



MTX-StarEnergy-E

Software User Manual

Index

General Notes	4
Important Information	4
Revisions.....	4
User Manual	5
1. Introduction	5
2. Step-by-Step Configuration.....	6
3. Configuration.....	8
3.1 WAN	8
3.1.1 WAN: Status	8
3.1.2 WAN: Basic Settings	9
3.1.3 WAN: Keep Online.....	10
3.2 LAN	12
3.2.1 LAN: Basic Settings	12
3.3 Firewall	13
3.3.1 Firewall: Authorized IPs	13
3.4 Serial Settings: Serial PortX.....	14
3.5 VPN: IPSec	16
3.5.1 Other: AT Command.....	17
3.5.2 Other: Meter Connected.....	19
3.5.3 Other: SMS Control.....	20
3.5.4 Other: Periodic Auto-reset.....	21
3.5.5 Other: Time Servers (NTP)	22
3.5.6 Other: Remote Console (TCP Server)	23
3.5.7 Other: SNMP	24
3.5.8 Other: TACACS+.....	41
3.5.9 Other: HTTPS.....	42
3.5.10 Other: User Permissions	44
3.5.11 Other: Passwords	45
3.5.12 Other: CA Certificates.....	46
3.5.13 Other: Syslog.....	47

3.5.14 Other: Backup/Factory.....	49
3.5.15 Other: Firmware Upgrade.....	51
4. AT commands	52
5. LEDs	55
1. Appendix:	57
1.1 Example - Remote FW update via SFTP and SNMP, using an AT command, but without prior SFTP configuration.....	57
1.2 Example - Remote FW update via SFTP and SNMP, using an AT command with prior SFTP configuration.....	60
1.3 Example - Remote CONFIGURATION update via SFTP and SNMP, using an AT command, but without prior SFTP configuration.....	64
1.4 Example - Configuring the MTX-StarEnergy router to send SNMP alerts.....	66
Offices and support.....	70

General Notes

The product is deemed to have been accepted by the recipient and is provided without an interface for the recipient's products. The documentation and/or the product are provided for testing, evaluation, integration and information purposes. The documentation and/or products are provided "as is" and may include defects. The documentation and/or products are provided without a warranty of any kind, either express or implied. To the fullest extent permitted by the applicable laws, Matrix Electronics further disclaims all guarantees; including, but not limited to, all implied guarantees of merchantability, integrity, fitness for a particular purpose, and non-infringement of third party rights. All risks arising out of the use or performance of the product or the documentation are borne by the recipient. This product is not intended for use in life support devices or systems where a malfunction of the product can reasonably be expected to result in personal injury. Applications incorporating the described product must be designed in accordance with the technical specifications provided in these guidelines. Failure to follow any of the required procedures may result in a malfunction or serious discrepancies in the results. Furthermore, all safety instructions related to the use of mobile technical systems, including GSM products, which also apply to cell phones, must be strictly followed. Regardless of the legal theory on which a claim may be based, neither Matrix Electronics nor its suppliers shall be held liable for any consequential, incidental, direct, indirect, punitive or other damages (including, without limitation, damages for lost profits, interruption of business, loss of business data or information, or other pecuniary losses) arising from the use, or inability to use, the documentation and/or the product, even if Matrix Electronics has been advised of the possibility of such damages occurring. The foregoing limitations of liability shall not apply in the event of mandatory liability, e.g. pursuant to the Spanish Product Liability Law, or in the event of intent, gross negligence, injury to life, body and health, or breach of a condition in relation to the contract. However, claims for damages arising from a breach of a condition relating to the contract, shall be limited to the foreseeable damage which is intrinsic to the contract, unless caused by intent or gross negligence, or is based on the liability for injury to life, body and health. The aforementioned provision does not imply a change in the burden of proof to the detriment of the recipient. Subject to change without notice. The interpretation of this general note will be governed and interpreted in accordance with Spanish law, without reference to any other substantive law.

Important Information

This technical description contains important information for the launch and use of the MTX-StarEnergy-E device. Please read it carefully before you start work with the equipment. The warranty will be void if damage occurs due to non-compliance with these instructions. We cannot accept liability for related losses.

Revisions

REVISION	DATE
5.2.4.10.7.14	2021/05

User Manual

1. Introduction

The MTX-StarEnergy modem/router is a device belonging to the Titan router family. It has been specifically designed to be used in scenarios involving the remote reading of energy meters.

We provide free, fast and efficient support to all users of MTX modems and routers when required. If you still have questions after reading this manual, do not hesitate to write to us at the following email address: iotsupport@mtxm2m.com. Similarly, if you need a feature which is not included in our routers, or if you need a special customization, please let us know and we will perform a study to include it.

2. Step-by-Step Configuration

The MTX-StarEnergy router is configured using a Web environment.

The MTX-StarEnergy router uses a USB port to create a network connection providing access to said Web configuration environment.

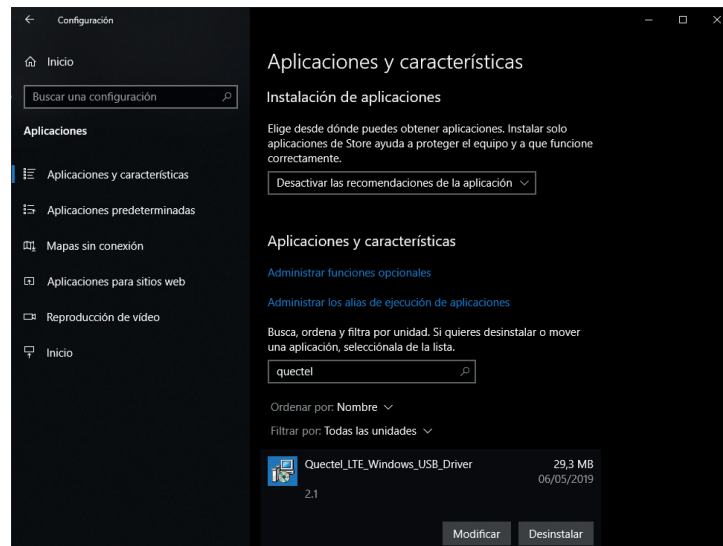
Minimum Requirements

- A PC with Windows 10, and a Web browser (Chrome, IExplorer, Firefox, etc.) and a USB port.
- A USB cable to connect the PC to the MTX-StartEnergy router.

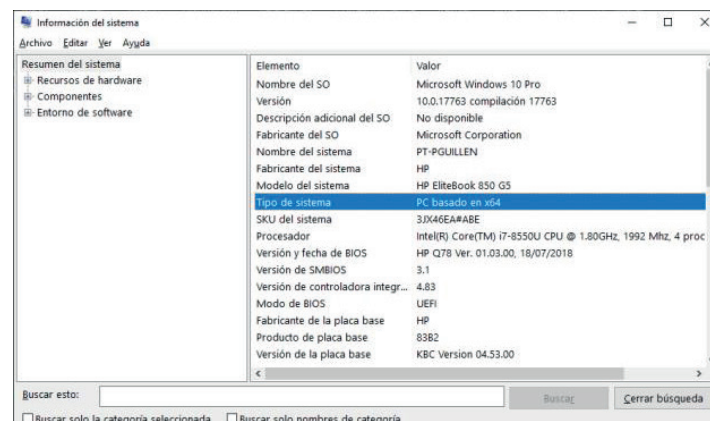
Installing the USB Driver

If you don't already have the drivers installed on your computer, this is the first thing you should do. The steps to install the driver are as follows:

- Unzip the file “1_Quectel_LTE_Windows_USB_Driver_V2.1.5.zip” and run the program “setup.exe”.



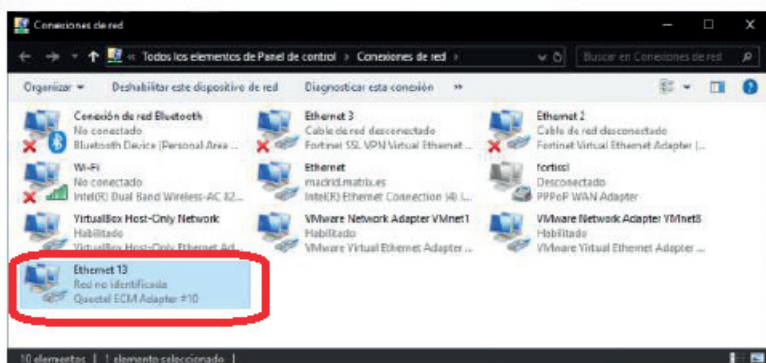
- Check if you are using a 32-bit or 64-bit system. To do this, go to the Windows start menu and type in "System Information", a window similar to the following will appear:



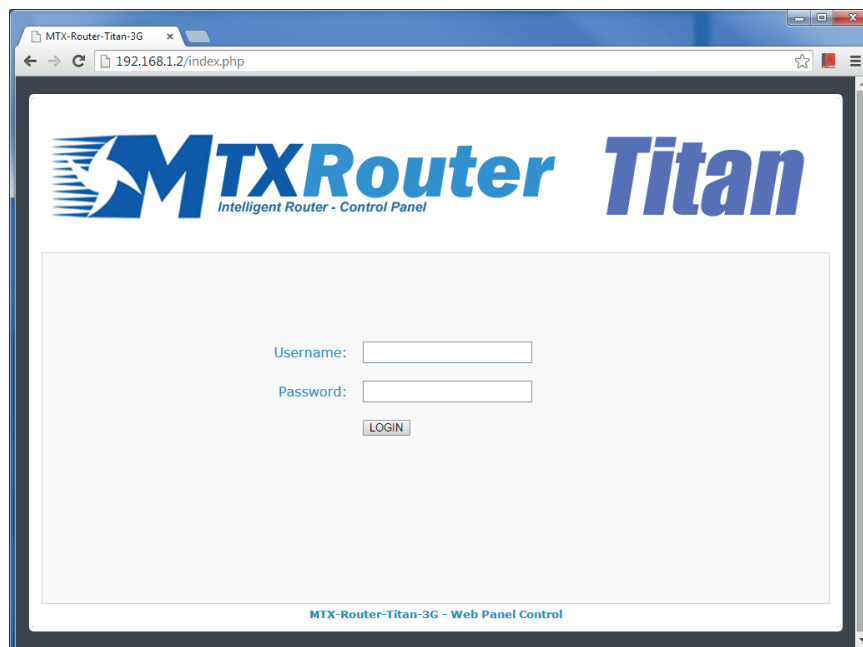
- Unzip the file “2_quectel_ecm_drivers_v1.02.0505.zip”.

Run ecm_driver_setup.exe for 64 or 32 bit depending on your system, select option “1” and press “ENTER”.

- Insert a SIM card into the MTX-StarEnergy router and connect the antenna. Then power on the device and connect it to your PC using the USB cable.
- Go to the “Network Connections” menu (type “View network connections” in the Windows Start menu) and check that a network connection named Quectel ECM has been created, as shown below.



- In the interface’s connection properties, configure a network address with IP 192.168.1.X, where X is not 2 (192.168.1.2 is the default IP address of the MTX-StarEnergy router).
- Open a browser and go to the MTX-StarEnergy router’s configuration web interface at <http://192.168.1.2>. The default username is “admin” and the password is “admin”.



3. Configuration

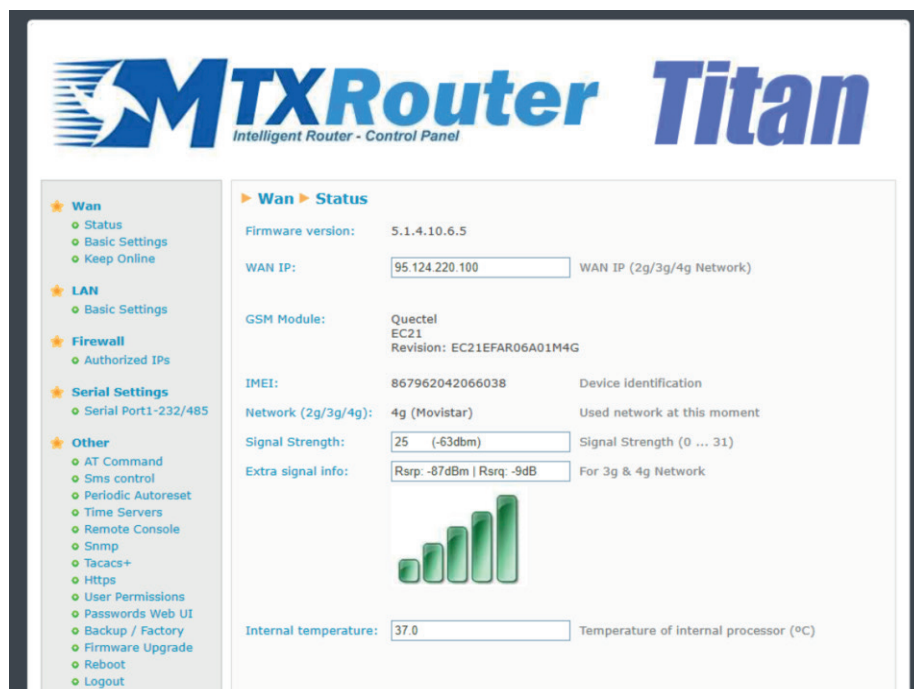
3.1 WAN

The WAN section covers all aspects related to the MTX-StarEnergy router's 2G/3G/4G configuration, including the connection status, network configuration parameters and connection monitoring.

3.1.1 WAN: Status

This screen shows the general status of the MTX-StarEnergy router.

- **Firmware Version:** Firmware version of the MTX-StarEnergy router.
- **WAN IP:** WAN IP address (IP address assigned to the connection (2G/3G/4G) if it is activated).
- **GSM Module:** indicates the manufacturer and model of the internal GSM module of the MTX-StarEnergy router.
- **IMEI:** IMEI of the MTX-StarEnergy router's internal GSM module.
- **Network (2G/3G/4G):** indicates whether the current WAN connection is using the 2G (GPRS), 3G, or 4G network. The operator is shown in brackets.
- **Signal Strength:** indicates the strength of the signal. 0=none, 31=maximum
- **Extra signal info:** shows additional information when the modem is registered on 3G and 4G networks.
- **Internal Temperature:** displays the internal temperature of the processor. (This does not indicate the ambient temperature).



3.1.2 WAN: Basic Settings

This section covers the configuration of the WAN connection (4g/3g/2g) parameters. You will need to know about your SIM card, including the APN, username and password. Your provider must give them to you.

- Enabled WAN: check the box to allow the MTX-StarEnergy router to enable the 4g/3g/2g connection.
- APN: Operator APN. Ask your GSM provider.
- Username: operator username. Ask your GSM provider.
- Password: operator password. Ask your GSM provider.
- Sim card Pin: if your SIM card has a PIN you must enter it here.
- Authentication: you must indicate the authentication method. Normally Auto.
- Network selection:
 - Auto (4G/3G/2G): the MTX-StarEnergy will use 4G if there is coverage, or 3G and 2G otherwise, in that order.
 - Auto (4G/2G): the MTX-StarEnergy will use 4G if there is coverage, or 2G otherwise, in that order.
 - 4G: the MTX-StarEnergy will use the 4G network in all cases. If there is no 4G coverage, it will not switch to 2G or 3G.
 - 3G: the MTX-StarEnergy will use the 3G network in all cases. If there is no 3G coverage, it will not switch to 2G or 4G.

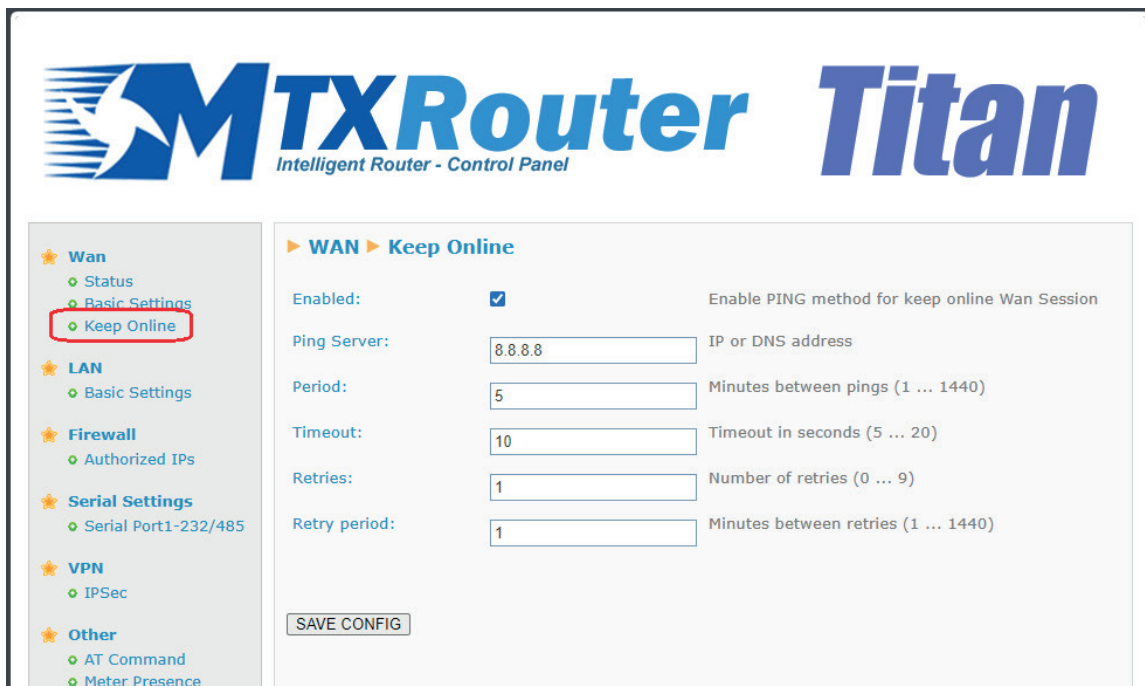
- 2G: the MTX-StarEnergy will use the 2G network in all cases.
- DNS1 and DNS2: DNS servers for domain name resolution. We recommend you use Google 8.8.8.8 and 8.8.4.4 if you are going to use static DNS servers. In the drop down menu you can also specify that it uses those assigned automatically by the phone provider.
- Remote management: if you check the box, you can access the web configuration page of the MTX-StarEnergy remotely via HTTP, through its public IP address (the one indicated in WAN>Status) and through the port specified in the next paragraph.
- Remote TCP Port: indicates the remote configuration TCP port. For example, if you specify 8080, the configuration URL will be <http://x.x.x.x:8080>.

Additional Notes

- If you want remote access via HTTPS rather than HTTP, please do not check the “Remote management” checkbox, check the checkbox you will find in the “Other” > “HTTPS” menu. With this configuration you will not have remote access via HTTP, but you will via HTTPS (a certificate generated and self-signed by the MTX-StarEnergy will be used by default for the connection. You can also use a proprietary certificate).
- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.

3.1.3 WAN: Keep Online

On this screen you can configure a PING to check the MTX-StarEnergy’s connectivity. If the PING fails X times (a configurable value) consecutively, the 4G/3G/2G session will be restarted. See the additional notes on this point for more options.



The screenshot shows the MTXRouter Titan Intelligent Router - Control Panel. The left sidebar contains a navigation menu with the following items: Wan (Status, Basic Settings, Keep Online), LAN (Basic Settings), Firewall (Authorized IPs), Serial Settings (Serial Port1-232/485), VPN (IPSec), and Other (AT Command, Meter Presence). The 'Keep Online' option under 'Wan' is highlighted with a red rectangle. The main content area is titled 'WAN > Keep Online' and contains the following configuration options:

Parameter	Value	Description
Enabled:	<input checked="" type="checkbox"/>	Enable PING method for keep online 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 configuration area is a 'SAVE CONFIG' button.

- Enabled: check the box to allow the MTX-StarEnergy to send a PING to periodically check connectivity.
- Ping Server: indicates the IP or DNS address of the server to PING.
- Period: indicates the number of minutes between each PING.
- Timeout: specifies the timeout in seconds to wait for a PING response.
- Retries: specifies the number of PING retries in case of failure.
- Retry period: indicates the number of minutes between each PING retry.

In the case of the example on the previous screen, server 8.8.8.8 is PINGed every 5 minutes, with a timeout of 10 seconds. In the event of failure, 1 additional retry is performed after 1 minute. If the number of retries is exhausted, which in this example is 1, the MTX-StarEnergy will restart the 4G/3G/2G connection.

