activa la casilla se activa la interfaz Wifi del equipo basado en TITAN.
- **Wifi mode:** Permite seleccionar entre modo de trabajo “Wifi Access Point” o “Wifi Client”. Utilice el modo “Wifi Access Point” si quiere utilizar el equipo basado en TITAN para dar acceso a Internet a dispositivos Wifi utilizando la interfaz 4G/3G/2G. Utilice “Wifi Client” si quiere utilizar como salida a Internet una infraestructura Wifi existente (por ejemplo, el router fibra de una empresa).
- **Wifi SSID:** SSID público (en modo “Wifi Access Point” indica el SSID que creará el equipo basado en TITAN, en modo “Wifi Client” indica el SSID al que se conectará el equipo basado en TITAN).
- **Security:** permite especificar el modo de seguridad Wifi. Se recomienda WPA2
- **KEY:** especifica el password wifi, necesario para el modo WPA2.

ADVERTENCIA: siguiendo las recomendaciones de la “European Cybersecurity Certification Group”: **el password como mínimo 17 caracteres de los cuales se incluya al menos una mayúscula, una minúscula y un número.**

- **Channel:** selección del canal (1...11)
- **IP Mode:** en el modo “Wifi Client”, especifica si se utilizará como dirección IP Local Wifi una dirección IP estática o bien tiene que tomar la IP por DHCP.
- **IP Address:** dirección IP de la interfaz Wifi. Por defecto 192.168.2.1
- **IP Subnet Mask:** mascara de subred de la interfaz Wifi
- **DNS1:** servidor de DNS principal
- **DNS2:** servidor de DNS secundario
- **IP Gateway:** En el modo “Wifi Client” permite especificar el gateway cuando la IP local es estática.
- **Internet Access:** activar para poder acceder a Internet desde un dispositivo Wifi
- **LAN Access:** activar para poder acceder a dispositivos conectados al puerto Ethernet del equipo desde un dispositivo Wifi.

★ **Mobile**

- ◆ Status
- ◆ Basic Settings
- ◆ Keep Online

★ **Ethernet**

- ◆ Basic Settings
- ◆ DHCP Server

★ **Wifi**

- ◆ Basic Settings
- ◆ DHCP Server

★ **Firewall**

- ◆ NAT
- ◆ Authorized IPs
- ◆ MAC Filter
- ◆ Routes

★ **Serial Settings**

- ◆ Serial Port1-RS232
- ◆ Serial Port2-RS485
- ◆ SSL Certificates

★ **External Devices**

- ◆ Logger configuration
- ◆ ModBus Devices
- ◆ Generic Serial Device
- ◆ Temperature Sensor
- ◆ IEC102 Meter
- ◆ GPS Receiver

★ **VPN**

► **Wifi ► Basic Settings**

Enabled:	Disabled	Enable Wifi
Wifi mode:	Wifi Access Point	Select between Wifi Access Point or Wifi Client
Wifi SSID:		Select the public name for the Wifi Network
Security:	OPEN	Select security mode
KEY:		Password for WPA2-Personal security mode (Min. 17 characters. Must include uppercase, lowercase, and numbers)
Channel:	1	Wifi Channel
IP Address:	192.168.2.1	Local IP LAN
IP Subnet Mask:	255.255.255.0	Local Mask
DNS 1:	8.8.8.8	DNS Server 1
DNS 2:	8.8.4.4	DNS Server 2
IP Gateway:		Left blank if not used or using another WAN interface
Internet access:	☐	Check if wifi devices can access to Internet
LAN access:	☐	Check if wifi devices can connect with LAN devices

SAVE CONFIG

En la parte final de esta sección, puede encontrar la opción de añadir una "White List" para solamente autorizar conexiones a las MACs autorizadas. Asi mismo, a continuación podrá encontrar una tabla con los clientes WiFi conectados:

- ZeroTier
- Device Manager
 - KARE
- Other
 - AT Command
 - DynDns
 - Private DynDns
 - Sms control
 - Periodic Autoreset
 - Time Servers
 - Remote Console
 - Snmp
 - Tacacs+
 - Ldap
 - Mqtt / Mqtts
 - Http / Https
 - User Permissions
 - Passwords Web UI
 - CA Certificates
 - Email Config
 - ModBus Slave
 - Titan Scripts
 - Connectivity tools
 - Digital I/O
 - Custom Skin
 - Led Config

Wifi Basic Settings White List

MAC List:

If MACs are listed here, only these MACs will be authorized to connect.

Example:
7C:2A:DB:87:28:D1
AA:03:B1:04:67:21

SAVE CONFIG

Wifi Basic Settings Connected Wifi Clients

MAC	IP
-----	----

REFRESH LIST

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.3.2- Wifi → DHCP Server

Desde esta sección se puede habilitar y configurar el servidor DHCP asignado en la interfaz Wifi del equipo basado en TITAN.

- **Enabled:** si activa la casilla se activará el servidor DHCP de la interfaz Wifi.
- **Starting IP Address:** indica la primera dirección IP que asignará el servidor DHCP
- **Ending IP Address:** indica la última dirección IP que asignará el servidor DHCP
- **MAC Address / IP Address:** estos dos parámetros permiten que el servidor DHCP asigne siempre la misma IP a una determinada dirección MAC.

The screenshot shows the webdyn TITAN web interface. The top header features the 'webdyn' logo with the 'flexitron group' tagline and the 'TITAN' logo with the tagline 'Makes your APPLICATION happen'. A left sidebar contains a menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), and Serial Settings (Serial Port1-RS232). The main content area is titled 'Wifi > DHCP Server'. It includes a 'Enabled' checkbox, 'Starting IP Address' and 'Ending IP Address' input fields, and a 'SAVE CONFIG' button. Below this is a table with two columns: 'MAC Address' and 'IP Address'. The table has two rows for configuration. The first row has a 'MAC Address' input field and a description 'Set a MAC address (ex 54:42:49:0A:E9:2C)'. The second row has an 'IP Address' input field and a description 'Set assigned IP address (ex 192.168.2.120)'. An 'Important note' states: 'This IP must be outside the previous range of automatic assignment'. A 'SAVE RULE' button is at the bottom of the table.

MAC Address	IP Address

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Pulse el botón "SAVE RULE" por cada pareja MAC / IP que quiera crear. Puede crear hasta 10. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios

4.4- Firewall

Sección para configurar los aspectos de seguridad del equipo.

4.4.1- Firewall → NAT

Sección desde donde se puede mapear puertos para el acceso externo a dispositivos internos conectados al equipo. Por ejemplo, si dispone de una cámara IP conectada al puerto Ethernet del equipo basado en TITAN y se desea tener acceso a ésta desde un ordenador remoto debe configurarse apropiadamente esta sección. Puede crear hasta un total de 10 reglas.

- **Service name:** nombre descriptivo de una regla de mapeado
- **Protocol:** indica el protocolo del mapeado de puertos. TCP, UDP o ambos.
- **Port:** indica el puerto de entrada al equipo basado en TITAN por la interfaz WAN
- **Output port:** indica el puerto de redirección hacia el dispositivo interno conectado al equipo basado en TITAN.
- **Server IP Address:** dirección IP del dispositivo a controlar externamente (por ejemplo, la dirección IP de una cámara).
- **Interface:** interfaz de red a la que aplicar NAT:
 - Mobile – 4G/3G/2G (ppp0)
 - ZeroTier1 (zt0)
 - ZeroTier2 (zt1)
 - ZeroTier3 (zt2)

The screenshot shows the webdyn TITAN user interface. The top header features the webdyn logo and the TITAN logo with the tagline "Makes your APPLICATION happen". On the left is a sidebar menu with categories: Mobile, Ethernet, Wifi, Firewall, and Serial Settings. The 'Firewall' category is expanded, showing 'NAT' as the selected option. The main content area is titled 'Firewall > NAT' and contains a table with columns: Service name, Protocol, In. Port, Out. Port, Destination IP, and Interface. Below the table is a form for creating a new NAT rule. The form fields are: Service name (text input), Protocol (dropdown menu set to TCP+UDP), Port (text input), Output Port (text input), Server IP Address (text input), and Interface (dropdown menu set to Mobile - 4G/3G/2G (ppp0)). Each field has a descriptive tooltip. At the bottom left of the form is a 'SAVE SERVICE' button.

Service name	Protocol	In. Port	Out. Port	Destination IP	Interface
Service name:	Protocol:	Port:	Output Port:	Server IP Address:	Interface:

Service name: Insert a name for the service

Protocol: Select TCP/UDP protocol

Port: Input port (0 ... 65535) - Router

Output Port: Output port (0 ... 65535) - Destination server

Server IP Address: Set the IP of the destination server

Interface: Network interface.
Normally: WAN - 4G/3G/2G (ppp0)

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Recuerde también que para realizar un NAT correctamente:
 - 1.- La dirección IP de LAN del dispositivo a controlar debe estar dentro del rango de red de la dirección IP de LAN del equipo basado en TITAN.
 - 2.- La dirección IP de Gateway del dispositivo a controlar debe ser la dirección IP de LAN del equipo basado en TITAN. Consulte los ejemplos del Anexo para más información.
- Es posible especificar la interfaz para NAT. Si desconoce la utilidad utilice la opción “auto”. El uso de esta opción, por ejemplo, puede resultar útil para OpenVPN, si quiere acceder a los dispositivos que cuelgan del puerto Ethernet vía NAT (y así disponer de la misma configuración para acceder remotamente a distintos puntos).

4.4.2 - Firewall → Authorized IPs

Esta pantalla le permite definir hasta 3 direcciones IP autorizadas para aceptar conexiones en la interfaz WAN para los diferentes servicios del equipo. Por ejemplo, si especifica una dirección IP autorizada 90.166.108.200 (por ejemplo, la dirección IP de su oficina), únicamente se podrá acceder a ciertos servicios del equipo basado en TITAN desde dicha dirección IP.

- **Authorized IP1:** Dirección IP autorizada número 1
- **Authorized IP2:** Dirección IP autorizada número 2
- **Authorized IP3:** Dirección IP autorizada número 3
- **Router configuration:** Especifica si se aceptan conexiones remotas al entorno de configuración web del equipo desde cualquier dirección IP o únicamente desde direcciones IP autorizadas.
- **Serial Gateways:** Especifica si se aceptan conexiones remotas a los servicios de pasarelas 4G/3G/2G-RS232/485 desde cualquier IP o únicamente desde direcciones IP autorizadas.
- **Remote console:** Especifica si se aceptan conexiones remotas al servicio de consola remota (telnet o SSH) desde cualquier IP o únicamente desde direcciones IP autorizadas.
- **NAT:** Especifica si se aceptan conexiones remotas a los puertos mapeados del equipo desde cualquier IP o únicamente desde direcciones IP autorizadas.
- **ModBus TCP Slave:** Especifica si se aceptan conexiones remotas al servicio Modbus TCP Slave del equipo basado en TITAN desde cualquier IP o únicamente desde direcciones IP autorizadas.
- **SNMP:** Especifica si se aceptan conexiones remotas al servicio SNMP del equipo basado en TITAN desde cualquier IP o únicamente desde direcciones IP autorizadas.
- **OpenVPN:** Especifica si se aceptan conexiones remotas al servicio "OpenVPN Server" del equipo basado en TITAN desde cualquier IP o únicamente desde direcciones IP autorizadas.
- **MQTT:** Especifica si se aceptan conexiones remotas al servicio MQTT del equipo basado en TITAN desde cualquier IP o únicamente desde direcciones IP autorizadas.
- **NTP Server:** Especifica si se aceptan conexiones remotas al servicio "NTP Server" del equipo basado en TITAN desde cualquier IP o únicamente desde direcciones IP autorizadas.
- **TCP & UDP exceptions:** Especifica si se aceptan conexiones remotas a las excepciones de los puertos TCP y UDP del equipo basado en TITAN desde cualquier IP o únicamente desde direcciones IP autorizadas.
- **Outgoing Connections:** Permite especificar si desde el equipo basado en TITAN es posible dar acceso a Internet hacia todas las direcciones IP o bien sólo hacia las direcciones IPs autorizadas. Por ejemplo, imagine que sólo quiere que los dispositivos Ethernet o Wifi conectados al TITAN puedan enviar datos a su servidor, impidiendo que el equipo pueda ser usado indebidamente para otro tipo de acciones (navegación por Internet, etc ...)
- **PING:** Únicamente responderá a peticiones PING realizadas desde las IPs autorizadas

★ Mobile

- ◆ Status
- ◆ Basic Settings
- ◆ Keep Online

★ Ethernet

- ◆ Basic Settings
- ◆ DHCP Server

★ Wifi

- ◆ Basic Settings
- ◆ DHCP Server

★ Firewall

- ◆ NAT
- ◆ Authorized IPs
- ◆ MAC Filter
- ◆ Routes

★ Serial Settings

- ◆ Serial Port1-RS232
- ◆ Serial Port2-RS485
- ◆ SSL Certificates

★ External Devices

- ◆ Logger configuration
- ◆ ModBus Devices
- ◆ Generic Serial Device
- ◆ Temperature Sensor
- ◆ IEC102 Meter
- ◆ GPS Receiver

★ VPN

- ◆ IPSec

► Firewall ► Authorized IPs (for WAN interfaces)

Authorized IP1:		Remote connections from this IP are allowed
Authorized IP2:		Remote connections from this IP are allowed
Authorized IP3:		Remote connections from this IP are allowed
Router configuration:	ALLOW ANY IP	Security for remote configuration connection
Serial gateways:	ALLOW ANY IP	Security for remote serial connection
Remote console:	ALLOW ANY IP	Security for remote console connection
NAT:	ALLOW ANY IP	Security for NAT connections
ModBus TCP Slave:	ALLOW ANY IP	Security for ModBus TCP Slave connections
SNMP:	ALLOW ANY IP	Security for SNMP
OpenVPN:	ALLOW ANY IP	Security for OpenVPN (Mode server)
MQTT:	ALLOW ANY IP	Security for MQTT Broker
NTP Server:	ALLOW ANY IP	Security for NTP Server
TCP & UDP exceptions:	ALLOW ANY IP	Security for TCP & UDP port exceptions
Outgoing connections:	ALLOW ANY IP	Security for outgoing connections
PING:	ALLOW ANY IP	Security for incoming PING from WAN

SAVE CONFIG

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Las restricciones de IP son únicamente a nivel de conectividad WAN. El acceso wifi queda protegido por la propia clave de red WPA2. Es decir, si dispone Wifi y necesita seguridad, active WPA2 en la sección Wifi > Basic Settings
- Si utiliza restricciones "Outgoing connections" recuerde que necesita especificar la dirección IP del servidor DNS a utilizar en caso de que use nombres de dominio en lugar de direcciones IP.
- Si necesita más de 3 direcciones IPs autorizadas, puede especificar más de una dirección IP en cualquier casilla, separando éstas por ",".

4.4.3 - Firewall → MAC Filter

Desde esta sección es posible configurar al dispositivo para filtrar las comunicaciones a través de la interfaz Ethernet (o Wifi) en función de las direcciones MAC.

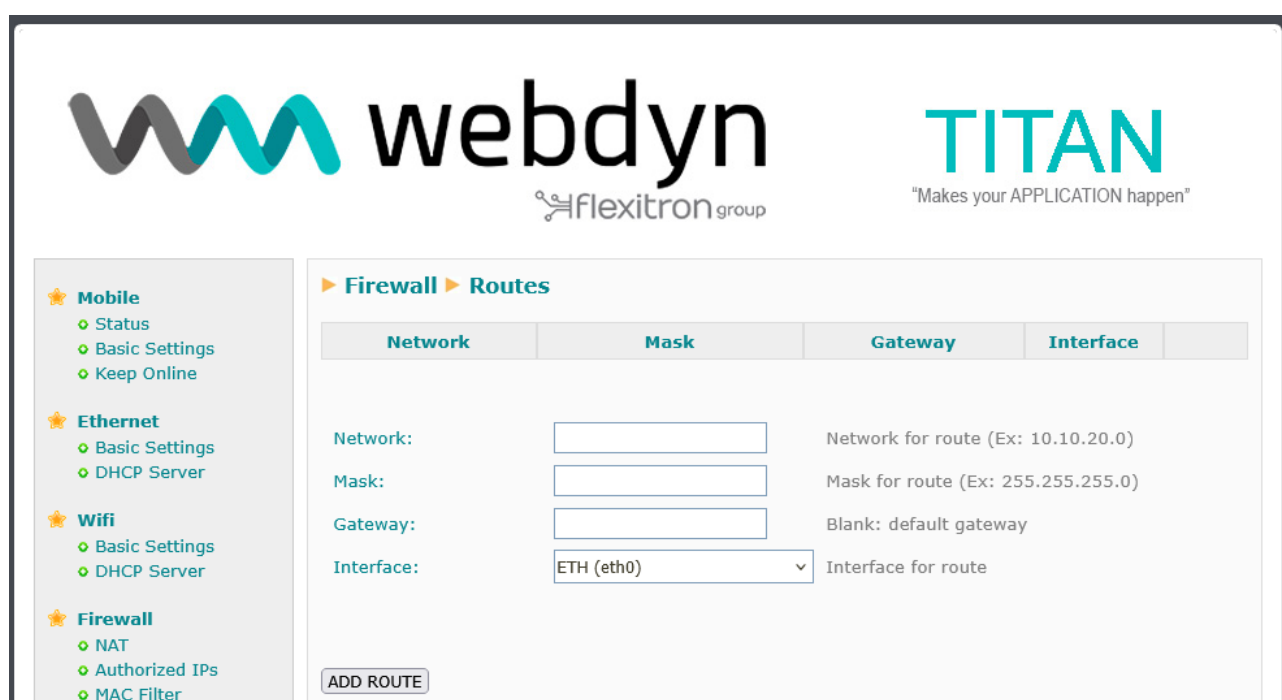
- **Mode** – All MAC allowed except listed: Todas las direcciones MAC son permitidas excepto las direcciones MAC indicadas en la lista, las cuales serán bloqueadas. Esta es la configuración por defecto.
- **Mode** – Only listed MAC allowed: Todas las direcciones MAC están bloqueadas excepto las direcciones MAC indicadas en la lista, las cuales serán permitidas.
- **MAC List**: Lista de direcciones permitidas o bloqueadas, en función del modo de operación.

The screenshot shows the webdyn TITAN configuration interface. The top header features the webdyn logo (a stylized 'w' with a blue and grey wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". A left sidebar contains a menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), and Firewall (NAT, Authorized IPs, MAC Filter, Routes). The main content area is titled "Firewall > MAC Filter". It includes a "Mode:" dropdown menu set to "All MAC allowed except listed" with the label "MAC Filter mode". Below this is a "MAC list:" text area with a blue border and a diagonal line in the bottom right corner. To the right of the text area, an "Example:" shows two MAC addresses: "01:02:03:04:05:06" and "07:08:09:00:0a:0b", followed by the text "(File: 'macs.mtx')". At the bottom left of the main area is a "SAVE CONFIG" button.

4.4.4 - Firewall → Routes

Desde esta sección es posible configurar al dispositivo para añadir hasta 5 rutas de direccionamiento por interfaz.

- **Network** – Indica la red para la ruta a configurar.
- **Mask** – Indica la máscara de red para la ruta a configurar.
- **Gateway** – Dirección IP del gateway a utilizar para la ruta a configurar.
- **Interface** – Interface física de la ruta a configurar.



The screenshot shows the webdyn TITAN configuration interface. The top header includes the webdyn logo (a stylized 'w' with a blue and grey wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". The left sidebar contains a menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), and Firewall (NAT, Authorized IPs, MAC Filter). The main content area is titled "Firewall > Routes" and features a table with four columns: Network, Mask, Gateway, and Interface. Below the table, there are input fields for each column: Network (text input), Mask (text input), Gateway (text input), and Interface (dropdown menu showing "ETH (eth0)"). To the right of each input field is a descriptive text: "Network for route (Ex: 10.10.20.0)", "Mask for route (Ex: 255.255.255.0)", "Blank: default gateway", and "Interface for route". At the bottom left of the main area is a button labeled "ADD ROUTE".

Network	Mask	Gateway	Interface
Network:	Mask:	Gateway:	Interface:
			ETH (eth0)
Network for route (Ex: 10.10.20.0)	Mask for route (Ex: 255.255.255.0)	Blank: default gateway	Interface for route

ADD ROUTE

4.5- Serial Settings → Serial portX

Desde la sección Serial Settings es posible establecer la configuración de cada puerto serie del equipo basado en TITAN (velocidad, paridad, ...) así como la función especial que tendrá cada uno de ellos (pasarelas IP-serie, pasarelas Modbus TCP-RTU, ...)

4.5.1- Serial Settings >> Serial portX

Los equipos basados en TITAN cuentan con varios puertos serie. Con ellos pueden realizar pasarelas 4G/3G/2G-Serie y CSD-Serie para controlar remotamente dispositivos RS232 o RS485. El número de puertos serie de tipo RS232 o RS485 dependerá del modelo de equipo basado en TITAN utilizado.

- **Baudrate:** especifica la velocidad del puerto serie (115200, ... , 300)
- **Data bits:** especifica el número de bits de datos (7, 8)
- **Parity:** especifica la paridad (none, even [par], odd [impar])
- **Stop bits:** número de bits de stop (1, 2)
- **Flow Control:** especifica el control de flujo (none, hardware)
- **Timeout ms:** indica los milisegundos de espera sin recibir datos por el puerto serie, antes de enviar los datos por IP. Si especifica un "0" (valor por defecto), los datos se van enviando vía IP según van llegando por el puerto serie. Un número por ejemplo de 10, especifica que no se envíen datos si no hay un periodo de mínimo 10ms sin recibir datos por el puerto serie. Esto permite que los datos lleguen al destino menos fragmentados.
- **Allow local embedded AT Commands:** seleccionando esta casilla se permite el envío de comandos AT LOCALES embebidos en una pasarela 4G/3G/2G-Serie de tipo Server o Client. Los comandos AT deben enviarse a través del puerto serie RS232 o RS485 del equipo basado en TITAN pero encapsulados entre los tags <MTXTUNNEL> y </MTXTUNNEL>. Por ejemplo, si se desea obtener la cobertura puede enviarse el comando <MTXTUNNEL>AT+CSQ</MTXTUNNEL>. O si se desea resetear un equipo remotamente, puede enviarse el comando <MTXTUNNEL>AT^MTXTUNNEL=REBOOT </MTXTUNNEL>
- **Allow remote embedded AT Commands:** seleccionando esta casilla se permite el envío de comandos AT REMOTOS embebidos en una pasarela 4G/3G/2G-Serie de tipo Server o Client. Los comandos AT deben enviarse a través de la conexión de la pasarela establecida pero encapsulados entre los tags <MTXTUNNELR> y </MTXTUNNELR>. Por ejemplo, si se desea obtener la cobertura puede enviarse el comando <MTXTUNNELR>AT+CSQ</MTXTUNNELR>. O si se desea resetear un equipo remotamente, puede enviarse el comando <MTXTUNNELR>AT^MTXTUNNEL=REBOOT </MTXTUNNELR>
- **Allow incoming GSM call (CSD Data Call):** seleccionando esta casilla indica que se acepta una llamada de tipo CSD por el puerto serie. Únicamente válido para trabajar cuando el puerto está configurado como una pasarela de tipo TCP Server o TCP Client y para algunos casos (como la lectura de contadores IEC-102) cuando está configurado como "Nothing or Used by External Devices". Cuando se recibe una llamada CSD y es aceptada, las conexiones IP se suspenden hasta que la llamada CSD finaliza.

- **Function: Nothing or Used by External Device:** seleccione esta opción de funcionamiento si no desea utilizar un determinado puerto serie como pasarela IP /serie o bien si desea que el puerto serie (RS232 o RS485) sea usado por un dispositivo externo especificado en la sección de configuración “External Devices”. Por ejemplo, si desea usar un sensor de temperatura o cualquier otro dispositivo especificado en el menú “External Devices” debe seleccionar esta opción.
- **Function: Serial – IP Gateway (TCP Server):** seleccione esta opción de funcionamiento si desea establecer una pasarela Serie – 4G/3G/2G transparente en modo TCP Server, es decir, un escenario donde el equipo basado en TITAN está a la escucha en un determinado puerto TCP a la espera de recibir una conexión para establecer la pasarela.
 - **TCP Local Port:** puerto TCP de escucha para la pasarela Serie – 4G/3G/2G
 - **Timeout:** tiempo (segundos) sin datos en la pasarela para cerrar el socket automáticamente.
 - **TCP Local Priority Port:** puerto TCP prioritario de escucha para para la pasarela Serie – 4G/3G/2G. Si hay una conexión activa en este puerto no se admitirán conexiones en el puerto TCP Local Port. Útil para lectura de contadores eléctricos con prioridad de conexión IP.
 - **Close IEC102 session:** seleccione esta opción sólo si está utilizando la pasarela IP-Serie para la lectura de contadores con protocolo IEC-60870-5-102. Al activar esta opción el router Titan analiza los paquetes circulantes del protocolo IEC-60870-5-102, obteniendo la dirección de enlace y punto de medida del contador. Esta información es usada cada vez que se inicia una pasarela IP-Serie contra el contador con el fin de cerrar la sesión con el contador que pudiera haber abierta.
 - **Temporal client RS232:** Seleccione esta opción si quiere activar un socket temporal cuando está trabajando en modo TCP Server pero no establecida la pasarela IP/Serie y recibe datos por el puerto serie. Si activa esta opción es necesario tener bien configurados los parámetros “Remote IP”, “Remote TCP Port”, “ID String” de la sección TCP Client que se expone a continuación.
 - **Temporal client Wakeup:** Esta opción permite activar un socket temporal cuando está trabajando en modo TCP Server pero no establecida la pasarela IP/Serie y llega la hora configurada. Si activa esta opción es necesario tener bien configurados los parámetros “Remote IP”, “Remote TCP Port”, “ID String” de la sección TCP Client que se expone a continuación.
 - **Temporal client Time:** indica el tiempo en que un socket temporal está activo.
 - **Temporal client Random:** es posible establecer un tiempo aleatorio en segundos para un cliente temporal que se añade a la hora de Wakeup. Esto sólo es útil si tiene un gran número de equipos conectándose a una misma hora, y quiere introducir un tiempo aleatorio para distribuir el número de conexiones simultáneas contra un servidor.
 - **SSL/TLS enabled:** si se necesitan securizar las pasarelas TCP Server es posible hacerlo mediante esta opción. Si se activa debe configurarse también la sección de certificados “Serial Settings → SSL Certs”
- **Function: Serial – IP Gateway (TCP Client):** seleccione esta opción de funcionamiento si desea establecer una pasarela Serie – 4G/3G/2G transparente en modo TCP Client, es decir, un escenario donde el equipo basado en TITAN se conecta a una determinada IP / puerto TCP para establecer la pasarela serie – 4G/3G/2G
 - **Remote IP:** dirección IP a la que se conectará el equipo basado en TITAN

- **Remote TCP Port:** puerto TCP al que se conectará el equipo basado en TITAN
 - **Reconnection time:** en caso de caída de una conexión o problemas con éstas, indica cuántos milisegundos deben dejarse entre intento e intento de conexión. 0 = reconexión inmediata. Tenga cuidado con este valor si no cuenta con una tarjeta SIM con tarifa plana o dispone de un volumen de datos mensual contratado muy ajustado.
 - **ID String:** cadena que se envía justo tras establecerse el socket con la IP remota. Este texto le permitirá identificar el dispositivo que realiza la conexión. Por ejemplo, si dispone de 100 equipos basados en TITAN en este modo de funcionamiento, le permite distinguir tras una conexión cual de esos 100 dispositivos ha realizado la conexión. Es posible añadir los tags especiales [IMEI] , [CR] y [LF] que serán substituidos por el IMEI, y los caracteres 0x13 y 0x10 respectivamente.
 - **SSL/TLS enabled:** si se necesitan securizar las pasarelas TCP Client es posible hacerlo mediante esta opción. Si se activa debe configurarse también la sección de certificados “Other>CA-Root Certificates” y “Serial Settings>SSL/TLS Certificates (TCP CLIENT)”
- **Function: Serial – IP Gateway (Modbus TCP / Modbus RTU):** seleccione esta opción de funcionamiento si desea establecer una pasarela Serie – 4G/3G/2G con conversión de protocolos Modbus TCP – Modbus RTU. No use esta opción si su software de control utiliza Modbus RTU, pues bastaría con utilizar una pasarela TCP Server normal. Use esta opción si su software de control usa protocolo Modbus TCP. Si tiene dudas consulte en contact@webdyn.com
- **TCP Local Port:** puerto TCP de escucha.
 - **Timeout:** tiempo, en segundos, sin intercambio de datos en la pasarela Modbus para cerrar el socket automáticamente. Si se especifica “0”, la opción queda desactivada.
 - **Priority over scripts:** si se activa esta opción, una conexión Modbus TCP/RTU establecida por la pasarela tendrá prioridad sobre las lecturas Modbus realizadas desde TITAN Scripts y sobre las lecturas autónomas Modbus del equipo. Mientras la pasarela esté activa, dichas lecturas quedarán pausadas y se reanudarán automáticamente al finalizar la conexión.
 - **SSL/TLS enabled:** si se quiere hacer segura la pasarela (necesarios configurar “Serial Settings>SSL/TLS Certificates (TCP CLIENT)”)
- **Function: Serial – IP Gateway (MQTT):** seleccione esta opción si desea establecer una pasarela IP-Serie a través de protocolo MQTT. Para poder utilizar esta opción es necesario configurar el cliente MQTT que encontrará en el apartado “Other - MQTT”
- **TX Mqtt Topic:** El equipo basado en TITAN reenviará al topic MQTT definido en este parámetro todos los datos recibidos en el puerto serie (datos enviados en modo RAW).
 - **TX Mqtt Broker:** permite seleccionar el bróker MQTT al que se enviarán los datos recibidos por el puerto serie. Puede seleccionarse Primary, Secondary o Both.
 - **RX Mqtt Topic:** El equipo basado en TITAN se suscribirá al topic MQTT definido en este parámetro y reenviará por su puerto serie todos los datos recibidos en dicho topic (datos enviados en modo RAW)
 - **RX Mqtt Broker:** permite seleccionar el bróker MQTT desde el que se recibirán los datos que serán reenviados por el puerto serie. Puede seleccionarse Primary, Secondary o Both. Si se selecciona Both, tenga presente que podrían recibirse datos duplicados si ambos brókers publican en el mismo topic.

- **Function: Serial – IP Gateway (UDP):** seleccione esta opción de funcionamiento si desea establecer una pasarela IP – Serie transparente mediante protocolo UDP
 - **Remote IP:** dirección IP del servidor remoto donde se enviarán los datos vía UDP
 - **Remote UDP Port:** puerto UDP del servidor remoto
 - **Local UDP Port:** puerto UDP de escucha del equipo

- ★ **Mobile**
 - ◊ Status
 - ◊ Basic Settings
 - ◊ Keep Online
- ★ **Ethernet**
 - ◊ Basic Settings
 - ◊ DHCP Server
- ★ **Wifi**
 - ◊ Basic Settings
 - ◊ DHCP Server
- ★ **Firewall**
 - ◊ NAT
 - ◊ Authorized IPs
 - ◊ MAC Filter
 - ◊ Routes
- ★ **Serial Settings**
 - ◊ Serial Port1-RS232
 - ◊ Serial Port2-RS485
 - ◊ SSL Certificates
- ★ **External Devices**
 - ◊ Logger configuration
 - ◊ ModBus Devices
 - ◊ Generic Serial Device
 - ◊ Temperature Sensor
 - ◊ IEC102 Meter
 - ◊ GPS Receiver
- ★ **VPN**
 - ◊ IPsec
 - ◊ OpenVPN Client
 - ◊ OpenVPN Server
 - ◊ ZeroTier
- ★ **Device Manager**
 - ◊ KARE
- ★ **Other**
 - ◊ AT Command
 - ◊ DynDns
 - ◊ Private DynDns
 - ◊ Sms control
 - ◊ Periodic Autoreset
 - ◊ Time Servers
 - ◊ Remote Console
 - ◊ Snmp
 - ◊ Tacacs+
 - ◊ Ldap
 - ◊ Mqtt / Mqtts
 - ◊ Http / Https
 - ◊ User Permissions
 - ◊ Passwords Web UI
 - ◊ CA Certificates
 - ◊ Email Config
 - ◊ ModBus Slave
 - ◊ **Titan Scripts**
 - ◊ Connectivity tools
 - ◊ Digital I/O
 - ◊ Custom Skin
 - ◊ Led Config
 - ◊ Syslog
 - ◊ Backup / Factory
 - ◊ Firmware Upgrade
 - ◊ Reboot
 - ◊ Logout

Serial Gateway ▶ Com1 Settings

Baudrate:	115200	Baudrate of serial port
Data bits:	8	Number of data bit
Parity:	none	Parity
Stop bits:	1	Number of stop bits
Flow Control:	none	Flow control of serial port
Timeout ms:	50	msec without serial data before sending (default: 50)

☐ **Allow local embedded AT commands**
☐ **Allow remote embedded AT commands**
☐ **Allow incoming GSM call (CSD Data Call)**

Ex.: <MTXTUNNEL>AT</MTXTUNNEL>

Ex.: <MTXTUNNELR>AT</MTXTUNNELR>

Only **TCP Server** and **TCP Client** functions or **Nothing**. 2G (CSD) network required.

☒ **Function: Nothing or used by External Device or Script**

☐ **Function: Serial - IP Gateway (TCP Server)**

TCP Local Port:

Timeout:

TCP Local Priority Port:

Close IEC102 session ☐

Temporal client RS232 ☐

Temporal client Wakeup

Temporal client time:

Temporal client Random

SSL/TLS enabled ☐

Listening TCP Port (1 ... 65535)

Seconds without data for closing. (0...7200)
0=not used.

Listening TCP Local Priority Port (0 ... 65535).
0=not used.

Close IEC 60870-5-102 meter session

Check if you need a temporal TCP Client when data is present at serial port.
DDHHMM. Example: XX2200 starts a temporal client every day at 22:00

Seconds for temporal client

Seconds. Random time for temporal client Wakeup

SSL/TLS Enabled (**SSL Certs** needed)

☐ **Function: Serial - IP Gateway (TCP Client)**

Remote IP:

Remote TCP Port:

Reconnection time:

ID String:

SSL/TLS enabled ☐

Address of remote IP server

Port number of remote server (1 ... 65535)

Milliseconds between connection attempts

This identification String is sent in each connection (can be used for device identification)

SSL/TLS Enabled (**CA Certs** needed)
(**SSL Certs** needed if client authentication)

☐ **Function: Serial - IP Gateway (ModBus TCP / ModBus RTU)**

TCP Local Port:

Timeout:

Priority over scripts ☐

SSL/TLS enabled ☐

Listening TCP Port (1 ... 65535). Normally 502

Seconds without data for closing. (0...7200)
0=not used.

Pause Titan Scripts and autonomous Modbus reads while this gateway is connected.

SSL/TLS Enabled (**SSL Certs** needed)

☐ **Function: Serial - IP Gateway (MQTT)**

TX Mqtt Topic:

TX Mqtt Broker:

RX Mqtt Topic:

RX Mqtt Broker:

All data received by serial will be retransmitted to this MQTT topic

Broker used for serial to MQTT data

All data received by IP in this MQTT topic will be retransmitted by the serial port.

Broker used for MQTT to serial data. Both can deliver duplicates

☐ **Function: Serial - IP Gateway (UDP)**

Remote IP:

Remote UDP Port:

Local UDP Port:

Address of remote IP server (can be included several IP between ';')

Remote UDP port (1 ... 65535)

Local UDP port (1 ... 65535)

☐ **Function: Direct (Internal modem)**

Allow mtxtunnel comands ☐

This option allows send AT commands to internal modem from external application under your responsibility.

Allow execution of mtxtunnel commands. Only recommended in physical secure environments.

SAVE CONFIG

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- De aparecer un puerto serie de tipo TTL hace referencia a un puerto serie interno del equipo basado en TITAN para tarjetas especiales de comunicaciones (RF868 MHz, GPS, ...), es decir, no es un puerto serie externo del equipo.
- Por motivos de seguridad, siempre que sea posible, se recomienda la activación de la opción SSL/TLS. Las comunicaciones sin activación de SSL/TLS no son seguras. Alternativamente, otra opción es utilizar las pasarelas IP-Serie a través de VPN.

4.5.2.- Serial Settings → SSL Certificates

Las pasarelas IP-Serie del equipo basado en TITAN pueden establecerse utilizando conexiones SSL/TLS, tanto en conexiones TCP cliente como en conexiones TCP servidor. En caso de utilizar conexiones SSL/TLS es necesario configurar la sección de certificados correspondiente.

La sección **Serial Gateway → SSL/TLS Certificates (TCP SERVERS)** hace referencia a los certificados cuando el puerto COM se ha configurado como un socket TCP Server

The screenshot shows the webdyn TITAN web interface. The top header includes the webdyn logo (a stylized 'w' with a blue and green wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". Below the header is a left sidebar with a navigation menu. The main content area is titled "Serial Gateway ▶ SSL/TLS Certificates (TCP SERVERS)".

The sidebar menu includes:

- ★ Mobile
 - ◇ Status
 - ◇ Basic Settings
 - ◇ Keep Online
- ★ Ethernet
 - ◇ Basic Settings
 - ◇ DHCP Server
- ★ Wifi
 - ◇ Basic Settings
 - ◇ DHCP Server
- ★ Firewall
 - ◇ NAT
 - ◇ Authorized IPs
 - ◇ MAC Filter
 - ◇ Routes
- ★ Serial Settings
 - ◇ Serial Port1-RS232
 - ◇ Serial Port2-RS485
 - ◇ SSL Certificates
- ★ External Devices
 - ◇ Logger configuration
 - ◇ ModBus Devices
 - ◇ Generic Serial Device
 - ◇ Temperature Sensor
 - ◇ IEC102 Meter
 - ◇ GPS Receiver

The main content area is titled "Serial Gateway ▶ SSL/TLS Certificates (TCP SERVERS)". It contains the following sections:

Certificate for SSL/TLS Servers (PEM format)

Field	File Name	Examinar...	Upload	Status
Server certificate:	file 'serial-server.crt'	No se ha seleccio...o ningún archivo.	Upload	not uploaded
Server KEY:	file 'serial-server.key'	No se ha seleccio...o ningún archivo.	Upload	not uploaded

Below the table is a button: **DELETE CERTIFICATE**

Certificates for authorized SSL/TLS clients (if needed) (PEM format)

Field	File Name	Examinar...	Upload	Status
Client certificate 1:	file 'serial-client1.crt'	No se ha seleccio...o ningún archivo.	Upload	not uploaded
Client certificate 2:	file 'serial-client2.crt'	No se ha seleccio...o ningún archivo.	Upload	not uploaded
Client certificate 3:	file 'serial-client3.crt'	No se ha seleccio...o ningún archivo.	Upload	not uploaded

Below the table are three buttons: **DELETE CERTIFICATE 1**, **DELETE CERTIFICATE 2**, and **DELETE CERTIFICATE 3**.

Client authentication: ☒ Check for client authentication

At the bottom is a button: **SAVE CONFIG**

- **Server Certificate:** Certificado (formato PEM) para ser usado por el equipo basado en TITAN cuando para cualquier servicio configurado como TCP Server.
- **Server KEY:** Clave privada del certificado usado por el equipo basado en TITAN al ser configurado por TCP Server.
- **Client certificate 1:** En caso de usar "Client authentication", este campo permite introducir el certificado autorizado 1.
- **Client certificate 2:** En caso de usar "Client authentication", este campo permite introducir el certificado autorizado 2.

- **Client certificate 3:** En caso de usar “Client authentication”, este campo permite introducir el certificado autorizado 3.
- **Client authentication:** Si se activa esta casilla el equipo basado en TITAN sólo permitirá la conexión a sus sockets TCP Server a clientes que usen los certificados de cliente autorizados.

La sección **Serial Gateway → SSL/TLS Certificates (TCP CLIENT)** hace referencia a los certificados cuando el puerto COM se ha configurado como un socket TCP Client

Los certificados para sockets TCP Cliente son únicamente necesarios cuando el servidor TCP remoto (donde se conectará el equipo basado en TITAN) necesita autenticación por certificado.

- **Client Port1 Certificate:** Certificado (formato PEM) para ser usado por el equipo basado en TITAN cuando un puerto serie Port1 actúa como cliente TCP con SSL/TLS con identificación por certificado
- **Client Port1 KEY:** Clave privada del certificado usado por el equipo basado en TITAN cuando un puerto serie Port1 actúa como cliente TCP con SSL/TLS con identificación por certificado.
- **Client Port2 Certificate:** Certificado (formato PEM) para ser usado por el equipo basado en TITAN cuando un puerto serie Port2 actúa como cliente TCP con SSL/TLS con identificación por certificado
- **Client Port2 KEY:** Clave privada del certificado usado por el equipo basado en TITAN cuando un puerto serie Port2 actúa como cliente TCP con SSL/TLS con identificación por certificado.

La sección **Serial Gateway → SSL/TLS Certificates → Tools** es una utilidad que le permite generar un par de claves .crt y .key de forma cómoda para realizar tests de funcionamiento. No es recomendable usarlas en producción, pues la recomendación actual es utilizar claves RSA superiores a 3000 bits.

- ◊ Led Config
- ◊ Syslog
- ◊ Backup / Factory
- ◊ Firmware Upgrade
- ◊ Reboot
- ◊ Logout

▶ Serial Gateway ▶ SSL/TLS Certificates ▶ Tools

With this tool you can generate a pair of files certificate.crt and certificate.key for your tests.

Process Status:

REFRESH

GENERATE FILES

DELETE FILES

4.6- External Devices

Desde esta sección se configura el datalogger interno, así como periféricos serie externos (sondas de temperatura, dispositivos Modbus RTU o Modbus TCP, dispositivos RS232-485 genéricos, etc ...).

4.6.1- External Devices → Logger configuration

Si necesita que el equipo basado en TITAN recoja datos de dispositivos externos (dispositivos Modbus, sensores de temperatura, dispositivos serie genéricos, receptores GPS, dispositivos W-Mbus, contadores IEC-102, ...) para enviarlos a un servidor externo necesita primero configurar el Logger interno, esto es, cómo recoger los datos, dónde y cómo enviarlos. Para eso es esta sección.

Esta sección se permite configurar los parámetros relativos al datalogger interno. Puede enviar los datos a un servidor mediante HTTP/HTTPS, FTP/FTPS o MQTT/MQTTS. En todos los casos se enviarán los datos en formato JSON

Parámetros generales:

The screenshot shows the webdyn TITAN configuration interface. The top header includes the webdyn logo and the TITAN logo with the tagline "Makes your APPLICATION happen". On the left, there is a sidebar menu with sections: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), and Wifi (Basic Settings, DHCP Server). The main content area is titled "External Devices - Logger" and contains the following configuration fields:

- ID:** A text input field containing "pepinoLogger". To its right, it says "Optional. Device identification".
- Send mode:** A dropdown menu set to "FIFO". To its right, it says "Send mode (normally FIFO)".
- Time format:** A dropdown menu set to "unix (yyyy-mm-ddTHH:mm:ss)". To its right, it says "Time format used in timestamp logger data".
- Use script:** An unchecked checkbox. To its right, it says "Check for customized json using 'Json Transformer Script' in [Script section](#)".
- Use array:** An unchecked checkbox. To its right, it says "Check if you want to send more than one JSON per transmission".
- Check date:** An unchecked checkbox. To its right, it says "Save data in Logger only if date has been set (check [Time Servers](#))".

- **ID:** Opcional. Es un parámetro de texto que permite introducir un string identificativo que se incluye dentro del JSON.
- **Send mode:** FIFO or LIFO: En modo FIFO los datos se transmiten al servidor en orden de llegada, es decir, los primeros datos en entrar el datalogger son los primeros en enviarse. El modo LIFO es al revés, son los últimos datos recibidos los primeros en enviarse. El modo LIFO puede resultar útil en aquellas aplicaciones donde siempre se quieran visualizar los datos en pantalla en tiempo real. Por ejemplo, puede darse el caso que un equipo esté varios días sin cobertura, almacenando gran cantidad de datos sin poder transmitirlos. Una vez vuelva la cobertura, podría tardar cierto tiempo en enviarse todos los datos acumulados al servidor. En modo LIFO, al enviar los últimos datos recogidos en primer lugar, rápidamente podría visualizarse en una pantalla los datos en tiempo real mientras van llegando posteriormente el resto de datos capturados con anterioridad.

