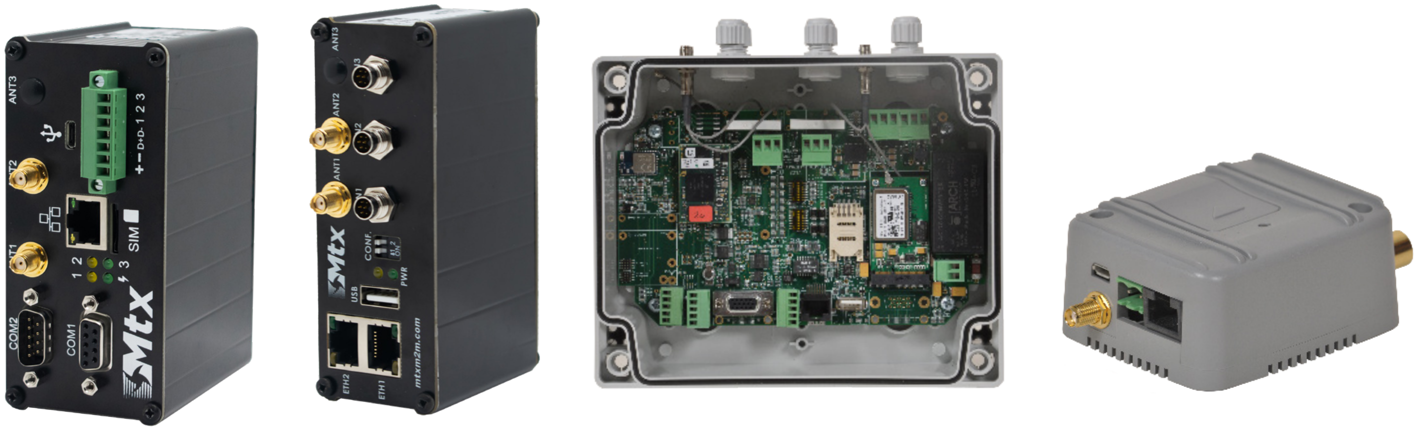
Mtx flexitron group

#WeAreConnectivity

SMART SOLUTIONS FOR A CHANGING WORLD



MTX-ROUTER-TITAN

MTX-ROUTER-TITAN II, MTX-ROUTER-TITAN, MTX-ROUTER-TITAN mini

SOFTWARE & HARDWARE

USERGUIDE

www.mtxm2m.com

INDEX

GENERAL NOTES

Product is deemed accepted by recipient and is provided without interface to recipient's products. The documentation and/or product are provided for testing, evaluation, integration and information purposes. The documentation and/or product are provided on an "as is" basis only and may contain deficiencies or inadequacies. The documentation and/or products are provided without warranty of any kind, express or implied. To the maximum extent permitted by applicable law, Matrix Electronica further disclaims all warranties, including without limitation any implied warranties of merchantability, completeness, fitness for a particular purpose and non-infringement of third-party rights. The entire risk arising out of the use or performance of the product and documentation remains with recipient. This product is not intended for use in life support appliances, 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 to be in accordance with the technical specifications provided in these guidelines. Failure to comply with any of the required procedures can result in malfunctions or serious discrepancies in results.

Furthermore, all safety instructions regarding the use of mobile technical systems, including GSM products, which also apply to cellular phones must be followed. Matrix Electronica or its suppliers shall, regardless of any legal theory upon which the claim is based, not be liable for any consequential, incidental, direct, indirect, punitive or other damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information or data, or other pecuniary loss) arising out the use of or inability to use the documentation and/or product, even if Matrix Electronica has been advised of the possibility of such damages. The foregoing limitations of liability shall not apply in case of mandatory liability, e.g. under the Spanish Product Liability Act, in case of intent, gross negligence, injury of life, body or health, or breach of a condition which goes to the root of the contract. However, claims for damages arising from a breach of a condition, which goes to the root of the contract, shall be limited to the foreseeable damage, which is intrinsic to the contract, unless caused by intent or gross negligence or based on liability for injury of life, body or health. The above provision does not imply a change on the burden of proof to the detriment of the recipient. Subject to change without notice at any time. The interpretation of this general note shall be governed and construed according to Spanish law without reference to any other substantive law.

IMPORTANT INFORMATION

This technical description contains important information for start up and use of the MTX-Router-Titan devices. Read it carefully before we start working with Titan router devices. The warranty will be void should damage occur due to non-compliance with these instructions for use. We cannot accept any responsibility for consequential loss.

SERVICE AND SUPPORT

To contact customer support please use the contact details below:

Address: Alejandro Sánchez 109, 28019 Madrid (Spain)
Email: gsmsupport@matrix.es
Website: mtxm2m.com

REVISION INFORMATION: VERSION 4.00.4.01 Release: January 2018

INTRODUCTION AND MODELS

Titan devices are 4G/3G/2G routers with advanced Gateway capacities.

As well as the classic router capacities, these devices can create 3G-RS232/485 gateways, control USB devices remotely, execute SMS commands (to check coverage, change relays, etc.) accept GSM data (CSD) calls to access devices such as electricity meters, read TCP or RTU modbus devices remotely, send temperature, distance data to the cloud, and many more possibilities.

For a greater understanding of the possibilities of these routers, we strongly recommend that you read Chapter 2 of this manual – the FAQs. After reading this, you will have a greater vision of what it can do. Once you have read the FAQs, take a look at the examples in the Annex. These examples will provide you with a clearer understanding of the routers' possibilities.

All users of our MTX modems and routers are provided with assistance with free technical support that offers quick and efficient responses. Therefore, if you still have doubts after reading this manual, do not hesitate to get in touch with us via email at gsmsupport@matrix.es. Likewise, if you have the need for a characteristic not yet included in our routers, or require a customized product, please let us know and we can investigate it for you.

MODELS

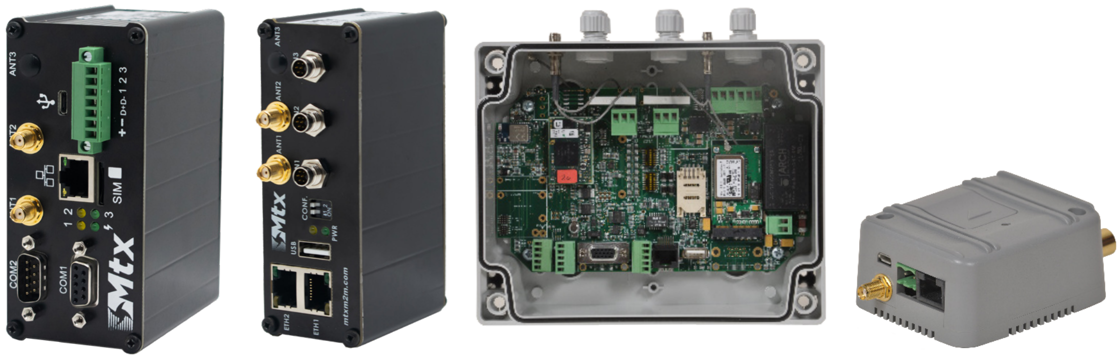
MTX-Router-Titan-II-SI
MTX-Router-Titan-II-SI-3G
MTX-Router-Titan-II-SI-3G-GPS
MTX-Router-Titan-II-SI-4G Cat1
MTX-Router-Titan-II-SI-4G Cat4
MTX-Router-Titan-II-SI-4G AT&T
MTX-Router-Titan-3G
MTX-Router-Titan-3G-GPS
MTX-Router-Titan-3G-WC25
MTX-Router-Titan-3G-W-MBus
MTX-Router-Titan-4G-GPS
MTX-Router-Titan-4G-W-MBus
MTX-Router-Titan (only Eth & WiFi)
MTX-Router-Titan-3G-mini
MTX-Router-Titan-3G-mini-GPS
MTX-Router-Titan-4G-mini-GPS
MTX-Router-Titan-mini (only Eth & WiFi)

FAQS, BASIC CONCEPTS

If we still have doubts after reading the previous list of benefits, it is recommend to read the following FAQs where everything we need to know about the main characteristics of the MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices is explained in a detailed manner.

- **What is the physical structure of the MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices like?**

  Below we have an image of the MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini:



- **What can I do with the MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices?**

  Basically, everything that can be done with a standard router is possible with this device, with the addition of several advanced gateway benefits. For example, we can give Internet connectivity to the devices connected to our Ethernet port, as well as providing NAT to connect via Internet to devices that are attached to the port.

- **Is it possible to connect WiFi enabled devices to Internet using a WiFi connection?**

  Essentially, yes. MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini can be used as an Access Point WiFi, and therefore can provide an Internet connection to WiFi enabled devices.

- **What is offered in terms of serial gateways?**

  Up to three simultaneous serial gateways can be used, whether they are of the form TCP Client or TCP Server. This means that we can control three or more serial devices.

- **What about RS232 or RS485 serial gateways?**

  With the MTX-Router-Titan device, we can have up to three RS232 gateways and one of these can be configured to be RS485. With the MTX-Router-Titan mini device, we can have up to two RS232 gateways, one of which is configureable to be RS485.

- **It would be interesting if the MTX-Router-Titan devices allowed Internet connectivity (via ETH or WiFi), but oure also capable of picking up and managing a GSM data (CSD) call for Metering applications. Is it possible?**

  Yes, but with restrictions. The MTX-Router-Titan must force itself to work in 2G mode. In this way, it can carry out the normal functions of the router at the same time that it manages a CSD calls that is received without problem.

- **I want a router but I need to be able to send AT commands directly to it to be able to send SMS, consult the network coverage, etc. Does the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini allow this?**

  Yes, both do, and in several ways. We can send AT commands from a serial port or a Telnet connection via IP and even SMS.

- **I notice that both the MTX-Router-Titan II, MTX-Router-Titan and the MTX-Router-Titan mini have a USB port. Could I connect a USB device to the gateway to create a USB gateway; i.e. control a USB device remotely?**

  If the USB uses the FTDI driver, then yes. For other types of drivers, we must investigate further. Please send an email to gsmsupport@matrix.es for more information.

- **Do the MTX-Router-Titan devices support a Modbus TCP to Modbus RTU gateway?**

  Yes, it does support this protocol conversion.

- **Can it also read Modbus RTU devices autonomously to send the data to the cloud?**

  Yes, it can. The MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices can read Modbus RTU devices, store the readings and send them to web platforms via a JSON object when there is network coverage.

- **In other words, the MTX-Router-Titan has the capability of a datalogger and can store data?**

  It can store many different types of data to send them later to web platforms. Amongst these we have ModBus readings, temperature readings, distance sensors, waveflows, etc.

- **Temperatures and distances?**

  We can directly connect an MTX-Temp-RS232 temperature sensor to a serial port on the MTX device and carry out many things. For example, we can periodically read and send to the cloud the temperatures, we can send an SMS alarm or IP message when the temperature is above or below a pre-determined level, etc. The Maxbotix RS232 distance sensor works exactly the same. The MTX device can periodically send the measurements, or send SMS alarms or IP messages whenever the distance measured is greater than or less than a particular value. Typical applications include grain silos.

- **Does it work the same for waveflows?**

  It works in a similar way. The MTX-Router-Titan device can read waveflows (pulse counters for electricity or water meters for metering applications) and send them to the cloud. Several utilities have been incorporated to check the RF link level in the MTX-Router-Titan device's web configuration environment.

- **What is meant by the web configuration environment?**

  All device configurations can be carried out by using the web configuration, i.e. on the devices' internal webserver.

- **Is it possible to read or load a complete configuration in the routers belonging to the Titan family? This helps the production process when there is a considerable number of devices to be configured.**

  Essentially, we can create backups/restorations of complete configurations.

- **Do the MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices have DynDNS?**

  Yes, they do, and compatible with NO-IP. Also, there is the possibility of using private DNS to send the current IP address, either every time it changes or periodically, to a private server such as our business server.

- **Can the relays also be controlled?**

  Yes, they can. The MTX-Router-Titan device has two relays and the MTX-Router-Titan mini device, being smaller, has just one relay. The relays can be changes from a web browser, via SMS, AT commands, Telnet or according to a timetable and even a temperature (high or low) or distance (longer or shorter).

- **If we talk about a timetable, does this mean that the MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini have a real time clock?**

  Yes, they are synchronized using NTP via Internet using UTC time.

- **Is there a digital entry to send alarms in case of changes?**

  Yes, but only with the MTX-Router-Titan mini device.

- **Can the MTX devices be configured by SMS?**

  Yes, they can. We can send AT commands via SMS in order to restart the device, change the configuration, find out the IP address, check the network coverage, etc.

- **I would like to be able to personalize the web configuration environment with my company's logos and images. Can this be done?**

  Yes. Users are free to customize the web configuration environment using their logos, headers/footers, etc. We can even choose which menus the final user can see/change.

- **Do the MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini have an LED indicator light?**

  Yes, they do. There is also a user-configurable LED that can illuminate in red if the device cannot read the IP address, or if the network coverage is weak, etc.

- **Finally, can MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices carry out all the previous simultaneously?**

  Yes, they can. For example, 3G-RS232 gateways can run alongside a USB gateway whilst allowing a device to connect to the Internet using its Ethernet connection, or giving WiFi connectivity to PDAs, whilst using DynDNS, timed relays, or sending to the cloud readings from water meters obtained by RF868MHz, etc. All this can work simultaneous and in harmony.

SOFTWARE

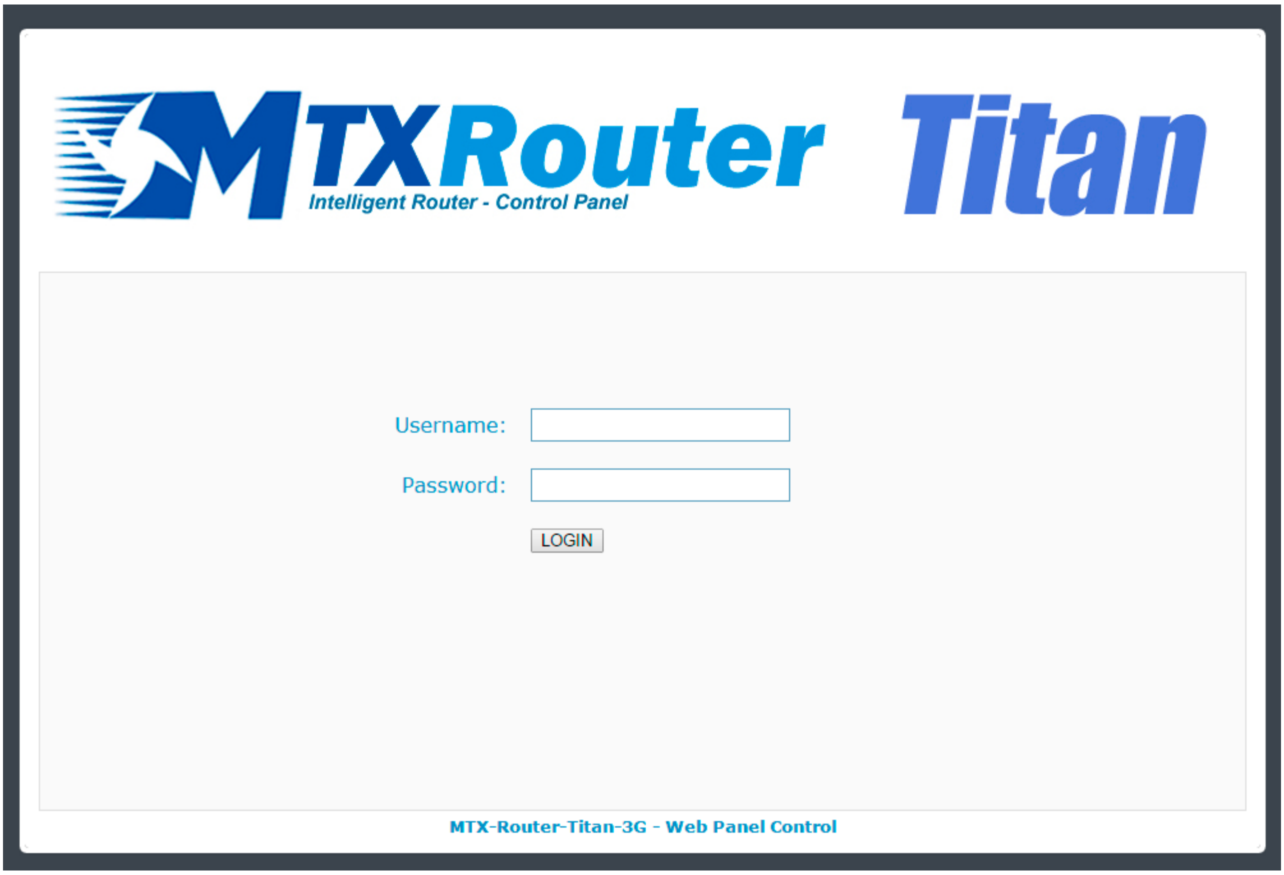
1. Step-by-Step Configuration

As previously mentioned, the configuration of the MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices is done using a web environment. What is needed?

- A PC with a web browser (Chrome, IExplorer, Firefox...) and Ethernet port
- An Ethernet cable to connect the PC with the MTX device

Steps to access the configuration environment.

1. Connect the Ethernet cable to the PC and MTX device.
2. The PC must have a fixed IP address and of the form 192.168.1.X, given the default IP address of the MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices is 192.168.1.2.
3. Open a browser with the address http://192.168.1.2:


MTXRouter Titan
Intelligent Router - Control Panel
Username:
Password:
LOGIN
MTX-Router-Titan-3G - Web Panel Control

4. Use the default username and password: admin and admin

2. Configuration

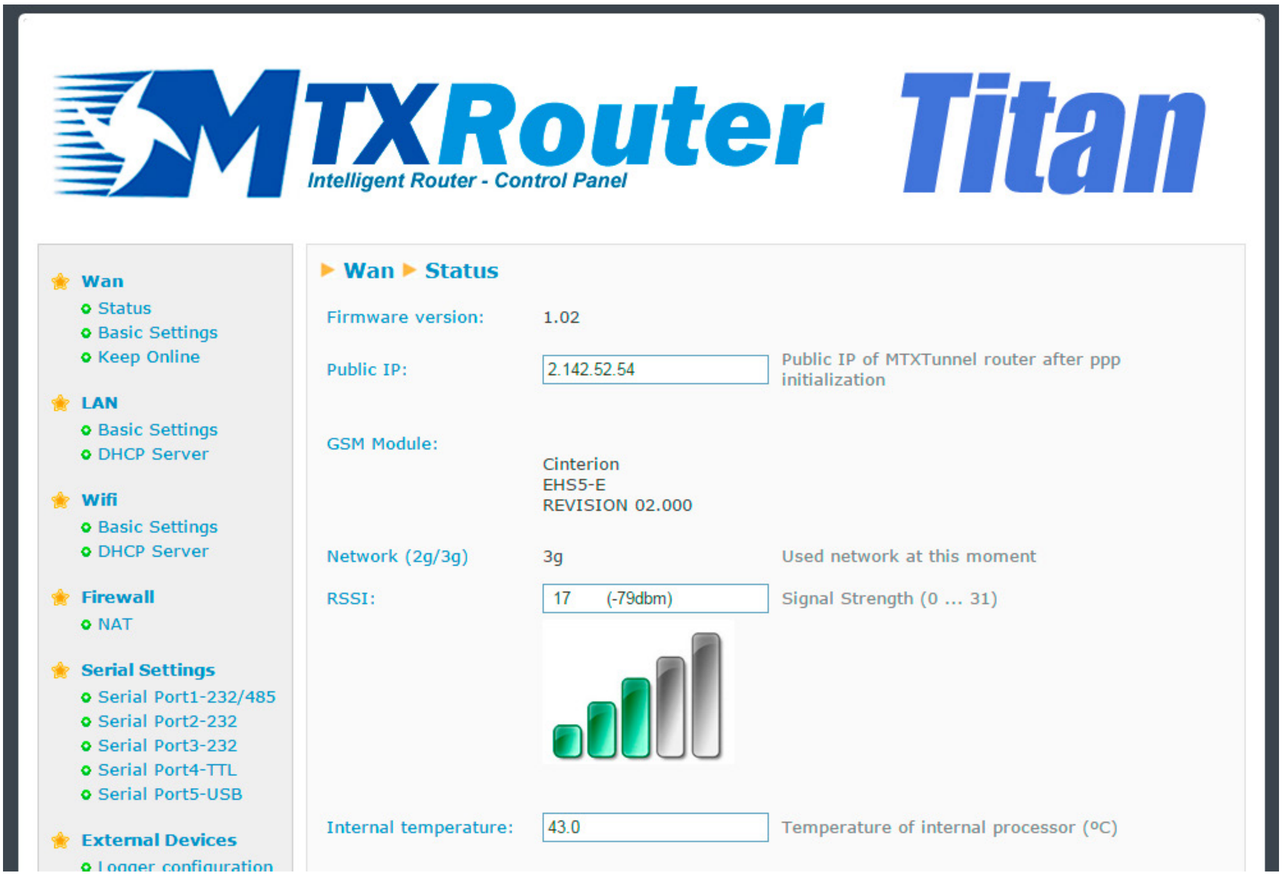
2.1 WAN

The WAN section refers to everything related to the 2G/3G route configuration, from the connection status, network configuration parameters and supervision of the connection.

2.1.1 WAN: Status

This screen shows the general status of the router.

- Public IP: WAN IP address (address of the GPRS/3G connection) if available
- GSM Module: indicates the manufacturer and the router's internal GSM module model
- Network (2G/3G): indicates if the current WAN connection is using 2G (GPRS) or 3G
- RSSI: indicates the signal strength. 0=none, 31=maximum
- Internal Temperature: shows the internal processor's temperature (it does not indicate the outside temperature. To find this out, a MTX-Temp-RS232 peripheral device can be connected to the router)



Firmware version: 1.02

Public IP: 2.142.52.54 — Public IP of MTXTunnel router after ppp initialization

GSM Module: Cinterion
EHS5-E
REVISION 02.000

Network (2g/3g) 3g — Used network at this moment

RSSI: 17 (-79dbm) — Signal Strength (0 ... 31)

Internal temperature: 43.0 — Temperature of internal processor (ºC)

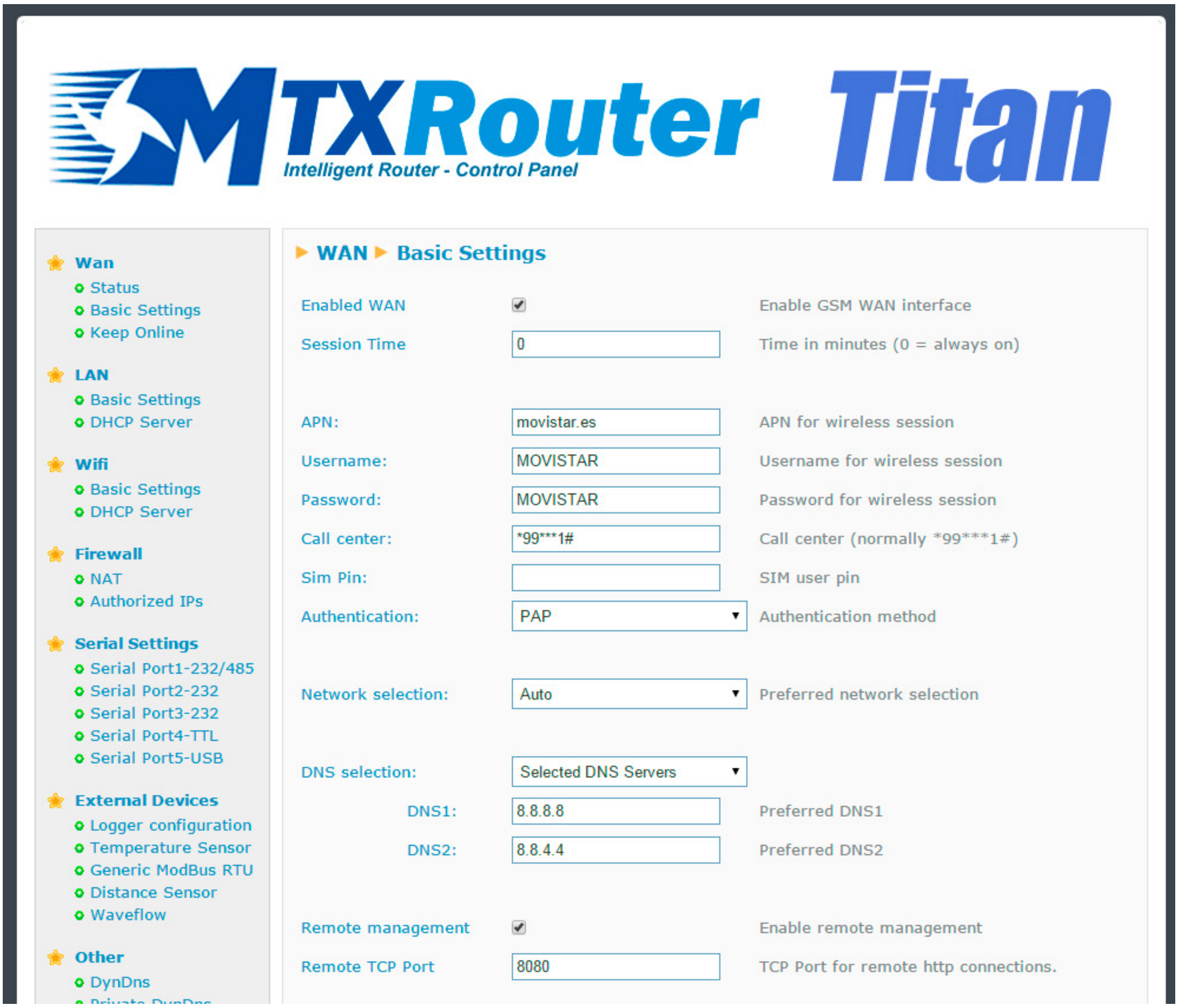
2.1.2 WAN: Basic Settings

This section assists with the configuration of the WAN (2G/3G) connection parameters. We will need to know certain information about the SIM card such as the APN, login and password. Our network provider should provide we with these.

Enabled WAN: select this to allow the MTX-Router-Titan to activate the 2G/3G device.

Session Time: indicates the time in minutes that the 2G/3G connection should be active. If the value is "0", it means that the connection is active all the time. If a value greater than 0 is specified, the number specifies the number of minutes during which the connection will be active following an event such as an SMS message being received or a missed call. Go to the configuration "Other > SMS Control" to activate and configure these events for when a number greater than 0 is specified.

- APN: operator APN. Consult our GSM provider for this.
- Username: operator Username. Consult our GSM provider for this
- Password: operator Password. Consult our GSM provider for this.
- Call center: call center number. Usually *99***1#
- SIM pin: if our SIM card has a PIN number, it should be specified here.
- Authentication: the method of authentication. Usually PAP
- Network selection:
  - auto: the router will use 3G when 3G coverage is available, and 2G in the event that there is no 3G coverage
  - 3G: the router will use 3G networks in every case. If there is no 3G coverage, it will not change to 2G
  - GPRS: the router will use 2G networks in all cases
- DNS1 and DNS2: DNS servers for domain name resolution. It is recommended that those belonging to Google (8.8.8.8 and 4.4.4.4) are used, or whatever our provider gives we
- Remote management: if activated, we will be able to access the router's web configuration remotely via the public IP address (indicated in WAN>Status)
- Remote TCP Port: indicates the TCP port for remote configuration. For example, if the value is 8080, the URL of the configuration will be http://x.x.x.x:8080. The standard default port is 80, but if we wish to use NAT to the TCP80 port in an ETH device (IP camera, PLC), we will need to change it, for example, to 8080



▶ WAN ▶ Basic Settings

Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP	Authentication method
Network selection:	Auto	Preferred network selection
DNS selection:	Selected DNS Servers	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	8080	TCP Port for remote http connections.

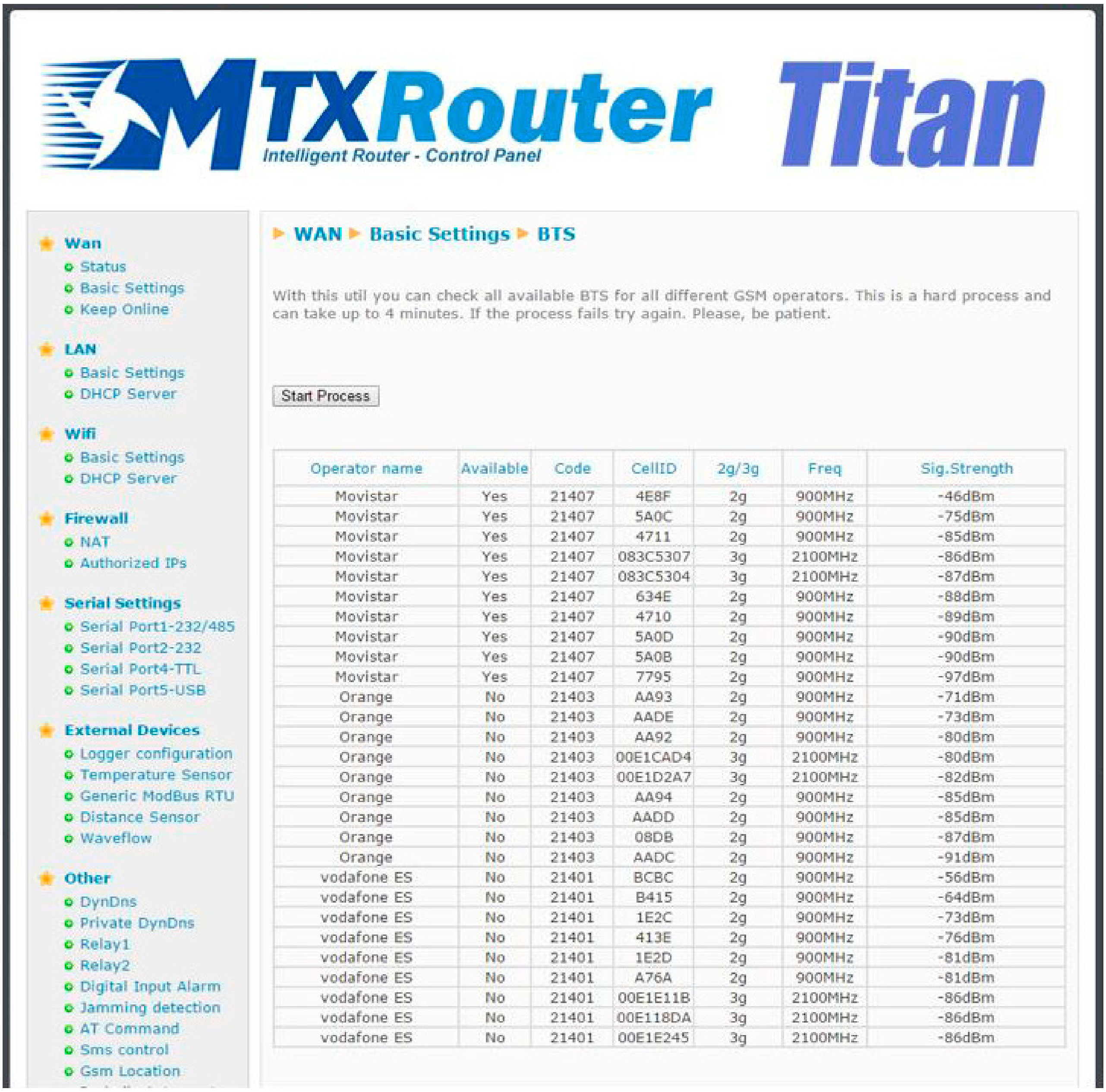
ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.

2.1.3 WAN: Basic Settings, Utilities

The utilities that we can find at the bottom of the “WAN > Basic Settings” screen allow we to select the main and secondary GSM operators when using a Global SIM card. (A Global SIM card allows we to connect to several network operators that are available. For example, in Spain, we would be able to connect to Movistar, Vodafone or Orange).

- Strong scanning: scans the GSM stations for all available network operators. This action uses a significant amount of processing power and therefore can take up to 4 minutes. On occasion, it may be necessary to try the process again. If successful, a list of the detected BTS will be shown, indicating the operator’s name, its code, its availability and the type of network (2G/3G). This could be very useful in helping we decide the best operator to use in a particular place.



▸ WAN ▸ Basic Settings ▸ BTS

With this util you can check all available BTS for all different GSM operators. This is a hard process and can take up to 4 minutes. If the process fails try again. Please, be patient.

Operator name	Available	Code	CellID	2g/3g	Freq	Sig.Strength
Movistar	Yes	21407	4E8F	2g	900MHz	-46dBm
Movistar	Yes	21407	5A0C	2g	900MHz	-75dBm
Movistar	Yes	21407	4711	2g	900MHz	-85dBm
Movistar	Yes	21407	083C5307	3g	2100MHz	-86dBm
Movistar	Yes	21407	083C5304	3g	2100MHz	-87dBm
Movistar	Yes	21407	634E	2g	900MHz	-88dBm
Movistar	Yes	21407	4710	2g	900MHz	-89dBm
Movistar	Yes	21407	5A0D	2g	900MHz	-90dBm
Movistar	Yes	21407	5A0B	2g	900MHz	-90dBm
Movistar	Yes	21407	7795	2g	900MHz	-97dBm
Orange	No	21403	AA93	2g	900MHz	-71dBm
Orange	No	21403	AADE	2g	900MHz	-73dBm
Orange	No	21403	AA92	2g	900MHz	-80dBm
Orange	No	21403	00E1CAD4	3g	2100MHz	-80dBm
Orange	No	21403	00E1D2A7	3g	2100MHz	-82dBm
Orange	No	21403	AA94	2g	900MHz	-85dBm
Orange	No	21403	AADD	2g	900MHz	-85dBm
Orange	No	21403	08DB	2g	900MHz	-87dBm
Orange	No	21403	AADC	2g	900MHz	-91dBm
vodafone ES	No	21401	BCBC	2g	900MHz	-56dBm
vodafone ES	No	21401	B415	2g	900MHz	-64dBm
vodafone ES	No	21401	1E2C	2g	900MHz	-73dBm
vodafone ES	No	21401	413E	2g	900MHz	-76dBm
vodafone ES	No	21401	1E2D	2g	900MHz	-81dBm
vodafone ES	No	21401	A76A	2g	900MHz	-81dBm
vodafone ES	No	21401	00E1E11B	3g	2100MHz	-86dBm
vodafone ES	No	21401	00E118DA	3g	2100MHz	-86dBm
vodafone ES	No	21401	00E1E245	3g	2100MHz	-86dBm

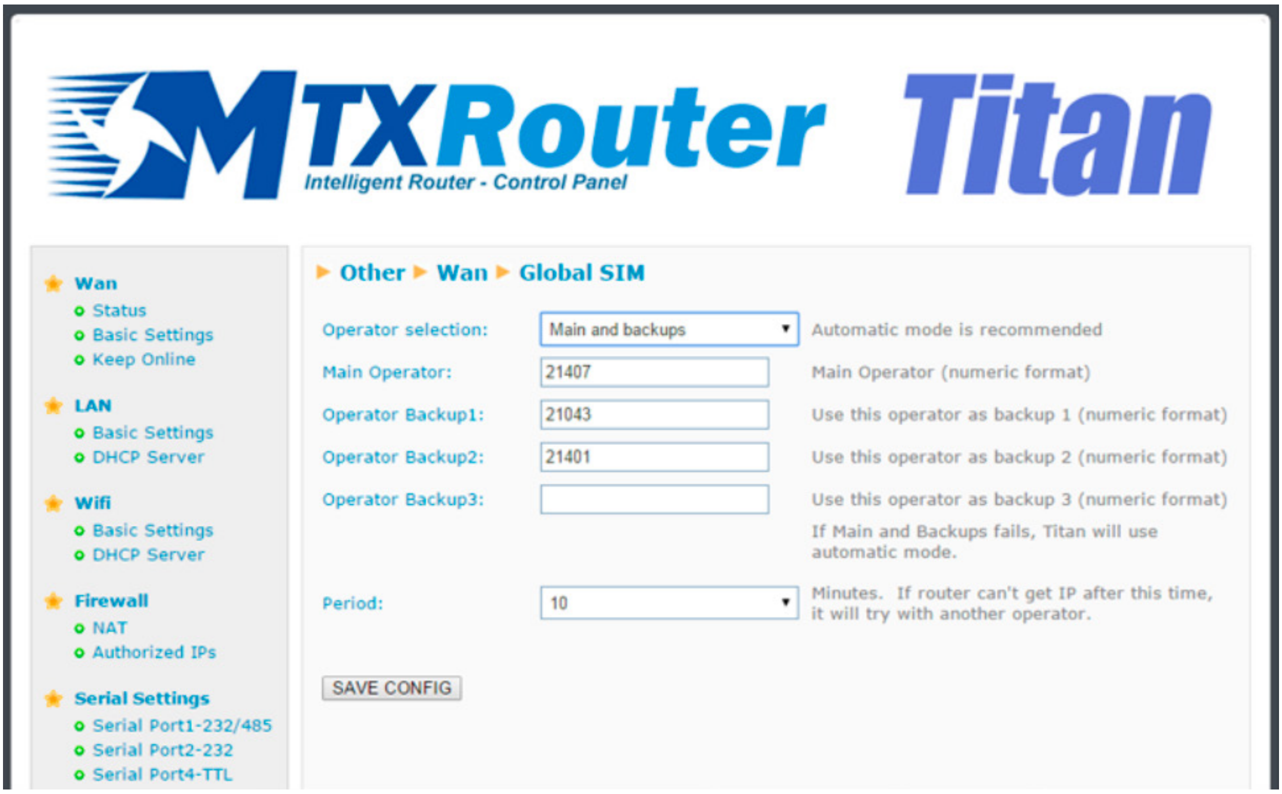
With Strong Scanning, 3G connectivity is lost during the process and therefore we recommend using the Ethernet interface to carry this out. Because of this, “Strong Scanning” has two buttons – “start process from Ethernet” and “Start process from 3G”.

If the process is carried out using Ethernet, press this button and the results will be shown on screen once finished.

If the process is carried out using 3G, press this button and after five minutes, the device will reset itself. We will have to return to the screen manually and press the “See last results” button in order to see the results.

- Light scanning: this carries out a similar process, but only those operators that are available for our SIM card are identified. 3G connectivity is not lost during the process, which could last up to 2 minutes, meaning that it is ideal when carried out remotely via 3G.

- Choose operators: this allows we to choose the GSM operator and the secondary operators. It can only be used when a Global SIM (allowing connections to several operators) is inserted. The default setting is “Automatic”.