Additional Notes:

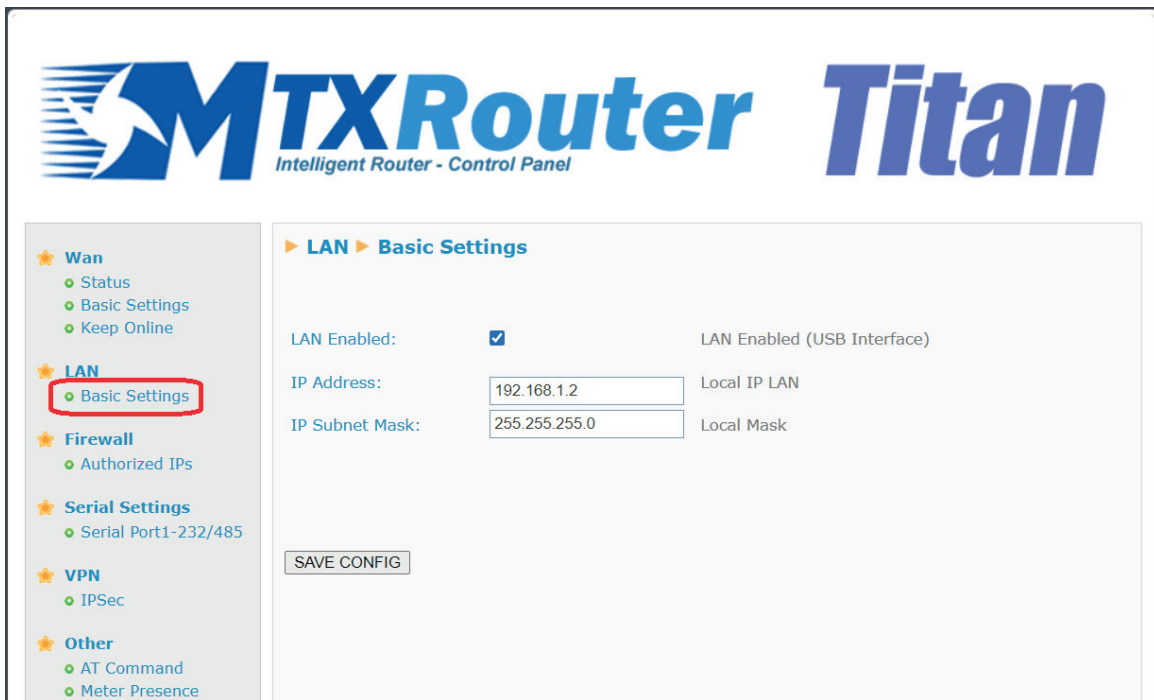
- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.
- Do not forget the “Other > Periodic Autoreset” configuration section, where you can establish an additional watchdog for this method and indicate a period after which the MTX-StarEnergy will restart fully (with power off / power on of the electronics) if it is not able to obtain an IP from the telephone operator.

3.2 LAN

The “LAN” configuration section refers to the local network settings. In the case of the MTX-StarEnergy, it refers to a LAN connection via a USB cable.

3.2.1 LAN: Basic Settings

This section lets you configure the basic network parameters of the network connection (emulated through the USB interface).



The screenshot displays the MTXRouter Titan Intelligent Router - Control Panel. The left sidebar contains a navigation menu with categories: Wan (Status, Basic Settings, Keep Online), LAN (Basic Settings, highlighted with a red box), Firewall (Authorized IPs), Serial Settings (Serial Port1-232/485), VPN (IPSec), and Other (AT Command, Meter Presence). The main content area is titled 'LAN Basic Settings' and includes the following fields: 'LAN Enabled' (checked), 'LAN Enabled (USB Interface)', 'IP Address' (192.168.1.2), 'Local IP LAN', 'IP Subnet Mask' (255.255.255.0), and 'Local Mask'. A 'SAVE CONFIG' button is located at the bottom left of the main content area.

- LAN Enabled: lets you enable/disable the LAN interface (the USB port). If you disable it, make sure you have remote access to the MTX-StarEnergy via HTTP/HTTPS, SSH, SNMP or SMS. If you do not, you will not be able to access the device’s configuration page, you will then have to follow the steps to restore the factory configuration.
- IP Address: local IP address of the emulated IP interface (by default, 192.168.1.2).
- IP Subnet Mask: subnet mask.

Additional Notes:

- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.

3.3 Firewall

In this section we can configure certain security aspects of the MTX-StarEnergy router related to remote IP connectivity.

3.3.1 Firewall: Authorized IPs

This screen lets you define, if required, up to 3 IP addresses authorized to connect to/from the WAN port (4G/3G/2G interface) for the MTX-StarEnergy services. For example, if an authorized IP address of 90.166.108.200 is specified (such as the public IP of an office), certain services will only be accessible from that IP address. It also lets you assign certain services that can only be used over the WAN via IPsec.

The screenshot shows the MTXRouter Titan Intelligent Router - Control Panel. On the left is a sidebar menu with categories: Wan (Status, Basic Settings, Keep Online), LAN (Basic Settings), Firewall (Authorized IPs, highlighted with a red box), Serial Settings (Serial Port1-232/485), VPN (IPSec), and Other (AT Command, Meter Presence, Sms control, Periodic Autoreset, Time Servers, Remote Console). The main content area is titled 'Firewall > Authorized IPs (for WAN interface)'. It contains three input fields for 'Authorized IP1:', 'Authorized IP2:', and 'Authorized IP3:', each followed by the text 'Remote connections from this IP are allowed'. Below these are six dropdown menus for 'Router configuration', 'Serial gateways', 'Remote console:', 'SNMP:', 'Outgoing connections:', and 'PING:', each followed by a description of the security setting. All dropdowns are currently set to 'ALLOW ANY IP'. At the bottom left of the main area is a 'SAVE CONFIG' button.

- Authorized IP1: authorized IP address number 1.
- Authorized IP2: authorized IP address number 2.
- Authorized IP3: authorized IP address number 3.
- Router configuration: specifies whether remote connections to the web configuration environment are accepted from any IP, only from authorized IP addresses, or only via IPSEC.
- Serial Gateways: specifies whether remote connections to 2G/3G/4G-RS232/485 gateway services can be made from any IP, only from authorized IP addresses, or only via IPSEC.
- Remote console: specifies whether to accept remote connections to the remote console service from any IP, only from authorized IP addresses, or only via IPSEC.
- SNMP: specifies whether the device's GET/SET SNMP commands can be accessed from any IP, only from authorized IP addresses, or only via IPSEC.
- PING: specifies whether PINGs are accepted from any IP address, or only PING requests made from authorized IPs should be accepted.

- **Outgoing Connections:** lets you specify whether the MTX-StarEnergy router can provide Internet access to all IP addresses or only to authorized IP addresses.

Additional Notes:

- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.
- If you use restrictions on “Outgoing connections”, remember that you also need to specify the IP address of the DNS server.
- If you need more than 3 authorized IP addresses, you can specify more than one IP address in any box, separating them by a comma “,”.

3.4 Serial Settings: Serial PortX

In this section we can configure a transparent gateway, or one with FT1.2 CSD/4G/3G/2G <> RS232/RS485 encapsulation to remotely access RS232 and RS485 serial devices, such as electricity meters.

MTXRouter Titan
Intelligent Router - Control Panel

Serial Gateway ▶ Com1 Settings

Baudrate: 9600 Baudrate of serial port
Data bits: 8 Number of data bit
Parity: none Parity
Stop bits: 1 Number of stop bits
Timeout ms: 0 msec without serial data before sending (normally: 0)

☒ **Allow incoming GSM call (CSD Data Call)**
CSD timeout: 900 Call will be closed if no traffic in X seconds (0=no timeout, 1 ... 7200)

☒ **FT1.2 Frame Encapsulation**
Enable FT1.2 frame encapsulation

Function: Serial - IP Gateway (TCP Server)

Enable Priority: ☒ Priority TCP Port Enabled
TCP Priority Port: 20010 Listening TCP Port (1 ... 65535)
Priority timeout: 900 Socket will be closed if no traffic in X seconds (0=no timeout, 1 ... 7200)

Enable secondary: ☒ Secondary TCP Port Enabled
TCP Second. Port: 20011 Listening TCP Port (1 ... 65535)
Secondary timeout: 900 Socket will be closed if no traffic in X seconds (0=no timeout, 1 ... 7200)

SAVE CONFIG

- Baudrate: specifies the speed of the serial port (115200, ..., 300).
- Data bits: specifies the number of data bits (7, 8).
- Parity: specifies the parity (none, even [even], odd [odd]).
- Stop bits: number of stop bits (1, 2).
- Timeout ms: indicates the number of milliseconds the device will wait without receiving data through the serial port before sending the data via IP. If you specify a "0" (default value), the data will be sent via IP as it arrives at the serial port. A value of 10, for example, specifies that no data is sent if a period of at least 10ms has not passed without receiving data at the serial port. This allows the data to reach its destination without the usual fragmentation problems associated with some data management protocols and platforms. It should not be used if the "FT1.2 Frame Encapsulation" option is activated.
- Allow incoming GSM calls (CSD Data Call): selecting this box indicates that CSD calls are accepted. Only valid when the MTX-StarEnergy router is configured in AUTO (4G/3G/2G), AUTO (4G/2G) or 2G mode, as long as your phone provider allows this. When a CSD data call is received, the 2G/3G/4G data connection is closed and the CSD call is accepted and answered, creating a CSD-RS232/RS485 gateway.
- CSD timeout: specifies the seconds that must elapse before closing a CSD-RS232/485 gateway if there is no traffic on it. A time of 0 indicates that there is no timeout.
- FT1.2 Frame Encapsulation: select this option if you want the MTX-StarEnergy router to activate the encapsulation option for IEC 101/102 protocols. With this mode activated, all input and output data frames at the CSD-RS232/RS485 and IP-RS232/RS485 gateways will be checked (headers, integrity, etc.) before being forwarded through the corresponding interface, otherwise it is discarded.
- Enable Priority: select this option if you want to establish an IP-RS232/485 gateway, i.e. a scenario in which the MTX-StarEnergy router is listening on a certain TCP port waiting to receive a connection to establish the gateway. This gateway will have priority over the secondary gateway. This means that, if the priority gateway is established, the secondary one cannot be established. Moreover, if the secondary one is established, the secondary one will be closed to make way for the priority one).
- TCP Priority Port: TCP listening port for the IP-RS232/RS485 primary gateway.
- Priority timeout: specifies the time, in seconds, that must elapse before closing an IP-RS232/485 priority gateway if there is no traffic on it. A time of 0 indicates that there is no timeout.
- Enable Secondary: select this option if you want to establish an IP-RS232/485 gateway, i.e. a scenario in which the MTX-StarEnergy router is listening on a certain TCP port waiting to receive a connection to establish the gateway. This gateway will be secondary to the primary gateway. This means that, if the priority gateway is established, this secondary gateway cannot be established.
- TCP Secondary Port: TCP listening port for the IP-RS232/RS485 secondary gateway.
- Secondary timeout: specifies the time, in seconds, that must elapse before a secondary IP-RS232/485 gateway closes if there is no traffic on it. A time of 0 indicates that there is no timeout.

Additional Notes:

- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.
- If a primary type connection enters when the secondary gateway is already established, the MTX-StarEnergy router will close the secondary gateway, close the IEC session with the meter automatically with the Link Address and Measurement Point used by the secondary connection and, lastly, it will give way to the primary connection. A secondary connection cannot be established while the primary connection is still in use.
- It should be noted that the serial port configuration refers to the 2 serial ports (one RS232 and one RS485) of the MTX-StarEnergy router. The gateways established, whether they are of the CSD-Serial or the IP-Serial type, will be established through both serial ports (RS232 and RS485) simultaneously. This is an important feature as you can connect an electricity meter to one or another serial port (RS232 or RS485) without having to configure the type of port to be used in the MTX-StarEnergy router, making life far easier.

3.5 VPN: IPSec

In this section we can activate a secure IPSec connection which will work as a “client” or a “server” in a highly configurable way.

The screenshot displays the MTXRouter Titan Intelligent Router - Control Panel. The left sidebar contains a navigation menu with categories: Wan (Status, Basic Settings, Keep Online), LAN (Basic Settings), Firewall (Authorized IPs), Serial Settings (Serial Port1-232/485), VPN (IPSec), and Other (AT Command, Meter Presence, Sms control, Periodic Autoreset, Time Servers, Remote Console, Snmp, Tacacs+, Https, User Permissions, Passwords Web UI, CA-Certificates, Syslog, Backup / Factory, Firmware Upgrade, Reboot, Logout). The main content area is titled 'VPN > IPSec' and shows the 'Enabled' checkbox checked, with a 'SAVE CONFIG' button. Below this, the 'Configuration Files' section shows the 'IPsec config file: 'ipsec.conf'' with a link to find examples. A text area displays the configuration file content:

```
config setup
    charondebug="ike 1, knl 1, cfg 0"
    uniqueids=no

conn server
    auto=add
    keyexchange=ikev2
    type=tunnel
    compress=no
    forceencaps=yes
    dpdaction=clear
    dpddelay=300s
    rekey=no
    eap_identity=%identity

    left=%any
    leftid=@titan
    leftcert=server-cert.pem
    leftsendcert=always
    leftsubnet=192.168.1.0/24
    leftfirewall=yes
```

At the bottom, it shows 'IPsec secrets files: 'ipsec.secrets' click for Show/Hide'.

See the AN41, AN42, AN43, AN44, AN45, AN46, and AN7 Application Notes for the Titan family of routers for more information about their configuration. Note that, at the bottom of the configuration page you will find a series of examples with the most common configurations ready to use.

<div> <div>VPN</div> <div>IPSec</div> <div>Examples</div> </div>		
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

Additional Notes:


- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.
- Remember that, in the Firewall > Authorized IPs configuration section you will find an option to specify which IP services must be used over the WAN only via IPSEC, such as IP-Serial gateways, for example.

3.5.1Other: AT Command

In this section we can send an AT command directly to the MTX-StarEnergy router and even to the internal modem. For example, we may want to check the coverage or to identify nearby telephone cells, etc.

We can also configure up to 5 special AT commands which configure the MTX-StarEnergy when booting (i.e. they are auto-executed when the device boots).

- AT Command: AT command for real-time execution (e.g. AT+COPS?). Once you click on the “SEND AT COMMAND” button, the AT command will be executed and you will see the response.
- AT1, ... AT5: AT initialization commands.



Wan

Status

Basic Settings

Keep Online

LAN

Basic Settings

Firewall

Authorized IPs

Serial Settings

Serial Port1-232/485

Other

AT Command

Sms control

Periodic Autoreset

Time Servers

Remote Console

Snmp

Tacacs+

Https

User Permissions

Passwords Web UI

Backup / Factory

Firmware Upgrade

Reboot

Logout

Other AT Command

AT Command:

AT+COPS?

Execute custom AT Command

AT+COPS?

+COPS: 0,0,"Movistar",7

OK

SEND AT COMMAND

Init commands

AT1:

Custom initialization command 1

AT2:

Custom initialization command 2

AT3:

Custom initialization command 3

AT4:

Custom initialization command 4

AT5:

Custom initialization command 5

SAVE CONFIG

Additional Notes:

- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes made. Remember that you must restart the device for the new changes to take effect.
- Point 4 of this document includes a list with the special AT commands that can be sent via this interface.

3.5.2 Other: Meter Connected

This configuration section lets you activate the presence service of an IEC electricity meter. Once activated, the MTX-StarEnergy router will periodically check that the meter is present. If it detects that it is not and SNMP TRAPS are configured, the router will send a TRAP reporting the situation.

The screenshot shows the MTXRouter Titan Intelligent Router - Control Panel. On the left is a sidebar menu with categories: Wan (Status, Basic Settings, Keep Online), LAN (Basic Settings), Firewall (Authorized IPs), Serial Settings (Serial Port1-232/485), VPN (IPSec), and Other (AT Command, Meter Presence, Sms control). The 'Meter Presence' option under 'Other' is highlighted with a red rectangle. The main content area is titled 'Other > Meter Presence' and contains the following configuration fields:

Field	Value	Description
Enabled:	<input checked="" type="checkbox"/>	Enable Meter Presence service
Period:	60	Seconds (10 ... 86400)
Retries:	1	Number of retries (0 ... 9)
Link address:	1	Meter Link Address (default 1)

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

- Enabled: checking this box activates the electricity meter presence detection service.
- Period: frequency, in seconds, to check the presence of the electricity meter.
- Retries: in the event of an error in the presence check, it will indicate how many attempts must be made to consider that there is effectively no meter present.
- Link address: Link address of the meter, needed to perform the presence check.

Additional Notes:

- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.
- Configure the OTHER > SNMP section, activating the presence TRAP, if you wish to receive TRAPS when the meter is absent/recovered.
- The presence detection service will not be active while there are gateways established with the meter for reading it, such as CSD<>RS232/RS485 or IP<>RS232/RS485 gateways, so as not to interfere with communications.
- The Link address used by the MTX-StarEnergy router will be the one specified in this configuration section, both in the first instance and whenever the parameter (Link Address) is configured again. However, the MTX-StarEnergy also listens to IP-Serial communications coming from both the primary and secondary gateways. In the event that the Link address used by the gateways is different from the one set in this section, the MTX-StarEnergy router will store the new (link) address in its internal non-volatile memory and use the new link address

instead of the one in the configuration. Obviously, this will only happen when the link address used in the gateways is correct (the meter responds correctly to them), for the purpose of avoiding incorrect configurations of the reading software causing an incorrect configuration of the presence service.

3.5.3 Other: SMS Control

This section lets you configure how the MTX-StarEnergy router can be configured using SMS messages. For example, we can change the configuration and read statuses using SMS commands, we can also specify the telephone numbers authorized to do this.

The screenshot shows the MTXRouter Titan Intelligent Router - Control Panel. The left sidebar contains a menu with categories: Wan, LAN, Firewall, Serial Settings, VPN, and Other. The 'Other' category is expanded, and 'Sms control' is highlighted with a red box. The main content area is titled 'Other > SMS control' and contains the following configuration options:

- 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)
 - 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:**
 - Alias 1:
 - Alias 2:
- AT COMMAND:**
 - AT*MTXTUNNEL=REBOOT
 - AT*MTXTUNNEL=SETPAR#

- AT enabled: check this box if you need to be able to send AT commands by SMS to the MTX-StarEnergy router, e.g. to find out the coverage remotely, to perform a reset or to change the configuration, etc.
- AT header: here you can enter the header text for SMS command messages. For example, if you type "mtx" in this box, when an AT command is sent by SMS, e.g. the AT+CSQ command to find out the general coverage level, you must send an SMS message with the following text (without the quotes) "mtx AT+CSQ".
- All phones: this box must be checked if you want all phones to be authorized to send AT commands to the MTX-StarEnergy router via SMS. Do not check this box if you want to specify a set of authorized phone numbers. It can also be activated if the phone provider lets you filter SMS messages, i.e. if phone numbers are filtered at the network level (by the phone provider) and not at the device level.

- Authorized Number X: up to 10 authorized phone numbers can be entered in these boxes, as long as the “All phones” option is not selected.
- Alias/ATCommand: Up to 10 aliases can be entered to execute SMS commands. For example, the AT command that resets the MTX-StarEnergy router is AT^MTXTUNNEL=REBOOT. If, for example, the alias “reset” is configured, you just need to send an SMS message with the text “reset” to the MTX-StarEnergy router for it to restart, instead of having to send an SMS with “mtx AT^MTXTUNNEL=REBOOT ”, which is far longer and more difficult to remember.

Aliases can also be used to send parameters. For example, imagine that you have set the MTX-StarEnergy router to “2g” mode and you want to be able to change the working mode to “auto2”, so that the MTX-StarEnergy router connects to 2g/4g depending on the networks available in the area.

To do this you can specify an alias such as “network[params]” next to the command “AT^MTXTUNNEL=SETPARAM,WAN_NETWORK,[*1]”.

If you send the MTX-StarEnergy router an SMS message with the text “network auto2”, the setting will change from “2g” to “auto2”. (NB: Do not forget to send a reset SMS to the device so that the new configuration takes effect).