- **Time format:** el objeto JSON de datos incluye siempre un timestamp (fecha y hora) con el momento en el que fue registrado el dato guardado. Este parámetro permite especificar el formato de dicho timestamp.
- **Use script:** Si se activa esta casilla, antes de que el equipo basado en TITAN almacene datos recogidos (por ejemplo, una lectura Modbus) en su memoria interna (datalogger) en el formato JSON predeterminado del equipo basado en TITAN, pueden formatearse dichos datos para almacenarse con otro formato. Esto puede resultar muy útil para el envío de datos a plataformas que necesiten de una estructura concreta. Consulte la nota de aplicación relacionada con los 'JSON Transformer Script' para más información.

Por ejemplo, unos registros Modbus leídos por el equipo basado en TITAN se almacenarían de forma estándar con el siguiente formato:

```
{"IMEI":"869101054287806","TYPE":"MODB","TS":"2022-06-03T11:38:01Z","ID":"TRES","A":"192.168.1.28:502","ST":"1","N":"6","V":[1,2,3,4,5,6],"P":"ID0001"}
```

Pero quizás pueda interesarnos cambiar esta estructura, añadir nuevos campos personalizados, etc

```
{"data":{"IMEI":"869101054287806","TYPE":"MODB","TS":"2022-06-03T11:38:01Z","ID":"TRES","A":"192.168.1.28:502","ST":"1","N":"6","V":[1,2,3,4,5,6],"P":"ID0001","myField1":123,"myField2":456}}
```

Este cambio de formato puede realizarse mediante los "JSON Transformer Scripts"

- **Use array:** Por defecto el equipo basado en TITAN envía los datos a un servidor (MQTT, HTTP) registro a registro, es decir, una transmisión por registro enviado. Si selecciona la opción "Use array" los datos son enviados en forma de array, permitiendo en envío simultáneo de hasta 100 lecturas y acelerando enormemente el proceso de envío de datos.

Por ejemplo, si esta casilla no está seleccionada, los datos son transmitidos en el formato JSON estándar del equipo basado en TITAN

```
{"IMEI":"869101054287806","TYPE":"MODB","TS":"2022-06-03T11:38:01Z","ID":"TRES","A":"192.168.1.28:502","ST":"1","N":"6","V":[1,2,3,4,5,6],"P":"ID0001"}
```

Si la casilla está seleccionada, los datos se transmiten en forma de array con un contenido entre 1 y 100 elementos, dependiendo de los datos almacenados en el interior del datalogger.

```
[{"IMEI":"869101054287806","TYPE":"MODB","TS":"2022-06-03T11:38:01Z","ID":"TRES","A":"192.168.1.28:502","ST":"1","N":"6","V":[1,2,3,4,5,6],"P":"ID0001"}, {"IMEI":"869101054287806","TYPE":"MODB","TS":"2022-06-03T11:39:01Z","ID":"TRES","A":"192.168.1.28:502","ST":"1","N":"6","V":[1,2,3,4,5,6],"P":"ID0001"}, {"IMEI":"869101054287806","TYPE":"MODB","TS":"2022-06-03T11:40:01Z","ID":"TRES","A":"192.168.1.28:502","ST":"1","N":"6","V":[1,2,3,4,5,6],"P":"ID0001"}, ... ]
```

- **Check date:** los datos serán salvados en el "Logger" si la fecha está establecida.

Modo HTTP

- NAT
- Authorized IPs
- MAC Filter
- Routes
- ★ **Serial Settings**
 - Serial Port1-RS232
 - Serial Port2-RS485
 - SSL Certificates
- ★ **External Devices**
 - Logger configuration
 - ModBus Devices
 - Generic Serial Device
 - Temperature Sensor
 - IEC102 Meter
 - CAN Receiver

Communication mode: WEB PLATFORM (HTTP REST)

Enabled: ☐ Communication mode HTTP enabled

Mode: Method of sending data

Custom header1: Optional. Custom header1. For example: Content-type:application/json

Custom header2: Optional. Custom header2. For example: IDENTITY_KEY;YOUR_KEY

Custom header3: Optional. Custom header3.

Server: Destination URL. Example: www.mydomain.com/setdata.php

Server Username: Optional. Blank if no server authentication required

Server Password: Optional. Blank if no server authentication required

- **Enabled:** Click para habilitar el modo de envío de datos a una plataforma web vía HTTP/HTTPS
- **Mode:** modo de envío de datos. Puede seleccionar entre HTTP GET (JSON), HTTPS GET (JSON), HTTP POST (JSON), HTTPS POST (JSON)
- **Custom header1, Custom header2 y Custom header3:** Le permite añadir headers a las peticiones HTTP/HTTPS. Muchas plataformas WEB obligan a incluir un header con un token identificativo. Desde esta sección puede configurarlo.
- **Server:** URL completo para el envío de datos recogidos en el datalogger. Por ejemplo www.metering.es/json/set.asp?data=
- **Server Username:** En caso de que su plataforma cuente con acceso restringido, introduzca aquí el nombre de usuario.
- **Server Password:** En caso de que su plataforma cuente con acceso restringido, introduzca aquí el Password de usuario.

Modo FTP SERVER

- VPN - IPSec - OpenVPN Client - OpenVPN Server - ZeroTier - Device Manager - KARE - Other - AT Command - DynDns - Private DynDns - Sms control - Periodic Autoreset - Time Servers	Communication mode: FTP SERVER	
	Enabled:	☐ Communication mode FTP enabled
	FTP prot.:	FTP / FTPS protocol
	FTP Server:	Destination FTP Server. Example: ftp.mydomain.com
	FTP port:	FTP server port. Default 21
	FTP Path:	FTP path. Example: /dev/plcs/
	FTP Username:	FTP Username
	FTP Password:	FTP Password
FTP File Period:	FTP File Period (one file every minute, hour, day)	

- **Enabled:** Click para habilitar el modo de envío de datos a un servidor FTP (el formato del archivo de datos es en formato JSON).
- **FTP prot.:** Permite seleccionar el protocolo de envío, escogiendo entre FTP o el protocolo seguro FTPS.
- **FTP Server:** Servidor FTP para el envío de datos (IP o DNS)
- **FTP port:** Puerto del servidor FTP, normalmente 21.
- **FTP Path:** Ruta dentro del servidor donde realizar el volcado de datos.
- **FTP Username:** El nombre de usuario de una cuenta de su servidor FTP que permita escritura
- **FTP Password:** El Password de una cuenta de su servidor FTP que permita escritura

FTP File Period: Cada cuanto tiempo quiere que el TITAN envíe el fichero de datos acumulado a su servidor (cada día, cada hora o cada minuto)

Modo MQTT

- Remote Console - Snmp - Tacacs+ - Ldap - Mqtt / Mqtts - Http / Https - User Permissions - Passwords Web UI - CA Certificates - Email Config - ModBus Slave - Titan Scripts	Communication mode: MQTT	
	Enabled:	☒ Communication mode MQTT enabled
	MQTT Topic	MQTT Topic. Example: [IMEI]/logger
	MQTT Broker	Broker used by logger MQTT
	Confirm policy	Any deletes when one broker confirms. All waits for every selected broker
Note: Other>MQTT menu must be configured		

- **Enabled:** Click para habilitar el modo de envío de datos a un bróker MQTT (todos los datos son enviados en formato JSON).
- **MQTT Topic:** Topic MQTT al que se enviarán los datos almacenados en el logger.
- **MQTT Broker:** permite seleccionar el bróker MQTT utilizado para el envío de los datos del logger. Puede seleccionarse Primary, Secondary o Both.
- **Confirm policy:** permite definir cuándo se considera enviado un registro cuando se utiliza la opción Both. El valor "Any" elimina el registro cuando al menos un bróker confirma el envío. El valor "All" espera la confirmación de todos los brókers seleccionados.

Real Time Status.

Permite ver el estado del datalogger interno del equipo basado en TITAN y poder visualizar los datos pendientes de envío. Puede resultar útil también para algunas aplicaciones en los que no se desee transmitir datos a un servidor remoto.

The screenshot displays the webdyn TITAN web interface. At the top, the 'webdyn' logo is on the left and the 'TITAN' logo with the tagline 'Makes your APPLICATION happen' is on the right. A left sidebar contains a navigation menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), and External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor, IEC102 Meter, GPS Receiver). The main content area is titled 'Z-Other > Logger Registers (pending of transmission)'. It features a large empty rectangular box for data. Below this box, there are controls: 'Show: Max 100 rows' with a dropdown arrow, a 'Text filter:' input field, and a 'SHOW DATA' button. At the bottom of the main area, there are three buttons: 'RETURN TO LOGGER PAGE', 'DELETE ALL PENDING REGISTERS FROM LOGGER', and 'COPY TO CLIPBOARD'.

Desde esta sección también puede eliminar todos los datos que el equipo basado en TITAN tenga pendientes de envío pulsando el botón “DELETE ALL PENDING REGISTERS FROM LOGGER”. También podrá filtrar por texto.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Cuando se utiliza el modo de envío HTTP o MQTT los datos se van enviando a su servidor según se van recogiendo. En caso de falta de cobertura 4G/3G/2G o problemas con el envío de datos (por ejemplo, una caída del servidor remoto), el equipo basado en TITAN almacenará los datos en su interior para un posterior envío cuando la comunicación se normalice.
- Cuando se utiliza el modo de envío FTP los datos se almacenan en un fichero de estructura de registros JSON y se envían según el intervalo de tiempo seleccionado (minuto, hora, día) para el envío. En caso de falta de cobertura GSM o problemas con el envío de datos (por ejemplo, una caída del servidor remoto), el equipo basado en TITAN almacenará los datos en su interior para su posterior envío cuando la comunicación se normalice.
- El nombre del fichero FTP que se crea en su servidor tendrá el formato:
 IMEI-año-mes-día.txt → Si el periodo seleccionado de envío de datos es “cada día”.
 IMEI-año-mes-día-hora.txt → Si el periodo seleccionado de envío de datos es “cada hora”.
 IMEI-año-mes-día-hora-minuto.txt → Si el periodo seleccionado de envío de datos es “cada minuto”.
- Si utiliza el modo MQTT, recuerde configurar adecuadamente la sección “OTHER → Mqtt”. En esa sección debe introducir todos los parámetros de configuración necesarios para conectar el equipo basado en TITAN a su bróker MQTT
- Por motivos de seguridad, siempre que sea posible, se recomienda encarecidamente de comunicaciones SSL/TLS como es HTTPS, MQTTS o FTPS. Las comunicaciones HTTP, MQTT o FTP (sin SSL/TLS) no son seguras.

4.6.2- External Devices → Temperature Sensor

Si su modelo de equipo basado en TITAN soporta una sonda de temperatura MTX-Temp-RS232 podrá enviar la temperatura de forma periódica a una plataforma web, enviar un mensaje SMS de alerta cuando la temperatura esté por encima o por debajo de un determinado umbral, etc.

- **Enabled:** Active esta casilla si tiene una sonda de temperatura MTX-Temp-RS232 conectado a un puerto serie.
- **Communication Port:** Seleccione el puerto serie del equipo donde tiene conectada la sonda de temperatura MTX-Temp-RS232.
- **Interval:** Si pretende enviar de forma periódica lecturas de la temperatura a su servidor web, indique aquí el periodo, en minutos.
- **Logger:** Si quiere utilizar el logger interno para almacenar datos de temperatura (para su posterior envío a una plataforma web, debe seleccionar esta opción. ¿Cuándo no debería activarse esta opción? Pues por ejemplo cuando únicamente quiere enviar un SMS de alerta ante una temperatura fuera de márgenes.
- **Alarms enabled:** Seleccione esta opción si quiere activar las alarmas por temperatura fuera de margen.
- **Max Temperature:** Temperatura máxima a partir de la cual se considera alarma por temperatura alta.
- **Text alarm on (max):** Texto de alarma enviado cuando se produce una alarma por temperatura alta.
- **Text alarm off (max):** Texto de alarma enviado cuando se desactiva una alarma por temperatura alta.
- **Min Temperature:** Temperatura mínima a partir de la cual se considera alarma por temperatura baja.
- **Text alarm on (min):** Texto de alarma enviado cuando se produce una alarma por temperatura baja.
- **Text alarm off (min):** Texto de alarma enviado cuando se desactiva una alarma por temperatura baja.
- **Phone numbers:** Números de teléfono (separados por punto y coma “;”) a los que enviar los mensajes de alarma por SMS
- **Current temperature:** indica, de haber un sensor de temperatura MTX-Temp-RS232 conectado, la temperatura actual en tiempo real.

★ Mobile

- ◆ Status
- ◆ Basic Settings
- ◆ Keep Online

★ Ethernet

- ◆ Basic Settings
- ◆ DHCP Server

★ Wifi

- ◆ Basic Settings
- ◆ DHCP Server

★ Firewall

- ◆ NAT
- ◆ Authorized IPs
- ◆ MAC Filter
- ◆ Routes

★ Serial Settings

- ◆ Serial Port1-RS232
- ◆ Serial Port2-RS485
- ◆ SSL Certificates

★ External Devices

- ◆ Logger configuration
- ◆ ModBus Devices
- ◆ Generic Serial Device
- ◆ Temperature Sensor
- ◆ IEC102 Meter
- ◆ GPS Receiver

★ VPN

- ◆ IPSec
- ◆ OpenVPN Client

► External Devices ► Temperature Sensor

Enabled:	☐	Enable Temperature sensor
Communication Port:	Serial Port 1	Select the connected port
Interval:	5	Reading period (minutes)
Logger:	☐	Check if logger must be used Please, configure logger before using this option
Alarms Enabled:	☐	Enable alarm of temperature sensor
Max Temperature:	50	Select high temperature
Text alarm on (max):		Text of SMS when alarm activated (max temp)
Text alarm off (max):		Text of SMS when alarm deactivated (max temp)
Min Temperature:	0	Select low temperature
Text alarm on (min):		Text of SMS when alarm activated (min temp)
Text alarm off (min):		Text of SMS when alarm deactivated (min temp)
Phone numbers:		Phone numbers for SMS alarm message. (separated with ;)
Current temperature:	ERROR °C	Real time value

SAVE CONFIG REFRESH

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- La histéresis que utiliza el equipo es de 1 grado. Por ejemplo, si configura como temperatura alta 50°C, la alarma saltará al llegar a los 50°C, pero no se considerará que la alarma ha desaparecido hasta bajar por lo menos a 49°. Esto evita continuos envíos de SMS cuando la temperatura está justo en el umbral seleccionado.
- Ejemplo de formato de la trama JSON enviada:

```
{ "IMEI": "358884050088207", "TS": "25/12/2014 17:40:09", "TYPE": "TEMP",  
  "P": "1234", "TEM": 25.5, "TEMH": 0, "TEML": 0 }
```

Donde:

IMEI: número identificativo del equipo. Único para cada equipo

TS: timestamp DD:MM:YYYY HH:MM:SS

TYPE: tipo de trama. En este caso temperatura

P: campo ID del Logger (External Devices > Logger configuration)

TEM: temperatura

TEMH: alarma por temperatura alta (0=no, 1=sí)

TEML: alarma por temperatura baja (0=no, 1=sí)

4.6.3- External Devices → Modbus Devices

Basic Mode

Desde la versión de firmware 5.3.6.25 es posible escoger entre “**Basic Mode**” (único modo existente hasta el firmware 5.3.6.24) y “Expert Mode”.

Los equipos basados en TITAN están preparados para leer, almacenar y enviar a un servidor externo (vía HTTP/HTTPS, FTP o MQTT/MQTTS) registros de dispositivos externos Modbus RTU y Modbus TCP. Es decir, puede programar una lectura periódica de hasta 40 dispositivos Modbus RTU y/o TCP, seleccionando los registros de lectura, y enviando posteriormente las lecturas a un servidor mediante un objeto JSON.

- **Enabled:** Active esta casilla si tiene un o varios dispositivos Modbus RTU conectados a un puerto serie y pretende leer de forma autónoma los registros Modbus.
- **Serial Port:** Permite seleccionar el puerto serie RS232 o RS485 del equipo basado en TITAN donde tiene conectado el equipo Modbus RTU.
- **Logger:** Si quiere utilizar el logger interno para almacenar los registros Modbus leídos (para su posterior envío a una plataforma web) debe seleccionar esta opción.
- **Device name:** nombre identificativo de un dispositivo Modbus RTU o Modbus TCP.
- **Address:** dirección Modbus rtu del dispositivo a leer. En caso de ser un dispositivo modbus tcp debe especificarse la IP y puerto (formato IP:puerto)
- **Command:** comando Modbus de lectura.
- **Start:** registro inicial de lectura
- **Num Words:** número de registros a leer
- **Reg type:** tipo de registro a leer
- **Period:** periodo de lectura, es decir, cada cuántos minutos se deben leer el conjunto de registros.

Importante: Consulte la nota de aplicación AN27 (ANV6_27-Router-TITAN-Modbus-RTU-TCP-Concentrator-multimap_HTTP.pdf y ANV6_32-Router-TITAN-Modbus-RTU-TCP-Concentrator-multimap_MQTT.pdf) donde encontrará información detallada y con ejemplos de cómo usar esta funcionalidad de los equipos basados en TITAN.

★ **Mobile**

- ◆ Status
- ◆ Basic Settings
- ◆ Keep Online

★ **Ethernet**

- ◆ Basic Settings
- ◆ DHCP Server

★ **Wifi**

- ◆ Basic Settings
- ◆ DHCP Server

★ **Firewall**

- ◆ NAT
- ◆ Authorized IPs
- ◆ MAC Filter
- ◆ Routes

★ **Serial Settings**

- ◆ Serial Port1-RS232
- ◆ Serial Port2-RS485
- ◆ SSL Certificates

★ **External Devices**

- ◆ Logger configuration
- ◆ ModBus Devices
- ◆ Generic Serial Device
- ◆ Temperature Sensor
- ◆ IEC102 Meter
- ◆ GPS Receiver

★ **VPN**

- ◆ IPsec
- ◆ OpenVPN Client

► **External Devices** ► **ModBus**

[Change to expert mode](#)

Enabled: ☐ Enable Modbus Devices

Serial Port: Select the connected serial port if needed

Logger: ☐ Check if logger must be used. Please, configure logger before using this option

[SAVE CONFIG](#)

[VIEW LOG](#)

Dev. name	Addr.	Comm.	Start @	Num word/bit	Reg Type	Period
-----------	-------	-------	---------	--------------	----------	--------

Device name / ID: Insert the device name or ID

Address: Modbus RTU address or IP:port address

Command: Modbus read command

Start: Address of the first register

Number Words / Bits: Words for command 0x03/0x04. Bits for 0x01/0x02

Reg Type: Type of registers for command 0x03/0x04

Period: Read period (minutes)

[SAVE DEVICE](#) (Max 40 modbus devices)

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Si desea crear un nuevo dispositivo Modbus RTU debe completar los datos del formulario y pulsar el botón "SAVE DEVICE".
- Ejemplo de formato de la trama JSON almacenada con las lecturas para enviar a un servidor es el siguiente:

```
{"IMEI":"354740050367237","TS":"17/02/2014 19:02:46","TYPE":"MODB",
"P":"1234","ST":1,"A":1,"V":[1,2,3,4,5,6,7,8,9,10]}
```

Donde:

IMEI: número identificativo del equipo. Único para cada equipo

TS: timestamp DD:MM:YYYY HH:MM:SS

TYPE: tipo de datos. En este caso Modbus

P: campo ID del Logger (External Devices > Logger configuration)

ST: registro inicial

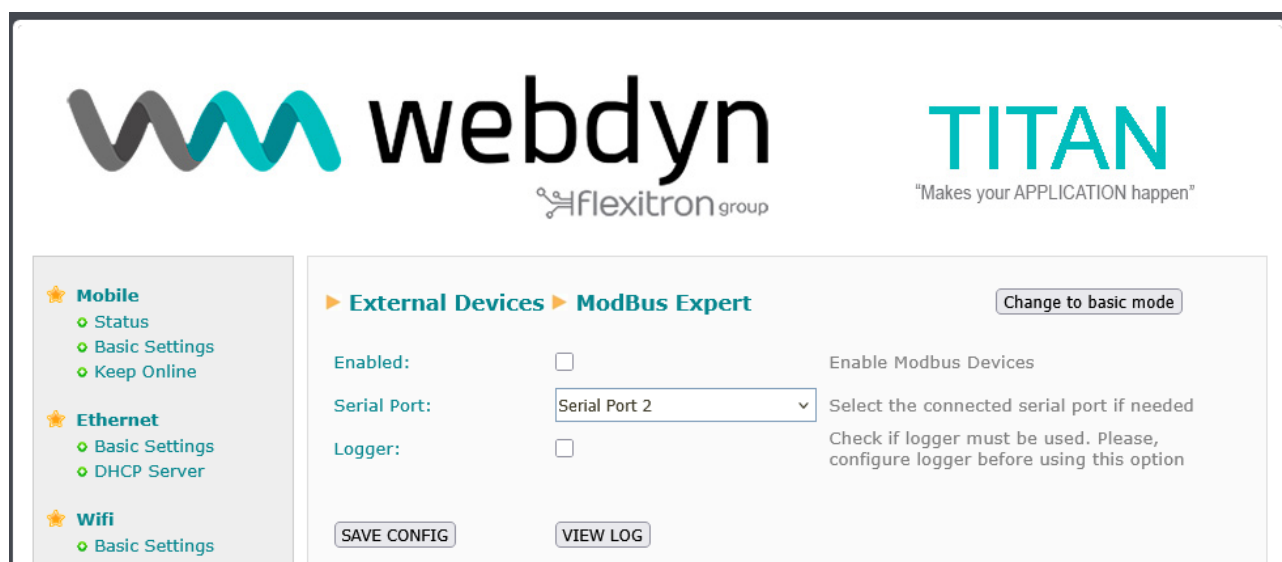
A: dirección Modbus del dispositivo leído

V: array con los registros leídos

- Se recomienda leer el capítulo de los comandos AT disponibles, ya que es posible leer y cambiar valores de registros Modbus vía comandos AT, desde el entorno de configuración web, desde Remote Console (Telnet), SSH, o bien desde SMS, etc
- En los campos “Start” y “Num Words” es posible establecer registros no consecutivos a partir de la versión de firmware 3.26. Consulte la nota de aplicación AN27 (ANV6_27-Router-TITAN-Modbus-RTU-TCP-Concentrator-multimap_HTTP.pdf) y AN32 ANV6_32-Router-TITAN-Modbus-RTU-TCP-Concentrator-multimap_MQTT.pdf) para más información y ejemplos.

Expert Mode

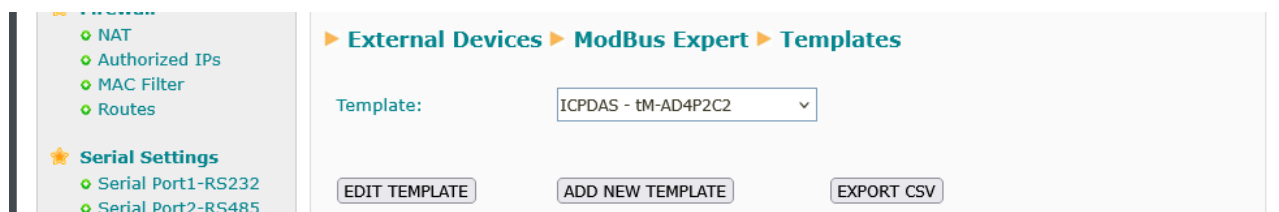
El modo de funcionamiento “Expert Mode” es muy similar al “Basic Mode” pero con un aumento significativamente elevado de prestaciones con respecto a su predecesor. La pantalla principal está dividida en tres secciones diferenciadas. La primera se muestra en la siguiente pantalla:



- **Enabled:** Active esta casilla activar el servicio de Modbus “Expert Mode”. Si estuviera activado el servicio Modbus “Basic mode”, éste sería desactivado automáticamente ya que no es posible utilizar ambos servicios de forma simultánea.

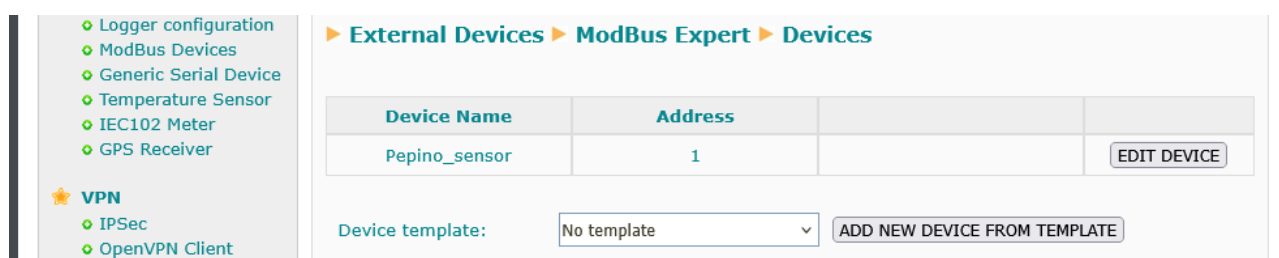
- **Serial Port:** Permite seleccionar el puerto serie RS232 o RS485 del equipo basado en TITAN donde tiene conectado los equipos Modbus RTU. También puede escoger la opción “None” si únicamente va a trabajar con dispositivos modbus TCP. Si va a trabajar simultáneamente con equipos Modbus RTU y Modbus TCP, especifique el puerto serie al que están conectados sus dispositivos Modbus RTU (“Serial Port 1” para RS232 y “Serial Port 2” para RS485)
- **Logger:** Active esta casilla si desea almacenar las lecturas de los registros Modbus en el datalogger interno del router Titan para su envío posterior a una plataforma WEB (HTTP, MQTT, FTP).

La siguiente sección muestra las plantillas de dispositivos. Las plantillas de dispositivos son útiles si pretende añadir a una instalación múltiples dispositivos de un mismo tipo. Creando una plantilla se puede añadir rápidamente un nuevo dispositivo Modbus basado en una plantilla sin necesidad de crear todo el mapa de registros modbus de nuevo.



- **Edit template:** Permite editar la plantilla indicada en el desplegable “Template”.
- **Add new template:** Permite crear una nueva plantilla
- **Export CSV:** Permite exportar una plantilla en formato CSV. Útil para importarla en otros equipos.

La última sección de la pantalla muestra una tabla los dispositivos modbus creados.



En dicha tabla se muestra el nombre del dispositivo y si dirección modbus RTU o modbus TCP. Pulsando el botón “**EDIT DEVICE**” de uno de los dispositivos se accederá a la pantalla de edición de los registros modbus correspondientes de ese dispositivo.

Para añadir un nuevo dispositivo a la lista basta con escoger una plantilla desde la que se desee partir para la creación de este. Si no se desea seleccionar ninguna plantilla, simplemente debe seleccionarse “No template” y pulsar el botón “**ADD NEW DEVICE FROM TEMPLATE**”.

En esa última sección se incluye un botón con nombre “**RESTART MODBUS SERVICE**”. Si el servicio modbus expert está funcionando, permite la recarga de la configuración de todos los equipos y el reinicio del servicio. Eso permite cambios en las configuraciones de los dispositivos modbus (modificaciones, eliminación de dispositivos, alta de nuevos dispositivos) y reiniciar el servicio sin necesidad de reiniciar el router Titan.

Pantalla de edición de dispositivos (External Devices>ModBus Expert>Devices):

Si damos al botón de “ADD NEW DEVICE FROM TEMPLATE”:

Nos saldrá la siguiente pantalla:

v[x]	register	type	flip	com.	name	units	mode
0		UInt16	No	3			Not used
	Period factor	1	Script:				
1		UInt16	No	3			Not used
	Period factor	1	Script:				
2		UInt16	No	3			Not used
	Period factor	1	Script:				
3		UInt16	No	3			Not used
	Period factor	1	Script:				

La sección superior de la pantalla anterior permite configurar los siguientes parámetros:

- **Name:** Nombre del dispositivo
- **Template Brand:** No editable. Importada de la plantilla utilizada.
- **Template Model:** No editable. Importada de la plantilla utilizada.
- **Address:** Dirección modbus RTU del dispositivo o dirección IP con el formato IP@ID:PORT, donde IP es la dirección IP del dispositivo modbus TCP, ID (opcional) su dirección interna (normalmente 1) y PORT el puerto TCP.
- Ejemplos válidos: 192.168.1.100:502 , [192.168.1.100@1:502](#) También es posible establecer la dirección "0" si desea deshabilitar en algún momento el dispositivo (para no ser leído) si necesidad de eliminarlo.
- **Period:** Indica el periodo base, en minutos, en el que los registros modbus leídos serán almacenados en el interior del datalogger del router Titan para su posterior envío a una plataforma WEB. Por ejemplo, si especifica 5, los registros leídos son almacenados, por defecto, cada 5 minutos.

La sección inferior muestra el mapa completo de registros modbus del dispositivo:

v[x]	register	type	flip	com.	name	units	mode
0		UInt16 ▾	No ▾	3 ▾			Not used ▾
	Period factor	1 ▾	Script:				

- **V[0]:** Es un array donde se almacena el valor leído por el registro. Es importante para la sección "Script", como se verá más adelante.
- **Register:** Debe indicarse el número de registro a leer. Por ejemplo, el 40000. En el caso de que el registro sea de tipo String, debe indicarse la dirección del registro, seguido de "_" y finalizado por el número de caracteres. Por ejemplo, para un String de longitud 10 que empieza en el registro 42000, debería indicarse "42000_10"
- **Type:** debe indicarse el tipo de registro modbus a leer. Tipos de datos disponibles:
 - **UInt16:** Unsigned integer de 16 bits (1 WORD)
 - **UInt32:** Unsigned integer de 32 bits (2 WORD)
 - **UInt64:** Unsigned integer de 64 bits (4 WORD)
 - **Int16:** Integer de 16 bits (1 WORD)
 - **Int32:** Integer de 32 bits (2 WORD)
 - **Int64:** Integer de 64 bits (4 WORD)
 - **Float:** Float (32 bits, 2 WORD)
 - **Double:** Double (64 bits, 4 WORD)
 - **String:** String (X WORD)
 - **Bit:** Bit (1 WORD)
- **Flip:** Permite la rotación de words o bytes de un tipo de datos, permitiendo todas la combinaciones.
 - **No:** No se realiza ninguna rotación
 - **W:** Rotación de words del registro
 - **B:** Rotación de bytes de cada word
 - **W+B:** Rotación de words y bytes.
 - **W2:** Rotación de 2 words del registro

- **W2+B:** Rotación de 2 words y bytes

Ejemplo de rotación para un registro de tipo **DOUBLE**:

No: AB CD EF GH
W: GH EF CD AB
B: BA DC FE HG
W+B: HG FE DC BA
W2: EF GH AB CD
W2+B: FE HG BA DC

- **Com.:** especifica el comando de lectura del registro
 - **1:** Lectura de registros de tipo bobina (coils)
 - **2:** Lectura de registros de tipo bit (discrete inputs)
 - **3:** Lectura de registros de retención (holding registers)
 - **4:** Lectura de registros de entrada (input Registers).
- **name:** (Opcional). Texto con el nombre del registro.
- **name:** (Opcional). Texto con las unidades del registro.
- **mode:** Indica qué debe hacerse con el registro. Las opciones son las siguientes:
 - **Not used:** El registro no será leído por el router.
 - **Not saved:** El registro será leído, pero la lectura no será almacenada en el datalogger. Esto puede ser útil para determinados tipos de registros dependientes de otros. Por ejemplo, si un registro X sólo indicara si un tercer registro tiene las unidades en voltios o milivoltios, podría ser necesario leerlo, pero no almacenar la información en el datalogger. En ese caso, el modo "Not saved" es el adecuado.
 - **Instant:** El registro será leído, y cuando llegue el momento indicado en el periodo, el valor leído en ese momento (valor instantáneo) será el que se almacene en el datalogger.
 - **Average:** El registro será leído, y cuando llegue el momento indicado en el periodo, el valor medio registrado durante el periodo de lectura es el que será almacenado en el datalogger.
 - **Minimun:** El registro será leído, y cuando llegue el momento indicado en el periodo, el valor mínimo leído durante el periodo de lectura es el que será almacenado en el datalogger.
 - **Maximun:** El registro será leído, y cuando llegue el momento indicado en el periodo, el valor máximo leído durante el periodo de lectura es el que será almacenado en el datalogger.

Nota: El número de muestras que se toman para la generación de los valores medios variarán en función del número de dispositivos y de los registros a leer. El router Titán leerá todos los registros de forma cíclica a la mayor velocidad posible. A mayor número de dispositivos y mayor número de lecturas a realizar, menor número de muestras.

- **Period factor:** Campo numérico que permite un múltiplo de periodo para el registro. Por ejemplo, si el campo “Period” tuviera un valor de 5, la lectura de los registros, por defecto, se almacenarán en el datalogger cada 5 minutos. Pero si algún determinado registro quiere almacenarse cada 15 minutos, en el campo “Period factor” debería indicarse un “3”. Los datos se almacenarían en el datalogger 1 de cada 3 veces cada 5 minutos, es decir, cada 15 minutos.
- **Script:** (Opcional). Pequeño script en javascript (v5) que puede introducirse para operar sobre un valor leído. Permite el acceso a los valores v[x] y permite también el acceso al objeto “mtx” (véase la sección TITAN SCRIPTS para más información sobre el objeto “mtx”).

Ejemplos:

v[x]	register	type	flip	com.	name	units	mode
0	40000	UInt16 ▾	No ▾	4 ▾	Voltage	Volts	Instant ▾
	Period factor	1 ▾	Script:	return v[0]/1000;			

El script “**return v[0]/1000;**” haría que el valor almacenado en el datalogger no sea directamente el valor leído del registro 40000, sino que antes de almacenarlo en el datalogger se dividirá por 1000 para almacenar el valor en voltios.

v[x]	register	type	flip	com.	name	units	mode
0	40000	UInt16 ▾	No ▾	4 ▾	Voltage	Volts	Instant ▾
	Period factor	1 ▾	Script:	if (v[1]==0) {return v[0];} else {return v[0]/1000;}			

El script:

```

If (V[1]==0) {
    return v[0];
} else {
    return v[0]/1000;
}

```

haría que el valor almacenado en el datalogger no sea el valor leído del registro 40000, sino que antes de almacenarlo, si el registro v[1] tiene el valor “0”, se almacena directamente el valor de v[0]. En cambio, si v[1] tiene el valor “1”, se almacena el valor v[0]/1000;

Es decir, los scripts permiten realizar operaciones de los registros antes de almacenarlos en el datalogger, permitiendo incluso interaccionar con el valor de otros registros.

v[x]	register	type	flip	com.	name	units	mode
0	30000	Int16 ▾	No ▾	3 ▾	Temperature	Celsius	Average ▾
	Period factor	1 ▾	Script:	if (v[0]>=300) mtx.modbusTCPSetBit("192.168.1.10",502,5,1)			

Imaginemos que con esta configuración, en el registro 30000, v[0], se almacena la temperatura media, que el sensor devuelve en décimas de grado. Por ejemplo, devuelve 300 para indicar 30.0°C, 252 para indicar 25.2°C, etc. Se pretende almacenar en el datalogger la media de la temperatura, pero almacenando el valor en grados celsius, de ahí que tendremos que incluir un “**return v[0]/10;**” en el script.

Pero adicionalmente, se necesita que, si la temperatura es igual o mayor a 30°C, se escriba un valor “1”, en el registro modbus 10000 de tipo bit de un PLC que funciona con modbus TCP para que active un ventilador. También se precisa que, si la temperatura es inferior a 29°C, se escriba un “0” en dicho registro 10000 para que se detenga el ventilador.

Por tanto, el script final quedaría así:

```
if (v[0]>=300)
    mtx.modbusTCPSetBit("192.168.1.10",502,5,10000,1);
elseif (v[0]<=290)
    mtx.modbusTCPSetBit("192.168.1.10",502,5,10000,0);
return v[0]/10;
```

Nota: Desde el script de un registro es posible hacer referencia al valor de otro registro. Por ejemplo, desde el script del registro v[1], se puede hacer referencia al registro v[0]. El v[0] hace referencia al valor del registro sin pasar por el script que pueda estar presente en el registro v[0]. En otras palabras, si en el registro v[0] existe un script que dice "return v[0]*2;", las referencias a v[0] desde el script de v[1] serán al valor de v[0] antes de multiplicarse por 2. Si se desea obtener el valor de v[0] después de que haya pasado por el script (es decir, el valor multiplicado por 2), en el script de v[1] se debe hacer referencia a **vs[0]** en lugar de **v[0]**.

Formato de almacenamiento en Datalogger.

Cuando los registros modbus se almacenan en la memoria del datalogger, se guardan con el siguiente formato JSON, descrito con un ejemplo:

```
{"IMEI":"865583042283167","TYPE":"MODB2","TS":"2023-10-03T11:46:00Z","P":"TITAN","ID":"Device2","A":"2","data":[{"R":30000,"V":"30.0","N":"Temperature","M":"3","U":"Celsius","S":"OK"},{"R":30001,"V":"40.0","N":"Humidity","M":"3","U":"%", "S":"OK"}]}
```

Donde:

IMEI: imei del router
TYPE: tipo de trama
TS: timestamp de cuando se leyeron los registros modbus
P: Campo “ID” de la sección de configuración “Logger”
ID: Campo “ID” de la sección de dispositivo Modbus
A: Dirección modbus del dispositivo
R: Dirección del registro
V: Valor del registro
N: Nombre del registro
M: Modo del registro (2: valor instantáneo, 3: valor medio, 4: valor máx, 5: valor mín)
U: Unidades
S: Status de la lectura (OK: lectura correcta, ERR: lectura incorrecta)

Notas adicionales.

- Se recomienda la lectura de la nota de aplicación “**ANV6_72-Router-Titan-Modbus-Expert**” para una mayor comprensión.
- Desde los TITAN Scripts es posible obtener los valores actuales de un dispositivo Modbus Expert en formato JSON, tanto usando la última lectura ya realizada por el servicio Modbus Expert como forzando una lectura Modbus en el momento de la ejecución del script. Consulte las funciones ``mtx.modbusExpertGetJson(deviceName)`` y ``mtx.modbusExpertReadJson(deviceName)`` en la sección de TITAN Scripts.

4.6.4- External Devices → GPS Receiver

Este menú permite configurar los datos de posicionamiento GPS de los equipos basados en TITAN que utilizan un módulo GPS interno o, si no dispone de módulo GPS interno, un receptor GPS NMEA conectado en uno de sus puertos RS232 o RS485

- **Enabled:** Active esta casilla si tiene un módulo GPS interno (o externo) conectado al equipo basado en TITAN que quiere utilizar.
- **Serial Port:** Seleccione el puerto serie del equipo basado en TITAN donde tiene conectado el GPS.
- **Interval:** Seleccione, en segundos, el periodo de lectura del GPS (obtendrá una posición GPS cada dicho número de segundos). Indique como valor mínimo 30 segundos.
- **Logger:** active esta casilla si quiere grabar en el logger interno las posiciones GPS leídas para, por ejemplo, enviarlas a su plataforma Web mediante HTTP/HTTPS, MQTT/MQTTS o FTP. Muy útil si desea usar el equipo basado en TITAN para implementar un sistema de control de flotas por GPS.
- **System time:** active esta casilla si quiere que la hora del sistema se sincronice con la hora leída del GPS.
- **TCP port listener:** permite obtener las tramas NMEA a través de una conexión IP realizada sobre el equipo basado en TITAN. Por ejemplo, si abre un socket contra la IP del equipo basado en TITAN al puerto especificado en este punto, podrá obtener en tiempo real las tramas NMEA de posicionamiento.
- **TCP Client IP:** Permite especificar una dirección IP para enviar las tramas NMEA a un servidor externo.
- **TCP Client Port:** Permite especificar el puerto TCP a donde enviar las tramas NMEA del servidor externo especificado en el parámetro "TCP Client IP".
- **TCP Client Timeout:** especifica los segundos que el equipo basado en TITAN debe dejar pasar entre que se detecta un cierre del socket y se vuelve a abrir de nuevo.

★ **Mobile**

- ◆ Status
- ◆ Basic Settings
- ◆ Keep Online

★ **Ethernet**

- ◆ Basic Settings
- ◆ DHCP Server

★ **Wifi**

- ◆ Basic Settings
- ◆ DHCP Server

★ **Firewall**

- ◆ NAT
- ◆ Authorized IPs
- ◆ MAC Filter
- ◆ Routes

★ **Serial Settings**

- ◆ Serial Port1-RS232
- ◆ Serial Port2-RS485
- ◆ SSL Certificates

★ **External Devices**

- ◆ Logger configuration
- ◆ ModBus Devices
- ◆ Generic Serial Device
- ◆ Temperature Sensor
- ◆ IEC102 Meter
- ◆ GPS Receiver

★ **VPN**

- ◆ IPSec
- ◆ OpenVPN Client
- ◆ OpenVPN Server
- ◆ ZeroTier

★ **Device Manager**

- ◆ KARE

★ **Other**

- ◆ AT Command
- ◆ DynDns
- ◆ Private DynDns

▶ **External Devices** ▶ **GPS Receiver**

Enabled:	☐	Enable GPS Receiver
Serial Port:	Serial Port 1	Select the connected serial port
Interval:	60	Reading period for logger (seconds, minimum 30)
Logger:	☐	Check if logger must be used. Please, configure logger before using this option
System time:	☐	Check for System time synchronization
TCP port listener:	20030	Redirect NMEA data to TCP server socket port if greater than 0 (1 frame / second)
TCP Client IP:		If filled with IP or DNS, Titan will send NMEA raw data to this server
TCP Client Port:	20030	
TCP Client timeout:	5	If socket closes, will wait this seconds in order to re-open the socket.

SAVE CONFIG

▶ **External Devices** ▶ **GPS Receiver** ▶ **Data**

Current gps position:

Gps Date:	
Gps Time:	
Latitude:	
Longitude:	
Speed (Km/h):	
Course:	
Altitude (m):	
Status:	

REFRESH DATA

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.6.5- External Devices → Generic Serial Device

Desde esta sección puede configurar un datalogger de dispositivos serie RS232 o RS485. Básicamente el equipo basado en TITAN leerá, almacenará los datos serie recogidos por cualquier de las interfaces antes mencionadas y los enviará a una plataforma Web vía HTTP/S, MQTT/S o FTP.

Especialmente indicado para recoger datos de dispositivos serie que emiten una trama de datos cada cierto tiempo (sensores de temperatura, de humedad, alarmas serie, ...)

- **Enabled:** Active esta casilla si quiere conectar un dispositivo serie y que el equipo basado en TITAN realice la función de datalogger.
- **Serial Port:** Seleccione el puerto serie del equipo basado en TITAN donde está conectado el dispositivo serie a loggear.
- **Interval:** Si especifica un "0" recogerá todas las tramas serie recibidas. Si especifica "1" recogerá una de cada dos tramas recibidas. Si especifica "2" recogerá una trama de cada tres tramas recibidas.
- **Only changes:** Active la casilla si sólo quiere loggear tramas que difieran de la trama anteriores. Por ejemplo, si conecta un sensor de temperatura dicho sensor puede estar emitiendo los mismos datos serie durante bastante tiempo hasta que cambie de temperatura. Si activa esta casilla únicamente se recogerán los datos serie cuando éstos cambien.
- **Mode:** modo de comunicación con Titan (RAW o binary).
- **Logger:** active esta casilla si quiere grabar en el logger interno los datos serie para enviarlos posteriormente a su plataforma Web mediante HTTP/HTTPS, FTP o MQTT/MQTTS
- **TX period:** un número mayor que 0 indica el periodo (en segundos) en los que se enviarán las tramas de datos "TX Frame1", "TX Frame2", "TX Frame3", "TX Frame4", "TX Frame5" por el puerto serie. Esta opción le permite "interrogar" a dispositivos serie con protocolos propietarios.
- **TX FrameX:** indica una trama de datos que será reenviada por el puerto serie cada X segundos especificados en el parámetro "TX period". Dichas tramas deben especificarse en formato hexadecimal. Ejemplo: 0102030A0D...