Other ▸ Wan ▸ Global SIM

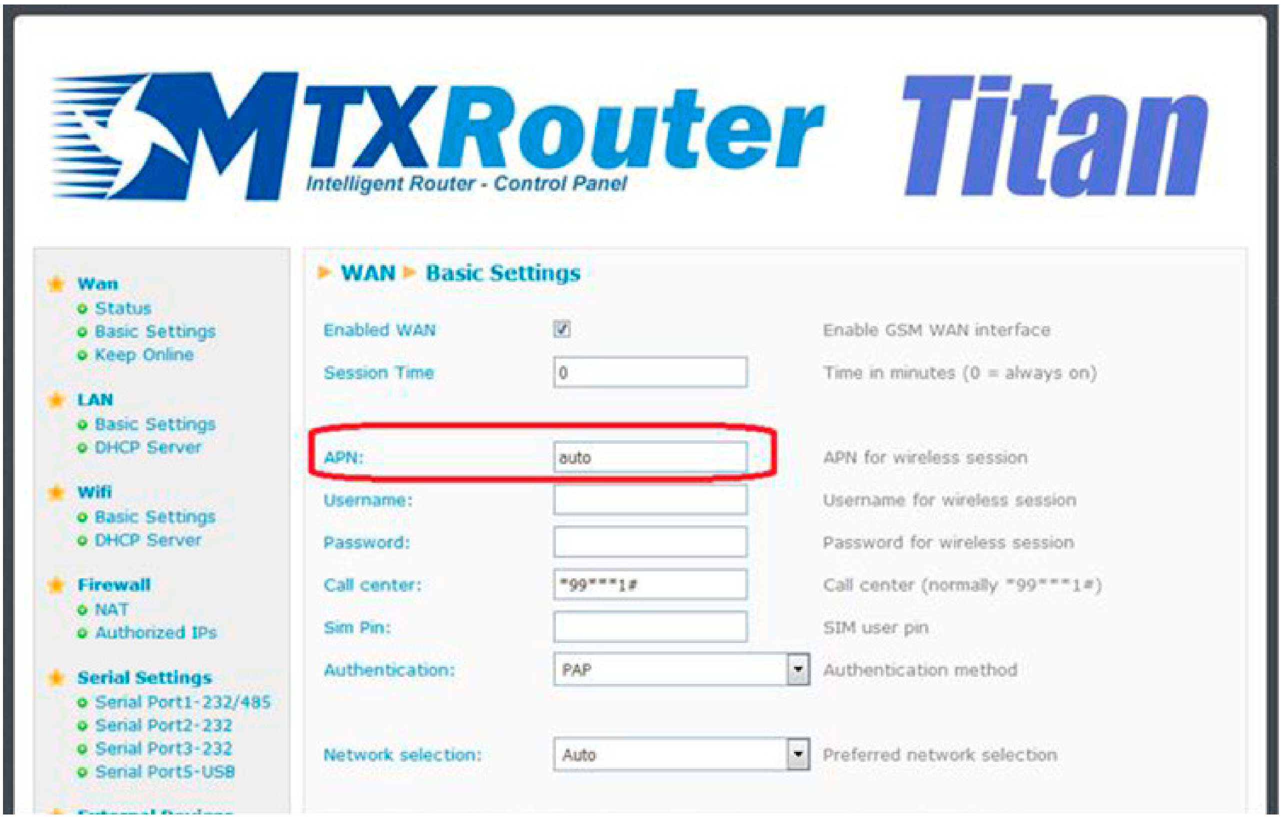
Operator selection:	Main and backups	Automatic mode is recommended
Main Operator:	21407	Main Operator (numeric format)
Operator Backup1:	21043	Use this operator as backup 1 (numeric format)
Operator Backup2:	21401	Use this operator as backup 2 (numeric format)
Operator Backup3:		Use this operator as backup 3 (numeric format) If Main and Backups fails, Titan will use automatic mode.
Period:	10	Minutes. If router can't get IP after this time, it will try with another operator.

Example contained in the screenshot above. We choose the “Main and Backups” option, which forces the indicated GSM operators to be used. The main operator is 21407 (Movistar). If an IP address is not obtained using this network, the process is retried using operator 21043 (Orange), and if this fails, it tries again with operator 21401 (Vodafone). If the third network operator also fails, the router will try to connect to a GSM network automatically.

If we select the “Automatic” option instead of “Main and Backups”, the router will try to select the operator in the order that is stablished in the SIM card’s internal tables. Except for in locations prone to connectivity problems, we recommend we use the “Automatic” option.

The section Wan > Basic Settings > Utils is not available for 4G models.

- Automatic APN: This new feature will work when we enter the text “auto” in the “APN” field. That is, as indicated in the following figure:

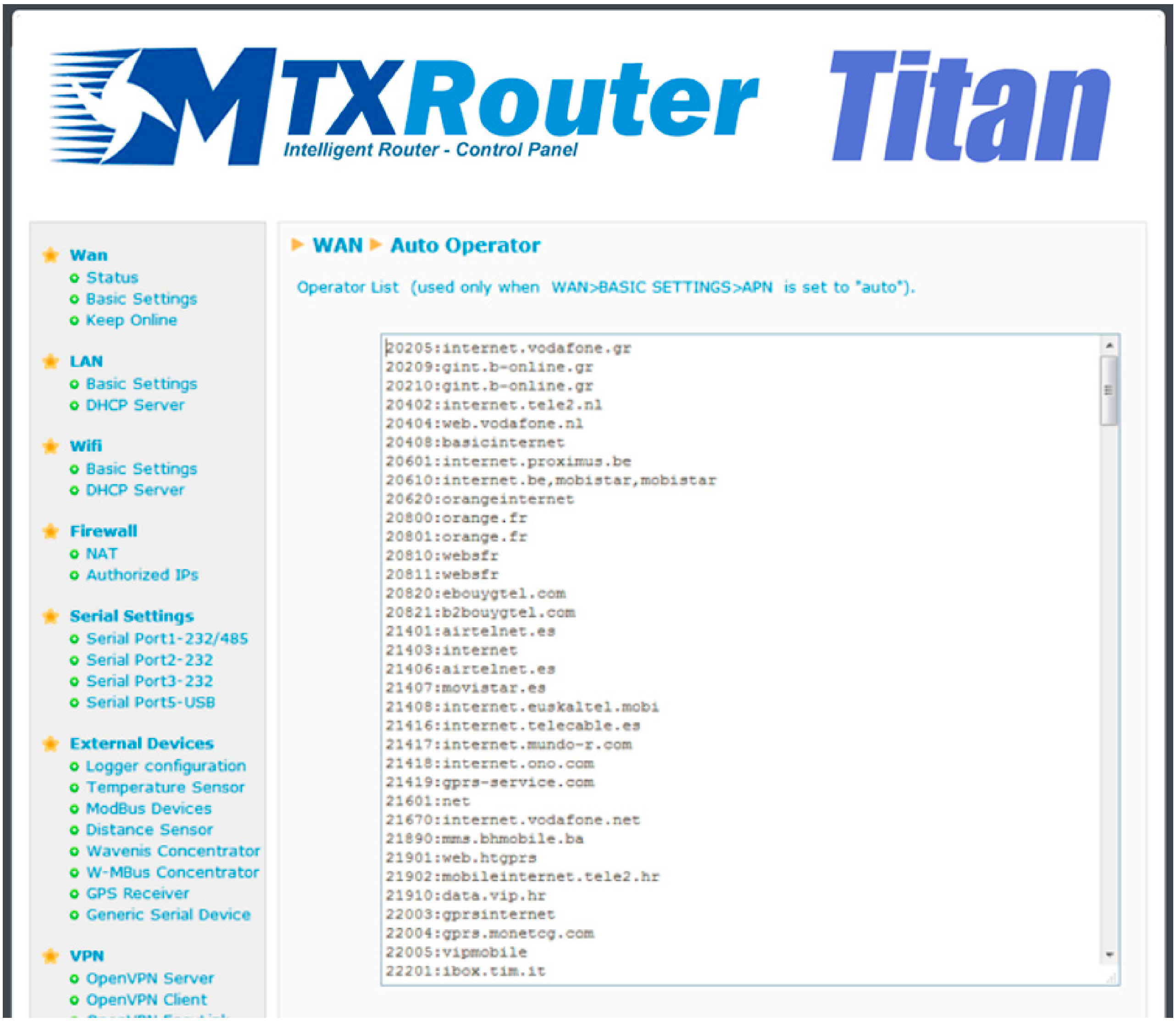


WAN ▸ Basic Settings

Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	auto	APN for wireless session
Username:		Username for wireless session
Password:		Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP	Authentication method
Network selection:	Auto	Preferred network selection

When “auto” is specified in the APN field, the Titan router will not use the APN, Username and Password fields in this section, instead, it will look up in the table (which can be consulted by pressing the “Automatic APN “) The appropriate APN, Username and Passwords. This is particularly useful if we intend to send the router to a third party and only have to insert the SIM without configuring anything else.

Although the list of operators has a considerable number of data (apn, username, password) it is strongly recommended to review the list and update it with the desired operators.



WAN ▶ Auto Operator

Operator List (used only when WAN>BASIC SETTINGS>APN is set to "auto").

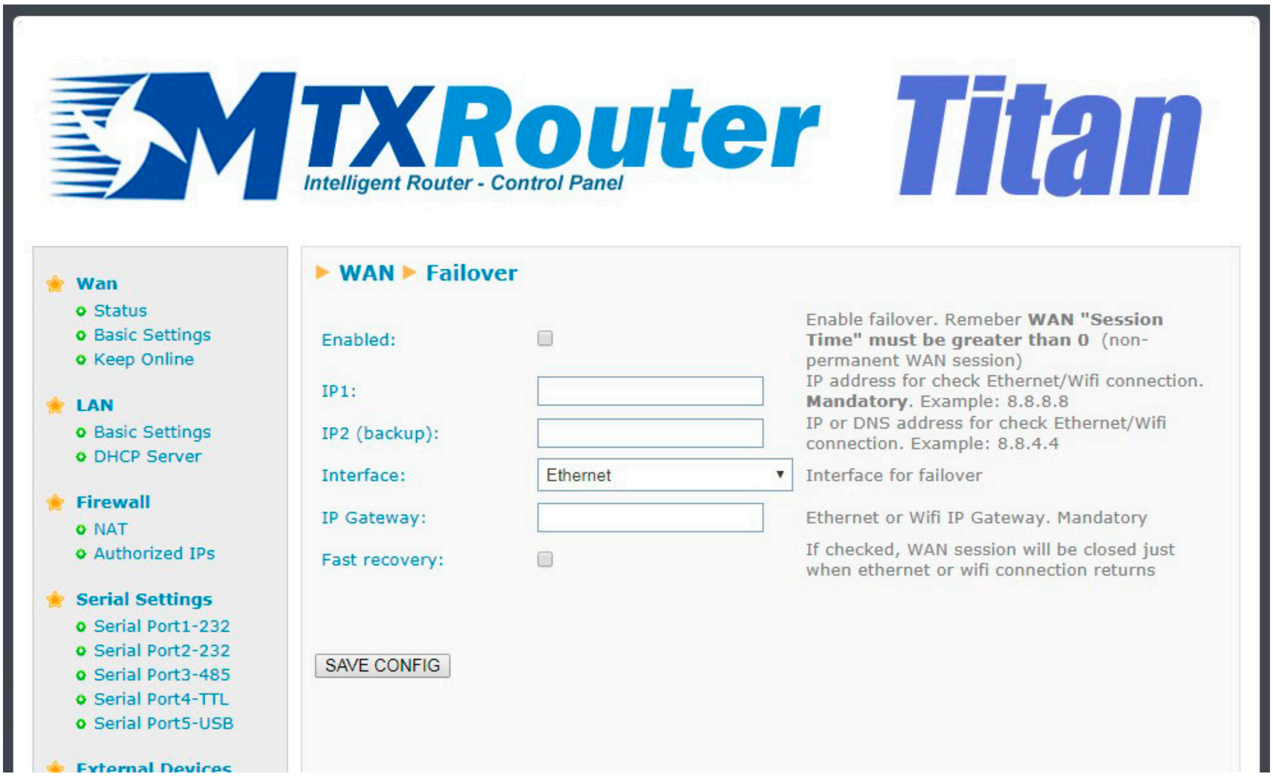
```
20205:internet.vodafone.gr
20209:gint.b-online.gr
20210:gint.b-online.gr
20402:internet.tele2.nl
20404:web.vodafone.nl
20408:basicinternet
20601:internet.proximus.be
20610:internet.be,mobistar,mobistar
20620:orangeinternet
20800:orange.fr
20801:orange.fr
20810:websfr
20811:websfr
20820:ebouygtel.com
20821:b2bouygtel.com
21401:airtelnet.es
21403:internet
21406:airtelnet.es
21407:movistar.es
21408:internet.euskaltel.mobi
21416:internet.telecable.es
21417:internet.mundo-r.com
21418:internet.ono.com
21419:gprs-service.com
21601:net
21670:internet.vodafone.net
21890:mms.bhmobile.ba
21901:web.htgprs
21902:mobileinternet.tele2.hr
21910:data.vip.hr
22003:gprsinternet
22004:gprs.monetcg.com
22005:vipmobile
22201:ibox.tim.it
```

The format of the file is very simple:

codigoSim: apn, username, password

The username and password only need to be indicated in those operators that actually use them, not being necessary otherwise.

Failover: in case we are using the Ethernet interface or the Titan router WiFi as an Internet output and it fails, we can configure this section so the Titan router automatically connects to the Internet via 2G/3G/4G.



▶ WAN ▶ Failover

Enabled:	□	Enable failover. Remeber **WAN "Session Time" must be greater than 0** (non-permanent WAN session)
IP1:		IP address for check Ethernet/Wifi connection. **Mandatory**. Example: 8.8.8.8
IP2 (backup):		IP or DNS address for check Ethernet/Wifi connection. Example: 8.8.4.4
Interface:	Ethernet	Interface for failover
IP Gateway:		Ethernet or Wifi IP Gateway. Mandatory
Fast recovery:	□	If checked, WAN session will be closed just when ethernet or wifi connection returns

- Enabled: activate this box to enable the Failover
- IP1: IP address for the periodic ping by the used interface (Ethernet or WiFi) to make sure the communications are working
- IP2: backup IP address for the periodic ping by the used interface (Ethernet or WiFi) to make sure the communications are working
- Interface: specify the interface being used to access the Internet (Ethernet or WiFi)
- IP gateway: specify the output gateway IP address used for the Ethernet or WiFi connection
- Fast recovery: select this box in case we want the 2G/3G/4G connection to end when the Ethernet or WiFi connection is restored. Otherwise it will be connected the amount of time specified in WAN > Basic Settings > Session Time

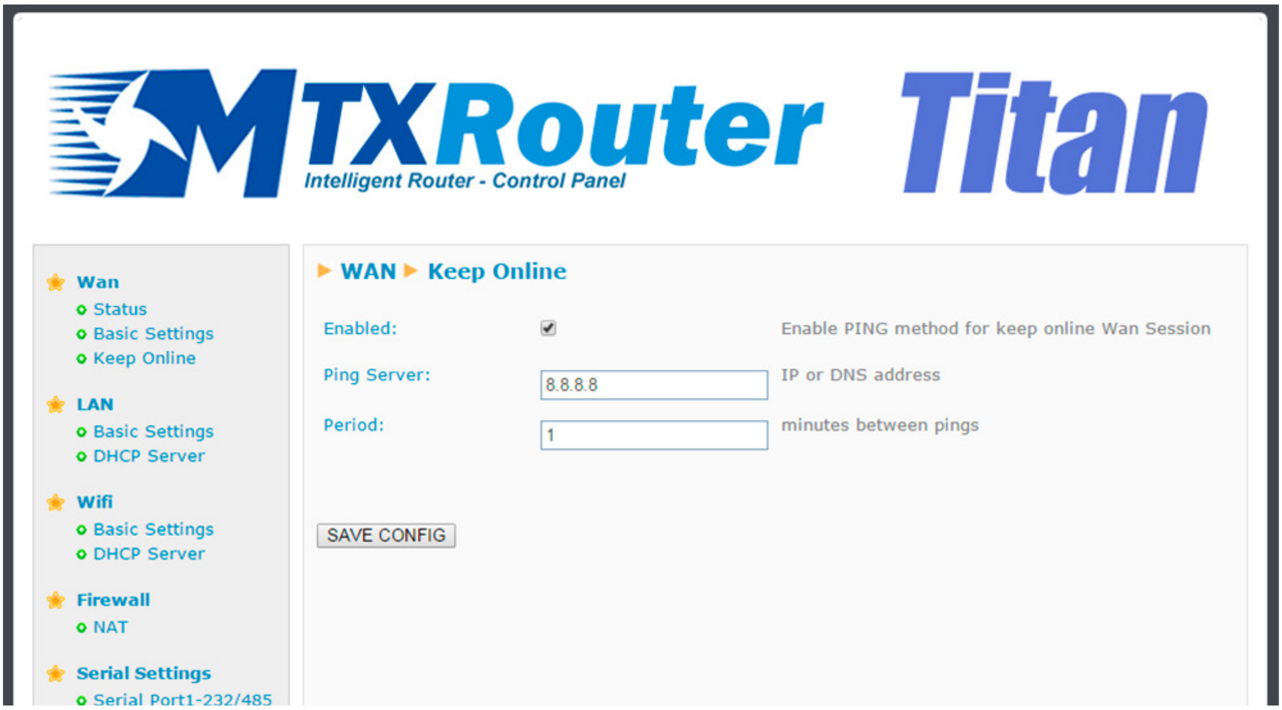
Important: in case we use the Failover feature we need to make sure to enable the box “WAN > Basic Settings > Enabled WAN” and to enter a value > 0 in the field “WAN > Basic Settings > Session Time.” That value will be the minutes the 2G/3G/4G connection will be enabled in case there is a problem with the Ethernet or WiFi interface.

2.1.4 WAN: Keep Online

On this screen we can configure a PING to ensure the router’s connectivity. If the PING fails on three occasions, the 2G/3G connection will be reset. We recommend the use of this characteristic.

- Enabled: activate to allow the Titan to periodically send a PING to check the connectivity

- Ping Server: indicates the server's IP address where the PING should be sent
- Period: indicates how frequently a PING should be sent



WAN ▶ Keep Online

Enabled: ☑ Enable PING method for keep online Wan Session

Ping Server: 8.8.8.8 IP or DNS address

Period: 1 minutes between pings

ADDITIONAL NOTES

- Once the configuration is finished, click "SAVE CONFIG" to save the changes. Remember that the router should be restarted for the changes to take effect

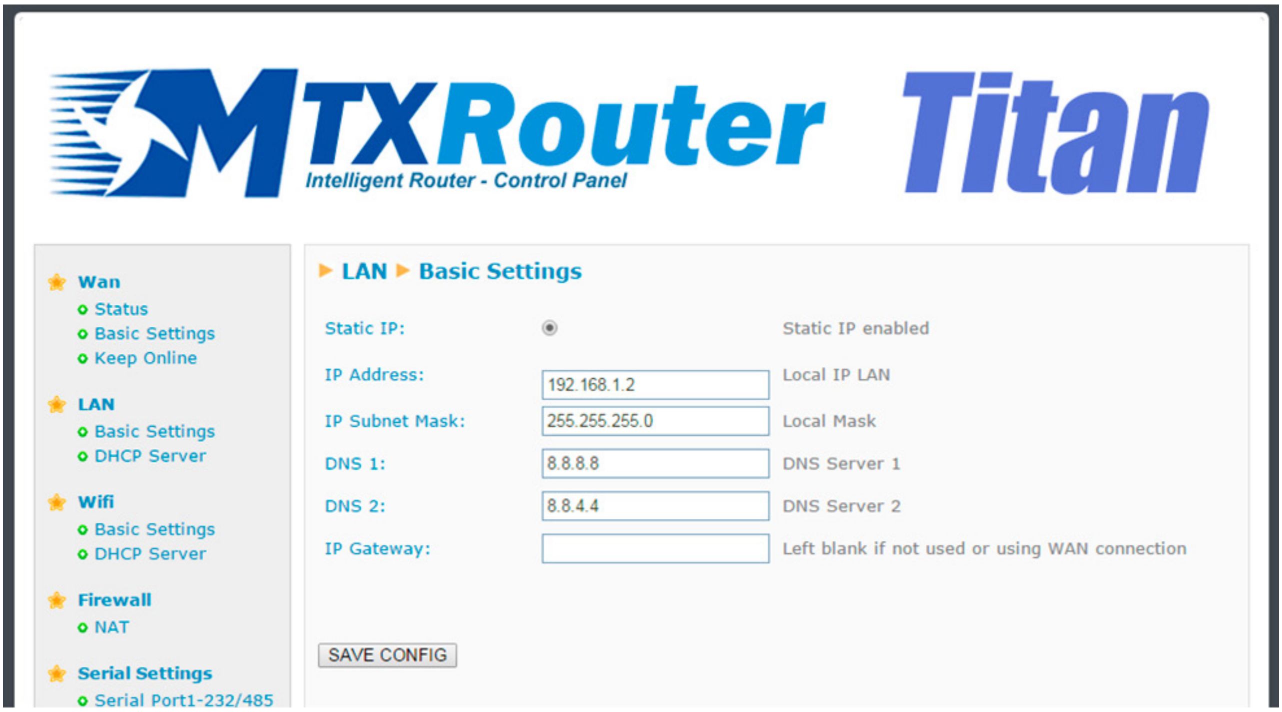
2.2 LAN

The "LAN" configuration section refers to the Ethernet configuration.

2.2.1 LAN: Basic Settings

This section allows we to configure the basic network parameters for an Ethernet connection.

- Static IP: a static IP address will be assigned
- IP address: a local IP address of the Ethernet interface (by default 192.168.1.2)
- IP subnet mask: subnet mask
- DNS1: main DNS server
- DNS2: secondary DNS server
- IP gateway: leave blank if we want to use 2G/3G networks. Useful to provide Internet connectivity to WiFi devices redirecting the output towards an ADSL router IP address instead of via 2G/3G



▸ LAN ▸ Basic Settings

Static IP:	●	Static IP enabled
IP Address:	192.168.1.2	Local IP LAN
IP Subnet Mask:	255.255.255.0	Local Mask
DNS 1:	8.8.8.8	DNS Server 1
DNS 2:	8.8.4.4	DNS Server 2
IP Gateway:		Left blank if not used or using WAN connection

SAVE CONFIG

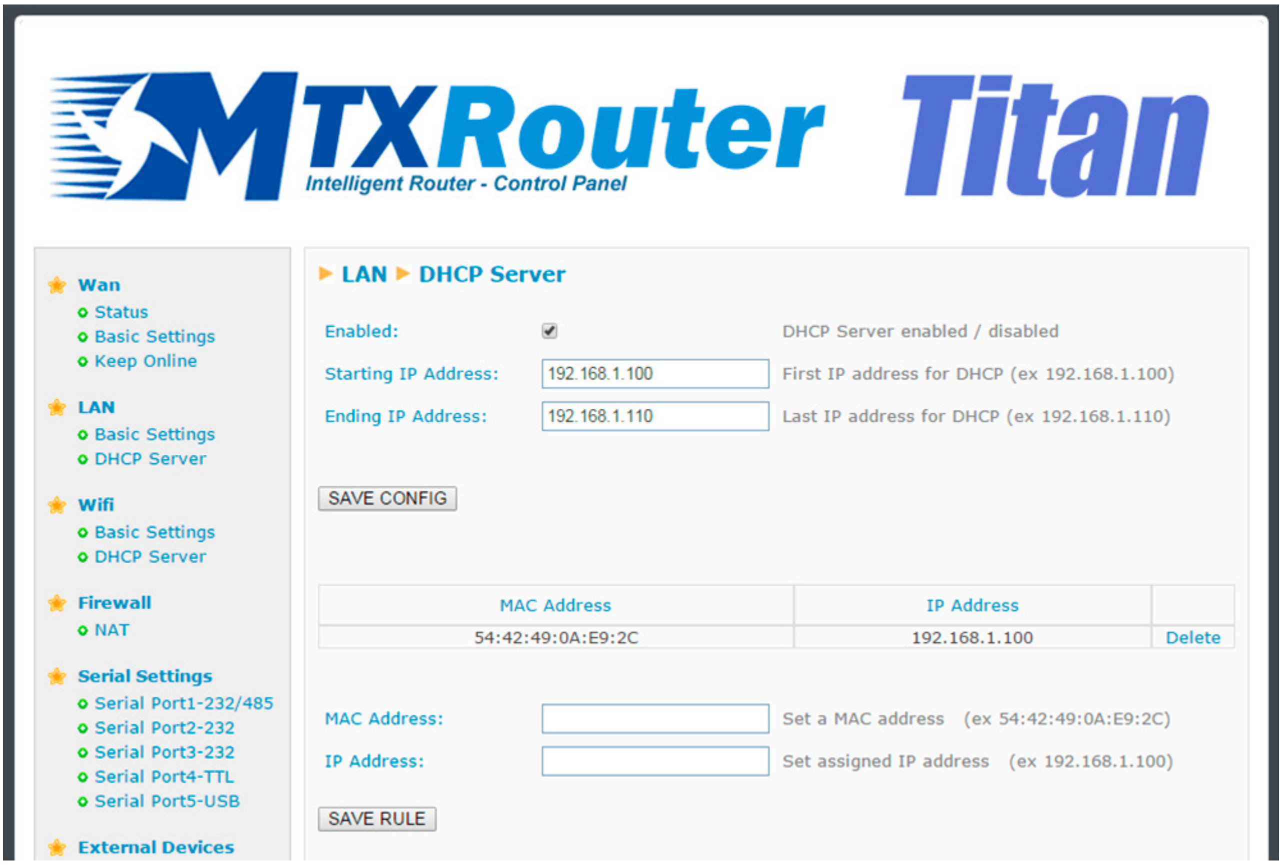
ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.

2.2.2 LAN: DHCP Server

This section shows we how to enable and configure the DHCP server assigned to the router’s Ethernet interface.

- Enabled: if activated, the DHCP server of the Ethernet interface is activated
- Starting IP Address: indicates the first IP address that the DHCP server will assign
- Ending IP Address: indicates the last IP address that the DHCP server will assign
- MAC Address/IP Address: these two parameters allows the DHCP server to assign the same IP address to a specific MAC address



▶ LAN ▶ DHCP Server

Enabled: ☑ DHCP Server enabled / disabled

Starting IP Address: 192.168.1.100 First IP address for DHCP (ex 192.168.1.100)

Ending IP Address: 192.168.1.110 Last IP address for DHCP (ex 192.168.1.110)

MAC Address	IP Address	
54:42:49:0A:E9:2C	192.168.1.100	Delete

MAC Address: Set a MAC address (ex 54:42:49:0A:E9:2C)

IP Address: Set assigned IP address (ex 192.168.1.100)

ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Click “SAVE RULE” for each MAC/IP pairing that we wish to create. Up to 10 can be created.
- Remember that the router should be restarted for the changes to take effect.

2.3 WiFi

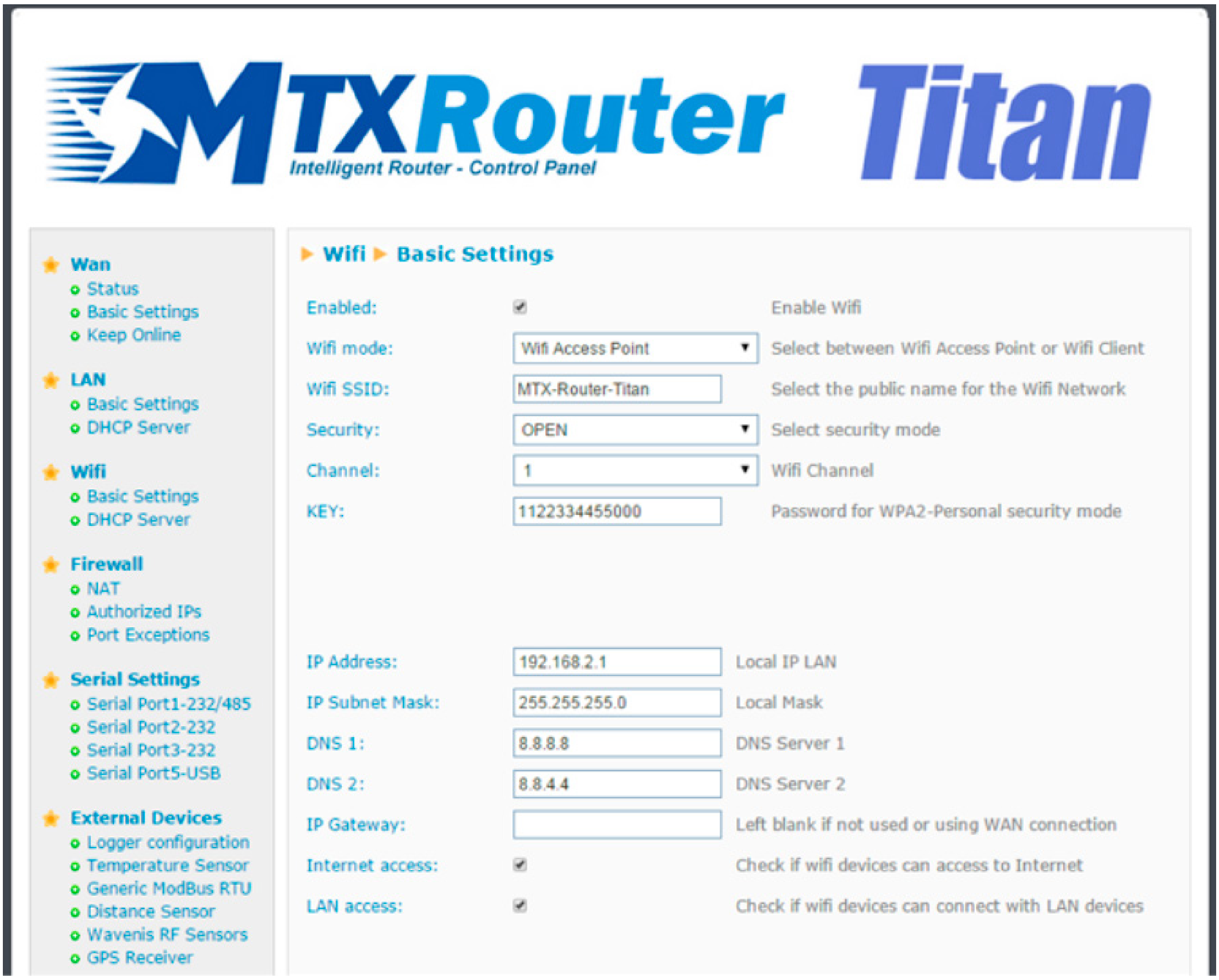
The “WiFi” configuration section refers to the WiFi network configuration. By using a WiFi connection, we can provide WiFi enabled devices with access to the Internet.

2.3.1 WiFi: Basic Settings

This section explains the basic configuration parameters for a WiFi connection.

- Enabled: This parameter activates the WiFi interface for the Titan router
- WiFi mode: this parameter allows we to select either “WiFi Access Point” or “WiFi Client” as the work mode. “WiFi Access Point” is recommended if we wish to use the Titan router to provide Internet access to WiFi enabled devices using 3G. “WiFi Client” is recommended if we wish to use an existing WiFi infrastructure (for example, the company’s ADSL/cable connection) to provide Internet access

- WiFi SSID: public SSID (in "WiFi Access Point" mode this indicates the SSID created by the Titan router; in "WiFi Client" mode this indicates the SSID that the Titan router will connect to)
- Security: this parameter allows we to specify the WiFi security mode. WPA2 is recommended
- KEY: this parameter specifies the WiFi password that is necessary for WPA2 mode
- IP Mode: in "WiFi Client" mode this specifies if a local static IP address is to be used or whether the IP address should be taken using DHCP
- IP Address: this parameter indicates the IP address for the WiFi interface. The default value is 192.168.2.1
- Subnet mask: this parameter indicates the subnet mask for the WiFi interface
- DNS1: this parameter indicates the main DNS server
- DNS2: this parameter indicates the secondary DNS server
- IP Gateway: in "WiFi client" mode, this parameter allows we to specify the gateway to be used when the local IP address is static
- Internet access: this parameter should be activated in order to connect to the Internet from a WiFi enabled device
- LAN access: this parameter should be activated in order to connect to devices connected to the router's Ethernet port from a WiFi device



▶ Wifi ▶ Basic Settings

Enabled:	☑	Enable Wifi
Wifi mode:	Wifi Access Point ▾	Select between Wifi Access Point or Wifi Client
Wifi SSID:	MTX-Router-Titan	Select the public name for the Wifi Network
Security:	OPEN ▾	Select security mode
Channel:	1 ▾	Wifi Channel
KEY:	1122334455000	Password for WPA2-Personal security mode
IP Address:	192.168.2.1	Local IP LAN
IP Subnet Mask:	255.255.255.0	Local Mask
DNS 1:	8.8.8.8	DNS Server 1
DNS 2:	8.8.4.4	DNS Server 2
IP Gateway:		Left blank if not used or using WAN connection
Internet access:	☑	Check if wifi devices can access to Internet
LAN access:	☑	Check if wifi devices can connect with LAN devices

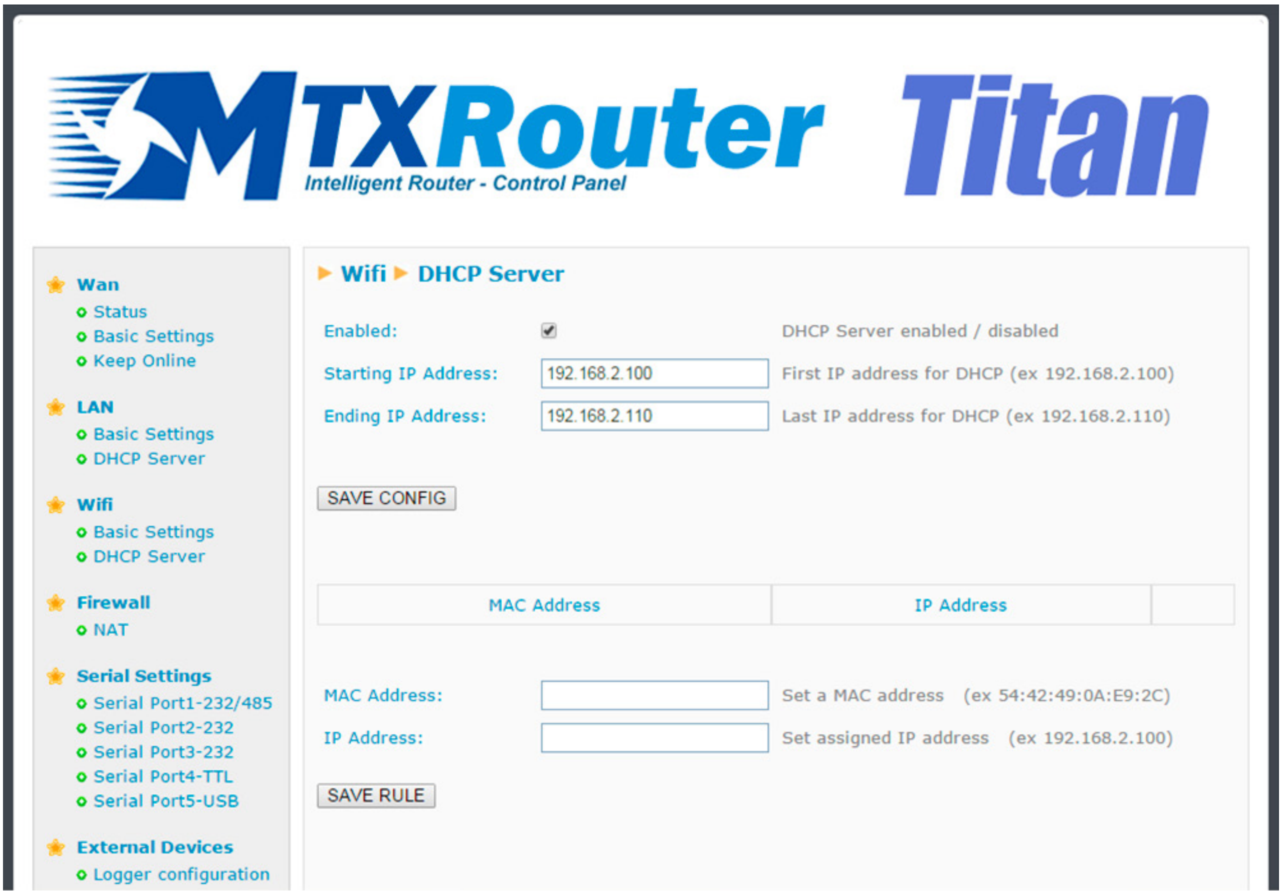
ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.

2.3.2 WiFi: DHCP Server

In this section we see how to enable and configure the DHCP server assigned to the router’s WiFi interface.

- Enabled: if selected, the DHCP server belonging to the Ethernet interface will be activated
- Starting IP address: indicates the first IP address that the DHCP server will assign
- Ending IP address: indicates the last IP address that the DHCP server will assign
- MAC address/IP address: these two parameters allow the DHCP server to always assign the same IP address to a particular MAC address



▶ Wifi ▶ DHCP Server

Enabled:	☑	DHCP Server enabled / disabled
Starting IP Address:	192.168.2.100	First IP address for DHCP (ex 192.168.2.100)
Ending IP Address:	192.168.2.110	Last IP address for DHCP (ex 192.168.2.110)

MAC Address	IP Address	

MAC Address:		Set a MAC address (ex 54:42:49:0A:E9:2C)
IP Address:		Set assigned IP address (ex 192.168.2.100)

ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Click “SAVE RULE” for each MAC/IP pairing that we wish to create. Up to 10 can be created.
- Remember that the router should be restarted for the changes to take effect.