- Alias Result OK: text that is sent in response when the execution of an ALIAS command is successful.
- Alias Result ERROR: text that is sent in response when the execution of an ALIAS command fails.

Additional Notes:

- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.
- Responses to SMS commands are sent to the phone number that sent the message. If you want to receive the response, make sure that the MTX-StarEnergy router has a SIM card with SMS messaging enabled.

3.5.4 Other: Periodic Auto-reset

In this section you can configure a scheduled auto-reset.

- Auto-reset not enabled: activate this option if you do not want the device to reset itself periodically.
- Auto-reset every X hours: activate this option if you want the device to reset itself every few hours. This is usually set to 24 hours in metering applications.
- Auto-reset at specific time: activate this option if you want the device to reset itself at a certain time of day.
- Auto-reset if the router can't obtain an IP within X minutes: lets you specify the number of minutes after which the device will reset itself if it cannot obtain an IP address.

MTXRouter Titan
Intelligent Router - Control Panel

- Wan
 - Status
 - Basic Settings
 - Keep Online
- LAN
 - Basic Settings
- Firewall
 - Authorized IPs
- Serial Settings
 - Serial Port1-232/485
- VPN
 - IPSec
- Other
 - AT Command
 - Meter Presence
 - Sms control
 - Periodic Autoreset**
 - Time Servers
 - Remote Console
 - Snmp
 - Tacacs+
 - Https
 - User Permissions

Other ▶ Periodic Autoreset

☐ Autoreset not enabled

☒ Autoreset every X hours

Number of hour: Every X hours device will be rebooted

☐ Autoreset at specific hour

Hour for autoreset 0 ... 23

☒ Reset if router can't obtain IP after X minutes

Time for reset 5 ... 1440 min.

Additional Notes:

- Once the configuration process is complete, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the changes to take effect.

3.5.5 Other: Time Servers (NTP)

The MTX-StarEnergy router has a supercap real-time clock that enables it to keep time even if power is lost. Said internal clock periodically needs to be synchronized with time servers using the NTP protocol, meaning the device always has the correct time.

MTXRouter Titan
Intelligent Router - Control Panel

- Wan
 - Status
 - Basic Settings
 - Keep Online
- LAN
 - Basic Settings
- Firewall
 - Authorized IPs
- Serial Settings
 - Serial Port1-232/485
- VPN
 - IPSec
- Other
 - AT Command
 - Meter Presence
 - Sms control
 - Periodic Autoreset
 - Time Servers**
 - Remote Console
 - Snmp

WAN ▶ Time Server (NTP)

Enabled: ☒ Enable NTP

NTP Server 1: IP or DNS address

NTP Server 1 port: UDP port. Default 123

NTP Server 2: IP or DNS address

NTP Server 2 port: UDP port. Default 123

Time zone: Select the timezone

Current Time: 07-04-2021 11:48:43 Current date & time of the system

- Enabled: check this box if you want to use NTP time servers.
- NTP Server 1: IP or DNS address of the NTP 1 time server.
- NTP Server 1 port: UDP port of the NTP 1 time server.
- NTP Server 2: IP or DNS address of the NTP 2 time server.
- NTP Server 2 port: UDP port of the NTP 2 time server.
- Time Zone: lets you specify the time zone.

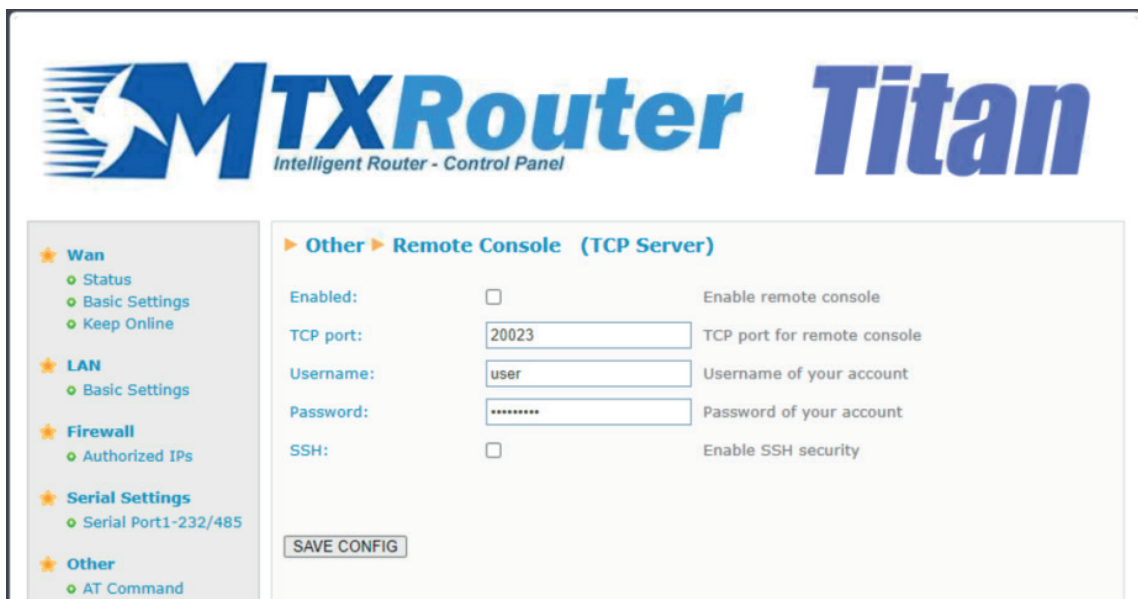
Additional Notes:

- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.

3.5.6 Other: Remote Console (TCP Server)

If at any time you need to perform a remote action with the MTX-StarEnergy router, the “Telnet or SSH type” connection can be configured in this section. By sending AT commands via a telnet or SSH connection, you can make configuration changes to the MTX-StarEnergy router or restart it, etc. In other words, the same action that can be performed using SMS, SNMP, HTTP/HTTPS messaging, but using a Telnet connection or secure SSH connection.

- Enabled: check this box if you want to use this special connection.
- TCP Port: listening TCP port where the connection must be made.
- Login: username (will be requested after establishing the connection).
- Password: user password (will be requested after entering the username).
- SSH: check the box if you want to use SSH instead of Telnet.



The screenshot shows the MTXRouter Titan Intelligent Router - Control Panel. The main heading is "MTXRouter Titan" with the subtitle "Intelligent Router - Control Panel". On the left, there is a sidebar menu with the following items: Wan (Status, Basic Settings, Keep Online), LAN (Basic Settings), Firewall (Authorized IPs), Serial Settings (Serial Port1-232/485), and Other (AT Command). The main content area is titled "Other > Remote Console (TCP Server)". It contains the following configuration options:

- Enabled: ☐ Enable remote console
- TCP port: TCP port for remote console
- Username: Username of your account
- Password: Password of your account
- SSH: ☐ Enable SSH security

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

Additional Notes:

- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect. If you check/uncheck the SSH box, you will also need to re-enter the password.

3.5.7 Other: SNMP

The MTX-StarEnergy device lets you execute SET and GET operations using the SNMP protocol from standard SNMP applications, TRAPS alarms can also be sent.

The screenshot displays the 'MTXRouter Titan' control panel. On the left, a sidebar lists navigation options: Wan, LAN, Firewall, Serial Settings, VPN, Other, and Snmp (highlighted with a red box). The 'Other' section includes AT Command, Meter Presence, Sms control, Periodic Autoreset, Time Servers, Remote Console, Snmp, and Tacacs+. The main content area is titled 'Other > SNMP' and contains the following configuration fields:

- Enabled:** A checked checkbox labeled 'Enable SNMP v2c'.
- SNMP Version:** A dropdown menu set to 'SNMPv3'.
- UDP Port:** A text box containing '161'.
- Custom OID:** A text box containing '.45711.1.1'.
- Community:** A text box containing 'public'.
- Username:** A text box containing 'myuser'.
- Auth Password:** A masked text box.
- Priv. Password:** A masked text box.
- Auth Protocol:** A dropdown menu set to 'SHA'.
- Priv Protocol:** A dropdown menu set to 'AES-128'.
- Engine ID:** A text box containing 'AUTO'.
- Traps Enabled:** A checked checkbox labeled 'Enable Traps'.

- Enabled: must be activated if you want to enable the MTX-StarEnergy router’s SNMP service.
- SNMP Version: either SNMPv2c or SNMP v3 can be connected.
- UDP port: the standard UDP port for SNMP is 161, but you can also specify a UDP of your choice.
- Custom OID: lets you change the default value for the Enterprise-Product OID (.45711.1.1) if you need to adjust it to match your corporate values.
- Community: password to execute SET and GET commands. Only required for SNMPv2.
- Username: username when using SNMPv3 (not required for SNMPv2).
- Auth Password: authentication password for SNMPv3 (not required for SNMPv2).
- Priv Password: privacy password for SNMPv3 (not necessary for SNMPv2).
- Auth Protocol: authentication protocol (MD5 or SHA).
- Priv Protocol: encryption protocol (DES, AES128).

- EngineID: lets you specify the EngineID for SNMPv3. Use the value "AUTO" if you want the MTX-StarEnergy router to use its own unique EngineID, or specify the EngineID in HEX format (e.g. 010203040506AABBCCDDEEFF).

The screenshot shows the MTX-StarEnergy router configuration interface. On the left, a sidebar lists various configuration options, with 'Snmp' highlighted. The main area displays the SNMP configuration settings. At the top, 'Priv Protocol' is set to 'AES-128' and 'Engine ID' is set to 'AUTO'. Below this, 'Traps Enabled' is checked. The 'Traps' section includes 'Traps - UDP Port' (162), 'Traps - IP' (77.231.220.143), and 'Traps - Community' (public). The 'Alarm' section includes 'Alarm Presence' (checked), 'Alarm Power' (checked), and 'Alarm OS' (checked). The 'Number traps alarm ON' is set to 10, 'Number traps alarm OFF' is set to 5, and 'Trap period' is set to 30. A 'SAVE CONFIG' button is located at the bottom left of the configuration area.

- Traps Enabled: enable the TRAPS alarm service in the MTX-StarEnergy router.
- Traps – UDP Port: lets you specify the port for SNMP TRAPS.
- Traps – IP: IP address for sending SNMP TRAPS.
- Community: community field for sending TRAPS v2c.
- Alarm Presence: activates/deactivates the presence TRAP. If the meter's "Presence" service is activated, a change in the presence detection state of the meter will cause notification TRAPS to be sent.
- Alarm Power: activates/deactivates the external power TRAP. An alarm TRAP is sent when the MTX-StarEnergy router detects a loss of power, and when the power supply is restored. The MTX-StarEnergy router has a supercap that enables the power supply failure detection and alarm system to operate for approximately 1 minute without external power.
- Alarm OS: activates/deactivates the operating system alarm TRAP. An alarm TRAP is sent when the MTX-StarEnergy router detects an internal anomaly, such as a lack of flash memory or SD memory.
- Number TRAPS alarm ON: indicates the number of TRAPS that will be sent when an alarm is activated. For example, if 10 is specified, the MTX-StarEnergy router will send 10 ON alarm TRAPS every X seconds (configurable).
- Number TRAPS alarm OFF: indicates the number of TRAPS that will be sent when an alarm is deactivated. For example, if 5 is specified, the MTX-StarEnergy router will send 5 OFF alarm TRAPS every X seconds (configurable).
- Trap period: Number of seconds between TRAPS of the same type being sent.

Additional Notes:

- Once the configuration process is complete, click on the “SAVE CONFIG” button to save the changes. Remember that the MTX-StarEnergy router must be restarted for the new changes to take effect.
- The previous screen has a link marked “Click here to download MIB”. This will download the MIB with the OIDs.
- If you want the MTX-StarEnergy router to only send TRAPS when an alarm is activated (and not when one is deactivated), simply enter “0” in the “Number TRAPS alarm OFF” field.
- The alarm status is saved in non-volatile memory. This implies that if, for example, a Power alarm is activated (due to a loss of external power), the number of TRAPS configured in the “Number TRAPS alarm ON” field are sent and the MTX-StarEnergy router loses all power and turns off, when it regains power and turns on, the number of TRAPS configured in “Number TRAPS alarm OFF” will be sent, this is because when it restarts, it recovers the prior alarm configuration.

Other: SNMP Details

Below is an illustration of how the MTX-StarEnergy router’s various SNMP OIDs are organized, together with descriptions of all the OIDs and TRAPS.

The screenshot shows the ManageEngine MibBrowser Free Tool interface. On the left, a tree view displays the hierarchy of loaded MIB modules: IANAType-MIB, RFC1213-MIB, TITAN-MIB, enterprises, mibm2m, routers, titan, mobile, and miscellaneous. The 'mobile' folder is expanded, showing various mobile-related OIDs. The 'miscellaneous' folder is also expanded, showing the 'mobileLink' OID. On the right, the details for the 'mobileLink.0' OID are displayed. The Host is 88.28.221.24, Port is 161, and the Community is *****. The Set Value is AT*MTXTUNNEL=OTAPCONFIGSFTP,77.231.220.143:20022,sftpuse. The Device Type is Not Available. The Suggested OIDs are None. The Object ID is .iso.org.dod.internet.private.enterprises.mibm2m.routers.titan.miscellaneous.meterLink.0. The details section shows the following information:

OID	Description
mobileLink.0	867962046823806
mobile_frequencyBand.0	LTE BAND 3
mobile_imsi.0	214075536243578
mobile_homePlmn.0	21407
mobile_ratType.0	FDD LTE
meterLink.0	1

The “mobile” section covers all OIDs related to the communications module and its registration on the network.

mobile_imei	.1.3.6.1.4.1.45711.1.1.1.1.0
	communication module IMEI
mobile_frequencyBand	.1.3.6.1.4.1.45711.1.1.1.2.0
	current working frequency band
mobile_imsi	.1.3.6.1.4.1.45711.1.1.1.3.0
	IMSI of the SIM card
mobile_homePlmn	.1.3.6.1.4.1.45711.1.1.1.4.0
	current PLMN
mobile_homeOperator	.1.3.6.1.4.1.45711.1.1.1.5.0
	SIM card home operator
mobile_subscription_address	.1.3.6.1.4.1.45711.1.1.1.6.0
	apn – ipv4 – assigned IP address
mobile_ratType	.1.3.6.1.4.1.45711.1.1.1.7.0
	Type of technology
mobile_registeredMcc	.1.3.6.1.4.1.45711.1.1.1.8.0
	Current MCC
mobile_registeredMnc	.1.3.6.1.4.1.45711.1.1.1.9.0
	Current MNC
mobile_registeredPlmn	.1.3.6.1.4.1.45711.1.1.1.10.0
	current PLMN
mobile_registeredLac	.1.3.6.1.4.1.45711.1.1.1.11.0

	Current LAC
mobile_registeredOperator	.1.3.6.1.4.1.45711.1.1.1.12.0
	Current operator
mobile_uli_cellId	.1.3.6.1.4.1.45711.1.1.1.13.0
	Current CellID
mobile_uli_cgi	.1.3.6.1.4.1.45711.1.1.1.14.0
	Current Cell Global Identity
mobile_uli_signal_strength	.1.3.6.1.4.1.45711.1.1.1.15.0
	Signal Strength in dBm
mobile_uli_signal_quality	.1.3.6.1.4.1.45711.1.1.1.16.0
	signal quality in dB
mobile_3G_RSCP	.1.3.6.1.4.1.45711.1.1.1.17.0
	RSCP, valid when registered to 3G
mobile_4G_RSRP	.1.3.6.1.4.1.45711.1.1.1.18.0
	RSRP, valid when registered to 4G
mobile_icc	.1.3.6.1.4.1.45711.1.1.1.19.0
	ICC of the SIM card

The “miscellaneous” section covers all the OIDs related to the device’s status.

identifier	.1.3.6.1.4.1.45711.1.1.2.1.0
	unique manufacturer device identifier
specificType	.1.3.6.1.4.1.45711.1.1.2.2.0

	device type (router)
birthDate	.1.3.6.1.4.1.45711.1.1.2.3.0
	first date/time read by NTP
serialNumber	.1.3.6.1.4.1.45711.1.1.2.4.0
	device serial number
model	.1.3.6.1.4.1.45711.1.1.2.5.0
	Router model
Software	.1.3.6.1.4.1.45711.1.1.2.6.0
	FW version of the router
operationalStatus	.1.3.6.1.4.1.45711.1.1.2.7.0
	Router status report (autocheck)
upTime	.1.3.6.1.4.1.45711.1.1.2.8.0
	Date/time of last start (UTC+0)
clock	.1.3.6.1.4.1.45711.1.1.2.9.0
	Router time (UTC+0)
meterLink	.1.3.6.1.4.1.45711.1.1.2.10.0
	Energy meter's current link address
meterPoint	.1.3.6.1.4.1.45711.1.1.2.11.0
	Current reading point of the energy meter
meterSource	.1.3.6.1.4.1.45711.1.1.2.12.0
	Default, auto, manual
pendingConfig	.1.3.6.1.4.1.45711.1.1.2.13.0

	<p>0= no configurations pending application.</p> <p>1= if there are configurations pending application. The MTX-StarEnergy must be reset to apply the new config.</p>
executingOTAP	.1.3.6.1.4.1.45711.1.1.2.14.0
	<p>0= no OTAP is running</p> <p>1= an OTAP is running</p>
executingAT	.1.3.6.1.4.1.45711.1.1.2.15.0
	<p>0= no AT commands are running</p> <p>1= an AT command is running</p>

The “actions” section covers the OIDs for actions that can be carried out via SNMP.

mtxReset	.1.3.6.1.4.1.45711.1.1.3.1.0
	Lets you reset the router by entering '1'
mtxATCommand	.1.3.6.1.4.1.45711.1.1.3.2.0
	Lets you execute an AT command on the router

The mtxATCommand OID is special. It allows AT commands to be executed remotely on the MTX-StarEnergy router via SNMP. The correct process to execute an AT command via SNMP is as follows:

- Enter the AT command to be executed in the “mtxATCommand” OID.
- Read the “executingAT” OID. If it returns value “1” the command is being executed. When it has finished executing, it will return “0”.
- Read the “mtxATCommand” OID and this will return the response to the AT command executed.

This OID is useful for remotely executing FW update AT commands, to load remote configurations, and to perform other actions on the router. See chapter 4 for the most relevant AT commands.

The “config_” sections cover OIDs and the various basic configurations that can be applied to the MTX-StarEnergy router.