★ **Mobile**

- ◆ Status
- ◆ Basic Settings
- ◆ Keep Online

★ **Ethernet**

- ◆ Basic Settings
- ◆ DHCP Server

★ **Wifi**

- ◆ Basic Settings
- ◆ DHCP Server

★ **Firewall**

- ◆ NAT
- ◆ Authorized IPs
- ◆ MAC Filter
- ◆ Routes

★ **Serial Settings**

- ◆ Serial Port1-RS232
- ◆ Serial Port2-RS485
- ◆ SSL Certificates

★ **External Devices**

- ◆ Logger configuration
- ◆ ModBus Devices
- ◆ Generic Serial Device

► **External Devices** ► **Generic Serial Device**

Enabled:	☐	Enable Generic Serial Device
Serial Port:	Serial Port 1	Select the connected serial port
Interval:	0	0=save every serial frame
Only changes:	☐	Check for register every serial frame if different than previous one.
Mode:	Raw (Default)	Communication mode with Titan
Logger:	☐	Check if logger must be used. Please, configure logger before using this option
TX Period:	0	Period of TX Frames (seconds 30 ... 86400. 0=no TX Data)
TX Frame1:		HEX Frame 1 (max length 256)
TX Frame2:		HEX Frame 2 (max length 256)
TX Frame3:		HEX Frame 3 (max length 256)
TX Frame4:		HEX Frame 4 (max length 256)
TX Frame5:		HEX Frame 5 (max length 256)

SAVE CONFIG

VIEW LOG

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.6.6- External Devices → IEC102 Meter

Desde esta sección puede configurar el equipo basado en TITAN para leer un contador eléctrico con protocolo IEC 60870-5-102.

- **Enabled:** Active esta casilla si tiene quiere conectar un contador eléctrico con protocolo IEC-60870-5-102 al que el equipo basado en TITAN debe interrogar autónomamente.
- **Communication Mode:** interfaz de la comunicación (serie o IP).
- **Communication Port:** Seleccione el puerto serie del equipo basado en TITAN donde está conectado el contador eléctrico IEC-60870-5-102.
- **IP:** En caso de modo de comunicación TCP/IP, indica la dirección IP del contador eléctrico IEC-60870-5-102.
- **TCP Port:** En caso de modo de comunicación TCP/IP, indica el puerto TCP de escucha del contador eléctrico IEC-60870-5-102.
- **Period:** periodo (en minutos) en el que el contador eléctrico IEC-60870-5-102 será interrogado por el equipo basado en TITAN para leer los valores instantáneos.
- **ID Meter:** Introduzca un texto identificativo para el contador eléctrico.
- **Link Address:** dirección de enlace del contador eléctrico.
- **Meas. Address:** dirección de punto de medida del contador eléctrico.
- **Password:** contraseña del contador eléctrico.
- **Fiscal close:** Active la casilla si además de leer los valores instantáneos, el equipo basado en TITAN debe leer los cierres fiscales. De activar la casilla, cada medianoche el equipo basado en TITAN leerá y almacenará los cierres del contador.
- **Sign:** Seleccione la casilla si desea que los parámetros PAT/FPT, PAF1/FPF1, PAF2/FPF2, PAF3/FPF3 contengan un valor negativo si la energía es exportada.
- **Optical probe with echo:** Seleccione la casilla si está utilizando una sonda óptica con eco (si no selecciona esta casilla y la sonda óptica tiene eco no funcionará la lectura del contador).
- **Fiscal close days:** Indique el número de días para la realización de la lectura de los cierres fiscales. Por defecto 31 días.
- **Logger:** active esta casilla si quiere grabar en el logger interno los datos serie para enviarlos posteriormente a su plataforma Web mediante HTTP/HTTPS, FTP o MQTT/MQTTS

★ **Mobile**

- ◇ Status
- ◇ Basic Settings
- ◇ Keep Online

★ **Ethernet**

- ◇ Basic Settings
- ◇ DHCP Server

★ **Wifi**

- ◇ Basic Settings
- ◇ DHCP Server

★ **Firewall**

- ◇ NAT
- ◇ Authorized IPs
- ◇ MAC Filter
- ◇ Routes

★ **Serial Settings**

- ◇ Serial Port1-RS232
- ◇ Serial Port2-RS485
- ◇ SSL Certificates

★ **External Devices**

- ◇ Logger configuration
- ◇ ModBus Devices
- ◇ Generic Serial Device
- ◇ Temperature Sensor
- ◇ IEC102 Meter
- ◇ GPS Receiver

★ **VPN**

► **External Devices** ► **IEC102 Meter**

Enabled:	☐	Enable IEC-60870-5-102 protocol
Communication Mode:	Serial ▼	Select the communication interface
Communication Port:	Serial Port 1 ▼	Select the serial port for reading
Period:	15 minutes ▼	Reading period for instant values
ID Meter:	ID00000	Customizable label for identification
Link address:	1	Link address of meter (1...65535)
Meas. address:	1	Measurement address (1...65535)
Password:	1	Password of meter (1...4294967295)
Fiscal close:	☐	Read and send Fiscal close data once per day (Contract I)
Sign:	☐	Parameters pat/fpt, paf1/fpf1, paf2/fpf2, paf3/fpf3 negative if exported
Opt. probe with echo:	☐	Check if you are using an optical probe with echo
Fiscal close days:	31	Number of days (1 ... 31) Default 31
Logger:	☐	Logger must be used. Please, configure logger before using this option. Time Servers also have to be configured.

SAVE CONFIG

VIEW LOG

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Si necesita leer también los totales integrados (curvas de carga) necesitará hacerlo desde la sección de scripts.

Importante: lectura de la curva de carga (CCINx2).

A diferencia de los valores instantáneos (CTAVC2) y los cierres fiscales (CTAVM2), la curva de carga no se lee automáticamente por la configuración del menú. Cada lectura requiere un disparo explícito mediante el comando

AT^MTXTUNNEL=SETIEC102_CCINX2, esperar unos 20s y por último el comando AT^MTXTUNNEL=GETIEC102_CCINX2 para la lectura de los datos.

Si necesita un envío periódico continuo de curva al logger, debe disparar el SET/GET desde un sistema externo (scheduler, plataforma) o desde la sección TITAN Scripts (a modo de plantilla, ver ejemplo 52 donde se usan los cierres fiscales).

- Las tramas enviadas por el equipo basado en TITAN tienen el siguiente formato:

Ejemplo de una trama almacenada en el Logger con los valores instantáneos:

```
{
  "IMEI": "867962046823806",
  "TYPE": "IEC102",
  "TS": "2021-11-02T15:14:04Z",
  "P": "1234",
  "ID": "ID00000",
  "VABA": 0,
  "VABRI": 0,
  "VABRC": 0,
  "PAT": 0,
  "PRT": 0,
  "FPT": 1000,
  "PAF1": 0,
  "PRF1": 0,
  "FPF1": 1000,
  "PAF2": 0,
  "PRF2": 0,
  "FPF2": 1000,
  "PAF3": 0,
  "PRF3": 0,
  "FPF3": 1000,
  "IF1": 0,
  "TF1": 1337,
  "IF2": 0,
  "TF2": 1108,
  "IF3": 0,
  "TF3": 3
}
```

Donde:

IMEI:	número identificativo del equipo basado en TITAN
TYPE:	tipo de JSON. En este caso tipo IEC102
TS:	timestamp de cuando se recogieron los datos
P:	campo identificativo opcional (del Logger)
ID:	Identificador del contador
VABA:	Energía absoluta activa
VABRI:	Energía absoluta reactiva inductiva
VABRC:	Energía absoluta reactiva capacitiva
PAT:	Potencia total activa
PRT:	Potencia total reactiva
FPT:	Factor de potencia total
PAF1:	Potencia Activa Fase I
PAF1Dir	Imported (0) / Exported (1)
PRF1:	Potencia Reactiva Fase I
FPF1:	Factor de Potencia Fase I
PAF2:	Potencia Activa Fase II
PAF2Dir	Imported (0) / Exported (1)
PRF2:	Potencia Reactiva Fase II
FPF2:	Factor de Potencia Fase II
PAF3:	Potencia Activa Fase III
PAF3Dir	Imported (0) / Exported (1)
PRF3:	Potencia Reactiva Fase III
FPF3:	Factor de Potencia Fase III
IF1:	Intensidad de Fase I
TF1:	Voltaje de Fase I
IF2:	Intensidad de Fase II
TF2:	Voltaje de Fase II

IF3: Intensidad de Fase III

TF3: Voltaje de Fase III

- OpenVPN Server
- ZeroTier

Device Manager

- KARE

Other

- AT Command
- DynDns
- Private DynDns
- Sms control
- Periodic Autoreset
- Time Servers
- Remote Console
- Snmp
- Tacacs+
- Ldap
- Mqtt / Mqtts
- Http / Https
- User Permissions
- Passwords Web UI
- CA Certificates
- Email Config
- ModBus Slave
- Titan Scripts**
- Connectivity tools
- Digital I/O
- Custom Skin
- Led Config
- Syslog
- Backup / Factory
- Firmware Upgrade
- Reboot
- Logout

► External Devices ► IEC102 Meter ► Read Instant Values

TS:	TimeStamp (Titan time)
VabA:	Active absolute energy
VabRi:	Inductive Reactive Absolute Energy
VabRc:	Absolute Reactive Capacitive Energy
pat:	Total Active Power
patDir:	Imported (0) / Exported (1)
prt:	Total Reactive Power
fpt:	Total power factor
paf1:	Active Power Phase I
paf1Dir:	Imported (0) / Exported (1)
prf1:	Reactive Power Phase I
fpf1:	Power Factor Phase I
paf2:	Active Power Phase II
paf2Dir:	Imported (0) / Exported (1)
prf2:	Reactive Power Phase II
fpf2:	Power Factor Phase II
paf3:	Active Power Phase III
paf3Dir:	Imported (0) / Exported (1)
prf3:	Reactive Power Phase III
fpf3:	Power Factor Phase III
if1:	Current Phase I
tf1:	Voltage Phase I
if2:	Current Phase II
tf2:	Voltage Phase II
if3:	Current Phase III
tf3:	Voltage Phase III

REFRESH DATA

FORCE READ

(Force read will take 10 seconds)

■ Consulte la nota de aplicación **ANV6_51-Router-TITAN-Metering-IEC-60870-5-102.pdf**

Ejemplo de una trama almacenada en el Logger con los cierres fiscales:

```
{"IMEI":"869101057093607","TYPE":"IEC102_CTAVM2","TS":"09/06/2023
08:46:23","P":"1234","ID":"ID00000","CTAVM2":
[
  {"DO":20,"EaA":0,"EiA":0,"CA":2,"EaRi":0,"EiRi":0,"CRi":2,"EaRc":0,"EiRc":0,"C
Rc":2,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-
0","CMA":2,"EPA":0,"CE":128,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-
09T12:58-0"},
  {"DO":21,"EaA":0,"EiA":0,"CA":2,"EaRi":0,"EiRi":0,"CRi":2,"EaRc":0,"EiRc":0,"C
Rc":2,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-
0","CMA":2,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-
09T12:58-0"},
  {"DO":22,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"C
Rc":0,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-
0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-
09T12:58-0"},
  {"DO":23,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"C
Rc":0,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-
0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-
09T12:58-0"},
  {"DO":24,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"C
Rc":0,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-
0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-
09T12:58-0"},
  {"DO":25,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"C
Rc":0,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-
0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-
09T12:58-0"},
  {"DO":26,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"C
Rc":0,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-
0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-
09T12:58-0"}
]
}
```

Donde:

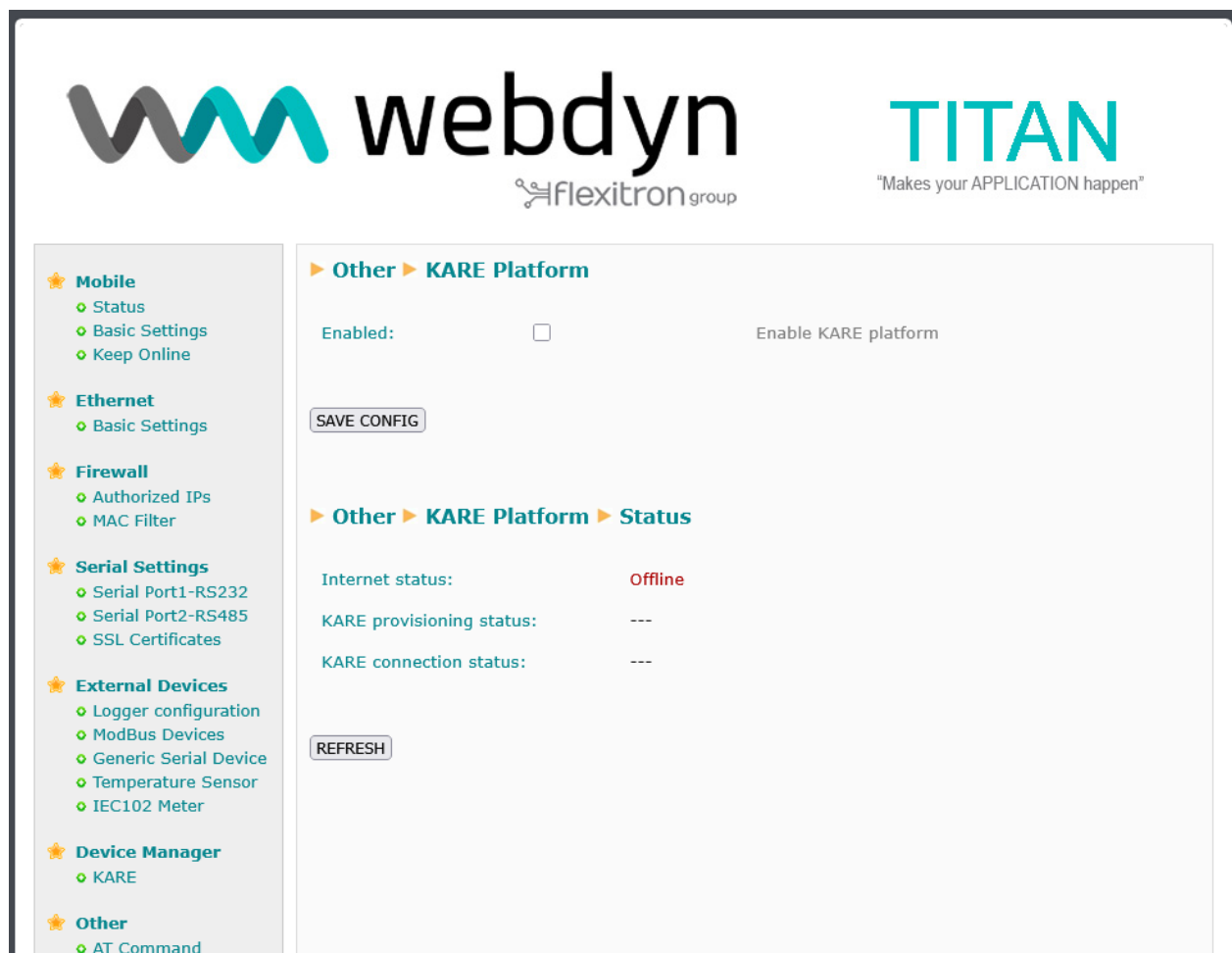
IMEI:	número identificativo del equipo basado en TITAN
TYPE:	tipo de JSON. En este caso tipo IEC102_CTAVM2
TS:	timestamp de cuando se recogieron los datos
P:	campo identificativo opcional (del Logger)
ID:	Identificador del contador

CTAVM2:	Array de datos con las lecturas obtenidas.
DO:	Dirección del objeto
EaA:	Energía absoluta Activa
EiA:	Energía incremental Activa
CA:	Cualificador de Energía Activa
EaRi:	Energía absoluta Reactiva Inductiva
EiRi:	Energía incremental Reactiva Inductiva
Cri:	Cualificador de Energía Reactiva Inductiva
EaRc:	Energía absoluta Reactiva Capacitiva
EiRc:	Energía incremental Reactiva Capacitiva
CRc:	Cualificador de Energía Reactiva Capacitiva
R7:	Registro 7 reserva
C7:	Cualificador del Registro 7 de reserva
R8:	Registro 8 reserva
C8:	Cualificador del Registro 8 de reserva
MPA:	Máximo de las Potencias
FMPA:	Fecha del Máximo
CMA:	Cualificador de Máximos
EPA:	Excesos de las Potencias
CE:	Cualificador de Excesos
DINI:	Inicio del período
DEND:	Fin del período

4.7- Device Manager → KARE

4.7.1- KARE

En esta sección se da la posibilidad de conectarse a la plataforma KARE.



- **Enabled:** habilita la comunicación con la plataforma KARE.

Tras marcar el check de “*Enabled*”, dar a “SAVE CONFIG” y reiniciar el dispositivo, el equipo iniciará un proceso de *provisioning* con KARE. Una vez que se haya hecho correctamente el *provisioning* y se esté conectado a la plataforma, veremos algo tal que así:

★ **Mobile**

- ◆ Status
- ◆ Basic Settings
- ◆ Keep Online

★ **Ethernet**

- ◆ Basic Settings
- ◆ DHCP Server

★ **Wifi**

- ◆ Basic Settings
- ◆ DHCP Server

★ **Firewall**

- ◆ NAT
- ◆ Authorized IPs
- ◆ MAC Filter
- ◆ Routes

★ **Serial Settings**

- ◆ Serial Port1-RS232

► **Other ► KARE Platform**

Enabled: ☒ Enable KARE platform

SAVE CONFIG

DETACH FROM PLATFORM

► **Other ► KARE Platform ► Status**

Internet status: **Online**

KARE provisioning status: **Done**

KARE connection status: **Connected**

REFRESH

Véase cómo para este último caso, aparece un nuevo botón llamado "DETACH FROM PLATFORM". En caso de que queramos desvincularnos y que el equipo no esté conectado a la plataforma, habrá que darle aquí y reiniciar el dispositivo.

Notas adicionales.

- La plataforma KARE es un servicio de suscripción. Para más información contactar con nuestro equipo de soporte.

4.8- Other

4.8.1- Other → AT Command

Desde esta sección es posible enviar un comando AT directamente al módem interno del equipo basado en TITAN. Por ejemplo, puede ser interesante para comprobar la cobertura, identificar las celdas de telefonía de alrededor etc.

Por otro lado, también es posible configurar hasta 5 comandos AT especiales con los que configurar el equipo en el momento de arranque.

- **AT Command:** comando AT para ejecución en tiempo real (por ejemplo, AT+CSQ). Una vez pulse el botón “SEND AT COMMAND” se ejecutará el comando AT.
- **AT1, ... AT5:** comandos AT de inicialización.

The screenshot shows the webdyn TITAN configuration interface. The header includes the webdyn logo (flexitron group) and the TITAN logo with the tagline "Makes your APPLICATION happen". A left sidebar lists various configuration categories: Mobile, Ethernet, Wifi, Firewall, Serial Settings, External Devices, VPN, Device Manager, and Other. The 'Other' category is selected, showing 'AT Command' and 'AT1, ... AT5' options. The main content area for 'AT Command' features a text input for the command, a larger text area for the response, and buttons for 'SEND AT COMMAND' and 'COPY TO CLIPBOARD'. Below this, there is a section for 'Init commands' with five input fields labeled AT1 through AT5, each with a corresponding label 'Custom initialization command 1' through '5'. A 'SAVE CONFIG' button is located at the bottom of the configuration area.

Notas adicionales.

- Si ha establecido comandos AT de inicialización pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.8.2- Other → DynDns

Los equipos basados en TITAN son compatibles con el servicio de DynDNS y de No-IP. Si no dispone de una tarjeta SIM con IP fija y le interesa usar los servicios externos de DynDNS o NO-IP puede configurarlos desde esta sección.

- **Enabled:** Active esta casilla si quiere activar el uso de DynDNS o NO-IP.
- **Mode:** modo de comunicación: HTTP o HTTPS.
- **Server:** Especifique el servidor del servicio (members.dyndns.org o dynupdate.no-ip.com).
- **Domain:** indique la dns que ha creado (por ejemplo, midominio.dyndns.org)
- **Login:** login de su cuenta en DynDNS o NO-IP
- **Password:** contraseña de su cuenta en DynDNS o NO-IP
- **Period:** periodo, en minutos, en el cual se refresca la IP actual en los servidores de DynDNS o NO-IP
- **Hide WAN IP:** si la casilla es seleccionada, la IP será detectada por el servidor de DynDNS. Obligatorio activar si se desea utilizar DynDNS utilizando como salida a Internet el puerto Ethernet o Wifi del equipo basado en TITAN.

The screenshot shows the webdyn TITAN configuration interface. The top header features the webdyn logo (a stylized 'w' with a blue wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". Below the header is a sidebar menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), and Serial Settings (Serial Port1-RS232, Serial Port2-RS485). The main content area is titled "Other → DynDns" and contains the following settings:

Field	Value	Description
Enabled:	☐	Enable DynDNS
Mode:	http	Communication mode
Server:		members.dyndns.org, dynupdate.no-ip.com, ...
Domain:		Your domain. For example myDomain.dyndns.org
Login:		Login of your account
Password:		Password of your account
Period:	60	Minutes. Public IP is sent every time it changes. But it is recommended force an update every 60 minutes.
Hide WAN IP:	☐	Public IP detected by server (mandatory if Ethernet or Wifi gateways are used)

A "SAVE CONFIG" button is located at the bottom left of the configuration area.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

- La IP se actualiza en los servidores de DynDNS o NO-IP cada vez que ésta cambia. No obstante, se recomienda el uso del parámetro de configuración “Period”, por ejemplo, a un valor de 60, para que pase lo que pase, ésta se envíe cada hora.

4.8.3- Other → Private DynDns

El servicio Private DynDNS permite el envío de la dirección IP actual del equipo basado en TITAN y de ciertos valores de estado a su propio servidor. El envío de datos puede realizarse bien mediante HTTP (HTTP/S GET, HTTP/S POST) o bien mediante el envío de una trama específica mediante socket a un puerto TCP configurable y también vía MQTT.

- **Use script:** marcar esta casilla en el caso de que se quiera usar un JSON personalizado para las DNS privadas. Dicho JSON custom se consigue utilizando *Json Transformed Script* en *Other>Titan Scripts*.

Método HTTP ó Socket TCP

- **Enabled:** Active esta casilla si quiere activar el uso de Private DNS.
- **Mode:** puede escoger entre socket TCP y HTTP/S GET, HTTP/S POST y HTTP/S PUT
- **Server:** la IP o DNS del servidor remoto
- **Server Login:** login de su servidor web (si utiliza un modo “HTTP”)
- **Password:** contraseña de su servidor web (si utiliza un modo “HTTP”)
- **TCP Port:** puerto TCP si usa el modo “socket”
- **ID:** cadena identificativa (tanto para el modo “http get” o “socket”)
- **Period:** periodo, en minutos, en el cual se refresca la IP actual en su servidor. Tenga presente que independientemente de este periodo, en el momento que cambie la IP pública, es enviada.
- **Custom header1:** Cabecera HTTP personalizada 1
- **Custom header2:** Cabecera HTTP personalizada 2
- **Custom header3:** Cabecera HTTP personalizada 3
- **IO Status:** activar si se desea enviar también el estado de la entradas y salidas digitales y contadores.

Método MQTT

- **Enabled:** Active esta casilla si quiere activar el uso de MQTT
- **Period:** periodo, en minutos, en el cual se enviará la IP actual a su servidor vía MQTT. Tenga presente que independientemente de este periodo, en el momento que cambie la IP pública, también es enviada.
- **MQTT Topic:** Tópico MQTT que se utilizará para informar con la IP
- **MQTT Broker:** permite seleccionar el bróker MQTT utilizado para publicar la información de Private DynDNS. Puede seleccionarse Primary, Secondary o Both.
- **MQTT QoS :** Calidad de servicio utilizada por MQTT para el envío de la IP
- **IO Status:** activar si se desea enviar también el estado de la entradas y salidas digitales y contadores.

★ **Mobile**

- ◆ Status
- ◆ Basic Settings
- ◆ Keep Online

★ **Ethernet**

- ◆ Basic Settings
- ◆ DHCP Server

★ **Wifi**

- ◆ Basic Settings
- ◆ DHCP Server

★ **Firewall**

- ◆ NAT
- ◆ Authorized IPs
- ◆ MAC Filter
- ◆ Routes

★ **Serial Settings**

- ◆ Serial Port1-RS232
- ◆ Serial Port2-RS485
- ◆ SSL Certificates

★ **External Devices**

- ◆ Logger configuration
- ◆ ModBus Devices
- ◆ Generic Serial Device
- ◆ Temperature Sensor
- ◆ IEC102 Meter
- ◆ GPS Receiver

★ **VPN**

- ◆ IPsec
- ◆ OpenVPN Client
- ◆ OpenVPN Server
- ◆ ZeroTier

★ **Device Manager**

- ◆ KARE

★ **Other**

- ◆ AT Command
- ◆ DynDns
- ◆ Private DynDns
- ◆ Sms control
- ◆ Periodic Autoreset
- ◆ Time Servers
- ◆ Remote Console
- ◆ Snmp
- ◆ Tacacs+
- ◆ Ldap
- ◆ Mqtt / Mqtt

► **Other ► Private DynDns**

Use script: ☐

Check for customized json using Json Transformed Script in [Script section](#).

Communication mode: WEB PLATFORM (HTTP REST)

Enabled: ☐

Enable Private DynDns

Mode:

Communication mode

Server:

IP or DNS of remote server. Example: www.myweb.com/set.asp?data=

Server Login:

User (only for "http get" mode)

Server Password:

Password (only for "http get" mode)

TCP Port:

TCP port of remote server (only "socket" mode)

ID

String for device identification

Period:

Minutes. Public IP is sent every time it changes. But it is recommended force an update every 60 minutes

Custom header1:

Optional. Custom header1. For example: Content-type:application/json

Custom header2:

Optional. Custom header2. For example: IDENTITY_KEY;YOUR_KEY

Custom header3:

Optional. Custom header3.

I/O status: ☐

Send I/O status and counters

Communication mode: MQTT

Enabled: ☐

Communication mode MQTT enabled

Period:

Minutes. Public IP is sent every time it changes. But it is recommended force an update every 60 minutes

MQTT Topic

MQTT Topic. Example: [IMEI]/dns

MQTT Broker

Broker used to publish DNS MQTT updates

MQTT QoS

MQTT QoS for DNS. Normally 0

I/O status: ☐

Send I/O status and counters

Note1: Other>MQTT menu must be configured.

Note2: Other>Digital IO must be enabled if I/O Status is used

SAVE CONFIG

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Ejemplo de formato de la trama JSON enviada:

```
{"TYPE":"DNS","IMEI":"867962046823806","IP":"88.28.221.24","P":"","CSQ":24,"MOD":"","VER":"5.2.6.02","IMSI":"214075536243578","TECH":"4g","TS":"2021-11-02T16:00:51Z","CID":"214;07;21E0;13B6D0A","RSSI":"-65","RSRP":"-91","RSRQ":"-6","IO0":0,"IO1":0,"IO2":0,"IO3":0,"IO4":0,"CO0":0,"CO1":5,"CO2":0}
```

Donde:

TYPE: tipo de trama. En este caso DNS.

IMEI: número identificativo del equipo. Único para cada equipo

P: campo ID del Logger (External Devices > Logger configuration)

IP: IP of WAN interface (2g / 3g)

CSQ: 0...31 (signal strength)

MOD: Modelo de equipo basado en TITAN

Ver: FW Version

IMSI: IMSI de la tarjeta SIM

TECH: tecnología usada (2g,3g,4g)

TS: timestamp

CID: identificación de celda de telefonía usada

RSSI: nivel de potencia de la señal.

RSRP: rsrp de 3G

RSRQ: rsrq de 3G

IOx: valor actual de la entrada / salida digital “x”

COx: valor actual del contador de pulsos asociada a la entrada digital “x”

- Por motivos de seguridad, siempre que sea posible, se recomienda encarecidamente el uso de comunicaciones SSL/TLS como es HTTPS. Las comunicaciones HTTP (sin SSL/TLS) no son seguras.

4.8.4- Other → SMS Control

Esta sección permite configurar el control del equipo por SMS. Por ejemplo, puede configurar esta sección para que el equipo se reinicie o cambie una salida digital al recibir un SMS, o especificar los números de teléfono autorizados para ello.

- **AT enabled:** active esta casilla si desea que el equipo basado en TITAN acepte comandos AT por SMS, por ejemplo, para conocer la cobertura de forma remota, para realizar un reset, cambiar una configuración, ...
- **AT header:** escriba aquí el texto cabecero de los mensajes SMS de comando. Por ejemplo, si escribe en esta casilla el texto "mtx", cuando envíe un comando AT por SMS, supongamos el comando "AT+CSQ" para conocer la cobertura del equipo, necesitaría enviar un SMS con el texto "mtx AT+CSQ"
- **All phones:** active esta casilla si desea que todos los teléfonos sean capaces de enviar comandos AT al equipo. No active esta casilla si desea especificar números de teléfono autorizados.
- **Authorized Number X:** en estas casillas podrá especificar hasta 10 números de teléfonos autorizados.
- **Alias / ATCommand:** es posible introducir hasta 10 alias para ejecutar comandos SMS. Imagine que quiere enviar un SMS para actualizar un determinado registro MODBUS de un dispositivo externo. Por ejemplo, puede configurar un ALIAS para que cuando el equipo basado en TITAN reciba el texto "**reg on**" realmente internamente se ejecute el comando AT: **at^mtxtunnel=setmodbus,1;5;16;2** escribiendo el valor 2 en el registro 5 del dispositivo con dirección Modbus 1.
- **Alias Result OK:** texto que se enviará como respuesta en el caso de que la ejecución de un comando ALIAS sea satisfactoria. Si lo desea puede devolver una respuesta personalizada para cada ALIAS indicando la respuesta entre tags: **<a1>Ok</a1><a2>Perfect</a2>...**
- **Alias Result ERROR:** texto que se enviará como respuesta en el caso de que la ejecución de un comando ALIAS sea errónea. Si lo desea puede devolver una respuesta personalizada para cada ALIAS indicando la respuesta entre tags: **<a1>Error</a1><a2>Upsss</a2>...**
- **Alias Hide AT:** marcar en caso de que se quiera ocultar el comando AT en la respuesta SMS.
- **SIM 1 Serv. Center:** actualiza el teléfono del centro de mensajería SMS a utilizar por la tarjeta SIM1 para el envío de mensajes SMS. Déje el campo en blanco si no desea modificar el número por defecto.
- **SIM 2 Serv. Center:** actualiza el teléfono del centro de mensajería SMS a utilizar por la tarjeta SIM2 (en caso de que su dispositivo cuente con DUAL-SIM) para el envío de mensajes SMS. Déje el campo en blanco si no desea modificar el número por defecto.

★ **Mobile**

- ◇ Status
- ◇ Basic Settings
- ◇ Keep Online

★ **Ethernet**

- ◇ Basic Settings
- ◇ DHCP Server

★ **Wifi**

- ◇ Basic Settings
- ◇ DHCP Server

★ **Firewall**

- ◇ NAT
- ◇ Authorized IPs
- ◇ MAC Filter
- ◇ Routes

★ **Serial Settings**

- ◇ Serial Port1-RS232
- ◇ Serial Port2-RS485
- ◇ SSL Certificates

★ **External Devices**

- ◇ Logger configuration
- ◇ ModBus Devices
- ◇ Generic Serial Device
- ◇ Temperature Sensor
- ◇ IEC102 Meter
- ◇ GPS Receiver

★ **VPN**

- ◇ IPsec
- ◇ OpenVPN Client
- ◇ OpenVPN Server
- ◇ ZeroTier

★ **Device Manager**

- ◇ KARE

★ **Other**

- ◇ AT Command
- ◇ DynDns
- ◇ Private DynDns
- ◇ Sms control
- ◇ Periodic Autoreset
- ◇ Time Servers
- ◇ Remote Console
- ◇ Snmp
- ◇ Tacacs+
- ◇ Ldap
- ◇ Mqtt / Mqtts
- ◇ Http / Https
- ◇ User Permissions
- ◇ Passwords Web UI
- ◇ CA Certificates
- ◇ Email Config
- ◇ ModBus Slave
- ◇ **Titan Scripts**
- ◇ Connectivity tools
- ◇ Digital I/O
- ◇ Custom Skin
- ◇ Led Config
- ◇ Syslog
- ◇ Backup / Factory
- ◇ Firmware Upgrade
- ◇ Reboot

► **Other ► SMS control**

SMS function

AT : ☐ enabled

Send AT Commands by SMS allowed (you can reboot the device, get IP Wan, get GSM RSSI, change configuration, ...)

AT header:

Header of at commands

Authorized phone numbers:

☐ all phones

All Phones are allowed.

Note: This option is not recommended for security reasons. Only authorized numbers should be allowed

Authorized number 1

Authorized number 2

Authorized number 3

Authorized number 4

Authorized number 5

Authorized number 6

Authorized number 7

Authorized number 8

Authorized number 9

Authorized number 10

ALIAS

AT COMMAND

Alias 1:

Alias 2:

Alias 3:

Alias 4:

Alias 5:

Alias 6:

Alias 7:

Alias 8:

Alias 9:

Alias 10:

Alias Result OK:

Returned message for OK

Alias Result ERROR:

Returned message for ERROR

Alias Hide AT:

☒

Check in you want to hide the AT command in the SMS response.

SIM 1 Serv. Center:

Optional. SMS SIM 1 Server Center Address. Example: +34609090909

SIM 2 Serv. Center:

Optional. SMS SIM 2 Server Center Address. Example: +34609090909

SAVE CONFIG

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Consulte la nota de aplicación ANV6_3 para una mayor información a través de ejemplos. Comprobará también cómo añadir parámetros a los ALIAS

4.8.6- Other → Periodic autoreset

Desde esta sección se puede configurar un autoreset programado del equipo basado en TITAN.

- **Autoreset not enabled:** active la opción si no desea que el equipo basado en TITAN se resetee de forma automática.
- **Autoreset every X hours:** active la opción si desea que el equipo basado en TITAN se autoresetee cada cierto número de horas.
 - **Number of hour:** en caso de escoger un autoreset cada X horas, en esta casilla debe especificar dicha X, esto es, el número de horas tras el que se efectúa el reset. Especificar 24 para un reset diario.
- **Autoreset at specific hour:** seleccione esta opción si desea que el equipo basado en TITAN se autoresetee a una determinada hora del día
 - **Hour for autoreset:** hora específica para el autoreseteo diario.
- **Reset if router can't obtain Mobile IP after X minutes:** opción muy recomendable para situaciones de pérdida de contexto. Por ejemplo, permite especificar en "Time for reset" los minutos tras los que el equipo basado en TITAN debe autoresetearse en caso de no poder obtener una dirección IP.

The screenshot displays the webdyn TITAN configuration interface. The top header features the webdyn logo (a stylized 'w' with a blue and grey wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". A left sidebar contains a navigation menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), and External Devices (Logger configuration, ModBus Devices, Generic Serial Device). The main content area is titled "Other > Periodic Autoreset" and contains three radio button options: "Autoreset not enabled" (selected), "Autoreset every X hours" (with a "Number of hour" input field set to 12 and a note "Every X hours device will be rebooted"), and "Autoreset at specific hour" (with an "Hour for autoreset" input field set to 0 and a range "0 ... 23"). Below these is an unchecked checkbox for "Reset if router can't obtain Mobile IP after X minutes" with a "Time for reset" input field set to 60 and a range "5 ... 60 min.". A "SAVE CONFIG" button is located at the bottom left of the main area.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.8.7- Other → Time Servers (NTP)

El equipo basado en TITAN dispone en su interior de un reloj en tiempo real el cual le permite mantener la hora incluso tras la pérdida de alimentación durante unas horas. Periódicamente dicho reloj interno necesita ser sincronizado con servidores de tiempo mediante protocolo NTP.

The screenshot displays the webdyn TITAN configuration interface. The top header features the webdyn logo (a stylized 'w' with a blue and grey wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". A left sidebar contains a menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor, IEC102 Meter, GPS Receiver), and VPN. The main content area is titled "Other → Time Servers (NTP)". It contains two sections. The first section, "Time Servers (NTP)", has a "Enabled" checkbox checked, followed by fields for "NTP Server 1" (time1.google.com), "NTP Server 1 port" (123), "NTP Server 2" (time2.google.com), "NTP Server 2 port" (123), and a "Time zone" dropdown set to "UTC". A "Current Time" field shows "30-06-2026 11:11:21". A "SAVE CONFIG" button is at the bottom. The second section, "Local Time Server", has an "Enabled" checkbox unchecked, an "NTP Server port" field set to "123", and a "SAVE CONFIG" button at the bottom.

Time Servers (NTP)

- **Enabled:** active esta casilla si quiere usar servidores de tiempo NTP.
- **NTP Server 1:** dirección IP o DNS del servidor NTP de hora 1
- **NTP Server 1 port:** puerto del servidor NTP de hora 1
- **NTP Server 2:** dirección IP o DNS del servidor NTP de hora 2
- **NTP Server 2 port:** puerto del servidor NTP de hora 2
- **Time Zone:** permite especificar la zona horaria.

Time Servers (NTP) → Local Time Server.

También es posible configurar el Titan como un servidor de tiempo NTP. Para ello basta con activar la casilla enabled y seleccionar el puerto UDP deseado (por defecto 123). Resulta útil por ejemplo para dotar de hora a dispositivos incluso sin necesidad de usar una tarjeta SIM (siempre y cuando sea un modelo Titan con GPS).

- **Enabled:** active esta casilla si quiere usar el router Titan como un servidor de tiempo NTP
- **NTP Server port:** puerto del servidor NTP del router Titan

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.8.8- Other → Remote console (TCP Server)

Si en alguna ocasión necesita realizar alguna operación especial sobre el equipo basado en TITAN mediante una conexión tipo “Telnet” o “SSH”, puede hacerlo configurando esta sección. Es decir, mediante esta conexión especial es posible también el envío de comandos AT al equipo basado en TITAN a través de una conexión tipo TELNET o SSH. Con ello podrá hacer un cambio de configuración del equipo, conmutar una salida digital, etc. Consulte la sección 5 de este manual para obtener la lista de comandos AT disponibles.

- **Enabled:** active esta casilla si quiere usar esta conexión especial.
- **TCP Port:** puerto TCP de escucha del equipo, donde deberá realizar la conexión.
- **Username:** nombre de usuario que se solicitará tras realizar la conexión.
- **Password:** Password de usuario que se solicitará tras introducir el nombre de usuario
- **SSH:** Active la casilla si quiere utilizar SSH en lugar de Telnet.
- **Disable local authentication:** marcar en caso de que no se quieran conexiones locales.
- **Remote service:** servicios de autenticación remotos: None, TACACS+ y LDAP.

The screenshot displays the webdyn TITAN configuration interface. The top header features the webdyn logo and the TITAN logo with the tagline "Makes your APPLICATION happen". A left sidebar contains a navigation menu with categories: Mobile, Ethernet, Wifi, Firewall, Serial Settings, and External Devices. The main content area is titled "Other → Remote Console" and contains the following settings:

- Enabled:** A checkbox that is currently unchecked. To its right is the text "Enable remote console".
- TCP port:** A text input field containing "20023". To its right is the text "TCP port for remote console. 22 is not allowed."
- Username:** A text input field. To its right is the text "Username of your local account".
- Password:** A text input field. To its right is the text "Password of your local account" and a note: "Note: Min. 17 characters. Must include uppercase, lowercase, and numbers."
- SSH:** A checkbox that is currently unchecked. To its right is the text "Enable SSH security".

Below these settings is a "SAVE CONFIG" button. Further down, there is a sub-section titled "Other → Remote Console → Authentication Methods" with the following settings:

- Disable local authentication:** A checkbox that is currently unchecked. To its right is the text "Check if you don't want local connections."
- Remote service:** A dropdown menu currently set to "None". To its right is the text "Remote authentication service".

At the bottom of this section is another "SAVE CONFIG" button.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios. **Si activa / desactiva la casilla SSH, asegúrese de reintroducir también el password.**
- El acceso a la consola remota la podrá realizar tanto a nivel local (Ethernet o Wifi) como de forma remota a través de la conexión 4G/3G/2G.
- Por motivos de seguridad, se recomienda no utilizar la consola remota sin activar la opción de SSH. En caso de no ser posible, se recomienda utilizar el servicio a través de una conexión VPN.

4.8.9- Other → SNMP

Los equipos basados en TITAN cuentan con protocolo SNMP. Mediante SNMP podrá realizar operaciones SET y GET desde aplicativos SNMP estándar

- **Enabled:** Seleccionar si se quiere habilitar el servicio SNMP del equipo basado en TITAN
- **SNMP Version:** Puede seleccionarse entre SNMPv2c y SNMP v3.

ADVERTENCIA: SNMP v2c se considera inseguro según la “European Cybersecurity Certification Group”, pero se mantiene por compatibilidad. **Se recomienda usar SNMP v3.**

- **UDP port:** El puerto UDP estándar para SNMP es el 161, pero puede especificar uno personalizado.
- **Custom OID:** Permite cambiar el Enterprise-Product OID del valor por defecto (.45711.1.1) por si quiere ajustarlo a sus valores corporativos.
- **Community:** El Password para poder ejecutar comandos SET y GET. Únicamente necesario para SNMPv2
- **Username:** Username en el caso de utilizar SNMPv3 (no necesario para SNMPv2)
- **Auth Password:** Password de autenticación para SNMPv3 (no necesario para SNMPv2)
- **Priv Password:** Password de privacidad para SNMPv3 (no necesario para SNMPv2)
- **Auth Protocol:** Protocolo para autenticación (MD5 o SHA)
- **Priv Protocol:** Protocolo de encriptación (DES, AES128)
- **Engine ID:** para SNMPv3 (AUTO o HEX custom)
- **Traps – Enabled:** Habilita los traps del equipo basado en TITAN
- **Traps – UDP Port:** Permite especificar el puerto para los TRAPS SNMP.
- **Traps – IP 1: dirección IP principal para el envío de TRAPS SNMP.**
- **Traps – IP 2: segunda dirección IP opcional para el envío de TRAPS SNMP.**
- **Traps – IP 3: tercera dirección IP opcional para el envío de TRAPS SNMP.**

NOTA: Los TRAPS SNMP se enviarán a todas las direcciones IP configuradas. Si sólo desea enviar traps a un destino, complete únicamente el campo “Traps – IP 1”.

- **Traps – Community:** Campo community para el envío de TRAPS (sólo para SNMPv2c)
- **Alarm OS:** Habilita los traps de alarma del sistema operativo del equipo ante un fallo crítico.
- **Number traps alarm ON:** Indica el número de traps que enviará cuando un trap de alarma se activa.
- **Number traps alarm OFF:** Indica el número de traps que enviará cuando un trap de alarma se desactiva.
- **Trap period:** Indica el periodo, en segundos, entre envío de traps de alarma.