2.4 Firewall

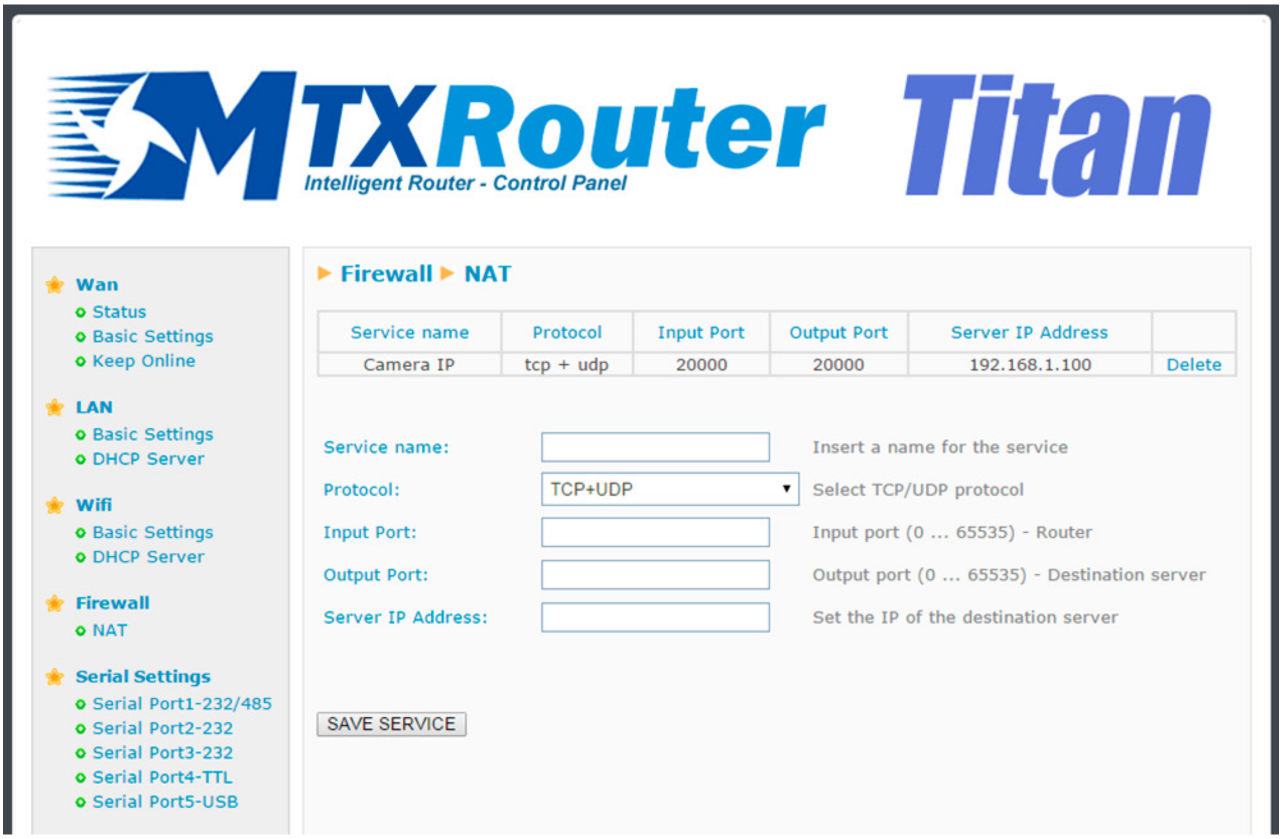
Section to configure the security aspects of the router.

2.4.1 Firewall: NAT

This section will outline from where we can map ports to access, from external devices, internal devices that are connected to the router. For example, if there is an IP camera connected to the MTX-Router-Titan-3G’s Ethernet port and we wish to have access from an outside computer, we should configure this section appropriately. We can create up to 10 rules.

- Service name: name to describe the mapping rule
- Protocol: indicates the protocol for port mapping. TCP, UDP or both
- Input port: indicates the “listening” port for the MTX-Router-Titan-3G device

- Output port: indicates the “listening” port of the device that is connected to the MTX-Router-Titan-3G which we wish to control externally; i.e. the data received in the router’s “input port” are redirected to the internal “output port”
- Server IP address: IP address of the device to be controlled externally (for example, the camera’s IP address)



▶ Firewall ▶ NAT

Service name	Protocol	Input Port	Output Port	Server IP Address	
Camera IP	tcp + udp	20000	20000	192.168.1.100	Delete

Service name: Insert a name for the service

Protocol: TCP+UDP Select TCP/UDP protocol

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

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

Server IP Address: Set the IP of the destination server

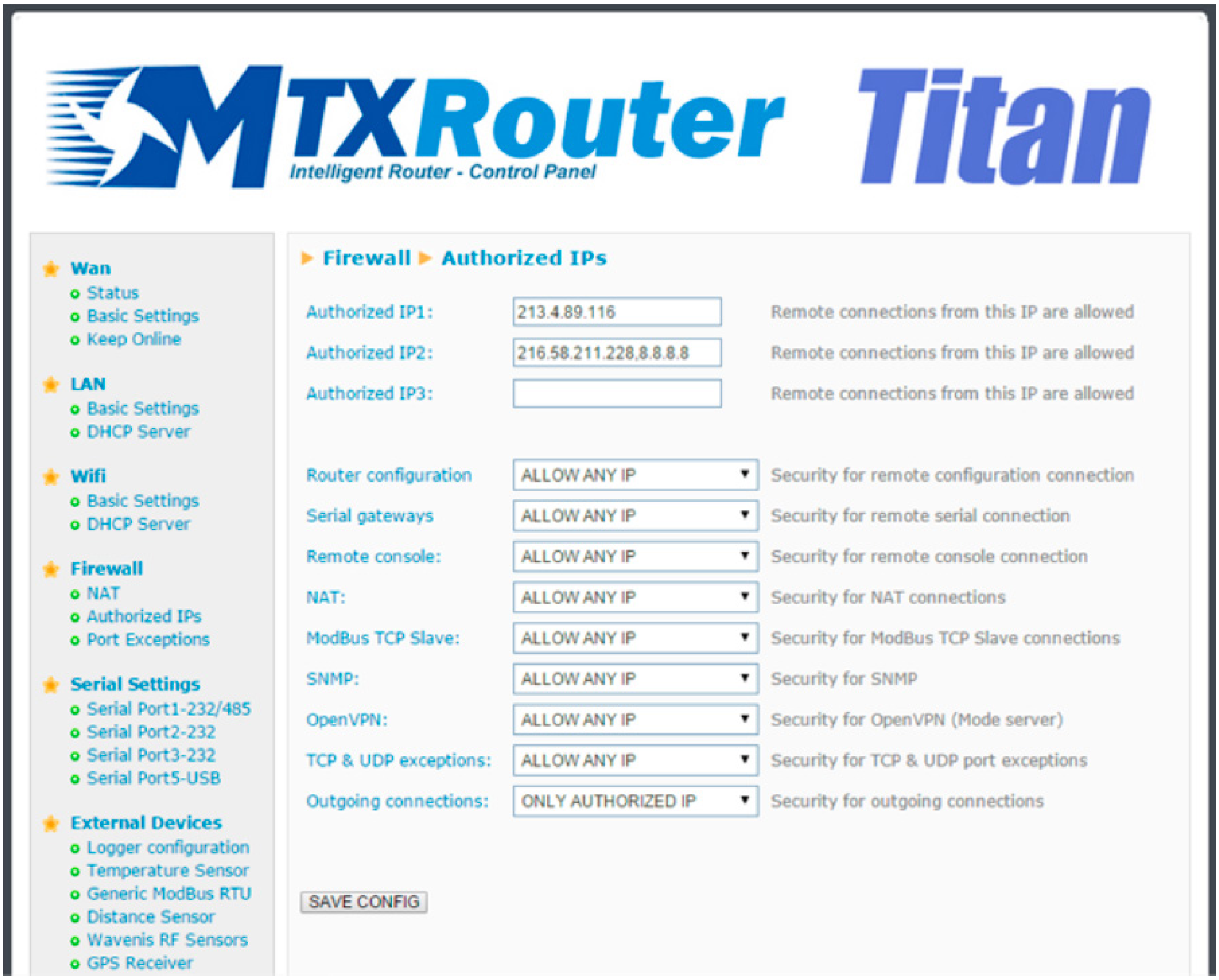
ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.
- Also remember that to create a NAT correctly:
  1. The LAN IP address of the device to be controlled should be within the network range of the LAN IP address of the MTX-Router-Titan II, MTX-Router-Titan device or the MTX-Router-Titan mini device.
  2. The Gateway IP address of the device to be controlled should be the LAN IP address of the MTX-Router-Titan II, MTX-Router-Titan device or the MTX-Router-Titan mini device. Consult the examples contained in the Annex for more information.

2.4.2 Firewall: Authorized IPs

This screen allows we to define, if we wish to, up to three authorized IP addresses to create WAN connections (using a 3G interface) in the different router services. For example, if we specify as an authorized IP address 90.166.108.200 (the office IP address), it will only be possible to access certain services from this IP address.

- Authorized IP1: frst authorized IP address
- Authorized IP2: second authorized IP address
- Authorized IP3: third authorized IP address
- Router configuration: specifies if remote connections to the web configuration environment of the 485 router will be from any IP address or only from those that have been authorized
- Serial gateways: specifies if remote connections to 3G-RS232/485 gateway services will be accepted from any IP address or only from those that have been authorized
- Remote console: specifies if remote connections to remote control services will be accepted from any IP address or only from those that have been authorized
- NAT: specifies if remote connections to the router's mapped ports will be accepted from any IP address or only from those that have been authorized
- ModBus TCP slave: specifies whether remote connections to the Titan router's Modbus TCP Slave are accepted from any IP address or only authorized IP addresses
- SNMP: specifies whether remote connections to the Titan router's SNMP service are accepted from any IP address or only authorized IP addresses
- OpenVPN: specifies whether remote connections to the Titan router's "OpenVPN Server" service are accepted from any IP address or only authorized IP addresses
- Outgoing Connections: This allows the user to specify whether Internet Access can be provided to all IP addresses or only authorized IP addresses. For example, if we only want those Ethernet or WiFi devices that are connected to the Titan router to be able to send data to the server, this would restrict unauthorized use for any other activity (Internet browsing, etc.)



▶ Firewall ▶ Authorized IPs

Authorized IP1:	213.4.89.116	Remote connections from this IP are allowed
Authorized IP2:	216.58.211.228,8.8.8.8	Remote connections from this IP are allowed
Authorized IP3:		Remote connections from this IP are allowed
Router configuration	ALLOW ANY IP	Security for remote configuration connection
Serial gateways	ALLOW ANY IP	Security for remote serial connection
Remote console:	ALLOW ANY IP	Security for remote console connection
NAT:	ALLOW ANY IP	Security for NAT connections
ModBus TCP Slave:	ALLOW ANY IP	Security for ModBus TCP Slave connections
SNMP:	ALLOW ANY IP	Security for SNMP
OpenVPN:	ALLOW ANY IP	Security for OpenVPN (Mode server)
TCP & UDP exceptions:	ALLOW ANY IP	Security for TCP & UDP port exceptions
Outgoing connections:	ONLY AUTHORIZED IP	Security for outgoing connections

ADDITIONAL NOTES

- Once the configuration is finished, click "SAVE CONFIG" to save the changes. Remember that the router should be restarted for the changes to take effect.
- The IP restrictions are only for 3G connections. WiFi access remains protected by the WPA2 password. Therefore, if we have WiFi and require security, activate WPA2 in the section WiFi > Basic Settings.
- If the "Outgoing connections" restriction is used, remember that the DNS server's IP address must be specified if domain names are used instead of IP addresses.
- If we need to authorize more than three IP addresses, we can specify more than one IP address in any box, separating them using a comma, as shown in the previous example.

2.5 Serial Settings: Serial portX

The MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices have several serial ports and USB. Using these, we can create serial/3G, USB/3G or serial/CSD gateways to remotely control serial devices. The number of RS232 or RS485 serial ports will depend on the MTX-Router-Titan model used.

- Baudrate: specifies the serial port velocity (115200, … , 300)
- Data bits: specifies the number of data bits (7, 8)
- Parity: specifies the parity (none, even [par], odd [impar])
- Stop bits: specifies the number of stop bits (1, 2)
- Flow control: specifies the flow control (none, hardware)
- Timeout ms: indicates the time (in milliseconds) that the device must wait without receiving data in its serial port before sending the data via IP. If a value of "0" is specifies (the default value), the data will be sent as they arrive in the serial port. A value of 10 for example means that the data will not be sent until 10ms have passed without receiving serial ports. This allows the data to be received at the destination less fragmentated
- Allow embedded AT commands: by selecting this check box, embedded AT commands can be sent in a 3G-Serial gateway in either Server or Client mode. The AT commands must be sent between the tags <MTXTUNNELR> and </MTXTUNNELR>. For example, if we want to obtain the network coverage, the following command can be sent: <MTXTUNNELR>AT+CSQ</MTXTUNNELR>, or if we wish to remotely reset a device, we can send the following command: <MTXTUNNELR>AT^MTXTUNNEL=REBOOT </MTXTUNNELR>
- Allow incoming GSM calls (CSD Data Call): by selecting this option, we accept CSD calls via serial ports. This is only valid to work when the port is configured as a gateway of the TCP Server or TCP Client type, and when the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini device is configured to work in 2G mode. When a CSD call is received and accepted, the 2G connection is suspended until the call ends. Only one serial port can be specified with this option. Useful for metering applications. Consult the examples in the Annex for a better understanding. This option (CSD data call) is not available for 3G models with GPS or 4G models
- Function: nothing or used by external device. Select this option if we do not wish to use a specific serial port (such as IP/serial gateway) or if we do not want the port to be used by an external device specified in the configuration section "External Devices". For example, if we wish to use a temperature sensor, a distance sensor or any other device specified in the "External Devices" section, we must select this option
- Function: serial-IP gateway (TCP Server). Select this option if we wish to create a Serial-3G/2G transparent gateway in TCP server mode; i.e. a scenario in which the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini device is listening in a specific TCP port for a connection to create the gateway
- TCP local port: the TCP port waiting for the Serial-3G/2G gateway
- TCP Temporal client RS232: select this option if we want to activate a temporary socket (lasting 1 minute) when it is not in TCP Server mode, the IP/Serial gateway is not established and data is being received via the serial port. If activated, we must configure the TCP Client parameters "Remote IP", "Remote TCP Port", and "ID String" correctly, which will be shown below
- Temporal client wakeup: this option allows the user to activate a temporary socket when in TCP Server mode without the IP/Serial gateway established at the configured time. If activated, the parameters "Remote IP", "Remote TCP Port", and "ID String" from the TCP Client section must be correctly configured, as detailed below
- Temporal client time: this option indicates the period in which a temporary socket is active

- Temporal client random: this option allows the user to establish a random time for a temporary client that is added upon Wakeup. This is useful if we have a large number of devices connecting to each other at the same time and therefore wish to use a random time to distribute the connections to a server

- Temporal client Ovpn: this option is to be used if we have the OpenVPN section configured as "Under Request" and allows the OpenVPN to be activated 30 seconds before activing a temporary client. This option therefore offers greater security to our 3G-RS232 gateways. Once the temporary socket closes, the OpenVPN connection is also closed, freeing up the server

- SSH Enabled: by activing this option, we will be able to configure an IP-Serial Gateway with SSH security, encrypting communications. For such gateways, the port to be uses is 20022

- SSH Password: if we have SSH encryption enabled, the password is to be specified here. The username will be sshcom1, sshcom2, sshcom3, sshcom4 or sshcom5, depending on the associated serial port

- Function: serial-IP gateway (TCP Client): select this option if we wish to create a transparent Serial-3G/2G gateway in TCP client mode; i.e. a scenario in which the MTX-Router-Titan-3G or MTX-Router-Titan-3G-mini device connects to a specific IP/TCP port to establish the serial-3G/2G port

- Remote IP: IP address to which the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini device will connect

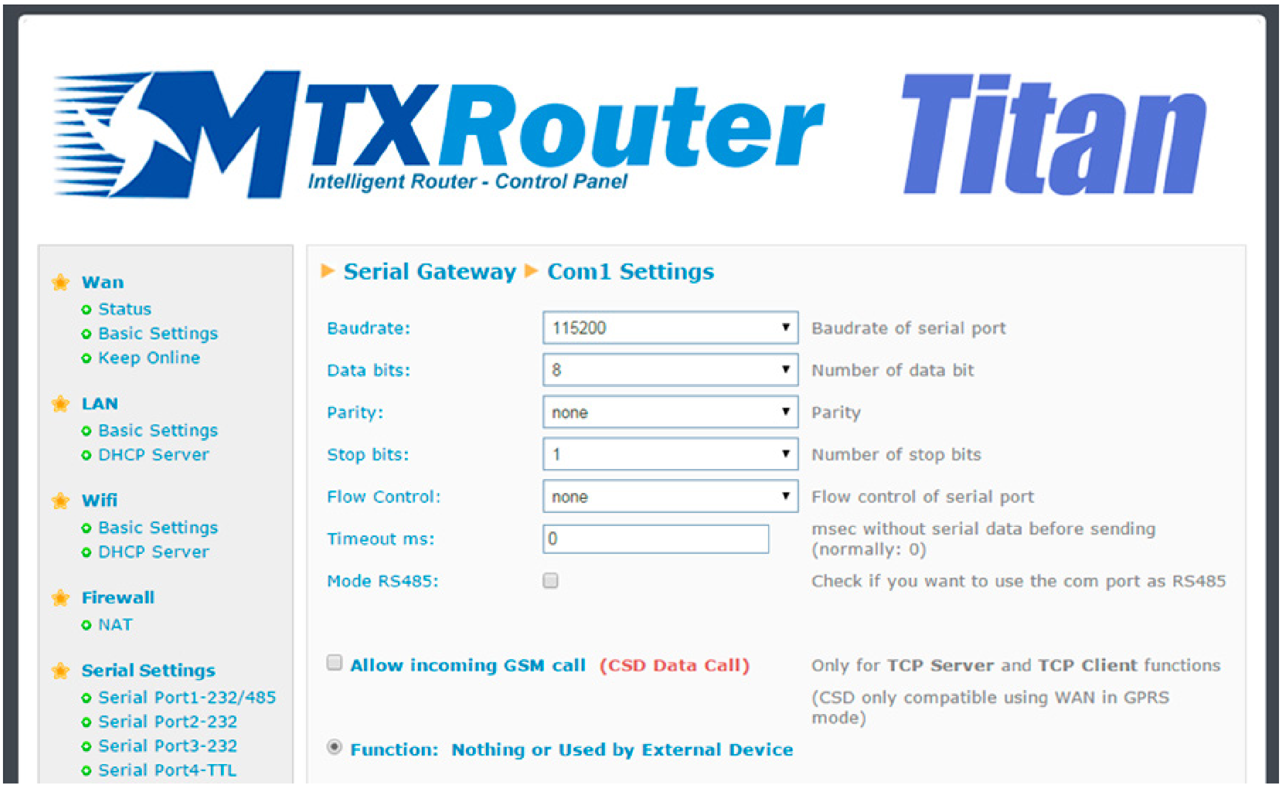
- Remote TCP Port: TCP port to which the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini will connect

- Reconnection time: in the event of a connection failure, or any connection problems, this parameter specifies how many milliseconds it should wait between attempts to connect again. 0 = immediate reconnection. Remember to adjust this value accordingly if we have a restricted data allowance for our SIM card.

- ID String: string that is sent just after the socket is established with the remote IP address. This text will allow we to identify the device that will create the connection. For example, if we have 100 MTX-Router-Titan-3G devices which work in this mode, this parameter allows we to identify which of the 100 devices has made the connection (after it has been made)

- Function: serial-IP gateway (Modbus TCP / Modbus RTU). Select this option if we wish to create a Serial-3G/2G gateway with ModBus TCP – ModBus RTU protocol. Do not use this option if we control software uses ModBus RTU protocol as a standard TCP server gateway would be sufficient. Do use this option if our control software uses ModBus TCP protocol. If we have any questions, get in touch with us at gsmsupport@matrix.es

- Function: direct (Internal Modem). Select this option if we wish to directly communicate with the internal modem of the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini device. For example, if we wish to make a GSM call, if we want to send an SMS or if we want to send any AT command. Using this option could, on occasion, affect the rest of the router's benefits (for example, if we send a special AT command to activate the Power Saving Mode, or to restart the internal modem, etc.). If we have any doubts, get in touch with us at gsmsupport@matrix.es. It is only possible to configure a serial port in the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini device with the mode "Function: Direct". This option (Direct, Internal Modem) is not supported for 3G models with GPS or 4G models



▸ Serial Gateway ▸ Com1 Settings

Baudrate:	115200 ▾	Baudrate of serial port
Data bits:	8 ▾	Number of data bit
Parity:	none ▾	Parity
Stop bits:	1 ▾	Number of stop bits
Flow Control:	none ▾	Flow control of serial port
Timeout ms:	0	msec without serial data before sending (normally: 0)
Mode RS485:	□	Check if you want to use the com port as RS485

□ Allow incoming GSM call (CSD Data Call) — Only for **TCP Server** and **TCP Client** functions (CSD only compatible using WAN in GPRS mode)

● Function: Nothing or Used by External Device

ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.
- The serial ports of the type TTL refer to an internal serial port belonging to the MTX-Router-Titan-3G device for special communication cards (RF868MHz, GPS, etc.); i.e. it is not an external serial port of the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini device.
- The serial ports of the type USB refer to a virtual serial port that is created inside the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini device when a connection to a USB device is made. Do not use this COM if a USB device is not connected. Remember that the USB device (if we wish to create a USB-3G/2G gateway) should be of the type FTDI. For any other type of driver, get in touch with us at gsmsupport@matrix.es.

2.6 External Devices

In this section we will configure the MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices’ internal datalogger, as well as external serial peripheral devices (temperature and distance sensors, generic modbus RTU devices, Radio Sensors (Wavenis) etc.).

2.6.1 External Devices: Logger Configuration

If we need the Titan device to collect data from external devices (Modbus, temperature and distance sensors, pulse counters, alarms, relays, etc.) in order to send them to our external server, first we must configure the internal logger, that is, how and where to collect the data from, and how to send it.

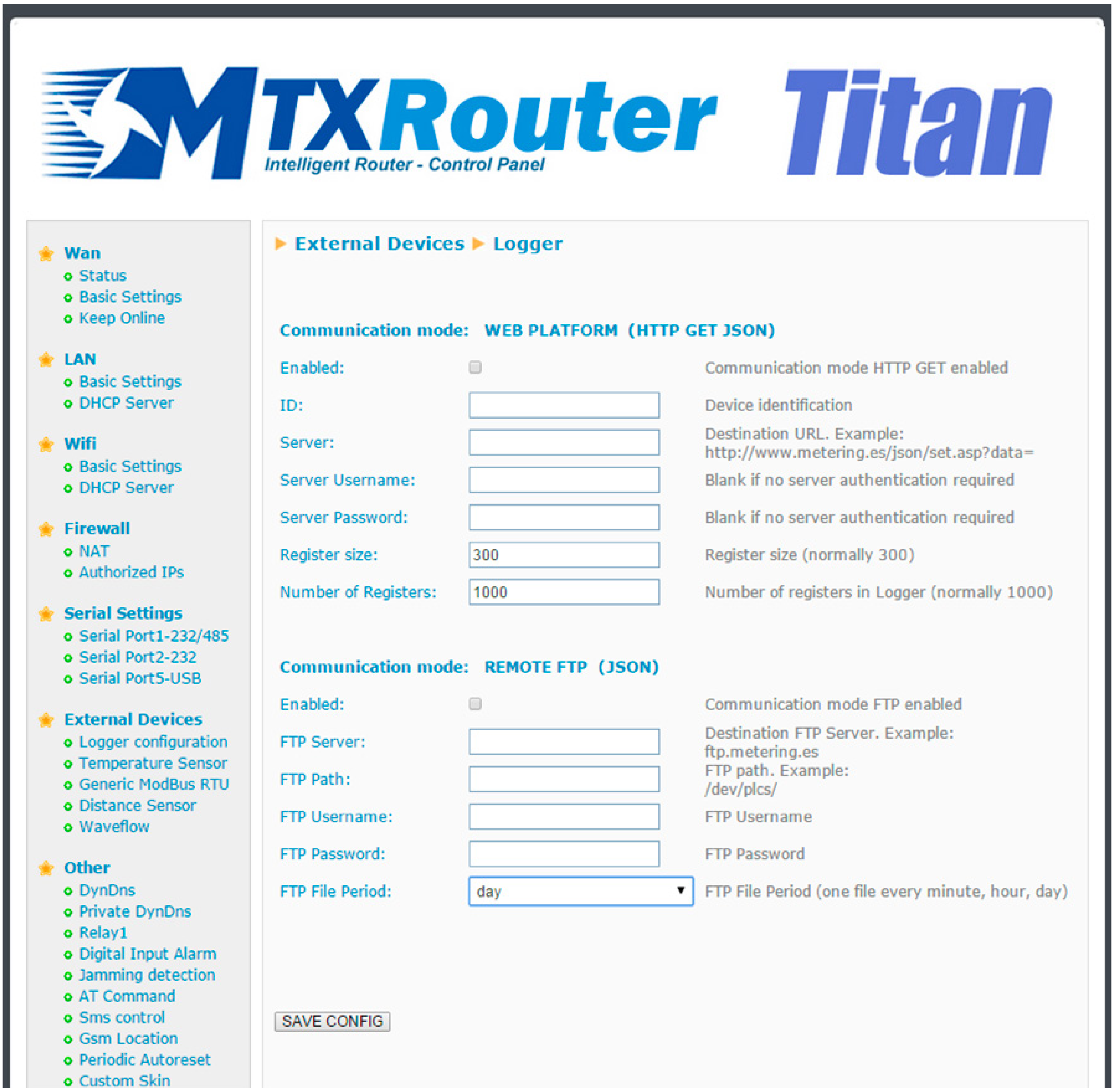
This section allows to configure the options related to the internal datalogger. We can send data via HTTP GET JSON (ideal for collecting data in JSON format from a platform using PHP, ASP, etc.) and/or via FTP.

WEB PLATFORM (HTTP GET JSON) Mode

- Enabled: click to set up the mode to send data to a platform via HTTP GET (in JSON format)
- Mode: data sending mode. The options available HTTP GET (JSON), HTTPS GET (JSON), HTTP GET (PARAMETERS), HTTPS GET (PARAMETERS), HTTP PUT (PARAMETERS), HTTPS PUT (PARAMETERS), or directly with the GroveStreams platform
- Custom parameters: this option allows we to add optional parameters for HTTP GET and HTTP PUT methods.
- Custom header1 and Custom header2: this option allows we to add headers to the HTTP requests. Many web platforms require the use of a header with a token for identificative purposes. This can be configured in this section
- Server: complete URL for the sending of data collected in the datalogger. For example, http://www.metering.es/json/set.asp?data=
- Server login: if our platform has restricted access, input here the username
- Server password: if our platform has restricted access, input here the password
- ID: this parameter allows us to send an additional identity parameter within the JSON object, allowing we to know which device is receiving data if we do not want to use the device's IMEI
- Register size: maximum size of the router's internal register. Normally 300
- Number of registers: maximum number of registers in the datalogger. Normally 1000

FTP (JSON) Mode

- Enabled: click to set up the mode to send data to a FTP server (the file format is JSON)
- FTP server: FTP server used to send data
- FTP path: path inside the server where to send the data
- FTP username: the username of the FTP server account that allows we to write
- FTP password: the password of the FTP server account that allows we to write
- FTP file period: the frequency with which we want the Titan to send the data files to the server (every day, every hour, every minute, etc.)



▶ External Devices ▶ Logger

Communication mode: WEB PLATFORM (HTTP GET JSON)

Enabled:	□	Communication mode HTTP GET enabled
ID:		Device identification
Server:		Destination URL. Example: http://www.metering.es/json/set.asp?data=
Server Username:		Blank if no server authentication required
Server Password:		Blank if no server authentication required
Register size:	300	Register size (normally 300)
Number of Registers:	1000	Number of registers in Logger (normally 1000)

Communication mode: REMOTE FTP (JSON)

Enabled:	□	Communication mode FTP enabled
FTP Server:		Destination FTP Server. Example: ftp.metering.es
FTP Path:		FTP path. Example: /dev/plcs/
FTP Username:		FTP Username
FTP Password:		FTP Password
FTP File Period:	day	FTP File Period (one file every minute, hour, day)

ADDITIONAL NOTES

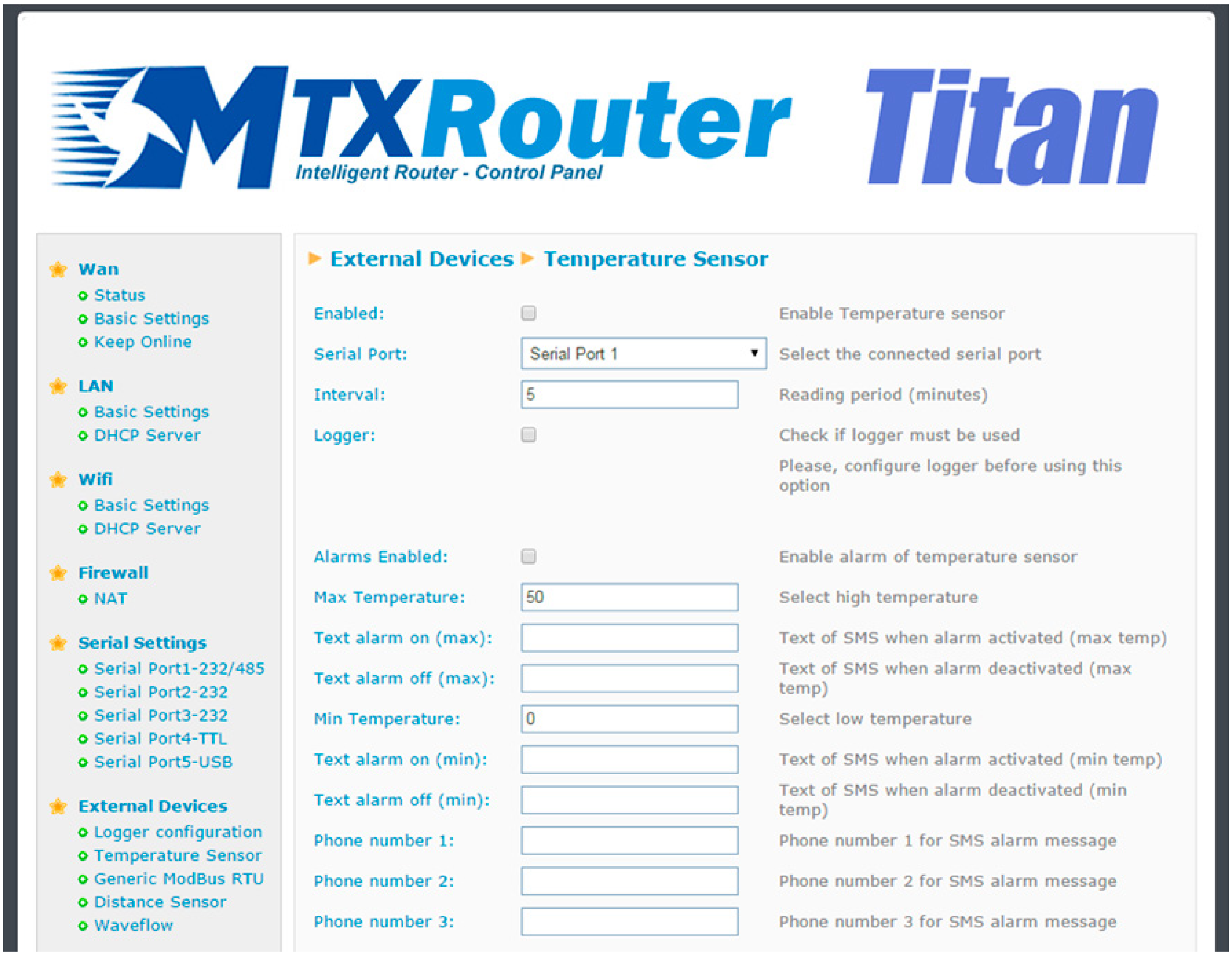
- Once the configuration is finished, click "SAVE CONFIG" to save the changes. Remember that the router should be restarted for the changes to take effect.
- When HTTP GET mode is used to send the data, it is sent to the server as it is received. If there is no GSM coverage or problems occur with the sending of data (for example, the remote server fails), the Titan device will store the data in its internal memory and send it when communications are restored.
- When FTP mode is used to send data, it is stored in a JSON register file and it is sent according to the frequency specified (every minute, hour, day, etc.). If there is no GSM coverage or problems occur with the sending of data, (for example, the remote server fails), the Titan device will store the data in its internal memory and send it when communications are restored.

- The FTP file created on our server will have the following format:
  - IMEI-year-month-day.txt > if the frequency chosen is “every day”
  - IMEI-year-month-day-time.txt > if the frequency chosen is “every hour”
  - IMEI-year-month-day-time-minute.txt > if the frequency chosen is “every minute”

2.6.2 External Devices: Temperature Sensor

The MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices are prepared to manage the MTX-Temp-RS232 temperature gauge. For example, we can send the temperature periodically to a web platform, send an SMS alert when the temperature is above or below a pre-determined level, or even change a relay when the temperature is outside a particular margin (Other >> Relay).

- Enabled: activate this option if we have a MTX-Temp-RS232 temperature gauge connected to a serial port
- Serial Port: select the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini device’s serial port where the MTX-Temp-RS232 temperature gauge is connected
- Interval: if we wish to send temperature readings periodically to our webserver, we can specify here the period (in minutes)
- Logger: if we wish to use the internal logger to store temperature data (to later send this to a web platform), we need to select this option. This option should not be selected if we only want to send an SMS alert when the temperature is outside preset margins
- Alarms enabled: select this option if we want to activate the alarms when the temperature is outside margins
- Max Temperature: the maximum temperature before which an alarm is sent due to high temperature.
- Text alarm on (max): text for the alarm to be sent when the temperature is considered to be high
- Text alarm off (max): text for the alarm to be sent when the high temperature alert is deactivated
- Min Temperature: minimum temperature before which an alarm is sent due to low temperature
- Text alarm on (min): text for the alarm to be sent when the temperature is considered to be low
- Text alarm off (min): text for the alarm to be sent when the low temperature alert is deactivated
- Phone number 1: first telephone number where the SMS alarms are to be sent
- Phone number 2: second telephone number where the SMS alarms are to be sent
- Phone number 3: third telephone number where the SMS alarms are to be sent
- Current temperature: indicates the current temperature in real time if a MTX-Temp-RS232 temperature sensor is connected



▶ External Devices ▶ Temperature Sensor

Enabled:	□	Enable Temperature sensor
Serial Port:	Serial Port 1 ▼	Select the connected serial port
Interval:	5	Reading period (minutes)
Logger:	□	Check if logger must be used Please, configure logger before using this option
Alarms Enabled:	□	Enable alarm of temperature sensor
Max Temperature:	50	Select high temperature
Text alarm on (max):		Text of SMS when alarm activated (max temp)
Text alarm off (max):		Text of SMS when alarm deactivated (max temp)
Min Temperature:	0	Select low temperature
Text alarm on (min):		Text of SMS when alarm activated (min temp)
Text alarm off (min):		Text of SMS when alarm deactivated (min temp)
Phone number 1:		Phone number 1 for SMS alarm message
Phone number 2:		Phone number 2 for SMS alarm message
Phone number 3:		Phone number 3 for SMS alarm message

ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.
- The hysteresis that the MTX devices use is 1 degree. For example, if we configure 50ºC to be a high temperature, the alarm will be activated when the temperature reaches 50ºC. However, it will not be considered deactivated until it falls below 49ºC, so as to avoid the constant sending of SMS messages when the temperature is just inside the selected range.
- Sample format of the JSON string sent:

```
{“IMEI”:”358884050088207”,”TS”:”25/12/2014 17:40:09”,”TYPE”:”TEMP”,
”P”:”1234”,”TEMP”:25.5,”ALTH”:0,”ALTL”:0}
```

Where:

- IMEI: the router’s ID number. Unique for each device
- TS: time stamp DD:MM:YYYY HH:MM:SS.

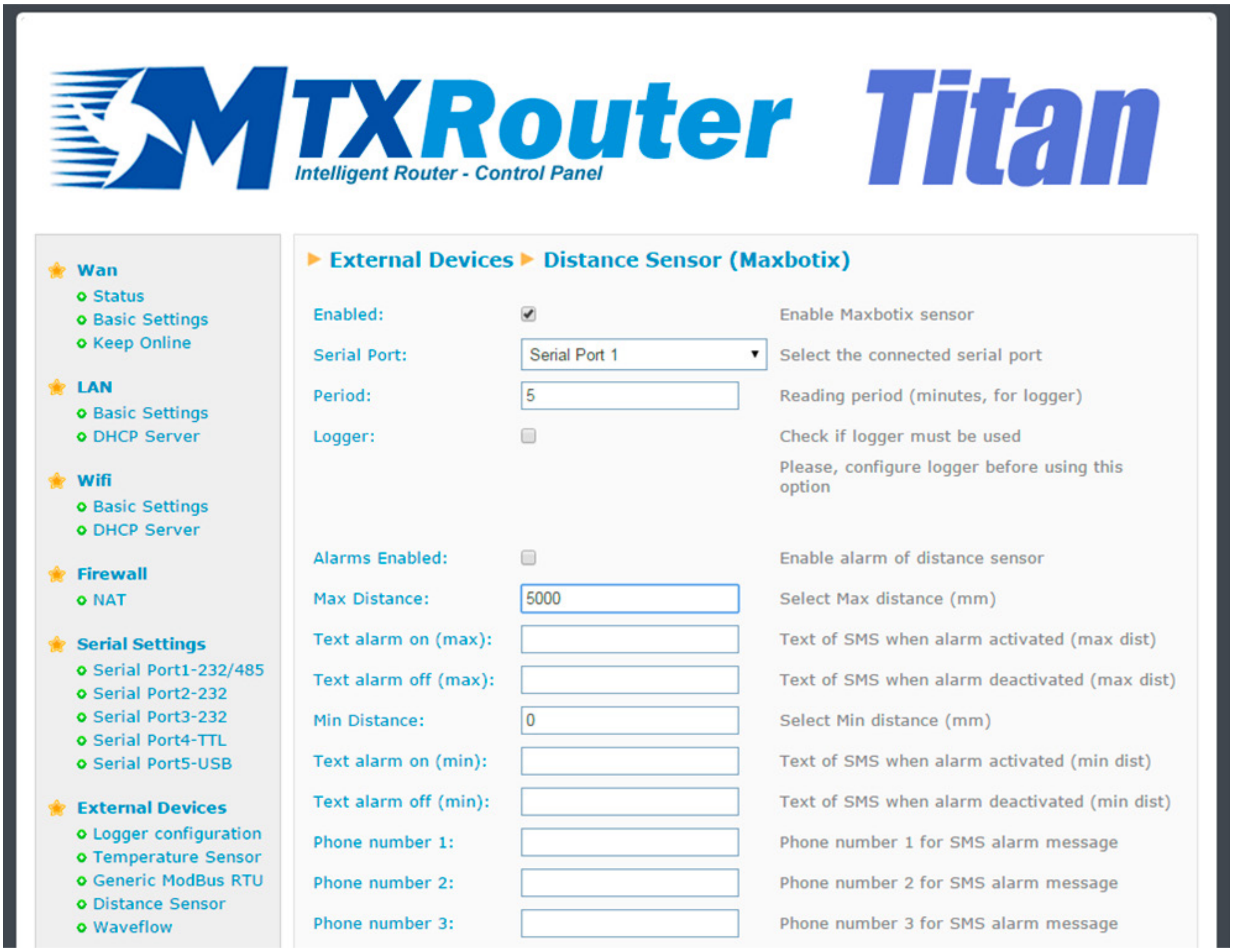
- TYPE: type of string. In this case it is temperature.
- P: the logger's ID field (External Devices > Logger configuration)
- TEMP: temperature
- ALTH: alarm due to high temperature (0=no, 1=yes)
- ALTL: alarm due to low temperature (0=no, 1=yes)

2.6.3 External Devices: Distance Sensor

The MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices are prepared to manage a Maxbotix distance sensor with an RS232 output (get in touch with us at gsmsupport@matrix.es if we have doubts regarding the appropriate model). For example, we can send the measured distance periodically to a web platform, send an SMS alert when the distance is longer or shorter than a pre-determined value, or even change a relay when the distance falls outside a particular range (for this, take a look at the section Other >> Relay).