WAN_APN	.1.3.6.1.4.1.45711.1.1.4.1.0
	Network connection APN
WAN_NETWORK	.1.3.6.1.4.1.45711.1.1.4.2.0
	Lets you indicate the network to be used Possible values: auto > 4g/3g/2g, auto2 >4g/2g, 2g, 3g, 4g
WAN_AUTHENTICATION	.1.3.6.1.4.1.45711.1.1.4.3.0
	Possible values: auto, pap, chap
WAN_USERNAME	.1.3.6.1.4.1.45711.1.1.4.4.0
	Username for the network connection
WAN_PASSWORD	.1.3.6.1.4.1.45711.1.1.4.5.0
	Password for the network connection

KEEP_ENABLED	.1.3.6.1.4.1.45711.1.1.5.1.0
	Possible values: 0: keepalive disabled, 1: keepalive enabled
KEEP_IP	.1.3.6.1.4.1.45711.1.1.5.2.0
	IP or DNS for the keep alive PING
KEEP_PERIOD	.1.3.6.1.4.1.45711.1.1.5.3.0
	Minutes between pings (1...1440)
KEEP_TIMEOUT	.1.3.6.1.4.1.45711.1.1.5.4.0
	PING retries after a failure (0 ... 9)
KEEP_RETRY	.1.3.6.1.4.1.45711.1.1.5.5.0

	Seconds to timeout (5 ... 20)
KEEP_RETRY_PERIOD	.1.3.6.1.4.1.45711.1.1.5.6.0
	Minutes between retries (1...1440)

AUTORESET_MODE	.1.3.6.1.4.1.45711.1.1.6.1.0
	“none”: no autoreset, “time”: autoreset at a specific time, “timer”: Auto reset every X hours
AUTORESET_TIMER	.1.3.6.1.4.1.45711.1.1.6.2.0
	When in “timer” mode, the number of hours between autoresets (1 ... 24)
AUTORESET_HOUR	.1.3.6.1.4.1.45711.1.1.6.3.0
	When in “time” mode, the time at which the autoreset is carried out (0 ... 23)
AUTORESET_IP_ENABLED	.1.3.6.1.4.1.45711.1.1.6.4.0
	0: autoreset as could not get disabled IP, 1: autoreset as could not get enabled IP
AUTORESET_IP_TIMER	.1.3.6.1.4.1.45711.1.1.6.5.0
	Minutes for autoreset if cannot get IP (5 ... 1440)

SERIAL_BAUDRATE	.1.3.6.1.4.1.45711.1.1.7.1.0
	Serial port speed: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
SERIAL_DATABITS	.1.3.6.1.4.1.45711.1.1.7.2.0
	Number of bits: 7, 8
SERIAL_PARITY	.1.3.6.1.4.1.45711.1.1.7.3.0

	0=none, 1=odd, 2=even
SERIAL_STOPBITS	.1.3.6.1.4.1.45711.1.1.7.4.0
	Stop bits: 1, 2
SERIAL_PORT1_ENABLED	.1.3.6.1.4.1.45711.1.1.7.5.0
	Main port enabled (1) or disabled (0)
SERIAL_PORT1_TCPPORT	.1.3.6.1.4.1.45711.1.1.7.6.0
	Primary TCP Port: 1 ... 65535
SERIAL_PORT1_TIMEOUT	.1.3.6.1.4.1.45711.1.1.7.7.0
	Number of seconds for timeout for the main port. 0=no timeout. 1 ... 7200
SERIAL_PORT2_ENABLED	.1.3.6.1.4.1.45711.1.1.7.8.0
	Secondary port enabled (1) or disabled (0)
SERIAL_PORT2_TCPPORT	.1.3.6.1.4.1.45711.1.1.7.9.0
	Secondary TCP Port: 1 ... 65535
SERIAL_PORT2_TIMEOUT	.1.3.6.1.4.1.45711.1.1.7.10.0
	Number of seconds for timeout for the secondary port. 0=no timeout. 1 ... 7200
SERIAL_IEC	.1.3.6.1.4.1.45711.1.1.7.11.0
	Encapsulation enabled (1) or disabled (0)
SERIAL_MSTOSEND	.1.3.6.1.4.1.45711.1.1.7.12.0
	Waiting time before serial retransmission in milliseconds
SERIAL_CSD_ENABLED	.1.3.6.1.4.1.45711.1.1.7.13.0
	CSD calls enabled (1) or disabled (0)

SERIAL_CSD_TIMEOUT	.1.3.6.1.4.1.45711.1.1.7.14.0
	Number of seconds for timeout for CSD communications. 0=no timeout. 1 ... 7200
SMS_ENABLED	.1.3.6.1.4.1.45711.1.1.8.1.0
	SMS commands enabled (1) or disabled (0)
SMS_HEADER	.1.3.6.1.4.1.45711.1.1.8.2.0
	Header for SMS commands
SMS_ALLPHONES	.1.3.6.1.4.1.45711.1.1.8.3.0
	1: all phones are authorized. 0: only configured phones are authorized
SMS_PHONE1	.1.3.6.1.4.1.45711.1.1.8.4.0
	Authorized phone number 1
SMS_PHONE2	.1.3.6.1.4.1.45711.1.1.8.5.0
	Authorized phone number 2
SMS_PHONE3	.1.3.6.1.4.1.45711.1.1.8.6.0
	Authorized phone number 3
SMS_PHONE4	.1.3.6.1.4.1.45711.1.1.8.7.0
	Authorized phone number 4
SMS_PHONE5	.1.3.6.1.4.1.45711.1.1.8.8.0
	Authorized phone number 5
SMS_PHONE6	.1.3.6.1.4.1.45711.1.1.8.9.0
	Authorized phone number 6

SMS_PHONE7	.1.3.6.1.4.1.45711.1.1.8.10.0
	Authorized phone number 7
SMS_PHONE8	.1.3.6.1.4.1.45711.1.1.8.11.0
	Authorized phone number 8
SMS_PHONE9	.1.3.6.1.4.1.45711.1.1.8.12.0
	Authorized phone number 9
SMS_PHONE10	.1.3.6.1.4.1.45711.1.1.8.13.0
	Authorized phone number 10

NTP_ENABLED	.1.3.6.1.4.1.45711.1.1.9.1.0
	NTP service enabled (1) or disabled (0)
NTP_SERVER1	.1.3.6.1.4.1.45711.1.1.9.2.0
	IP or DNS of the NTP1 Server
NTP_SERVER2	.1.3.6.1.4.1.45711.1.1.9.3.0
	IP or DNS of the NTP2 Server
NTP_TIMEZONE	.1.3.6.1.4.1.45711.1.1.9.4.0
	Time zone: “UTC”, “Europe/Madrid”
NTP_PORT1	.1.3.6.1.4.1.45711.1.1.9.5.0
	NTP1 Server Port
NTP_PORT2	.1.3.6.1.4.1.45711.1.1.9.6.0
	NTP2 Server Port

SNMP_TRAPS_ENABLED	.1.3.6.1.4.1.45711.1.1.10.1.0
	SNMP TRAP service enabled (1) or disabled (0)
SNMP_TRAPS_SERVER	.1.3.6.1.4.1.45711.1.1.10.2.0
	SNMP TRAP server IP
SNMP_TRAPS_PRESENCE	.1.3.6.1.4.1.45711.1.1.10.3.0
	Meter's PRESENCE TRAP enabled (1) or disabled (0)
SNMP_TRAPS_POWER	.1.3.6.1.4.1.45711.1.1.10.5.0
	EXTERNAL POWER SUPPLY failure TRAP enabled (1) or disabled (0)
SNMP_TRAPS_OS	.1.3.6.1.4.1.45711.1.1.10.6.0
	Internal operating system alarm TRAP enabled (1) or disabled (0)
SNMP_TRAPS_PERIOD	.1.3.6.1.4.1.45711.1.1.10.8.0
	Time, in seconds, between TRAPS of the same type being sent. Possible values 10 ... 3600.
SNMP_TRAPS_NUMBERON	.1.3.6.1.4.1.45711.1.1.10.9.0
	Number of TRAPS to send when the alarm is activated. Possible values 0 ... 1440.
SNMP_TRAPS_OFF	.1.3.6.1.4.1.45711.1.1.10.10.0
	Number of TRAPS to send when the alarm is deactivated. Possible values 0 ... 1440.
SFTP_FW_SERVER	.1.3.6.1.4.1.45711.1.1.11.1.0
	SFTP server for remote FW updates

SFTP_FW_FILE	.1.3.6.1.4.1.45711.1.1.11.2.0
	Path and File for remote FW updates
SFTP_FW_USERNAME	.1.3.6.1.4.1.45711.1.1.11.3.0
	SFTP Server username for remote FW updates
SFTP_FW_PASSWORD	.1.3.6.1.4.1.45711.1.1.11.4.0
	SFTP Server password for remote FW updates
SFTP_CONFIG_SERVER	.1.3.6.1.4.1.45711.1.1.11.5.0
	SFTP server for remote updating of the full configuration
SFTP_CONFIG_FILE	.1.3.6.1.4.1.45711.1.1.11.6.0
	Path and File for remote updating of the full configuration
SFTP_CONFIG_USERNAME	.1.3.6.1.4.1.45711.1.1.11.7.0
	SFTP Server username for remote updating of the full configuration
SFTP_CONFIG_PASSWORD	.1.3.6.1.4.1.45711.1.1.11.8.0
	SFTP Server password for remote updating of the full configuration
LAN_BASIC_ENABLED	.1.3.6.1.4.1.45711.1.1.12.1.0
	LAN interface (USB) enabled (1) or disabled (0)
METER_PRES_ENABLED	.1.3.6.1.4.1.45711.1.1.13.1.0
	Meter presence detection service enabled (1) or disabled (0)

METER_PRES_PERIOD	.1.3.6.1.4.1.45711.1.1.13.2.0
	Seconds. Presence detection interval (10 ... 86400)
METER_PRES_RETRYNUM	.1.3.6.1.4.1.45711.1.1.13.3.0
	Number of retries if presence detection fails (0 ... 9)
METER_PRESS_LINK	.1.3.6.1.4.1.45711.1.1.13.4.0
	Link Address of the meter

PLATFORM_ENABLED	.1.3.6.1.4.1.45711.1.1.14.1.0
	OTAP status send to platform service enabled (1) or disabled (0)
PLATFORM_SERVER	.1.3.6.1.4.1.45711.1.1.14.2.0
	DNS or IP of the platform
PLATFORM_PORT	.1.3.6.1.4.1.45711.1.1.14.3.0
	TCP Port of the platform

The “alarms” section covers OIDs relating to the statuses of the MTX-StarEnergy router’s alarms, indicating “0” if an alarm is not activated and with “1” if an alarm is activated.

Presence	.1.3.6.1.4.1.45711.1.1.19.1.0
	0 = meter presence alarm not activated 1 = meter presence alarm activated
Power	.1.3.6.1.4.1.45711.1.1.19.3.0
	0 = power failure alarm not activated 1 = power failure alarm activated
OS	.1.3.6.1.4.1.45711.1.1.19.4.0

0 = operating system alarm not activated
 1 = operating system alarm activated Low flash memory
 2 = operating system alarm activated Low SD flash memory (system logs)

Information about SNMP TRAPS

presenceTrap	.1.3.6.1.4.1.45711.1.1.20.1.0
	Meter presence alarm TRAP. Severity "2" when alarm activated. Severity "6" when alarm deactivated.
powerTrap	.1.3.6.1.4.1.45711.1.1.20.3.0
	Loss of power supply alarm TRAP. Severity "3" when alarm activated. Severity "6" when alarm deactivated.
osTrap	.1.3.6.1.4.1.45711.1.1.20.4.0
	Operating system alarm TRAP. Severity "5" when alarm activated. Severity "6" when alarm deactivated.
severity	.1.3.6.1.4.1.45711.1.1.20.100.0
	Severity of the TRAP. 1=All, 2=Critical, 3=Major, 4=Minor, 5=Warning, 6=Clear, 7=Info

As well as the alarm status, the TRAPS will include the OID corresponding to the serial number of the device serialNumber (.1.3.6.1.4.1.45711.1.1.2.4.0).

In the case of presence TRAPS, the OIDs corresponding to meterLink (.1.3.6.1.4.1.45711.1.1.2.10.0) and meterSource (.1.3.6.1.4.1.45711.1.1.2.12.0) are also included in the TRAP.

As we mentioned at the beginning of this chapter, we can configure a number of TRAPS X to be sent when an alarm is activated, a number of TRAPS Y to be sent when an alarm has been deactivated, and the time period between sends. For example, if 10 alarm TRAPS are defined for activation and 5 alarm TRAPS for deactivation and they are sent every 30 seconds, if a presence is followed by an alarm deactivation, the result will be as follows:


As an example, the PRESENCE ALARM deactivation TRAP would provide the following data. A "0" indicating that the presence alarm is deactivated. Severity 6 (CLEAR), the presence detection operating mode (in this example auto), the link address (in this example 1715) and the serial number of the MTX-StarEnergy router (in this example 0123456789ABCD).

Trap Details	
TimeStamp	0 hours, 13 minutes, 18 seconds.
Enterprise	
Generic Type	
Specific Type	
Message	<pre>.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 0 hours, 13 minutes, 18 seconds.: .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapOID.0: Object ID: .1.3.6.1.4.1.45711.1.1.20.1.0: .iso.org.dod.internet.snmpV2.snmpModules.10.1.3.0: IpAddress: 77.231.195.167: .iso.org.dod.internet.private.enterprises.mt.xm2m.routers.titan.traps.presenceTrap.0: 0: .iso.org.dod.internet.private.enterprises.mt.xm2m.routers.titan.traps.severity.0: 6: .iso.org.dod.internet.private.enterprises.mt.xm2m.routers.titan.miscellaneous.meterSource.0: manual: .iso.org.dod.internet.private.enterprises.mt.xm2m.routers.titan.miscellaneous.meterLink.0: 1715: .iso.org.dod.internet.private.enterprises.mt.xm2m.routers.titan.miscellaneous.serialNumber.0: 0123456789ABCDEF0:</pre>
Severity	6
Entity	din-167-195-231-77.ipcom.comunitel.net
RemotePort	47888
LocalPort	162
Community	null
Node	88.28.221.24
Source	88.28.221.24
TimeReceived	Wed Apr 21 13:56:11 CEST 2021
HelpURL	

3.5.8 Other: TACACS+

An external Tacacs+ server must be used to authenticate the device's HTTP/HTTPS and Telnet/SSH services, it can be configured in this section.

- **Server:** IP or DNS address of the Tacacs+ server.
- **Port:** listening port of the Tacacs+ server (by default 49).
- **KEY:** encryption password.
- **Service http:** check the box if you want Web access to the device to use the Tacacs+ authentication service.
- **Service https:** check the box if you want to be able to access the device via the Web to use the Tacacs+ authentication service.



MTXRouter

Intelligent Router - Control Panel

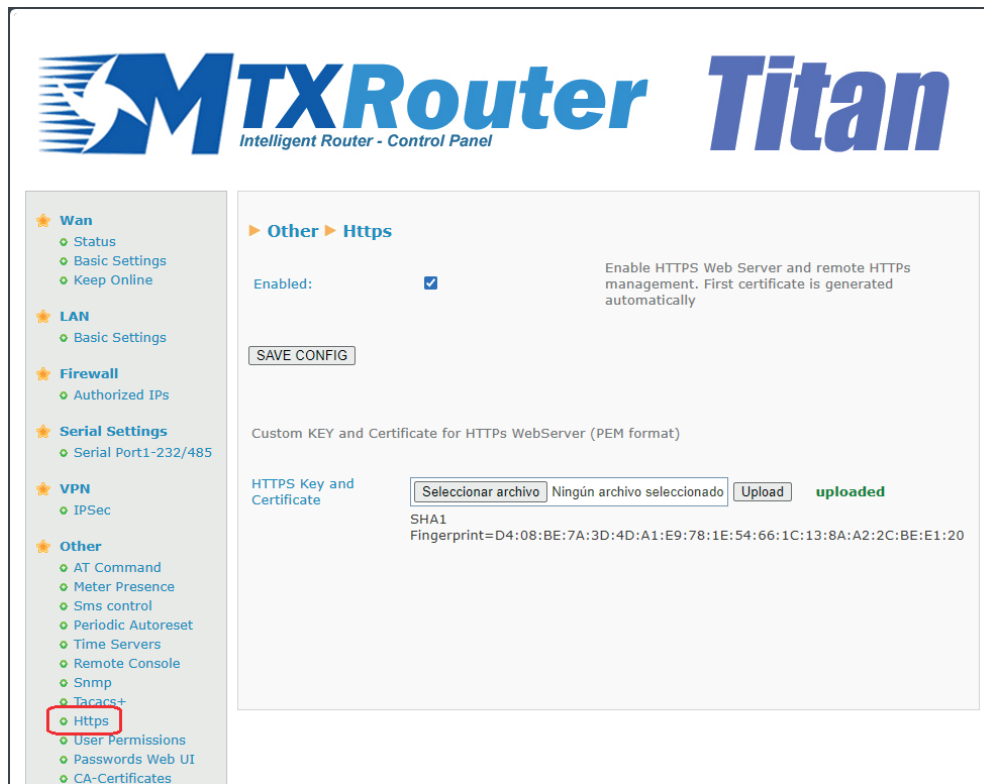
Titan

Additional Notes:

- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.
- Keep in mind that the MTX-StarEnergy router lets you use the username and password locally assigned to the "admin" user, meaning that, if the router is not connected to the Internet (change of operator, etc.), you can still access the device. You must therefore keep the “admin” user’s local password safe.

3.5.9 Other: HTTPS

In this section you can activate HTTPS for the configuration environment, if necessary. Activating this section enables the device's WEB server to be accessed via a secure HTTPS connection.



- Enabled: enables the HTTPS service (self-signed certificates are generated automatically after rebooting).

Additional Notes:

- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.
- When trying to connect to the MTX-StarEnergy router via HTTPS, the browser will probably show a warning message about the self-signed digital certificate. This is normal.
- A KEY and a Certificate in PEM format can also be installed for the browser. Format:

-----BEGIN PRIVATE KEY-----

MIICeAIBADANBgkqhkiG9w0BAQEFAASCAmIwggJeAgEAAoGBALT2iyN3y9T5H6hL
GiHfMxbEKZGqzZI4BRLsjcxupUBVU3laAQ2WYiZmn36aY4cLp7kR+h6b9hWPd9dg
5qpgPfnuwttgbQzFLmlypbyGhPAHc2axqYxmyhq8GwAGm2FhW+1ak8jbJAF2Ug8i
kiJmmLF8FUzNdcwmMxnIQVb6kEKIAGMBAAECgYEAmeBx8iZhXU84nlyJoQPsnPRX
ORH2p29+PVy/NMfGyyi+8XOTPT5QV+Sxvk/g+wclV0JTwRsQ4TTy7Ee/6orMuKZy
QdH1EO4znPkXT1erTaQCRp9qbXs+urxZ+L8d/ah//sDrHRTxJocCwjyxp10LvC
i7cFnyvl8pMTiOMogGUCQQDt+nj26yk3z6facW9WUMikhpZT3Zc+LyDehg5NoHMw
dKZPIS4U0AvCpgzb22A8L7NkGDSni4ZR0H/KH4rK39f/AkEAWqrAtOcMBuqbFZm2
Yp31G6PEAQdlssBSqeF9ZFHarM2Y0TOR3XGhk1LOVqrgALTeMxZi24uFeN4G6IdM
hjmFWwJBAlQJttf5PhNTSeRvj8CqbcirS/kYN3QvHeOZKZJ0dbTq4+O/96Ngk0Xa
b8QEge6i4LummoBjb5EWphB1U8KgU+OCQG/Oeg3QT1du97AtjfobdAroXWJmCQZc
m23+M/pNJSF6wKeYLAyaLS3acJGjhl6BpsTk3Af9rs57iqeSol0Vab8CQQCru+V0
zw3y0DT2AWxBYwuoD9t9cX2REUhYeExYHGVW2d9tiuuokM6d2Nxj4JPGK+QzWyE+
D+JIZPWsfGP2n9aR