★ Mobile

- ◇ Status
- ◇ Basic Settings
- ◇ Keep Online

★ Ethernet

- ◇ Basic Settings
- ◇ DHCP Server

★ Wifi

- ◇ Basic Settings
- ◇ DHCP Server

★ Firewall

- ◇ NAT
- ◇ Authorized IPs
- ◇ MAC Filter
- ◇ Routes

★ Serial Settings

- ◇ Serial Port1-RS232
- ◇ Serial Port2-RS485
- ◇ SSL Certificates

★ External Devices

- ◇ Logger configuration
- ◇ ModBus Devices
- ◇ Generic Serial Device
- ◇ Temperature Sensor
- ◇ IEC102 Meter
- ◇ GPS Receiver

★ VPN

- ◇ IPsec
- ◇ OpenVPN Client
- ◇ OpenVPN Server
- ◇ ZeroTier

★ Device Manager

- ◇ KARE

★ Other

- ◇ AT Command
- ◇ DynDns
- ◇ Private DynDns
- ◇ Sms control
- ◇ Periodic Autoreset
- ◇ Time Servers
- ◇ Remote Console

► Other ► SNMP

Enabled:	☐	Enable SNMP v2c
SNMP Version:	SNMPv2c	SNMPv2 or SNMPv3
UDP Port:	161	Default UDP port 161
Custom OID:	.45711.1.1	Enterprise-Product OID. Default: .45711.1.1
Community:	public	Only SNMPv2. Password for GET and SET commands
Username:		Only SNMPv3.
Auth Password:		Only SNMPv3 Note: Min. 17 characters. Must include uppercase, lowercase, and numbers.
Priv. Password:		Only SNMPv3 Note: Min. 17 characters. Must include uppercase, lowercase, and numbers.
Auth Protocol:	MD5	Only SNMPv3.
Priv Protocol:	DES	Only SNMPv3.
Engine ID:	AUTO	Only SNMPv3. "AUTO" or custom HEX
Traps Enabled:	☒	Enable Traps
Traps - UDP Port:	162	Default UDP port 162
Traps - IP 1:	192.168.1.61	Primary IP for sending traps
Traps - IP 2:	192.168.1.62	Optional IP for sending traps
Traps - IP 3:	192.168.1.63	Optional IP for sending traps
Traps - Community:	public	Only SNMPv2. Community for traps
Alarm OS:	☐	Enable trap for Oper. System alarm
Number traps alarm ON:	10	Number the traps sent when an alarm is activated. 0 ... 1440
Number traps alarm OFF:	5	Number the traps sent when an alarm is deactivated. 0 ... 1440
Trap period:	60	Period between traps (10...3600 sec)

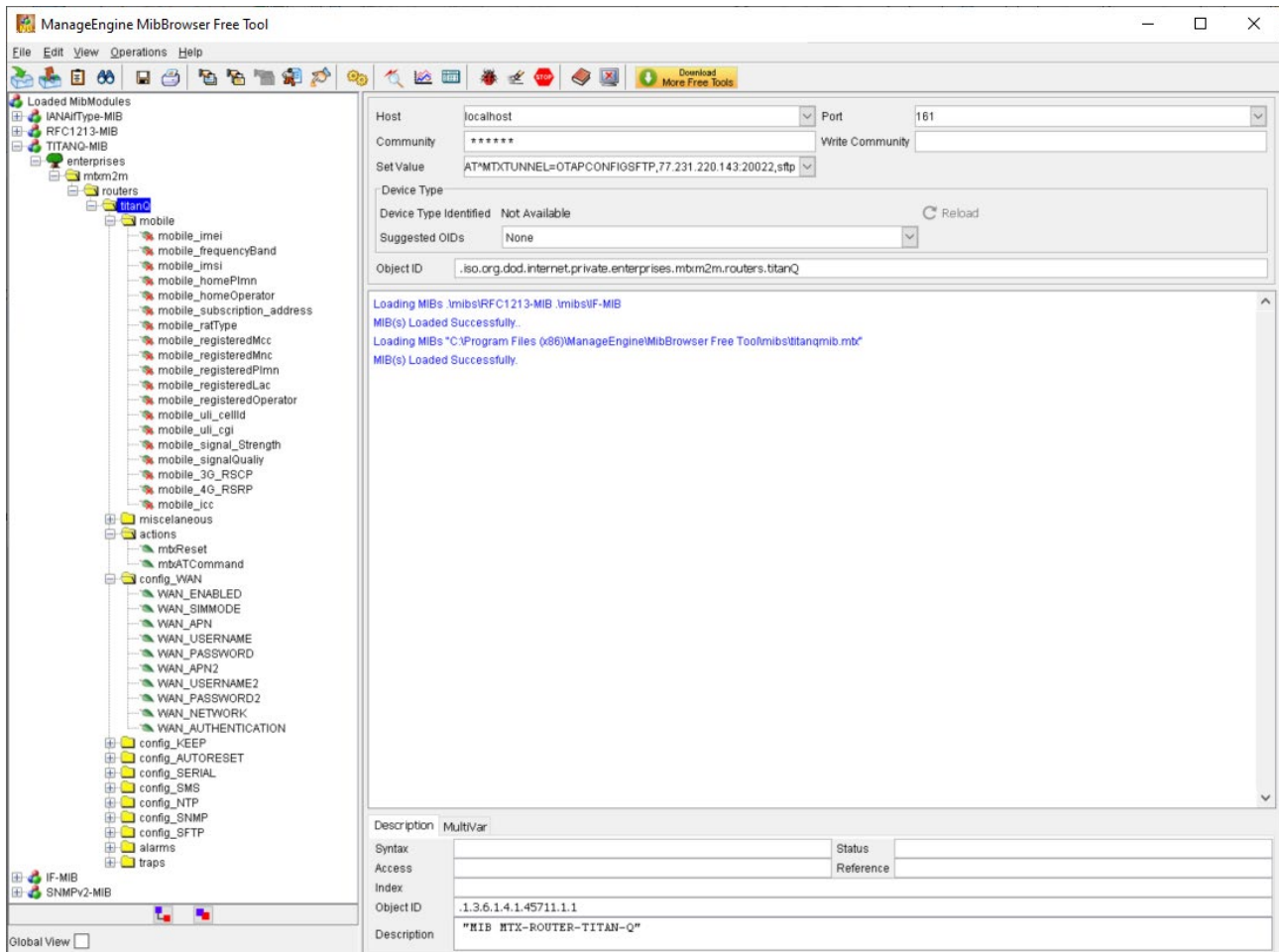
[Click here for download MIB](#)

SAVE CONFIG

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- En la pantalla anterior existe un link con el texto "Click here for download MIB". Descargue el fichero para obtener el MIB con los OID.

- Mediante SNMP podrá monitorizar el equipo, por ejemplo, interrogando al equipo para obtener la RSSI (cobertura), la fecha y hora, el tiempo de funcionamiento, si está trabajando en modo 4G/3G/2G, o el operador utilizado.
- Una opción muy interesante es la sección “Action”. En ella verá que podrá hacer 2 cosas. Una de ellas es resetear el equipo remotamente. La otra es que puede ejecutar un comando AT remotamente mediante SNMP (escribiendo en el registro ejecutará el comando AT y leyéndolo obtendrá la respuesta). Mediante el envío de comandos AT podrá realizar cualquier cosa a través de SNMP, desde leer un equipo Modbus conectado al equipo, cambiar parámetros de configuración, leer una posición GPS, leer una entrada digital, cambiar el estado de una salida digital ...



- Por motivos de seguridad, no se recomienda el uso de los protocolos MD5 y DES al considerarse inseguros en la actualidad. Utilice en su lugar protocolos como SHA y AES.

4.8.10- Other >> TACACS+

Los equipos basados en TITAN cuentan con la opción de autenticación por Tacacs+. Esta característica permitirá la autenticación externa para los servicios HTTP, Telnet y SSH del equipo basado en TITAN. Para utilizar esta característica es preciso configurar esta sección.

- **Server:** Dirección IP ó DNS del servidor Tacacs+
- **KEY:** Password de encriptación.



The screenshot shows the webdyn TITAN configuration interface. At the top, there is a logo for 'webdyn flexitron group' and 'TITAN' with the tagline 'Makes your APPLICATION happen'. On the left, there is a sidebar with navigation options: 'Mobile' (Status, Basic Settings, Keep Online) and 'Ethernet' (Basic Settings, DHCP Server). The main content area is titled 'Other >> TACACS+'. It contains two input fields: 'Server:' and 'KEY:'. To the right of the 'Server:' field is the text 'Remote server IP or DNS'. To the right of the 'KEY:' field is the text 'Key for Tacacs+'. At the bottom left of the main content area is a button labeled 'SAVE CONFIG'.

Notas adicionales.

- El servicio TACACS+ en los routers Titan utiliza autenticación y autorización.
- Para la autorización el router Titan buscará los servicios "webdyn_http_admin", "webdyn_http_user", "webdyn_http_guest", "webdyn_telnet_admin", "webdyn_ssh_admin"
- Consulte la nota de aplicación **ANV6_74** donde se explica en detalle con un ejemplo como configurar el router Titan y su servicios TACACS+.
- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.8.11- Other >> LDAP

Los equipos basados en TITAN cuentan con la opción de autenticación por LDAP. Esta característica permitirá la autenticación externa para los servicios HTTP, Telnet y SSH del equipo basado en TITAN. Para utilizar esta característica es preciso configurar esta sección.

- **Server:** Dirección IP ó DNS del servidor LDAP
- **TCP Port:** Puerto TCP del servidor LDAP
- **SSL/TLS** Marque esta casilla si su servidor LDAP utiliza SSL/TLS
- **Search base** DN base para la búsqueda de usuarios en el servidor LDAP
- **Authorization base** DN base para comprobar la autorización en el servidor LDAP

The screenshot shows the webdyn TITAN configuration interface. The top header features the webdyn logo (a stylized 'w' with a blue and grey wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". Below the header, there is a left sidebar with navigation options: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), and Firewall. The main content area is titled "Other >> LDAP" and contains the following configuration fields:

Field	Value	Label/Example
Server:	[Empty text box]	IP or DNS
TCP Port:	389	0 ... 65535
SSL/TLS:	☐	Enable LDAPS
Search base:	[Empty text box]	Example: OU=users,DC=webdyn,DC=com
Authorization base:	[Empty text box]	Example: OU=roles,DC=webdyn,DC=com

At the bottom of the configuration area is a "SAVE CONFIG" button.

Notas adicionales.

- El servicio LDAP en los routers Titan utiliza autenticación y autorización.
- Para la autorización el router Titan buscará un CN "webdyn_http_admin", "webdyn_http_user", "webdyn_http_guest", "webdyn_telnet_admin", "webdyn_ssh_admin" en un atributo "memberOf"
- Consulte la nota de aplicación **ANV6_75** donde se explica en detalle con un ejemplo como configurar el router Titan y su servicios LDAP
- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Se recomienda encarecidamente la activación de la opción SSL/TLS (LDAPS) por motivos de seguridad. LDAP sin la activación SSL/TLS no es seguro.

4.8.12- Other → MQTT

MQTT Broker

Los equipos basados en TITAN pueden trabajar como broker MQTT.

The screenshot shows the webdyn TITAN configuration interface. At the top, there are logos for webdyn (flexitron group) and TITAN ("Makes your APPLICATION happen"). On the left, a sidebar lists navigation options: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), and Wifi (Basic Settings, DHCP Server). The main content area is titled "Other ▶ MQTT Broker" and contains the following configuration fields:

Field	Value / Description
Enabled:	☐ Enable MQTT broker service. Note: This broker does not support MQTTS. Use it only locally or through a VPN.
TCP Port:	1883 Listening port (for example 1883)
Anonymous User:	☐ Allow anonymous user (no user / password is needed)
User:	Username (used if anonymous is not selected)
Password:	Password (used if anonymous is not selected)

- **Enabled:** seleccionar si se quiere habilitar el servicio broker MQTT.
- **TCP Port:** puerto TCP de escucha.
- **Anonymous User:** marcar en caso de que se quiera permitir usuarios anónimos (si se marca, los campos de "User" y "Password" no son necesarios).

MQTT Client

Los equipos basados en TITAN pueden trabajar como cliente MQTT conectándose contra un bróker MQTT / MQTT. Configurar el equipo basado en TITAN como cliente MQTT permite enviar los datos recogidos en el datalogger interno (datos de sensores, equipos Modbus, ...) vía MQTT. Debe configurar apropiadamente esta sección si selecciona el envío por MQTT en la sección LOGGER.

Importante: A partir de esta versión (v7.02) el equipo basado en TITAN puede mantener hasta dos conexiones MQTT cliente independientes: Primary MQTT Client y Secondary MQTT Client. La configuración del cliente Primary mantiene la compatibilidad con versiones anteriores. El cliente Secondary permite configurar un segundo bróker MQTT con sus propios parámetros de conexión, topics AT, topics de respuesta, topics de script, QoS, KeepAlive y persistencia.

En las secciones que utilizan MQTT podrá seleccionarse el destino del envío mediante los valores Primary, Secondary o Both. La opción Primary usa el cliente MQTT principal, Secondary usa el cliente MQTT secundario y Both envía la información a ambos brókers cuando estén configurados.

Parámetros de configuración:

- **Enabled:** Seleccionar si se quiere habilitar el servicio MQTT Cliente
- **Broker:** dirección URL del bróker MQTT destino.
- **Username:** Username MQTT. En blanco si no se usa.
- **Password:** Password MQTT. En blanco si no se usa
- **ID:** Campo de identificación de dispositivo
- **QoS:** Calidad de servicio (0,1,2)
- **KeepAlive:** Segundos para keepalive (recomendable 300)
- **Persistence:** Seleccionar si se quiere que los datos sean persistentes
- **AT Topic:** Tópico 1 al que se subscribirá el equipo basado en TITAN. Los comandos AT que envíe a este tópico se ejecutarán en el equipo.
- **AT Resp Topic:** Las respuestas a comandos AT recibidos por MQTT por el equipo basado en TITAN en el tópico "AT Topic" serán enviadas a este Topic vía MQTT.
- **AT Topic 2:** Tópico 2 al que se subscribirá el equipo basado en TITAN. Los comandos AT que envíe a este tópico se ejecutarán en el equipo.
- **AT Resp Topic 2:** Las respuestas a comandos AT recibidos por MQTT por el equipo basado en TITAN en el tópico "AT Topic 2" serán enviadas a este Topic vía MQTT
- **AT Topic 3:** Tópico 3 al que se subscribirá el equipo basado en TITAN. Los comandos AT que envíe a este tópico se ejecutarán en el equipo.
- **AT Resp Topic 3:** Las respuestas a comandos AT recibidos por MQTT por el equipo basado en TITAN en el tópico "AT Topic 3" serán enviadas a este Topic vía MQTT
- **MQTT Script Topic 1:** Topic MQTT en el que al recibir datos se ejecutará un script personalizable. Consulte la sección de scripts de este manual y las notas de aplicación para más información.
- **MQTT Script Topic 2:** Topic MQTT en el que al recibir datos se ejecutará un script personalizable. Consulte la sección de scripts de este manual y las notas de aplicación para más información.

- ★ **Firewall**
 - ◊ NAT
 - ◊ Authorized IPs
 - ◊ MAC Filter
 - ◊ Routes
- ★ **Serial Settings**
 - ◊ Serial Port1-RS232
 - ◊ Serial Port2-RS485
 - ◊ SSL Certificates
- ★ **External Devices**
 - ◊ Logger configuration
 - ◊ ModBus Devices
 - ◊ Generic Serial Device
 - ◊ Temperature Sensor
 - ◊ IEC102 Meter
 - ◊ GPS Receiver
- ★ **VPN**
 - ◊ IPSec
 - ◊ OpenVPN Client
 - ◊ OpenVPN Server
 - ◊ ZeroTier
- ★ **Device Manager**
 - ◊ KARE
- ★ **Other**
 - ◊ AT Command
 - ◊ DynDns
 - ◊ Private DynDns
 - ◊ Sms control
 - ◊ Periodic Autoreset
 - ◊ Time Servers
 - ◊ Remote Console
 - ◊ Snmp
 - ◊ Tacacs+
 - ◊ Ldap
 - ◊ Mqtt / Mqtts
 - ◊ Http / Https
 - ◊ User Permissions
 - ◊ Passwords Web UI
 - ◊ CA Certificates
 - ◊ Email Config
 - ◊ ModBus Slave
 - ◊ **Titan Scripts**
 - ◊ Connectivity tools
 - ◊ Digital I/O
 - ◊ Custom Skin
 - ◊ Led Config
 - ◊ Syslog
 - ◊ Backup / Factory
 - ◊ Firmware Upgrade
 - ◊ Reboot
 - ◊ Logout

► Other ► MQTT Client

Primary MQTT Client

Enabled:	☒	Enable MQTT / MQTTS client
		Destination MQTT/MQTTS Broker. Examples: tcp://test.mosquitto.org:1883 ssl://test.mosquitto.org:8883 (certificate needed) ssl://test.mosquitto.org:8884 (certificates needed)
MQTT Broker	tcp://broker.emqx.io:1883	
MQTT Username		MQTT Username (blank if not used)
MQTT Password		MQTT Password (blank if not used)
MQTT ID	pepinoTitan1	Device identification
MQTT Qos	0	MQTT Quality Of Service (0 ... 2)
MQTT Keepalive	60	Seconds for keepalive (30 ... 3600)
MQTT Persistence	☐	Data persistence
MQTT AT Topic	ATP1	This topic will be subscribed for receiving AT Commands (usefull for individual device)
MQTT AT Resp Topic	ATRP1	This topic will be used for publishing the AT Command Responses of AT Topic
MQTT AT Topic 2		This topic will be subscribed for receiving AT Commands (usefull for groups)
MQTT AT Resp Topic 2		This topic will be used for publishing the AT Command Responses of AT Topic 2
MQTT AT Topic 3		This topic will be subscribed for receiving AT Commands (usefull for all devices)
MQTT AT Resp Topic 3		This topic will be used for publishing the AT Command Responses of AT Topic 3
MQTT Script Topic 1		When data is received in this topic the 'Topic Script' will be executed.
MQTT Script Topic 2		When data is received in this topic the 'Topic Script' will be executed.

Secondary MQTT Client

Enabled:	☒	Enable Secondary MQTT / MQTTS client
		Destination MQTT/MQTTS Broker. Examples: tcp://test.mosquitto.org:1883 ssl://test.mosquitto.org:8883 (certificate needed) ssl://test.mosquitto.org:8884 (certificates needed)
MQTT Broker	tcp://broker.emqx.io:1883	
MQTT Username		MQTT Username (blank if not used)
MQTT Password		MQTT Password (blank if not used)
MQTT ID	pepinoTitan2	Device identification
MQTT Qos	0	MQTT Quality Of Service (0 ... 2)
MQTT Keepalive	60	Seconds for keepalive (30 ... 3600)
MQTT Persistence	☐	Data persistence
MQTT AT Topic	ATP2	This topic will be subscribed for receiving AT Commands (usefull for individual device)
MQTT AT Resp Topic	ATRP2	This topic will be used for publishing the AT Command Responses of AT Topic
MQTT AT Topic 2		This topic will be subscribed for receiving AT Commands (usefull for groups)
MQTT AT Resp Topic 2		This topic will be used for publishing the AT Command Responses of AT Topic 2
MQTT AT Topic 3		This topic will be subscribed for receiving AT Commands (usefull for all devices)
MQTT AT Resp Topic 3		This topic will be used for publishing the AT Command Responses of AT Topic 3
MQTT Script Topic 1		When data is received in this topic the 'Topic Script' will be executed.
MQTT Script Topic 2		When data is received in this topic the 'Topic Script' will be executed.

SAVE CONFIG

Status and certificates

En la sección de estado se muestra de forma independiente el estado de la conexión a Internet, el estado de conexión del Primary MQTT Client y del Secondary MQTT Client.

En caso de utilizar MQTTS con autenticación de cliente, los certificados `.crt` y `.key` pueden cargarse de forma independiente para el bróker Primary o para el bróker Secondary. La configuración de certificados del bróker Primary mantiene compatibilidad con configuraciones anteriores.

The screenshot shows a web interface with two main sections. The first section, titled 'Other > MQTT Client > Status', displays the following status information: 'Internet status: Online', 'Primary MQTT status: Connected', and 'Secondary MQTT status: Connected'. A 'REFRESH' button is located below this information. The second section, titled 'Other > MQTT Client > Certificates for MQTTS', contains instructions for configuring CA certificates. It includes a dropdown menu for 'Client certificate:' with 'Primary' selected, and a file selection area for 'file 'mqttts-client.crt''. Below this, it shows 'Primary: not uploaded' and 'Secondary: not uploaded'. A similar setup is shown for the 'Client KEY:' with 'file 'mqttts-client.key'' and 'Primary: not uploaded' and 'Secondary: not uploaded'. At the bottom, there is a dropdown menu for 'Primary' and a 'DELETE CERTIFICATES' button.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Nótese que es posible escribir el texto [IMEI] en lugar del número del IMEI. Es decir, si el IMEI es 012345678912345, sería lo mismo usar el TOPIC /0123456789012345/TEST que el topic /[IMEI]/TEST
- Recuerde que si utiliza MQTTS es posible que tenga que incluir el certificado CA usado por el broker MQTT en la sección “Other → CA Certificates”.
- En versiones anteriores de firmware TITAN la respuesta a los comandos AT en cualquier topic se enviaban a un único tópico. Si desea el mismo comportamiento puede configurar el mismo valor en los topics “AT Resp Topic”, “AT Resp Topic 2”, “AT Resp Topic 3”
- Por motivos de seguridad, se recomienda siempre el uso de un broker MQTT con comunicaciones SSL/TLS, es decir, cuya cabecera de conexión comienza con “ssl:// ...”

4.8.13- Other → HTTP / HTTPS

Configuración de HTTP y activación de HTTPS para el entorno de configuración.

- **HTTP Port:** indica el puerto TCP de configuración remota por HTTP. Por ejemplo, si especifica el 8080, la URL de configuración será <http://x.x.x.x:8080> . Por defecto el puerto estándar es 80, pero si desea hacer NAT hacia el puerto TCP80 de un dispositivo ETH interno (cámara IP, PLC) necesitará cambiarlo, por ejemplo, al 8080. El servicio HTTP no es usable de forma remota si HTTPS está habilitado.
- **HTTPS Enabled.** Activa el servicio HTTPS (los certificados se generan automáticamente tras el reinicio).
- **HTTP Port:** indica el puerto TCP de configuración por HTTPS. Por defecto 443.
- **HTTPS Key and Cert:** Es posible utilizar su propio certificado para el servidor HTTPS del equipo basado en TITAN. En este campo es posible introducir en formato PEM el CERTIFICADO y el KEY en un mismo archivo (formato PEM)

The screenshot shows the webdyn TITAN configuration interface. The top header includes the webdyn logo (a stylized 'w' with a blue wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". A left sidebar contains a menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), and External Devices. The main content area is titled "Other > Http/Https" and contains the following settings:

- HTTP port:** A text input field with the value "80". To its right, a note states: "HTTP port for **remote** WAN connections. Not used if HTTPS is enabled."
- HTTPS enabled:** A checkbox that is currently unchecked. To its right, a note states: "Enable HTTPS Web Server. First certificate is generated automatically"
- HTTPS port:** A text input field with the value "443". To its right, a note states: "HTTPS port for **remote** WAN connections"
- A "SAVE CONFIG" button.
- An **Important:** message in red text: "The **HTTP** is not a secure protocol. It is strongly recommended to enable **HTTPS** protocol to protect your connection."
- A section for "Custom KEY and Certificate for HTTPS WebServer (PEM format)" containing:
 - A label "HTTPS Key and Certificate file 'https.pem'" followed by a file selection interface with a button "Examinar...", a text field containing "No se ha seleccionado ningún archivo.", and an "Upload" button.
 - A status indicator "not uploaded" in red text.

Notas adicionales.

- **IMPORTANTE:** el protocolo HTTP es inseguro. Se recomienda encarecidamente habilitar el protocolo HTTPS para proteger la conexión. Tras configurar la contraseña inicial de administración, el equipo muestra un aviso de seguridad recomendando activar HTTPS. HTTP no cifra la comunicación con el equipo, por lo que se recomienda utilizar HTTPS siempre que sea posible.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Cuando intente conectarse al equipo basado en TITAN vía HTTPS su navegador probablemente le mostrará un mensaje de advertencia en relación al certificado digital auto firmado. Es completamente normal.

4.8.14- Other → User Permissions.

Desde esta sección puede configurar los permisos a los que tendrá acceso el usuario “user” y “guest”. Las opciones de configuración que no seleccione no aparecerán en el menú de la izquierda del entorno de configuración cuando se loguee dentro del equipo con el usuario “user” o “guest”.

The screenshot shows the webdyn TITAN configuration interface. The left sidebar contains a list of configuration categories, each with a star icon and a list of sub-items. The main area displays the 'User Permissions' section, which is currently expanded. It shows a list of permissions for 'User' and 'Guest' with checkboxes to enable or disable them. A 'SAVE CONFIG' button is located at the bottom of the main area.

Category	Sub-category	Permission	User	Guest
Mobile	Basic Settings	Basic Settings	☐	☐
		Keep Online	☐	☐
Ethernet	Basic Settings	Basic Settings	☐	☐
		DHCP Server	☐	☐
WiFi	Basic Settings	Basic Settings	☐	☐
		DHCP Server	☐	☐
Firewall	NAT	NAT	☐	☐
		Authorized IPs	☐	☐
Serial Settings	Serial Port 1	Serial Port 1	☐	☐
		Serial Port 2	☐	☐
External devices	Logger config.	Logger config.	☐	☐
		Modbus devices	☐	☐
VPN	IPSec	IPSec	☐	☐
		OpenVPN Client	☐	☐
Device Manager	KARE	KARE	☐	☐
		Other	☐	☐

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.8.15- Other → Passwords

Existen **tres** nombres de usuario para poder acceder a la configuración del equipo. El usuario “admin”, desde el que tendrá acceso a toda la configuración del equipo, y el usuario “user” desde el cual podrá tener acceso a las configuraciones que seleccione (muy útil si personaliza el equipo con sus logos). Desde esta sección puede cambiar el Password de ambos usuarios. También dispone del usuario “guest” que le permitirá acceder a los mismos menús que el usuario “user” pero sin poder realizar cambios de configuración.

**webdyn**
flexitron group

TITAN
"Makes your APPLICATION happen"

- ★ **Mobile**
 - ◇ Status
 - ◇ Basic Settings
 - ◇ Keep Online
- ★ **Ethernet**
 - ◇ Basic Settings
 - ◇ DHCP Server
- ★ **Wifi**
 - ◇ Basic Settings
 - ◇ DHCP Server
- ★ **Firewall**
 - ◇ NAT
 - ◇ Authorized IPs
 - ◇ MAC Filter
 - ◇ Routes
- ★ **Serial Settings**
 - ◇ Serial Port1-RS232
 - ◇ Serial Port2-RS485
 - ◇ SSL Certificates
- ★ **External Devices**
 - ◇ Logger configuration
 - ◇ ModBus Devices
 - ◇ Generic Serial Device
 - ◇ Temperature Sensor
 - ◇ IEC102 Meter
 - ◇ GPS Receiver
- ★ **VPN**
 - ◇ IPsec
 - ◇ OpenVPN Client
 - ◇ OpenVPN Server
 - ◇ ZeroTier
- ★ **Device Manager**
 - ◇ KARE
- ★ **Other**
 - ◇ AT Command

► Other ► Password Web UI

Administrator

Username: Mandatory. Default 'admin'

Password: Password for router administration
Note: Min. 17 characters. Must include uppercase, lowercase, and numbers.

Re enter Password: Re-enter password for router administration

General User

Username: Blank is not used

Password: Password for router administration (user)
Note: Min. 17 characters. Must include uppercase, lowercase, and numbers.

Re enter Password: Re-enter password for router administration (user)

Guest

Username: Blank is not used

Password: Password for router read mode (guest)
Note: Min. 17 characters. Must include uppercase, lowercase, and numbers.

Re enter Password: Re-enter password for router read mode (guest)

Authentication Methods

- **Disable local authentication:** deshabilita la autenticación local (**NOTA IMPORTANTE:** si la autenticación local es deshabilitada y no es posible comunicarse via LDAP o a un servidor TACACS+, necesitarás poner el equipo a valores de fábrica)
- **Remote service:** servicio de autenticación remota (LDAP, TACACS+)

Other > Password Web UI > Authentication Methods

Disable local authentication: ☐

Remote service: None

SAVE CONFIG

Warning: If local authentication is disabled and it is not possible to communicate with the LDAP or TACACS+ server, you will need to configure the default settings to access the router configuration.

Remote authentication service

Users activity

Al final de la sección de “Passwords Web UI”, podemos consultar a través de un botón la actividad de usuario:

Other > Password Web UI > Users activity

VIEW LOG

Dentro podremos ver todas las trazas de log referentes a cualquier tipo de actividad de cualquier usuario:

★ Mobile

- ◊ Status
- ◊ Basic Settings
- ◊ Keep Online

★ Ethernet

- ◊ Basic Settings
- ◊ DHCP Server

★ Wifi

- ◊ Basic Settings
- ◊ DHCP Server

★ Firewall

- ◊ NAT
- ◊ Authorized IPs
- ◊ MAC Filter
- ◊ Routes

★ Serial Settings

- ◊ Serial Port1-RS232
- ◊ Serial Port2-RS485
- ◊ SSL Certificates

★ External Devices

- ◊ Logger configuration
- ◊ ModBus Devices
- ◊ Generic Serial Device
- ◊ Temperature Sensor
- ◊ IEC102 Meter
- ◊ GPS Receiver

★ VPN

- ◊ IPSec
- ◊ OpenVPN Client
- ◊ OpenVPN Server
- ◊ ZeroTier

★ Device Manager

- ◊ KARE

► Z-Other ► Log Users/Services Activity

```
26/06/2026 11:31:58, http, admin, command AT*MTXTUNNEL=SCRIPTRUN,1
26/06/2026 11:32:11, http, admin, command AT*MTXTUNNEL=SCRIPTSTOP,1
26/06/2026 11:32:47, http, admin, command AT*MTXTUNNEL=SCRIPTRUN,1
26/06/2026 11:32:51, http, admin, command AT*MTXTUNNEL=SCRIPTSTOP,1
26/06/2026 11:33:06, http, admin, command AT*MTXTUNNEL=SCRIPTRUN,1
26/06/2026 12:02:21, http, admin, command AT*MTXTUNNEL=SCRIPTSTOP,1
26/06/2026 12:03:40, http, admin, save /external-modbusrtu-expert.php
26/06/2026 12:04:04, http, admin, command AT*MTXTUNNEL=REBOOT
26/06/2026 12:20:25, http, admin/192.168.1.61, new login
29/06/2026 07:25:22, http, admin/192.168.1.57, new login
29/06/2026 09:12:05, http, admin/192.168.1.57, new login
29/06/2026 09:41:20, http, admin, command AT*MTXTUNNEL=GETIEC102,
29/06/2026 11:16:30, http, admin/192.168.1.57, new login
29/06/2026 11:16:35, http, admin, command AT*MTXTUNNEL=GETIEC102,
29/06/2026 14:14:37, http, admin/192.168.1.57, new login
29/06/2026 15:02:20, http, admin/192.168.1.57, new login
29/06/2026 15:06:16, http, admin/192.168.1.57, new login
29/06/2026 15:06:34, http, admin, save /wan-settings.php
29/06/2026 15:06:45, http, admin, command AT*MTXTUNNEL=REBOOT
29/06/2026 15:08:20, http, admin/192.168.1.57, new login
30/06/2026 09:20:10, http, admin/192.168.1.57, new login
30/06/2026 10:40:13, http, admin/192.168.1.57, new login
30/06/2026 10:59:40, http, admin, command AT*MTXTUNNEL=GETTEMPERATURESERIAL
30/06/2026 11:03:06, http, admin, command AT*MTXTUNNEL=GETGPSPOSITION
30/06/2026 11:05:46, http, admin, command AT*MTXTUNNEL=GETIEC102,
```

REFRESH LOG

► Z-Other ► Log Users/Services Activity ► Config

Save failed login:

☐

Only recommended for debug purposes

SAVE CONFIG

De forma adicional, encontramos una última casilla:

- **Save failed login:** marcar en caso de que aquellos login que resulten fallidos deseen guardarse.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.8.16- Other → CA Certificates

Todos los servicios que utilizan conexiones seguras bajo SSL/TLS contra servidores HTTPS o MQTTS necesitan disponer del certificado CA Root utilizado por dicho servidor, con el fin de verificar el certificado del servidor. Desde esta sección es posible introducir hasta 2 servidores CA Root personalizados (en formato PEM).

También es posible seleccionar la opción "Allow all certificates". No es una opción recomendable a menos que disponga de una conexión segura (IPSec, OpenVPN, SIM con APN privado, etc) ya que no se realizará comprobación del certificado de un servidor remoto.

The screenshot shows the webdyn TITAN interface. The top header features the webdyn logo (a stylized 'w' with a blue and grey wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". Below the header is a left sidebar with a navigation menu containing sections like Mobile, Ethernet, Wifi, Firewall, Serial Settings, and External Devices, each with sub-items. The main content area is titled "Other → CA-Root Certificates" and contains the following elements:

- A sub-header "Custom CA-Root Certificates (PEM format)".
- Two rows for user-defined certificates:
 - "User CA-Root-1 file 'ca1.crt'" with an "Examinar..." button, a text field showing "No se ha seleccionado ningún archivo.", an "Upload" button, and a status "not uploaded".
 - "User CA-Root-2 file 'ca2.crt'" with similar controls and status.
- Three buttons: "DELETE User CA-Root-1", "DELETE User CA-Root-2", and "VIEW INTERNAL CA LIST".
- A section titled "CA-Root Certificates → Options" containing:
 - An option "Allow all certificates" with an unchecked checkbox.
 - A warning text: "Unsecure option. This option is not recommended if your device is not running over a secure connection (like IPSec, OpenVPN, SIM card with private APN, ...)"
 - A "SAVE CONFIG" button.

Notas adicionales.

- El equipo basado en TITAN dispone de una lista interna con los certificados CA Root más comunes. Si necesita utilizar un certificado no disponible, puede introducirlo aquí.

4.8.17- Other → Email Configuration

Los equipos basados en TITAN permiten el envío de notificaciones por email. También permiten el envío de emails a través de comandos AT (por ejemplo, si usted dispone de un PLC y quiere enviar un mensaje SMS o un EMAIL puede hacerlo mediante el envío de un comando AT al equipo basado en TITAN).

El equipo basado en TITAN debe estar previamente configurado para poder enviar correos electrónicos. Es decir, debe configurar el servidor SMTP a utilizar en esta sección.

- **Enabled:** Permite habilitar el servicio de email.
- **Smtp Server:** Indica la dirección IP o DNS del servidor SMTP (por ejemplo smtp.gmail.com, smtpout.secureserver.net, ...)
- **Smtp Port:** Puerto TCP del servidor SMTP
- **Authentication:** Seleccionar si el servidor SMTP requiere autenticación (normalmente sí)
- **TLS:** Seleccionar si el servidor SMTP requiere TLS
- **User:** Nombre de usuario de la cuenta de correo origen
- **Password:** Password de la cuenta de correo origen
- **Email address:** Dirección de correo origen desde la que se enviarán los emails

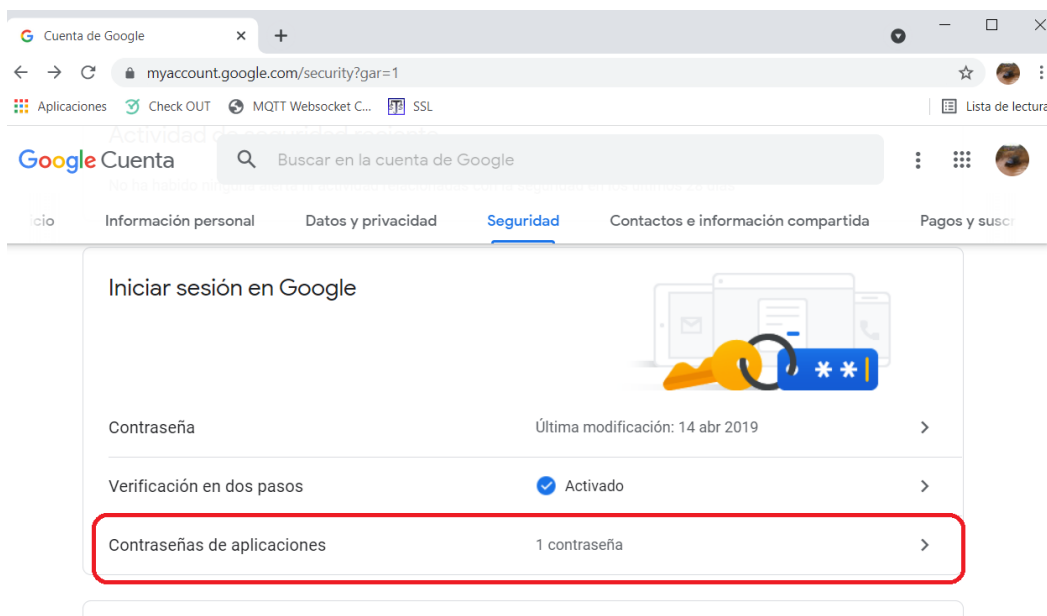
The screenshot displays the webdyn TITAN configuration interface. The top header features the webdyn logo (a stylized 'w' with a blue and grey wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". A left sidebar contains a navigation menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), and Serial Settings (Serial Port1-RS232). The main content area is titled "Other → Email configuration" and contains the following settings:

Enabled:	☐	Enable Email
Smtp Server:		Ex: smtp.gmail.com, smtpout.se, cureserver.net , ...
Smtp Port:	25	TCP port for SMTP Server (25, 465, 587, ...)
Authentication:	☒	Check if authentication is required
TLS:	☒	Check if TLS is required
User:		User of email account
Password:		Password of email account
Email address:		Email address for sending emails (Ex: myemail@gmail.com)

At the bottom left of the configuration area is a "SAVE CONFIG" button.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Tenga en cuenta que si usa el servidor SMTP de GMAIL deberá crear una “contraseña para aplicaciones”. Para ello vaya a su “Gestor de Cuenta Google”, seleccione el menú “Seguridad” y añada una “Contraseña para aplicaciones”.



- Por motivos de seguridad se recomienda encarecidamente la activación de las comunicaciones TLS. Las comunicaciones sin activación de TLS no son seguras.

4.8.18- Other → Modbus Slave

Los equipos basados en TITAN pueden ser configurados para actuar como un dispositivo Modbus TCP Slave y/o como Modbus RTU Slave. Por ejemplo, usando el protocolo Modbus puede conmutar remotamente (vía 4G/3G/2G, Ethernet o Wifi) las salidas digitales del equipo, consultar el estado de las entradas digitales, así como también enviar SMS, recibir SMS o incluso enviar Emails por Modbus.

The screenshot shows the webdyn TITAN configuration interface. On the left is a sidebar with navigation links: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), and Serial Settings (Serial Port1-RS232). The main content area is titled 'Other → ModBus TCP Slave' and contains the following settings:

- Enabled:** A checkbox that is currently unchecked. To its right is the text 'Enable Titan router as Modbus TCP Slave'.
- ModBus TCP Port:** A text input field containing the value '502'. To its right is the text 'Router waits for connections at this TCP port'.

Below this, there is another section titled 'Other → ModBus RTU Slave' with the following settings:

- Enabled:** A checkbox that is currently unchecked. To its right is the text 'Enable Titan router as Modbus RTU Slave'.
- ModBus RTU address:** A text input field containing the value '1'. To its right is the text 'Modbus RTU for Titan Router (1 ... 254)'.
- ModBus COM Port:** A dropdown menu currently showing 'Serial Port 1'. To its right is the text 'In the COM port configuration, select function "none" or external device.'

At the bottom left of the main content area is a button labeled 'SAVE CONFIG'.

A continuación, dispone de la tabla de memoria con las direcciones Modbus de los registros del equipo basado en TITAN. Los comandos Modbus admitidos son: 0x03 para realizar una lectura y 0x10 para escritura.

ID Registro	R/W	Valores posibles	Descripción
1	R	0 ... 32635	Versión de firmware
2	R	0 ... 32635	Subversión de firmware
6	R	0 ... 31	RSSI de la señal GSM
7	R	2,3,4	Tecnología usada (2=2g,3=3g,4=4g)
8	R	1 ... 31	Día
9	R	1 ... 12	Mes
10	R	2000 2099	Año
11	R	0 ... 23	Hora
12	R	0 ... 59	Minutos
13	R	0 ... 59	Segundos

20	W	1	Ejecuta un reset
30	RW	0,1	GPIO 0 (de existir)
31	RW	0,1	GPIO 1 (de existir)
32	RW	0,1	GPIO 2 (de existir)
33	RW	0,1	GPIO 3 (de existir)
34	RW	0,1	GPIO 4 (de existir)
98	W	0 ... 32635	Longitud del comando AT a ejecutar
99	R	0 ... 32635	Longitud de la respuesta del comando AT
100 ... 354	W	ASCII	Texto del comando AT (en ASCII)
500 ... 754	R	ASCII	Texto de la respuesta del comando AT (en ASCII)
1000	R/W	0, 1	1 indica nuevo SMS recibido. Un PLC tras leer el SMS debe escribir un 0.
1001	R	0 ... 18	Longitud del teléfono en envió el SMS
1002 ... 1019	R	ASCII	Número de teléfono que envió el SMS
1020	R	0 ... 160	Longitud del texto del mensaje SMS
1021 ... 1180	R	ASCII	Texto del mensaje SMS
1021 ... 1180	R	ASCII	Texto del mensaje SMS
10000	RW	0 ... 65535	Registro de usuario 10000
10001...19998	RW	ASCII	Registro de usuario de 10001 a 19998
19999	RW	0 ... 65535	Registro de usuario 19999

Comandos AT mediante protocolo Modbus

Otra característica muy interesante de los equipos basados en TITAN es que permiten la ejecución de comandos AT mediante protocolo Modbus. Por ejemplo, si se dispone de un PLC que actúa como Master Modbus TCP puede enviar vía protocolo Modbus TCP una orden al equipo para ejecutar un comando AT, pudiendo obtener datos como la cobertura, enviar un SMS, obtener la hora, resetear el equipo, etc.

El procedimiento para ejecutar un comando AT vía Modbus es muy sencillo. La mejor manera de entenderlo es mediante un ejemplo. Imaginemos que deseamos ejecutar el comando AT+CSQ para obtener la cobertura

1.- Escribimos el comando AT, en ASCII, a partir del registro 100.

ID Registro	Valor	Descripción
100	65	ASCII de la letra: A
101	84	ASCII de la letra: T
102	43	ASCII del carácter: +
103	67	ASCII de la letra: C
104	83	ASCII de la letra: S
105	81	ASCII de la letra: Q

2.- El comando AT+CSQ tiene 6 caracteres, por lo que para ejecutar el comando AT, escribimos un 6 en el registro 98. Tras la escritura en el registro 98 el comando AT se ejecutará de inmediato.

ID Registro	Valor	Descripción
98	6	Tamaño del comando a ejecutar

3.- Comprobamos el resultado de la ejecución del comando AT, para ello leemos el registro 99. El valor leído será la longitud de la respuesta. Un valor 0 indica que todavía no hay respuesta (no ha acabado la ejecución que habitualmente será inferior a 1 segundo). Un valor >0 indica la longitud de la respuesta.

ID Registro	Valor	Descripción
99	28	Tamaño de la respuesta del comando

4.- Finalmente, leemos los 28 registros donde está contenida la respuesta a partir del registro 500

ID Registro	Valor	Descripción
500	65	A
501	84	T
502	43	+
503	67	C
504	83	S
505	81	Q
506	13	\r
507	13	\r
508	10	\n
509	43	+
510	67	C
511	83	S
512	81	Q
513	58	:
514	32	[space]
515	49	1
516	54	6
517	44	,
518	57	9
519	57	9
520	13	\r
521	10	\n
522	13	\r
523	10	\n

524	79	O
525	75	K
526	13	\r
527	10	\n

En el caso de este comando AT, los registros relevantes son el 515 y 516 que indican una cobertura de un valor "16".

P.D. Recuerde que si quiere utilizar esta característica para enviar un SMS debe utilizar el comando AT indicado en esta guía: AT^MTXTUNNEL=SMS,telefono,mensaje

Recibir SMS por Modbus TCP

El procedimiento para recibir mensajes SMS por Modbus TCP es muy sencillo. Su PLC debe chequear periódicamente el registro 1000. Si el valor leído es un "1" implica que ha llegado un nuevo mensaje SMS. Debe entonces leerlo utilizando los registros implicados 1001-1180. Una vez leído debe escribir un "0" en el registro 1000.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Consulte la tabla de registros Modbus dentro de los menús de configuración del propio equipo basado en TITAN, en la sección Other > Modbus Slave

4.8.19 - Other → TITAN Scripts

Los equipos basados en TITAN permiten ejecutar un script programable por el usuario en lenguaje **JAVASCRIPT (ECMAScript 5)**. <https://www.w3schools.com/jsref/default.asp> Desde este script puede accederse a distintas características del equipo basado en TITAN para hacer pequeñas customizaciones (como leer dispositivos por el puerto serie, leer las entradas digitales, cambiar una salida digital, leer un dispositivo Modbus, enviar un mensaje SMS, enviar un EMAIL, un mensaje MQTT a un determinado topic, enviar un TRAP SNMP, guardar y leer ficheros en el equipo, etc. (Consulte los distintos ejemplos del equipo basado en TITAN para una mayor comprensión).