A typical application could be a grain or cement silo where the Maxbotix distance sensor (using ultrasound) sends the measurements periodically.

- Enabled: activate this option if we have a Maxbotix distance sensor with RS232 port connected to a serial port
- Serial Port: select the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini device's serial port where the Maxbotix distance sensor is connected
- Interval: if we wish to send distance readings periodically to our webserver, we can specify here the period (in minutes)
- Logger: if we wish to use the internal logger to store distance data (to later send this to a web platform), we need to select this option. This option should not be selected if we only want to send an SMS alert when the distance is outside preset margins
- Alarms enabled: select this option if we want to activate the alarms when the distance is outside margins
- Max Distance: the maximum distance before which an alarm is sent due to long distance
- Text alarm on (max): text for the alarm to be sent when the distance is considered to be long
- Text alarm off (max): text for the alarm to be sent when the long distance alert is deactivated
- Min Distance: minimum distance before which an alarm is sent due to short distance
- Text alarm on (min): text for the alarm to be sent when the distance is considered to be short
- Text alarm off (min): text for the alarm to be sent when the short distance alert is deactivated
- Phone number 1: first telephone number where the SMS alarms are to be sent
- Phone number 2: second telephone number where the SMS alarms are to be sent
- Phone number 3: third telephone number where the SMS alarms are to be sent
- Current distance: indicates the current temperature in real time if a Maxbotix distance sensor is connected



▸ External Devices ▸ Distance Sensor (Maxbotix)

Enabled:	☑	Enable Maxbotix sensor
Serial Port:	Serial Port 1 ▾	Select the connected serial port
Period:	5	Reading period (minutes, for logger)
Logger:	☐	Check if logger must be used Please, configure logger before using this option
Alarms Enabled:	☐	Enable alarm of distance sensor
Max Distance:	5000	Select Max distance (mm)
Text alarm on (max):		Text of SMS when alarm activated (max dist)
Text alarm off (max):		Text of SMS when alarm deactivated (max dist)
Min Distance:	0	Select Min distance (mm)
Text alarm on (min):		Text of SMS when alarm activated (min dist)
Text alarm off (min):		Text of SMS when alarm deactivated (min dist)
Phone number 1:		Phone number 1 for SMS alarm message
Phone number 2:		Phone number 2 for SMS alarm message
Phone number 3:		Phone number 3 for SMS alarm message

ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.
- Sample format of the JSON string sent:

```
{“IMEI”:”358884050088207”,”TS”:”25/12/2014 17:40:09”,”TYPE”:”DIST”,
”P”:”1234”,”DIS”:500,”ALDH”:0,”ALDL”:0}
```

Where:

- IMEI: the router’s ID number. Unique for each device
- TS: time stamp DD:MM:YYYY HH:MM:SS
- TYPE: type of string. In this case it is distance
- P: the logger’s ID field (External Devices > Logger configuration)
- DIS: distance read

- ALDH: alarm due to long distance (0=no, 1=yes)
- ALDL: alarm due to short distance (0=no, 1=yes)

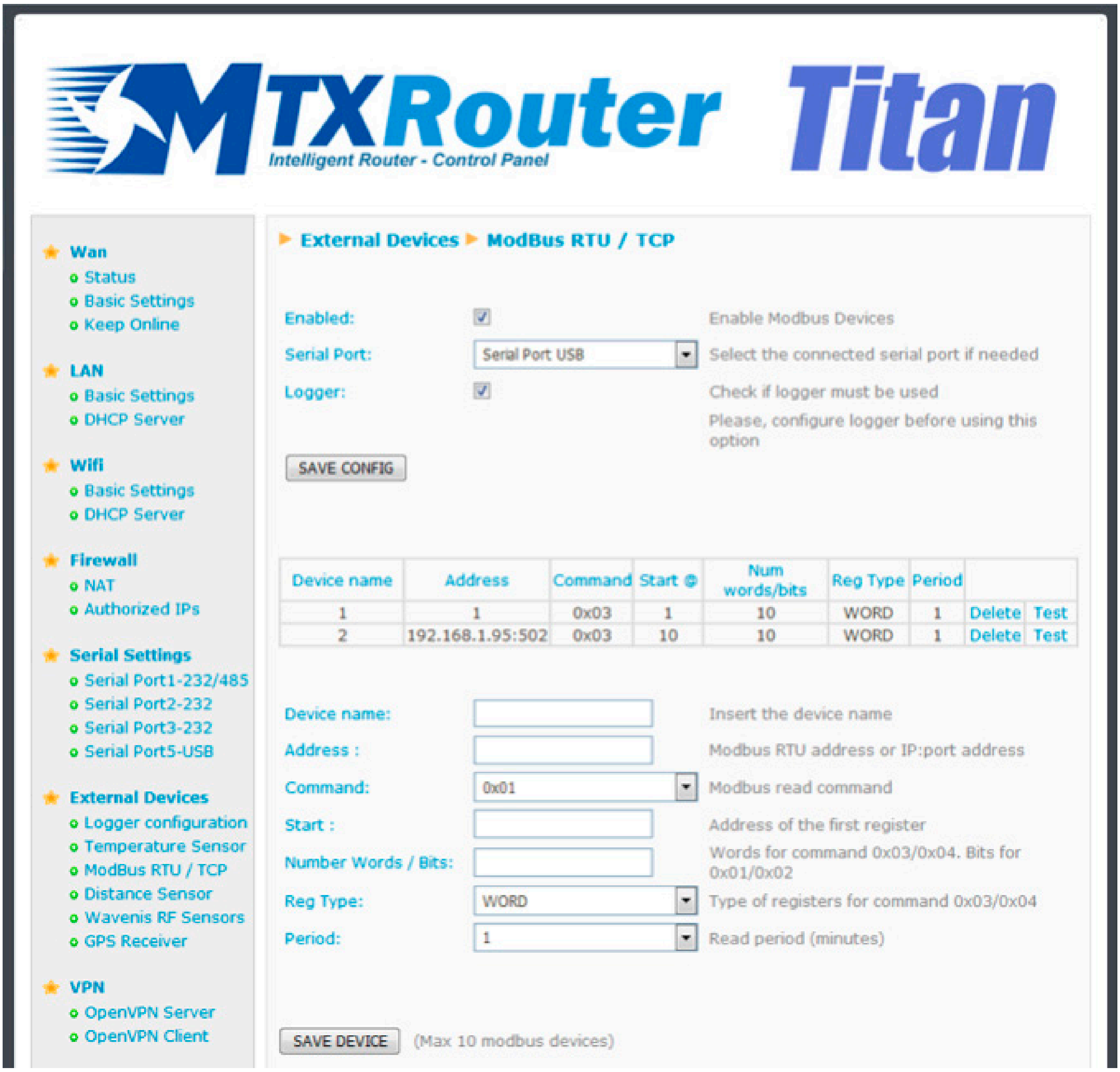
2.6.4 External Devices: Modbus RTU/TCP

The MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices are prepared to read, store and send registers from Modbus RTU devices. We can program a periodic reading of up to 10 Modbus devices, choosing the registers to be read, and the later sending of the readings to a webserver via a JSON object.

- Enabled: activate this option if we have one or more Modbus RTU devices connected to a serial port and we wish the Modbus registers to be read autonomously
- Serial Port: select the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini device's serial port where the Modbus RTU device is connected
- Logger: if we wish to use the internal logger to store the read Modbus registers (to later send this to a web platform), we need to select this option
- Device name: identifying name of the Modbus RTU device
- Address: Modbus RTU address of the device to be read.
- Command: modbus read command
- Start: register where reading shall start
- Num Words: number of registers to be read
- Reg type: type of registers to be read
- Period: period of readings; i.e. how often (in minutes) the registers should be read

We can create up to 10 devices. If we need to read a series of Modbus registers that are not consecutive in the same Modbus device, we will need to create several devices with the same Modbus address and choose a different range to be read in each one.

For example, if we have a device with Modbus address @1 and we wish to read the registers 1 to 10 and 100 to 110, we will need to create two devices with "Address" @1, one of these with the "Start" parameter set to 1, and the device with the "Start" parameter set to 100. In both devices the "Num Words" parameter should be set to 10.



External Devices ▸ ModBus RTU / TCP

Enabled: ☑ Enable Modbus Devices

Serial Port: Serial Port USB Select the connected serial port if needed

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

Device name	Address	Command	Start @	Num words/bits	Reg Type	Period		
1	1	0x03	1	10	WORD	1	Delete	Test
2	192.168.1.95:502	0x03	10	10	WORD	1	Delete	Test

Device name: Insert the device name

Address : Modbus RTU address or IP:port address

Command: 0x01 Modbus read command

Start : Address of the first register

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

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

Period: 1 Read period (minutes)

(Max 10 modbus devices)

ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.
- If we wish to create a new Modbus RTU device, we must complete the form data and click “SAVE DEVICE”.
- Sample format of the JSON string sent:

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

Where:

- IMEI: the router’s ID number. Unique for each device
- TS: time stamp DD:MM:YYYY HH:MM:SS
- TYPE: type of string. In this case it is modbus
- P: the logger’s ID field (External Devices > Logger configuration)
- ST: starting register
- A: modbus address of the device to be read
- V: array with the registers that have been read

- We recommend that we read the chapter about the available AT commands since we can use them to read and change values of Modbus registers either from the web configuration environment, Remote console (Telnet) or via SMS
- We can establish non-consecutive registries in the “Start” and “Num Words” fields, based on the firmware version 3.26. Check the Application Note 27 for more information and examples

2.6.4.1 External Devices: ModBus RTU/TCP, Modbus to SNMP Gateway

This section describes the process to implement a Modbus-SNMP gateway, allowing almost any Modbus RTU or Modbus TCP device to be intregated into an SNMP network. An additional Application Note is available (AN8-Router-Titan-Modbus-to-SNMP-Gateway.pdf) in which detailed information, including examples, regarding this option can be found.

- Enabled: activate this option to enable the Modbus-SNMP gateway
- Address: Modbus RTU or Modbus TCP device’s address
- Start: first register address to be mapped
- Number of words: number of Modbus registers to be mapped (maximum 500)
- Registers for Traps: several Modbus registers can be specified, separated by semi-colon. If there is a change in the value of one of these registers, the Titan router will send a TRAP
- Message for Traps: message to be sent in the generated TRAP
- Severity for Traps: severity to be send in the generated TRAP

2.6.5 External Devices: Wavenis

The Titan II, Titan and Titan-mini devices are ready to read, store and send registers from Waveflow 868MHz pulse counters as well as WaveTherm 868MHz temperature sensors. An internal Wavecard 868MHz communication card can be included, allowing for communications with Wavenis devices up to 1km away (in direct vision), or up to 16km away using up to 3 boosters. When using the Titan-mini model to read Waveflows, a Waveport (USB or RS232) device is required.

An Application Note is available for a greater understanding of its use, including examples (AN6-Router-Titan-Metering-Wavenis-Concentrator.pdf)

Periodic readings of up to 64 Waveflow devices and 5 Wavetherm devices can be programmed, sending at a later time the readings to a webserver via a JSON object or via the logger using FTP.

- Enabled: activate this option to enable Waveflow communications
- Serial Port: select the serial port “Serial Port 4 – TTL” for the Titan router and “Serial Port 5 – USB” when using the Titan-mini model
- Period: in this field, indicate how frequently (in minutes) we wish the data sensors to be read
- Number of attempts: in this field we can specify the number of attempts to take readings should an error occur
- Logger: select this option if we wish for the internal logger to be used to store the Modbus registers that are read (for later sending to the web platform)

2.6.5.1 External Devices: Wavenis, WaveTalk

This section allows we to configure up to 10 Wavetalk boosters. Remember that up to three boosters can be used between the Wavenis concentrator (the Titan router) and the sensors to be read. Here the MAC address of each WaveTalk booster should be specified.

2.6.5.2 External Devices: Wavenis, Waveflow-4

The following configuration parameters allow we to add Waveflow devices. Up to 64 can be added.

- Name/ID: name to identify a Waveflow device
- MAC address: Waveflow device’s MAC address (hexadecimal format)

If we wish to use boosters, this must be done by inputting the MAC address of the device to be used with boosters in the “MAC address” field. For example, if we wish to use boosters 2 and 5 for the Waveflow device with MAC address 010203040506, we would insert ‘010203040506;2;5’ (remember that semi-colons are used for separation).

2.6.5.3 External Devices: Wavenis, Wavetherm

The following configuration parameters allow we to add Wavetherm devices. Up to 5 can be added.

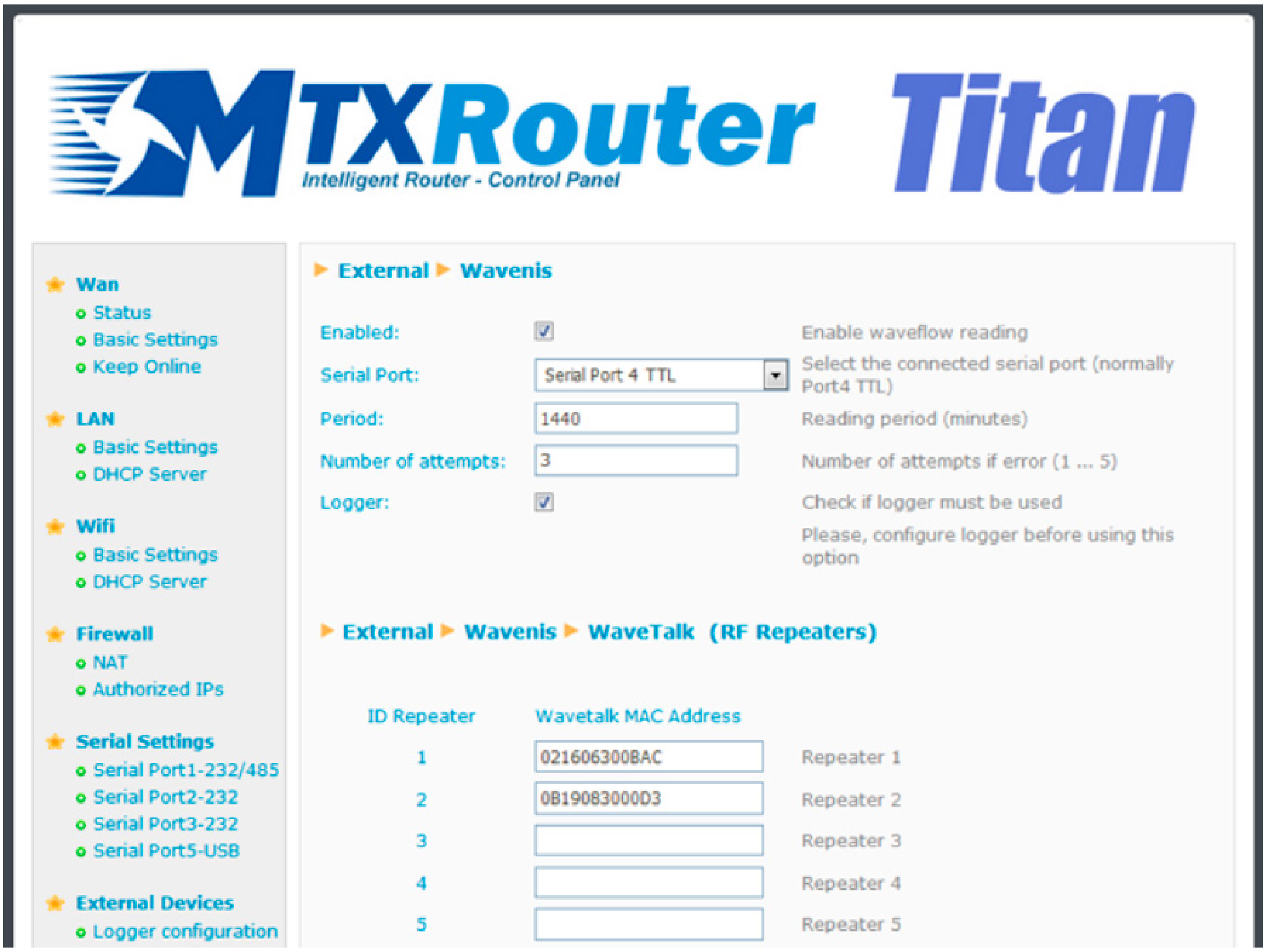
- Name/ID: name to identify a Wavetherm device
- MAC Address: Wavetherm device’s MAC address (hexadecimal format)

If we wish to use boosters, this must be done by inputting the MAC address of the device to be used with boosters in the “MAC address” field. For example, if we wish to use boosters 2 and 5 for the Wavetherm device with MAC address 010203040506, we would insert ‘010203040506;2;5’ (remember that semi-colons are used for separation).

2.6.5.4 External Devices: Wavenis, Tools

In this section we will find tools to remotely access Wavenis devices at any time. Simply input the device's MAC address (with boosters if applicable), and press the corresponding button.

- Waveflow-4 read: reading of the count, alarms and battery status of a Waveflow device with 4 entries
- Waveflow-4 reset Alarms: if alarms are used (battery, circuit shortage, etc.) these can be reset here
- WaveThern read: reading of the current temperature of a Wavetherm device
- Generic read RSSI: this field allows we to read the RSSI between the Wavenis communication concentrator (Titan router) and a remote device. If boosters are used, the RSSI should be indicated at the end. For example, if we wish to read a Wavenis device using boosters 3 and 5, by specifying the value '010203040506;3;5', the RSSI between booster 5 and the MAC device 010203040506 will be given
- Generic read battery counter: this field allows we to obtain an estimation of the remaining battery life

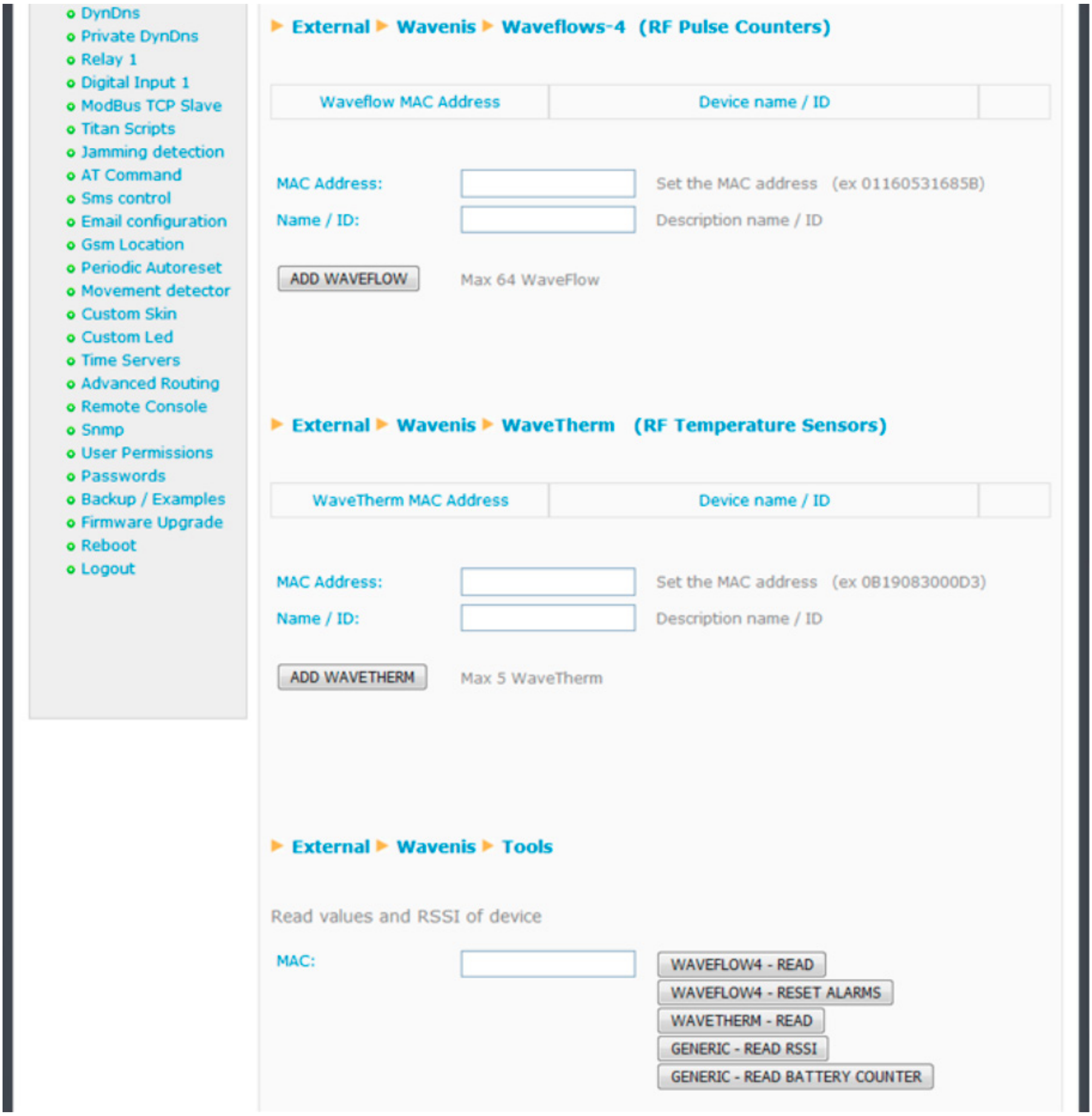


▸ External ▸ Wavenis

Enabled:	☑	Enable waveflow reading
Serial Port:	Serial Port 4 TTL ▾	Select the connected serial port (normally Port4 TTL)
Period:	1440	Reading period (minutes)
Number of attempts:	3	Number of attempts if error (1 ... 5)
Logger:	☑	Check if logger must be used Please, configure logger before using this option

▸ External ▸ Wavenis ▸ WaveTalk (RF Repeaters)

ID Repeater	Wavetalk MAC Address	
1	021606300BAC	Repeater 1
2	0B19083000D3	Repeater 2
3		Repeater 3
4		Repeater 4
5		Repeater 5



External ▸ Wavenis ▸ Waveflows-4 (RF Pulse Counters)

Waveflow MAC Address	Device name / ID	

MAC Address: Set the MAC address (ex 01160531685B)

Name / ID: Description name / ID

Max 64 WaveFlow

External ▸ Wavenis ▸ WaveTherm (RF Temperature Sensors)

WaveTherm MAC Address	Device name / ID	

MAC Address: Set the MAC address (ex 0B19083000D3)

Name / ID: Description name / ID

Max 5 WaveTherm

External ▸ Wavenis ▸ Tools

Read values and RSSI of device

MAC:

2.6.6 External Devices: GPS Receiver

The Titan routers are GPS enabled and can be ordered with an internal GPS module built in. These devices (MTX-Router-Titan-3G-mini-GPS or MTX-Router-Titan-4G-mini-GPS) can also be used with an external GPS module by connecting it to either the microUSB port or a serial port.

- Enabled: activate this option if we have an internal (or external) GPS module connected to the Titan router to be used

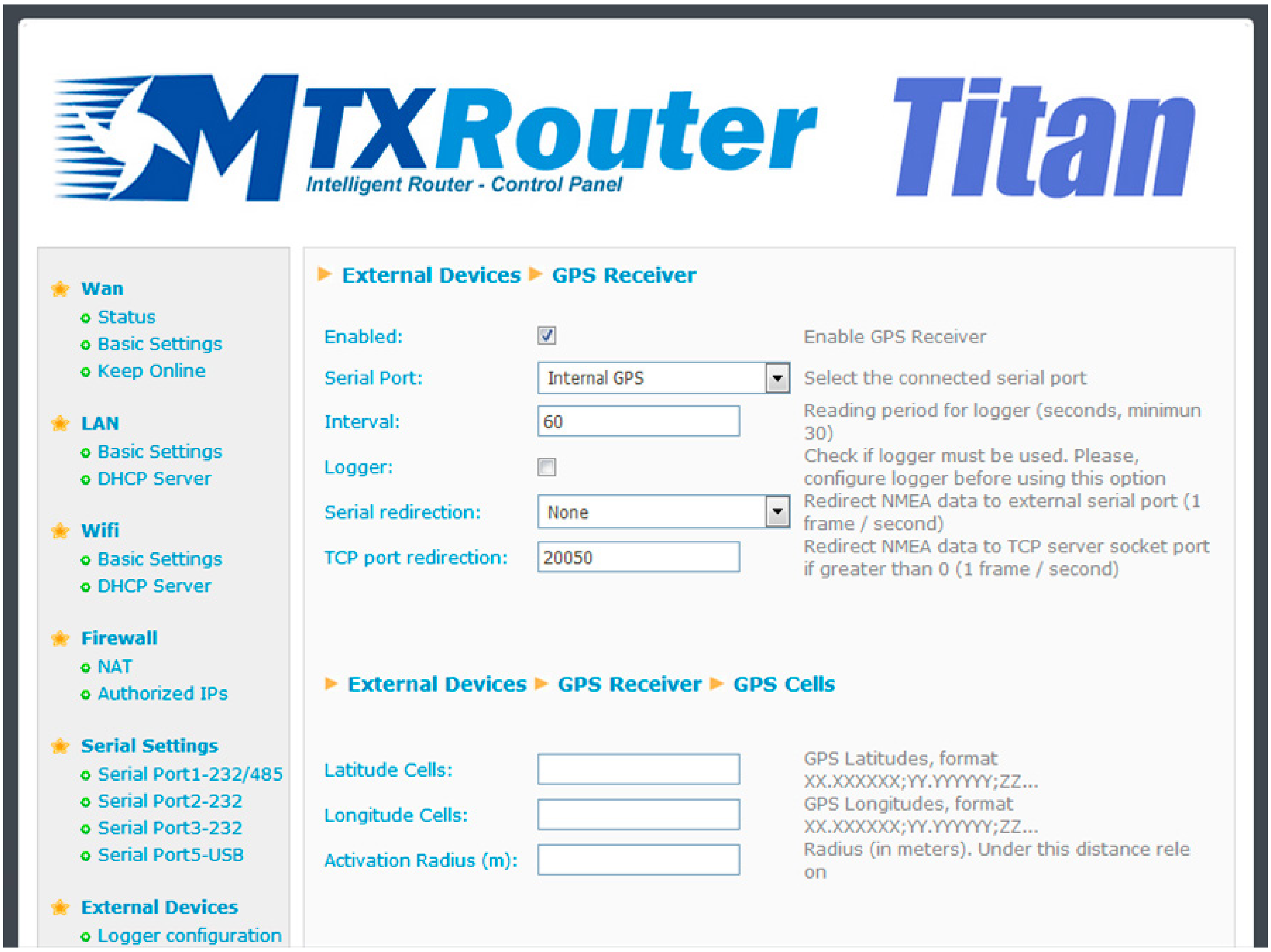
- Serial Port: select the MTX-Router-Titan II, MTX-Router-Titan or MTX-Router-Titan mini's serial port used to connect the GPS. For the MTX-Router-Titan-3G device using an internal GPS module, select "Serial Port 4 TTL". For the MTX-Router-Titan-3G-mini-GPS or MTX-Router-Titan-4G-mini-GPS devices, select "Internal GPS"

- Interval: select the period (in seconds) of GPS readings taken. A value greater than 30 seconds must be specified
- Logger: activate this option if we wish to save the GPS positions that are read in the internal logger for later sending to a web platform via HTTP or FTP. This is useful if we are using the Titan device to implement a fleet management system using GPS
- Output redirection: this option allows NMEA position frames to be redirected through one of the RS232, RS485 serial ports or the USB port of the Titan device. In this way, GPS can be used by an additional serial port device
- TCP Port Redirection: in the same way NMEA frames can be obtained via an RS232 or RS485 serial port or the USB port, it is also possible to obtain NMEA frames via a TCP socket by connecting to the Titan device by Ethernet, WiFi, 3G or 4G. If a TCP port greater than 0 is specified, the device will connect to said TCP port and obtain the NMEA frames

GPS Cells

Titan routers allow we to specify up to 20 GPS cells defined by longitude, latitude and radius. For example, a relay can be programmed to be activated when inside a GPS cell and deactivated when outside. This is useful to detect when machinery leaves the work area or to impede the opening of electronic lock system controlled containers outside loading areas, etc.

- Latitude cells: in this field we should state the latitude of the different GPS cells to be configured, separating them by a semi-colon
- Longitude cells: in this field we should state the longitude of the different GPS cells to be configured, separating them by a semi-colon
- Activation radius: in this field we should state the radius of the different GPS cells to be configured, separating them by a semi-colon



▸ External Devices ▸ GPS Receiver

Enabled:	☑	Enable GPS Receiver
Serial Port:	Internal GPS	Select the connected serial port
Interval:	60	Reading period for logger (seconds, minimun 30)
Logger:	☐	Check if logger must be used. Please, configure logger before using this option
Serial redirection:	None	Redirect NMEA data to external serial port (1 frame / second)
TCP port redirection:	20050	Redirect NMEA data to TCP server socket port if greater than 0 (1 frame / second)

▸ External Devices ▸ GPS Receiver ▸ GPS Cells

Latitude Cells:		GPS Latitudes, format XX.XXXXXX;YY.YYYYYY;ZZ...
Longitude Cells:		GPS Longitudes, format XX.XXXXXX;YY.YYYYYY;ZZ...
Activation Radius (m):		Radius (in meters). Under this distance rele on

ADDITIONAL NOTES

- Once the configuration is complete, press the “SAVE CONFIG” button to save the changes. Remember that the router should be reset in order for the changes to take effect.

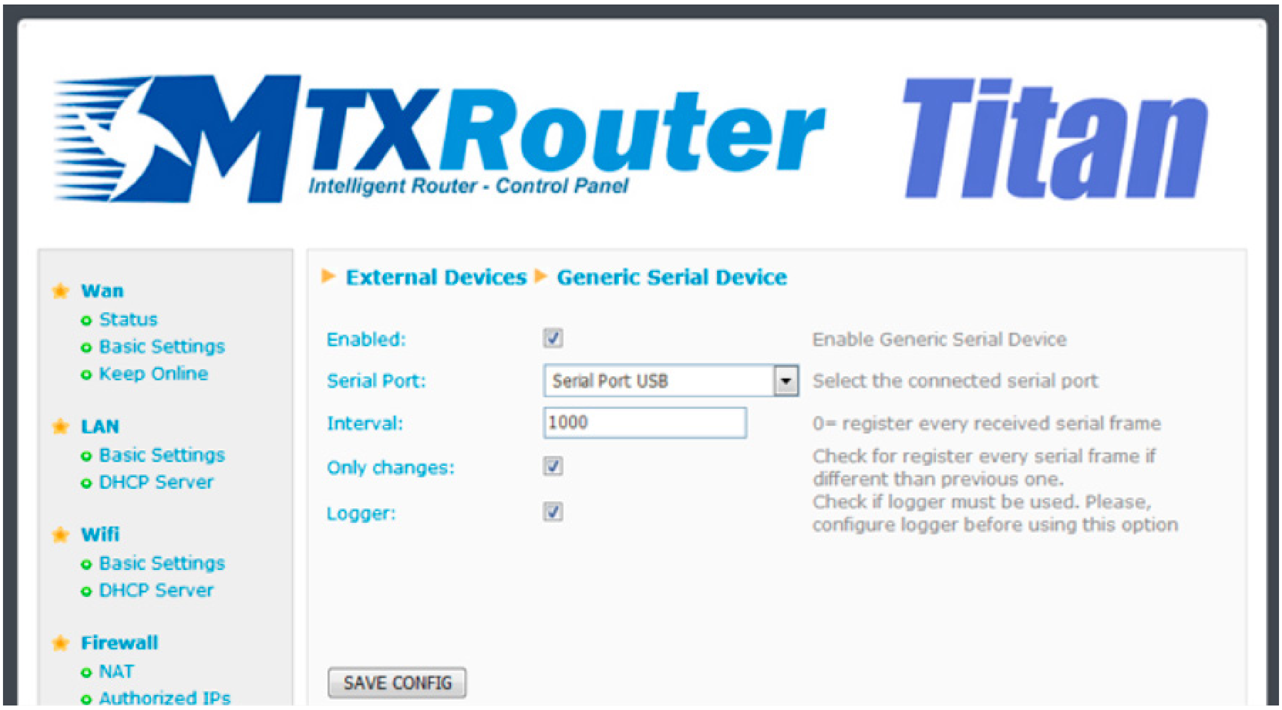
2.6.7 External Devices: Generic Serial Device

In this section we can configure a datalogger for RS232, RS485 or USB serial devices that allows we to read, store and send data collected from any of the previously mentioned interfaces. It is particularly useful to collect data from serial devices that send data frames periodically (temperature/humidity sensors, serial alarms, etc.).

- Enabled: activate this option if we wish to connect a serial device with the Titan router acting as a datalogger
- Serial Port: select Titan router’s serial port used for logging
- Interval: selecting a value of “0” means all serial frames that are received will be collected. A value of “1” will collect every other frame that is received. A value of “2” will collect one of every three frames received
- Only Changes: activate this option if we only wish to log frames that are different to the previous frame. For example, if we connect a temperature sensor, this could be sending the same data

if there is no change in temperature. By activating this option, only changes will be collected by the datalogger

- Logger: activate this option if we wish to save the data that is read in the internal logger for later sending to a web platform via HTTP or FTP



External Devices ▸ Generic Serial Device

Enabled:	☑	Enable Generic Serial Device
Serial Port:	Serial Port USB	Select the connected serial port
Interval:	1000	0= register every received serial frame
Only changes:	☑	Check for register every serial frame if different than previous one.
Logger:	☑	Check if logger must be used. Please, configure logger before using this option

SAVE CONFIG

ADDITIONAL NOTES

- Once the configuration is complete, press the “SAVE CONFIG” button to save the changes. Remember that the router should be reset in order for the changes to take effect.

2.6.8 External Devices: W-MBus Concentrator

From this section we can configure the Titan router as a W-MBus hub, to collect data from W-MBus devices, pack them and send them to a web platform. Remember that our Titan router must have the RF card (optional) in order to use this feature.

It has a very detailed application note with examples of use, consult it for more information: AN21-Router-Titan-Wireless-MBus-Concentrator.pdf.

- Enabled: check this box to activate the “W-Mbus Concentrator of the Titan Router” feature

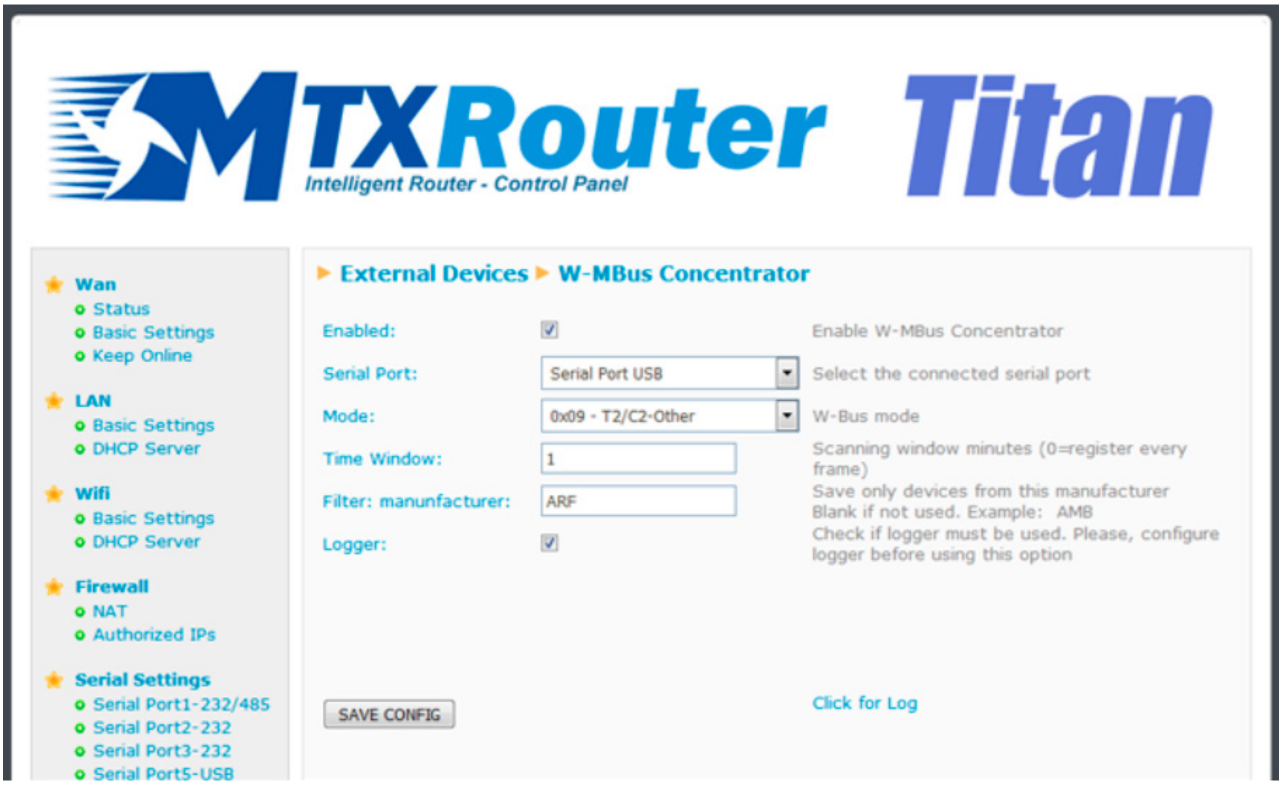
- Serial Port: select the serial port of the Titan router where the RF card (optional) is connected inside our Titan rotuer. Normally we must select “Serial Port USB”

- Mode: choose the W-MBus mode we need to use

- Time Window: indicates a temporary window (in minutes). Only one W-MBus data frame of each device received during said time window will be recorded

- Filter manufacturer: optional. It allows to introduce a manufacturer to receive only the data of equipment of this manufacturer. For example AMB, ARF...