-----END PRIVATE KEY-----

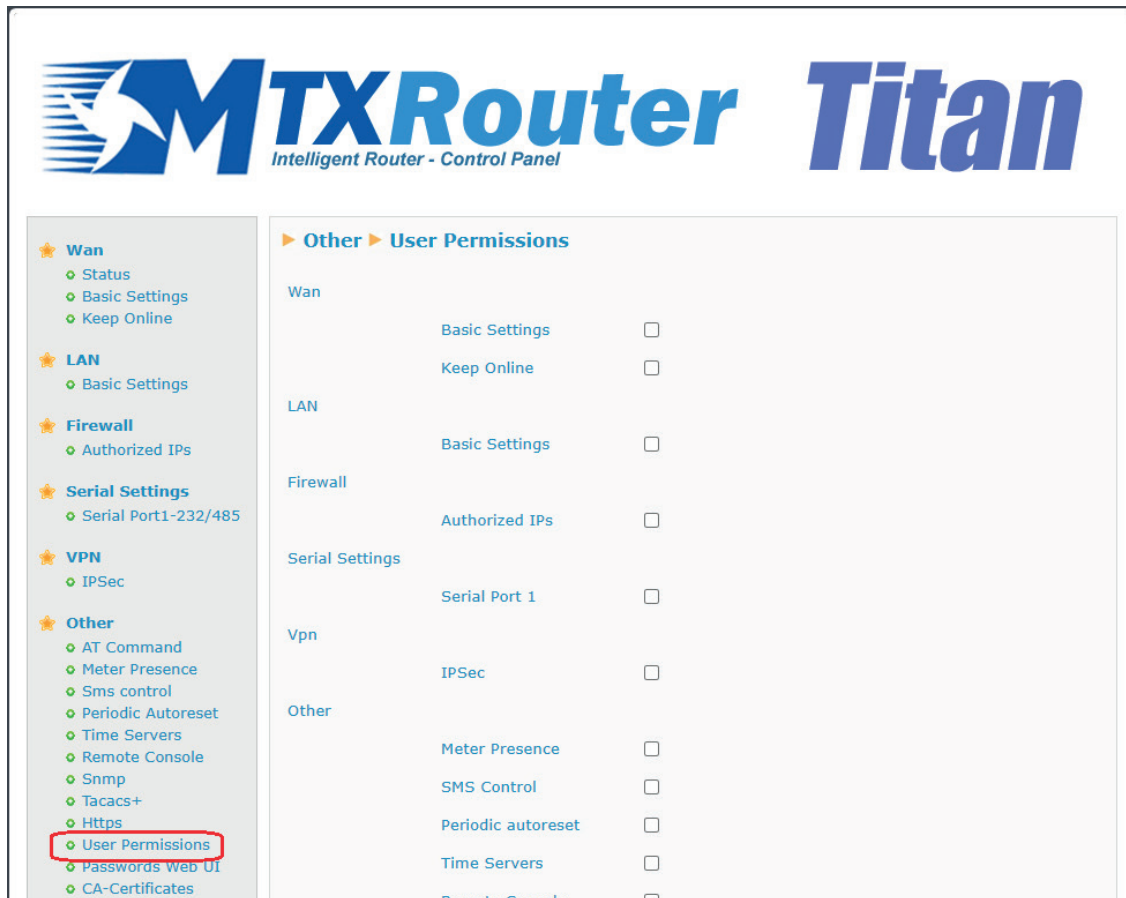
-----BEGIN CERTIFICATE-----

MIICljCCAf+gAwIBAgIJAN8keshbUKbKMA0GCSqGSIb3DQEBBQUAMGMxCzAJBgNV
BAYTAKVTMRIwEAYDVQQIDAICQVJDRUxPTkExEjAQBgNVBAcMCUJBUNFTE9OQTEP
MA0GA1UECgwGTVRYTTJNMQswCQYDVQQLDAJJVDEOMAwGA1UEAwwFVEIUQU4wIBcN
MjEwNDA2MTYwNTMwWWhGPMjEwMDA4MzAxNjA1MzBaMGMxCzAJBgNVBAYTAKVTMRIw
EAYDVQQIDAICQVJDRUxPTkExEjAQBgNVBAcMCUJBUNFTE9OQTEPMA0GA1UECgwG
TVRYTTJNMQswCQYDVQQLDAJJVDEOMAwGA1UEAwwFVEIUQU4wZ8wDQYJKoZIhvcN
AQEBBQADgYOAMIGJAoGBALT2iyN3y9T5H6hLGiHfMxbEKZGqzZI4BRLsjcxupUBV
U3laAQ2WYiZmn36aY4cLp7kR+h6b9hWPd9dg5qpgPfnuwttgbQzFLmlypbyGhPAH
c2axqYxmyhq8GwAGm2FhW+1ak8jbJAF2Ug8ikiJmmLF8FUzNdcwmMxnIQVb6kEKI
AGMBAAgJUDBOMB0GA1UdDgQWBBSlbdpvHfRJoxxchfPFEocykbVoNjAfBgNVHSME
GDAWgBSlbdpvHfRJoxxchfPFEocykbVoNjAMBgNVHRMEBTADAQH/MA0GCSqGSIb3
DQEBBQUAA4GBAH7z2zoB56rd67p8ZxBOpT+ISoHDAcOEG4JRyKVMOR3chL+8LQqf
ITi6kFsNxVLbhj6aDOjGRxP4BHjPw7TFmXrc7yc+xKPcXibi/V2x7zJYTu2Cs8Ck
vhbOQSUmoe3Cb8AV6zGU+ecYH5UjS8j/HhZ7xbkbggMC+aCxp76XJeB

-----END CERTIFICATE-----

3.5.10 Other: User Permissions

In this section the “admin” user can configure those permissions to which the “user” and “guest” users will have access. Configuration options that are not selected will not appear in the left-hand menu of the configuration page when logging in to the MTX-StarEnergy router using the username “user” or “guest”.



Additional Notes:

- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.

3.5.11 Other: Passwords

Three users can be given access the MTX-StarEnergy router's configuration page, each one having their own level of privileges. While "admin" users will have access to all MTX-StarEnergy configuration menus, "user" users will have access to those configuration menus which the "admin" user has selected for them (as indicated in point 3.6.10 of this manual), and "guest" users will have access the to same configuration menus as "user" users, but without being able to change them.

The screenshot displays the MTXRouter Titan Intelligent Router - Control Panel. The left sidebar contains a navigation menu with categories: Wan, LAN, Firewall, Serial Settings, VPN, and Other. The 'Other' category is expanded, showing options like AT Command, Meter Presence, Sms control, Periodic Autoreset, Time Servers, Remote Console, Snmp, Tacacs+, Https, User Permissions, Passwords Web UI (highlighted with a red box), CA-Certificates, and Syslog. The main content area is titled 'Other > Password Web UI' and contains two sections: 'Administrator' and 'General User'. Each section has input fields for Username, Password, and Re enter Password, along with a 'SAVE' button. The 'Administrator' section has a 'SAVE ADMIN PASS' button, and the 'General User' section has a 'SAVE USER PASS' button.

MTXRouter Titan
Intelligent Router - Control Panel

Other > Password Web UI

Administrator

Username: Mandatory. Default 'admin'

Password: Password for router administration

Re enter Password: Re-enter password for router administration

General User

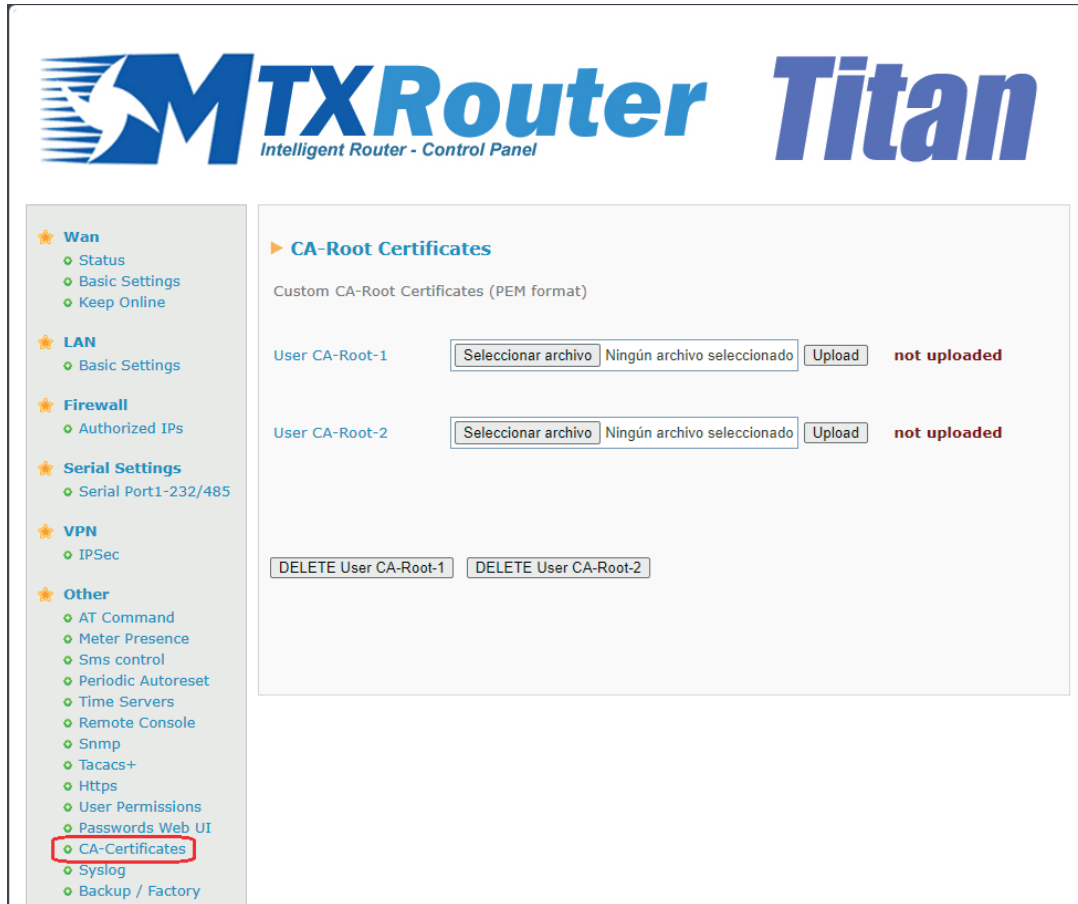
Username: Blank is not used

Password: Password for router administration (user)

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

3.5.12 Other: CA Certificates

The MTX-StarEnergy router has an internal list of the most commonly used CA certificates. If required in certain application scenarios, you can upload 2 user root CA certificates (in PEM format). These will be required if the MTX-StarEnergy router has to connect to an HTTPs server which has a self-signed certificate or a CA Root type which the MTX-StarEnergy router does not have.



Additional Notes:

- Remember that a backup of your router configuration is made (Backup), these certificates will also be included in the backup.

3.5.13 Other: Syslog

The MTX-StarEnergy router has a Syslog section where information messages from the operating system are shown, as well all messages from the router's own application. The Syslog is useful to check the device is working correctly and to establish the causes of any problems that may arise. The Syslog includes information about accessing the router (by who, how and from where the router was accessed), it will provide information about the network connection process (coverage, technology used, quality of service, it will identify problems if unable able to connect to the network, etc.) and will display a series of events such as information about meter presence detection, the connection of the IP-RS232/RS485 gateways, indicating both the IP and TCP port of origin, incoming CSD calls, reception of SMS commands, etc.

MTXRouter Titan
Intelligent Router - Control Panel

- ★ **Wan**
 - ◊ Status
 - ◊ Basic Settings
 - ◊ Keep Online
- ★ **LAN**
 - ◊ Basic Settings
- ★ **Firewall**
 - ◊ Authorized IPs
- ★ **Serial Settings**
 - ◊ Serial Port1-232/485
- ★ **VPN**
 - ◊ IPSec
- ★ **Other**
 - ◊ AT Command
 - ◊ Meter Presence
 - ◊ Sms control
 - ◊ Periodic Autoreset
 - ◊ Time Servers
 - ◊ Remote Console
 - ◊ Snmp
 - ◊ Tacacs+
 - ◊ Https
 - ◊ User Permissions
 - ◊ Passwords Web UI
 - ◊ CA-Certificates
 - ◊ **Syslog**
 - ◊ Backup / Factory
 - ◊ Firmware Upgrade
 - ◊ Reboot

ZLog > SYSLOG

Log:

```
Apr 7 19:20:43 starenergy local0.info Registration-status: Registered
Apr 7 19:20:43 starenergy local0.info Cellular-network-used: tech: 4G Operator:Movistar
Apr 7 19:20:43 starenergy local0.info Rssi: Signal Level-4G (RSSI: -65dBm, RSRP: -91dBm, RSRQ: -6dB): OK
Apr 7 19:21:09 starenergy local0.info Meter: presence OK - auto LA:1715
Apr 7 19:21:13 starenergy local0.info Registration-status: Registered
Apr 7 19:21:13 starenergy local0.info Cellular-network-used: tech: 4G Operator:Movistar
Apr 7 19:21:14 starenergy local0.info Rssi: Signal Level-4G (RSSI: -65dBm, RSRP: -92dBm, RSRQ: -7dB): OK
Apr 7 19:21:44 starenergy local0.info Registration-status: Registered
Apr 7 19:21:44 starenergy local0.info Cellular-network-used: tech: 4G Operator:Movistar
Apr 7 19:21:44 starenergy local0.info Rssi: Signal Level-4G (RSSI: -65dBm, RSRP: -92dBm, RSRQ: -9dB): OK
Apr 7 19:21:54 starenergy local0.notice Watchdog_Hw[934]: Watchdog ack received
Apr 7 19:22:09 starenergy local0.info Meter: presence OK - auto LA:1715
Apr 7 19:22:13 starenergy local0.info Registration-status: Registered
Apr 7 19:22:13 starenergy local0.info Cellular-network-used: tech: 4G Operator:Movistar
Apr 7 19:22:13 starenergy local0.info Rssi: Signal Level-4G (RSSI: -63dBm, RSRP: -92dBm, RSRQ: -8dB): OK
Apr 7 19:22:44 starenergy local0.info Registration-status: Registered
Apr 7 19:22:44 starenergy local0.info Cellular-network-used: tech: 4G Operator:Movistar
Apr 7 19:22:44 starenergy local0.info Rssi: Signal Level-4G (RSSI: -65dBm, RSRP: -91dBm, RSRQ: -6dB): OK
Apr 7 19:23:10 starenergy local0.info Meter: presence OK - auto LA:1715
Apr 7 19:23:13 starenergy local0.info Registration-status: Registered
Apr 7 19:23:13 starenergy local0.info Cellular-network-used: tech: 4G Operator:Movistar
Apr 7 19:23:13 starenergy local0.info Rssi: Signal Level-4G (RSSI: -63dBm, RSRP: -91dBm, RSRQ: -7dB): OK
Apr 7 19:23:43 starenergy local0.info Registration-status: Registered
Apr 7 19:23:43 starenergy local0.info Cellular-network-used: tech: 4G Operator:Movistar
Apr 7 19:23:43 starenergy local0.info Rssi: Signal Level-4G (RSSI: -57dBm, RSRP: -92dBm, RSRQ: -8dB): OK
Apr 7 19:23:56 starenergy local0.notice Watchdog_Hw[934]: Watchdog ack received
Apr 7 19:24:10 starenergy local0.info Meter: presence OK - auto LA:1715
Apr 7 19:24:14 starenergy local0.info Registration-status: Registered
Apr 7 19:24:14 starenergy local0.info Cellular-network-used: tech: 4G Operator:Movistar
Apr 7 19:24:14 starenergy local0.info Rssi: Signal Level-4G (RSSI: -63dBm, RSRP: -92dBm, RSRQ: -7dB): OK
Apr 7 19:24:39 starenergy local0.info KeepAlive: Keep alive to 8.8.8.8: OK
Apr 7 19:24:43 starenergy local0.info Registration-status: Registered
Apr 7 19:24:43 starenergy local0.info Cellular-network-used: tech: 4G Operator:Movistar
```

[REFRESH LOG](#) [SYSLOG CONFIG](#) [Click here for download current SYSLOG complete file](#)

At the bottom of the screen there are two buttons (in the lower left area) and one or more links (in the lower right area). The “REFRESH LOG” button is used to refresh the log window to display the latest available information (the last available 100KB of logs will be displayed). Clicking the link “Click here to download the complete current SYSLOG file” will download the complete LOG file of up to 1MB. The log files are rotating and can store up to 5 files. If historical log files exist, they can also be downloaded on the same screen. Lastly, the “SYSLOG CONFIG” button can be used to configure certain aspects of the SYSLOG system, as shown below.

MTXRouter Titan
Intelligent Router - Control Panel

Wan

- Status
- Basic Settings
- Keep Online

LAN

- Basic Settings

Firewall

- Authorized IPs

Serial Settings

- Serial Port1-232/485

VPN

- IPSec

Other

- AT Command
- Meter Presence
- Sms control
- Periodic Autoreset
- Time Servers
- Remote Console
- Snmp
- Tacacs+
- Https
- User Permissions
- Passwords Web UI
- CA-Certificates
- Syslog**
- Backup / Factory

Z-Other ▶ SYSLOG Config

Enabled Local: ☒ Enable Local Syslog

Enabled Server 1: ☒ Enable Remote Syslog Server 1

Remote Server 1: Remote Server 1 (DNS or IP)

Remote Port 1: Remote Server 1 UDP port

Enabled Server 2: ☒ Enable Remote Syslog Server 2

Remote Server 2: Remote Server 2 (DNS or IP)

Remote Port 2: Remote Server 2 UDP port

SAVE CONFIG

Enabled local: activates the local SYSLOG service storing the data in non-volatile memory.

Enabled Server 1: activates the SYSLOG remote sending service to remote server 1.

Remote Server 1: lets you specify the IP or DNS of remote SYSLOG server 1.

Remote Port 1: lets you specify the UDO port of remote SYSLOG server 1.

Enabled Server 2: activates the SYSLOG remote sending service to remote server 2.

Remote Server 2: lets you specify the IP or DNS of remote SYSLOG server 2.

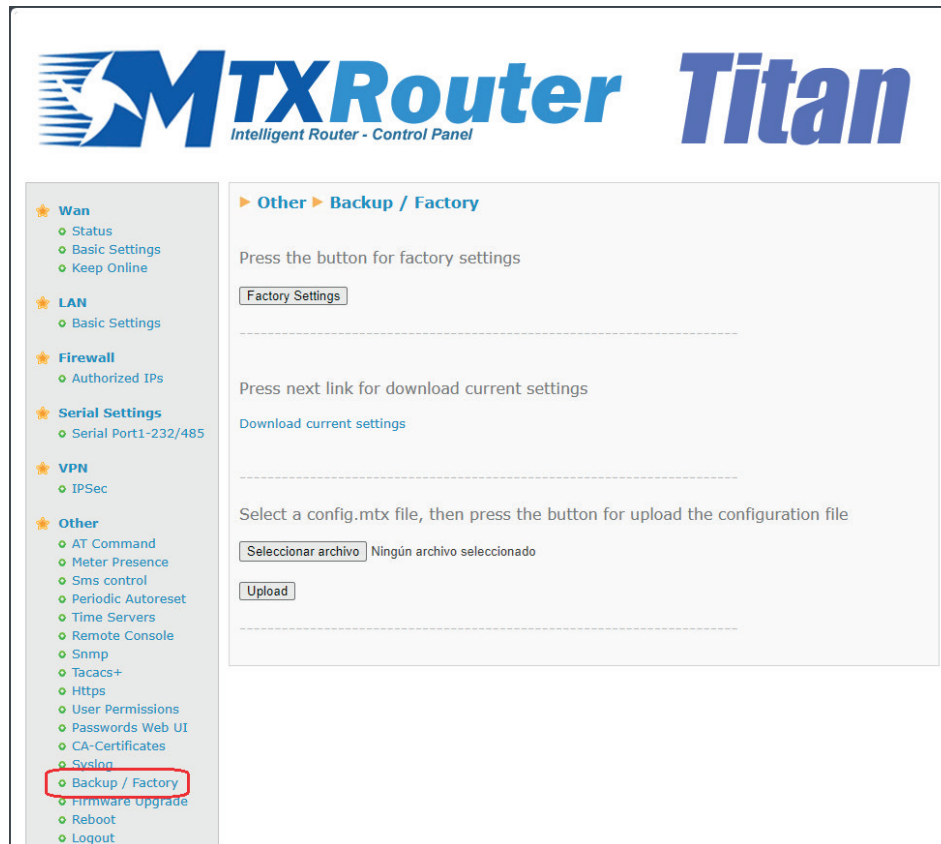
Remote Port 2: lets you specify the UDO port of remote SYSLOG server 2.

Additional Notes:

- Once the configuration process is finished, click on the “SAVE CONFIG” button to save the changes. Remember that you must restart the device for the new changes to take effect.

3.5.14 Other: Backup/Factory

You can make a full backup of the MTX-StarEnergy router's settings from this menu. You can save the configuration to a file and restore it back to the device when needed. You can also reset the MTX-StarEnergy to factory settings.