La pantalla de configuración de los TITAN Scripts tiene el siguiente aspecto:

The screenshot shows the webdyn TITAN Scripts v2 configuration page. The interface includes a sidebar menu on the left with categories like Mobile, Ethernet, Firewall, Serial Settings, External Devices, Device Manager, and Other. The main content area is titled 'Other ▶ Titan Scripts v2' and features a dropdown menu set to 'Example 1 - Hello World' with a 'Load Example' button. Below this, a text area displays a JavaScript script for printing 'Hello World' to the console with a 1-second pause. At the bottom of the script area are buttons for 'Run Script', 'Stop Script', 'Save Script', 'Delete Script', and 'Encrypt Script'. A section titled 'Other ▶ Titan Scripts v2 ▶ Console' contains a large text area for the console output and buttons for 'Run console', 'Stop console', and 'Clear console'.

webdyn flexitron group **TITAN** "Makes your APPLICATION happen"

★ **Mobile**

- ◇ Status
- ◇ Basic Settings
- ◇ Keep Online

★ **Ethernet**

- ◇ Basic Settings

★ **Firewall**

- ◇ Authorized IPs
- ◇ MAC Filter

★ **Serial Settings**

- ◇ Serial Port1-RS232
- ◇ Serial Port2-RS485
- ◇ SSL Certificates

★ **External Devices**

- ◇ Logger configuration
- ◇ ModBus Devices
- ◇ Generic Serial Device
- ◇ Temperature Sensor
- ◇ IEC102 Meter

★ **Device Manager**

- ◇ KARE

★ **Other**

- ◇ AT Command
- ◇ DynDns
- ◇ Private DynDns
- ◇ Sms control
- ◇ Periodic Autoreset
- ◇ Time Servers
- ◇ Remote Console
- ◇ Snmp
- ◇ Tacacs+
- ◇ Ldap
- ◇ Mqtt / Mqtts
- ◇ Http / Https
- ◇ User Permissions
- ◇ Passwords Web UI
- ◇ CA Certificates
- ◇ Email Config
- ◇ ModBus Slave
- ◇ **Titan Scripts**
- ◇ Connectivity tools
- ◇ Digital I/O
- ◇ Custom Skin
- ◇ Led Config
- ◇ Syslog

▶ **Other ▶ Titan Scripts v2**

Example 1 - Hello World Load Example

User script (File: 'script-user1.mtx')

```
1 mtx.println("EXAMPLE 1 - Running...");
2
3 //EXAMPLE: HOW TO SHOW DEBUG INFO
4
5 var i;
6 for (i=0;i<10;i++)
7 {
8     //***** PRINT "Hello World" BY CONSOLE
9     mtx.println("Hello World: " + i);
10
11     //***** PAUSE 1 SECOND
12     mtx.pause(1000);
13 }
14
15 mtx.println("EXAMPLE 1 - End");
16
```

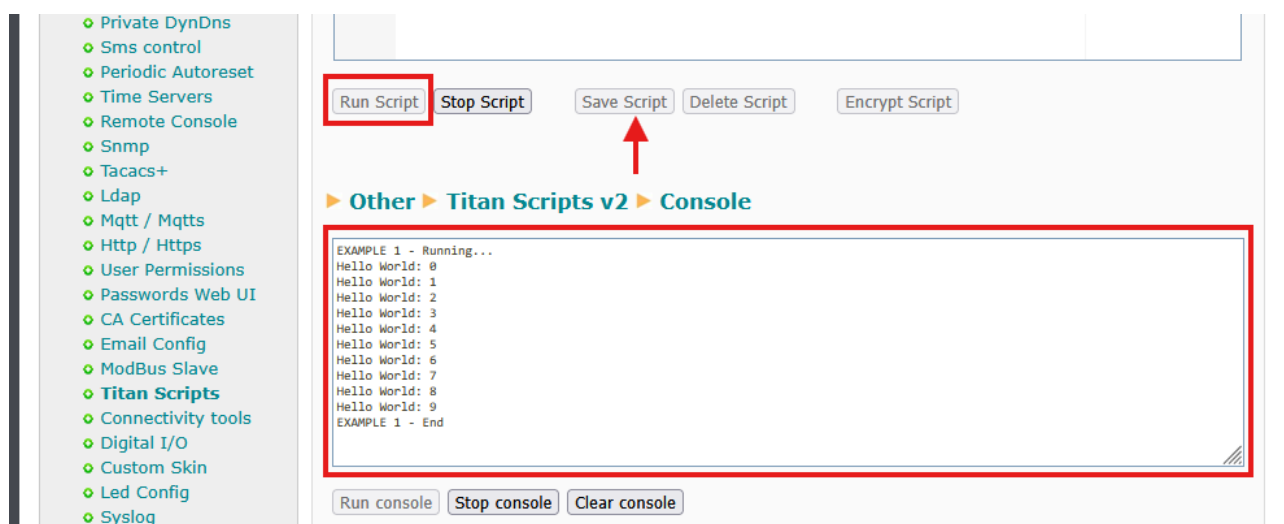
Run Script Stop Script Save Script Delete Script Encrypt Script

▶ **Other ▶ Titan Scripts v2 ▶ Console**

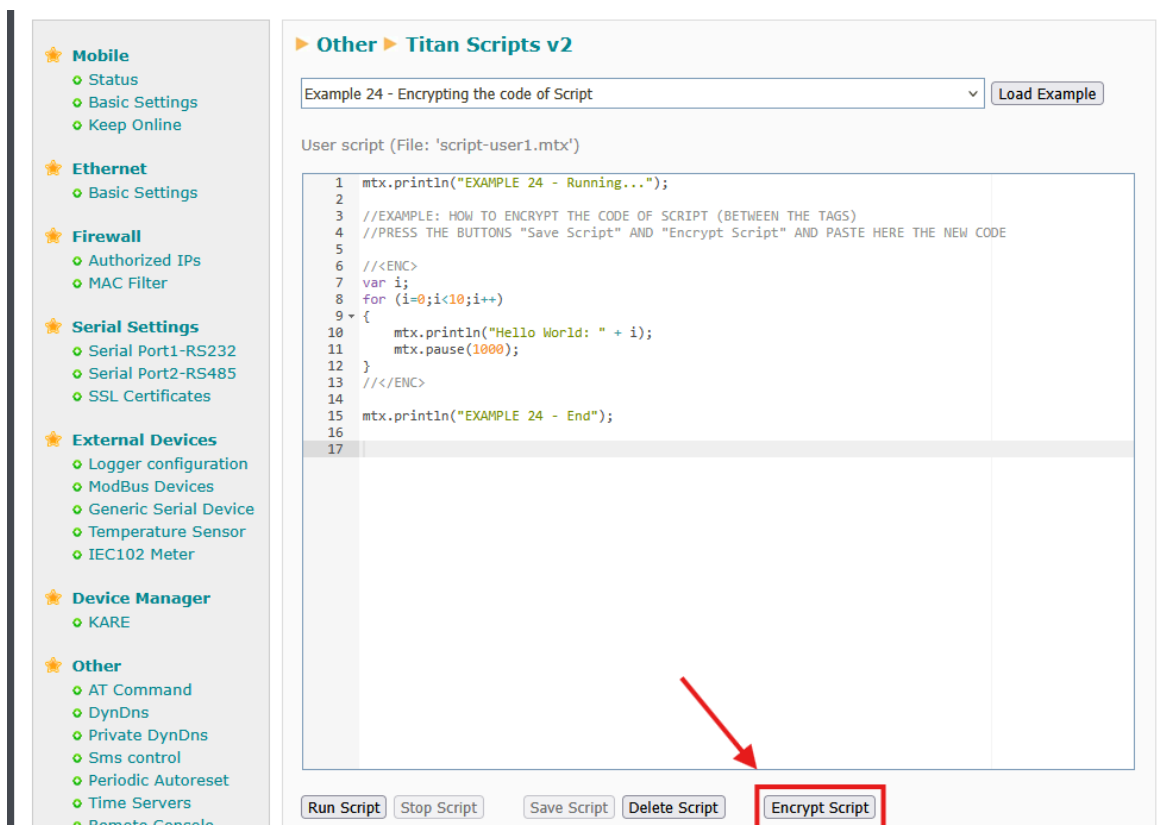
Run console Stop console Clear console

En el desplegable superior dispone de múltiples ejemplos con todas las características que puede utilizar. Para cargar un ejemplo seleccione en el desplegable el ejemplo que desee (recomendable la primera vez el ejemplo “Hello World”) y después pulse el botón **“Load Example”**. Tras esta acción el código fuente del ejemplo aparecerá en pantalla.

Después pulse el botón **“Save Script”** para guardar el código del ejemplo en la memoria de ejecución del equipo basado en TITAN. Tras ello ya puede pulsar el botón **“Run Script”** para ejecutar el script y en pocos segundos en la sección de consola aparecerán las trazas del programa **“mtx.println()”**.



En caso de querer encriptar el código de los scripts, pulse el botón **“Encrypt Script”** y se generará una ventana emergente con un nuevo código.



Tras pegar este nuevo código en el script el equipo basado en TITAN será capaz de ejecutarlo de la misma manera.

The screenshot displays the 'Titan Scripts v2' interface. On the left is a sidebar menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings), Firewall (Authorized IPs, MAC Filter), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor, IEC102 Meter), Device Manager (KARE), and Other (AT Command, DynDns, Private DynDns, Sms control, Periodic Autoreset, Time Servers, Remote Console, Snmp, Tacacs+, Ldap, Mqtt / Mqtts, Http / Https, User Permissions, Passwords Web UI, CA Certificates, Email Config, ModBus Slave, Titan Scripts, Connectivity tools, Digital I/O, Custom Skin, Led Config, Syslog). The main area is titled 'Other Titan Scripts v2' and features a dropdown menu showing 'Example 24 - Encrypting the code of Script' with a 'Load Example' button. Below this, a text area labeled 'User script (File: 'script-user1.mtx')' contains a script with line numbers 1 to 11. The script includes a header comment explaining how to encrypt the code and a base64-encoded payload. At the bottom of the editor are buttons for 'Run Script', 'Stop Script', 'Save Script', 'Delete Script', and 'Encrypt Script'. Below the editor is a 'Console' section titled 'Other Titan Scripts v2 Console' which shows the output of the script: 'EXAMPLE 24 - Running...' followed by ten 'Hello World' messages and 'EXAMPLE 24 - End'. At the bottom of the console are buttons for 'Run console', 'Stop console', and 'Clear console'.

```
1 mtx.println("EXAMPLE 24 - Running...");
2
3 //EXAMPLE: HOW TO ENCRYPT THE CODE OF SCRIPT (BETWEEN THE TAGS)
4 //PRESS THE BUTTONS "Save Script" AND "Encrypt Script" AND PASTE HERE THE NEW CODE
5
6 //<AES>
7 U2FsdGVkX1/sHyWdrf3DDd5D/9/pPdc9kvGu7SnmKmQf9THo35q8mQpm6eKVbqocsEN9fiyeNrXA
8 pJ1aRQkhy6SG0HL711L6iwy5wuRAFK/0ocVmZR5ikUj296Y9C3jKJHtEokTqlgpxulw66BfdIXw==
9 //</AES>
10
11 mtx.println("EXAMPLE 24 - End");
```

```
EXAMPLE 24 - Running...
Hello World: 0
Hello World: 1
Hello World: 2
Hello World: 3
Hello World: 4
Hello World: 5
Hello World: 6
Hello World: 7
Hello World: 8
Hello World: 9
EXAMPLE 24 - End
```

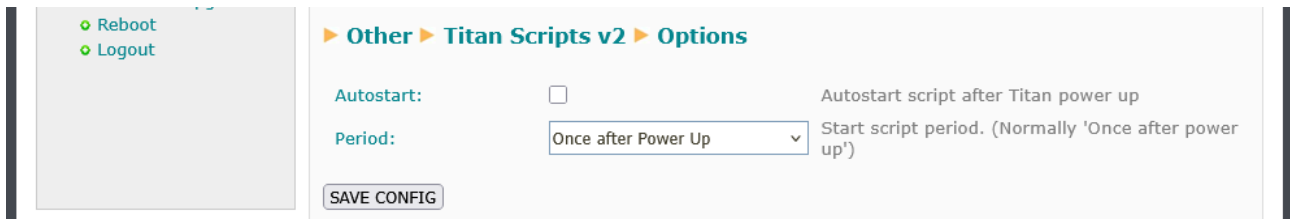
Para más información acerca de la encriptación de scripts, consultar ejemplos 24 y 25.

Opciones de configuración de los TITAN Scripts.

Una vez tenga desarrollado y funcionando su script deseará que éste se ejecute de forma autónoma cada vez que el equipo basado en TITAN se reinicie. Para ello necesitará activar la casilla **"Autostart"**. Una vez activada esa casilla debe especificar la forma de autoarranque. La forma habitual sera "Once after Power Up", es decir, el script se ejecutará una vez tras el arranque del equipo basado en TITAN. Esto es óptimo para la mayoría de aplicaciones del tipo:

```
while (true) {
...
}
```

en las que el código se ejecuta de forma cíclica. Pero quizás le resulte más cómodo que el script se ejecute automáticamente cada cierto intervalo de tiempo (cada 1 minuto, 2 minutos, 5 minutos, etc) para realizar ciertas tareas. Por ejemplo, imagine el caso en que necesita un script para leer un equipo Modbus RTU cada 15 minutos y enviar la lectura a un servidor MQTT. En este caso puede resultarle más cómodo ejecutar el script cada 15 minutos.



El objeto “mtx” de los TITANScripTs.

Como se indica en los párrafos anteriores, los TITANScripTs le permiten programar pequeños scripts en lenguaje JavaScript (ECMAScript 5) para interaccionar con ciertas características propias del equipo basado en TITAN. El acceso a dichas características se realiza a través de ciertas funciones de un objeto “mtx”. A continuación se describe cada una de estas funciones. Se recomienda encarecidamente estudiar los pequeños ejemplos incluidos en la sección “Other → TITAN ScripTs” para una mayor comprensión. **Tenga presente que los TITAN ScripTs han sido concebidos para llevar a cabo pequeñas personalizaciones en el comportamiento del equipo basado en TITAN, no estando diseñados para programar cualquier tipo de aplicación como podrían realizarse en otro tipo de lenguaje como “Java”, “C++”, “Python”, etc. Básicamente todo lo que puede hacer está contenido en los ejemplos incluidos.**

Funciones relacionadas con las ENTRADAS / SALIDAS DIGITALES IOx:

En las “Notas” de cada función encontrará un listado con los ejemplos de scripts disponibles con el uso de dicha función. Estos ejemplos se encuentran alojados dentro del propio router a través del menú “Other → TITAN ScripTs”.

- **Función:** **mtx.ioGet(idIO)**
Descripción: permite obtener el estado de una entrada/salida digital.
Parámetros: idIO: int 0,1,2,3,4, (identificador de la IO)
Respuesta: int (0=entrada no activada, 1=entrada activada, -1=error)
Notas: consulte los ejemplos: 3, 15, 16
- **Función:** **mtx.ioSet(idIO, value)**
Descripción: permite cambiar el estado de una salida digital.
Parámetros: idIO: (int) 0,1,2,3,4, (identificador de la IO)
value: (int) 0,1 (valor lógico de la salida digital)
Respuesta: boolean (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 16

- Función:** `mtx.counterGet(idIO)`
Descripción: permite obtener el valor del contador de pulsos asociado a una entrada.
Parámetros: idIO: int 0,1,2,3,4, (identificador de la entrada digital)
Respuesta: long valor del contador
Notas: consulte los ejemplos: 34
- Función:** `mtx.counterSet(idIO, value)`
Descripción: permite cambiar el valor inicial de un contador de pulsos
Parámetros: idIO: (int) 0,1,2,3,4, (identificador de la IO)
 value: (long) (valor del contador)
Respuesta: boolean (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 34

Funciones relacionadas con los LEDS del router:

- Función:** `mtx.ledSet(idLed, value)`
Descripción: permite encender / apagar un led
Parámetros: idLed: (int) 0,1,2, (identificador del led del equipo)
 value: (int) 0=apagado, 1=encendido, 2=parpadeo lento, 3=parpadeo rápido.
Respuesta: boolean (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 21

Funciones relacionadas con COMANDOS AT:

- Función:** `mtx.atSend(command, timeout)`
Descripción: permite ejecutar un comando AT sobre el propio equipo basado en TITAN
Parámetros: command: (String) comando AT a ejecutar
 timeout: (int) milisegundos de timeout
Respuesta: String: respuesta al comando AT. ""= Error
Notas: consulte los ejemplos: 2

Funciones relacionadas con MQTT:

- Función:** `mtx.mqttIsConnected()`
Descripción: devuelve si el equipo basado en TITAN está conectado a un broker MQTT
Parámetros: Ninguno.
Respuesta: boolean (true=Sí, false=No)
Notas: consulte los ejemplos: 4, 35
- Función:** `mtx.mqttSend(message, topic, qos)`
Descripción: permite enviar un mensaje MQTT de texto a un determinado topic mqtt con una determinada QoS

Parámetros: message: (String) Mensaje de texto a enviar
 topic: (String) Topic mqtt al que enviar el mensaje
 qos: (int) QoS del envío (0,1,2)
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 4, 8, 35

- Función:** **mtx. mqttSendArray(array byte, topic, qos)**
Descripción: permite enviar un mensaje MQTT de un array de bytes a un determinado topic mqtt con una determinada QoS
Parámetros: message: (array byte) Mensaje de texto a enviar
 topic: (String) Topic mqtt al que enviar el mensaje
 qos: (int) QoS del envío (0,1,2)
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 35
- Función:** **mtx. mqttSubscribe(topic)**
Descripción: los TITAN scripts permiten la subscripción a 1 topic MQTT para poder recibir comunicaciones de un broker. Mediante esta función es posible subscribirse a dicho topic.
Parámetros: topic: (String) Topic mqtt donde los TITAN scripts recibirán mensajes
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 35
- Función:** **mtx. mqttGetArray()**
Descripción: función que permite comprobar y recibir si hay datos llegados al topic configurado mediante la función anterior mtx.mqttSubscribe(topic)
Parámetros: Ninguno
Respuesta: array bytes: (null=no hay datos, !null=array de bytes con los datos)
Notas: consulte los ejemplos: 35

Las funciones MQTT mostradas a continuación mantienen compatibilidad con versiones anteriores y utilizan por defecto el bróker Primary:

- Función:** **mtx. mqttIsConnected(brokerId)**
Descripción: devuelve si el equipo basado en TITAN está conectado al bróker indicado.
Parámetros: brokerId: (String) "primary" o "secondary".
Respuesta: boolean (true=Sí, false=No)
Notas: consulte el ejemplo 61.
- Función:** **mtx. mqttSendTo(brokerId, message, topic, qos)**
Descripción: permite enviar un mensaje MQTT de texto al bróker indicado.
Parámetros: brokerId: (String) "primary", "secondary" o "both"; message: (String) Mensaje de texto; topic: (String) Topic mqtt; qos: (int) QoS del envío (0,1,2)
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte el ejemplo 61.
- Función:** **mtx. mqttSendArrayTo(brokerId, array byte, topic, qos)**
Descripción: permite enviar un mensaje MQTT de tipo array de bytes al bróker indicado.

Parámetros: brokerId: (String) "primary", "secondary" o "both"; message: (array byte)
 Datos a enviar; topic: (String) Topic mqtt; qos: (int) QoS del envío (0,1,2)
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte el ejemplo 61.

- Función:** **mtx.mqttSubscribeTo(brokerId, topic)**
Descripción: permite subscribirse a un topic MQTT en el bróker indicado.
Parámetros: brokerId: (String) "primary", "secondary" o "both"; topic: (String) Topic mqtt donde los TITAN scripts recibirán mensajes
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte el ejemplo 61.
- Función:** **mtx.mqttGetArrayFrom(brokerId)**
Descripción: permite comprobar y recibir si hay datos llegados al topic configurado mediante `mtx.mqttSubscribeTo`.
Parámetros: brokerId: (String) "primary" o "secondary".
Respuesta: array bytes: (null=no hay datos, !null=array de bytes con los datos)
Notas: consulte el ejemplo 61.

Funciones relacionadas con TRAPS SNMP:

- Función:** **mtx.trapSend(oid, message, severity)**
Descripción: envía un trap SNMP
Parámetros: oid: (String) OID del trap SNMP
 message: (String) Texto asociado al trap SNMP
 severity (int) Severidad del Trap (1, ... ,7)
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 5, 9. Si se utiliza esta función sin indicar IP destino, el TRAP se enviará a las direcciones configuradas en "Other > SNMP". Si se han configurado hasta 3 IPs de traps, el envío se realizará a todas ellas.
- Función:** **mtx.trapSend(oid, message, severity, ip, port, community)**
Descripción: envía un trap SNMP a una IP destino concreta, o a varias IPs separadas por coma.
Parámetros: oid: (String) OID del trap SNMP
 message: (String) Texto asociado al trap SNMP
 severity (int) Severidad del Trap (1, ... ,7)
 ip (String) IP destino o lista de IPs separadas por coma.
 port: (int) puerto UDP destino para el envío del TRAP SNMP.
 community: (String) community SNMP utilizada para el envío del TRAP.
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 5.
- Función:** **mtx.trapRXServiceStart_v1_v2c(community,port)**
Descripción: activa el servicio de recepción de traps SNMP v1 y v2c
Parámetros: community: (String) permite especificar el community de los traps. Si se

especifica un community vacío ("") se aceptan todos los traps
 port: (int) Puerto de recepción. 0 ... 65535. Normalmente 162.
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 60

- Función:** **mtx.trapRXServiceStop()**
Descripción: detiene el servicio de recepción de traps SNMP
Parámetros: Ninguno.
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 60
- Función:** **mtx.trapRXGet()**
Descripción: consulta si existen nuevos OIDs de TRAPS recibidos. En caso afirmativo la función devuelve el OID junto con su valor, en un formato "<OID>=<valor>". Un TRAP recibido puede contener varios OIDs, por lo que pueden ser necesarias varias lecturas por cada TRAP recibido.
Parámetros: Ninguno.
Respuesta: String: <OID>=<valor> cuando exista un nuevo OID para ser leído
 "" cuando no hayan nuevos OID para ser leídos.
Notas: consulte los ejemplos: 60
- Función:** **mtx.snmpModbusSetMode(setMode, modbusAddress, initialRegister)**
Descripción: función específica para implementar una pasarela Modbus SNMP. Permite especificar el modo de comportamiento de un router Titan cuando recibe un comando SNMP SET.
Parámetros: setMode (int) 0: escribe directamente en la memoria de usuario modbus.
 (int) 1: escribe directamente sobre el registro modbus de un dispositivo externo.
 modbusDevAddr: (String) dirección modbus de dispositivo en caso de usar el modo setMode 1. Para modbus TCP: ip@id:port y para modbus RTU: id
 initialRegister (int) dirección inicial del registro modbus del primero OID
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos de las notas de aplicación: AN79 y AN80.

Funciones relacionadas con SMS:

- Función:** **mtx.smsSend(phoneNumber, textMessage)**
Descripción: envía un mensaje SMS a un número de teléfono
Parámetros: phoneNumber: (String) Número de teléfono de envío
 textMessage: (String) Texto del mensaje SMS

Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 3, 10, 17, 18,40

- **Función:** **mtx.smsRead()**
Descripción: comprueba si ha llegado un nuevo mensaje SMS
Parámetros: Ninguno
Respuesta: array String: (null=no hay SMS nuevo, data[0]=número teléfono
data[1]=mensaje SMS)
Notas: consulte los ejemplos: 40

Funciones relacionadas con HTTP:

- **Función:** **mtx.httpRequest(url, headers,method,data,dataType)**
Descripción: envía un email a una dirección de correo
Parámetros: url: (String) Url de conexión
headers: (HashMap) Cabeceras HTTP personalizadas
method: (String) GET o POST
data: (String) datos a enviar con la petición http
dataType: (String) tipo de datos a enviar con la petición http
Notas: consulte los ejemplos: 39

Funciones relacionadas con EMAILS:

- **Función:** **mtx.emailSend(address, subject)**
Descripción: envía un email a una dirección de correo
Parámetros: address: (String) Dirección de email destino
subject : (String) Asunto del email enviado
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 6, 11

Funciones relacionadas con TELEGRAM:

- **Función:** **mtx.telegramSendMessage(apiToken, chatID,message)**
Descripción: envía un mensaje de texto a un grupo de chat de Telegram
Parámetros: apiToken: (String) API token del bot de Telegram
chatID : (String) Identificador de chat donde enviar el mensaje
message: (String) Mensaje de texto a enviar
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 41, 42

Funciones relacionadas con la TARJETA SIM:

- **Función:** **mtx.simID()**
Descripción: devuelve la tarjeta SIM que está siendo usada
Parámetros: Ninguno
Respuesta: int: (-1=ERROR, 0=no SIM, 1=SIM1, 2=SIM2)
Notas: consulte los ejemplos: 18

- Función:** **mtx.simInserted()**
Descripción: devuelve si la tarjeta SIM actual está insertada
Parámetros: Ninguno
Respuesta: int: (-1=ERROR, 0=no insertada, 1=insertada)
Notas: consulte los ejemplos: ---
- Función:** **mtx.simStatus()**
Descripción: devuelve el estado de la SIM actual
Parámetros: Ninguno
Respuesta: int: (-1=ERROR, 0=ERROR de SIM, 1=SIM OK)
Notas: consulte los ejemplos: 18

Funciones relacionadas con PUERTOS SERIE:

- Función:** **mtx.serialOpen(idPort,baudrate,databits,parity,stopbits,flowcontrol)**
Descripción: abre un puerto serie
Parámetros: idPort: (int) id del puerto serie (1,2)
 baudrate: (int) velocidad (460800, 230400, ... , 1200, 600, 300)
 databits: (int) número de bits por dato (8,7)
 paridad: (int) 0=ninguna, 1=impar, 2=par
 stopbits: (int) 1,2
 flowcontrol: (int) 0=no, 1=hardware (si disponible)
Respuesta: boolean: true: OK, false: ERROR
Notas: consulte los ejemplos: 19
- Función:** **mtx.serialClose(idPort)**
Descripción: cierra un puerto serie
Parámetros: idPort: (int) id del puerto serie (1,2)
Respuesta: boolean: true: OK, false: ERROR
Notas: consulte los ejemplos: ---
- Función:** **mtx.serialRead(idPort)**
Descripción: lee y devuelve los datos leídos por un puerto serie RS232 o RS485
Parámetros: idPort: (int) id del puerto serie (1,2)
Respuesta: byte []: array de bytes con los datos leídos
 null: no hay datos leídos.
Notas: consulte los ejemplos: 19
- Función:** **mtx.serialWrite(idPort,data,start,length)**
Descripción: envía un array de bytes por el puerto serie
Parámetros: idPort: (int) id del puerto serie (1,2)
 data: (byte[]) array de bytes para e
 start: (int) índice de inicio de envío del array de bytes
 length: (int) número de bytes a enviar.
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 19

Funciones relacionadas con MODBUS:

- Función:** **mtx.modbusRTUGetWords(address, command, start, numRegisters)**
Descripción: lee y devuelve los registros Modbus de un dispositivo modbus RTU
Parámetros: address: (int) dirección Modbus RTU (1 ... 254)
command: (int) comando Modbus 3 ó 4
start: (int) dirección de registro inicial a leer
numRegisters: (int) número de registros a leer (1 ... 64)
Respuesta: int []: array de WORDS con los datos leídos (valores 0 ... 65535)
null: ERROR de lectura.
Notas: consulte los ejemplos: 7, 8, 9, 10, 11, 12, 22, 30
- Función:** **mtx.modbusRTUSetWords(address, command, start, values[])**
Descripción: escribe registros Modbus en un dispositivo modbus RTU
Parámetros: address: (int) dirección Modbus RTU (1 ... 254)
command: (int) comando Modbus 16 ó 6
start: (int) dirección de registro inicial a escribir
values[]: (int[]) array con los WORDS a escribir
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 12
- Función:** **mtx.modbusRTUGetBits(address, command, start, numBits)**
Descripción: lee y devuelve los registros Modbus tipo bit de un dispositivo modbus RTU
Parámetros: address: (int) dirección Modbus RTU (1 ... 254)
command: (int) comando Modbus 1 ó 2
start: (int) dirección de registro bit inicial a leer (1 ... 65535)
numBits: (int) número de bits a leer (1 ... 64)
Respuesta: int []: array de BITS con los bits leídos (valores 0,1)
null: ERROR de lectura
Notas: consulte los ejemplos: 13
- Función:** **mtx.modbusRTUSetBit(address, command, start, value)**
Descripción: escribe 1 registro Modbus tipo bit en un dispositivo modbus RTU
Parámetros: address: (int) dirección Modbus RTU (1 ... 254)
command: (int) comando Modbus (5)
start: (int) dirección de registro bit inicial a escribir
values: (int) valor a escribir (0,1)
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 14
- Función:** **mtx.modbusTCPGetWords(ip, port, command, start, numRegisters)**
Descripción: lee y devuelve los registros Modbus de un dispositivo Modbus TCP
Parámetros: ip: (String) dirección IP del dispositivo Modbus TCP
port: (int) puerto TCP del dispositivo Modbus TCP
command: (int) comando Modbus 3 ó 4
start: (int) dirección de registro inicial a leer
numRegisters: (int) número de registros a leer (1 ... 64)
Respuesta: int []: array de WORDS con los datos leídos (valores 0 ... 65535)
null: ERROR de lectura.
Notas: consulte los ejemplos: ---

- Función:** **mtx.modbusTCPSetWords(ip, port, command, start, values[])**
Descripción: escribe registros Modbus en un dispositivo Modbus TCP
Parámetros: ip: (String) dirección IP del dispositivo Modbus TCP
port: (int) puerto TCP del dispositivo Modbus TCP
command: (int) comando Modbus 16 ó 6
start: (int) dirección de registro inicial a escribir
values[]: (int[]) array con los WORDS a escribir
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 22
- Función:** **mtx.modbusTCPGetBits(ip, port, command, start, numBits)**
Descripción: lee y devuelve los registros Modbus tipo bit de un dispositivo Modbus TCP
Parámetros: ip: (String) dirección IP del dispositivo Modbus TCP
port: (int) puerto TCP del dispositivo Modbus TCP
command: (int) comando Modbus 1 ó 2
start: (int) dirección de registro bit inicial a leer (1 ... 65535)
numBits: (int) número de bits a leer (1 ... 64)
Respuesta: int []: array de BITS con los bits leídos (valores 0,1)
null: ERROR de lectura.
Notas: consulte los ejemplos: ---
- Función:** **mtx.modbusTCPSetBit(ip, port, command, start, value)**
Descripción: escribe 1 registro Modbus tipo bit en un dispositivo Modbus TCP
Parámetros: ip: (String) dirección IP del dispositivo Modbus TCP
port: (int) puerto TCP del dispositivo Modbus TCP
command: (int) comando Modbus (5)
start: (int) dirección de registro bit inicial a escribir
values: (int) valor a escribir (0,1)
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: ---
- Función:** **mtx.modbusSaveWord(idRegister, registerValue)**
Descripción: escribe un valor de tipo word en la zona de memoria de usuario
Parámetros: idRegister: (int) dirección del registro (10000 ... 19999)
registerValue: (int) valor del registro (0 ... 65535)
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: ---
- Función:** **mtx.modbusSaveDWord(idRegister, registerValue)**
Descripción: escribe un valor de tipo double word en la zona de memoria de usuario
Parámetros: idRegister: (int) dirección del registro (10000 ... 19999)
registerValue: (long) valor del registro (0 ... 4294967295)
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 49
- Función:** **mtx.modbusReadWord(idRegister)**
Descripción: lee un valor de tipo word de la zona de memoria de usuario
Parámetros: idRegister: (int) dirección del registro (10000 ... 19999)
Respuesta: int: valor del registro leído (0 ... 65535)

-1: error
Notas: consulte los ejemplos: ---

- **Función:** **mtx.modbusReadDWord(idRegister)**
Descripción: lee un valor de tipo double word de la zona de memoria de usuario
Parámetros: idRegister: (int) dirección del registro (10000 ... 19999)
Respuesta: long: valor del registro leído (0 ... 4294967295)
-1: error
Notas: consulte los ejemplos: ---

Funciones relacionadas con MODBUS EXPERT:

- **Función:** **mtx. modbusExpertGetStatus (deviceName)**
Descripción: devuelve si la última lectura del dispositivo Modbus Expert fue correcta.
Parámetros: deviceName: (String) Nombre del dispositivo Modbus Expert.
Respuesta: boolean: (true=sin errores de lectura, false=error de lectura o dispositivo no encontrado)
Notas: consulte el ejemplo 62
- **Función:** **mtx. modbusExpertGetV(deviceName, indexV)**
Descripción: devuelve el valor bruto de un registro de un dispositivo Modbus Expert a partir de su índice V[x].
Parámetros: deviceName: (String) Nombre del dispositivo Modbus Expert.
indexV: (int) Índice V del registro.
Respuesta: String: valor del registro.
null: error.
Notas: consulte el ejemplo 62
- **Función:** **mtx. modbusExpertGetVS(deviceName, indexV)**
Descripción: devuelve el valor de un registro de un dispositivo Modbus Expert, a partir de su índice V[x], después de aplicar el script de conversión asociado al registro.
Parámetros: deviceName: (String) Nombre del dispositivo Modbus Expert.
indexV: (int) Índice V del registro.
Respuesta: String: valor del registro tras aplicar el script.
null: error.
Notas: consulte el ejemplo 62
- **Función:** **mtx. modbusExpertGetReg(deviceName, registerAddress)**
Descripción: devuelve el valor bruto de un registro de un dispositivo Modbus Expert a partir de su dirección Modbus.
Parámetros: deviceName: (String) Nombre del dispositivo Modbus Expert.
registerAddress: (int) dirección del registro Modbus.
Respuesta: String: valor del registro.
null: error.
Notas: consulte el ejemplo 62

- Función:** **mtx. modbusExpertGetRegS(deviceName, registerAddress)**
Descripción: devuelve el valor de un registro de un dispositivo Modbus Expert, a partir de su dirección Modbus, después de aplicar el script de conversión asociado al registro.
Parámetros: deviceName: (String) Nombre del dispositivo Modbus Expert.
registerAddress: (int) dirección del registro Modbus.
Respuesta: String: valor del registro tras aplicar el script.
null: error.
Notas: consulte el ejemplo 62
- Función:** **mtx. modbusExpertSetV(deviceName, indexV, value)**
Descripción: escribe un valor en un registro de un dispositivo Modbus Expert a partir de su índice V[x].
Parámetros: deviceName: (String) Nombre del dispositivo Modbus Expert.
indexV: (int) índice V del registro.
value: (String) valor a escribir.
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte el ejemplo 62
- Función:** **mtx. modbusExpertSetReg(deviceName, registerAddress, value)**
Descripción: escribe un valor en un registro de un dispositivo Modbus Expert a partir de su dirección Modbus.
Parámetros: deviceName: (String) Nombre del dispositivo Modbus Expert.
registerAddress: (int) dirección del registro Modbus.
value: (String) valor a escribir.
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte el ejemplo 62
- Función:** **mtx. modbusExpertGet.Json(deviceName)**
Descripción: devuelve un JSON con los valores actuales de un dispositivo Modbus Expert utilizando la última lectura realizada por el servicio Modbus Expert.
Parámetros: deviceName: (String) Nombre del dispositivo Modbus Expert.
Respuesta: String: String con el JSON del dispositivo.
null: error.
Notas: consulte el ejemplo 62
- Función:** **mtx. modbusExpertReadJson(deviceName)**
Descripción: fuerza una lectura real Modbus del dispositivo Modbus Expert y devuelve un JSON con los valores obtenidos.
Parámetros: deviceName: (String) Nombre del dispositivo Modbus Expert.
Respuesta: String: String con el JSON del dispositivo.
null: error.
Notas: consulte el ejemplo 62

Funciones relacionadas con contadores IEC-102:

- Función:** `mtx.iec102AddMeter(idMeter,linkAddress,measAddress,password)`
Descripción: Añade un contador al gestor de contadores. Máximo 100.
Parámetros:
idMeter (String) identificador del contador
linkAddress (int) dirección de enlace del contador
measAddress (int) dirección de punto de medida del contador
password (long) password del contador

Respuesta: boolean
true: contador añadido correctamente.
false: error
Notas: consulte los ejemplos: 32, 47, 48, 49
- Función:** `mtx.iec102AddMeter(idMeter,linkAddress,measAddress,password, ip, tcpPort)`
Descripción: Añade un contador a leer conexión TCP/IP (Ethernet) al gestor de contadores. Máximo 100.
Parámetros:
idMeter (String) identificador del contador
linkAddress (int) dirección de enlace del contador
measAddress (int) dirección de punto de medida del contador
password (long) password del contador
ip (String) IP del contador
tcpPort (int) puerto tcp de lectura del contador

Respuesta: boolean
true: contador añadido correctamente.
false: error
Notas: consulte los ejemplos: 32b
- Función:** `mtx.iec102DeleteAllMeters()`
Descripción: Elimina todos los contadores del gestor de contadores.
Parámetros:
Respuesta: boolean
true: contadores eliminados correctamente.
false: error
Notas: consulte los ejemplos: 32, 47, 48, 49
- Función:** `mtx.iec102GetAllMeters()`
Descripción: Devuelve una lista con todos los contadores almacenados en el gestor de contadores.
Parámetros:
Respuesta: ArrayList [] Lista con todos los identificadores de los contadores
Notas: consulte los ejemplos: 48, 49
- Función:** `mtx.iec102GetPresence()`
Descripción: Comprueba la presencia de un contador
Parámetros: idMeter (String) identificador del contador
Respuesta: int
-2: no inicializado todavía
-1: bus ocupado con lectura
0: contador detectado
>0: error
Notas: consulte los ejemplos: 47

- Función:** **mtx.iec102SetInstantValues(idMeter)**
Descripción: ejecuta la orden de leer los valores instantáneos del contador.
Parámetros: idMeter (String) identificador del contador
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 32, 48, 69
- Función:** **mtx.iec102GetInstantValues(idMeter)**
Descripción: lee los valores instantáneos del contador
Parámetros: idMeter (String) identificador del contador
Respuesta: String JSON con los datos leídos del contador
 ""
 ERROR
Notas: consulte los ejemplos: 32, 48, 69
- Función:** **mtx.iec102SetFiscalClose(idMeter, hourIni, minuteIni, dayIni, monthIni, yearIni, hourEnd, minuteEnd, dayEnd, monthEnd, yearEnd)**
Descripción: ejecuta la orden de lectura de los cierres fiscales
Parámetros: idMeter (String) identificador del contador
 hourIni (int) hora inicial (0 ... 23)
 minuteIni (int) minuto inicial (0 ... 59)
 dayIni (int) día inicial (1 ... 31)
 monthIni (int) mes inicial (1 ... 12)
 yearIni (int) año inicial (22 ... 99)
 hourEnd (int) hora final (0 ... 23)
 minuteEnd (int) minuto final (0 ... 59)
 dayEnd (int) día final (1 ... 31)
 monthEnd (int) mes final (1 ... 12)
 yearEnd (int) año final (22 ... 99)
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: ---
- Función:** **mtx.iec102GetFiscalClose(idMeter)**
Descripción: lee los valores de cierre del contador
Parámetros: idMeter (String) identificador del contador
Respuesta: String JSON con los datos leídos del contador
 ""
 ERROR
Notas: consulte los ejemplos: ---
- Función:** **mtx.iec102SetIntegratedTotal(idMeter, hourIni, minuteIni, dayIni, monthIni, yearIni, hourEnd, minuteEnd, dayEnd, monthEnd, yearEnd, mode, period)**
Descripción: ejecuta la orden de lectura de los totales integrados (curva de carga)
Parámetros: idMeter (String) identificador del contador
 hourIni (int) hora inicial (0 ... 23)
 minuteIni (int) minuto inicial (0 ... 59)
 dayIni (int) día inicial (1 ... 31)
 monthIni (int) mes inicial (1 ... 12)
 yearIni (int) año inicial (22 ... 99)
 hourEnd (int) hora final (0 ... 23)

minuteEnd	(int) minuto final (0 ... 59)
dayEnd	(int) día final (1 ... 31)
monthEnd	(int) mes final (1 ... 12)
yearEnd	(int) año final (22 ... 99)
mode	(int) 0 = absoluto, 1 = incremental
period	(int) 0 = horario, 1 = cuartohorario

Respuesta: boolean: (true=operación OK, false=operación ERROR)

Notas: consulte los ejemplos: 52

- Función:** **mtx.iec102GetIntegratedTotal(idMeter)**
Descripción: lee los valores de totales integrados (curva de carga) del contador
Parámetros: idMeter (String) identificador del contador
Respuesta: String JSON con los datos leídos del contador
" " ERROR
Notas: consulte los ejemplos: 52

Funciones relacionadas con GPS:

- Función:** **mtx.gpsGetData()**
Descripción: devuelve la posición GPS actual del equipo basado en TITAN.
Parámetros: Ninguno
Respuesta: String JSON con los datos GPS
" " ERROR (si no se detectan tramas NMEA)
Notas: consulte los ejemplos: 33

Funciones relacionadas con el LOGGER:

- Función:** **mtx.loggerWrite(data)**
Descripción: escribe datos en el Logger interno del equipo basado en TITAN
Parámetros: data: (String) datos a almacenar en el logger
Respuesta: boolean true = operación correcta
false = error (por ejemplo, longitud de datos mayor que el tamaño del registro del Logger).
Notas: consulte los ejemplos: 26

Funciones relacionadas con FICHEROS:

- Función:** **mtx.fileWrite(index, data, append)**
Descripción: escribe datos en un fichero dentro del equipo basado en TITAN
Parámetros: index: (int) índice del fichero (0 ... 9)
data: (String) datos a escribir en el fichero
append: (boolean) true=añade el texto al fichero existente
false=borra el fichero y graba el texto

Respuesta: boolean true = operación correcta
false = error (por ejemplo, longitud de datos del fichero mayor a 100KB).