- Logger: check this box if we want to save the W-MBus data to the internal logger for later upload to our Web platform via HTTP or FTP



External Devices ▸ W-MBus Concentrator

Enabled:	☑	Enable W-MBus Concentrator
Serial Port:	Serial Port USB	Select the connected serial port
Mode:	0x09 - T2/C2-Other	W-Bus mode
Time Window:	1	Scanning window minutes (0=register every frame)
Filter: manunfacturer:	ARF	Save only devices from this manufacturer Blank if not used. Example: AMB
Logger:	☑	Check if logger must be used. Please, configure logger before using this option

ADDITIONAL NOTES

- Once the configuration is finished, press the "SAVE CONFIG" button to save the changes. Remember to restart our router for the new changes to take effect.

2.7 Other

2.7.1 Other: DynDns

The MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini are compatible with the DynDNS service and the No-IP service. If we do not have a SIM card with fixed IP address and we wish to use the external services of DynDNS or No-IP, we can configure them in this section.

- Enabled: activate this option if we wish to activate the use of DynDNS or No-IP

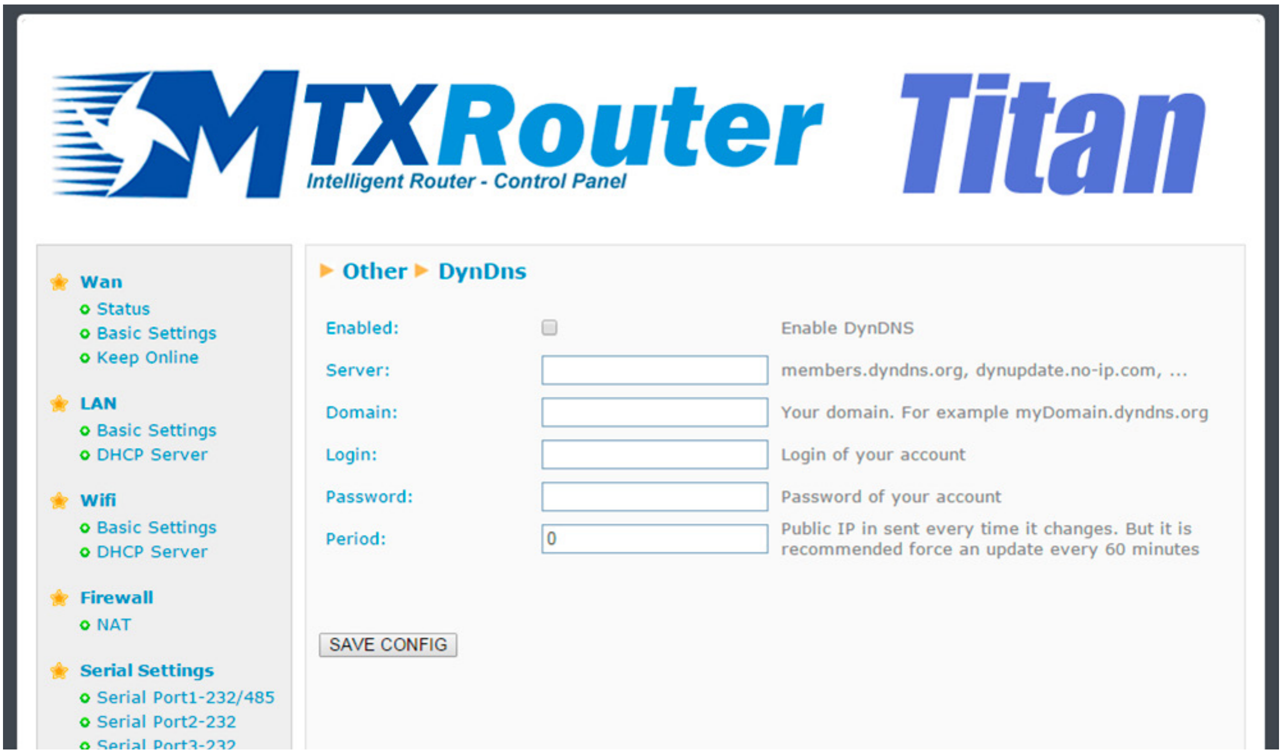
- Server: specify the service server (members.dyndns.org or dynupdate.no-ip.com)

- Domain: indicate the DNS that we have created (for example, midominio.dyndns.org)

- Login: login for our DynDNS or No-IP account

- Password: password for our DynDNS or No-IP account

- Period: the period, in minutes, that the current IP address in the DynDNS or No-IP servers should be refreshed



▶ Other ▶ DynDns

Enabled:	□	Enable DynDNS
Server:		members.dyndns.org, dynupdate.no-ip.com, ...
Domain:		Your domain. For example myDomain.dyndns.org
Login:		Login of your account
Password:		Password of your account
Period:	0	Public IP in sent every time it changes. But it is recommended force an update every 60 minutes

ADDITIONAL NOTES

- Once the configuration is finished, click "SAVE CONFIG" to save the changes. Remember that the router should be restarted for the changes to take effect.
- The IP address in the DynDNS or No-IP servers updates itself each time it is changed. However, we recommend that we use the "Period" parameter, with a value of 60 for example, so that it is sent every hour just in case.

2.7.2 Other Private DynDns

The DynDNS service allows the router's current IP address to be sent to our server in the event that we use a SIM card with a dynamic IP address. The sending of the IP address can be done via HTTP GET (JSON) or through the sending of a specific string via socket to a configurable TCP port.

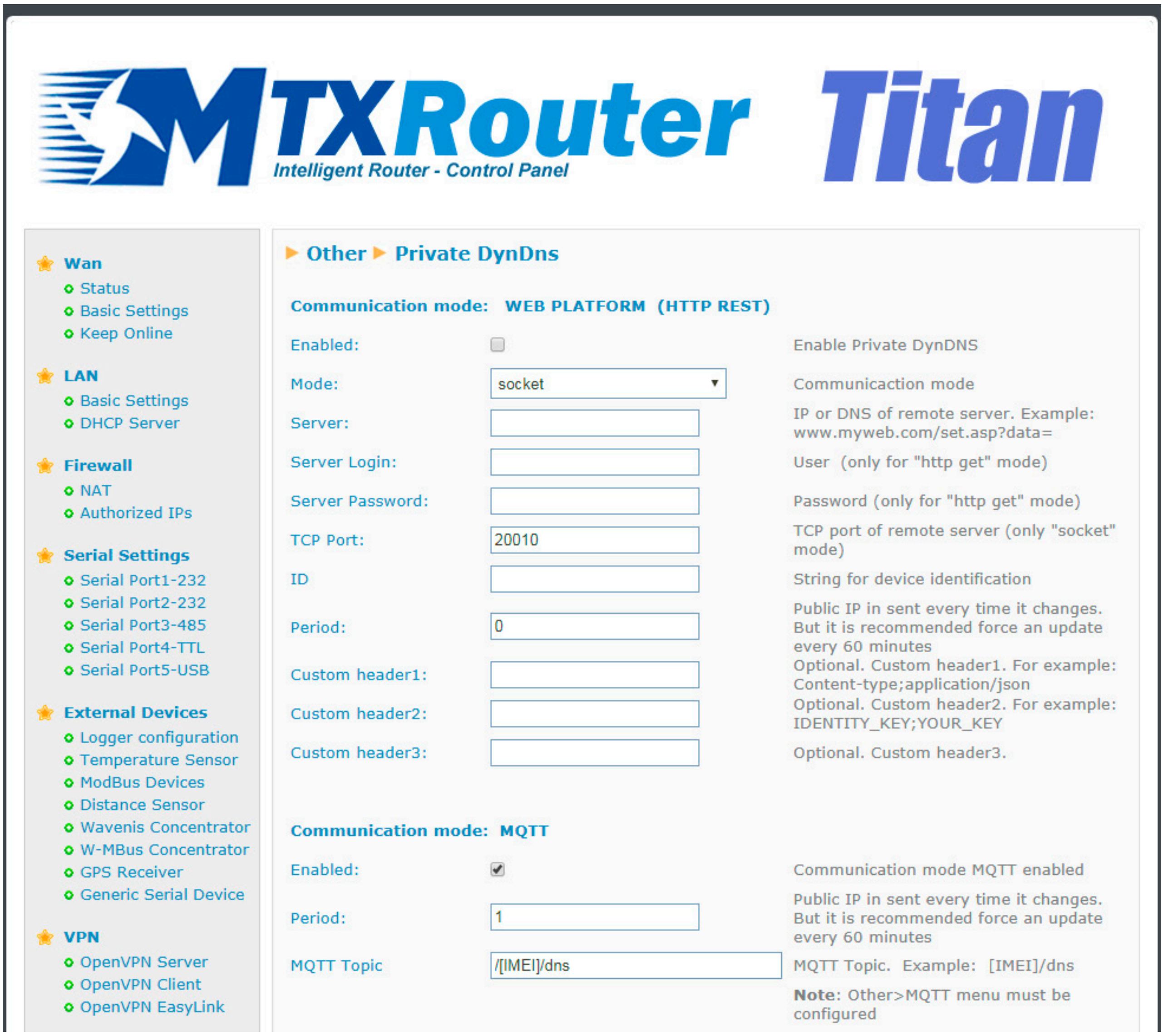
HTTP or Socket method:

- Enabled: activate this option if we wish to use the Private DNS
- Mode: we can choose between HTTP GET (JSON) or through a text string via a TCP socket
- Server: the IP or DNS where the IP is to be sent
- Server login: login for our webserver (if "http get" mode is used)
- Password: password for our webserver (if "http get" mode is used)

- TCP Port: TCP port if "socket" mode is used
- ID: ID chain (for both "http get" and "socket" mode)
- Period: period, in minutes, that the current IP address is to be refreshed in our server
- Custom header1: personalized HTTP header 1
- Custom header2: personalized HTTP header 2
- Custom header3: personalized HTTP header 3

MQTT method:

- Enabled: activate this box if we want to use MQTT
- Period: minutes to refresh the server IP address. If the public IP changes, it is immediately sent
- MQTT topic: MQTT topic used to inform with the IP



Other ▸ Private DynDns

Communication mode: WEB PLATFORM (HTTP REST)

Enabled:	□	Enable Private DynDNS
Mode:	socket	Communicaction mode
Server:		IP or DNS of remote server. Example: www.myweb.com/set.asp?data=
Server Login:		User (only for "http get" mode)
Server Password:		Password (only for "http get" mode)
TCP Port:	20010	TCP port of remote server (only "socket" mode)
ID		String for device identification
Period:	0	Public IP in sent every time it changes. But it is recommended force an update every 60 minutes
Custom header1:		Optional. Custom header1. For example: Content-type;application/json
Custom header2:		Optional. Custom header2. For example: IDENTITY_KEY;YOUR_KEY
Custom header3:		Optional. Custom header3.

Communication mode: MQTT

Enabled:	☑	Communication mode MQTT enabled
Period:	1	Public IP in sent every time it changes. But it is recommended force an update every 60 minutes
MQTT Topic	/[IMEI]/dns	MQTT Topic. Example: [IMEI]/dns
		Note: Other>MQTT menu must be configured

ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.
- Sample format of the JSON string sent:

```
{“IMEI”:”358884050088207”,”TYPE”:,”DNS”,”P”:”1234”,”IP”:”200.1.2.3”,
”RSSI”:25}
```

Where:

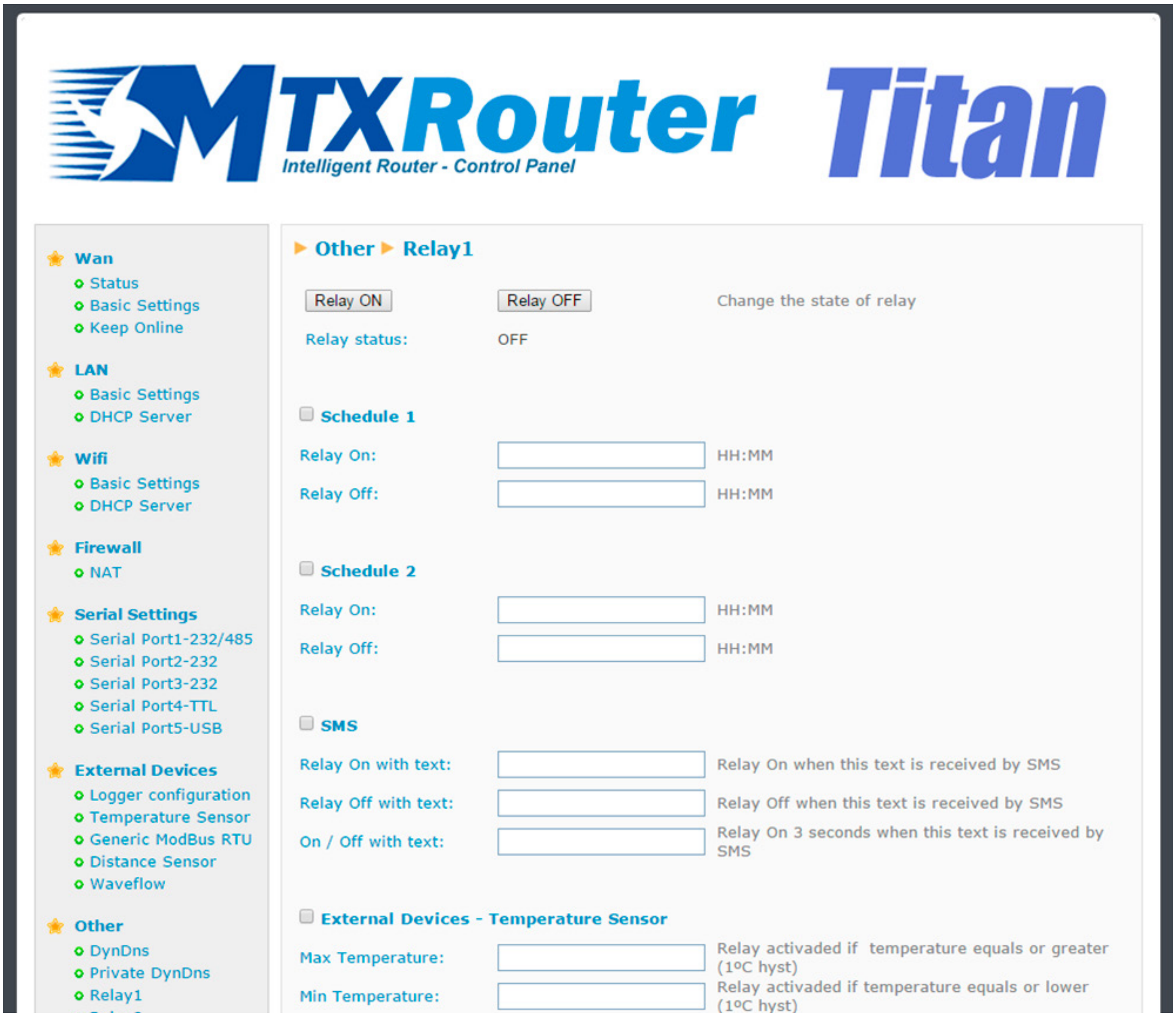
- TYPE: type of string. In this case DNS
- IMEI: router’s ID number. Unique for each device
- P: logger’s ID field (External Devices > Logger configuration)
- IP: IP of WAN interface (2G/3G)
- RSSI: 0…31 (signal strength)
- MOD: router Titan model
- Ver: FW version

2.7.3 Other: RelayX

The MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices contain relays. These relays can be changed manually via a web console, Telnet, and SMS, as well as via temporization or according to a measured temperature or distance. The different configurations are applied to each relay independently; i.e. each relay can be configured in a different way.

- Schedule1: activate this option if we wish to use schedule 1
- Schedule1 > Relay on: indicates the time the relay for schedule 1 shall change
- Schedule1 > Relay off: indicates the time the relay for schedule 1 shall change
- Schedule2: activate this option if we wish to use schedule 2
- Schedule2 > Relay on: indicates the time the relay for schedule 2 shall change
- Schedule2 > Relay off: indicates the time the relay for schedule 2 shall change
- SMS: activate this option if we wish to change relays by sending an SMS
- SMS > Relay On with text: SMS text used to activate the relay
- SMS > Relay Off with text: SMS text used to deactivate the relay
- SMS > On / Off with text: SMS text used to activate the relay for 3 seconds. Used to carry out resets of external devices with just one SMS
- External Devices > Temperature Sensor: activate this option if we wish to change a relay according to the temperature of a sensor connected to the router’s serial port

- External Devices > Temperature Sensor > Max Temperature: maximum temperature, after which the relay is activated. The hysteresis is 1 degree
- External Devices > Temperature Sensor > Min Temperature: minimum temperature, after which the relay is activated. The hysteresis is 1 degree
- External Devices > Distance Sensor: activate this option if we wish to change a relay according to the distance of a Maxbotix sensor connected to the router's serial port
- External Devices > Distance Sensor > Max Distance: maximum distance, after which the relay is activated. The hysteresis is 25cm
- External Devices > Distance Sensor > Min Distance: minimum distance, after which the relay is activated. The hysteresis is 25cm
- Jamming detection: activate this option if we want to change the relays when suspect jamming (GSM inhibitor) is detected
- Jamming > Seconds: how often the relay should be activated after suspect jamming is detected
- Astronomical clock: activate this option if we wish to change relays via an astronomical clock (the exact time of sunrise or sunset)
- Astronomical clock > Titan Latitude: in this field indicate the latitude of where the Titan is located for the astronomical clock calculations
- Astronomical clock > Titan Longitude: in this field indicate the longitud of where the Titan is located for the astronomical clock calculations
- Movement Detection: activate this option if we wish to change the relay when movement is detected (only available for Titan mini models)
- Movement Detection > Seconds: time (in seconds) during which the relay will be active after detecting movement
- GPS Area: activate this option if we wish to change the relay when the Titan router is located within a GPS area defined in the section "External Devices > GPS Receiver"
- BTC (Experimental): activate this option if we wish to change the relay when a bank transfer is detected in a specified Bitcoin address
- BTC > Address: incoming Bitcoin address
- BTC > Confirmations: number of necessary confirmations
- BTC > Price: number of Bitcoins per second that activate the relay. For example, if the price is 0.001, an incoming transfer of 0.060 BTC would activate the relay for 60 seconds
- Logger: activate this option if we wish to register and send the changes of a relay to our website via a JSON object



▸ Other ▸ Relay1

Change the state of relay

Relay status: OFF

□ Schedule 1

Relay On: HH:MM

Relay Off: HH:MM

□ Schedule 2

Relay On: HH:MM

Relay Off: HH:MM

□ SMS

Relay On with text: Relay On when this text is received by SMS

Relay Off with text: Relay Off when this text is received by SMS

On / Off with text: Relay On 3 seconds when this text is received by SMS

□ External Devices - Temperature Sensor

Max Temperature: Relay activaded if temperature equals or greater (1ºC hyst)

Min Temperature: Relay activaded if temperature equals or lower (1ºC hyst)

ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.
- Sample format of the JSON string sent:

```
{“IMEI”:”354740050367237”,”TS”:”17/02/2014 19:02:46”,”TYPE”:”RELAY”,
“P”:”1234”,”ID”:1,”VAL”:0,”WHY”,”AT”,WHYH”,””}
```

Where:

- IMEI: router’s ID number. Unique for each device
- TS: time stamp DD:MM:YYYY HH:MM:SS
- TYPE: type of string. In this case modbus

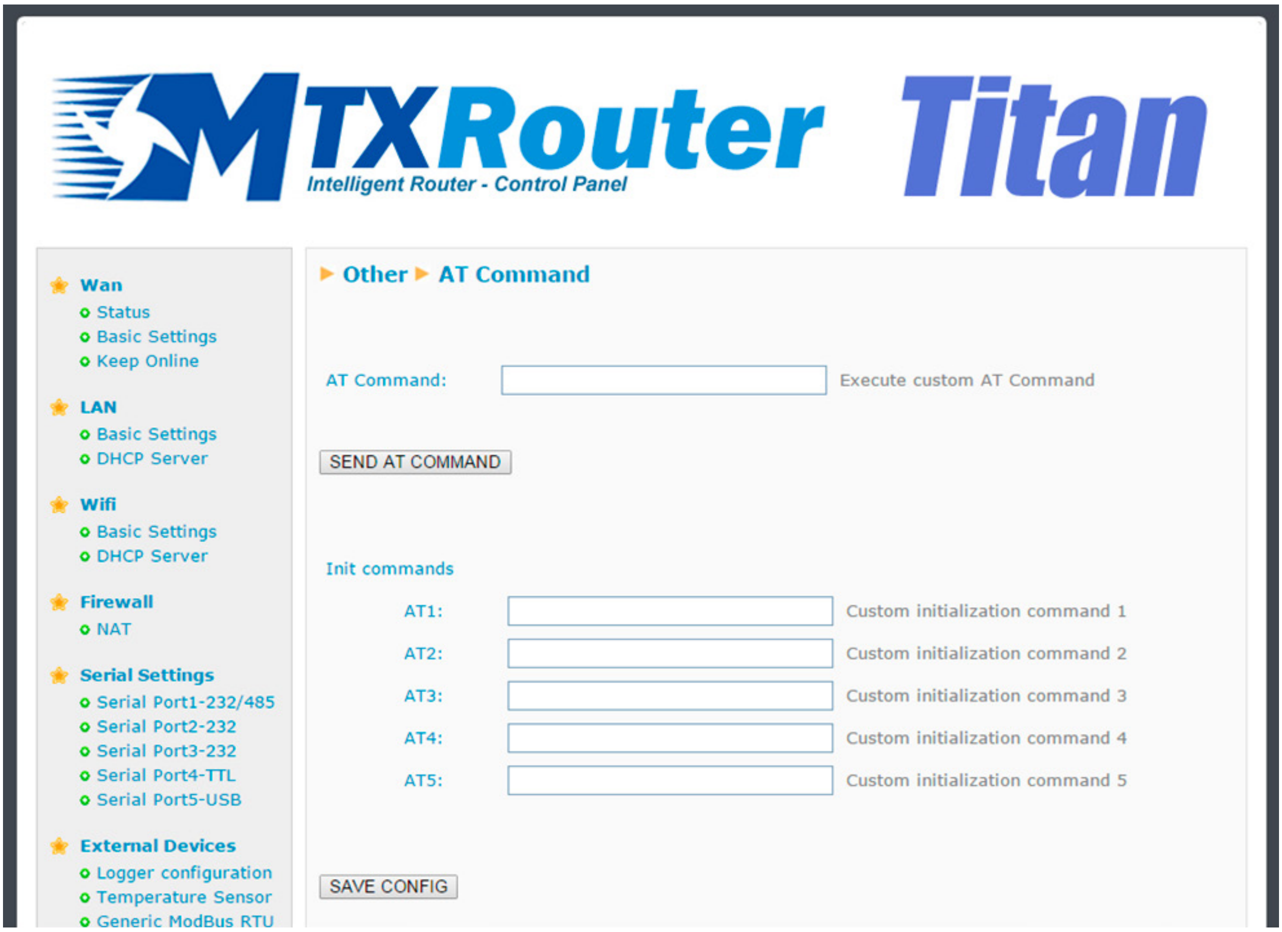
- P: logger’s ID field (External Devices > Logger configuration)
- ID: relay ID (0 or 1)
- WHY: reason why the relay has been changed
    - “SCHE1” > relay changed because of Schedule 1
    - “SCHE2” > relay changed because of Schedule 2
    - “TEMP” > relay changed because of temperature
    - “DIST” > relay changed because of distance
    - “AT” > relay changed because of AT command
    - “JAMM” > relay changed because of suspect jamming
    - “ACCEL” > relay changed because of detected movement
    - “GPS” > relay changed because of the GPS cell
    - “ASTRO” > relay changed because of the astronomic relay
    - “BITCOIN” > relay changed because of a received transfer
- WHYH: if the relay has been changed due to temperature or distance, indicate the temperature or distance that caused the change

2.7.4 Other: AT Command

In this section it is possible to send an AT command directly to the router’s internal modem. For example, it could be interesting to check the network coverage, identify the telephone cells in the area, etc.

It is also possible to configure up to five special AT commands which can be used to configure the router upon startup.

- AT Command: AT command for real time execution (for example AT+CSQ). Once “SEND AT COMMAND” is clicked, the command will be executed
- AT1… AT5: start up AT commands



▸ Other ▸ AT Command

AT Command: Execute custom 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

ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.

2.7.5 Other: SMS Control

This section allows we to configure the router control via SMS or a missed call. For example, we can configure it so that the router connects to 3G after receiving an SMS, or we can specify the telephone numbers authorized for this.

- SMS enabled: activate this option if we wish to be able to activate a 2G/3G connection temporarily in the router after an SMS is received. Watch out! The SMS command must be specified

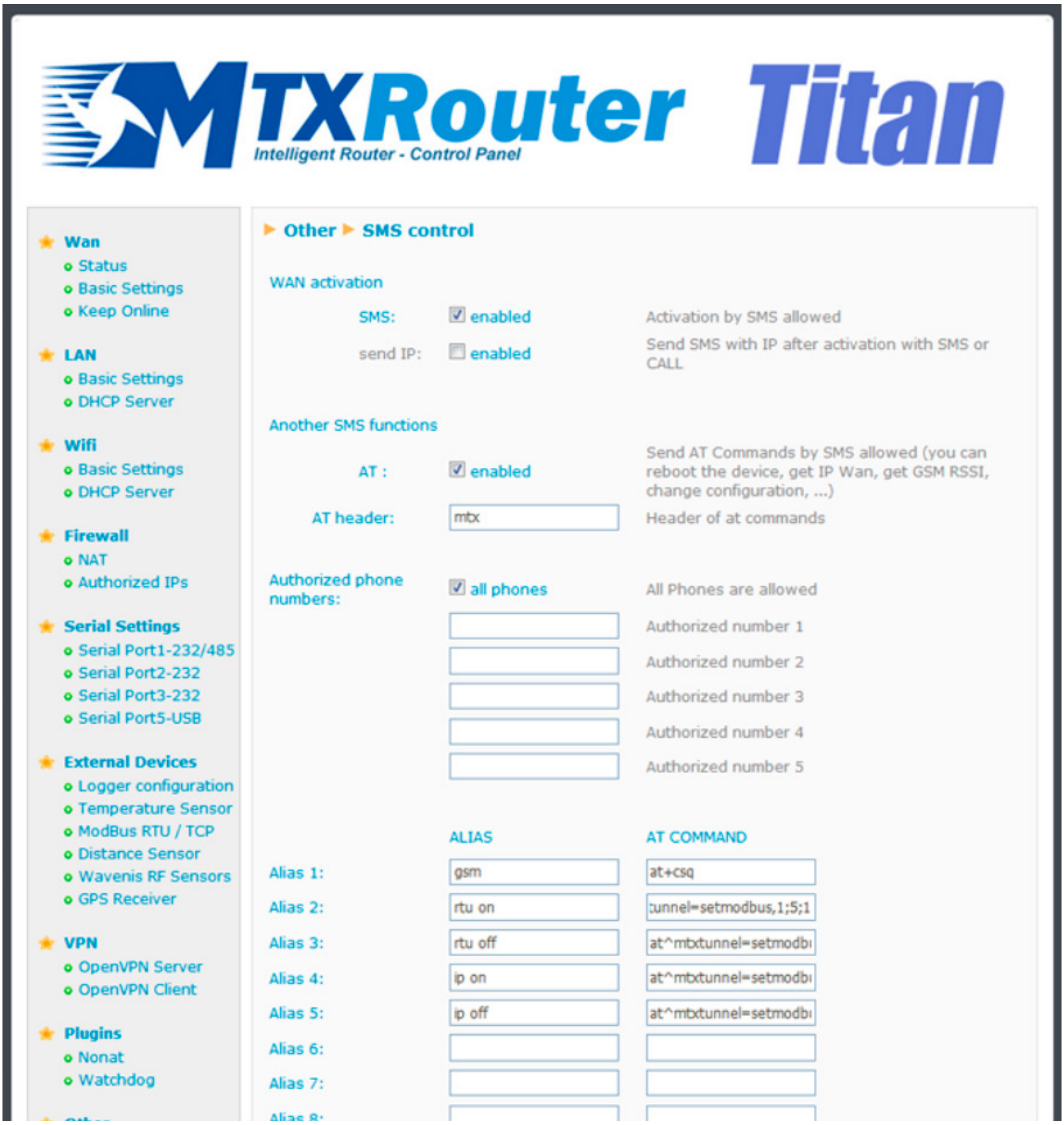
- Call enabled: activate this option if we wish to be able to activate a 2G/3G connection temporarily after a missed call is received. Ideal for telemaintenance where a connection to the router is only required at certain times

- Send IP: activate this option if we want the router to send an SMS with the IP address obtained after the SMS or missed call caused a connection to be made

- AT enabled: activate this option if we wisht o be able to send AT commands via SMS to the router, for example to find out the network coverage remotely, to carry out a reset, change a configuration, etc.
- AT header: write here the header text for the command SMS messages. For example, if we write “mtx” in this box, when an AT command is sent via SMS, let’s say the ATI command which is used to find out the router’s internal module, we would need to send an SMS with the text “mtx ATI”
- All phones: activate this option if we want all telephones to be able to send AT commands to the router. Do not activate this option if we only want a specified number of authorized telephones
- Authorized number X: in these boxes we can specify up to five authorized telephones

For firmware versions 3.x or later:

- Alias/ATCommand: up to 10 aliases can be introduced for the execution of AT commands. For example, if we wish to send an SMS to update a Modbus register on an external device, we can create an alias so that whenever the MTX device receives the text “reg on”, the AT command “at^mtxtunnel=setmodbus,1;5;2” is executed, writing the value “2” in register number 5 for the Modbus device with address 1
- Alias Result OK: text to be sent as a response when the execution of an alias command is successful. If required, a personalized response for each alias can created by indicating the response between the tags <a1>Ok</a1><a2>Perfect</a2>
- Alias Result ERROR: text to be sent as a response when the execution of an allias command produces an error. If required, a personalized response for each alias can created by indicating the response between the tags <a1>Error</a1><a2>Oops</a2>



▶ Other ▶ SMS control

WAN activation

SMS: ☑ enabled — Activation by SMS allowed

send IP: □ enabled — Send SMS with IP after activation with SMS or CALL

Another SMS functions

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

AT header: mtx — 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

	ALIAS	AT COMMAND
Alias 1:	gsm	at+csq
Alias 2:	rtu on	:unnel=setmodbus,1;5;1
Alias 3:	rtu off	at^mtxtunnel=setmodbi
Alias 4:	ip on	at^mtxtunnel=setmodbi
Alias 5:	ip off	at^mtxtunnel=setmodbi
Alias 6:		
Alias 7:		
Alias 8:		

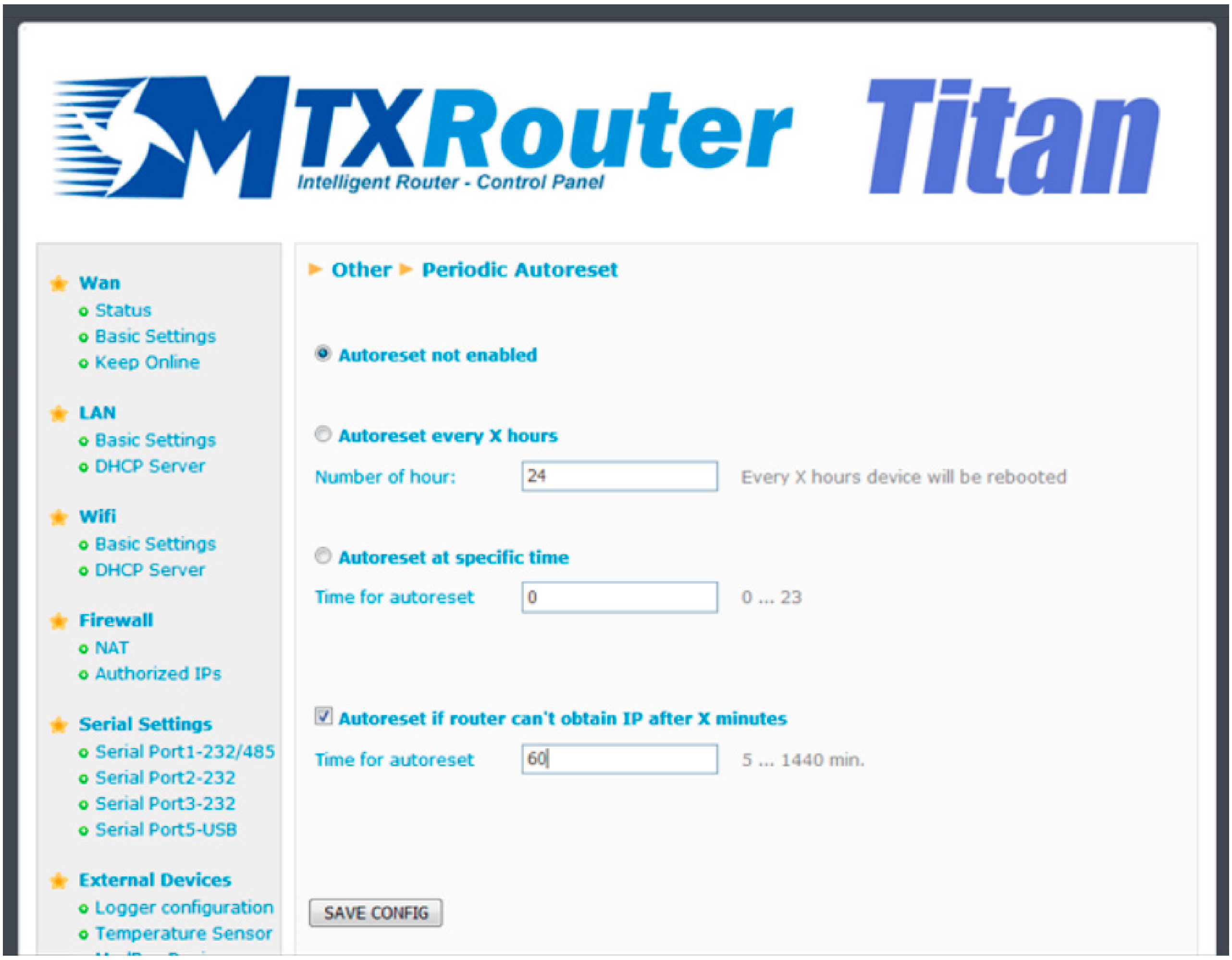
ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.
- Consult the Application Note ALIAS SMS for further information and examples.

2.7.6 Other: Periodic Autoreset

In this section we can configure a programmed autoreset of the router.

- Autoreset not enabled: activate this option if we do not want the router to reset automatically
- Autoreset every X hours: activate this option if we want the router to reset itself every X hours
- Number of hours: if we decide we want the router to reset itself every X hours, we need to specify in this box the frequency, in hours, of the reset. For a daily reset, input “24”
- Auturoreset at specific time: select this option if we want the router to reset itself a specific time of the day
- Time for autoreset: if we choose the previous option, specify here the time of reset
- Autoreset if router can’t obtain IP after X minutes: this option is highly recommended for situations where context can be lost. The option allows we to specify how long the router should wait after not being able to obtain an IP address before resetting itself



► Other ► Periodic Autoreset

● Autoreset not enabled

○ Autoreset every X hours

Number of hour: 24 Every X hours device will be rebooted

○ Autoreset at specific time

Time for autoreset 0 0 ... 23

☑ Autoreset if router can't obtain IP after X minutes

Time for autoreset 60 5 ... 1440 min.

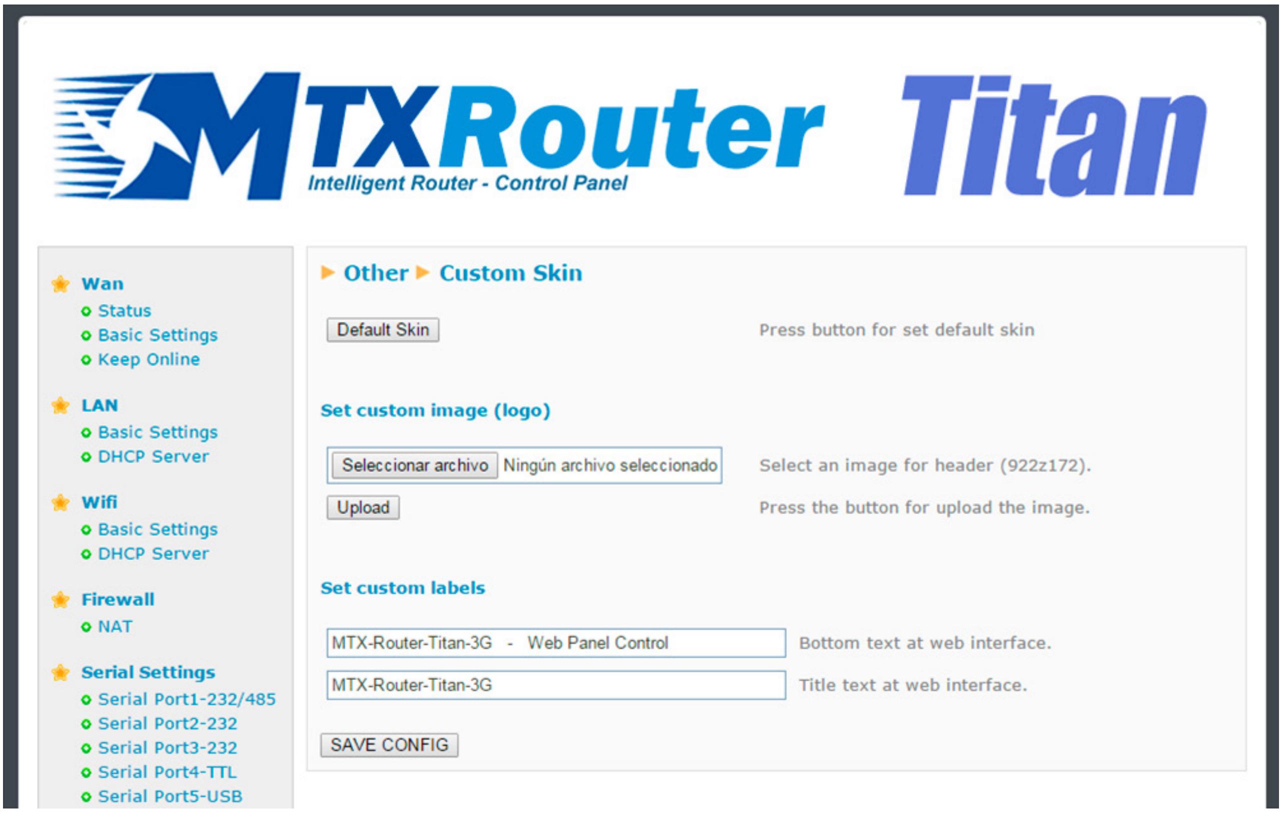
ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.