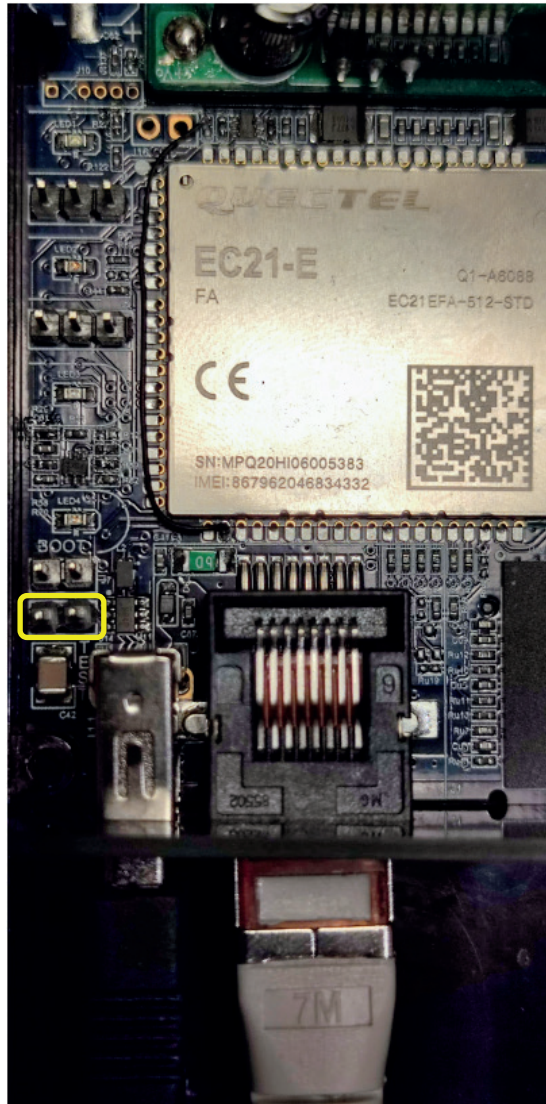


- “Factory Settings” button: press to restore the equipment with factory settings.
- Link “Download settings”: click the link to download the MTX-StarEnergy router's configuration in a file named “config.mtx”. The link will be greyed out if a new configuration has been applied to the router without rebooting it.
- “Select file” button: press to restore a previously saved configuration. After selecting the configuration file to restore, click the “Upload” button to load the file.

Additional Notes:

- The MTX-StarEnergy router can also be restored to factory settings using a jumper inside it. The procedure is as follows:
 - Turn off the power to the MTX-StarEnergy router and wait until the LEDs go out (until the supercap power runs out, or about 1 minute).
 - Connect the "factory settings" jumper as indicated in the following photo.
 - Turn on the MTX-StarEnergy router.
 - Wait until the red, blue and yellow LEDs are flashing slowly.

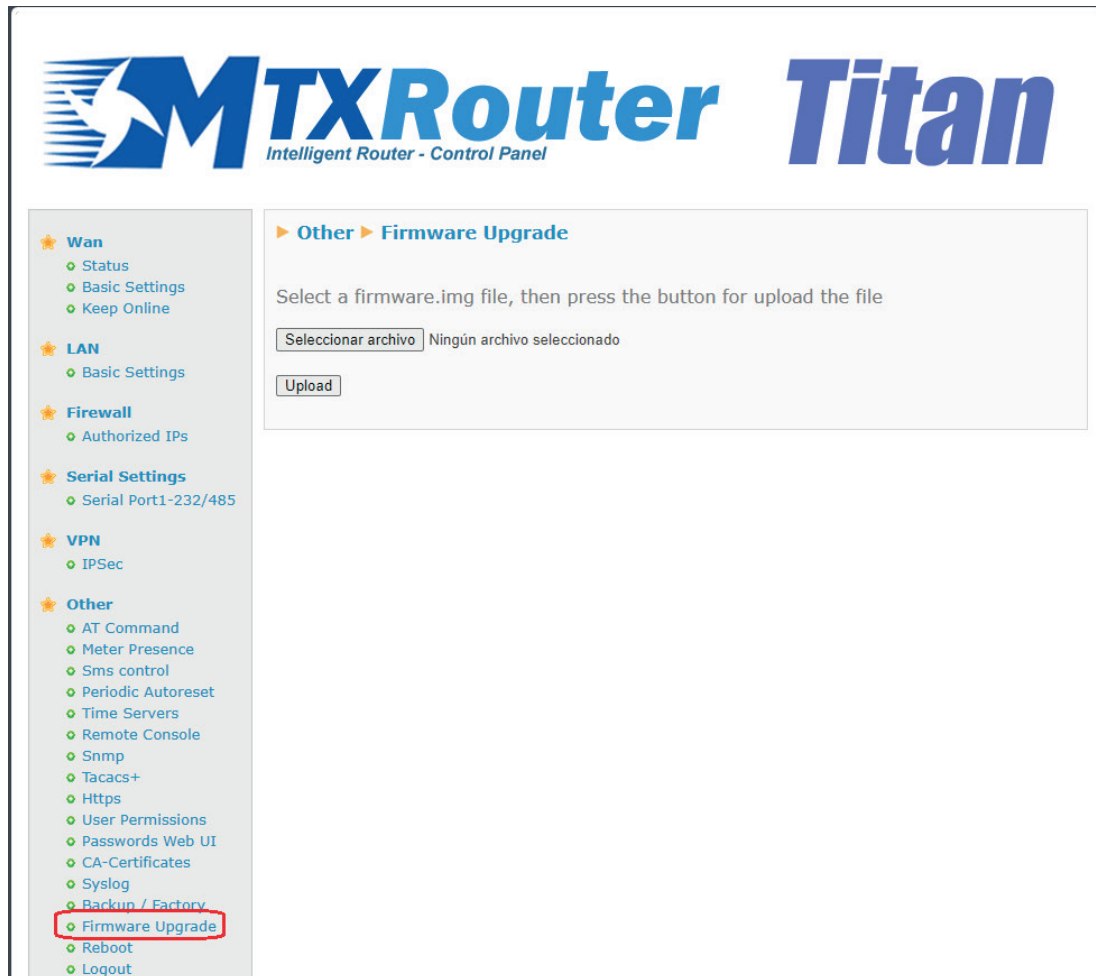
- Remove the "factory settings" jumper.
- Turn on the MTX-StarEnergy router.



3.5.15 Other: Firmware Upgrade

In this section you can update the MTX-StarEnergy router's FW either locally or remotely using the router's Web configuration environment. Simply click on "Select File" and choose the firmware file with which to update the device. Then click on the "Upload" button.

The update process will take approximately 2 minutes. The router will then reboot automatically.



Additional Notes:

- You can also launch the remote firmware update process using AT commands, they can be launched either by SNMP or by SSH. See the AT Commands and SNMP section for more information.

4. AT commands

The MTX-StarEnergy router's firmware lets you send AT commands directly to the internal modem and to the MTX-StarEnergy router itself using various interfaces:

- SMS.
- Telnet/SSH (remote console).
- Webserver.
- SNMP.

You can therefore send AT commands to the MTX-StarEnergy at your own risk. The accepted AT commands are those listed in the AT commands manual of the internal GSM module, plus the additional ones listed below:

```
AT^MTXTUNNEL=REBOOT
```

Action: reset the MTX-StarEnergy router.

```
AT^MTXTUNNEL=VERSION
```

Action: return the MTX-StarEnergy router's firmware version.

```
AT^MTXTUNNEL=GETIP
```

Action: return the WAN IP address (4G/3G/2G).

```
AT^MTXTUNNEL=GETTIME
```

Action: return the current time.

Example 1: AT^MTXTUNNEL=GETTIME

```
AT^MTXTUNNEL=GETTIME
```

```
21/05/2016 10:56:52
```

```
OK
```

```
AT^MTXTUNNEL=GETPARAM,paramName
```


Action: lets you read the value of a configuration parameter in the MTX-StarEnergy router. For example, you can check the configured APN field, the speed of the serial port, etc. using AT commands in the same way as with SNMP with the appropriate OIDs. Contact Matrix Electronics iotsupport@mtxm2m.com if you want to use this command to read a specific configuration parameter, instead of doing it via SNMP or WebServer.

Example 1: reading the speed of the serial port using an AT command.

```
AT^MTXTUNNEL=GETPARAM,COM1_BAUDRATE
```

```
AT^MTXTUNNEL=SETPARAM,paramName,paramValue
```

Action: lets you change the values of the MTX-StarEnergy router's configuration parameters. For example, you can change the configured APN field, the speed of the serial port, etc. using AT commands in the same way as with SNMP, through the appropriate OIDs. Contact Matrix Electronics iotsupport@mtxm2m.com if you want to use this command to change the configuration of a specific parameter, instead of doing it through SNMP or Webserver. Remember that you must reset the device for the changes to the configuration to take effect.

Example 1: change the speed of the serial port to 115200 using an AT command.

```
AT^MTXTUNNEL=SETPARAM,COM1_BAUDRATE,115200
```

```
AT^MTXTUNNEL=PRESENCE
```

Action: lets you change the execution of the electricity meter presence detection process without needing to wait for the programmed check interval to expire. The command will return OK if the meter is detected, an ERROR if it cannot be detected, or the [BUSY] ERROR if a CSD or IP session is open when trying to execute it.

```
AT^MTXTUNNEL=OTAPFWSFTP,<sftpserver>,<username>,<password>,<path/  
FirmwareFile.img>
```

Action: launch the MTX-StarEnergy router's FW update process. The <sftpserver>, <path/FirmwareFile.img>, <username> and <password> fields are optional. If the optional fields in the command are filled in, they will be used in the update process. If they are not used, those configured in the SNMP variables SFTP_FW_SERVER, SFTP_FW_FILE, SFTP_FW_USERNAME and SFTP_FW_PASSWORD will be used (see the SNMP section in this manual).

Example 1: FW update command specifying all parameters of the command.

```
AT^MTXTUNNEL=OTAPFWSFTP,77.231.220.143:20022,myuser,mypassword,sftpuser/otapfirmware/  
TITANSTARE-upgradeMicro_v4.10.7.10bXX.img
```

Example 2: FW update command specifying all parameters of the command.

```
AT^MTXTUNNEL=OTAPFWSFTP,,,,,
```

```
AT^MTXTUNNEL=OTAPCONFIGSFTP,<sftpserver>,<username>,<password>,<path/configFile.mtx>
```

Action: launch the MTX-StarEnergy router's configuration update process. The <sftpserver>, < path/configFile.mtx>, <username> and <password> fields are optional. If the optional fields are filled in the AT command, they will be used in the update process. If they are not used, the values of the SNMP variables SFTP_CONFIG_SERVER, SFTP_CONFIG_FILE, SFTP_CONFIG_USERNAME and SFTP_CONFIG_PASSWORD will be used (see the SNMP section in this manual).

Example 1: configuration file update specifying all the parameters of the command.

```
AT^MTXTUNNEL=OTAPCONFIGSFTP,77.231.220.143:20022,myuser,mypassword,sftpuser/otapconfig/config44.mtx
```

Example 2: configuration file update without specifying the parameters of the command (the “,” characters must be included).

```
AT^MTXTUNNEL=OTAPCONFIGSFTP,,,,
```

```
AT^MTXTUNNEL=DELETESYSLOG
```

Action: if the SYSLOG is enabled for storage in the router's internal non-volatile memory, executing this AT command causes the file and its prior versions to be deleted.

5. LEDs

The MTX-StarEnergy has 4 indicator LEDs coloured green, blue, orange and red. The following table describes the behaviour of each one:

	GREEN LED	BLUE LED	ORANGE LED	RED LED
Power off	OFF			
Power off	ON			
Boot failure	Fast blinking			
Power failure	Slow blinking			
Starting router			3 blinks	
Sim card detected and ready			Slow blinking/fast blinking/ON depending on the coverage	
SIM card not detected or incorrect PIN			OFF	
Not enough/critical coverage			Slow blinking	
Low coverage			Fast blinking	
Good coverage			ON	
No connection to APN		OFF		
APN connection ON (2G)		Slow blinking		
APN connection ON (3G)		Fast blinking		
APN connection ON (4G)		ON		

TCP port in listening state with TCP encapsulation disabled			OFF
TCP port in listening state with TCP encapsulation enabled			ON
Data transfer in progress			fast blinking
Default settings (jumper)	Slow blinking	Slow blinking	Slow blinking

1. Appendix:

1.1 Example - Remote FW update via SFTP and SNMP, using an AT command, but without prior SFTP configuration.

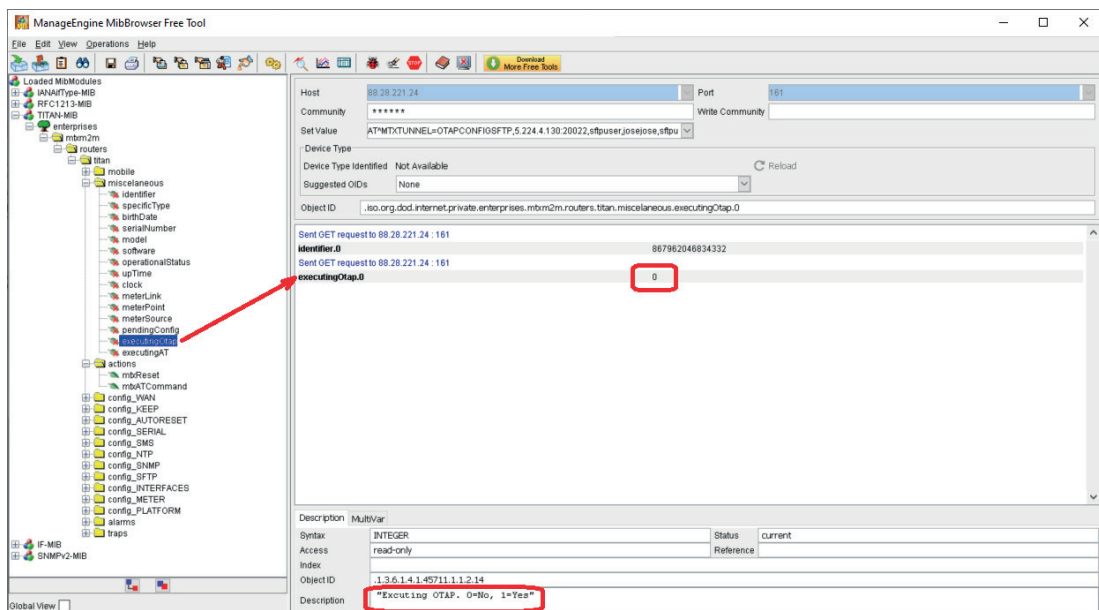
Description of how to update the MTX-StarEnergy router's FW using FW files hosted on an SFTP server via SNMP. In this example we will execute a single remote AT command without the need to configure the username, password, SFTP, server IP and file OIDs, which will improve security as confidential data does not need to be stored on the router.

In this example, the MTX-StarEnergy router's FW is assumed to be hosted on the following SFTP server:

- IP/DNS address: 5.224.1.130
- TCP Port: 20022
- Username: sftpuser
- Password: josejose
- FW path: sftpuser/otapfirmware/TITANSTARE-upgrade_v4.10.7.12XX.img

STEP 1 (optional):

The “executingOtap” OID can be read before starting an OTAP process. This will return a “1” if the MTX-StarEnergy router is in the middle of an OTAP process, and a “0” if it is not. In the following screenshot, as an OTAP process is not yet running, we can see that it returns a value of “0”.

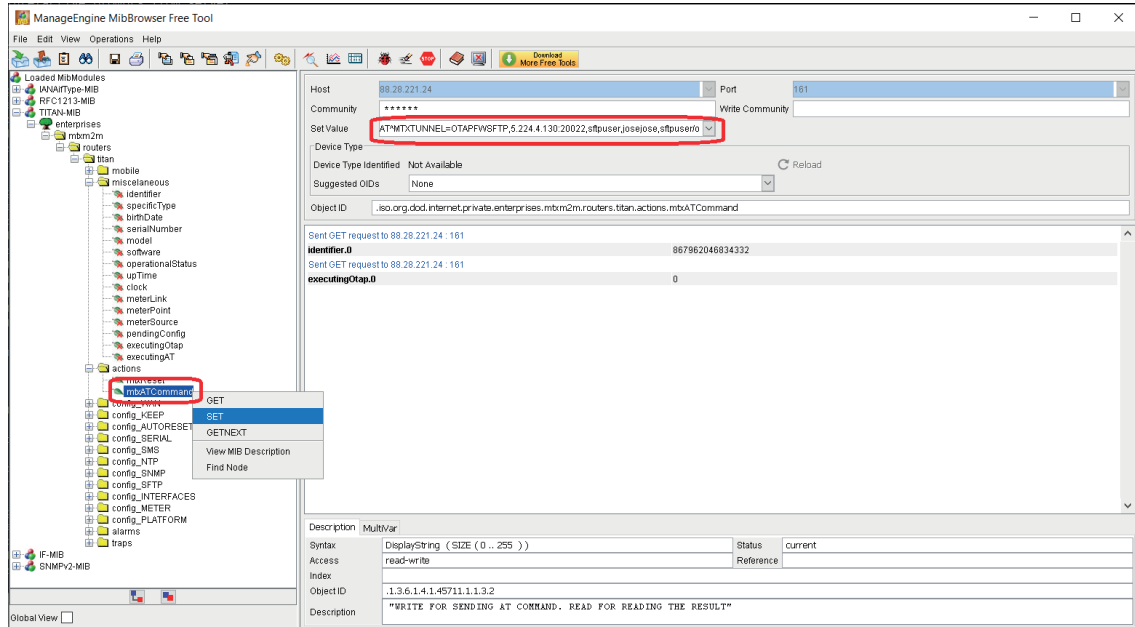


STEP 2:

To start an OTAP process, just execute (SET) the AT command:

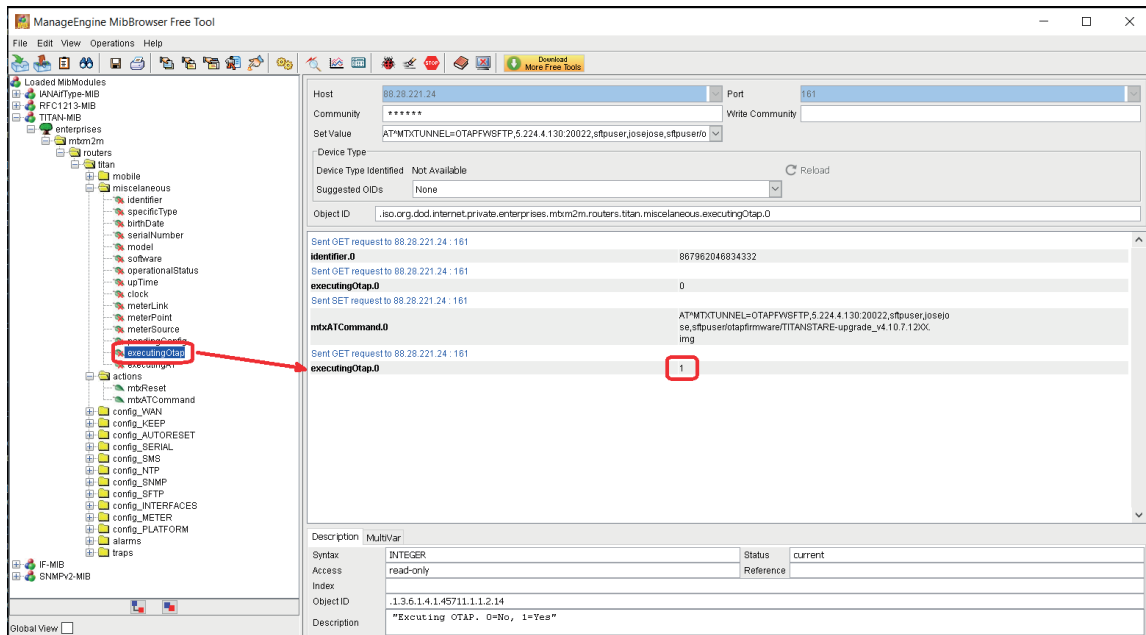
AT^MTXTUNNEL=OTAPFWSFTP,5.224.4.130:20022,sftpuser,josejose,sftpuser/otapfirmware/
TITANSTARE-upgrade_v4.10.7.14XX.img

in the “mtxATCommand” OID.