Notas: consulte los ejemplos: 27, 28, 30

- Función:** **mtx.fileRead(index)**

Descripción: lee datos de un fichero del equipo basado en TITAN

Parámetros: index: (int) índice del fichero (0 ... 9)

Respuesta: String datos contenidos en el fichero

Notas: consulte los ejemplos: 27, 29
- Función:** **mtx.fileSize(index)**

Descripción: devuelve la longitud de datos de un fichero

Parámetros: index: (int) índice del fichero (0 ... 9)

Respuesta: long tamaño del fichero (en bytes)

Notas: consulte los ejemplos: 28, 30
- Función:** **mtx.fileFtpDownload(tls, index, server, port, username, pass, remoteFile, timeout, addExtension)**

Descripción: recibe un fichero de datos del TITAN de un servidor remoto por FTP

Parámetros: tls: (int) 0=FTP, 1=FTPS
index: (int) índice del fichero (0 ... 9) donde guardar los datos
server: (String) IP o DNS del servidor FTP remoto
port: (int) 0 ... 65535
username: (String) Username del servidor FTP
pass: (String) Password del servidor FTP
remoteFile: (String) Fichero remoto que debe descargarse
timeout: (int) Segundos de timeout para completar descarga
addExtension: (String) Si se descarga el fichero se añade esta extensión

Respuesta: boolean true = operación correcta
false = error

Notas: consulte los ejemplos: 29
- Función:** **mtx.fileFtpUpload(tls, index, server, port, username, pass, remoteFile, timeout)**

Descripción: envía un fichero de datos del TITAN a un servidor remoto por FTP

Parámetros: tls: (int) 0=FTP, 1=FTPS
index: (int) índice del fichero (0 ... 9)
server: (String) IP o DNS del servidor FTP remoto
port: (int) 0 ... 65535
username: (String) Username del servidor FTP
pass: (String) Password del servidor FTP
remoteFile: (String) Fichero remoto que debe descargarse
timeout: (int) Segundos de timeout para completar el envío

Respuesta: boolean true = operación correcta
false = error

Notas: consulte los ejemplos: 28, 30

- Función:** **mtx.fileFtpRename(tls, server, port, username, pass, currentFileName, newFileName, timeout)**
Descripción: envía un fichero de datos del TITAN a un servidor remoto por FTP
Parámetros:
 - tls: (int) 0=FTP, 1=FTPS
 - server: (String) IP o DNS del servidor FTP remoto
 - port: (int) 0 ... 65535
 - username: (String) Username del servidor FTP
 - pass: (String) Password del servidor FTP
 - currentFileName (String) Nombre fichero remoto actual
 - newFileName (String) Nombre fichero remoto nuevo
 - timeout: (int) Segundos de timeout para completar la operación**Respuesta:** boolean
true = operación correcta
false = error
Notas: consulte los ejemplos: ---
- Función:** **mtx.scriptFtpDownload(tls, server, port, username, pass, remoteFile, timeout, addExtension)**
Descripción: descarga el fichero de script de un servidor FTP
Parámetros:
 - tls: (int) 0=FTP, 1=FTPS
 - server: (String) IP o DNS del servidor FTP remoto
 - port: (int) 0 ... 65535
 - username: (String) Username del servidor FTP
 - pass: (String) Password del servidor FTP
 - remoteFile: (String) Script remoto que debe descargarse
 - timeout: (int) Segundos de timeout para completar descarga
 - addExtension: (String) Si se descarga el fichero se añade esta extensión**Respuesta:** boolean
true = operación correcta
false = error
Notas: consulte los ejemplos: 31

Funciones relacionadas con el MODEM:

- Función:** **mtx.imeiCheck(imei, message)**
Descripción: comprueba si el IMEI pasado como parámetro es correcto
Parámetros:
 - imei: (String) imei a comprobar
 - message: (String) mensaje a devolver si es incorrecto**Respuesta:** void
Notas: consulte los ejemplos: 25
- Función:** **mtx.imeiGet()**
Descripción: devuelve el IMEI del módem interno del equipo basado en TITAN
Parámetros: Ninguno
Respuesta: String El imei del módem interno del equipo basado en TITAN
Notas: consulte los ejemplos: 30

Funciones relacionadas con OTAP:

- **Función:** `mtx.otapFTPConfig(tls, server, port, user, pass, remoteConfigFile, secTimeout, addExtension);`
Descripción: ejecuta un comando de descarga de configuración remota por FTP/FTPS. Si la configuración es descargada correctamente, es posible renombrar el fichero remoto (para que no se vuelva a descargar) e instalar la configuración.
Parámetros:
tls: (int) 0=no TLS, 1= sí TLS
server: (String) servidor FTP
port: (int) puerto FTP
user: (String) username de FTP
pass: (String) password de FTP
remoteConfigFile: (String) fichero remoto (ej: path1/path2/fichero)
sectimeout: (int) segundos de timeout
addExtension: (String) Si se descarga se añade esta extensión al fichero remoto (para que no se vuelva a descargar)
Respuesta: boolean true=proceso iniciado , false; proceso no iniciado
Notas: consulte los ejemplos: 37
- **Función:** `mtx.otapFTPLastStatus()`
Descripción: devuelve el estado actual de un proceso de OTAP
Parámetros:
Respuesta: int 0=none, 1=running, 2=OK, 3=ERROR
Notas: consulte los ejemplos: 37

Funciones relacionadas con el WATCHDOG:

- **Función:** `mtx.watchdogSet(mode, timeout)`
Descripción: inicializa el watchdog
Parámetros:
int mode: (int) 0=mode reset
timeout: (int) Segundos para reset si no hay refresco (0, 30 ... 100000). 0=Desactivado.
Respuesta: boolean true=OK, false: ERROR
Notas: consulte los ejemplos: 20
- **Función:** `mtx.watchdogKick()`
Descripción: refresca el watchdog para que no reinicie el módem
Parámetros: Ninguno
Respuesta: boolean true=OK, false: ERROR
Notas: consulte los ejemplos: 20

Funciones relacionadas con tiempo:

- **Función:** `mtx.pause(mseconds)`
Descripción: crea una pausa de los milisegundos configurados

- Parámetros:** mseconds (long) milisegundos de espera
Respuesta: boolean true = operación correcta
false = error
Notas: consulte los ejemplos: 1, 2, 3, 4, 5, ... , 35
- Función:** **mtx.timeStamp()**
Descripción: devuelve la fecha y hora del equipo basado en TITAN
Parámetros: Ninguno
Respuesta: String fecha y hora del equipo basado en TITAN
Notas: consulte los ejemplos: 28, 30
 - Función:** **mtx.timeGetYear()**
Descripción: devuelve el año
Parámetros: Ninguno
Respuesta: int año actual con cuatro dígitos
Notas: consulte los ejemplos: ---
 - Función:** **mtx.timeGetMonth()**
Descripción: devuelve el mes
Parámetros: Ninguno
Respuesta: int mes actual (1=Enero ... 12=Diciembre)
Notas: consulte los ejemplos: ---
 - Función:** **mtx.timeGetDay()**
Descripción: devuelve el día
Parámetros: Ninguno
Respuesta: int día actual (1 ... 31)
Notas: consulte los ejemplos: ---
 - Función:** **mtx.timeGetHour()**
Descripción: devuelve la hora
Parámetros: Ninguno
Respuesta: int hora actual (0 ... 23)
Notas: consulte los ejemplos: ---
 - Función:** **mtx.timeGetMinute()**
Descripción: devuelve los minutos
Parámetros: Ninguno
Respuesta: int minuto actual (0 ... 59)
Notas: consulte los ejemplos: ---
 - Función:** **mtx.timeGetSecond()**
Descripción: devuelve los segundos
Parámetros: Ninguno
Respuesta: int segundo actual (0 ... 59)
Notas: consulte los ejemplos: ---

Funciones relacionadas con Sockets:

- **Función:** **mtx. socketOpen (idSocket,ssl,ip,port)**
Descripción: Abre un socket TCP Cliente contra una IP/DNS
Parámetros: idSocket (int) identificador de socket (0 ... 9)
ssl (int) 0=no, 1=sí
idSocket (String) Dirección IP o DNS del servidor remoto
puerto TCP (int) Puerto TCP del servidor remoto (0 ... 65535)
Respuesta: boolean true = operación correcta
false = error
Notas: consulte los ejemplos: 45, 46
- **Función:** **mtx. socketClose (idSocket)**
Descripción: Cierra un socket TCP Cliente
Parámetros: idSocket (int) identificador de socket (0 ... 9)
Respuesta: boolean true = operación correcta
false = error
Notas: consulte los ejemplos: 45, 46
- **Función:** **mtx. socketIsOpen(idSocket)**
Descripción: Comprueba si un socket TCP Cliente tiene una conexión establecida
Parámetros: idSocket (int) identificador de socket (0 ... 9)
Respuesta: boolean true = sí, hay una conexión establecida
false = no, no hay una conexión establecida.
Notas: consulte los ejemplos: 45, 46
- **Función:** **mtx. socketSend(idSocket, data[])**
Descripción: envía datos a través de un socket TCP/IP
Parámetros: idSocket (int) identificador de socket (0 ... 9)
values[]: (byte[]) array con los bytes a enviar
Respuesta: boolean: (true=operación OK, false=operación ERROR)
Notas: consulte los ejemplos: 45, 46
- **Función:** **mtx. socketIsData(idSocket)**
Descripción: Comprueba si hay datos pendientes de leer en un socket TCP Cliente
Parámetros: idSocket (int) identificador de socket (0 ... 9)
Respuesta: boolean true = hay datos pendientes
false = no hay datos pendientes
Notas: consulte los ejemplos: 45, 46
- **Función:** **mtx. socketRead(idSocket)**
Descripción: Lee los bytes disponibles en un socket TCP Cliente
Parámetros: idSocket (int) identificador de socket (0 ... 9)
Respuesta: byte[] Array de bytes con los datos recibidos
null: error
Notas: consulte los ejemplos: 45, 46

Funciones de conversion de Datos:

- Función:** **mtx.convert2WordToUnsignedInt32 (word1, word2)**
Descripción: convierte 2 word a formato unsigned integer de 32 bits
Parámetros: word1 (int) 0 ... 65535
word2 (int) 0 ... 65535
Respuesta: unsigned int32 0 ... 4294967295
Notas: consulte los ejemplos: 14c
- Función:** **mtx.convert2WordToSignedInt32 (word1, word2)**
Descripción: convierte 2 word a formato signed integer de 32 bits
Parámetros: word1 (int) 0 ... 65535
word2 (int) 0 ... 65535
Respuesta: signed int32 -2147483648 ... 2147483647
Notas: consulte los ejemplos: 14c
- Función:** **mtx.convert2WordToFloat (word1, word2)**
Descripción: convierte 2 word a formato float
Parámetros: word1 (int) 0 ... 65535
word2 (int) 0 ... 65535
Respuesta: Float -3.4028235x10³⁸ ... 3.4028235x10³⁸
Notas: consulte los ejemplos: 14c
- Función:** **mtx.convert4WordToSignedInt64 (word1, word2, word3, word4)**
Descripción: convierte 4 word a formato signed integer de 64 bits
Parámetros: word1 (int) 0 ... 65535
word2 (int) 0 ... 65535
word3 (int) 0 ... 65535
word4 (int) 0 ... 65535
Respuesta: String -9223372036854775808 ... 9223372036854775807
Notas: consulte los ejemplos: 14c
En valor se devuelve en formato String porque javascript no soporta enteros de 64 bits. Útil para conformar JSONs de envío a plataformas.
- Función:** **mtx.convert4WordToDouble (word1, word2, word3, word4)**
Descripción: convierte 4 word a formato Double de 64 bits
Parámetros: word1 (int) 0 ... 65535
word2 (int) 0 ... 65535
word3 (int) 0 ... 65535
word4 (int) 0 ... 65535
Respuesta: Double -4.9x10³²⁴ ... 1.7976931348623157x10³⁰⁸
Notas: consulte los ejemplos: 14c

Funciones para la comunicación con la API de chatGPT

- Función:** **mtx.chatGPTInit(apiURL,apiKey)**
Descripción: Inicializa la configuración de comunicación con la API de chatGPT
Parámetros: apiURL (String) URL de la API de chatGPT
apiKey (String) API KEY de la API de chatGPT

Respuesta: boolean true = operación correcta
false = error
Notas: consulte los ejemplos: 57, 58, 59

- **Función:** **mtx.chatGPTGetTextResponse(apiModel,numTokens,prompt)**

Descripción: realiza una consulta a chatGPT

Parámetros: apiModel (String) Modelo de IA a utilizar de chatGPT
numTokens (int) número de tokens máximo a utilizar
prompt (String) Texto de consulta para chatGPT

Respuesta: String Respuesta de chatGPT a la pregunta.
"ERROR" = error

Notas: consulte los ejemplos: 57, 58, 59

- **Función:** **mtx.chatGPTGetImageResponse(apiModel,numTokens,prompt, locallImage, imageURL, urlUsername, urlPassword)**

Descripción: realiza una consulta a chatGPT sobre una imagen de una URL. Esa URL puede ser una imagen local tomada de una cámara web que devuelva una URL con la imagen captada o una imagen de internet. La diferencia radica que en la imagen local la imagen tiene que ser subida a chatGPT.

Parámetros: apiModel (String) Modelo de IA a utilizar de chatGPT
numTokens (int) número de tokens máximo a utilizar
prompt (String) Texto de consulta para chatGPT sobre la imagen
locallImage (boolean) "true" si la imagen es local y debe ser subida a chatGPT o "false" si la imagen está en Internet accesible por chatGPT.

imageURL (String): url a la imagen

urlUsername (String): en caso necesario, el username para poder acceder a la imagen con una autenticación básica HTTP.

urlPassword (String): en caso necesario, el password para poder acceder a la imagen con una autenticación básica HTTP.

Respuesta: String Respuesta de chatGPT a la pregunta.
"ERROR" = error

Notas: consulte los ejemplos: 57, 58, 59

Funciones VARIAS:

- **Función:** **mtx.hashSHA256(text)**

Descripción: devuelve el hash SHA256 de un texto

Parámetros: text (String) Texto a calcular el hash

Respuesta: String hash SHA256 del texto indicado.

Notas: consulte los ejemplos: ---

- **Función:** **mtx.mobileGetIP()**

Descripción: devuelve la dirección IP asociada a Mobile WAN

Parámetros: Ninguno

- Respuesta:** String ""= Ninguna, "x.x.x.x"
- Notas:** consulte los ejemplos: ---
- Función:** **mtx.powerStatus()**

Descripción: devuelve si el router dispone de alimentación externa. Útil para los equipos con batería interna o supercap.

Parámetros: Ninguno

Respuesta: int 0=no, 1=sí, -1=error

Notas: consulte los ejemplos: 6
 - Función:** **mtx.println(data)**

Descripción: envía datos de texto a la consola de debug

Parámetros: data (String) datos de texto a escribir por consola

Respuesta: void

Notas: consulte los ejemplos: 1, 2, 3, 4, 5, ... , 35
 - Función:** **mtx.ping(ip, timeout)**

Descripción: genera un ping a una IP o DNS remota

Parámetros: ip (String) IP o DNS remota para efectuar el PING
timeout (int) milisegundos de timeout

Respuesta: boolean true = ping correcto
false = ping error

Notas: consulte los ejemplos: 17
 - Función:** **mtx.base64Encode(data)**

Descripción: codifica un array de bytes en base64

Parámetros: data (byte[]) array de bytes a codificar

Respuesta: String datos codificados en base64
""= error

Notas: consulte los ejemplos: 26
 - Función:** **mtx.stringToByteArray(data)**

Descripción: convierte un String en un array de bytes

Parámetros: data (String) datos a convertir a array de bytes

Respuesta: byte[] array de bytes
null = error

Notas: consulte los ejemplos: 51
 - Función:** **mtx.byteArrayToString (data, init, length)**

Descripción: convierte un array de bytes en un String

Parámetros: data (byte[]) array de bytes
init (int) posición
length (int) número de bytes a convertir

Respuesta: String String con la conversión
"" = error

Notas: consulte los ejemplos: ---
 - Función:** **mtx.configParamGet(paramName)**

Descripción: Lectura del valor de un parámetro de configuración del Titan

Parámetros: paramName (String) Nombre del parámetro de configuración
Respuesta: String Valor del parámetro de configuración.

Notas: consulte los ejemplos: ---

- **Función:** **mtx.configParamSet(paramName,paramValue)**
Descripción: Escritura del valor de un parámetro de configuración del Titan
Parámetros: paramName (String) Nombre del parámetro de configuración
: paramValue (String) Valor del parámetro de configuración
Respuesta: boolean true = operación correcta
false = error
Notas: consulte los ejemplos: ---

Listado de Ejemplos.

En el entorno WEB de configuración del router, en la sección “Other → TITAN Scripts”, encontrará una serie de ejemplos de scripts. A continuación se muestra una descripción breve de cada uno de ellos.

Example 1.- Hello World

Ejemplo básico de cómo escribir trazas de debug por la salida estándar.

Example 2.- Request AT Command

Ejemplo que muestra cómo enviar comandos AT al módem interno del equipo (para obtener la cobertura, la identificación de la celda de telefonía usada, ...)

Example 3.- Send SMS when GPIO change

Ejemplo de cómo enviar un mensaje SMS cuando se detecta un cambio en una entrada digital del equipo.

Example 4.- Send MQTT message to broker

Ejemplo de cómo enviar un mensaje MQTT al broker al que está conectado el equipo.

Example 5.- Send SNMP TRAP

Ejemplo de cómo enviar un TRAP SNMP.

Example 6.- Send EMAIL when power fails

Ejemplo de cómo enviar un email. En este ejemplo el envío del email se produce cuando se detecta un fallo de alimentación. Ejemplo sólo válido para los modelos de router que dispongan de batería interna o supercap.

Example 7.- Read Modbus RTU word register

Ejemplo de cómo leer un registro Modbus RTU de tipo WORD desde los TITAN scripts.

Example 7b.- Read Modbus TCP word register

Ejemplo de cómo leer un registro Modbus TCP de tipo WORD desde los TITAN scripts.

Example 8.- Read Modbus RTU word register and send by MQTT

Ejemplo que muestra cómo lee un registro Modbus de tipo WORD y enviar el dato leído a un topic MQTT.

Example 9.- Read Modbus RTU word register and send TRAP

Ejemplo que muestra cómo lee un registro Modbus de tipo WORD y enviar un TRAP SNMP en función del valor del registro leído.

Example 10.- Read Modbus RTU word register and send SMS

Ejemplo que muestra cómo lee un registro Modbus de tipo WORD y enviar un SMS en función del valor del registro leído.

Example 11.- Read Modbus RTU word register and send EMAIL

Ejemplo que muestra cómo lee un registro Modbus de tipo WORD y enviar un EMAIL en función del valor del registro leído.

Example 12.- Write Modbus RTU word registers

Ejemplo que muestra cómo escribir en un registro Modbus de tipo WORD.

Example 13.- Read Modbus RTU bit register

Ejemplo que muestra cómo leer un registro Modbus de tipo bit.

Example 14.- Write Modbus RTU bit register

Ejemplo que muestra cómo escribir en un registro Modbus de tipo bit.

Example 14b.- Read Modbus RTU word registers, save data in LOGGER for scheduled sending

Ejemplo que muestra cómo leer registros modbus RTU de un dispositivo externo vía puerto serie RS485, crear un JSON con una estructura de datos personalizada y almacenar dicho JSON en el datalogger del Titan para que sea enviado mediante el método configurado (MQTT, HTTP, FTP).

Example 14c.- Convert Modbus word registers into Unsigned Int32, Signed Int32, Float, Int64

Ejemplo que muestra cómo leer registros modbus RTU de un dispositivo externo vía puerto serie RS485 como WORD y transformarlos en tipos unsigned integer de 32bits, signed integer de 32bits, float y signed integer de 64bits.

Example 15.- Read all Digital Inputs

Ejemplo que muestra cómo leer todas las IOs (entrada y/o salidas digitales) del equipo. Sólo válido para aquellos equipos que dispongan de entradas y/o salidas digitales.

Example 16.- Write Digital Output

Ejemplo que muestra cómo cambiar el estado de una salida digital del equipo. Sólo válido para aquellos equipos que dispongan de salidas digitales.

Example 17.- Ping ip and send SMS if problem with Ping

Ejemplo que muestra cómo realizar un PING a un dispositivo conectado al equipo y enviar un SMS en caso de problemas con el PING, por ejemplo para detectar el mal funcionamiento de un equipo conectado.

Example 18.- Send SMS Alarm when Backup SIM 2 is being used

Ejemplo que envía un SMS de aviso cuando la SIM secundaria entra en funcionamiento. Únicamente válido para equipos con DUAL SIM.

Example 19.- Read and Write data from SERIAL PORT

Ejemplo que muestra cómo hacer lecturas y escrituras en un puerto serie. Ejemplo válido únicamente para equipos que dispongan de uno o más puertos serie RS232 y/o RS485

Example 20.- Use of WATCHDOG

Ejemplo que muestra cómo utilizar el watchdog de los TITAN Scripts. Reinicio en caso de problemas de funcionamiento del script.

Example 21.- Use of LEDs for custom indications

Ejemplo que muestra cómo utilizar los LEDs de forma customizada, gestionando el encendido y apagado desde un script.

Example 22.- TITAN as MODBUS concentrator saving data into internal memory

Ejemplo que muestra cómo utilizar el equipo como concentrador Modbus guardando los datos leídos en memoria interna. Por ejemplo, es posible leer de forma autónoma diferentes sensores Modbus RTU y almacenar los registros leídos en diferentes posiciones dentro de la memoria del equipo y, desde una ubicación remota, leer vía Modbus TCP los datos de los registros almacenados dentro del equipo.

Example 23.- Exchanging data through AT Commands sent by SMS, MQTT, Telnet, SSH, HTTP ...

Ejemplo que muestra cómo intercambiar datos mediante comandos AT desde los scripts enviados por SMS, MQTT, Telnet, etc. Es decir, usted puede enviar un comando AT vía SMS, MQTT, Telnet, etc al equipo y desde el script programado por usted podrá recibir dichos datos y actuar en consecuencia.

Example 24.- Encrypting the code of Script

Ejemplo que muestra cómo encriptar el código de un script. Por ejemplo, si va a suministrar a un tercero un equipo con un script preprogramado y no desea mostrar el código fuente, puede encriptar el script tal y como se indica en este ejemplo.

Example 25.- Encrypting the code of Script and avoid the Piracy of the Script

Ejemplo que muestra cómo encriptar el código de un script. Por ejemplo, si va a suministrar a un tercero un equipo con un script preprogramado y no desea mostrar el código fuente para que no se lo copien o pirateen, puede encriptar el script tal y como se indica en este ejemplo.

Example 26.- Saving DATA into the internal TITAN LOGGER.

Ejemplo que muestra cómo almacenar datos en la memoria interna del equipo. De esa manera se aprovechará de los mecanismos automáticos del equipo con su memoria para el envío de los datos a un broker MQTT, servidor HTTP, etc.

Example 27.- Use of user FILES for read, write and append data.

Ejemplo que muestra cómo crear ficheros de usuario para escribir, leer y añadir datos.

Example 28.- Uploading user FILES by FTP

Ejemplo que muestra cómo enviar archivos de usuario por FTP.

Example 29.- Downloading user FILES by FTP

Ejemplo que muestra cómo recibir archivos de usuario por FTP.

Example 30.- Read Modbus RTU, save data into FILE, and send it by FTP

Ejemplo que muestra cómo leer datos Modbus RTU desde un script, guardar los datos en un fichero de usuario y enviar dicho fichero por FTP.

Example 31.- Download and install new version of SCRIPT from FTP Server

Ejemplo que muestra cómo actualizar de forma remota un script de usuario.

Example 32.- Read instant values of IEC-60870-5-102 Meter

Ejemplo que muestra cómo leer los valores instantáneos de un contador de energía con protocolo IEC-60870-5-102 desde un script.

Example 33.- Read GPS data from TITAN

Ejemplo que muestra cómo obtener la posición GPS desde un script. Sólo válido para aquellos equipos que dispongan de GPS.

Example 34.- Read digital COUNTERS

Ejemplo que muestra cómo leer el valor de los contadores de pulsos. Sólo válido para aquellos equipos que dispongan de entradas digitales.

Example 35.- Subscribe a MQTT topic. Read and Send byte array data

Ejemplo que muestra cómo suscribirse a un tópic MQTT para recibir un array de datos.

Example 36.- IO Line Passing by MQTT. Send digital input status to remote digital output.

Ejemplo pensado para utilizar 2 equipos basados en TITAN que dispongan de entradas / salidas digitales. Cuando se produzca un cambio de estado en una ENTRADA digital de un equipo, en el equipo remoto se cambiará el estado de una SALIDA digital. Es decir, es muestra cómo replicar una entrada digital en una salida digital remota.

Example 37.- Check and download by FTPS a remote router Configuration.

En este ejemplo se muestra como es posible hacer que un equipo basado en TITAN se descargue un fichero de backup de configuración por FTPS. El router se descarga el fichero, lo renombra en el servidor remoto (para no volverlo a descargar) e instala la configuración descargada.

Example 38.- Download by FTPS a remote file with AT inside and execute them

En este ejemplo se muestra como es posible hacer que un equipo basado en TITAN se descargue un fichero con comandos AT en su interior por FTPS. Una vez descargado el fichero el equipo basado en TITAN ejecutará los comandos AT leídos del mismo.

Example 39.- Send data by HTTP GET and HTTP POST with custom headers

Ejemplo demostrativo de cómo realizar peticiones HTTP/HTTPS con método GET y POST permitiendo además el uso de headers personalizados.

Example 40.- Read all received SMS from SCRIPT

Ejemplo de cómo leer desde un script todos los SMS que se reciben en el equipo basado en TITAN. Desde el script se puede, una vez recibido el SMS, obtener el número de teléfono del emisor del SMS y el mensaje texto asociado.

Example 41.- Send TELEGRAM message when a GPIO changes.

Ejemplo de cómo enviar un mensaje de texto a un grupo de chat de la aplicación de mensajería Telegram cuando cambia una entrada digital del equipo basado en TITAN. Consultar las notas de aplicación para más información.

Example 42.- Send TELEGRAM message when a MODBUS register changes.

Ejemplo de cómo enviar un mensaje de texto a un grupo de chat de la aplicación de mensajería Telegram cuando cambia el valor de un registro Modbus que lee el equipo basado en TITAN vía Modbus RTU de un dispositivo conectado por puerto RS485. Consultar las notas de aplicación para más información.

Example 43.- Read CellID and get approximate Latitude and Longitude from third party.

Ejemplo de cómo obtener la longitud y la latitud a partir de la información obtenida de la celda de telefonía utilizada por el módem. Adicionalmente se usa la API de una tercera parte.

Example 44.- Read the cheapest energy hour from REE website by HTTP REST api.

Ejemplo de cómo descargar de REE (Red Eléctrica de España) vía HTTP GET (REST API) las tarifas horarias del mercado eléctrico regulado en España. Una vez descargadas las tarifas de precio de la energía por hora, se busca la hora con el precio de la energía más reducido. Se activará la salida digital del equipo únicamente durante esa hora (por ejemplo,

para activar a su vez un termo eléctrico de agua caliente) con el fin de ahorrar al máximo en la factura eléctrica.

Example 45.- Read and send data through a TCP client SOCKET.

Ejemplo de cómo establecer un socket TCP cliente contra un servidor y de cómo enviar y recibir datos a través de él.

Example 46.- Read and send data through a TSSL/TLS CP client SOCKET.

Ejemplo de cómo establecer un socket TCP cliente con seguridad SSL/TLS contra un servidor y de cómo enviar y recibir datos a través de él.

Example 47.- Check presence of IEC-60870-5-102 Meter and send sms alarm if not detected

Ejemplo de cómo comprobar de forma periódica la presencia de un contador IEC-60870-5-102. En caso de fallo de presencia enviará un mensaje SMS de alarma para notificar la situación.

Example 48.- Read instant values of several IEC-60870-5-102 Meters and store data in LOGGER

Ejemplo que muestra cómo leer los valores instantáneos de varios contadores de energía con protocolo IEC-60870-5-102 desde un script. Se almacenarán los datos en el LOGGER interno para poder ser enviados a una plataforma WEB vía HTTP, MQTT ó FTP

Example 49.- Configuration of IEC-60870-5-102 to MODBUS TCP/RTU Gateway

Ejemplo de conversor IEC-60870-5-102 a Modbus. El ejemplo muestra cómo leer los valores instantáneos de un contador con protocolo IEC-60870-5-102 y almacenarlos en la zona de memoria de usuario para poder ser leídos vía modbus TCP o modbus RTU mediante un dispositivo externo (por ejemplo, un PLC).

Example 50.- Communication with ANDROID app by MQTT

Ejemplo que muestra como interaccionar desde un script con una app Android diseñada por el usuario. Es imprescindible consultar la nota de aplicación 61

Example 51.- Forward all received SMS via serial port RS232

Ejemplo que muestra como recibir un mensaje SMS desde un script y reenviar el contenido del mensaje directamente por el puerto serie RS232.

Example 52.- Read INTEGRATED values of IEC-60870-5-102 Meters and store data in LOGGER

Ejemplo que muestra como leer las curvas de carga (valores integrados) de un contador IEC-60870-5-102 cada día a las 2am y almacenar los datos en la memoria LOGGER para que los datos sean enviados automáticamente según configurado (MQTT, HTTP, FTP).

Example 53.- Configuration for DLMS/COSEM to MODBUS TCP/RTU Gateway

Ejemplo de conversor DLMS/COSEM a Modbus. El ejemplo muestra cómo leer los valores instantáneos de un contador con protocolo DLMS/COSEM y almacenarlos en la zona de memoria de usuario para poder ser leídos vía modbus TCP o modbus RTU mediante un dispositivo externo (por ejemplo, un PLC).

Example 54.- Read instant values of a DLMS COSEM meter and store data in LOGGER

Ejemplo que muestra cómo leer los valores instantáneos de un de energía con protocolo DLMS/COSEM desde un script. Se almacenarán los datos en el LOGGER interno para poder ser enviados a una plataforma WEB vía HTTP, MQTT ó FTP

Example 55.- Configure and join with a single ZEROTIER VPN

Ejemplo que muestra cómo configurar y conectarse a una VPN de Zerotier.

Example 56.- Configure and join with a several ZEROTIER VPNs

Ejemplo que muestra cómo configurar y conectarse a tres redes VPN de Zerotier de forma simultánea.

Example 57.- Ask CHATGPT about any question

Ejemplo que muestra como utilizar la API de chatGPT para realizar una pregunta textual y obtener una respuesta. En este ejemplo se pregunta sobre el pais en que se encuentra el dispositivo dadas unas coordenadas GPS.

Example 58.- Ask CHATGPT about what it sees in a remote IMAGE

Ejemplo que muestra como utilizar la API de chatGPT para realizar una pregunta de análisis de una imagen de una URL de Internet. En este ejemplo se pregunta a chatGPT sobre una imagen que representa un atasco de tráfico.

Example 59.- Ask CHATGPT about what it sees in a local IMAGE

Ejemplo que muestra como utilizar la API de chatGPT para realizar una pregunta de análisis de una imagen local tomada desde una cámara web.

Example 60.- Converting Received SNMP TRAPs to SMS Notifications

Ejemplo que muestra cómo iniciar desde un TITAN Script un servicio de recepción de TRAPS SNMP v1/v2c y enviar mensajes SMS cuando se recibe un trap con un OID determinado. El ejemplo permite asociar varios OIDs esperados con distintos textos de alarma y varios números de teléfono destino.

Example 61.- Send MQTT message to primary, secondary or both brokers

Ejemplo que muestra cómo enviar mensajes MQTT desde un TITAN Script seleccionando el bróker de destino: Primary, Secondary o Both. También muestra la compatibilidad de las funciones MQTT clásicas, que continúan utilizando el bróker Primary.

Example 62.- Modbus Expert script functions

Ejemplo que muestra cómo utilizar desde TITAN Scripts las funciones disponibles para Modbus Expert, incluyendo la lectura de valores por índice V, por dirección de registro, la escritura de registros y la obtención del JSON del dispositivo mediante ``mtx.modbusExpertGetJson`` y ``mtx.modbusExpertReadJson``.

JSON Transformer Function Script

La función JSON Transformer script permite cambiar el formato de datos antes de enviarlos a una plataforma WEB vía HTTP, MQTT o FTP. De esta forma puede ajustar el formato de los datos que envía el equipo basado en TITAN al que necesite la plataforma. Consulte la nota de aplicación **ANV6_57-Router-TITAN-Json_Transformer_Script** para una información completa de esta característica.

Other ▶ Titan Scripts v2 ▶ JSON Transformer Function Script

This function script allows to customize json sent by **Logger** and **private DNS** (File: 'script-transf.mtx')

```
function getTransformedJson (json)
{
  1 const objJson = JSON.parse(json);
  2 if (objJson.TYPE=='DNS')
  3 {
  4   objJson.myCustomField1 = 'myCustomValue1';
  5   objJson.myCustomField2 = 'myCustomValue2';
  6 }
  7 else
  8 {
  9   objJson.myCustomField3 = 'myCustomValue3';
 10   objJson.myCustomField4 = 'myCustomValue4';
 11 }
 12 mtx.println("Result: " + JSON.stringify(objJson));
 13 return JSON.stringify(objJson);
 14
}
```

Save JSON Transformer Script Delete JSON Script Load Example Encrypt Script

MQTT Topic Function Script

Esta característica permite ejecutar un script cuando el equipo basado en TITAN recibe datos en unos topics MQTT determinados. De esta manera puede recibir y tratar datos recibidos de una plataforma Web MQTT independientemente del formato de los mismos. Consulte la nora de aplicación **ANV6_58-Router-TITAN-Mqtt_Topic_Function_Script** para una información completa de esta característica.

Other ▶ Titan Scripts v2 ▶ MQTT Topic Function Script

This function script is executed when data is received in **Mqtt Script Topics** (File: 'script-mqtt.mtx')

```
function topicScript (topic, stringData)
{
  1
}
}
```

Save TOPIC Script Delete TOPIC Script Load Example Encrypt Script

NOTA: si se utiliza el cliente MQTT secundario, puede definirse la función ``topicScriptEx(brokerId, topic, data)``. El parámetro ``brokerId`` indica el bróker por el que se ha recibido el mensaje ("primary" o "secondary"). La función clásica ``topicScript(topic, data)`` se mantiene por compatibilidad.

4.8.20 - Other → Connectivity tools

En ocasiones resulta útil conocer el número de la tarjeta SIM insertada en el equipo basado en TITAN o comprobar la conectividad contra una IP o DNS determinada desde el punto de vista del equipo o comprobar la conectividad contra un puerto TCP de un servidor externo o simplemente saber si la sección de configuración de email es correcta. Esta sección dispone de una serie de herramientas básicas para resolver todas esas necesidades.

■ Utilidad “Send SMS”.

► Other ► Tools ► Send SMS

Number: Destination number

Message: SMS Message

Como su propio nombre indica, esta utilidad permite de una forma muy sencilla enviar un mensaje SMS desde un equipo basado en TITAN a un teléfono celular. Puede resultar útil para obtener el número de teléfono de la tarjeta SIM de forma rápida.

■ Utilidad “Send PING”.

► Other ► Tools ► Send PING

Host: IP or DNS

Esta utilidad permite realizar un PING desde el punto de vista del equipo basado en TITAN hacia una determinada IP o DNS, permitiendo comprobar la conectividad entre ambas entidades.

■ Utilidad “Send EMAIL”.

► Other ► Tools ► Send EMAIL

Email: Email address destination

Subject: Subject of email

Note: email settings need to be configured before using this tool

Esta utilidad permite comprobar la correcta configuración para el envío de emails desde el equipo basado en TITAN. Para ello previamente es necesario configurar la sección “Other→Email”.

■ Utilidad “Send TELEGRAM text message”.

► Other ► Tools ► Send TELEGRAM text message

Token ID: Bot token ID

Chat ID: ID of the chat group

Message: Text message for sending

Esta utilidad permite enviar un mensaje de texto a un contacto de Telegram.

■ Utilidad “Check TCP Connection”.

► Other ► Tools ► Check TCP Connection

IP or DNS: IP or DNS of remote host

TCP port: TCP port (1 ... 65535)

ASCII Data: (Optional) Send ascii test data if connection is successful

CHECK CONNECTION

Esta utilidad permite comprobar si un puerto TCP está disponible para conexión desde el punto de vista del equipo basado en TITAN. Para comprobar dicha conectividad el equipo crea un socket TCP Cliente que intenta conectarse contra la IP/DNS y puerto TCP indicados. Si consigue realizar la conexión el resultado se mostrará como satisfactorio. Opcionalmente es posible añadir un campo adicional de datos ASCII que el equipo basado en TITAN utilizará para enviar a través de dicho socket una vez se realice la conexión.

La sección inferior de la pantalla muestra una sección “Results” donde se muestra el resultado de las herramientas anteriores. El siguiente ejemplo muestra el resultado de un intento de conexión a la dirección www.google.com y al puerto TCP 80.

◊ Time Servers
◊ Remote Console
◊ Snmp
◊ Tacacs+
◊ Ldap
◊ Mqtt / Mqtts
◊ Http / Https
◊ User Permissions
◊ Passwords Web UI
◊ CA Certificates
◊ Email Config
◊ ModBus Slave
◊ Titan Scripts
◊ Connectivity tools
◊ Digital I/O
◊ Custom Skin
◊ Led Config
◊ Syslog
◊ Backup / Factory
◊ Firmware Upgrade
◊ Reboot
◊ Logout

► Other ► Tools ► Send TELEGRAM text message

Token ID: Bot token ID

Chat ID: ID of the chat group

Message: Text message for sending

SEND TELEGRAM

► Other ► Tools ► Check TCP Connection

IP or DNS: IP or DNS of remote host

TCP port: TCP port (1 ... 65535)

ASCII Data: (Optional) Send ascii test data if connection is successful

CHECK CONNECTION

► Other ► Tools ► Results

SUCCESSFUL CONNECTION. Connection with IP or DNS (www.google.com:80) can be established

4.8.21- Other → Digital I/O

Muchos modelos de módems y equipos basados en TITAN disponen de entradas y/o salidas digitales. Desde esta sección es posible configurarlas.

The screenshot shows the webdyn TITAN configuration interface. The top header features the webdyn logo (a stylized 'w' with a blue and grey wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". Below the logos, the interface is divided into a left sidebar and a main content area.

Left Sidebar: Contains a list of configuration categories, each with a star icon and a list of sub-items:

- ★ **Mobile**
 - ◆ Status
 - ◆ Basic Settings
 - ◆ Keep Online
- ★ **Ethernet**
 - ◆ Basic Settings
 - ◆ DHCP Server
- ★ **Wifi**
 - ◆ Basic Settings
 - ◆ DHCP Server
- ★ **Firewall**
 - ◆ NAT
 - ◆ Authorized IPs
 - ◆ MAC Filter
 - ◆ Routes
- ★ **Serial Settings**
 - ◆ Serial Port1-RS232
 - ◆ Serial Port2-RS485
 - ◆ SSL Certificates
- ★ **External Devices**
 - ◆ Logger configuration
 - ◆ ModBus Devices
 - ◆ Generic Serial Device
 - ◆ Temperature Sensor
 - ◆ IEC102 Meter
 - ◆ GPS Receiver

Main Content Area: The title bar reads "Other → Digital I/O".

Digital I/O Settings:

- Enable:** A checkbox that is currently unchecked.
- Period:** A dropdown menu set to "Not Logging".
- Text:** "Enable digital inputs and outputs" and "Period (minutes) for saving IO status and counters in Logger. Please, [configure logger](#) before using".
- Button:** "SAVE CONFIG".

Digital Inputs:

- Section Header:** "Other → Digital I/O → Digital Inputs".
- Text:** "Digital Input IO0: [CONFIG](#) Special functions of Digital Input IO-0".

Digital Outputs:

- Section Header:** "Other → Digital I/O → Digital Outputs".
- Text:** "Digital Output IO1: [CONFIG](#) Special functions of Digital Output IO-1".

Remember: you can also use I/O with "[Titan Scripts](#)" for special functionality

- **Enabled.** Activa el servicio de Entradas/Salidas del equipo basado en TITAN. Es necesario activarlo si pretende utilizarlas.
- **Period.** Permite establecer un periodo de tiempo (en minutos) en el que leer las entradas y salidas digitales, así como los contadores de pulsos y almacenar la lectura en el datalogger interno del equipo basado en TITAN para el posterior envío a una plataforma vía HTTP/S o MQTT/S.

Una vez habilitada la opción y reiniciado el equipo podrá configurar el comportamiento de las entradas y salidas digitales pulsando el botón "CONFIG" correspondiente a cada una de ellas. Recuerde que las entradas y salidas digitales pueden ser también gestionadas desde los TITAN Script.

Configuración de las entradas digitales

La pantalla de configuración de las entradas digitales presenta el aspecto siguiente.

The screenshot shows the webdyn TITAN configuration interface. The left sidebar contains a menu with categories: Mobile, Ethernet, Wifi, Firewall, Serial Settings, External Devices, and VPN. The main content area is titled 'Other > Digital I/O > Digital Input IO-0'. It features a 'Digital input mode' dropdown set to 'Normal'. Below this is a section for 'Alarm' configuration, including an 'SMS' checkbox (unchecked), 'Phone numbers' input fields, 'Text SMS Alarm On' and 'Text SMS Alarm Off' input fields, and a 'Logger' checkbox (unchecked). A 'SAVE CONFIG' button is present. At the bottom, there is a 'READ INPUT' button and a status field showing 'ERROR'. The right side of the interface includes descriptive text for each configuration option.

- **Digital input mode.** Indica el comportamiento de la entrada digital. Puede elegir entre “normal” si no quiere utilizar la entrada para alarmas, o bien elegir “Alarm (pin 0 → 1)” ó “Alarm (pin 1 → 0)” si desea configurar una alarma para que se active cuando el valor lógico de la entrada digital pase de 0 a 1 o viceversa.
- **SMS enabled.** Debe activarse si se pretende que el equipo basado en TITAN envíe un mensaje SMS cuando se active o desactive una alarma.
- **Phone numbers.** Introduzca aquí los números de teléfono a donde enviar los mensajes SMS. Si necesita que sean enviados a más de un número de teléfono puede indicar varios números de teléfono separados por “;”.
- **Test SMS Alarm On.** Texto del mensaje SMS a enviar cuando se activa la alarma.
- **Test SMS Alarm Off.** Texto del mensaje SMS a enviar cuando se desactiva la alarma.

- **Logger**: Debe activarse si se pretende que el equipo basado en TITAN guarde en el Logger el cambio de la entrada digital para que sea enviada a una plataforma vía HTTP/HTTPS, MQTT/MQTTS o FTP.

En caso de activarse el LOGGER, éste es el objeto JSON que se enviará al servidor.

```
{"IMEI":"867962046823806","TYPE":"GPIO","TS":"2021-11-03T08:16:00Z","ID":0,"VALUE":1,"DIR":"INPUT","P":"ID0001"}
```

Donde:

IMEI: imei del módem

TYPE: tipo de trama. En este caso "GPIO"

TS: Timestamp de cuando se produjo el evento

ID: Identificador de la IO (0, 1, ...)

VALUE: valor lógico de la entrada digital (0, 1)

DIR: indica si la GPIO es de tipo INPUT o OUTPUT

P: Campo ID configurado en la sección LOGGER

También es posible leer el valor de la entrada digital en tiempo real pulsando el botón "READ INPUT".



Configuración de las salidas digitales

La pantalla de configuración de las salidas digitales presenta el aspecto siguiente

★ **Mobile**

- ◇ Status
- ◇ Basic Settings
- ◇ Keep Online

★ **Ethernet**

- ◇ Basic Settings
- ◇ DHCP Server

★ **Wifi**

- ◇ Basic Settings
- ◇ DHCP Server

★ **Firewall**

- ◇ NAT

► **Other** ► **Digital I/O** ► **Digital Output IO-1**

On:

SET ON

Click for activate digital output IO-1

Off:

SET OFF

Click for deactivate digital output IO-1

► **Other** ► **Digital I/O** ► **Digital Output IO-1** ► **Status**

READ STATUS

ERROR

Click for read the status of digital output IO-1

Desde esta pantalla es posible cambiar el estado de una salida digital, así como leer el estado actual de la misma. Recuerde que también es posible cambiar el estado de una salida digital desde los TITAN Scripts.

4.8.22- Other → Custom Skin

El equipo basado en TITAN permite configurar con sus propios logotipos la cabecera del entorno de configuración web, así como el título y pie de página del mismo. Esto permite, en cierta manera, dar apariencia de producto customizado o marca blanca.

- **Set custom image:** seleccione una imagen del 922 x 172 pixeles (**tipo gif**) para el área de cabecera.
- **Set custom labels:** introduzca el texto que desee que aparezcan en el título y pie del entorno de configuración web.

The screenshot shows the Webdyn TITAN configuration interface. At the top, there is a header with the Webdyn logo (a stylized 'w' in blue and grey) and the text 'webdyn flexitron group'. To the right is the 'TITAN' logo with the tagline 'Makes your APPLICATION happen'.

The main content area is titled 'Other > Custom Skin'. It contains two sections:

- Set custom image (logo):** This section has a text input field with a placeholder 'Examinar...' and the text 'No se ha seleccionado ningún archivo.' To the right of this field is the instruction 'Select an image for header (922x172)'. Below the input field is an 'Upload' button with the instruction 'Press the button for upload the image. (If can't see image, press CTRL+F5 key)'.
- Set custom labels:** This section has two text input fields. The first is labeled 'Intelligent Router - Web Panel Control' and has the instruction 'Bottom text at web interface.' The second is labeled 'Intelligent Router' and has the instruction 'Title text at web interface.' Below these fields is a checkbox with the instruction 'Hide device's name on Mobile Status menu'.

At the bottom of the configuration area is a 'SAVE CONFIG' button.

On the left side of the interface, there is a sidebar menu with the following items:

- ★ **Mobile**
 - ◇ Status
 - ◇ Basic Settings
 - ◇ Keep Online
- ★ **Ethernet**
 - ◇ Basic Settings
 - ◇ DHCP Server
- ★ **Wifi**
 - ◇ Basic Settings
 - ◇ DHCP Server
- ★ **Firewall**
 - ◇ NAT
 - ◇ Authorized IPs
 - ◇ MAC Filter
 - ◇ Routes
- ★ **Serial Settings**
 - ◇ Serial Port1-RS232
 - ◇ Serial Port2-RS485

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios.
- Tenga presente que, si configura el equipo con su cabecera y textos customizados para que sean vistos por terceros, no tiene sentido que no use la sección "Other > User Permissions". Use dicha sección para que el usuario "user" no tenga acceso a la sección "Other > Custom Skin".

4.8.23- Other → Custom Led

Los equipos basados en TITAN disponen de varios leds configurables. Desde esta sección puede darle el comportamiento que más se ajuste a sus necesidades.

- **Not used:** El Led siempre estará apagado, sin uso.
- **IP:** El Led se encenderá si el equipo tiene dirección IP (WAN 4G/3G/2G)
- **RSSI:** El Led parpadeará cuando la cobertura sea baja y permanecerá encendido sin parpadear cuando la cobertura sea buena. Apagado indica cobertura crítica o nula.
- **SIM Error:** El Led se iluminará cuando se detecte fallo de tarjeta SIM
- **TITAN Scripts:** El Led va a ser utilizado desde la sección TITAN Scripts del equipo

The screenshot shows the webdyn TITAN configuration interface. The header includes the webdyn logo (a stylized 'w' with a blue and grey wave) and the TITAN logo with the tagline "Makes your APPLICATION happen". The left sidebar contains a menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), and Wifi (Basic Settings, DHCP Server). The main content area is titled "OTHER > Led Configuration" and contains three rows of configuration options:

Led	Configuration	Behavior
Led1 (yellow):	RSSI	Led behavior
Led2 (blue):	IP	Led behavior
Led3 (red):	SIM Error	Led behavior

At the bottom of the configuration area is a "SAVE CONFIG" button.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.