2.7.7 Other: Custom Skin

The router’s software allows we to configure the router with our own logos in the header of the web configuration, as well as using customized titles and footers. This allows we to give a personalized feel to the product.

- Set custom image: select an image with 922 x 172 pixels (tipo gif) for the header
- Set custom labels: input the text that we want to appear in the title and the footer



Other ▸ Custom Skin

Default Skin — Press button for set default skin

Set custom image (logo)

Seleccionar archivo Ningún archivo seleccionado — Select an image for header (922z172).

Upload

Press the button for upload the image.

Set custom labels

MTX-Router-Titan-3G - Web Panel Control — Bottom text at web interface.

MTX-Router-Titan-3G — Title text at web interface.

SAVE CONFIG

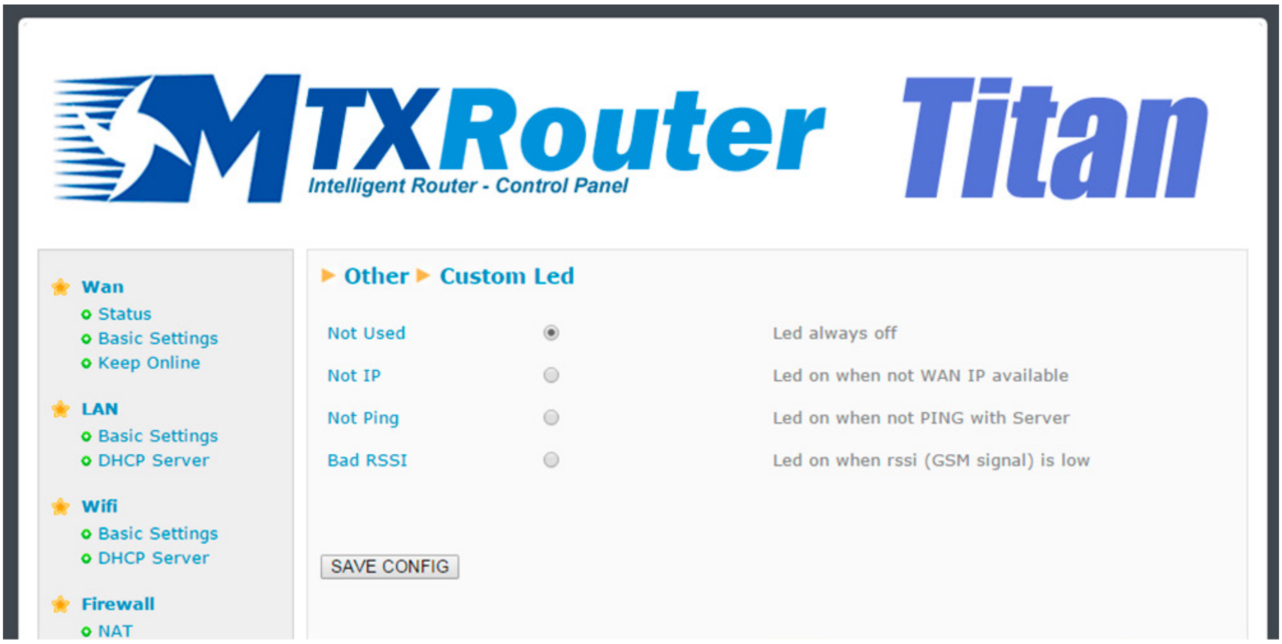
ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes.
- Remember that if we configure the router with our own header and customized texts for third party users, it is not necessary to use the section “Other > User Permissions”. This section is to be used for when the user does not have access to the section “Other > Custom Skin”.

2.7.8 Other: Custom LED

Both the MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices have a red LED which can be configured. In this section we can specify how it is to be used according to our needs.

- Not used: the LED will always be switched off, without use
- Not IP: the red LED will light up whenever the router does not have an assigned WAN IP address
- Not ping: the red LED will light up whenever the router does not receive a response to a PING configured in the “WAN” section (the ping that checks connectivity)
- Bad RSSI: the red LED will light up when the network coverage is weak, providing a sign that it would be better to move the antenna or use a higher power



▶ Other ▶ Custom Led

Not Used	●	Led always off
Not IP	○	Led on when not WAN IP available
Not Ping	○	Led on when not PING with Server
Bad RSSI	○	Led on when rssi (GSM signal) is low

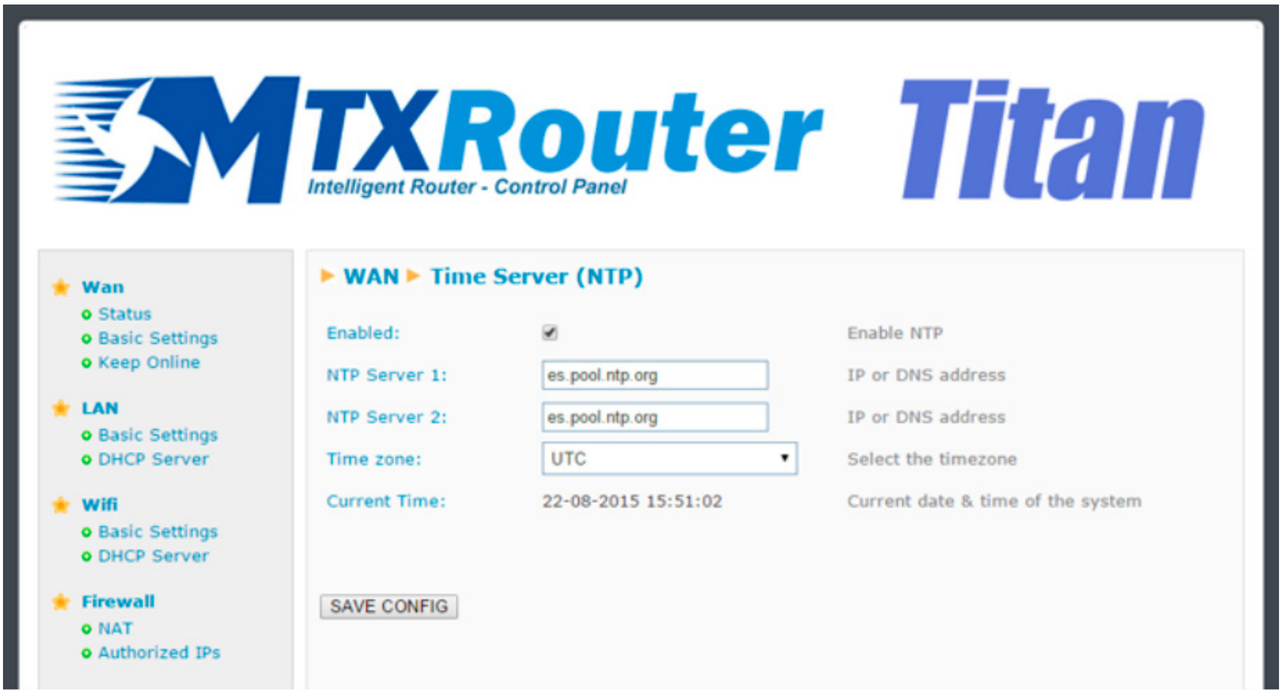
ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.

2.7.9 Other: Time Server (NTP)

The router has a real time clock that allows time to be kept in the event of a loss of power. This clock may periodically require synchronization with time servers via NTP protocol.

- Enabled: activate this option if we wish to use the NTP time servers
- NTP server 1: IP address or DNS of time server 1
- NTP server 2: IP address or DNS of time server 2



WAN ► Time Server (NTP)

Enabled:	☑	Enable NTP
NTP Server 1:	es.pool.ntp.org	IP or DNS address
NTP Server 2:	es.pool.ntp.org	IP or DNS address
Time zone:	UTC	Select the timezone
Current Time:	22-08-2015 15:51:02	Current date & time of the system

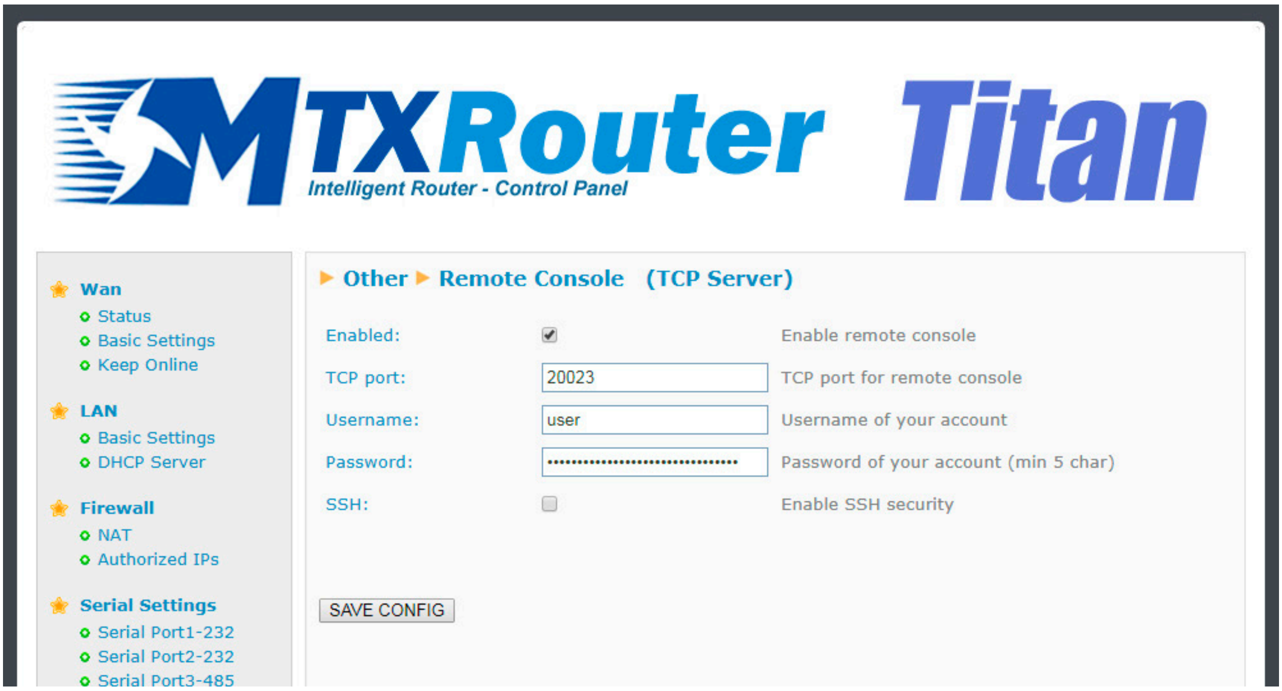
ADDITIONAL NOTES

- Once the configuration is finished, click "SAVE CONFIG" to save the changes. Remember that the router should be restarted for the changes to take effect.
- For firmware versions 2.05 or later, it is possible to specify the time zone. Previous firmware versions uso UTC time only.

2.7.10 Other: Remote Console

If at any time we need to carry out a special operation on the router via a Telnet-type connection, we can do so using this section. With this special connection we can send an SMS, change the router's configuration, change a relay, etc. by sending AT commands via a Telnet-type connection. Look at section 5 of this manual for a list of AT commands available.

- Enabled: activate this option if we want to use this special connection
- TCP Port: router's listening TCP port where the connection should be made
- Login: username that will be required after a connection is made
- Password: password that will be required after a connection is made
- SSH: activate this box if we want to use SSH instead of Telnet



► Other ► Remote Console (TCP Server)

Enabled:	☑	Enable remote console
TCP port:	20023	TCP port for remote console
Username:	user	Username of your account
Password:	••••••••••••••••••••••••••••••••	Password of your account (min 5 char)
SSH:	□	Enable SSH security

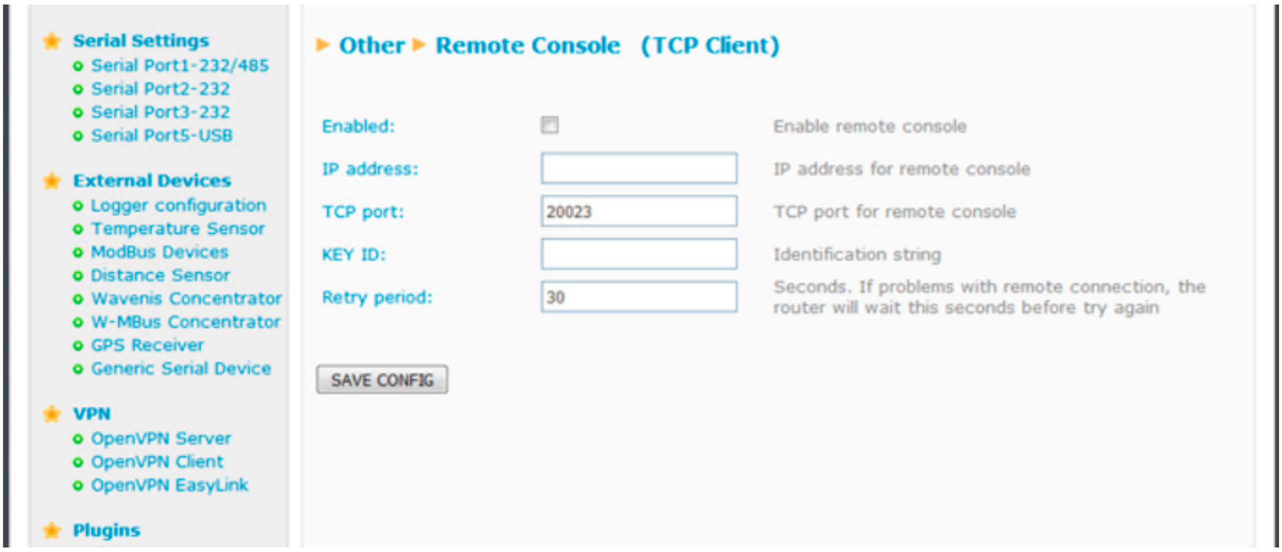
ADDITIONAL NOTES

- Once the configuration is finished, click "SAVE CONFIG" to save the changes. Remember that the router should be restarted for the changes to take effect. In case we activate/deactivate the SSH box, let's make sure we also re-enter the password
- The remote access to the console can be carried out on a local level (Ethernet or WiFi) or remotely via a 2G/3G connection

2.7.10b Other: Remote console (TCP Client)

If we ever need to perform any special operations on the router through a “Telnet-like” connection, we can do so by configuring this section. That is, with this special connection we can, by sending AT commands through a telnet connection, send an SMS, make a change of router configuration, switch a relay, etc. Refer to section 5 of this manual for the list of available AT commands.

- Enabled: check this box if we want to use the remote console in TCP Client mode
- IP address: Remote IP address to which the Titan router will be connected.
- TCP Port: The remote TCP port to which the Titan router will connect.
- KEY ID: identifying text. The first will send the router through the socket.
- Retry period: Seconds. In case of socket drop, it allows to indicate the time to start a new connection attempt



▶ Other ▶ Remote Console (TCP Client)

Enabled:	□	Enable remote console
IP address:		IP address for remote console
TCP port:	20023	TCP port for remote console
KEY ID:		Identification string
Retry period:	30	Seconds. If problems with remote connection, the router will wait this seconds before try again

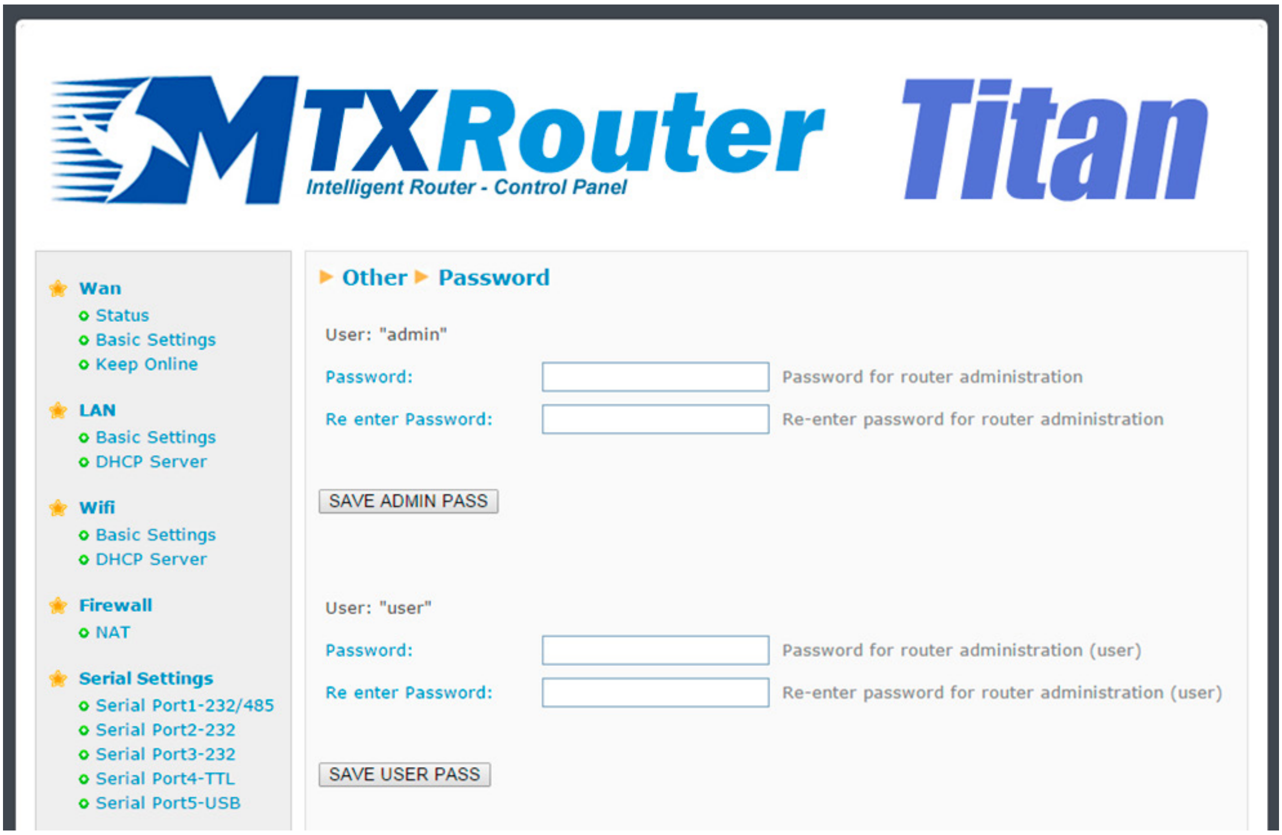
ADDITIONAL NOTES

- Once the configuration is finished press the “SAVE CONFIG” button to save the changes. Remember to restart our router for the new changes to take effect.
- The AT commands sent in “TCP Client” mode, for reasons of compatibility, must be encapsulated between the <MTXTUNNELR> </ MTXTUNNELR> tags. For example, to get the time:

```
<MTXTUNNELR> AT ^ MTXTUNNEL = GETTIME </ MTXTUNNELR>
```

2.7.11 Other: Passwords

There are two usernames that can be used to access the router’s configuration. The username “admin”, from which we will have access to the entire configuration, and “user” from which we will have access to only the selected configurations (useful for when the router is personalized we’re our logos). In this section we can change the password for both users. The “guest” user will allow us to access the same menus “user” does, but without the ability to change the configuration.



▶ Other ▶ Password

User: "admin"

Password: [ ] Password for router administration

Re enter Password: [ ] Re-enter password for router administration

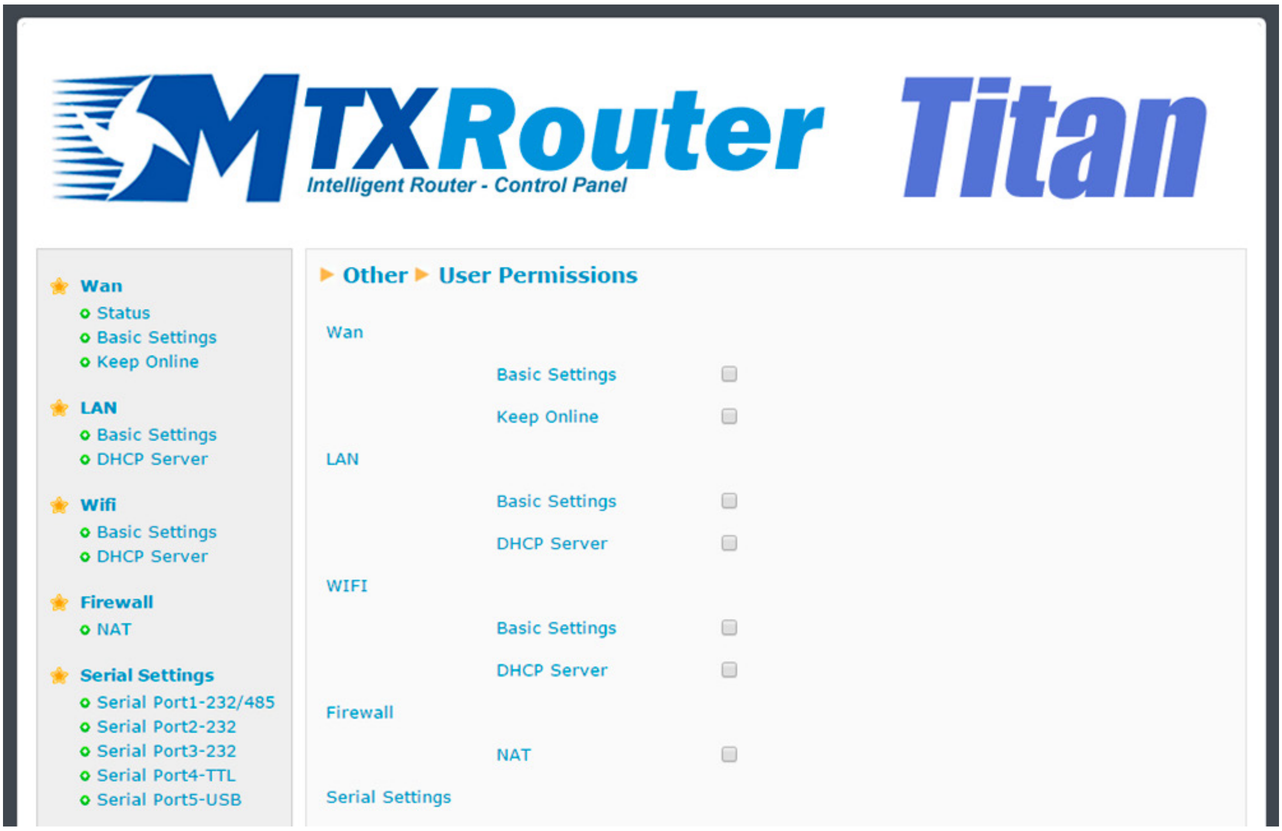
User: "user"

Password: [ ] Password for router administration (user)

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

2.7.12 Other: User Permissions

In this section we can configure the permissions for the users that use the “user” account. The configuration options that are not selected will not appear in the left-hand menu for the “user” account.



Other ▶ User Permissions

Wan

- Basic Settings □
- Keep Online □

LAN

- Basic Settings □
- DHCP Server □

WIFI

- Basic Settings □
- DHCP Server □

Firewall

- NAT □

Serial Settings

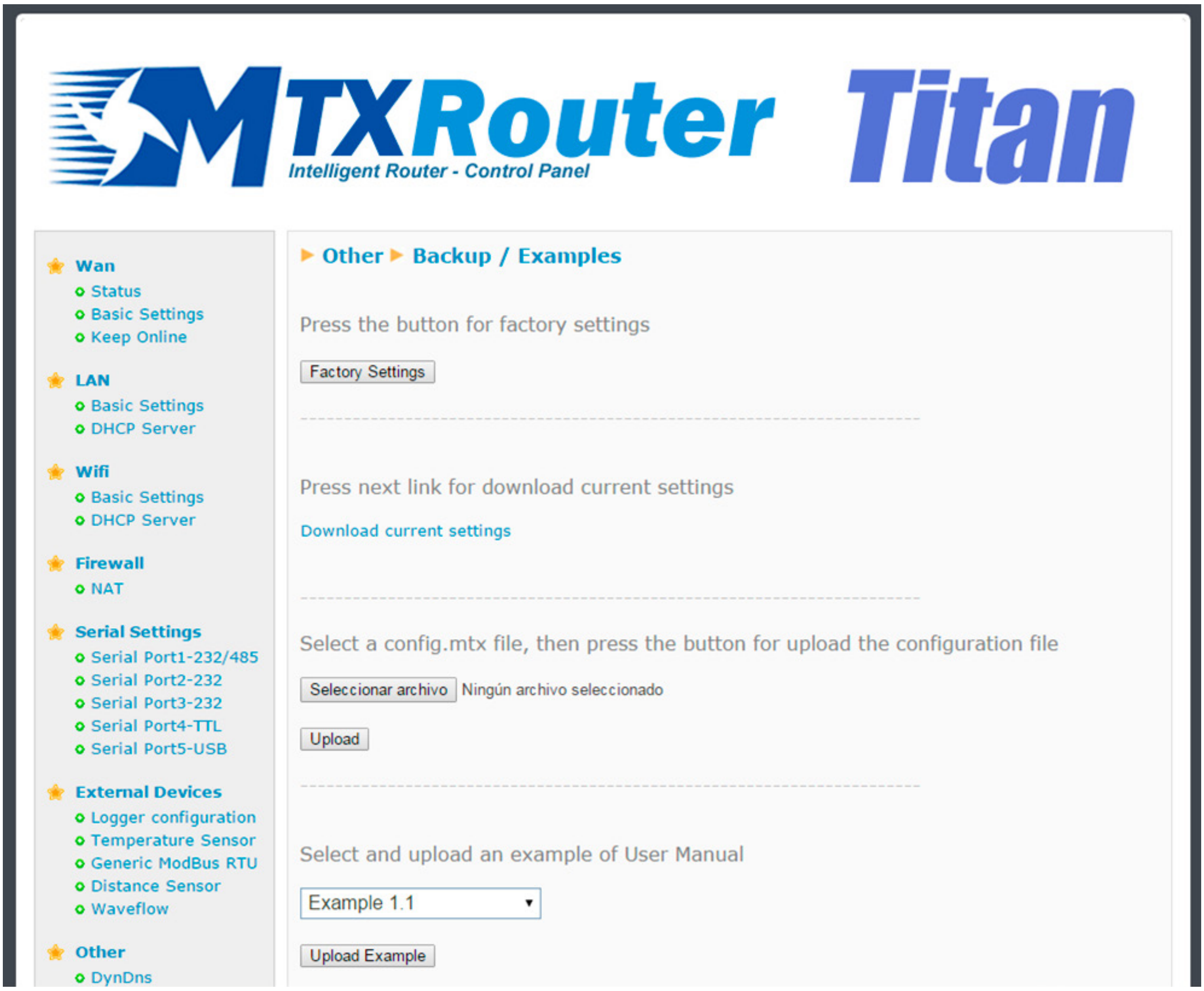
ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.

2.7.13 Other: Backup/Examples

We can create a complete security copy of the router's configuration from this menu. We can save the configuration in a file and in the router whenever needed. It also allows we to load the user manuals quickly and easily.

- "Factory Settings" button: press this button if we want to restore the router to its factory settings
- "Download settings" link: press this link to download the router's configuration in a file with the name "config.mtx"
- "Upload" button: to carry out a restoration according to a saved configuration, press this button to load the file after having indicated which file to use
- "Upload Example" button: this allows we to load the example configuration of the user manual



▶ Other ▶ Backup / Examples

Press the button for factory settings

Press next link for download current settings

Select a config.mtx file, then press the button for upload the configuration file

Ningún archivo seleccionado

Select and upload an example of User Manual

Example 1.1

ADDITIONAL NOTES

- We can also restore the router to its factory settings using a micro-switch located on the router.

Procedure for the MTX-Router-Titan mini Device

Open the SIM card compartment where we will see eight micro-switches. Make sure the router is switched off and place micro-switch 8 to the ON position and turn the router on. One minute after it starts-up, the red LED will flash to indicate that the factory settings have been restored. Disconnect the power source and return micro-switch 8 to the OFF position. Remember that the default IP address of the router is 192.168.1.2 and the login is “admin” and the password is “admin”. In “Hardware” section we will find more information about micro-switches.

Procedure for the MTX-Router-Titan-3G Device

Open the casing of the device where we will see two chips (SW1 and SW2), each with eight micro-switches. Make sure the router is switched off and place SW1’s micro-switch 1 to the ON position and turn the router on. One minute after it starts-up, the red LED will flash to indicate that the factory settings have been restored. Disconnect the power source and return SW1’s micro-switch 1 to the OFF position. Remember that the default IP address of the router is 192.168.1.2 and the login is “admin” and the password is “admin”. In “Hardware” section we will find more information about micro-switches.

Procedure for the MTX-Router-Titan II

Turn off the router and connect the digital input number 3 (marked with “3” on the green switch) to GND (marked with “-” on the green switch). Connect the router to a power input and 1 minute after the start, the led 1 will blink signaling that the default configuration has been restored. Remove the connection to the power input, disconnect the digital input 3 from GND and turn on the router. Remember the router default IP address is 192.168.1.2 with login “admin” and password “admin.”

Procedure for the MTX-Router-Titan II-R

With the router turned off, set switch number 2 to ON (down). You will find the swtich in the front of the router). Then power the router. After startup, after 1 minute, the upper green LED will flash intermittently, signaling that the factory settings have been restored. Turn off the power to the router, turn switch 2 back to OFF, and turn the router on again. Remember that the default IP address of the router is 192.168.1.2 with login “admin” and password “admin”.

2.7.14 Other: Digital Input X

This option is only available for those Titan mini devices that contain 1 digital input by default (customized versions with 2 digital inputs can be ordered). The digital input allows we to make a phone call to a cell phone or to send an SMS alert upon detection of changes in the input. It can also be used as a pulse counter; for example, it can be used to automatically send the count to a server via HTTP or FTP.

- Mode:

  Disabled if we do not want to use this option

  Pin 0 > 1 If we want the change of PIN from “0” to “1” to be considered an alarm

  Pin 1 > 0 If we want the change of PIN from “1” to “0” to be considered an alarm

  Pulse counter: this option allows we to use the digital input as a pulse counter (counting eah time contact is made with the input)

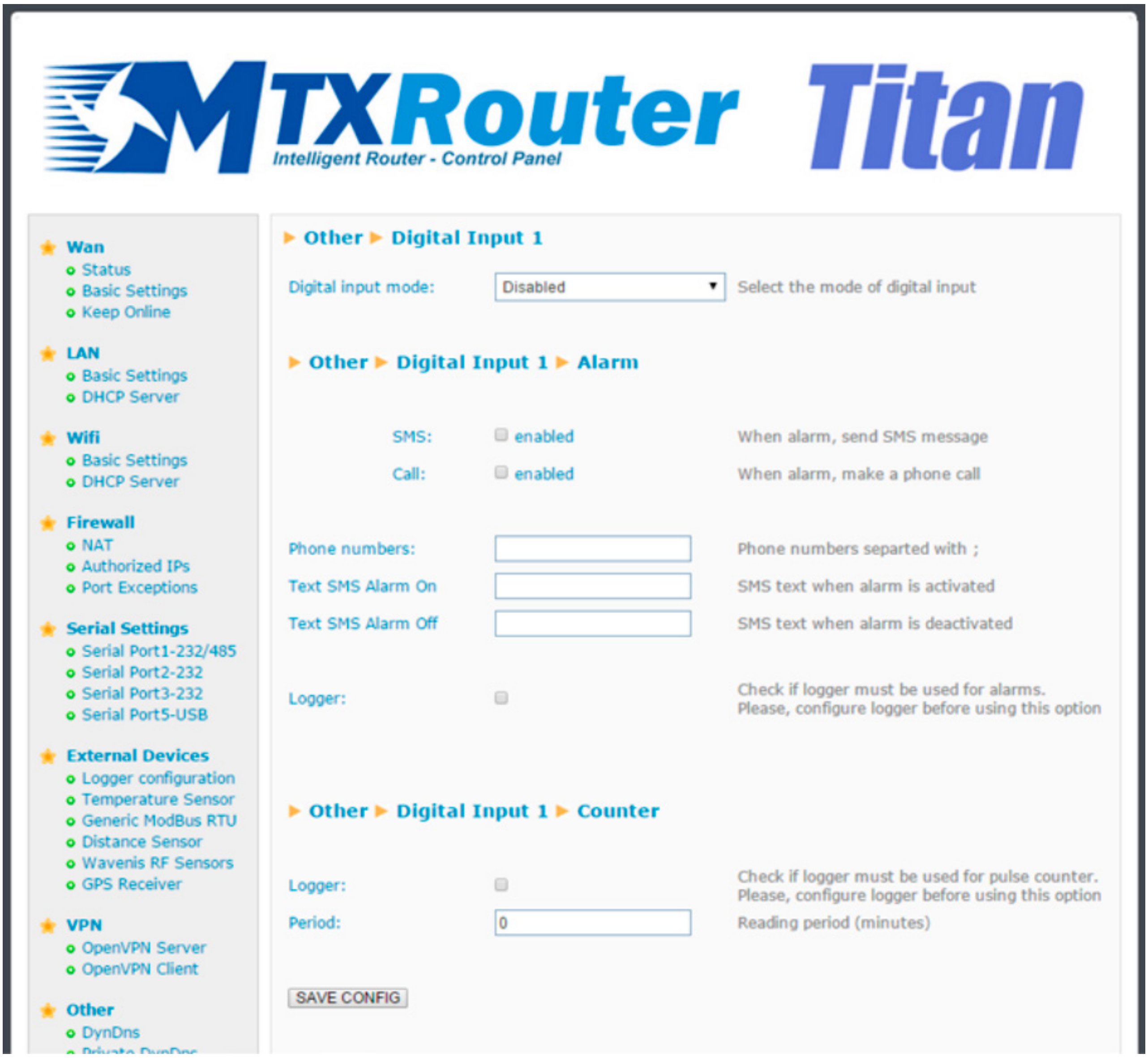
WAN session: in case there is no Titan router permanent connection configured, we could activate/deactivate the Titan router data session by activating/deactivating the digital input

Parameters used to configure the digital input as an alarm:

- SMS: select this option if we want to send an SMS alart when a change is detected
- Call: select this option if we want to make a call as an alarm when a change is detected
- Phone numbers: we can enter up to 5 telephone numbers to make calls or send SMS alarms
- Text SMS Alarm On: if we choose to send SMS alarms, the text inputted here will be sent when the alarm is activated
- Text SMS Alarm Off: if we choose to send SMS alarms, the text inputted here will be send when the alarm is deactivated
- Logger: activate this option if we want the data to be stored in the device's internal Logger to send it to the web platform or FTP server

Parameters used to configure the digital input as a pulse counter:

- Logger: activate this option if we want the data to be stored in the device's internal Logger to sent it to the web platform or FTP server
- Period: indicate the frequency (in minutes) with which the data from the pulse counter will be stored in the internal Logger. For example, a value of 1440 means the data will be stored every 24 hours (which also means the logger will send the data to the web platform via HTTP or FTP every 24 hours)



▸ Other ▸ Digital Input 1

Digital input mode: Disabled ▾ Select the mode of digital input

▸ Other ▸ Digital Input 1 ▸ Alarm

SMS: □ enabled When alarm, send SMS message

Call: □ enabled When alarm, make a phone call

Phone numbers: Phone numbers separted with ;

Text SMS Alarm On SMS text when alarm is activated

Text SMS Alarm Off SMS text when alarm is deactivated

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

▸ Other ▸ Digital Input 1 ▸ Counter

Logger: □ Check if logger must be used for pulse counter. Please, configure logger before using this option

Period: 0 Reading period (minutes)

ADDITIONAL NOTES

- Once the configuration is finished, click "SAVE CONFIG" to save the changes. Remember that the router should be restarted for the changes to take effect.
- Sample format of the JSON string sent when the Logger option is chosen:

```
{"IMEI":"354740050367237","TS":"17/02/2014 19:02:46","TYPE":"DINPUT",
"P":"1234","VAL":0,"ID:1,"COUNT":0}
```

Where:

- IMEI: the router's ID number. Unique for each device

- TS: time stamp DD:MM:YYYY HH:MM:SS
- TYPE: data type. in this case digital input
- P: logger ID field (external devices > logger configuration)
- VAL: 1: activated/0: deactivated
- ID: 1: digital input 1/2: digital input 2
- COUNT: if configured as a pulse counter, this value returns the number of pulses counted

2.7.15 Other: Jamming Detection

The MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices can be configured to detect possible cases of jamming and take the appropriate action. That is, the Titan devices are capable of detecting suspect interference caused by possible GSM/GPRS inhibitors. This can be useful for some security applications. This option is not available for 4G models.