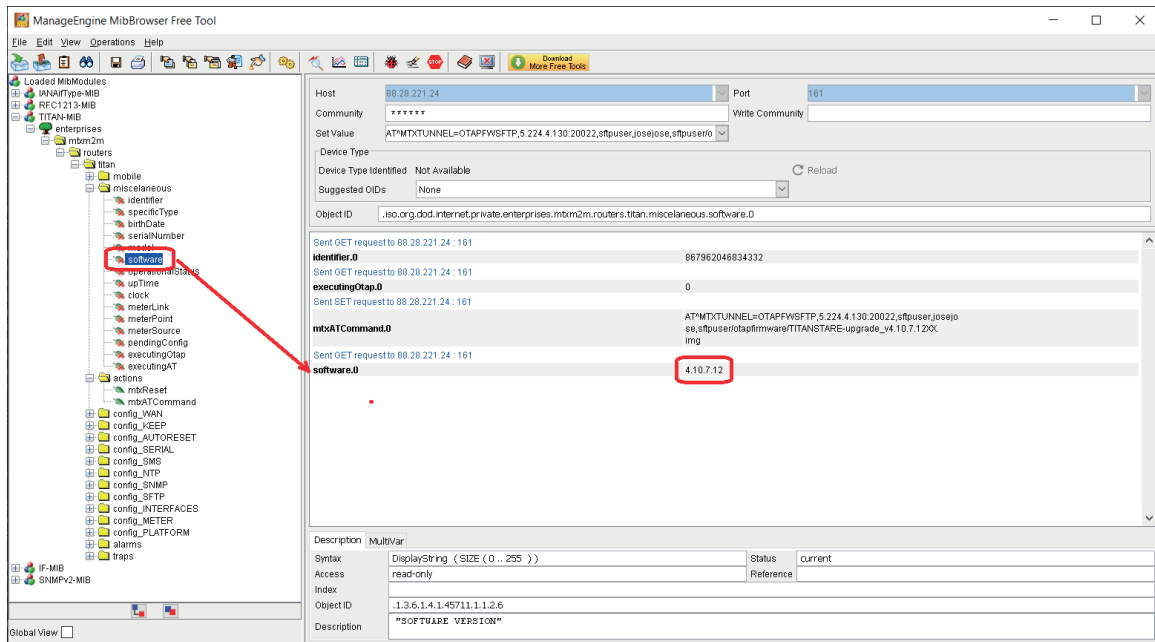
STEP 3 (optional):

As in step 1, we can see if the MTX-StarEnergy router is running an OTAP process. This log can be read after the upgrade before the router reboots.

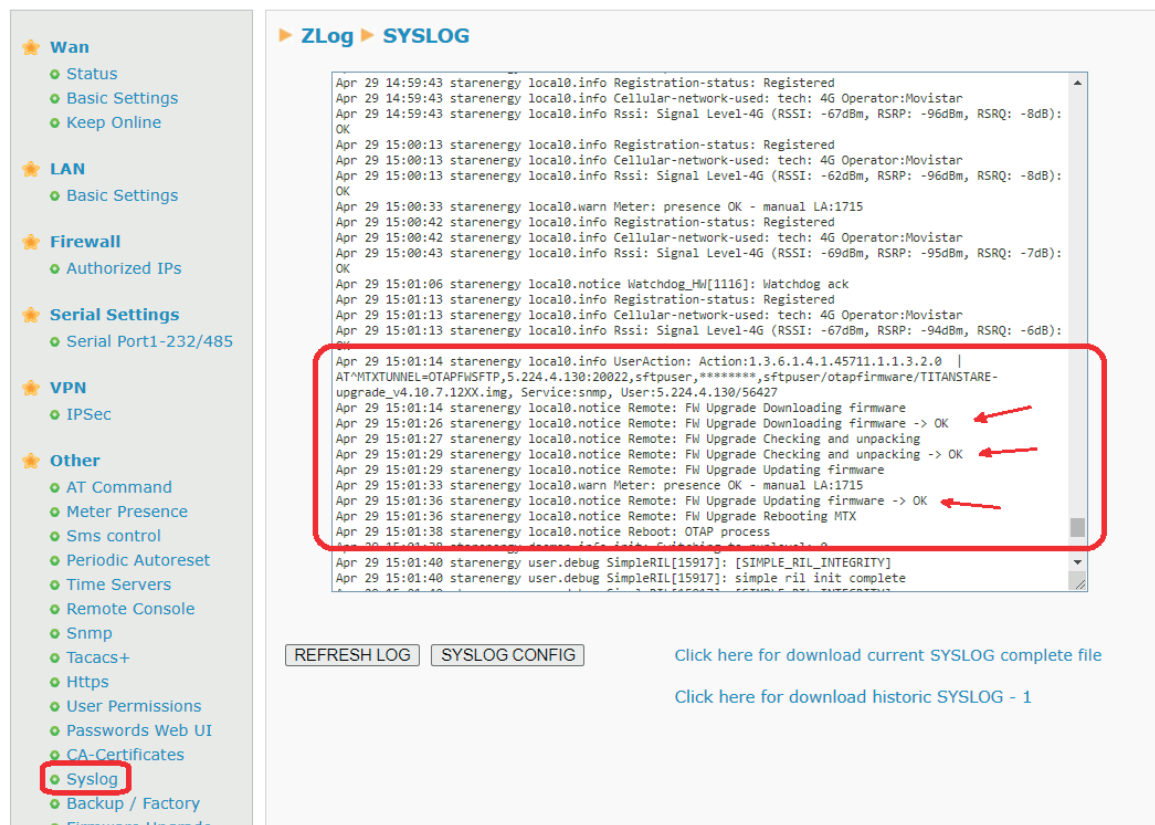


STEP 4 (optional):

Once the MTX-StarEnergy router has been updated it will automatically reboot, the new FW version can then be obtained.



If there are problems, go to the router's SYSLOG menu. Here you can check that the file was downloaded correctly, that the file was not corrupted, that it was unpacked correctly and that the update was performed correctly.



1.2 Example - Remote FW update via SFTP and SNMP, using an AT command and with prior SFTP configuration.

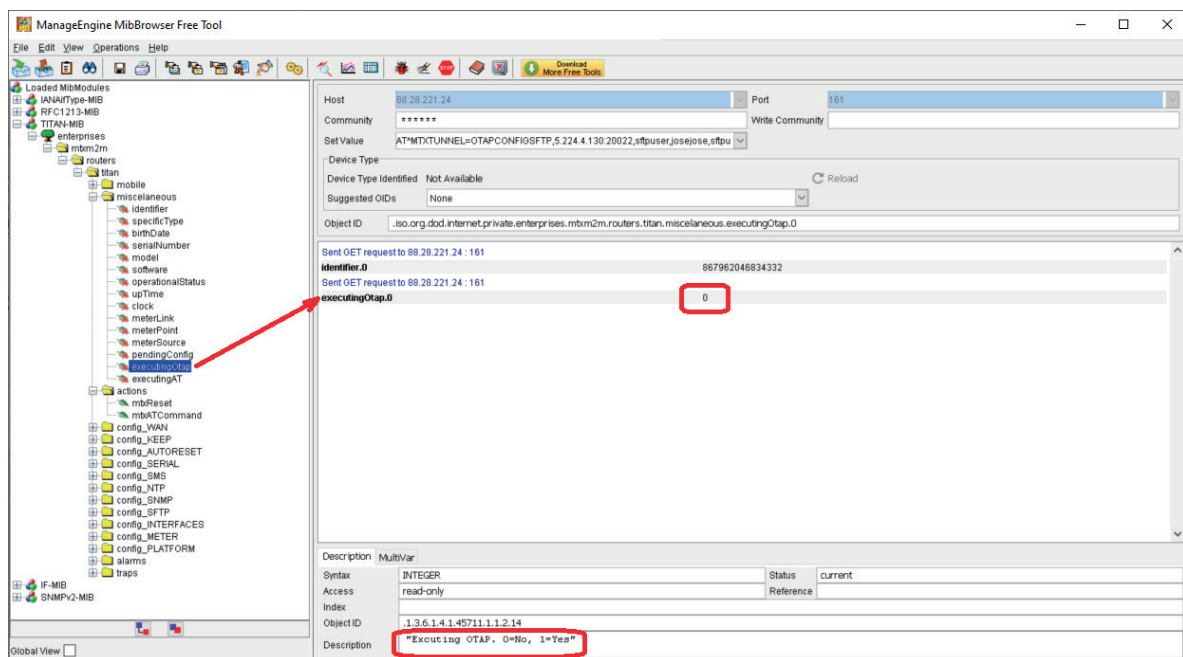
Description of how to update the MTX-StarEnergy router's FW using FW files hosted on an SFTP server via SNMP. In this example we will execute a single remote AT command with prior configuration of the username and password SFTP OIDs, the server IP and the file in the router.

In this example, the MTX-StarEnergy router's FW is assumed to be hosted on the following SFTP server:

- IP/DNS address: 5.224.1.130
- TCP Port: 20022
- Username: sftpuser
- Password: josejose
- FW path: sftpuser/otapfirmware/TITANSTARE-upgrade_v4.10.7.12XX.img

STEP 1 (optional):

The “executingOtap” OID can be read before starting an OTAP process. This will return a “1” if the MTX-StarEnergy router is in the middle of an OTAP process, and a “0” if it is not. In the figure below, since an OTAP process is not yet running, it will return a value of “0”.



STEP 2:

In this example, the Username, Password, server IP and FW file parameters are configured before starting the OTAP process. These parameters are stored in the OIDs included in the “config_SFTP” section.

The screenshot shows the ManageEngine MibBrowser Free Tool interface. On the left, the tree view displays the hierarchy of MIB modules, with 'config_SFTP' highlighted. On the right, the configuration details for 'config_SFTP' are shown. The 'Host' is set to '88.28.221.24' and the 'Port' is '161'. The 'Community' is '*****' and the 'Set Value' is 'josejose'. The 'Device Type' is 'Not Available'. The 'Object ID' is '.iso.org.dod.internet.private.enterprises.mtm2m.routers.titan.config_SFTP'. The configuration table lists the following parameters:

Parameter	Value
SFTP_FW_SERVER.0	5.224.1.130.20022
SFTP_FW_FILE.0	stfuserotapfirmware/TITANSTARE-upgrade_v4.10.7.120x.img
SFTP_FW_USERNAME.0	stfuser
SFTP_FW_PASSWORD.0	josejose

STEP 3:

Remember that, if a configuration change is made (using the Web interface or via SMS, SSH or SNMP) it will not be applied by the MTX-StarEnergy router until the next reboot (either by remote reset, automatic reset, etc. or an on/off power cycle). I.e. if you need to configure the OIDs listed in point 1.2 above in the example, you must restart the router afterwards. You can check if there are pending configuration changes on the router by reading the pendingConfig OID. A value of “1” indicates that the router has a configuration pending application and that a reset must therefore be executed. In short, before executing an OTAP, the pendingConfig OID must have a value of “0”.

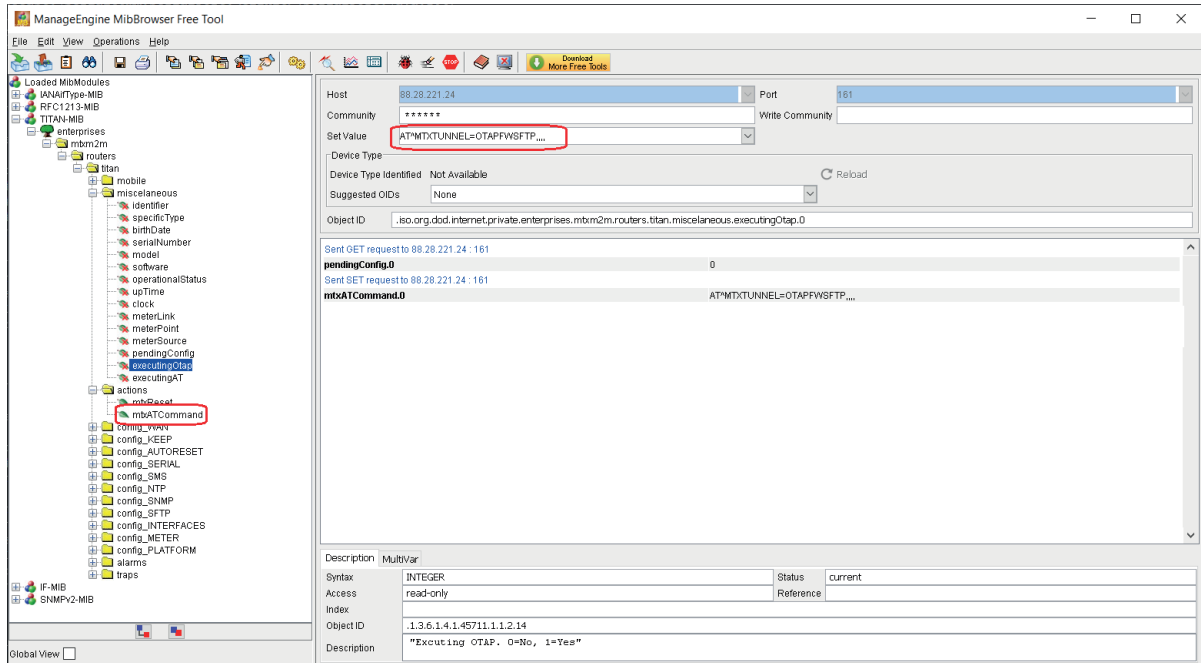
The screenshot shows the ManageEngine MibBrowser Free Tool interface, similar to the previous one, but with the 'config_SFTP' section highlighted in the tree view. The configuration details for 'config_SFTP' are shown on the right. The 'Host' is set to '88.28.221.24' and the 'Port' is '161'. The 'Community' is '*****' and the 'Set Value' is 'josejose'. The 'Device Type' is 'Not Available'. The 'Object ID' is '.iso.org.dod.internet.private.enterprises.mtm2m.routers.titan.config_SFTP'. The configuration table lists the following parameters:

Parameter	Value
SFTP_FW_SERVER.0	5.224.1.130.20022
SFTP_FW_FILE.0	stfuserotapfirmware/TITANSTARE-upgrade_v4.10.7.120x.img
SFTP_FW_USERNAME.0	stfuser
SFTP_FW_PASSWORD.0	josejose

STEP 4:

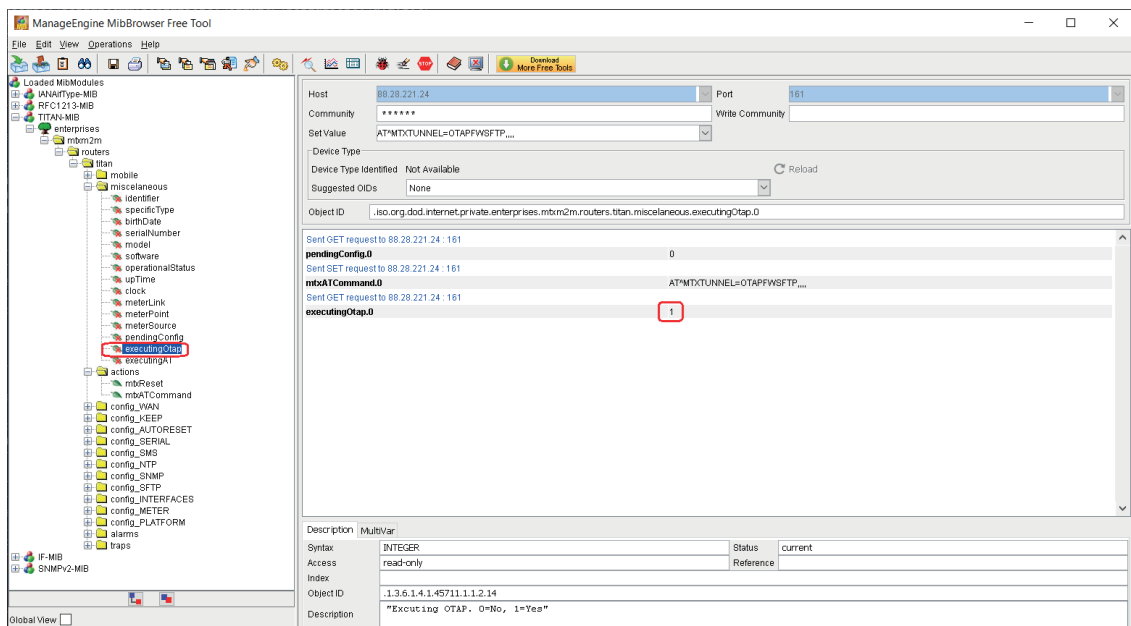
To execute the OTAP just send the command shown below. If no parameters are specified, the values shown in point 1.2 of this example will be used (SFTP server IP, file, username and password). The ",", must be included in the command, even if no configuration parameters are specified.

AT^MTXTUNNEL=OTAPFWSFTP,,,



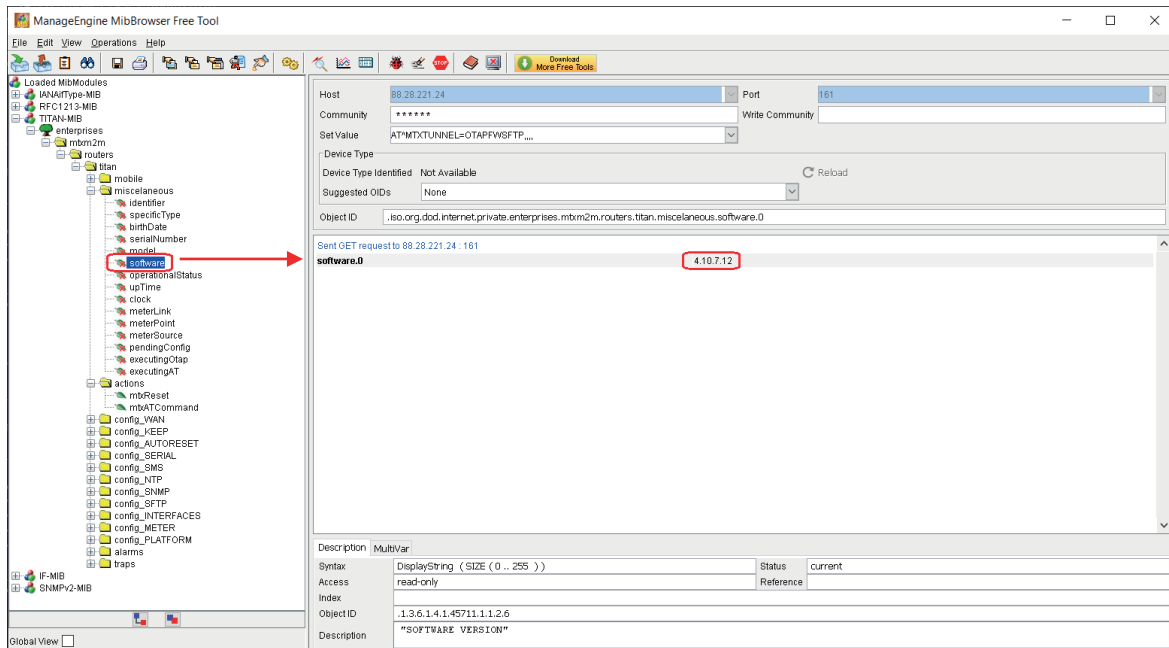
STEP 5 (optional):

As in step 1.1, we can see if the MTX-StarEnergy router is currently running an OTAP process. This log can be read before the router reboots. In the figure below, the value "1" indicates that the OTAP process is running.

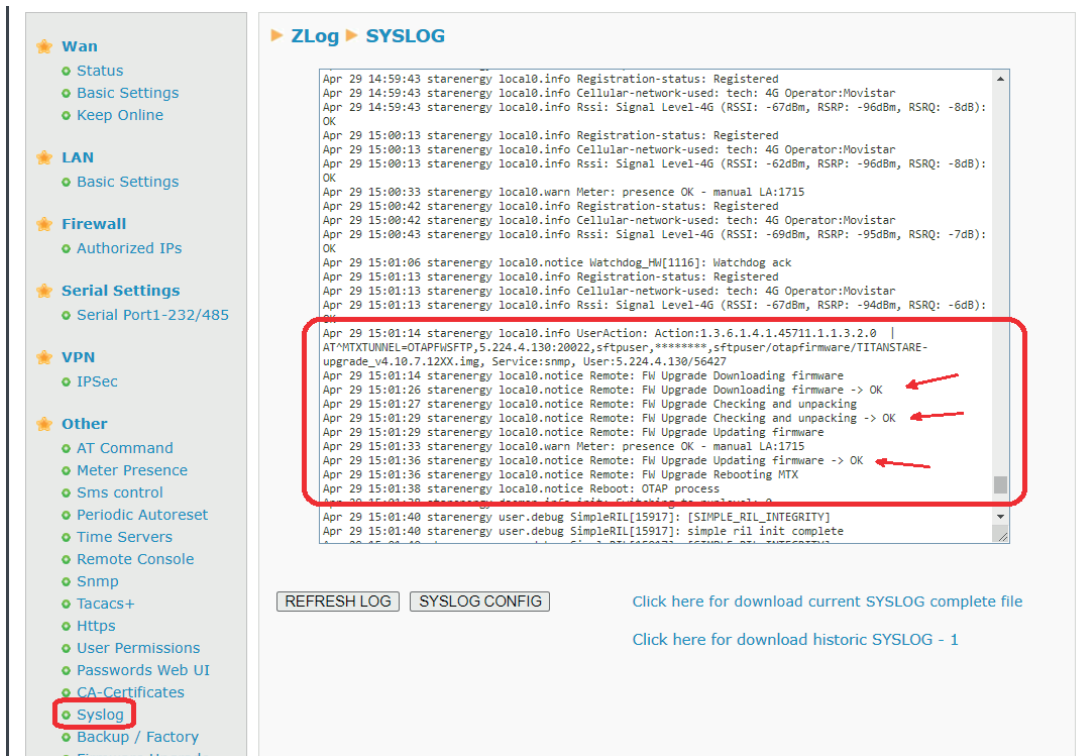


STEP 6 (optional):

Once the MTX-StarEnergy router has been updated it will reboot automatically, the new FW version can then be read.