4.8.24- Other → SYSLOG

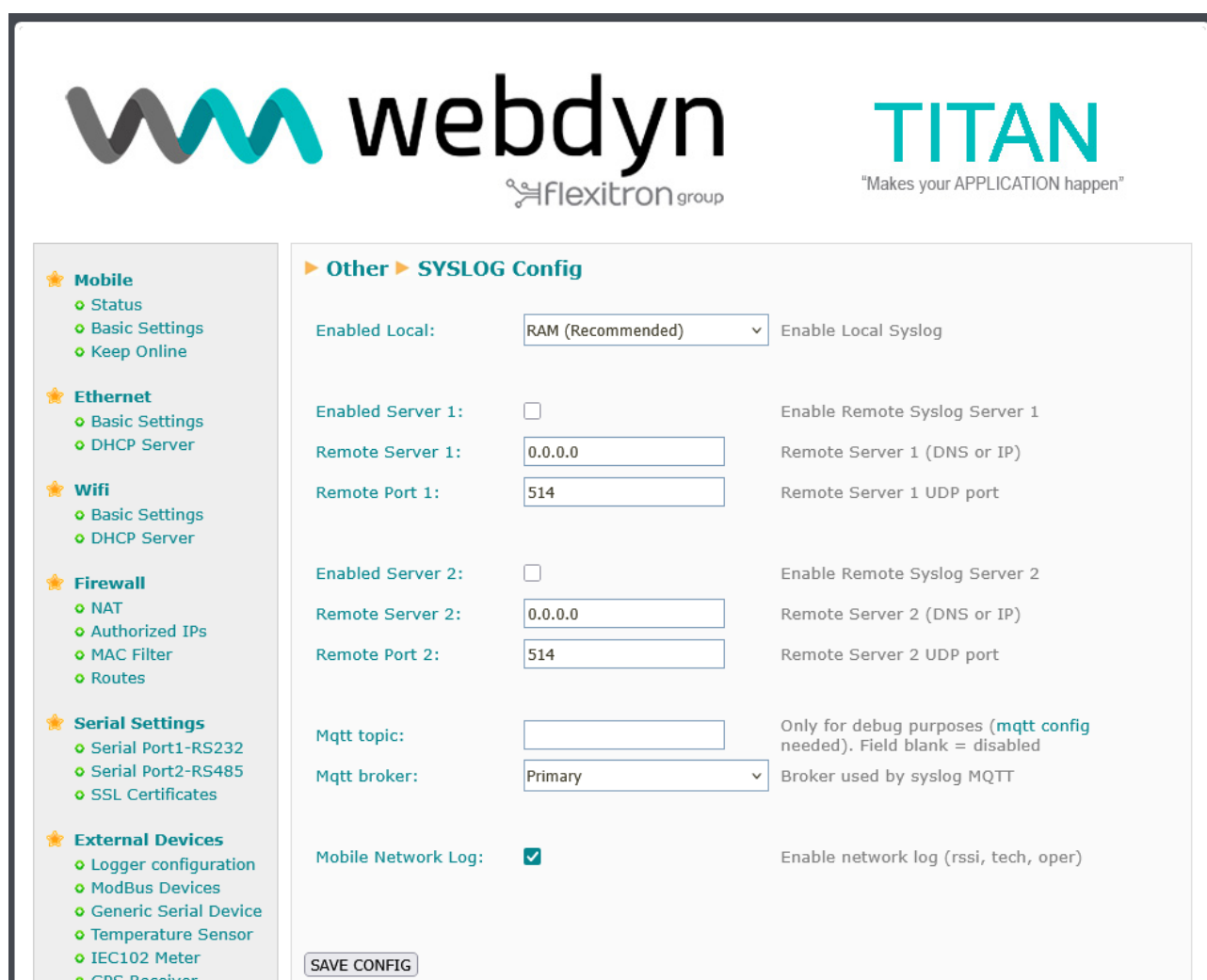
Desde esta sección es posible tener acceso a un log interno del equipo basado en TITAN donde es posible ver el estado del propio equipo (cobertura, registro en la red, operador, resultado de envíos a servidores ...), las acciones realizadas por usuarios, etc.

The screenshot displays the webdyn TITAN web interface. The top header features the webdyn logo and the TITAN logo with the tagline "Makes your APPLICATION happen". A left sidebar contains a navigation menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor, IEC102 Meter, GPS Receiver), and VPN. The main content area is titled "Other → SYSLOG" and shows a log of system events. The log entries include timestamps, device identifiers, and details about registration status, cellular network usage, and signal levels. Below the log, there are three buttons: "REFRESH LOG", "SYSLOG CONFIG", and "DELETE LOG". At the bottom right of the main area, there are two links: "Click here for download current SYSLOG complete file" and "Click here for download historic SYSLOG - 1".

Pulsando sobre el botón “**SYSLOG CONFIG**” se accederá a la sección de configuración del SYSLOG. En esta sección de configuración es posible establecer las siguientes configuraciones.

- **Enabled Local:** “**Disabled**”: no usará el SYSLOG. “**RAM**” (opción recomendada) guardará el SYSLOG en memoria RAM. “**FLASH**” (sólo disponible en algunos equipos basados en TITAN) guardará el SYSLOG en flash. Sólo recomendado para debug y no para uso permanente, pues su uso constante puede desgastar en exceso la memoria FLASH.
- **Enabled Server 1:** Activando la casilla se habilita el envío del SYSLOG vía UDP a un servidor remoto.
- **Remote Server 1:** IP o DNS del servidor remoto 1 para recibir el SYSLOG
- **Remote Port 1:** Puerto UDP del servidor remoto 1

- **Enabled Server 2:** Activando la casilla se habilita el envío del SYSLOG vía UDP a un segundo servidor remoto.
- **Remote Server 2:** IP o DNS del servidor remoto 2 para recibir el SYSLOG
- **Remote Port 2:** Puerto UDP del servidor remoto 2
- **MQTT Topic:** Si se especifica un topic MQTT se enviará el syslog en tiempo real al topic
- **MQTT Broker:** permite seleccionar el bróker MQTT utilizado para enviar el syslog cuando se ha configurado un "MQTT Topic". Puede seleccionarse Primary, Secondary o Both.
- **Mobile Network Log:** Activando la casilla se añade al SYSLOG el estado de la red de forma periódica.



The screenshot shows the webdyn TITAN configuration interface. The header includes the webdyn logo (Flexitron group) and the TITAN logo with the tagline "Makes your APPLICATION happen". On the left is a sidebar menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), and External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor, IEC102 Meter, GPS Receiver). The main content area is titled "Other > SYSLOG Config". It contains several configuration fields: "Enabled Local" (set to "RAM (Recommended)" with a dropdown arrow) and "Enable Local Syslog"; "Enabled Server 1" (checkbox), "Remote Server 1" (text field with "0.0.0.0"), "Remote Port 1" (text field with "514"), and "Enable Remote Syslog Server 1"; "Enabled Server 2" (checkbox), "Remote Server 2" (text field with "0.0.0.0"), "Remote Port 2" (text field with "514"), and "Enable Remote Syslog Server 2"; "Mqtt topic" (text field) with a note "Only for debug purposes (mqtt config needed). Field blank = disabled"; "Mqtt broker" (dropdown menu with "Primary" selected) with a note "Broker used by syslog MQTT"; and "Mobile Network Log" (checkbox checked) with a note "Enable network log (rssi, tech, oper)". At the bottom left of the main area is a "SAVE CONFIG" button.

Notas adicionales.

- Una vez finalizada la configuración pulse el botón "SAVE CONFIG" para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Por motivos de seguridad, se recomienda encarecidamente el envío de LOGS a un servidor destino a través de una VPN.

4.8.25- Other → Backup / Factory.

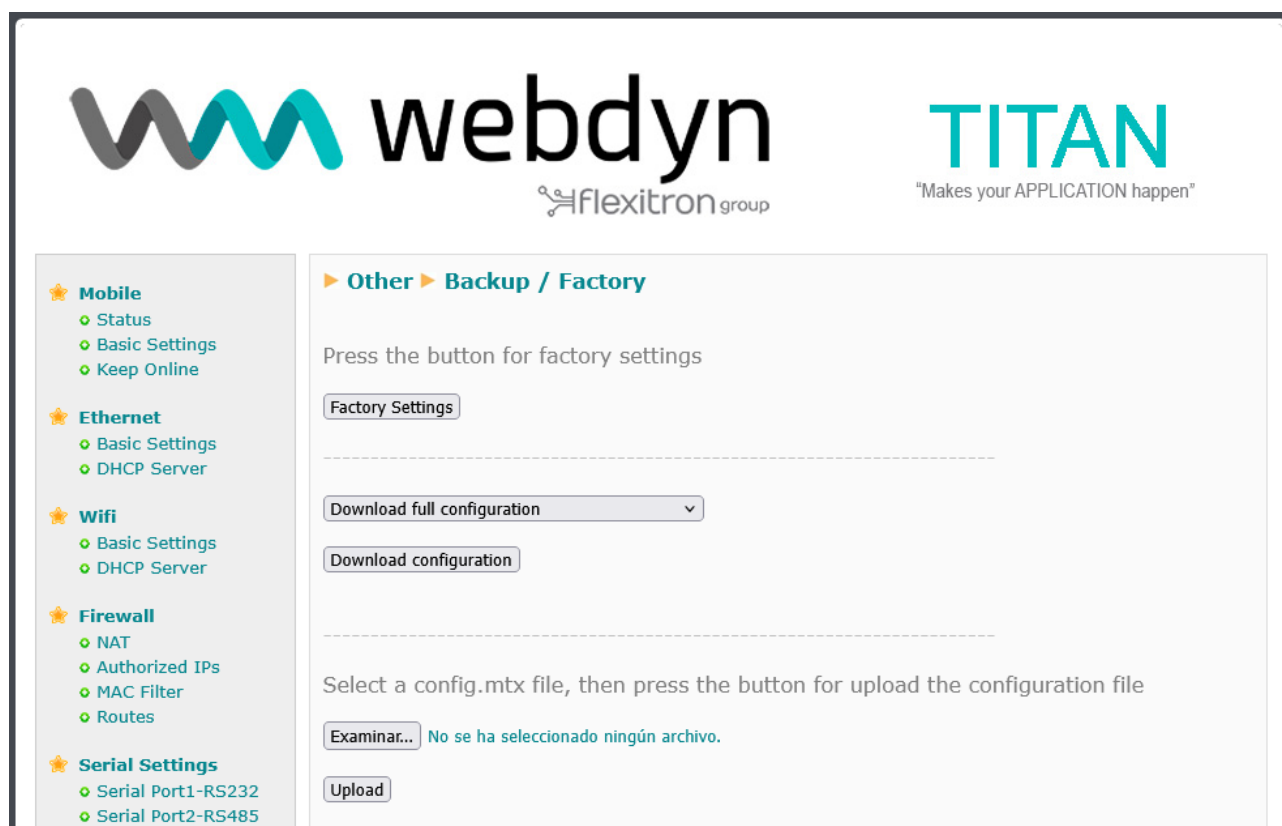
Puede realizar una copia de seguridad completa de la configuración del equipo desde este menú. Podrá salvar la configuración en un archivo y volverla a grabar en el equipo cuando lo necesite. También le permite configurar el equipo con la configuración de fábrica.

- **Botón “Factory Settings”:** pulse este botón si quiere restaurar el equipo con la configuración de fábrica.
- **Botón “Download settings”:** pulse el botón para descargar la configuración del equipo en un archivo de nombre “config.mtx”.
- **Botón “Seleccionar archivo”:** para hacer una restauración de una configuración guardada, tras indicar el archivo de configuración a usar, pulse el botón “Upload” para cargar el archivo.

NOTA

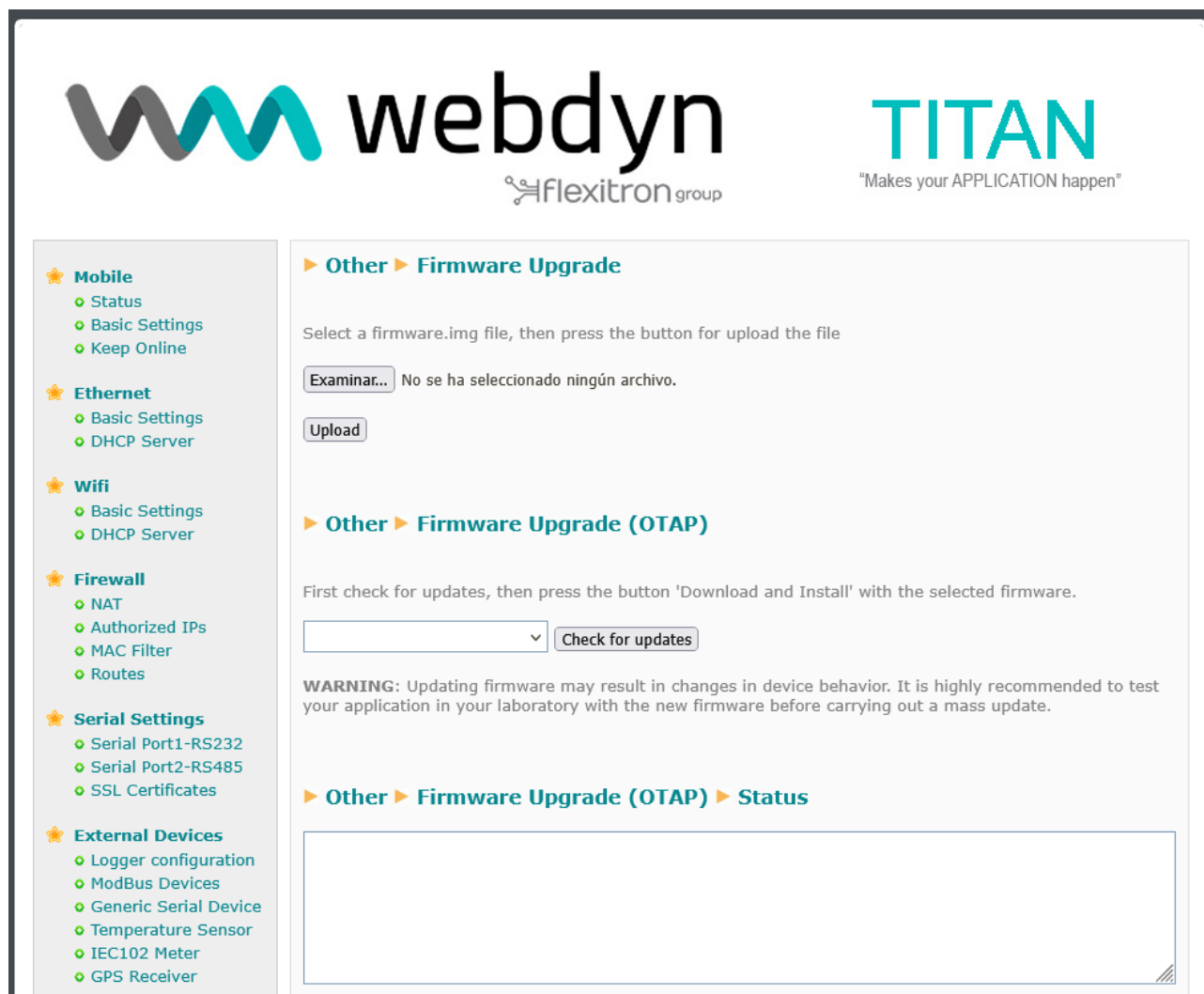
Archivos de configuración descargados de un equipo con versión v6.XX NO son compatibles con los equipos con versión v7.XX, y viceversa.

Por ejemplo, si le da a “Download configuration” a un equipo con Titan v6.40, y luego en otro equipo con Titan v7.01 le da a “Upload” con el fichero .mtx generado en el otro, obtendrá error.



4.8.26- Other → Firmware Upgrade

Desde esta sección es posible actualizar el firmware del router Titan de dos formas, localmente o remotamente.



Firmware Upgrade

Si dispone del fichero de firmware para actualizar el equipo, pulse sobre el botón “seleccionar archivo”, seleccione dicho fichero y tras ello pulse el botón “Upload”. El proceso puede durar hasta 2 minutos y el router Titan podrá reiniciarse hasta 2 veces al finalizar el proceso.

Firmware Upgrade (OTAP)

Otra opción para actualizar el Firmware del dispositivo es mediante el proceso de OTAP. Si pretende utilizar esta opción es necesario que el router Titan tenga acceso a Internet, pues el firmware será descargado desde los servidores de Webdyn. Para llevar a cabo el proceso de OTAP debe pulsar sobre el botón “Check for updates”. Tras unos segundos, en caso de haber actualizaciones de

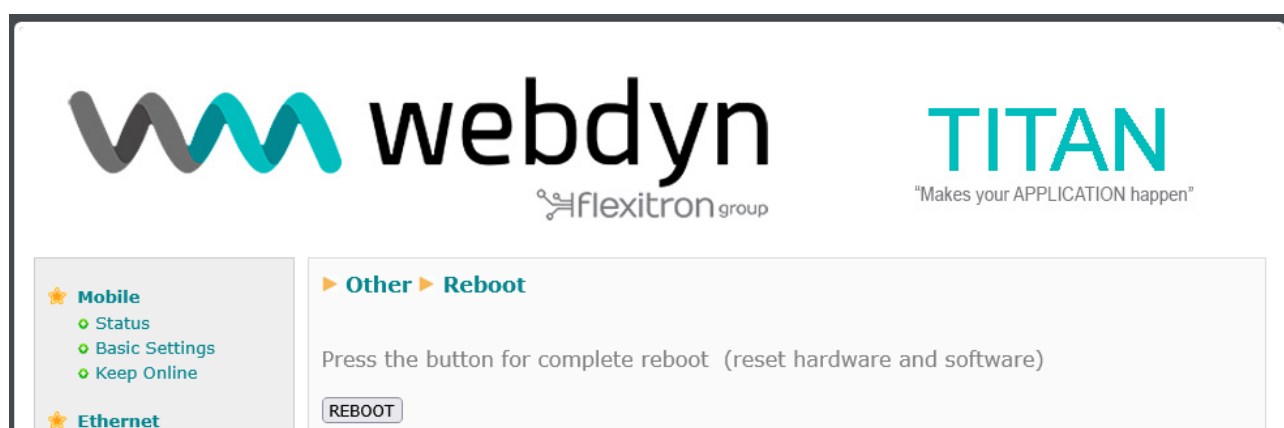
firmware para su router, aparecerán en el desplegable. Seleccione la versión de firmware que desee instalar y pulse sobre el botón “Download and Install” para iniciar el proceso.

Recuerde que todo proceso de cambio de firmware en cualquier dispositivo conlleva riesgos. Es altamente recomendable que compruebe que el escenario que tiene configurado en el router Titan funciona correctamente en laboratorio con la versión de firmware que pretende instalar antes de proceder a actualizaciones masivas de firmware de dispositivos ubicados en lugares remotos.

4.8.27- Other → Reboot.

Desde esta sección es posible reiniciar el equipo. Por ejemplo, para aplicar los cambios tras un cambio de configuración. Para ello tan solo basta con pulsar el botón 'Reboot'

Dependiendo del equipo también se dispone de la opción "Power down". Mediante esta opción es posible apagar un modelo de equipo que cuente con batería interna, como ocurre por ejemplo con el modelo MTX-Router-Q. Antes de pulsar el botón "Power down" debe retirar la alimentación (220Vac) al equipo y tras ello, pulsar el botón. Pasados unos segundos todos los leds permanecerán apagados.



4.8.28- VPN → OpenVPN Server

Los routers basados en TITAN pueden actuar como Servidor OpenVPN. Mediante establecimiento de una VPN, todos los dispositivos que cuelguen del bus Ethernet del equipo, o incluso las pasarelas IP-RS232/485, serán accesibles de forma segura desde el otro extremo de la red VPN. Una infraestructura VPN resulta muy útil para esquivar la mayoría de problemas con proxys, firewalls, etc sobre todo con el uso de tarjetas SIM de un operador que otorgue direcciones IP de rango privado (10.x.x.x)

The screenshot shows the webdyn TITAN router configuration page for the OpenVPN Server. The sidebar on the left lists various configuration categories: Mobile, Ethernet, Firewall, Serial Settings, External Devices, and VPN. The main content area is titled 'VPN > OpenVPN Server'. It contains several configuration options: 'Enabled' (checkbox), 'Mode' (dropdown menu set to 'Always On'), 'Protocol' (dropdown menu set to 'udp'), 'Port' (input field set to '1194'), 'LZO compression' (checkbox checked), 'Auth' (dropdown menu set to 'SHA256'), 'Cipher' (dropdown menu set to 'AES-256-GCM'), 'Server subnet' (input field), 'Server mask' (input field), 'Allow LAN access' (checkbox), and 'Client to client' (checkbox). To the right of these fields are descriptive text blocks for each setting. At the bottom, there are input fields for 'Client 1', 'Client 2', and 'Client 3'.

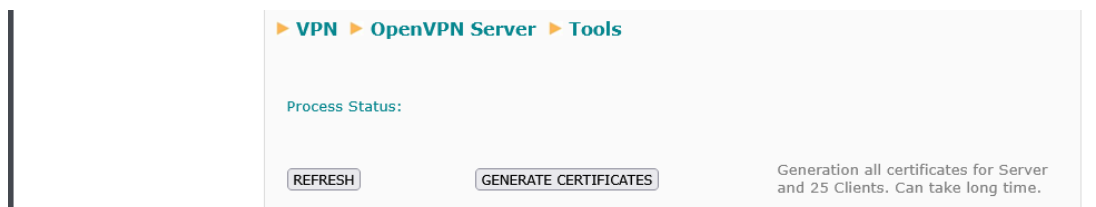
- **Enabled:** Active esta casilla si quiere activar el servicio de OpenVPN en modo Servidor
- **Mode:** Permite establecer el modo de conexión de la VPN. Un valor de "Always On" mantendrá la VPN activa en todo momento. Un valor de "Under Request" habilitará la VPN durante el tiempo que usted decida. Por ejemplo, quizás pueda interesarle activar la VPN únicamente en momentos muy puntuales para labores de mantenimiento. Cuando quiera activar la VPN únicamente tendrá que hacerlo enviando un comando AT (vea el capítulo 5 referente a comandos AT) vía SMS, o por Telnet, o por Webserver o SNMP o incluso por Modbus TCP. Pasado el tiempo configurado la VPN se cerrará.
- **Protocol:** puede establecer el protocolo de establecimiento. Puede usar tanto protocolo UDP como TCP.
- **Port:** el puerto estándar es el 1194, pero puede especificar el puerto para la VPN que más le convenga.

- **LZO compression:** active la casilla si desea activar esta opción.
- **Auth:** permite escoger el método de autenticación.
- **Cipher:** permite escoger el algoritmo de cifrado.
- **Server Subnet:** indique la subred que se creará tras la creación de la VPN. Por ejemplo, si indica la subred 10.8.0.0, al activarse la VPN, el equipo basado en TITAN adoptará la dirección 10.8.0.1.
- **Server Mask:** indique la máscara de red a aplicar en la VPN
- **Allow Lan Access:** active la casilla si quiere poder acceder remotamente a los dispositivos que cuelguen del puerto Ethernet del equipo. No la active si únicamente quiere poder acceder al equipo basado en TITAN y a las pasarelas IP-RS232/485 que éste gestiona.
- **Client to client:** habilita el modo cliente a cliente.
- **Ficheros necesarios para OpenVPN**

Para poder utilizar los equipos basados en TITAN como servidor OpenVPN necesitará crear y hacer un upload de los ficheros **ca.crt** (certificado de autoridad), **server.crt** (certificado del servidor), **server.key** (clave privada del servidor), **dh1024.pem** (Diffie Hellman parameters).

En la parte inferior de la pantalla verá que puede hacer download de unos ficheros demo que únicamente deberían ser utilizados a modo de pruebas. Recuerde que en una aplicación real debería generar sus propios certificados.

Al final de la página web en la sección de OpenVPN Server podrá encontrar un mecanismo para generar todos los certificados para el servidor y los 25 clientes. **IMPORTANTE:** el uso de esta herramienta puede tomar hasta 80 min hasta generar todos los certificados.



Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- **Dispone de notas de aplicación (documentos PDF externos a este documento) con ejemplos de la funcionalidad OpenVPN con los equipos basados en TITAN.**

4.8.29- VPN → OpenVPN Client

Los routers basados en TITAN pueden actuar como Cliente OpenVPN. Mediante establecimiento de una VPN, todos los dispositivos que cuelguen del bus Ethernet del equipo, o incluso las pasarelas IP-RS232/485, serán accesibles de forma segura desde el otro extremo de la red VPN. Una infraestructura VPN resulta muy útil para esquivar la mayoría de los problemas con proxys, firewalls, etc sobre todo con el uso de tarjetas SIM de un operador que otorgue direcciones IP de rango privado (10.x.x.x)

The screenshot shows the webdyn TITAN configuration interface. The left sidebar contains a navigation menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings), Firewall (Authorized IPs, MAC Filter), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor, IEC102 Meter), VPN (IPSec, OpenVPN Client, OpenVPN Server, ZeroTier), Device Manager (KARE), and Other (AT Command, DynDns, Private DynDns, Sms control, Periodic Autoreset). The main content area is titled 'VPN > OpenVPN Client'. It features a configuration form with the following fields: 'Enabled' (checkbox), 'Mode' (dropdown menu set to 'Always On'), 'Protocol' (dropdown menu set to 'udp'), 'LZO compression' (checkbox checked), 'Auth' (dropdown menu set to 'SHA256'), 'Cipher' (dropdown menu set to 'AES-256-CBC'), 'IP Server' (text input), 'Port Server' (text input set to '1194'), 'Username' (text input), and 'Password' (text input). To the right of these fields are descriptive labels: 'Enable OpenVPN Client', 'Always on or under request (ex, by SMS)', 'Communication protocol', 'Enable LZO compression. Normally yes.', 'Authentication', 'Cipher', 'IP of remote OpenVPN Server', 'Port of remote OpenVPN Server (def 1194)', 'Username. Blank if not used', and 'Password. Blank if not used'. Below the form are 'SAVE CONFIG' and 'VIEW LOG' buttons. At the bottom, there are sections for uploading certificates and keys: 'Certificate Authority: 'ovpnc-ca.crt'', 'Client certificate: 'ovpnc-client.crt'', 'Client KEY: 'ovpnc-client.key'', and 'Extra parameters (no mandatory, only if needed) 'ovpnc-client.extra''. Each section has an 'Examinar...' button, a text area showing 'No se ha seleccionado ningún archivo.', an 'Upload' button, and a status indicator 'not uploaded'. A 'DELETE FILES' button is located at the bottom left of the main content area.

- **Enabled:** Active esta casilla si quiere activar el servicio de OpenVPN en modo Cliente
- **Mode:** Permite establecer el modo de conexión de la VPN. Un valor de "Always On" mantendrá la VPN activa en todo momento. Un valor de "Under Request" habilitará la VPN durante el tiempo que usted decida. Por ejemplo, quizás pueda interesarle activar la VPN únicamente en momentos muy puntuales para labores de mantenimiento. Cuando quiera activar la VPN únicamente tendrá que hacerlo enviando un comando AT (vea el capítulo 5 referente a comandos AT) vía SMS, o por Telnet, o por Webserver o SNMP o incluso por Modbus TCP. Pasado el tiempo configurado la VPN se cerrará.

- **Protocol:** puede establecer el protocolo de establecimiento. Puede usar tanto protocolo UDP como TCP.
- **Port:** el puerto estándar es el 1194, pero puede especificar el puerto para la VPN que más le convenga.
- **LZO compression:** active la casilla si desea activar esta opción.
- **Auth:** permite escoger el método de autenticación.
- **Cipher:** permite escoger el algoritmo de cifrado.
- **IP Server:** indique la dirección IP Pública del servidor remoto que actuará como servidor OpenVPN
- **Port Server:** puerto remoto del servidor OpenVPN.
- **Username:** campo usuario (dejar en blanco si no se usa).
- **Password:** campo contraseña (dejar en blanco si no se usa).
- **Ficheros necesarios para OpenVPN**

Para poder utilizar los equipos basados en TITAN como cliente OpenVPN necesitará crear y hacer un upload de los ficheros **ca.crt** (certificado de autoridad), **client.crt** (certificado del cliente), **client.key** (clave privada del cliente).

En la parte inferior de la pantalla verá que puede hacer download de unos ficheros demo que únicamente deberían ser utilizados a modo de pruebas. Recuerde que en una aplicación real debería generar sus propios certificados.

Al final puede encontrar ficheros de ejemplo con fines de pruebas/test así como el estado del cliente OpenVPN:



Notas adicionales.

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- **Dispone de notas de aplicación (documentos PDF externos a este documento) con ejemplos de la funcionalidad OpenVPN con los equipos basados en TITAN.**

4.8.30- VPN → IPSec

Los routers basados en TITAN cuentan con la característica IPSEC. Mediante el establecimiento de una VPN, todos los dispositivos que cuelguen del bus Ethernet del equipo, o incluso las pasarelas IP-RS232/485, serán accesibles de forma segura desde el otro extremo de la red VPN. Una infraestructura VPN resulta muy útil para esquivar la mayoría de los problemas con proxys, firewalls, etc sobre todo con el uso de tarjetas SIM de un operador que otorgue direcciones IP de rango privado (10.x.x.x)

**webdyn**
flexitron group

TITAN
"Makes your APPLICATION happen"

- ★ **Mobile**
 - ◇ Status
 - ◇ Basic Settings
 - ◇ Keep Online
- ★ **Ethernet**
 - ◇ Basic Settings
- ★ **Firewall**
 - ◇ Authorized IPs
 - ◇ MAC Filter
- ★ **Serial Settings**
 - ◇ Serial Port1-RS232
 - ◇ Serial Port2-RS485
 - ◇ SSL Certificates
- ★ **External Devices**
 - ◇ Logger configuration
 - ◇ ModBus Devices
 - ◇ Generic Serial Device
 - ◇ Temperature Sensor
 - ◇ IEC102 Meter
- ★ **VPN**
 - ◇ IPsec
 - ◇ OpenVPN Client
 - ◇ OpenVPN Server
 - ◇ ZeroTier
- ★ **Device Manager**
 - ◇ KARE
- ★ **Other**
 - ◇ AT Command
 - ◇ DynDns
 - ◇ Private DynDns
 - ◇ Sms control
 - ◇ Periodic Autoreset
 - ◇ Time Servers
 - ◇ Remote Console
 - ◇ Snmp
 - ◇ Tacacs+
 - ◇ Ldap
 - ◇ Matt / Matts

VPN ▶ IPsec

Enabled: ☐ Enable IPsec vpn service

[SAVE CONFIG](#)

VPN ▶ IPsec ▶ Configuration Files

IPsec config file: **'ipsec.conf'** (find examples at the bottom of this page)

```
config setup
charondebug="ike 1, knl 1, cfg 2"
uniqueids=yes

conn client
    auto=start
    keyexchange=ikev2
    type=tunnel
    compress=no
    forceencaps=yes
    closeaction=restart
    keyingtries=%forever
    dpdaction=restart
    dpddelay=30s
    dpdtimeout=120s
    ikelifetime=1800s
    authby=rsasig

    left=%any
    leftsourceip=172.17.101.225
    leftsubnet=172.17.96.0/21
```


IPsec secrets files: **'ipsec.secrets'** click for **Show/Hide**

```
: RSA xclient1-
key.pem
```


[SAVE CONFIG](#)

- **Enabled:** Active esta casilla si quiere activar el servicio de IPsec
- **ipsec.conf:** introduzca aquí el fichero de configuración de su VPN IPsec. Puede consultar y modificar los ejemplos de la zona inferior de la pantalla que más se ajuste a sus necesidades.
- **ipsec.secrets:** introduzca aquí el contenido del fichero ipsec.secrets de su VPN IPsec. Puede consultar y modificar los ejemplos de la zona inferior de la pantalla que más se ajuste a sus necesidades.

Equipo basado en TITAN actuando como cliente IPsec:

- xca1-cert.pem: fichero con el certificado CA root de su servidor IPSEC
- xclient1-cert.pem: fichero con el certificado de cliente
- xclient1-key.pem: fichero con la KEY

Equipo basado en TITAN actuando como servidor IPsec:

- ca-cert.pem: fichero CA root del equipo basado en TITAN
- ca-key.pem: fichero con la KEY del CA del equipo basado en TITAN
- server-cert.pem: fichero certificado del equipo basado en TITAN
- server-key.pem: fichero con la KEY del equipo basado en TITAN
- client1-cert.pem: fichero con el certificado del cliente 1 autorizado para conectarse
- client2-cert.pem: fichero con el certificado del cliente 1 autorizado para conectarse
- client3-cert.pem: fichero con el certificado del cliente 1 autorizado para conectarse

En la parte final puede encontrar una sección de “Status” así como una parte de ficheros de ejemplo para descargar:

VPNIPSecStatus

REFRESHVIEW LOGRESTART IPSEC

VPNIPSecExamples

Example1:	ipsec.conf ipsec.secrets	IPSec configured as IPSec Server - EAP authentication (user and password) - IKEV2
Example2:	ipsec.conf ipsec.secrets	IPSec configured as IPSec Server - authentication with PSK Key - IKEV2
Example3:	ipsec.conf ipsec.secrets	IPSec configured as IPSec Server - authentication with Certificate - IKEV2
Example4:	ipsec.conf ipsec.secrets	IPSec configured as IPSec Client - authentication with Certificate - IKEV2
Example5:	ipsec.conf ipsec.secrets	IPSec configured as IPSec Server - authentication with PSK Key - IKEV1
Example6:	ipsec.conf ipsec.secrets	IPSec configured as IPSec Server - authentication with Certificate - IKEV1
Example7:	ipsec.conf ipsec.secrets	IPSec configured as IPSec Client - authentication with PSK Key - IKEV1

Notas adicionales.

- **ADVERTENCIA**: IPSec con autenticación EAP o PSK necesita de una contraseña segura siguiendo las recomendaciones de la “European Cybersecurity Certification Group”: **el password como mínimo 17 caracteres de los cuales se incluya al menos una mayúscula, una minúscula y un número.**

- Una vez finalizada la configuración pulse el botón “SAVE CONFIG” para guardar los cambios. Recuerde que debe reiniciar el equipo para que se apliquen los nuevos cambios.
- Dispone de notas de aplicación (documentos PDF externos a este documento) con ejemplos de la funcionalidad IPSec con los equipos basados en TITAN.

4.8.31- VPN → Zerotier

Los routers Titan cuentan con el soporte de VPN del servicio ZeroTier desde la versión de FW 5.3.6.25. ZeroTier permite implementar una VPN de forma muy sencilla y rápida, permitiendo el acceso a los router Titan y a los dispositivos conectados a él desde cualquier ubicación. Consulte la nota de aplicación AN71 donde encontrará ejemplos de uso y una información más detallada.

**webdyn**
flexitron group

TITAN
"Makes your APPLICATION happen"

★ **Mobile**

- Status
- Basic Settings
- Keep Online

★ **Ethernet**

- Basic Settings

★ **Firewall**

- Authorized IPs
- MAC Filter

★ **Serial Settings**

- Serial Port1-RS232
- Serial Port2-RS485
- SSL Certificates

★ **External Devices**

- Logger configuration
- ModBus Devices
- Generic Serial Device
- Temperature Sensor
- IEC102 Meter

★ **VPN**

- IPSec
- OpenVPN Client
- OpenVPN Server
- ZeroTier

★ **Device Manager**

- KARE

★ **Other**

- AT Command
- DynDns
- Private DynDns
- Sms control
- Periodic Autoreset
- Time Servers
- Remote Console
- Snmp
- Tacacs+
- Ldap
- Mqtt / Mqtts
- Http / Https
- User Permissions
- Passwords Web UI
- CA Certificates
- Email Config
- ModBus Slave
- Titan Scripts**
- Connectivity tools
- Digital I/O
- Custom Skin
- Led Config
- Syslog
- Backup / Factory

▶ **VPN ▶ ZeroTier**

Enabled: ☐ Enable ZeroTier VPN service

TCP Port: TCP internal port (default 9993)

VPN1 Network ID: Network ID ZeroTier 1 (blank = not used)

VPN2 Network ID: Network ID ZeroTier 2 (blank = not used)

VPN3 Network ID: Network ID ZeroTier 3 (blank = not used)

SAVE CONFIG

▶ **VPN ▶ ZeroTier ▶ Status**

Device ID: ---

VPN1 Network name: ---

VPN1 IP & MAC: IP: --- MAC: ---

VPN1 interface: zt0

VPN1 status: ---

VPN2 Network name: ---

VPN2 IP & MAC: IP: --- MAC: ---

VPN2 interface: zt1

VPN2 status: ---

VPN3 Network name: ---

VPN3 IP & MAC: IP: --- MAC: ---

VPN3 interface: zt2

VPN3 status: ---

REFRESH

▶ **VPN ▶ ZeroTier ▶ Tools**

Device ID:

Restart device ID. You will need to accept again the device in your zerotier account.

contact@webdyn.com | webdyn.com

V7.02 subject to change | Webdyn © by Flexitron Group

Página 167

- **Enabled:** Active esta casilla si quiere activar el servicio de ZeroTier
- **TCP Port:** puerto TCP para uso interno del router Titan. Mantenga el puerto por defecto TCP 9993 si no lo necesita para otro servicio.
- **VPN1 Network ID:** identificador ZeroTier de la red VPN 1
- **VPN1 Network ID:** identificador ZeroTier de la red VPN 2
- **VPN1 Network ID:** identificador ZeroTier de la red VPN 3

- **Restart:** botón que permite cambiar el Device ID del dispositivo en la red de ZeroTier. Si se cambia el Device ID será necesario acudir al panel de control de ZeroTier (my.zerotier.com) y volver a aceptar el dispositivo en la red.

5.- Comandos AT

Los equipos basados en TITAN permiten el envío de comandos AT directamente al módem interno a través de múltiples interfaces:

- 1.- Mediante un puerto serie.,
- 2.- Mediante una pasarela 4G/3G/2G-Serie (a través de IP WAN, Ethernet o Wifi) a través de comandos AT embebidos.
- 3.- Mediante SMS
- 4.- Mediante Telnet (Remote Console, a través de 4G/3G/2G, Ethernet o Wifi)
- 5.- Mediante SSH (Remote Console, a través de 4G/3G/2G, Ethernet o Wifi)
- 5.- Mediante Webserver (a través de 4G/3G/2G, Ethernet o Wifi)
- 7.- Mediante Modbus RTU (a través de un puerto serie RS232 o RS485)
- 8.- Mediante Modbus TCP (a través de 4G/3G/2G, Ethernet o Wifi)
- 9.- Mediante SNMP (a través de 4G/3G/2G, Ethernet o Wifi)
- 10.- Mediante URL. Explicado al final de este punto.

Por tanto, bajo su responsabilidad, puede enviar comandos AT al equipo.

- **AT^MTXTUNNEL=REBOOT**

Acción: resetea el equipo basado en TITAN.

Resultado:

OK: Comando ejecutado correctamente.
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=REBOOT
OK

- **AT^MTXTUNNEL=VERSION**

Acción: devuelve la versión de firmware del equipo TITAN.

Resultado:

OK: Comando ejecutado correctamente.
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=VERSION
5.2.6.17
OK

- **AT^MTXTUNNEL=GETIP**

Acción: devuelve la dirección IP WAN (2G / 3G / 4G)

Resultado:

OK: Comando ejecutado correctamente.
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=GETIP
88.28.221.14
OK

- **AT^MTXTUNNEL=GETIMEI**

Acción: devuelve el IMEI del módem interno

Resultado:

OK: Comando ejecutado correctamente.
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=GETIMEI
869101054255506
OK

- **AT^MTXTUNNEL=GETCELLID**

Acción: devuelve la celda de telefonía que está siendo utilizada por el módem.

Resultado:

OK: Comando ejecutado correctamente.
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=GETCELLID
[4;214;07;219B;15F2D2A]
OK

Donde: 4 = tecnología utilizada (2=2g,3=3)

214 = MCC (Mobile Country Code)

07 = MNC (Mobile Network Code)

07 = LAC (Local Area Code)

15F2D2A = CID (Cell ID)

Comandos AT relacionados con mensajería:

- **AT^MTXTUNNEL=TRAP,<OID>;<myMessage>;<mySeverity>**

Acción: permite enviar un TRAP SNMP, con un OID determinado, el correspondiente mensaje asociado y la severidad.

Parámetros:

<OID>: OID del trap a enviar por SNMP
<myMessage>: mensaje de texto a enviar
<mySeverity>: 0 ... 7 severidad del trap

Resultado:

OK: Comando ejecutado correctamente. Mensaje enviado.
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=TRAP,1.3.6.1.4.1.45711.1.1.11.1.1;myMessage;5
OK

- **AT^MTXTUNNEL=SMS,<telephoneNumber>,<message>**

Acción: permite enviar un mensaje SMS a un determinado número de teléfono.

Parámetros:

<telephoneNumber>: número de teléfono al que enviar el mensaje SMS
<message>: mensaje de texto a enviar

Resultado:

OK: Comando ejecutado correctamente. Mensaje SMS enviado a la cola de salida.
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=SMS,+34677123456,alarma de robo
OK

- **AT^MTXTUNNEL=EMAIL,<destinationAddress>,<subject>**

Acción: permite enviar un email (únicamente el asunto) a una determinada dirección de correo electrónico. Para enviar el email debe tener previamente configurada la sección "Other > Email Configuration".

Parámetros:

<destinationAddress>: dirección de email destino
<subject>: mensaje a enviar por email

Resultado:

OK: Comando ejecutado correctamente. Email enviado.
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=EMAIL,jgallego@matrix.es,Alarma temperatura
OK

- **AT^MTXTUNNEL=TELEGRAM,SEND,<tokenID>,<chatID>,<message>**

Acción: permite enviar un mensaje de texto de Telegram a un determinado chat de un grupo de Telegram. Es necesario crear un bot con su tokenID y obtener el chatID del chat al que se pretende enviar el mensaje. Consulte las notas de aplicación para más información.

Parámetros:

<tokenID>: identificador de token
 <chatID>: identificador de chat
 <message>: mensaje a enviar por telegram

Resultado:

OK: Comando ejecutado correctamente. Mensaje enviado.
 ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=TELEGRAM,SEND,5416419553:ZZHof6enVx-y7uFQrL15cpf3QCHqNHp7Dtg,-730297962,My message
 OK

Comandos AT relacionados con E/S:

- **AT^MTXTUNNEL=GETIO,<idIO>**

Acción: devuelve el valor de una entrada o salida digital, donde idIO es el identificador de la IO (0,1,2...)

Parámetros:

<idIO>: 0, ... X número de I/O

Resultado:

OK: Comando ejecutado correctamente devolviendo el estado de la entrada o salida digital.
 ERROR: Comando ejecutado con error

Ejemplo: Lectura del estado de la entrada digital IO 0

AT^MTXTUNNEL=GETIO,0
 1
 OK

- **AT^MTXTUNNEL=SETIO,<idIO>,<value>**

Acción: permite cambiar el estado de una salida digital, donde idIO es el identificador de la IO (0,1,2...) y value el valor lógico de la salida (0, 1)

Parámetros:

<idIO>: 0, ... X número de I/O
<value>: 0,1 valor a establecer en la salida digital

Resultado:

OK: Comando ejecutado correctamente. Salida digital actualizada.
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=SETIO,3,1
OK

- **AT^MTXTUNNEL=GETCOUNTER,<idIO>**

Acción: devuelve el valor del contador de pulsos asociado a una entrada digital, donde idIO es el identificador de la IO (0,1,2...)

Parámetros:

<idIO>: 0, ... X número de I/O

Resultado:

OK: Comando ejecutado correctamente devolviendo el valor del contador de pulsos asociado a la entrada digital
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=GETCOUNTER,0
1022
OK

- **AT^MTXTUNNEL=SETCOUNTER,<idIO>,<value>**

Acción: permite cambiar el valor de un contador de pulsos asociado a una entrada digital, donde idIO es el identificador de la IO (0,1,2...) y value el valor del contador

Parámetros:

<idIO>: 0, ... X número de I/O
<value>: 0,1 valor a establecer en el contador asociado a la entrada digital.

Resultado:

OK: Comando ejecutado correctamente
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=SETCOUNTER,3,1000
OK

Comandos AT relacionados con OpenVPN:

- **AT^MTXTUNNEL=OVPNS,minutes**

Acción: si se tiene configurada la sección sección VPN > OpenVPN Server como una OpenVPN bajo demanda, con este comando AT puede activarse la OpenVPN en modo server durante los minutos especificados.