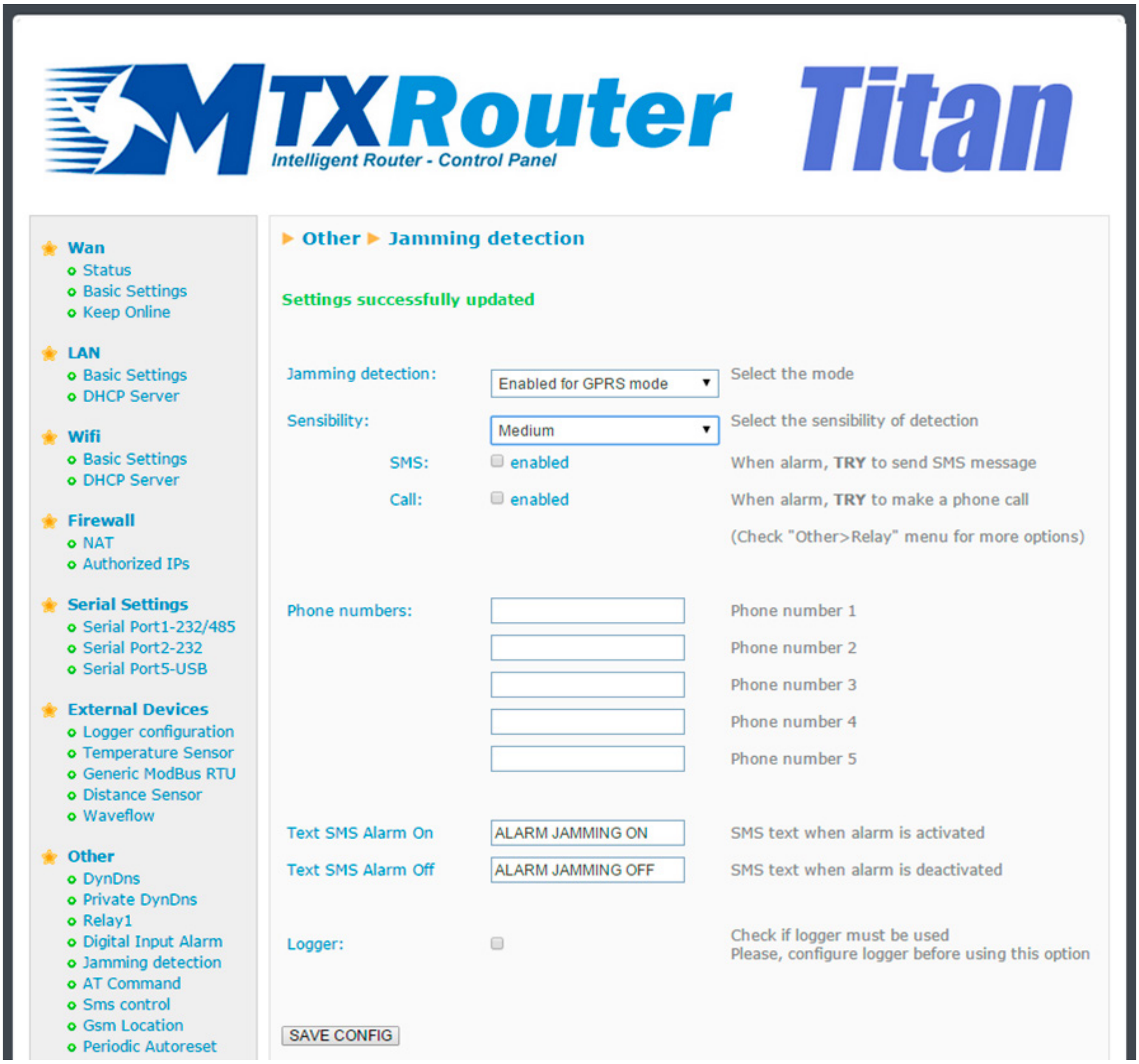
If jamming is detected, the routers can do three things: change a relay for a specific period of time that can be configured (for example to connect a light/sound signal), make a GSM call or send an SMS alert.

Remember that sending an SMS or making a GSM call is not always going to be possible given that it depends on the intensity of the jamming. If the jamming signal intensity is low (either because the intruder is getting closer or nearer), an SMS can be sent. If there is an intense level of jamming, the sending of an SMS will be impossible.

- Detection mode:

  "Disabled" if we do not want to use this option

  "Enabled for GPRS" if we want to activate jamming detection for GSM/GPRS networks
- Sensibility: select between low, medium or high sensitivity. Better detection is achieved with high sensitivity, although some false positives could occur
- SMS: select this option if we want to send an SMS alart when a change is detected
- Call: select this option if we want to make a call as an alarm when a change is detected
- Phone numbers: we can enter up to 5 telephone numbers to make calls or send SMS alarms
- Text SMS Alarm On: if we choose to send SMS alarms, the text inputted here will be sent when the alarm is activated
- Text SMS Alarm Off: if we choose to send SMS alarms, the text inputted here will be send when the alarm is deactivated
- Logger: activate this option if we want the data to be stored in the device's internal Logger to send it to the web platform or FTP server



▸ Other ▸ Jamming detection

Settings successfully updated

Jamming detection: Enabled for GPRS mode — Select the mode

Sensibility: Medium — Select the sensibility of detection

SMS: □ enabled — When alarm, **TRY** to send SMS message

Call: □ enabled — When alarm, **TRY** to make a phone call

(Check "Other>Relay" menu for more options)

Phone numbers: Phone number 1 / Phone number 2 / Phone number 3 / Phone number 4 / Phone number 5

Text SMS Alarm On: ALARM JAMMING ON — SMS text when alarm is activated

Text SMS Alarm Off: ALARM JAMMING OFF — SMS text when alarm is deactivated

Logger: □ — Check if logger must be used
Please, configure logger before using this option

ADDITIONAL NOTES

- Once the configuration is finished, click “SAVE CONFIG” to save the changes. Remember that the router should be restarted for the changes to take effect.
- Sample format of the JSON string sent when the Logger option is chosen:

```
{“IMEI”:”354740050367237”,”TS”:”17/02/2014   19:02:46”,”TYPE”:”JAMM”,
“P”:”1234”,”VAL”:1}
```

Where:

- IMEI: the router’s ID number. Unique for each device

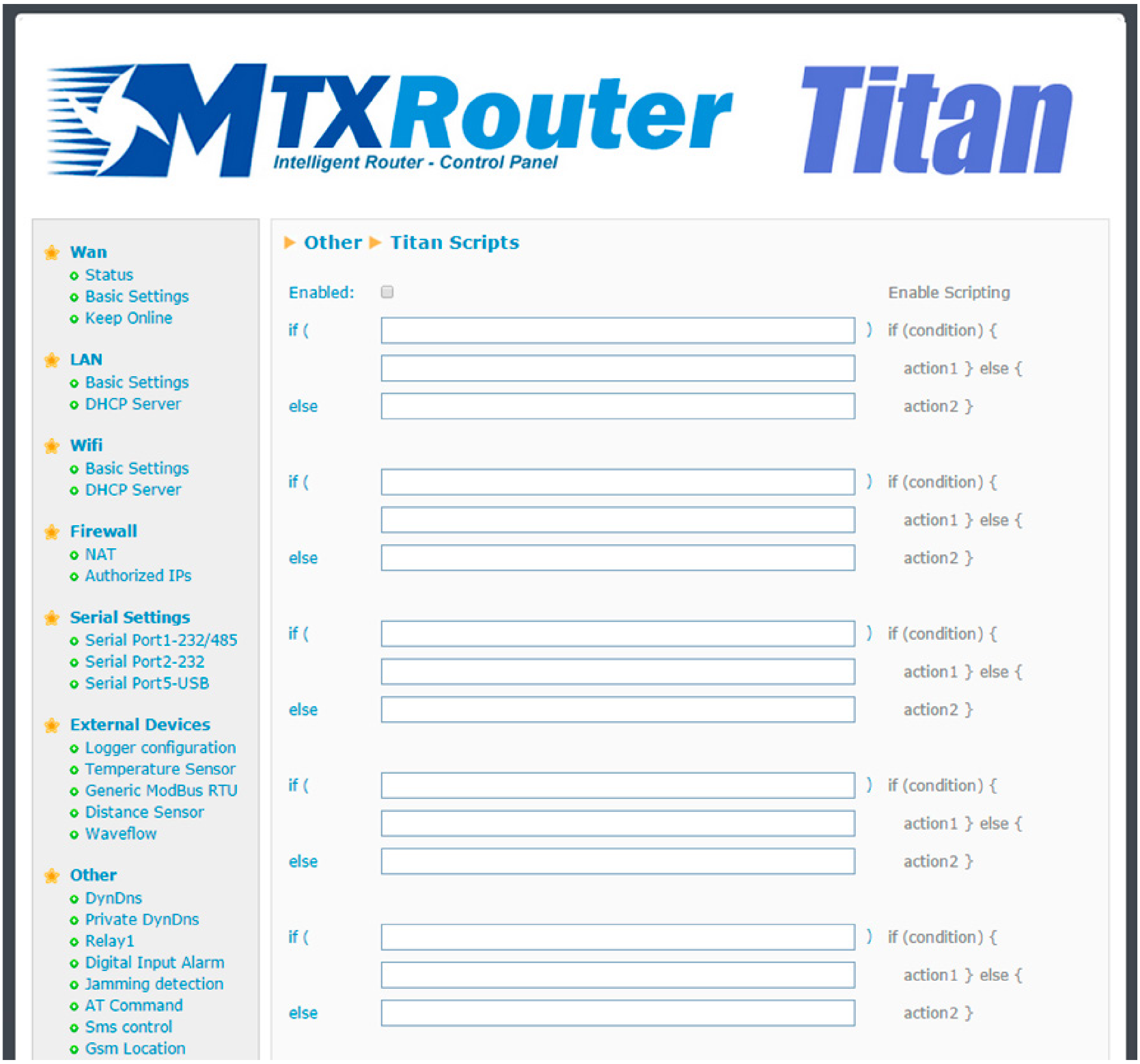
- TS: time stamp DD:MM:YYYY HH:MM:SS
- TYPE: data type. In this case digital input
- P: logger ID field (External Devices > Logger configuration)
- VAL: 1: activated/0: deactivated

2.7.16 Other: Titan Scripts

The MTX-Router-Titan II, MTX-Router-Titan and MTX-Router-Titan mini devices, from firmware version 1.06 onwards, allow the “Titan Scripts” to be edited. The “Titan Scripts” allow we to configure the device easily under given conditions. At the moment, the “Titan Scripts” are orientated to applications with Modbus devices.

For example, we can create a script so that whenever a Modbus register in device A has a specific value, the Titan writes a different value in a Modbus register in device B. Or, we can send an SMS; change a relay, etc. when a Modbus register in device A has a specific value.

The “Titan Scripts”, given they are editable by the user, allow we to create an infinite number of different applications with little effort. Below we have a guide showing the syntax of the “Titan Scripts” along with the available commands; however, the best way to learn how to use them and to see their potential is by understanding the examples found at the end of this section (4.7.16).



Enabled: ☐ Enable Scripting

if ( ) if (condition) {
action1 } else {
else action2 }

if ( ) if (condition) {
action1 } else {
else action2 }

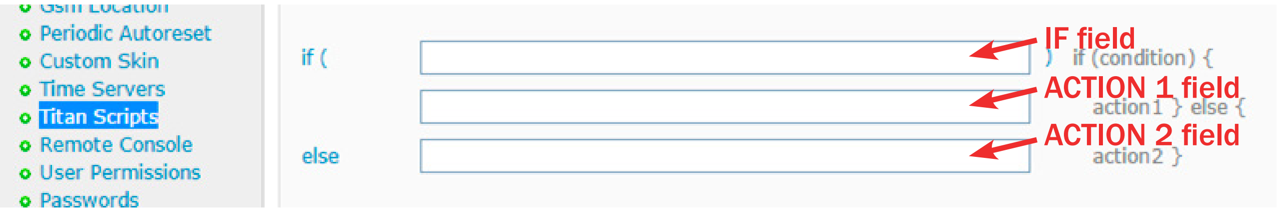
if ( ) if (condition) {
action1 } else {
else action2 }

if ( ) if (condition) {
action1 } else {
else action2 }

if ( ) if (condition) {
action1 } else {
else action2 }

Structure of the "Titan Scripts"

The Titan routers allow we to input up to 10 different scripts. The 10 possible scripts have the same structure, each with three text boxes, as shown below:

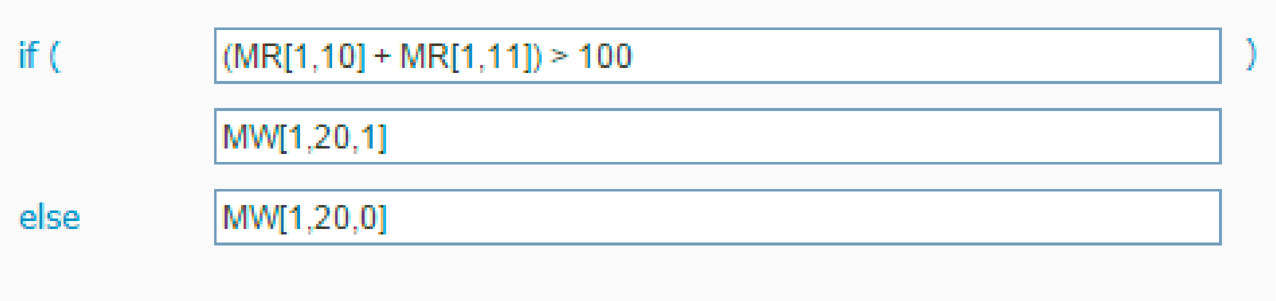


if ( ) if (condition) {
action1 } else {
else action2 }

The first text box (IF) indicates the condition; that is, the Titan device will evaluate the logical expression contained here. The second text box (action1) is the action to be executed when the IF condition is true. The third text box (action2) is the action to be carried out when the IF condition is false. In pseudocode:

```
If what the first text box says is true
    Execute the action in the second text box
If what the first text box is not true
    Execute the action in the third text box
```

Even though we still do not know the commands available, let's see an example:



```
if (    (MR[1,10] + MR[1,11]) > 100    )
        MW[1,20,1]
else    MW[1,20,0]
```

This example will be interpreted as follows:

```
If the sum of [register 10 of the Modbus device with the address 1] and [register 11 of the Modbus device with address 1] is greater than 100
    Write [the value "1" in register 20 of the Modbus device with address 1]
If the sum of [register 10 of the Modbus device with the address 1] and [register 11 of the Modbus device with address 1] is not greater than 100
    Write [the value "0" in register 20 of the Modbus device with address 1]
```

Commands Supported by the "Titan Scripts"

Below we can see the commands currently supported, showing what we can do with them. The best way to understand the workings of each of them is by reading the examples in this section of the manual.

"Modbus Read" command

- Syntax: MR[modbusAddress,modbusRegister]
- Description: reads a Modbus RTU device register. Can be used on the IF field, or the ACTION1 or ACTION2 fields

- Parameters:
  - modbusAddress: modbus device address
  - modbusRegister: address of Modbus register to be read
- Examples:
  - MR[1,10]: reads register 10 of the Modbus device with address 1
  - MR[192.168.1.20:502,10]: reads register 10 of the Modbus TCP device with IP address 192.168.1.20 and TCP port 502

“Modbus Write” command

- Syntax: MW[modbusAddress, modbusRegister,registerValue,commandWrite]
- Description: reads a Modbus RTU device register. It can be used on the ACTION1 and ACTION2 fields
- Parameters:
  - modbusAddress: modbus device address
  - modbusRegister: address of the Modbus device register to be written
  - registerValue: value to be written in the register
  - commandWrite: OPTIONAL PARAMETER. The Modbus writing commands 3 or 4 can be used. If not indicated, the Modbus command 3 will be used
- Examples:
  - MW[1,10,100]: writes the value “100” in register 10 of the Modbus device with address 1, using the Modbus writing command 3
  - MW[1,10,100,4]: writes the value “100” in register 10 of the Modbus device with address 1, using the Modbus writing command 4
  - MW[192.168.1.20:502,10,100]: writes the value “100” in reegister 10 of the Modbus TCP device with IP address 192.168.1.20 and TCP port 502 using the Modbus writing command 3
  - MW[1,10,100,4]: writes the value “100” in reegister 10 of the Modbus TCP device with IP address 192.168.1.20 and TCP port 502 using the Modbus writing command 4

“SET RELAY” command

- Syntax: SR[idRelay, relayValue]
- Description: activates or deactivates an internal relay of the Titan device. Can be used on the fields ACTION1 and ACTION2
- Parameters:
  - idRelay: possible values: 1 (Relay 1), 2 (Relay 2)
  - relayValue: possible values: 0 (relay not activated), 1 (relay activated)

- Examples:
  - SR[1,1]
  - Activates relay 1 of the Titan device
  - SR[2,0]
  - Deactivates relay 2 of the Titan device

"SEND SMS" command

- Syntax: SS[telephoneNumber, message]
- Description: sends an SNS to a specific telephone number
- Parameters:
  - telephoneNumber: Telephone number where the SMS is to be sent to
  - message: message to be sent
- Example:
  - SS[666123456,Alarm activated]
  - Sends an SMS to the number 666123455 with the text "Alarm activated"

"SEND EMAIL" command

- Sintasix: SE[emailDestination, subject]
- Descripción: sends an email to the email address provided
- Parameters:
  - emailDestination: email address of the recipient
  - subject: email subject
- Example:
  - SS[alarmas@gmail.com,Alarm activated]
  - Sends an email to the email address alarmas@gmail.com with the subject "Alarm activated"

"PAUSE" command

- Syntax: PA[seconds]
- Description: makes a pause in the management of the Titan scripts
- Parameters:
  - seconds: length (in seconds) of the pause

- Example:
    - PA[5]
    - Creates a 5 second pause

Comando "DATE"

- Syntax: DA[]
- Description: pauses the Titan script management process
- Parameters:
- Example:
    - SS[666123456,Alarm activated DA[]]
    - Sends an SMS to the cell 666123456 with the text "Alarm activated + date/time"
    - Generates a 5 second pause

Syntax of the "Titan Scripts"

The "Titan Scripts" syntax is very similar to that of Java. In each condition's "IF" field, we must specify a sentence that has a result of TRUE or FALSE, so that ACTION1 is executed if the IF condition is TRUE, and ACTION2 is executed if the IF condition is FALSE.

In the IF field, we can use all the standard operators in Java to create the condition:

&&: AND logic condition

| |: OR logic condition

+ - * /: add, subtract, multiply, divide operators

==: "equal to" condition

>: "more than" condition

<: "less than" condition

>=: "more than or equal to" condition

<=: "less than or equal to" condition

(): parenthesis to encompass expressions

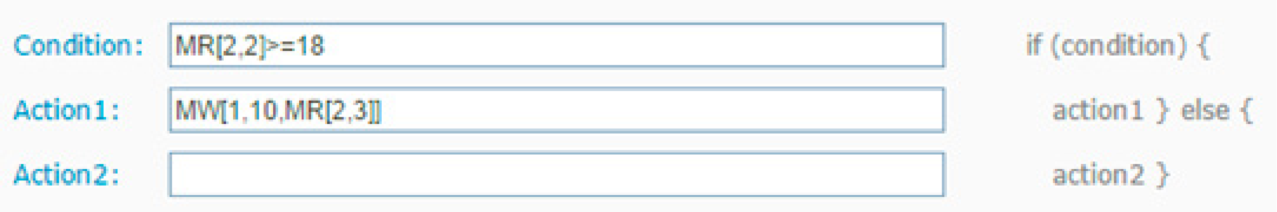
In the ACTION1 and ACTION2 field, we must use the MW, SR, SS action commands, although we can also use MR for more flexibility (this will become clearer in the examples that will come later). We can also use the operator && if we want ACTION1 and ACTION2 to carry out several actions. For example, we can make ACTION1 carry out two actions: write a Modbus register and send an SMS.

&&: concatenation of ACTION commands

Action Commands Execution Mode

Action fields have different execution modes. Edge mode (default), continuous (@) or only in the event of changes (#). The following examples show how this works.

- Edge execution (default mode):



Condition: MR[2,2]>=18

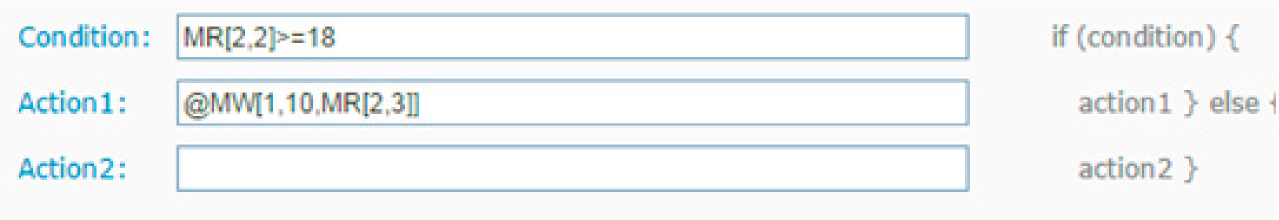
Action1: MW[1,10,MR[2,3]]

Action2:

```
if (condition) {
  action1 } else {
  action2 }
```

In this case the action MW[1,10,MR[2,3]] is executed just once upon the condition MR[2,2]>=18; i.e. once Action1 has been executed, it will not be executed again until the condition MR[2,2]>=18 is false, and then when the condition is true. This is useful when the user wants to send SMS message alerts or email alerts as this avoids continuous repeated messages.

- Continuous execution (@):



Condition: MR[2,2]>=18

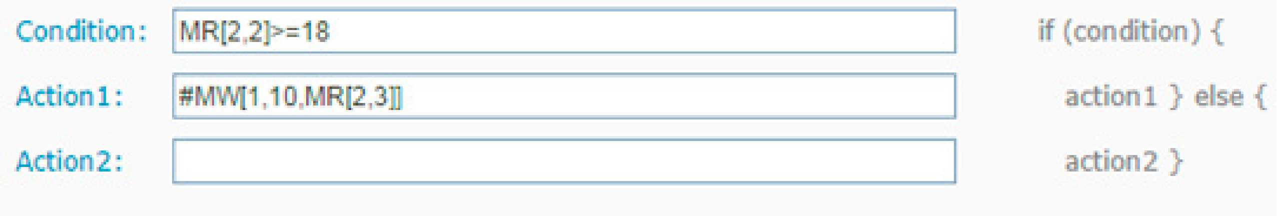
Action1: @MW[1,10,MR[2,3]]

Action2:

```
if (condition) {
  action1 } else {
  action2 }
```

In this case the action MW[1,10,MR[2,3]] is executed whenever the condition MR[2,2]>=18 is true. Do NOT use this option if SMS or emails will be sent as this will result in continuous messages being sent.

- Execution upon changes (#):



Condition: MR[2,2]>=18

Action1: #MW[1,10,MR[2,3]]

Action2:

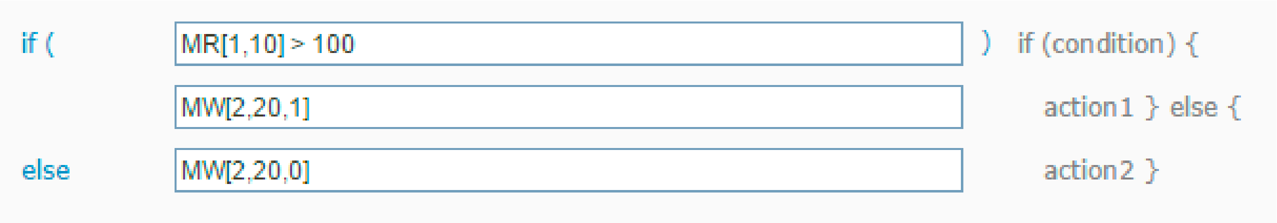
```
if (condition) {
  action1 } else {
  action2 }
```

In this case the action MW[1,10,MR[2,3]] is executed whenever there is a change in the action to be executed with respect to the the last execution. Therefore, for this example, it will be executed every time there is a change in the value MR[2,3].

Examples of “Titan Scripts”

The best way to understand how “Titan Scripts” work is by looking at examples. Below we can see a selection of examples to assist we.

EXAMPLE 1



if (	MR[1,10] > 100	) if (condition) {
	MW[2,20,1]	action1 } else {
else	MW[2,20,0]	action2 }

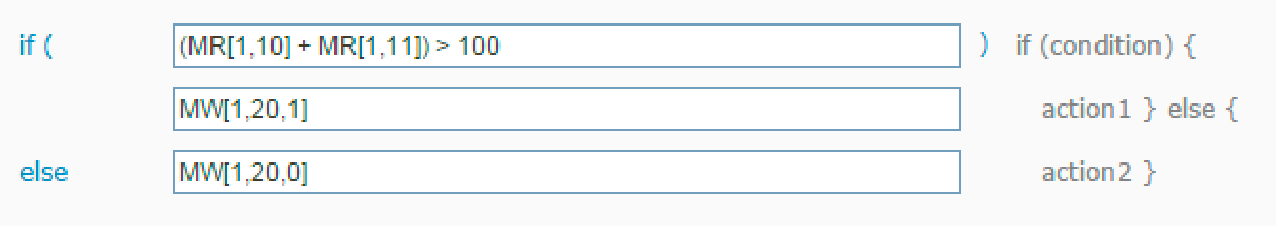
If [register 10 of the Modbus device with the address 1] is greater than 100

Write [the value “1” in register 20 of the Modbus device with address 2]

Otherwise

Write [the value “0” in register 20 of the Modbus device with address 2]

EXAMPLE 2



if (	(MR[1,10] + MR[1,11]) > 100	) if (condition) {
	MW[1,20,1]	action1 } else {
else	MW[1,20,0]	action2 }

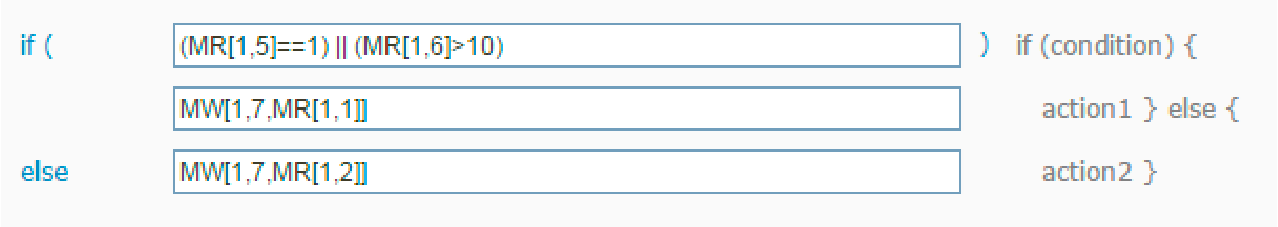
If [register 10 of the Modbus device with the address 1] plus [register 11 of the Modbus device with address 1] is greater than 100

Write [the value “1” in register 20 of the Modbus device with address 1]

Otherwise

Write [the value “0” in register 20 of the Modbus device with address 1]

EXAMPLE 3



```
if (    (MR[1,5]==1) || (MR[1,6]>10)    )  if (condition) {
        MW[1,7,MR[1,1]]                       action1 } else {
else    MW[1,7,MR[1,2]]                       action2 }
```

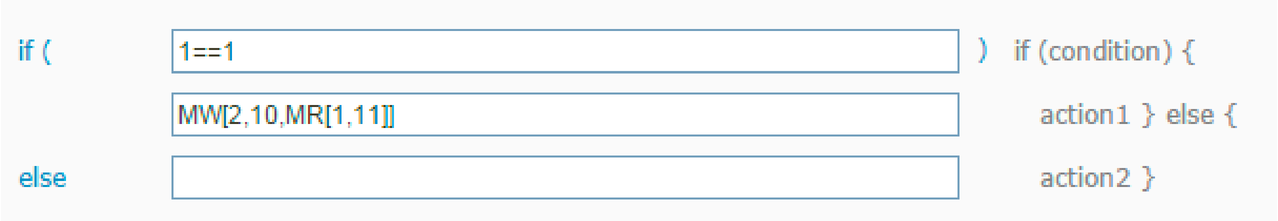
If [register 5 of the Modbus device with the address 1 has the value "1"] OR [register 6 of the Modbus device with address 1] is greater than 10

Write [in register 7 of the Modbus device with address 1 the current value of register 1 in the Modbus device with address 1]

Otherwise

Write [in register 7 of the Modbus device with address 1 the current value of register 2 in the Modbus device with address 1]

EXAMPLE 4

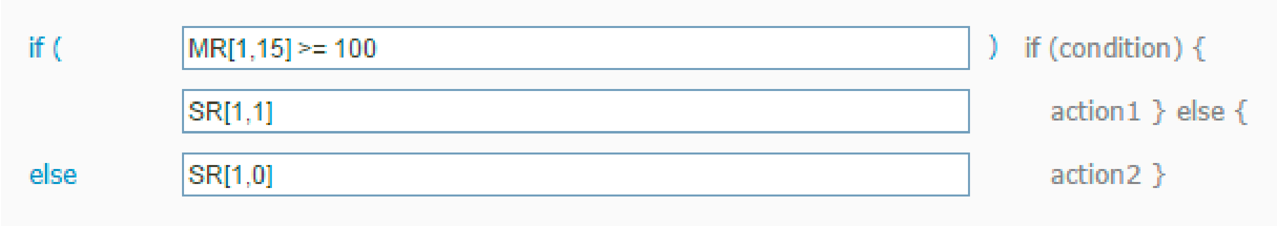


```
if (    1==1                 )  if (condition) {
        MW[2,10,MR[1,11]]          action1 } else {
else                               action2 }
```

Always (since the condition 1==1 will always be true)

Write [in register 10 of the Modbus device with address 2 [the current value of register 11 of the Modbus device with address 1]

EXAMPLE 5



```
if (    MR[1,15] >= 100      )  if (condition) {
        SR[1,1]                    action1 } else {
else    SR[1,0]                    action2 }
```

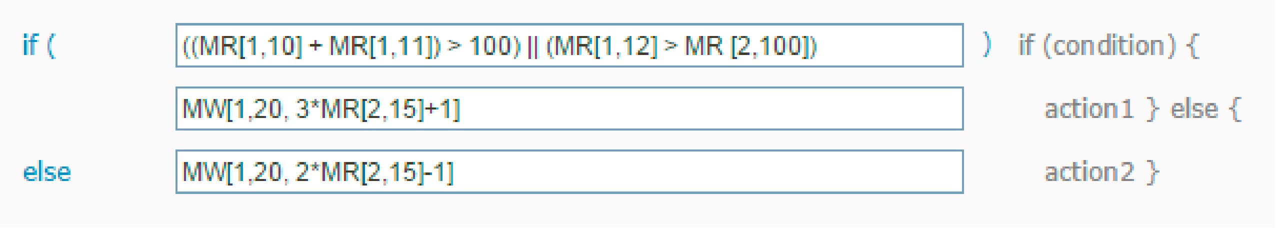
If [register 15 of the Modbus device with address 1] is greater than or equal to 100

> *Activate Titan device's Relay 1*

Otherwise

> *Deactivate Relay 1 on the Titan device*

EXAMPLE 6



```
if (    ((MR[1,10] + MR[1,11]) > 100) || (MR[1,12] > MR [2,100])   )  if (condition) {
        MW[1,20, 3*MR[2,15]+1]                                          action1 } else {
else    MW[1,20, 2*MR[2,15]-1]                                          action2 }
```

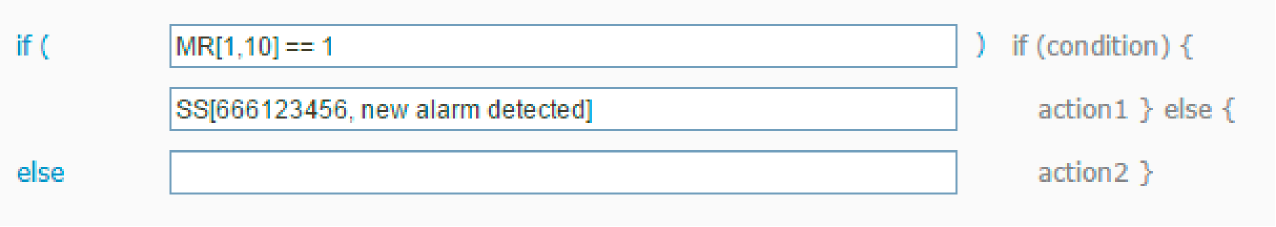
If (([register 10 of the Modbus device with address 1] + [register 11 of the Modbus device with address 1]) is greater than 100) OR if (([register 12 of the Modbus device with address 1] is greater than [register 100 of the Modbus device with address 2])

> *Write [in register 20 of the Modbus device with address 1 [the current value of register 15 of the Modbus device with address 2 multiplied by 3 plus 1]]*

Otherwise

> *Write [in register 20 of the Modbus device with address 1 [the current value of register 15 of the Modbus device with address 2 multiplied by 2 subtract 1]]*

EXAMPLE 7

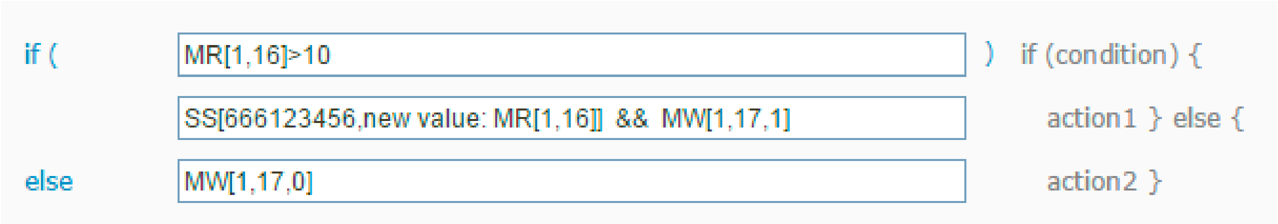


```
if (    MR[1,10] == 1                          )  if (condition) {
        SS[666123456, new alarm detected]             action1 } else {
else                                                  action2 }
```

If [register 10 of the Modbus device with address 1] is equal to 1

> *Send an SMS with the text "new alarm detected" to the telephone number 666123456*

EXAMPLE 8



if (MR[1,16]>10) if (condition) {

SS[666123456,new value: MR[1,16]] && MW[1,17,1] action1 } else {

else MW[1,17,0] action2 }

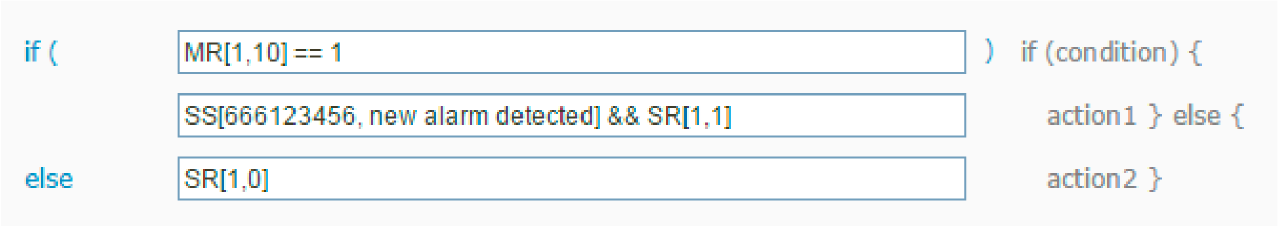
If [register 16 of the Modbus device with address 1] is greater than 10

> *Send an SMS with the text “new value: [value read from register 16 del of the Modbus device with address 1]” to the telephone number 666123456 AND AFTER Write [in register 17 of the Modbus device with address 1 the value 1]]*

Otherwise

> *Write [in register 17 of the Modbus device with address 1 the value 0]]*

EXAMPLE 9



if (MR[1,10] == 1) if (condition) {

SS[666123456, new alarm detected] && SR[1,1] action1 } else {

else SR[1,0] action2 }

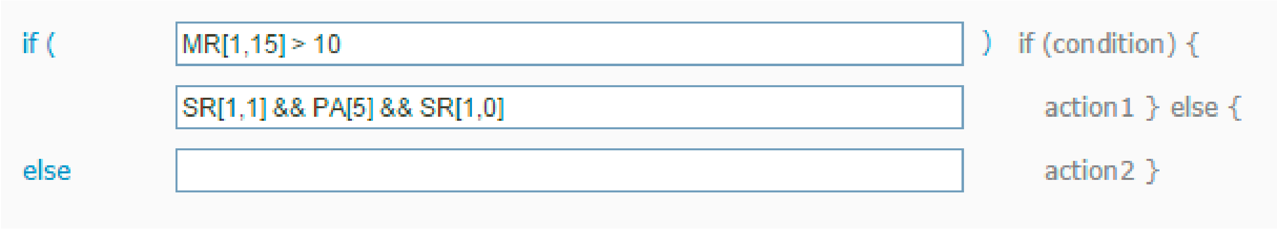
If [register 10 of the Modbus device with address 1] is equal to 1

> *Send an SMS with the text “new alarm detected” to the telephone number 666123456 AND AFTER Activate the Titan device’s internal Relay 1*

Otherwise

> *Deactivate the Titan device’s internal Relay 1*

EXAMPLE 10



if (MR[1,15] > 10) if (condition) {

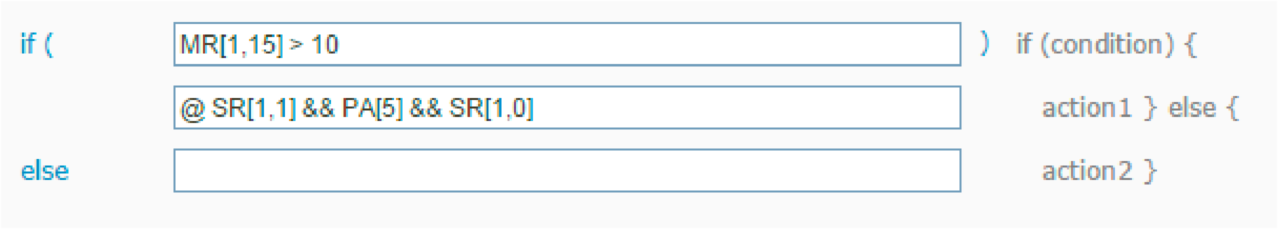
SR[1,1] && PA[5] && SR[1,0] action1 } else {

else action2 }

If [register 15 of the Modbus device with address 1] is greater than 10

[Activate the Titan device’s internal Relay 1] AND AFTER [pause for 5 seconds] AND AFTER [Deactivate the Titan device’s internal Relay 1]

EXAMPLE 11



if (MR[1,15] > 10) if (condition) {

@ SR[1,1] && PA[5] && SR[1,0] action1 } else {

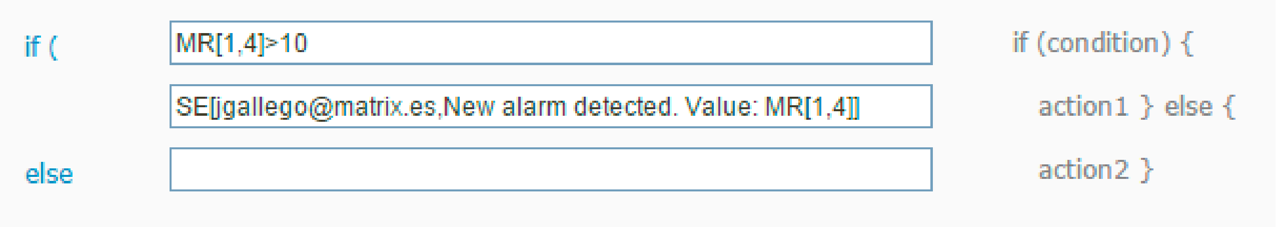
else action2 }

If [register 15 of the Modbus device with address 1] is greater than 10

CONTINUOUSLY [Activate the Titan device’s internal Relay 1] AND AFTER [pause for 5 seconds] AND AFTER [Deactivate the Titan device’s Relay 1]

The difference between example 10 and 11 lies in the @ symbol. This indicates that the action is continuously executed. This means that in example 10, ACTION1 is executed just once when the IF condition is true, and will not be executed again until ACTION1 changes or ACTION2 is executed. In example 11 however, ACTION1 is executed continuously whenever the IF condition is true; i.e. the relay is changing all the time.