If there are problems during the OTAP process, go to the router's SYSLOG menu. You can use it to check that the file was downloaded correctly, that the file was not corrupted, that it was unpacked correctly and that the update was performed correctly.



1.3 Example - Remote CONFIGURATION update via SFTP and SNMP, using an AT command, but without prior SFTP configuration.

Description of how to fully update the MTX-StarEnergy router's configuration via SNMP, from a configuration file hosted on an SFTP server. In this example we will execute a single remote AT command without the need to configure the username, password, SFTP, server IP and file OIDs, which will improve security as confidential data does not need to be stored on the router. Remember that you can configure each configuration parameter independently via SNMP with the corresponding OID, this method should only be used to change the entire configuration.

In this example, the MTX-StarEnergy router's FW is assumed to be hosted on the following SFTP server:

- IP/DNS address: 5.224.1.130
- TCP Port: 20022
- Username: sftpuser
- Password: josejose
- FW Path: sftpuser/otapconfig/config49.mtx

STEP 1 (optional):

The "executingOtap" OID can be read before starting an OTAP process. This will return a "1" if the MTX-StarEnergy router is in the middle of an OTAP process, and a "0" if it is not. In the figure below it will return a value of "0" as an OTAP process is not yet running. This OID is used for both FW and Configuration OTAPs.

The screenshot shows the ManageEngine MibBrowser Free Tool interface. On the left, a tree view displays various MIB modules, with a red arrow pointing to the 'executingOtap' OID under the 'miscellaneous' module. The main pane shows the details for the selected OID, including its name 'executingOtap.0' and its value '0'. The bottom pane provides a description of the OID: 'Executing OTAP. 0=No, 1=Yes'.

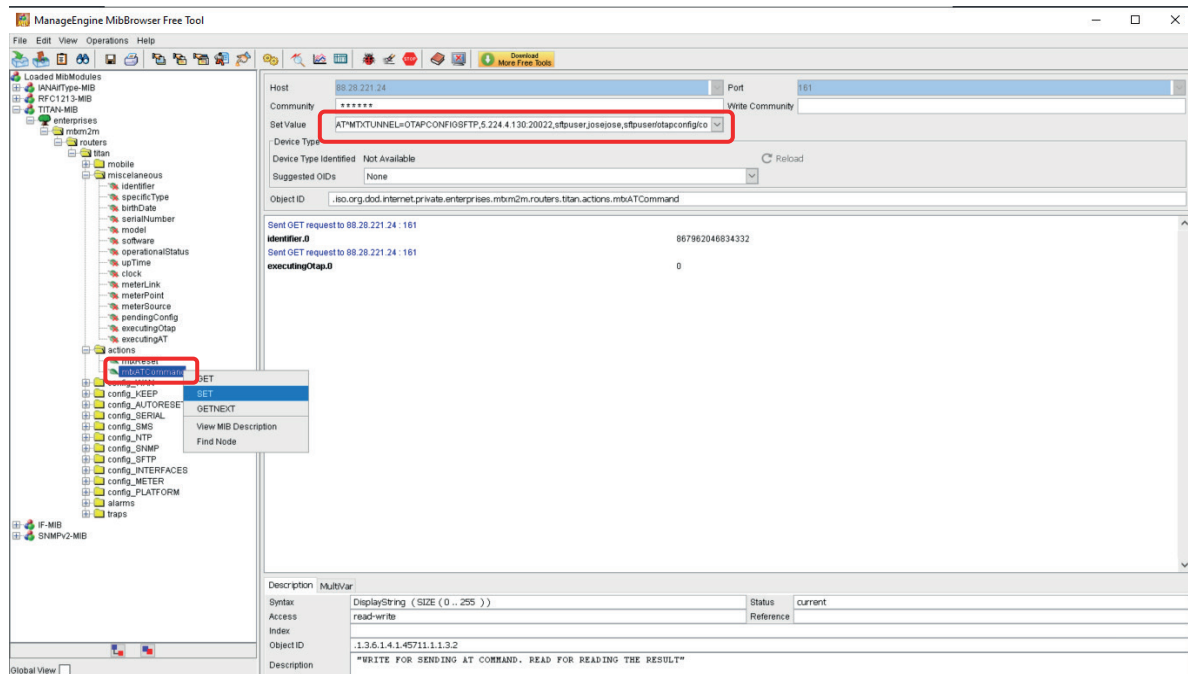
Description	MultiVar
INTEGER	Status
read-only	current
Index	Reference
Object ID	1.3.6.1.4.1.45711.1.1.2.14
Description	"Executing OTAP. 0=No, 1=Yes"

STEP 2:

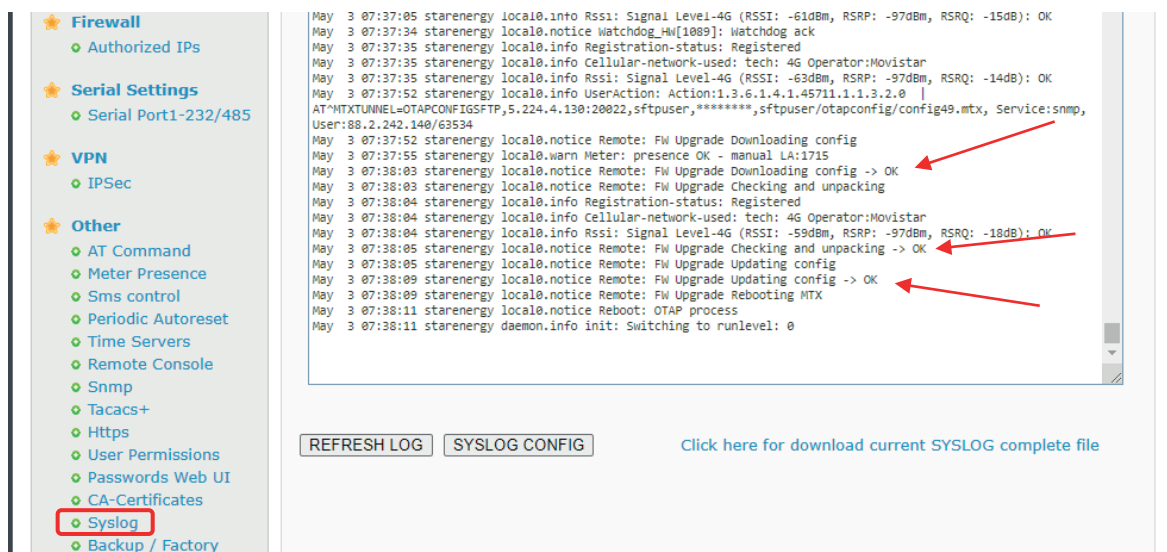
To start a configuration OTAP process, just execute (SET) the AT command:

AT^MTXTUNNEL=OTAPCONFIGSFTP,5.224.4.130:20022,sftpuser,josejose,sftpuser/otapconfig/config49.mtx

in the “mtxATCommand” OID.



After the remote configuration update, the router will automatically reboot with the new update. If there are problems with the update, go to the router's SYSLOG menu. Here you can check that the file was downloaded correctly, that the file was not corrupted, that it was unpacked correctly and that the update was performed correctly.



1.4 Example - Configuring the MTX-StarEnergy router to send SNMP alerts.

The MTX-StarEnergy router allows SNMP alerts to be sent. In this example, the router will be configured to send SNMP alerts to detect the lack of presence of the electricity meter, a loss of power and alerts about the router's operating system.

STEP 1:

1.- Configuring the SNMP service. In this example the following general SNMP configuration will be used:

<ul style="list-style-type: none">Wan<ul style="list-style-type: none">StatusBasic SettingsKeep OnlineLAN<ul style="list-style-type: none">Basic SettingsFirewall<ul style="list-style-type: none">Authorized IPsSerial Settings<ul style="list-style-type: none">Serial Port1-232/485VPN<ul style="list-style-type: none">IPSecOther<ul style="list-style-type: none">AT CommandMeter PresenceSms controlPeriodic AutoresetTime Servers	<h3>Other ▶ SNMP</h3> <p>Enabled: <input checked="" type="checkbox"/> Enable SNMP v2c</p> <p>SNMP Version: <input type="text" value="SNMPv3"/> SNMPv2 or SNMPv3</p> <p>UDP Port: <input type="text" value="161"/> Default UDP port 161</p> <p>Custom OID: <input type="text" value=".45711.1.1"/> Enterprise-Product OID. Default: .45711.1.1</p> <p>Community: <input type="text" value="public"/> Only SNMPv2. Password for GET and SET commands</p> <p>Username: <input type="text" value="myuser"/> Only SNMPv3.</p> <p>Auth Password: <input type="text" value="*****"/> Only SNMPv3 (min 8 char)</p> <p>Priv. Password: <input type="text" value="*****"/> Only SNMPv3 (min 8 char)</p> <p>Auth Protocol: <input type="text" value="SHA"/> Only SNMPv3.</p> <p>Priv Protocol: <input type="text" value="AES-128"/> Only SNMPv3.</p> <p>Engine ID: <input type="text" value="AUTO"/> Only SNMPv3. "AUTO" or custom HEX</p>
---	---

The configuration related to SNMP TRAPS will be as follows, in which the UDP port and the destination IP address for sending TRAPS are activated and specified:

<ul style="list-style-type: none">SnmTacacs+HttpsUser PermissionsPasswords Web UI	<p>Traps Enabled: <input checked="" type="checkbox"/> Enable Traps</p> <p>Traps - UDP Port: <input type="text" value="162"/> Default UDP port 162</p> <p>Traps - IP: <input type="text" value="5.224.4.130"/> IP for sending traps</p>
---	--

You must also select the SNMP alerts that you want to send. In this example, we will select all of them: the meter presence detection alert, the power failure alert, and OS alerts.

<ul style="list-style-type: none">Backup / FactoryFirmware UpgradeRebootLogout	<p>Alarm Presence: <input checked="" type="checkbox"/> Enable trap for Presence alarm</p> <p>Alarm Power: <input checked="" type="checkbox"/> Enable trap for Power alarm</p> <p>Alarm OS: <input checked="" type="checkbox"/> Enable trap for Oper. System alarm</p>
---	---

Lastly, we can specify the number of TRAPS to be sent when an alert is activated, the number when an alert is deactivated, and the interval (in seconds) between sending TRAPS for the same type of alert. In this example we will configure the MTX-StarEnergy router to send 10 TRAPS when an alert is activated, 5 TRAPS when it is deactivated, with a 60 second interval between sends.

Number traps alarm ON:	<input type="text" value="10"/>	Number the traps sent when an alarm is activated. 0 ... 1440
Number traps alarm OFF:	<input type="text" value="5"/>	Number the traps sent when an alarm is deactivated. 0 ... 1440
Trap period:	<input type="text" value="60"/>	Period between traps (10...3600 sec)

STEP 2:

The “Other > Meter Presence” menu section must be configured appropriately. In said menu you must specify the interval (in seconds) for checking the presence of the electricity meter, the number of retries in the event of a communications failure with the meter, and the Link Address for the meter.

- Wan
 - Status
 - Basic Settings
 - Keep Online
- LAN
 - Basic Settings
- Firewall
 - Authorized IPs
- Serial Settings
 - Serial Port1-232/485
- VPN
 - IPSec
- Other
 - AT Command
 - Meter Presence
 - Sms control
 - Periodic Autoreset

Other ▶ Meter Presence

Enabled: ☒ Enable Meter Presence service

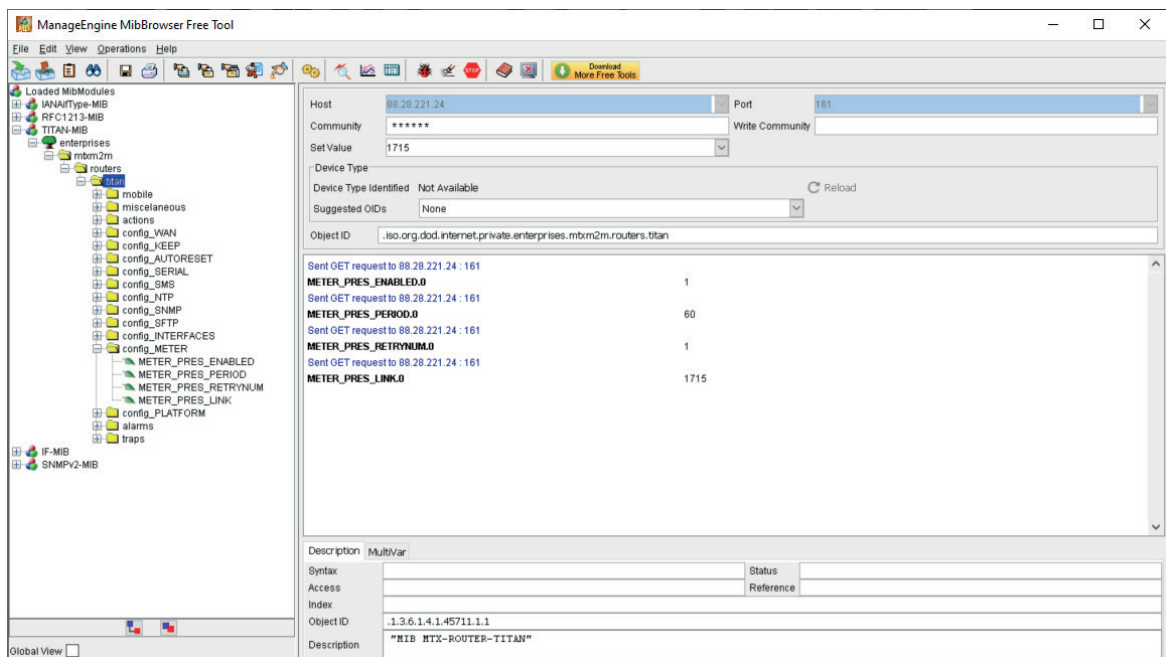
Period: Seconds (10 ... 86400)

Retries: Number of retries (0 ... 9)

Link address: Meter Link Address (default 1)

SAVE CONFIG

This can also be done via SNMP from the config_METER section.



STEP 3:

The MTX-StarEnergy router must be restarted for the new configuration to take effect.

STEP 4:

Considerations:

- The MTX-StarEnergy has an internal supercap giving it an autonomy of a little less than 1 minute.
- The MTX-StarEnergy router stores the power alarm status in non-volatile memory. This implies that if the device turned off due to a power loss (after the supercap runs out), when power returns and it restarts, the MTX-StarEnergy router takes into account the fact that, before shutting down due to a loss of power, the “power” alarm was activated, meaning that the TRAPS for the deactivated “power” alarm will be sent.
- The MTX-StarEnergy router also stores the electricity meter presence alarm status in non-volatile memory. Therefore, when the MTX-StarEnergy router’s presence detection alarm is activated (due to a communication failure with the meter) and it turns off, if the meter is present when communication is restored, the corresponding “alarm off” TRAPS will be sent. The active presence alarm TRAP is also reset each time a reading is taken to check presence. This means that if the meter presence check is configured to be performed every 12 hours and communication fails, the MTX-StarEnergy router will send the 10 presence alarm TRAPS every 12 hours.

STEP 5:

Example of a power alarm TRAP. The contents of a typical power alarm TRAP (loss of power supply) is shown below. To reproduce this TRAP, simply cut off the power to the MTX-StarEnergy. If the MTX-StarEnergy router is configured as shown in this example, it will send the alarm TRAP. It contains (*1) the OID of the TRAP, (*2) the value of the TRAP (1=alarm active, 0=alarm deactivated), (*3) the severity and (*4) the serial number of the MTX-StarEnergy router.

The screenshot shows a 'Trap Details' window with the following content:

TimeStamp	0 hours, 0 minutes, 54 seconds.
Enterprise	
Generic Type	
Specific Type	
Message	<pre>.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 0 hours, 0 minutes, 54 seconds.: .iso.org.dod.internet.snmpV2.snmpModules.is.1.3.0: IpAddress: 88.2.242.140: .iso.org.dod.internet.private.enterprises.mtxsm.router.titan.traps.powerTrap.0: 1: .iso.org.dod.internet.private.enterprises.mtxsm.router.titan.traps.severity.0: 3: .iso.org.dod.internet.private.enterprises.mtxsm.router.titan.miscellaneous.serialNumber.0: 0123456789ABCD:</pre>
Severity	Clear

Annotations in the image:

- *1 points to the Object ID: .1.3.6.1.4.1.48711.1.1.20.3.0:
- *2 points to the value 1:
- *3 points to the severity 3:
- *4 points to the serial number 0123456789ABCD:

STEP 6:

Example of a presence alarm TRAP. The contents of a meter not present alarm TRAP is shown below. To reproduce this TRAP, simply disconnect the meter from the MTX-StarEnergy router. If the MTX-StarEnergy router is configured as shown in this example, it will send the alarm TRAP as soon as a new presence detection process starts. It contains (*1) the OID of the TRAP, (*2) the value of the TRAP (1=alarm active, 0=alarm deactivated), (*3) the severity, (*4) the value of the “meterSource” OID which can have a value of “manual”, “default” or “auto”, (*5) the link address of the meter and (*6) the serial number of the MTX-StarEnergy.

Trap Details

Timestamp

0 hours, 19 minutes, 18 seconds.

Enterprise

Generic Type

Specific Type

Message

```

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 0 hours, 19 minutes, 18 seconds.:
.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapOID.0: Object ID: .1.3.6.1.4.1.45711.1.1.20.1.0:
.iso.org.dod.internet.snmpV2.snmpModules.18.1.3.0: IPAddress: 88.2.242.140:
.iso.org.dod.internet.private.enterprises.mtxmlm.routers.titan.traps.presenceTrap.0: 1:
.iso.org.dod.internet.private.enterprises.mtxmlm.routers.titan.traps.severity.0: 2:
.iso.org.dod.internet.private.enterprises.mtxmlm.routers.titan.miscellaneous.meterSource.0: manual:
.iso.org.dod.internet.private.enterprises.mtxmlm.routers.titan.miscellaneous.meterLink.0: 1715:
.iso.org.dod.internet.private.enterprises.mtxmlm.routers.titan.miscellaneous.serialNumber.0: 0123456789ABCD:

```

*1

*2

*3

*4

*5

*6

Offices and support

SPAIN

C/ Alejandro Sánchez 109
28019 Madrid
Tel: +34 915602737
Email: contact@webdyn.com

FRANCE

26 Rue des Gaudines
78100 Saint-Germain-en-Laye
Tel: +33 139042940
Email: contact@webdyn.com

INDIA

803-804 8th floor, Vishwadeep Building
District Centre, Janakpurt, 110058 Delhi
Tel: +91 1141519011
Email: contact@webdyn.com

PORTUGAL

Av. Coronel Eduardo Galhardo 7-1°C
1170-105 Lisboa
Tel: +351.218162625
Email: comercial@lusomatrix.pt

TAIWAN

5F, No. 4, Sec. 3 Yanping N. Rd.
Datong Dist. Taipei City, 103027
Tel: +886 965333367
Email: contact@webdyn.com

SUPPORT

Madrid office

Tel: +34 915602737
Email: iotsupport@mtxm2m.com

Saint-Germain-en-Laye office

Tel: +33 139042940
Email: support@webdyn.com

Delhi office

Tel: +91.1141519011
Email: support-india@webdyn.com

Taipei City office

Tel: +886.905655535
Email: iotsupport@mtxm2m.com