Parámetros:

<minutes>: 1 ... 525600 minutos

Resultado:

OK: Comando ejecutado correctamente
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=OVPNS,5

(Este ejemplo activaría la VPN durante 5 minutos)

- **AT^MTXTUNNEL=OVPNC,<minutes>**

Acción: si se tiene configurada la sección sección VPN > OpenVPN Client como una OpenVPN bajo demanda, con este comando AT puede activarse la OpenVPN en modo cliente durante los minutos especificados.

Parámetros:

<minutes>: 1 ... 525600 minutos

Resultado:

OK: Comando ejecutado correctamente
ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=OVPNC,5

(Este ejemplo activaría la VPN durante 5 minutos)

Comandos AT relacionados con test de conectividad:

- **AT^MTXTUNNEL=COMMAND,<timeout>,<command>**

Acción: permite ejecutar ciertos comandos especiales en el interior del Equipo basado en TITAN. Por el momento únicamente los comandos “ping” y “traceroute”. Se permite especificar un timeout (en segundos) así como el comando a ejecutar.

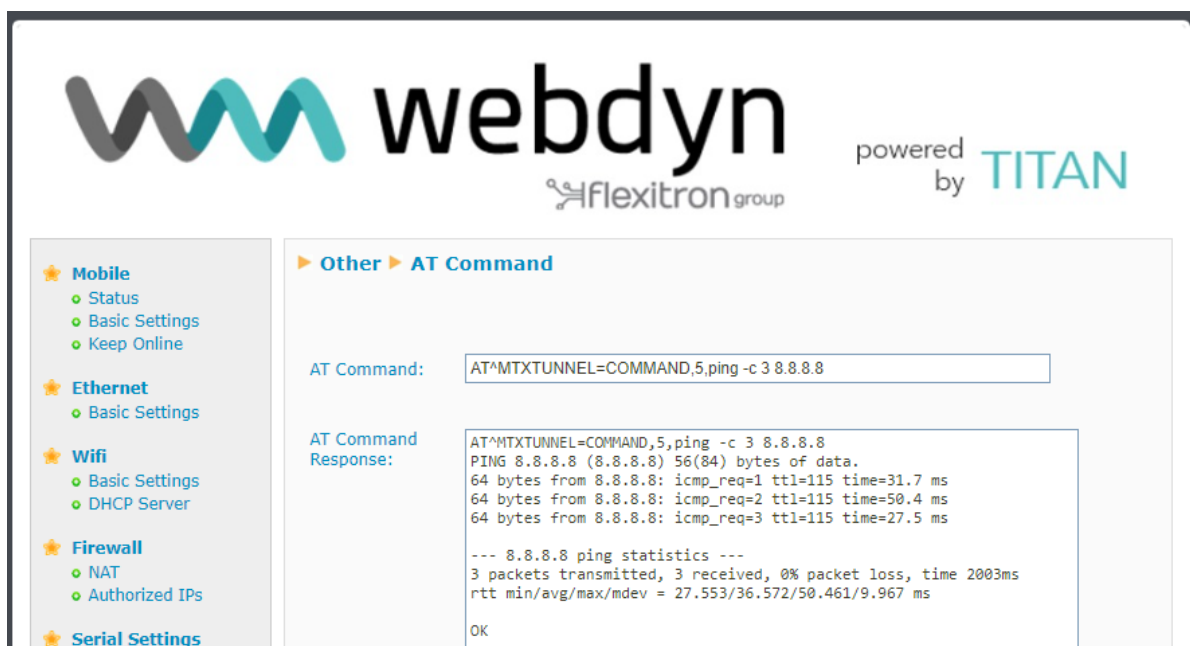
Parámetros:

<timeout>: 1 ... 60 segundos de timeout

<command>: ping, traceroute

Ejemplo: AT^MTXTUNNEL=COMMAND,5,ping -c 3 8.8.8.8

(Este ejemplo ejecutaría 3 PINGs a la IP 8.8.8.8 con un timeout de 5 segundos)

**Comandos AT relacionados con MODBUS:**

- **AT^MTXTUNNEL=GETMODBUS,<modbusAddress>;<addressFirstRegister>;<numWords>;<comand>**

Acción: Devuelve el valor de uno o varios registros Modbus de un dispositivo. Atención: los parámetros relacionados con modbus están separados por “;” no por “,”

Parámetros:

<modbusAddress>: dirección del equipo Modbus (1 ... 255) o dirección IP@dir:puerto

<addressFirstRegister>: dirección del primer registro a leer (0 ... 65535)

<numWords>: número de registros Modbus a leer (1 ... 64)

<command>: Comando modbus de escritura (5,6,15,16)

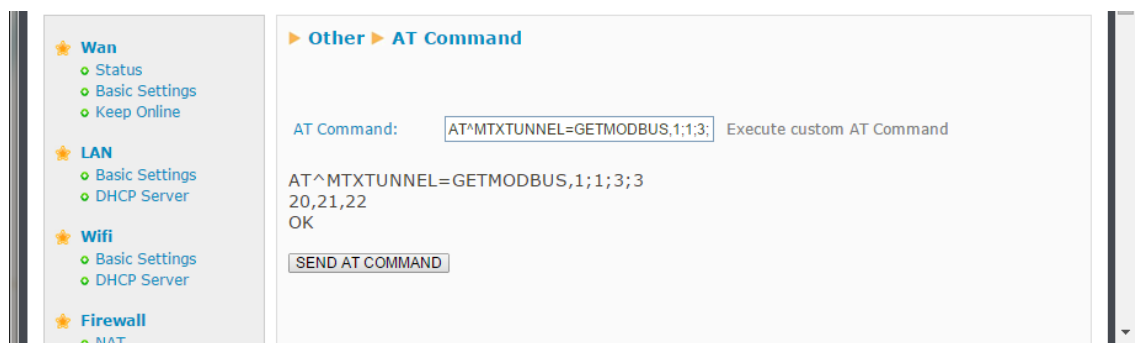
Resultado:

OK: Comando ejecutado correctamente. Devolverá los words leídos separados por “,”

ERROR: Comando ejecutado con error

Ejemplo: AT^MTXTUNNEL=GETMODBUS,192.168.1.200:502;1;1;3;3

enviado desde el entorno de configuración Web (aunque podría enviarse igualmente por SMS o por Remote Console (Telnet)), obteniendo como respuesta los valores 20,21,22



- **AT^MTXTUNNEL=SETMODBUS,<modbusAddress>;<addressFirstRegister>;<command>;<data1>;<data2>;< ...dataX>**

Acción: Establece el valor de uno o varios registros Modbus en un dispositivo. Atención: los parámetros relacionados con modbus están separados por “;” no por “,”

Resultado:

OK: Comando ejecutado correctamente

ERROR: Comando ejecutado con error

Parámetros:

<modbusAddress>: dirección del equipo Modbus (1 ... 255) o dirección IP@dir:puerto

<addressFirstRegister>: dirección del primer registro a escribir (0 ... 65535)

<command>: Comando modbus de escritura (5,6,15,16)

-<data1>, .. <dataX>: valores de los registros Modbus a escribir (0 ... 65535)

Ejemplo: AT^MTXTUNNEL=SETMODBUS,1;3;16;10;11;12;13;14;15

escribe en el dispositivo Modbus RTU con dirección 1, empezando en el registro 3 y utilizando el comando Modbus de escritura 16, los valores 10,11,12,13,14 y 15.

Ejemplo: AT^MTXTUNNEL=SETMODBUS,192.168.1.202@1:502;3;16;10;11;12;13;14;15

escribe en el dispositivo Modbus TCP con dirección IP **192.168.1.202** usando la dirección RTU **@1** y el puerto TCP **502**, empezando en el registro **3** y utilizando el comando Modbus de escritura **16**, los valores 10,11,12,13,14 y 15.

Ejemplo: AT^MTXTUNNEL=SETMODBUS,**1**;**3**;**6**;10

escribe en el dispositivo Modbus RTU con dirección **1**, en el registro **3** y utilizando el comando Modbus de escritura **6**, el valor 10

Ejemplo: AT^MTXTUNNEL=SETMODBUS,**1**;**18**;**5**;1

escribe en el dispositivo Modbus RTU con dirección **1**, en el coil **18** y utilizando el comando Modbus de escritura **5**, el valor 1

Ejemplo: AT^MTXTUNNEL=SETMODBUS,**1**;**25**;**15**;1;0;1;0;1

escribe en el dispositivo Modbus RTU con dirección **1**, a partir del coil **25** y utilizando el comando Modbus de escritura **15**, el valor de coils 1,0,1,0 y 1

Comandos AT relacionados con MQTT:

- AT^MTXTUNNEL= GETMQTTSTATUS[=<brokerId>]

Acción: devuelve el estado de conexión MQTT del equipo. Si no se especifica parámetro, se consulta el bróker Primary. El parámetro `<brokerId>` puede ser `primary`, `secondary` o `both`.

Resultado:

[1]: si el bróker indicado está conectado
[0]: si no está conectado.

Ejemplos:

AT^MTXTUNNEL=GETMQTTSTATUS

[1]

OK

AT^MTXTUNNEL=GETMQTTSTATUS=secondary

[0]

OK

Comandos AT relacionados con la hora del sistema:

- **AT^MTXTUNNEL=GETTIME**

Acción: Devuelve la hora actual del sistema en formato YYYY-MM-DDTHH:NN:SSZ (UTC)

Resultado:

OK: Comando ejecutado correctamente
ERROR: Comando ejecutado con error

Ejemplo:

```
AT^MTXTUNNEL=GETTIME
2016-21-05T10:56:52Z
OK
```

- **AT^MTXTUNNEL=SETTIME,<dateAndHour>**

Acción: Establece la hora actual.

Parámetros:

<dateAndHour> fecha / hora en formato UTC YYYY-MM-DDTHH:NN:SSZ

Resultado:

OK: Comando ejecutado correctamente
ERROR: Comando ejecutado con error

Ejemplo:

```
AT^MTXTUNNEL=SETTIME,2023-01-10T14:42:23Z
OK
```

Comandos AT relacionados con la configuración del dispositivo Titan:

- **AT^MTXTUNNEL=GETPARAM,<paramName>**

Acción: permite leer el valor de cualquier parámetro de configuración del equipo basado en TITAN. Por ejemplo, podrá consultar la configuración de cada parámetro desde una Plataforma Web o desde un dispositivo conectado al puerto Ethernet o Wifi del TITAN. Si hace doble click con el ratón sobre cualquier campo de cualquier página de configuración del TITAN obtendrá el nombre del campo.

Parámetros:

<paramName> nombre del parámetro de configuración a leer

Resultado:

OK: Lectura del parámetro de configuración correcta
ERROR: Error en la lectura del parámetro de configuración correcta

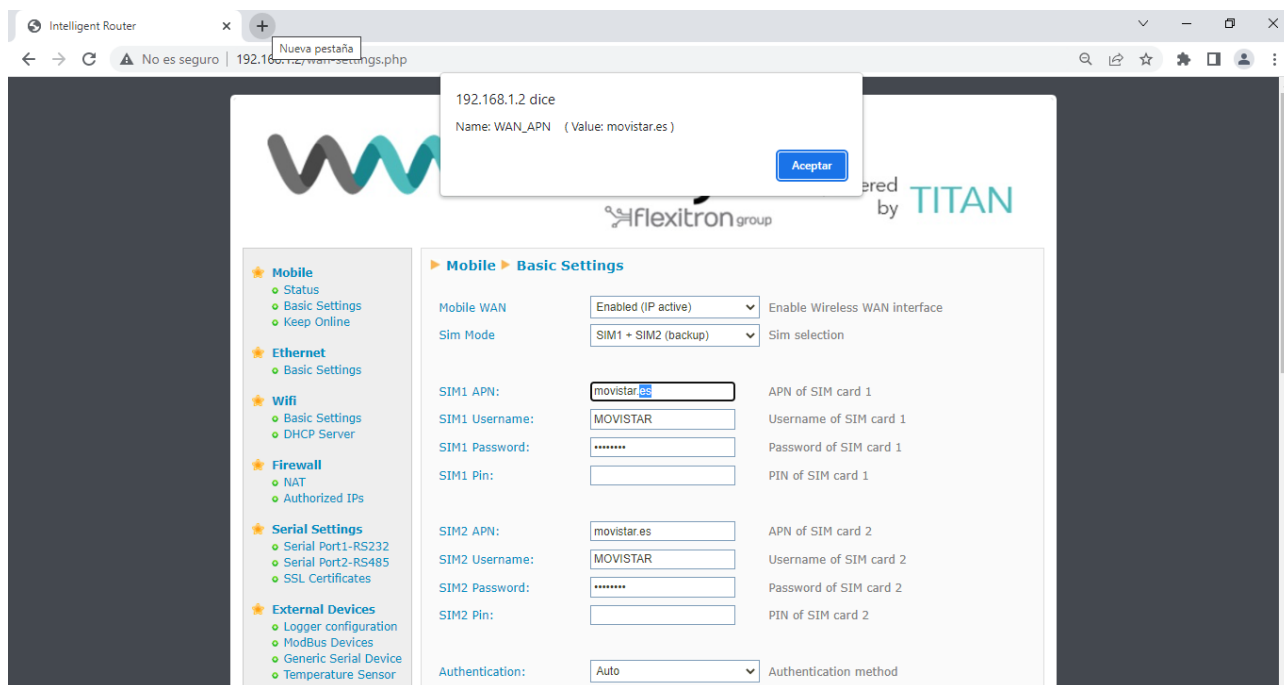
Ejemplo:

```
AT^MTXTUNNEL=GETPARAM,WAN_APN  
m2m.movistar.es  
OK
```

- **AT^MTXTUNNEL=SETPARAM,<paramName>,<paramValue>**

Acción: permite cambiar el valor de cualquier parámetro de configuración del equipo basado en TITAN. Por ejemplo, podrá cambiar la configuración de casi cualquier parámetro del equipo desde una Plataforma Web o desde un dispositivo conectado al puerto Ethernet o Wifi. Si hace doble click con el ratón sobre cualquier campo de cualquier página de configuración del dispositivo TITAN obtendrá el nombre del campo. Para poder ver el nombre del campo con “doble click” debe previamente enviar el comando AT:

```
AT^MTXTUNNEL=SETPARAM,MTX_SHOWNAMES,1
```



Parámetros:

<paramName> nombre del parámetro de configuración a modificar
<paramValue> Nuevo valor del parámetro de configuración

Resultado:

OK: El valor del parámetro de configuración se cambió correctamente
 ERROR: Error en el cambio de valor del parámetro de configuración.

Ejemplo:

AT^MTXTUNNEL=SETPARAM,WAN_APN,m2m.movistar.es
 OK

- **AT^MTXTUNNEL=SETFILE,<fileName>,<length>,<{data_base64}>**

Acción: de igual forma que el comando AT^MTXTUNNEL=SETPARAM permite cambiar mediante un comando AT el valor de un parámetro de configuración, este parámetro permite cambiar la configuración de los parámetros de tipo fichero (scripts, certificados, operadores,). El nombre del fichero aparece junto a las casillas de configuración correspondientes.

Parámetros:

<fileName> nombre del fichero

<length> longitud de datos del campo data_base64, sin contar las { }

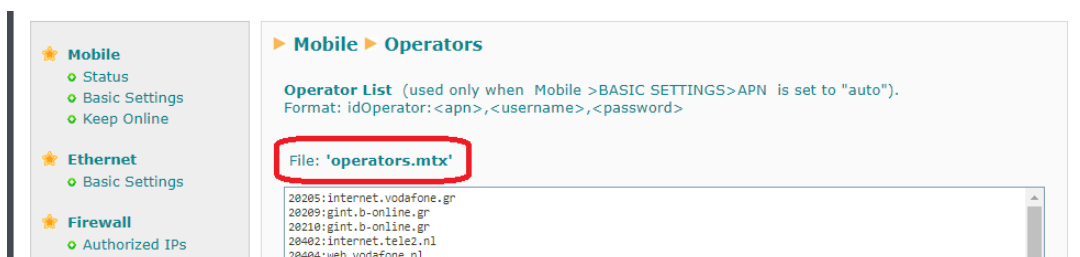
<{data_base64}>: datos del fichero codificados en base64. El texto debe indicarse entre { }

Resultado:

OK: El fichero fue cargado correctamente
 ERROR: Error en la ejecución del comando.

Ejemplo:

Por ejemplo, si desea modificar el fichero "operators.mtx" que se encuentra en la sección Mobile → Basic Settings → Operators



El comando AT a enviar sería:

```
AT^MTXTUNNEL=SETFILE,operators.mtx,220,{MjE0MDY6YWlydGVsbmV0LmVzCjlxNDA3Om1vdmIzdGFyLmVzLE1PVkItVEFSLE1PVkItVEFSCjlxNDA4OmludGVybmV0LmV1c2thbHRlbC5tb2JpCjlxNDE2OmludGVybmV0LnRlbGVjYWJsZS5lcwoyMTQxNzppbnRlcm5ldC5tdW5kby1yLmNvbQoyMTQxODppbnRlcm5ldC5vbm8uY29tCg==}
```

Nota: algunos links de utilidad para sus pruebas son los siguientes:

<https://www.base64encode.org/>

- **AT^MTXTUNNEL=GETFILEHASH,<fileName>**

Acción: devuelve el HASH de un fichero almacenado dentro del dispositivo.

Parámetros:

<fileName> nombre del fichero

Resultado:

{<HASH>}OK: HASH del fichero.

ERROR: Error en la ejecución del comando.

Ejemplo:

Por ejemplo, si desea consultar el HASH del fichero "operators.mtx"

AT^MTXTUNNEL=GETFILEHASH,operators.mtx

{06FD031D0CE8B58EA41A4E282047818E0EB74EFEEF3097F719968571DD7D8BC3}

OK

Comandos AT relacionados con contadores IEC-60870-5-102

- **AT^MTXTUNNEL=SETIEC102,<IDMETER>**

Acción: mediante la ejecución de este comando es posible forzar un inicio de lectura de los valores de tiempo real de un contador con protocolo IEC-60870-5-102. El servicio de la sección "External Devices → IEC102 Meter" debe estar activo y correctamente configurado.

Parámetros:

<IDMETER>: identificador del contador. Etiqueta configurada en la sección "External Devices → IEC102 Meter" o en el código de un script mediante la función `mtx.iec102AddMeter`

Resultado:

OK: Se inició el proceso.

ERROR: Error en el inicio del proceso

BUSY: Bus serie ocupado por una llamada CSD, pasarela IP-RS232

Ejemplo:

AT^MTXTUNNEL=SETIEC102,ID0001

OK

NOTA

Los valores instantáneos también se leen automáticamente cada Period minutos si tiene activado el servicio en External Devices › IEC102 Meter. Este comando solo es necesario si quiere forzar una lectura adicional fuera del ciclo.

- **AT^MTXTUNNEL=GETIEC102,<IDMETER>**

Acción: lectura del resultado de la ejecución del comando AT^MTXTUNNEL=SETIEC102,<IDMETER>. El servicio de la sección “External Devices →IEC102 Meter” debe estar activo y correctamente configurado.

Parámetros:

<IDMETER>: identificador del contador. Etiqueta configurada en la sección “External Devices →IEC102 Meter” o en el código de un script mediante la función mtm. iec102AddMeter

Resultado:

OK: Lectura correcta
ERROR: Error en la lectura o todavía no ha finalizado el proceso de lectura.

Ejemplo:

```
AT^MTXTUNNEL=GETIEC102,ID0001
{"IMEI":"869101054255506","TYPE":"IEC102","TS":"2023-01-
26T09:22:37Z","P":"MTX1","ID":"ID0001","VABA":0,"VABRI":0,"VABRC":0,"PAT":0,"
PRT":0,"FPT":1000,"PAF1":0,"PRF1":0,"FPF1":1000,"PAF2":0,"PRF2":0,"FPF2":100
0,"PAF3":0,"PRF3":0,"FPF3":1000,"IF1":0,"TF1":1156,"IF2":0,"TF2":1141,"IF3":0,"TF
3":1}
OK
```

- **AT^MTXTUNNEL=SETIEC102_CTAVM2, <IDMETER>, <hourIni>, <minuteIni>, <dayIni>, <monthIni>, <yearIni>, <hourEnd>, <minuteEnd>, <dayEnd>, <monthEnd>, <yearEnd>**

Acción: mediante la ejecución de este comando es posible forzar un inicio de lectura de los cierres fiscales (contrato I) de un contador con protocolo IEC-60870-5-102. El servicio de la sección “External Devices →IEC102 Meter” debe estar activo y correctamente configurado.

Parámetros:

<IDMETER>: identificador del contador. Etiqueta configurada en la sección “External Devices →IEC102 Meter” o en el código de un script mediante la función mtm. iec102AddMeter
<hourIni>: hora inicial del intervalo (0 ... 23)
<minuteIni>: minuto inicial del intervalo (0 ... 59)
<dayIni>: día inicial del intervalo (1 ... 31)
<monthIni>: mes inicial del intervalo (1 ... 12)
<yearIni>: año inicial del intervalo (20 ... 99)
<hourEnd>: hora final del intervalo (0 ... 23)
<minuteEnd>: minuto final del intervalo (0 ... 59)
<dayEnd>: día final del intervalo (1 ... 31)
<monthEnd>: mes final del intervalo (1 ... 12)
<yearEnd>: año final del intervalo (20 ... 99)

Resultado:

OK: Se inició el proceso.
ERROR: Error en el inicio del proceso
BUSY: Bus serie ocupado por una llamada CSD, pasarela IP-RS232

Ejemplo:

```
AT^MTXTUNNEL=SETIEC102_CTAVM2,ID001,0,0,22,12,22,0,0,24,1,23
OK
```

NOTA

El rango de fechas debe contener al menos un cierre fiscal completo. Los cierres ocurren al final de cada mes; pedir rangos a mitad de mes puede devolver "sin datos" aunque la comunicación funcione. Si quiere el último mes cerrado, use rangos del tipo 1/M-1/YY → 1/M/YY.

- **AT^MTXTUNNEL=GETIEC102_CTAVM2,<IDMETER>**

Acción: lectura del resultado de la ejecución del comando AT^MTXTUNNEL=SETIEC102_CTAVM2,<IDMETER>. El servicio de la sección "External Devices → IEC102 Meter" debe estar activo y correctamente configurado.

Parámetros:

<IDMETER>: identificador del contador. Etiqueta configurada en la sección "External Devices → IEC102 Meter" o en el código de un script mediante la función `mtx.iec102AddMeter`

Resultado:

OK: Lectura correcta
 ERROR: Error en la lectura o todavía no ha finalizado el proceso de lectura.

Ejemplo:

```
AT^MTXTUNNEL=GETIEC102_CTAVM2,ID001
{"IMEI":"869101054255506","TYPE":"IEC102_CTAVM2","TS":"2023-01-26T09:41:29Z","P":"MTX1","ID":"ID001","CTAVM2":[{"DO":20,"EaA":0,"EiA":0,"CA":2,"EaRi":0,"EiRi":0,"CRi":2,"EaRc":0,"EiRc":0,"CRc":2,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-0","CMA":2,"EPA":0,"CE":128,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-09T12:58-0"},{"DO":21,"EaA":0,"EiA":0,"CA":2,"EaRi":0,"EiRi":0,"CRi":2,"EaRc":0,"EiRc":0,"CRc":2,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-0","CMA":2,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-09T12:58-0"},{"DO":22,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"CRc":0,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-09T12:58-0"},{"DO":23,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"CRc":0,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-09T12:58-0"},{"DO":24,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"CRc":0,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-09T12:58-0"},{"DO":25,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"CRc":0,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-09T12:58-0"},{"DO":26,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"CRc":0,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-0"}]}
```

0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-09T12:58-0"}}}
OK

- **AT^MTXTUNNEL=SETIEC102_CCINX2, <IDMETER>, <hourIni>, <minuteIni>, <dayIni>, <monthIni>, <yearIni>, <hourEnd>, <minuteEnd>, <dayEnd>, <monthEnd>, <yearEnd>, <absoluteIncremental>, <period>**

Acción: mediante la ejecución de este comando es posible forzar un inicio de lectura de los totales integrados (curva de carga) de un contador con protocolo IEC-60870-5-102. El servicio de la sección "External Devices → IEC102 Meter" debe estar activo y correctamente configurado.

Parámetros:

<IDMETER>: identificador del contador. Etiqueta configurada en la sección "External Devices → IEC102 Meter" o en el código de un script mediante la función `mtx. iec102AddMeter`

<hourIni>: hora inicial del intervalo (0 ... 23)

<minuteIni>: minuto inicial del intervalo (0 ... 59)

<dayIni>: día inicial del intervalo (1 ... 31)

<monthIni>: mes inicial del intervalo (1 ... 12)

<yearIni>: año inicial del intervalo (20 ... 99)

<hourEnd>: hora final del intervalo (0 ... 23)

<minuteEnd>: minuto final del intervalo (0 ... 59)

<dayEnd>: día final del intervalo (1 ... 31)

<monthEnd>: mes final del intervalo (1 ... 12)

<yearEnd>: año final del intervalo (20 ... 99)

<absoluteIncremental>: tipo de ASDU enviado al contador.

0 → ASDU 122 (C_CI_NT_2, absoluto)

1 → ASDU 123 (C_CI_NU_2, incremental)

Importante: No todos los contadores implementan ambos modos. Si recibe ERROR repetidamente con uno de los dos, pruebe el otro.

<regSelector>: selector de dirección de registro. Añade un offset a la dirección de registro 11 que es donde se guarda la curva estándar según la normativa de la Red Eléctrica de España (REE). Debido a la flexibilidad que proporciona la norma en este aspecto, los fabricantes de los contadores pueden usar para este propósito otros registros considerados como "reserva":

0 → registro 11 (curva estándar REE)

1 → registro 12 (RESERVA según REE, comportamiento depende del fabricante)

Algunos contadores solo aceptan registro 11 con cierto ASDU; otros solo aceptan registro 12 con otro ASDU. Si con el valor 0 falla, pruebe 1 antes de descartar el contador.

Resultado:

OK: Se inició el proceso.
ERROR: Error en el inicio del proceso
BUSY: Bus serie ocupado por una llamada CSD, pasarela IP-RS232

Ejemplo:

AT^MTXTUNNEL=SETIEC102_CCINX2,ID001,15,0,19,1,23,20,0,19,1,23,1,0
OK

NOTA → Funcionamiento de la pareja **SETIEC102_CCINX2/ GETIEC102_CCINX2**:

El SET siempre devuelve OK con tal de que el formato sea correcto: solo encola una petición. La comunicación real con el contador la realiza un hilo interno que comprueba la cola cada ~5 segundos.

Después del SET hay que esperar entre 20 y 30 segundos antes de lanzar el GET. El GET devolverá ERROR mientras la lectura esté en curso o si ha fallado, y devolverá el JSON con los datos solo cuando la lectura haya terminado correctamente.

• **AT^MTXTUNNEL=GETIEC102_CCINX2,<IDMETER>**

Acción: lectura del resultado de la ejecución del comando AT^MTXTUNNEL=SETIEC102_CCINX2,<IDMETER>. El servicio de la sección "External Devices → IEC102 Meter" debe estar activo y correctamente configurado.

Parámetros:

<IDMETER>: identificador del contador. Etiqueta configurada en la sección "External Devices → IEC102 Meter" o en el código de un script mediante la función `mtx.iec102AddMeter`

Resultado:

OK: Lectura correcta
ERROR: Error en la lectura o todavía no ha finalizado el proceso de lectura.

Ejemplo:

AT^MTXTUNNEL=GETIEC102_CCINX2,ID001

```
{"IMEI":"869101054255506","TYPE":"IEC102_CCINX2","TS":"2023-01-26T09:54:10Z","P":"MTX1","ID":"ID001","CCINX2":[{"DO":11,"TI1":0,"TI2":0,"TI3":0,"TI4":0,"TI5":0,"TI6":0,"TI7":0,"TI8":0,"Q1":0,"Q2":0,"Q3":0,"Q4":0,"Q5":0,"Q6":0,"Q7":128,"Q8":128,"DATE":"2023-01-19T15:00-00"},{"DO":11,"TI1":0,"TI2":0,"TI3":0,"TI4":0,"TI5":0,"TI6":0,"TI7":0,"TI8":0,"Q1":0,"Q2":0,"Q3":0,"Q4":0,"Q5":0,"Q6":0,"Q7":128,"Q8":128,"DATE":"2023-01-19T16:00-00"},{"DO":11,"TI1":0,"TI2":0,"TI3":0,"TI4":0,"TI5":0,"TI6":0,"TI7":0,"TI8":0,"Q1":0,"Q2":0,"Q3":0,"Q4":0,"Q5":0,"Q6":0,"Q7":128,"Q8":128,"DATE":"2023-01-19T17:00-00"},{"DO":11,"TI1":0,"TI2":0,"TI3":0,"TI4":0,"TI5":0,"TI6":0,"TI7":0,"TI8":0,"Q1":0,"Q2":0,"Q3":0,"Q4":0,"Q5":0,"Q6":0,"Q7":128,"Q8":128,"DATE":"2023-01-19T18:00-00"},{"DO":11,"TI1":0,"TI2":0,"TI3":0,"TI4":0,"TI5":0,"TI6":0,"TI7":0,"TI8":0,"Q1":0,"Q2":0,"Q3":0,"Q4":0,"Q5":0,"Q6":0,"Q7":128,"Q8":128,"DATE":"2023-01-19T19:00-00"},{"DO":11,"TI1":0,"TI2":0,"TI3":0,"TI4":0,"TI5":0,"TI6":0,"TI7":0,"TI8":0,"Q1":0,"Q2":0,"Q3":0,"Q4":0,"Q5":0,"Q6":0,"Q7":128,"Q8":128,"DATE":"2023-01-19T20:00-00"}]}
```

OK

Siendo DO: dirección del objeto

Tlx, donde x=1...8, los totales integrados, donde:

Dirección	Objeto de Información
1	Totales Integrados de Activa Entrante.
2	Totales Integrados de Activa Saliente
3	Totales Integrados de Reactiva primer cuadrante
4	Totales Integrados de Reactiva segundo cuadrante
5	Totales Integrados de Reactiva tercer cuadrante
6	Totales Integrados de Reactiva cuarto cuadrante
7	Datos de reserva 1
8	Datos de reserva 2

Qx, donde x=1...8, los cualificadores, donde:

Bit	Iden.	Descripción
7	IV	La lectura es válida (IV=0)
6	CA	Contador sincronizado durante el período (CA=1)
5	CY	Overflow (CY=1)
4	VH	Verificación horaria durante el período (VH=1)
3	MP	Modificación de parámetros durante el período (MP=1)
2	INT	Se produjo un intrusismo durante el período (INT=1)
1	AL	Período incompleto por fallo de alimentación en el período (AL=1)
0	RES	Reserva. Nótese su empleo en Tarificación.

NOTA →Funcionamiento de la pareja **SETIEC102_CCINX2/ GETIEC102_CCINX2**:

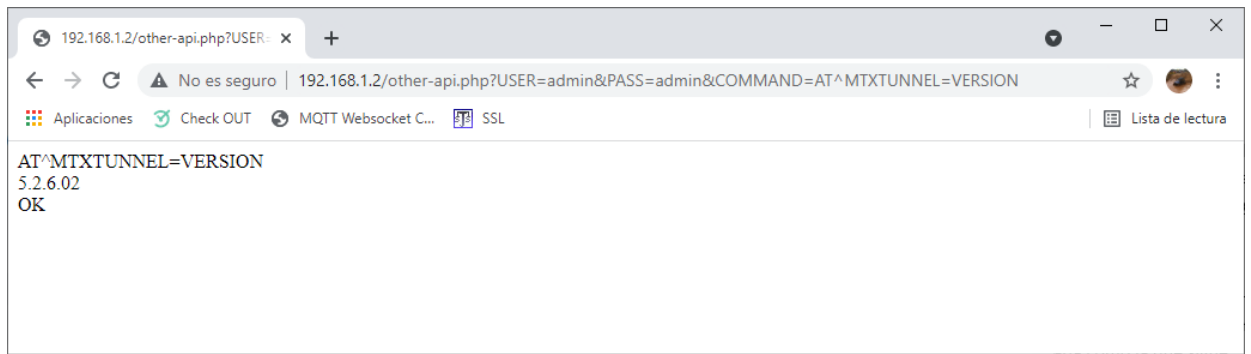
El SET siempre devuelve OK con tal de que el formato sea correcto: solo encola una petición. La comunicación real con el contador la realiza un hilo interno que comprueba la cola cada ~5 segundos.

Después del SET hay que esperar entre 20 y 30 segundos antes de lanzar el GET. El GET devolverá ERROR mientras la lectura esté en curso o si ha fallado, y devolverá el JSON con los datos solo cuando la lectura haya terminado correctamente.

Para el resto de los comandos estándar consulte en el manual de comandos AT del módulo interno gsm del equipo basado en TITAN para obtener información sobre el formato y la funcionalidad exacta de cada uno de los comandos del módulo. Si no dispone de la documentación solicítela en contact@webdyn.com

Además del envío de comandos AT por SMS, Telnet, Modbus TCP, ... es posible enviar comandos AT vía HTTP GET tanto de forma local como remota. Por ejemplo, para ejecutar un comando de lectura de temperatura del módulo GSM, bastaría con hacer una llamada como la que sigue:

http://192.168.1.2/other-api.php?USER=admin&PASS=admin&COMMAND=AT^MTXTUNNEL=VERSION



6.- Novedades en versiones de Firmware

- 6.17** - Posibilidad de lectura autónoma de las curvas de carga para contadores IEC-60870-5-102 desde un Script. Nuevas funciones de SCRIPT `mtx.iec102SetIntegratedTotal` y `mtx.iec102GetIntegratedTotal`.
- Nuevo SCRIPT de ejemplo 52, donde se muestra cómo leer las curvas de carga de un contador IEC-60870-5-102.
- Nuevos comandos `AT^MTXTUNNEL=SETIEC102_CCINX2` y `AT^MTXTUNNEL = GETIEC102_CCINX2` para la lectura de de las curvas de carga para contadores IEC-60870-5-102
- 6.18** - Mejoras en la gestión de las conexiones TCP Client ante la pérdida de contexto.
- 6.19.-** - Filtrado por MAC desde la sección "Firewall → Mac Filter"
- IEC60870-5.102. Añadido parámetros (`patDir`, `paf1Dir`, `paf2Dir`, `paf3Dir`) para especificar energía importada/exportada en el JSON de valores de energía instantáneos.
- IEC60870-5.102. Nuevo parámetro de configuración en la sección "External Devices → Meter 102" que permite asignar signo a los parámetros `pat/fpt`, `paf1/fpf1`, `paf2/fpf2`, `paf3/fpf3`
- Mejoras estéticas en la pantalla de programación de los Titan Scripts
- Añadido método HTTP PUT y HTTPS PUT en las opciones de envío del LOGGER y de los SCRIPTS.
- Modificación del SCRIPT ejemplo 39 incluyendo el método HTTP PUT.
- Nueva función `mtx.loggerSendingEnabled` para la sección SCRIPTS. Mediante esta función es posible habilitar / deshabilitar el servicio de envío de los datos almacenados en el LOGGER.
- Nuevo SCRIPT de ejemplo 7b. Lectura de un registro modbus TCP.
- Nuevo SCRIPT de ejemplo 14b. Lectura de registros modbus RTU, personalización del JSON de envío, almacenamiento en LOGGER y programación de envío dentro de un horario específico.
- Nuevo comando `AT^MTXTUNNEL=GETFILEHASH, <filename>` que permite leer el HASH de un fichero interno de configuración.
- 6.20.-** - Corregido problema por el que no era posible enviar por SMS los caracteres especiales `^` `_`
- Mejora en la gestión de envíos de SMSs desde los script
- En el campo "ID String" de las pasarelas IP-Serie de tipo cliente es posible especificar los tags [IMEI] , [CR] y [LF] para que éstos sean automáticamente reemplazados por el IMEI y los caracteres especiales `0x13` y `0x10`
- Nuevas funciones para los scripts: `mtx.convert2WordToUnsignedInt32` , `mtx.convert2WordToSignedInt32` , `mtx.convert2WordToFloat32` , `mtx.convert4WordToSignedInt64` útiles para conversiones de datos modbus
- Añadido el comando de escritura modbus `0x06`

- Nuevas funciones para los scripts `mtx.configParamGet` y `mtx.configParamSet` que permiten leer la configuración del router y cambiarla desde los scripts.
 - Añadidos los scripts de ejemplo 53 y 54 de lectura de contadores DLMS
- 6.21.-**
- Posibilidad de editar dispositivos Modbus dados de alta en la sección “External Devices → Modbus Devices”
 - Soporte para el nuevo dispositivo WEBDYN-EXPERT-ROUTER
- 6.22.-**
- Soporte para lectura autónoma de contadores con protocolo IEC-60870-5-102 mediante una interfaz de sonda óptica.
 - Soporte para el nuevo dispositivo WEBDYN-EASY-ROUTER
- 6.24.-**
- Nueva característica de actualización de firmware mediante OTAP.
 - Nuevas opciones de configuración de la característica SIM SWAP para equipos con DUAL SIM.
 - Opción de cierre automático de sesiones con protocolo IEC-60870-5-102 para las pasarelas TCP Server - RS232/RS485
- 6.25.-**
- Nueva característica VPN “ZeroTier”. Nueva nota de aplicación AN71.
 - Nueva característica de lectura de dispositivos modbus “Modbus Expert”. Nueva nota de aplicación AN72.
 - Nueva característica para configuraciones desde un PC para producciones masivas. Nueva nota de aplicación AN73.
- 6.30**
- Método de autenticación para HTTP (GUI), Telnet y SSH por LDAP.
 - Nuevo asistente de inteligencia artificial como ayuda para el desarrollo de scripts.
 - Nuevas funciones de script relacionadas con chatGPT
 - Nueva función de script para el uso de HASH SHA256
 - Nota de aplicación AN74 para de uso de autenticación por TACACS+
 - Nota de aplicación AN74 para de uso de autenticación por LDAP.
 - Nota de aplicación AN75 explicativa sobre la herramienta “Titan Script Assistant” de inteligencia artificial.
 - Nuevos Scripts de ejemplo relacionados con la API de chatGPT para análisis de datos textuales e imágenes.
 - Nuevo tipo de datos UINT64 en la sección de Modbus Expert
 - Nuevos métodos de flip de doble word en la sección de Modbus Expert
 - Nuevas funciones del objeto “mtx” para scripts: `mtx.modbusExpertGetStatus`, `mtx.modbusExpertGetReg`, `mtx.modbusExpertSetReg`, `mtx.modbusExpertSetV`, `mtx.modbusExpertSetV`

6.35

- Nota de aplicación AN78 en la que se muestra cómo usar el servicio Modbus Experts junto con los Titan Script para la expansión de las E/S del router utilizando un dispositivo modbus Externo con entradas digitales, entradas analógicas y salidas digitales.
- Nota de aplicación AN79 en la que se muestra cómo implementar una pasarela Modbus TCP a SNMP (para proporcionar comunicaciones SNMP a dispositivos Modbus TCP que no cuenten con SNMP).
- Nota de aplicación AN80 en la que se muestra cómo implementar una pasarela Modbus RTU a SNMP (para proporcionar comunicaciones SNMP a dispositivos Modbus RTU que no cuenten con SNMP).
- Modificación (sobrecarga) de la función de scripts "trapSend" permitiendo nuevos parámetros.
- Nueva función snmpModbusSetMode para los scripts que permite definir el comportamiento del Titan ante un comando SET SNMP recibido cuando trabaja como pasarela modbus – snmp.
- Nueva función que permite enviar comandos AT a través de 1 puerto serie de los router Titan. Esto permite utilizar el router casi como si se tratara de un módem convencional (para envío de SMS, realización y recepción de llamadas CSD, etc).
- Nuevas funciones para scripts "mtx.trapRXServiceStart_v1_v2c", "mtx.trapRXServiceStop", "mtx.trapRXGet"
- Nota de aplicación AN80 que muestra cómo implementar una pasarela de TRAPS SNMP recibidos a alertas SMS.
- Nuevo ejemplo 3b en la sección de Titan Scripts para realizar una llamada GSM de audio antes el cambio de una entrada digital.
- Nuevo ejemplo 60 en la sección de Titan Scripts para implementar una pasarela de TRAPS SNMP recibidos a alertas SMS.

6.36

- Nuevos parámetros de configuración añadidos.

6.40

- Nueva funcionalidad para poder leer contadores eléctricos con protocolo IEC60870-5-102 y puerto Ethernet.
- Añadidos nuevos comandos AT.
- Corregidos errores menores.
- Corregido bug en FTPS relacionado con error "522 SSL connection failed: session reuse required"
- Posibilidad de leer las curvas cuarto-horarias en modo ABSOLUTO y no sólo en modo INTERVALO
- Corregido bug en processFrame_C_CI_Nx_2: el parser solo aceptaba ASDU 0x0B y 0x15 en las tramas de datos. Algunos contadores responden con ASDU 0x08, lo que provocaba que la lectura de la curva de carga en modo absoluto fallara, aunque la trama del contador fuera correcta.

6.41

- Se guarda el valor de los contadores en EEPROM.

6.42

- Añadidos nuevos parámetros de configuración relacionados con los puertos COM.
- Se añade compatibilidad con el módulo de Quectel EC21-A

7.01

- Añadido sección para nueva plataforma KARE
- Mejoras generales de ciberseguridad para normativa RED DA.
- Longitud mínima de passwords de entrada se incrementan de 10 a 17 caracteres
- Longitud mínima de passwords de SNMPv3 se incrementan de 10 a 17 caracteres y se exige mínimo 1 mayúscula, 1 minúscula y 1 número
- Longitud mínima de passwords de WIFI se incrementan de 10 a 17 caracteres y se exige mínimo 1 mayúscula, 1 minúscula y 1 número
- Para HTTPS se genera un certificado de 3072 bits.
- OTAP: longitud de las claves de las firmas aumentada a 3072 bits.
- Mejoras en OpenVPN server al limitar a TLS1.2 con ciphers modernos.
- Corregidos bugs referentes a la sección de IEC102
- Corregido bug de FTP que hacía que los archivos generados se envían sin la estructura de array JSON, es decir, no se incluyen los corchetes [] que deberían encapsular los registros.

7.02

- Soporte para doble cliente MQTT: Primary MQTT Client y Secondary MQTT Client.
- Posibilidad de seleccionar el bróker MQTT de destino en logger, Private DynDNS, syslog, zlog, pasarelas Serie-MQTT y TITAN Scripts.
- Añadida política de confirmación MQTT del logger cuando se envía a ambos brókers: Any o All.
- Añadido soporte de certificados MQTTS independientes para el bróker Primary y Secondary.
- Los comandos AT recibidos por MQTT pueden gestionarse también desde el bróker secundario.
- Añadidas nuevas funciones MQTT para TITAN Scripts con selección de bróker.
- Añadida función `topicScriptEx(brokerId, topic, data)` para identificar el bróker MQTT que ha recibido el mensaje.
- Añadidas funciones de TITAN Scripts para obtener en JSON los valores de dispositivos Modbus Expert.
- Nuevo ejemplo 61 de TITAN Scripts para envío MQTT a Primary, Secondary o Both.
- Nuevo ejemplo 62 de TITAN Scripts con funciones Modbus Expert.
- Posibilidad de configurar hasta tres direcciones IP destino para TRAPS SNMP.
- Añadida prioridad configurable de pasarelas Modbus TCP/RTU sobre lecturas Modbus de TITAN Scripts y lecturas autónomas.
- Añadido timeout de inactividad configurable para pasarelas Modbus TCP/RTU.
- Añadido aviso inicial recomendando el uso de HTTPS tras la configuración de la contraseña de administración.
- Corregido el estado MQTT mostrado cuando se utiliza LAN privada con MQTT privado.
- Corregido el autoreset diario a las 00:00 cuando se utiliza el modo por horas.

SALES CONTACT

SPAIN

C/ Alejandro Sánchez 109
28019 Madrid

Phone 1: 902.19.81.46
Phone 2: +34-91.560.27.37
Email: contact@webdyn.com

FRANCE

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

Phone: +33.139042940
Email: contact@webdyn.com

INDIA

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

Phone: +91.1141519011
Email: contact@webdyn.com

PORTUGAL

LusoMatrix Lda.
Av. Coronel Eduardo Galhardo 7-1°C
1170-105 Lisbon, Portugal

Phone: +351.218162625
Email: comercial@lusomatrix.pt

SUPPORT

Madrid Offices

Phone: +34.915602737
Email: iotsupport@matrix.es

Saint-Germain-en-Laye Offices

Phone: +33.139042940
Email: support@webdyn.com

Delhi Offices

Phone: +91.1141519011
Email: support-india@webdyn.com