EXAMPLE 12



if (MR[1,4]>10

SE[jgallego@matrix.es,New alarm detected. Value: MR[1,4]]

else

If [register 4 in Modbus device with address 1] is greater than 10

> *Send an email with the text "New alarm detected. Value [value read from register 4 of the Modbus device with address 1]" to the email jgallego@matrix.es*

ADDITIONAL NOTES

- Remember that if the command SE[] is used to send emails, the device must be configured beforehand using the menu "Other > Email configuration".

2.7.17 Other: Modbus TCP Slave

The Titan routers can be configured to behave as a Modbus TCP/RTU slave device. For example, using Modbus TCP protocol, it is possible to change the internal relays remotely (via 3G, Ethernet or WiFi) as well as consulting their statuses, the status of the digital input and sending/receiving SMS messages or sending emails via Modbus TCP.

Remember that relays can also be controlled remotely via AT commands, be these sent by SMS, 3G, Ethernet or WiFi. This can be configured using the menu "Other > Remote Console".

Below we can find a table with the Modbus address for the Titan registers. The Modbus commands that are permitted are 0x03 to read and 0x10 to write.

REGISTER ID	R/W	POSSIBLE VALUES	DESCRIPTION
1	R	0 ... 32635	Firmware version
2	R	0 ... 32635	Firmware subversion
3	R/W	0, 1	Relay 1 (0 = relay open/1 = relay activated)
4	R/W	0, 1	Relay 2 (0 = relay open/1 = relay activated)
5	R	0, 1	Digital input status. 0 = input to GND, 1 = input not connected
98	W	0 ... 32635	Length of AT command to be executed
99	R	0 ... 32635	Length of AT command response
100 ... 354	W	ASCII	AT command text (in ASCII)
500 ... 754	R	ASCII	AT command response text (in ASCII)
1000	R/W	0, 1	1 indicates a new SMS received. A PLC should write '1' after reading the SMS
1001	R	0 ... 18	Length of cell number that sent the SMS
1002 ... 1019	R	ASCII	Cell number that sent the SMS
1020	R	0 ... 18	Length of SMS
1021 ... 1180	R	ASCII	Text of SMS

AT Commands via Modbus TCP Protocol

Another interesting characteristic of the Titan routes is the option to execute AT commands via Modbus protocol. For example, if we have a PLC acting as a Master Modbus TCP, we can send an AT command via Modbus TCP protocol to the router in order to obtain information such as network coverage, or send an SMS, read a radio sensor (temperature, pulse counter, digital input or a 4/20mA input, etc.), read the time or reset the router.

The following pages will explain the process of sending AT commands via Modbus TCP.

Procedure for Sending AT Commands via Modbus TCP

The process is simple and the best way to understand it is using a practical example. For example, imagine we want to execute the command AT+CSQ to obtain the network coverage.

- First we must write the AT command in ASCII code, using the registers 100 and onwards

REGISTER ID	VALUE	DESCRIPTION
100	65	ASCII for letter: A
101	84	ASCII for letter: T
102	43	ASCII for character: +
103	67	ASCII for letter: C
104	83	ASCII for letter: S
105	81	ASCII for letter: Q

- The command AT+CSQ has six characters, therefore we must input in register 98 the value “6” for the command to be executed

REGISTER ID	VALUE	DESCRIPTION
98	6	Size of command to be executed

- Then we must check the command’s execution, which we can see in register 99. The value we are reading represents the length of the response. A value of 0 indicates there is no response (the execution is incomplete)

REGISTER ID	VALUE	DESCRIPTION
99	28	Size of response to command

- Finally, we must read the 28 registers where the response is contained (register 500 onwards)

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

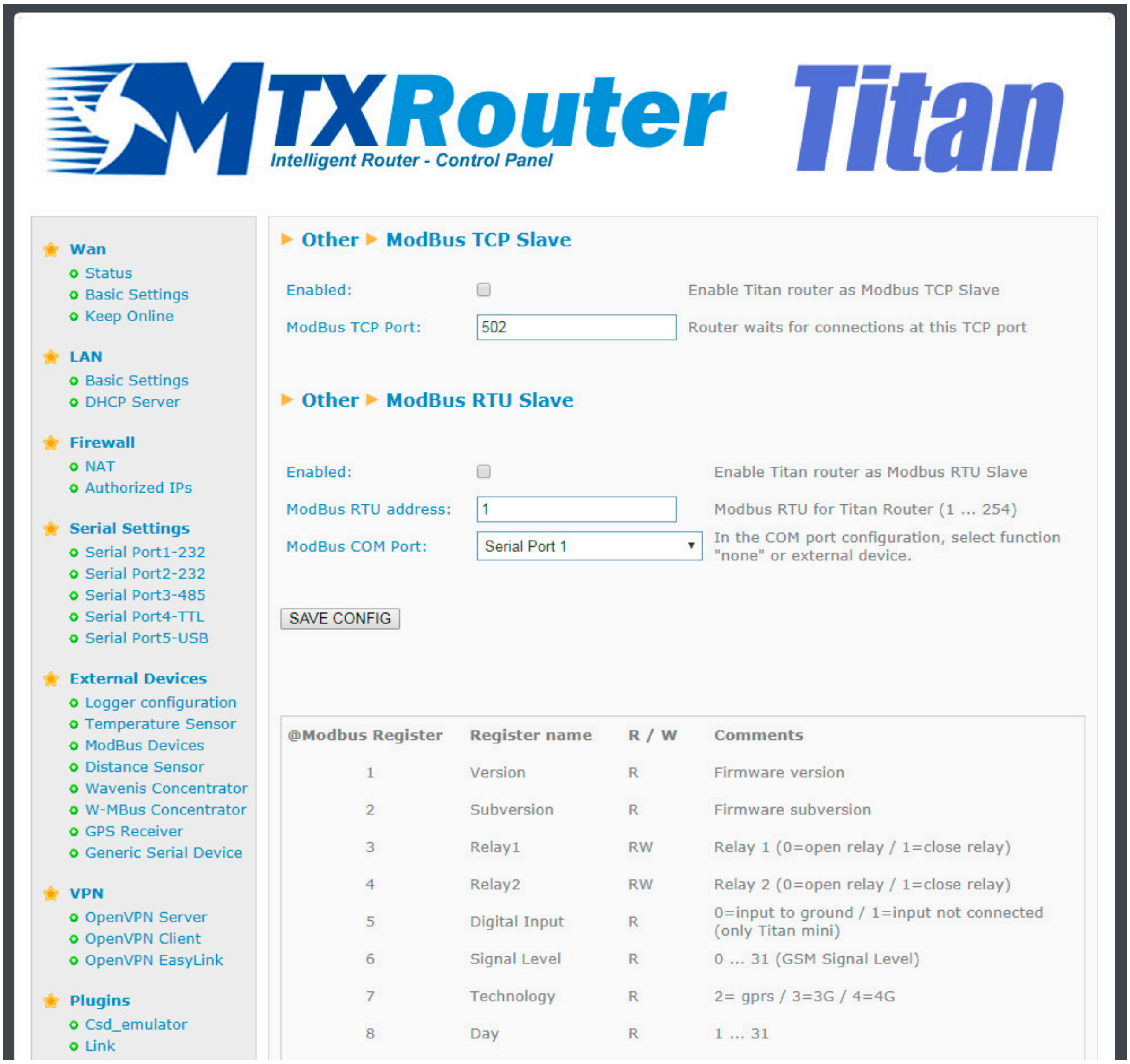
521	10	\n
522	13	\r
523	10	\n
524	79	O
525	75	K
526	13	\r
527	10	\n

For this AT command the relevant registers are 515 and 516, which indicate a network coverage of 16.

Remember that in order to use this characteristic to send SMS messages, the AT command is AT^MTXTUNNEL=SMS,phone,message, as previously outlined in this guide.

Procedure for Receiving SMS Messages

The process for receiving SMS messages via Modbus TCP is very simple. The PLC should periodically check register 1000. If the value read is “1”, this indicates that there is a new SMS message, which can be read from regsiters 1001 to 1180. After reading the message, the value of register 1000 should be changed back to “0”.



▶ Other ▶ ModBus TCP Slave

Enabled: □ Enable Titan router as Modbus TCP Slave

ModBus TCP Port: 502 Router waits for connections at this TCP port

▶ Other ▶ ModBus RTU Slave

Enabled: □ Enable Titan router as Modbus RTU Slave

ModBus RTU address: 1 Modbus RTU for Titan Router (1 ... 254)

ModBus COM Port: Serial Port 1 In the COM port configuration, select function "none" or external device.

SAVE CONFIG

@Modbus Register	Register name	R / W	Comments
1	Version	R	Firmware version
2	Subversion	R	Firmware subversion
3	Relay1	RW	Relay 1 (0=open relay / 1=close relay)
4	Relay2	RW	Relay 2 (0=open relay / 1=close relay)
5	Digital Input	R	0=input to ground / 1=input not connected (only Titan mini)
6	Signal Level	R	0 ... 31 (GSM Signal Level)
7	Technology	R	2= gprs / 3=3G / 4=4G
8	Day	R	1 ... 31

ADDITIONAL NOTES

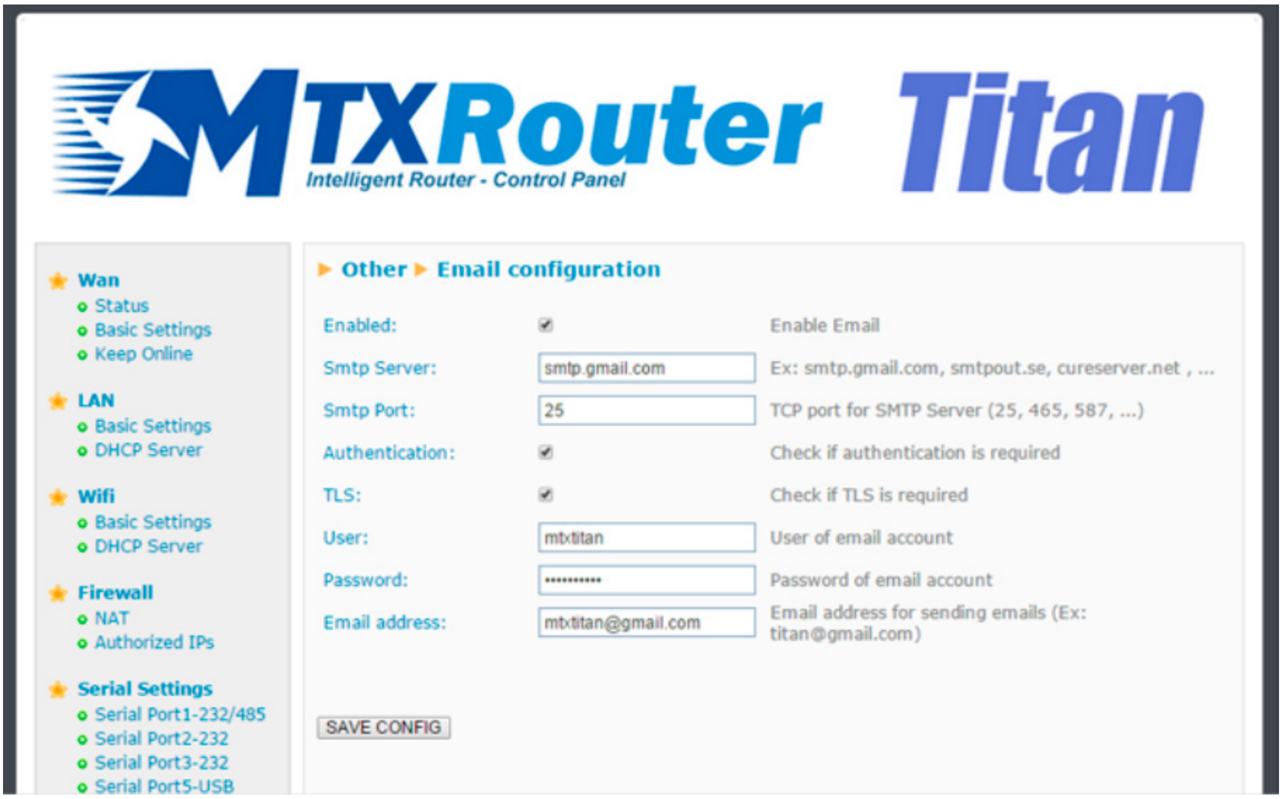
- Once configured click on the “SAVE CONFIG” button to save changes. Restart the router so changes apply
- Check the modbus registry table inside the Titan router configuration menus, in the section Other > Modbus Slave

2.7.18 Other: Email Configuration

Titan routers are able to send email notifications. They also allow emails to be sent using AT commands. For example, if we have a PLC and wish to send an SMS or email, we can send an AT command to the MTX-Router-Titan-3G device to do it.

The router must be configured beforehand to be able to receive emails:

- Enabled: select this box if we wish to activate this option
- Smtp server: Indicate the address or DNS or the SMTP server (for example, smtp.gmail.com, smtpout.secureserver.net, etc.)
- Smtp Port: TCP port of the SMTP server
- Authentication: select this box if the SMTP server requires authentication (usually the case)
- TLS: select this box if the SMTP server requires TLS
- User: username of the sender’s email account
- Password: password of the sender’s email account
- Email address: sender’s email from which emails are sent



▸ Other ▸ Email configuration

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

SAVE CONFIG

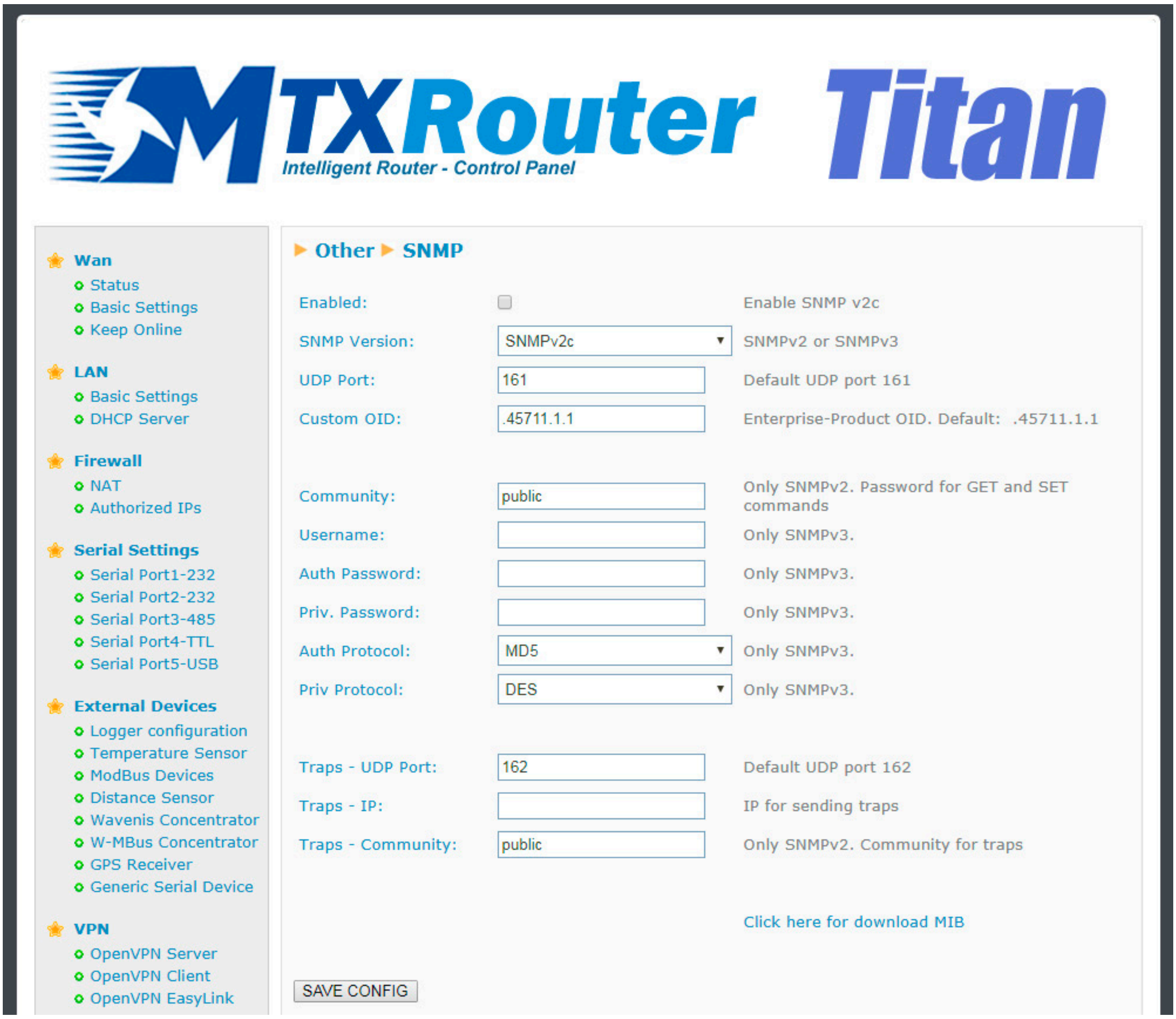
ADDITIONAL NOTES

- Once the configuration is complete, press the “SAVE CONFIG” button to save the changes. Remember that the router should be reset in order for the changes to take effect.
- If we use a Gmail SMTP server, we may have to activate certain configurations in our account in order to be able to send emails from an IOT device. To do this:
  1. Activate the option: http://www.google.com/settings/security/lesssecureapps
  2. Activate: http://www.google.com/accounts/DisplayUnlockCaptcha

2.7.19 Other: SNMP

Titan routers include SNMP protocol for firmware versions 1.11 or later. Via SNMP we can carry out SET and GET operations from standard SNMP applications.

- Enabled: select this box if we wish to activate the Titan router's SNMP service
- SNMP Version: SNMPv2 or SNMPv3
- UDP port: the standard UDP port for SNMP is 161, but this can be changed here
- Custom OID: this option allows we to change the Enterprise-Product OID of the default value (.45711.1.1) if we wish to tune this to our business values
- Community: the password required to execute SET and GET commands. Only necessary for SNMPv2
- Username: only necessary for SNMPv3
- Auth Password: autentication password for SNMPv3
- Priv Password: privacy password for SNMPv3
- Auth Protocol: autentication protocol (MD5 or SHA)
- Priv Protocol: encryption protocol (DES, AES128, AES192, AES256)
- Traps – UDP port: this option allows we to specify the port for SNMP Traps
- Traps – IP: the IP address for sending SNMP Traps
- Community: community field for sending Traps



▸ Other ▸ SNMP

Enabled:	□	Enable SNMP v2c
SNMP Version:	SNMPv2c ▾	SNMPv2 or SNMPv3
UDP Port:	161	Default UDP port 161
Custom OID:	.45711.1.1	Enterprise-Product OID. Default: .45711.1.1
Community:	public	Only SNMPv2. Password for GET and SET commands
Username:		Only SNMPv3.
Auth Password:		Only SNMPv3.
Priv. Password:		Only SNMPv3.
Auth Protocol:	MD5 ▾	Only SNMPv3.
Priv Protocol:	DES ▾	Only SNMPv3.
Traps - UDP Port:	162	Default UDP port 162
Traps - IP:		IP for sending traps
Traps - Community:	public	Only SNMPv2. Community for traps

Click here for download MIB

SAVE CONFIG

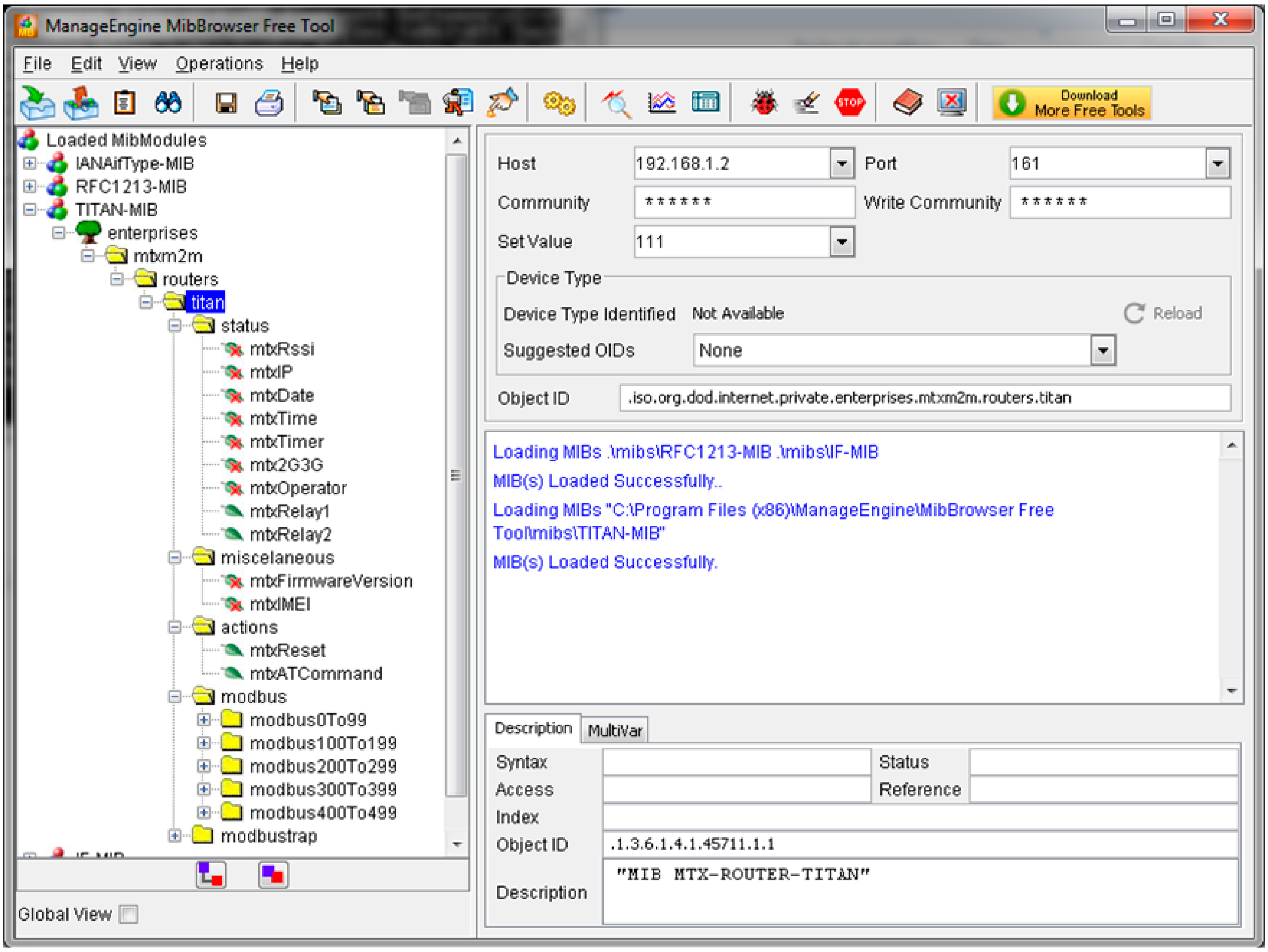
ADDITIONAL NOTES

- Once the configuration is complete, press the “SAVE CONFIG” button to save the changes. Remember that the router should be reset in order for the changes to take effect.

- On the previous screen we can see a link with the text “Click here for download MIB”. Download the file to obtain the MIB with the OIDs.

- Using SNMP we can monitor the router. We can request information from the router such as the RSSI (network coverage), the time and date, the up time, whether it is working in 2G or 3G mode, the network operator being used, etc. We can also find out the status of the router relays, as well as change their statuses. The same is possible with digital inuts and pulse counters.

- An interesting option can be found in the section “Action”. Here we will see that two actions are possible. Firstly, we can reset the router remotely. Secondly, we can execute an AT command remotely via SNMP (writing in the corresponding register will excute the AT command and reading the register will obtain the response). Sending AT commands allows we to carry out any action using SNMO from reading a Modbus device that is connected to the router to changing configuration parameters or reading the GPS position.



Host 192.168.1.2 Port 161

Community ****** Write Community ******

Set Value 111

Device Type

Device Type Identified Not Available

Suggested OIDs None

Object ID .iso.org.dod.internet.private.enterprises.mtxm2m.routers.titan

```
Loading MIBs .\mibs\RFC1213-MIB .\mibs\IF-MIB
MIB(s) Loaded Successfully..
Loading MIBs "C:\Program Files (x86)\ManageEngine\MibBrowser Free
Tool\mibs\TITAN-MIB"
MIB(s) Loaded Successfully.
```

Object ID .1.3.6.1.4.1.45711.1.1

Description "MIB MTX-ROUTER-TITAN"

- There is an Application Note regarding the use of SNMP and Traps, where we can find further examples of their applications and obtain a greater understanding of their capabilities:

  AN8-Router-Titan-Modbus-to-SNMP-Gateway.pdf

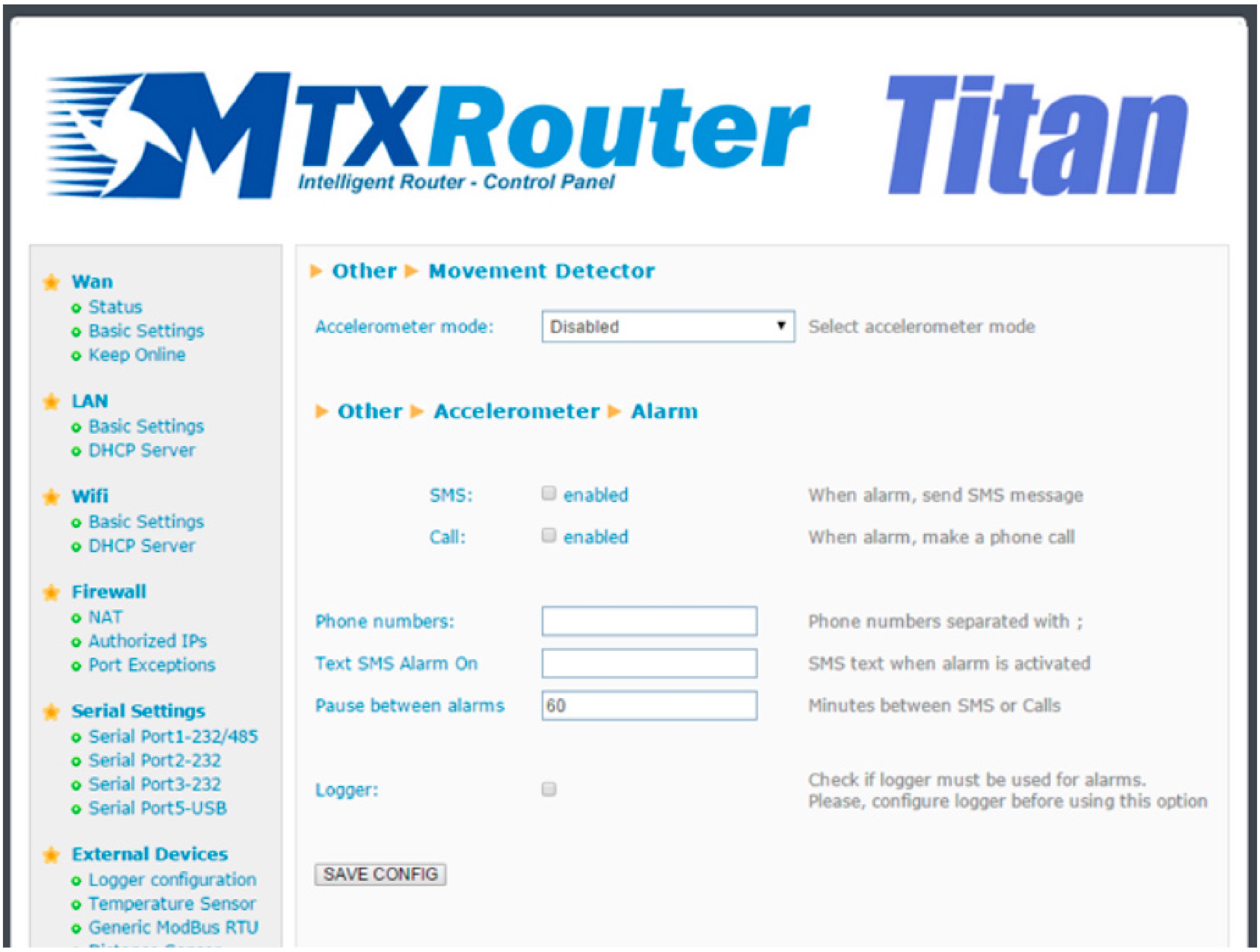
  AN10-Router-Titan-sending-SMS-Emails-Traps-with-ModbusTCP.pdf

2.7.20 Other: Movement Detector

The Titan mini routers contain a movement detection system that allows we to send SMS alarms, make telephone calls or change a relay upon detecting movement.

- Accelerometer mode: this option activates the movement detection system with different sensitivity modes
- SMS: this option activates the sending of SMS messages in the event of detected movement
- Call: this option activates the telephone call option in the even of detected movement
- Phone numbers: list of numbers (separated by semi-colon) to which SMS messages will be sent and phone calls will be made
- Text SMS Alarm On: Text of the SMS alarm

- Pause between alarms: this field indicates the time (in minutes) between alarms. For example, a value of 60 means that no alarms or calls will be made for an hour after the last message was sent or the last call was made



▶ Other ▶ Movement Detector

Accelerometer mode: Disabled ▾ Select accelerometer mode

▶ Other ▶ Accelerometer ▶ Alarm

SMS: □ enabled When alarm, send SMS message

Call: □ enabled When alarm, make a phone call

Phone numbers: Phone numbers separated with ;

Text SMS Alarm On SMS text when alarm is activated

Pause between alarms 60 Minutes between SMS or Calls

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

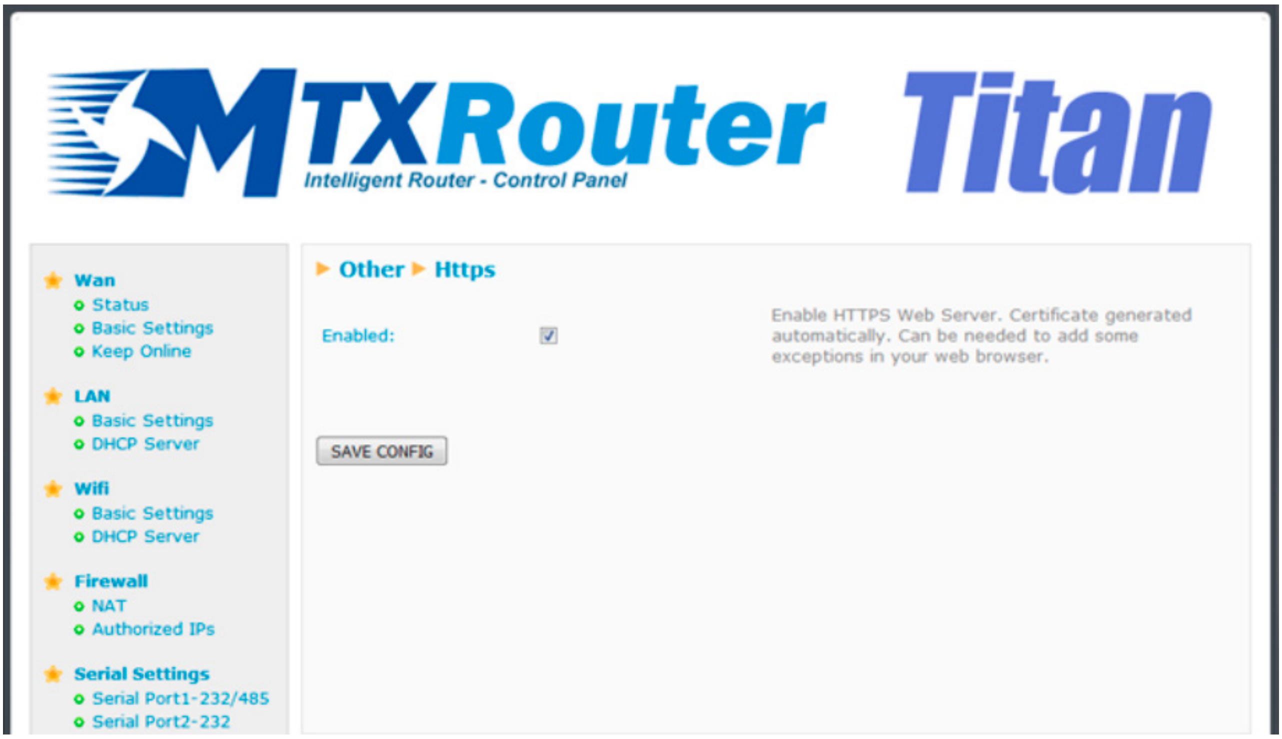
ADDITIONAL NOTES

- Once the configuration is complete, press the "SAVE CONFIG" button to save the changes. Remember that the router should be reset in order for the changes to take effect.

2.7.21 Other: HTTPS

Titan mini router allows we to enable HTTPS in the configuration environment if necessary.

- Enabled: enables the HTTPs service (certificates are generated automatically after the restart



Enabled: ☑

Enable HTTPS Web Server. Certificate generated automatically. Can be needed to add some exceptions in your web browser.

ADDITIONAL NOTES

- Once the configuration is finished press the “SAVE CONFIG” button to save the changes. Remember to restart our router for the new changes to take effect.
- When we try to connect to the Titan router via HTTPS our browser will probably show we a warning message regarding the self-signed digital certificate. It is completely normal.

2.7.22 OTher: MQTT

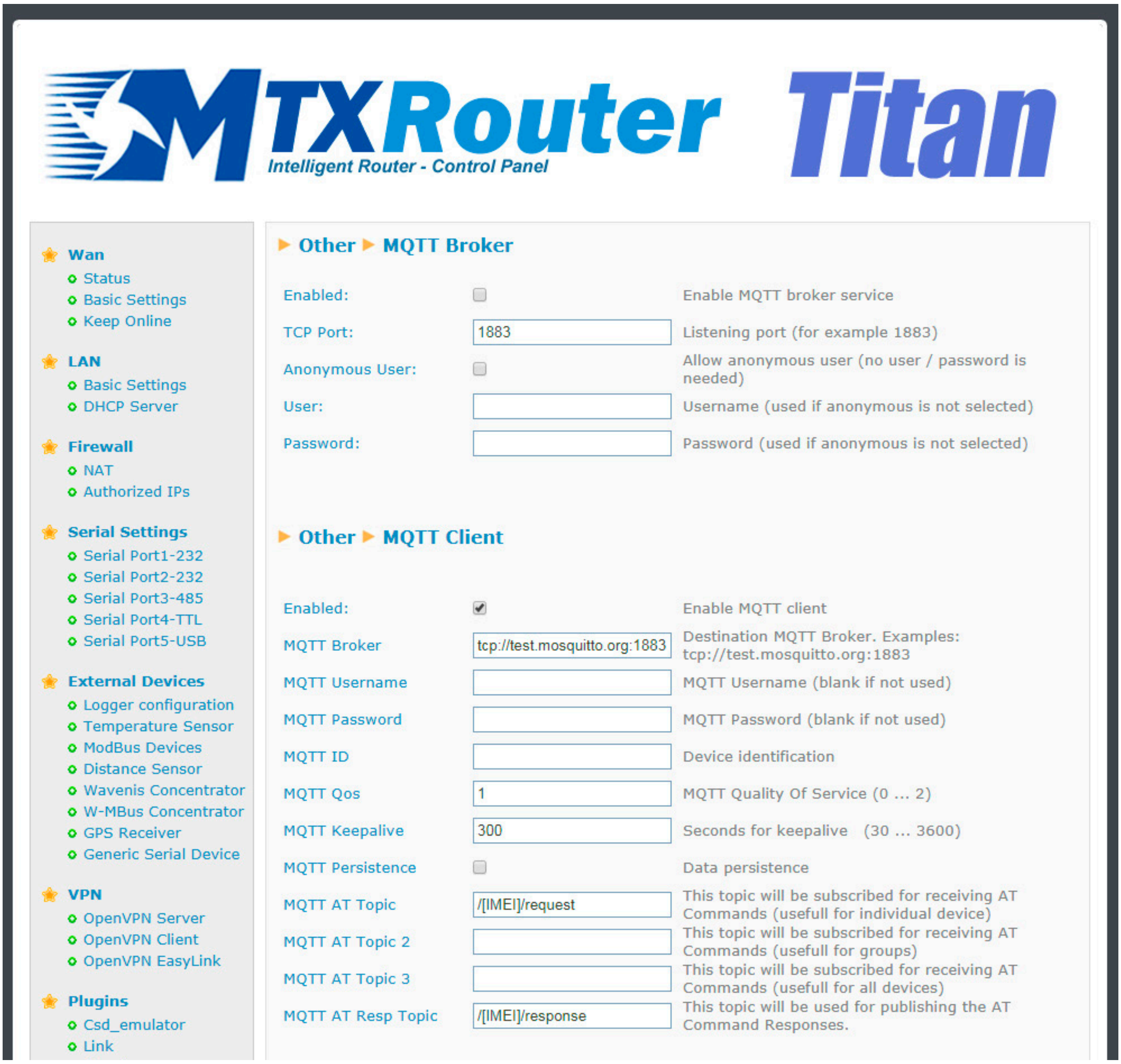
Titan routers can work as basic MQTT broker or as MQTT client. Configuring the Titan router as MQTT client it can send the data gathered in the Logger (sensor data, modbus equipment, ...) via MQTT. This section should be properly configured if we select send via MQTT in the Logger section.

Other: MQTT broker

- Enabled:
- Anonym user:
- User:
- Password:

Other: MQTT client:

- Enabled: select to enable the MQTT client service
- Username: leave blank if we are not using it
- Password: leave blank if we are not using it
- ID: device identification field
- QoS: quality of service (0, 1, 2)
- KeepAlive: in seconds (300 recommended)
- Persistence: select in case we want data to be persistent
- AT Topic: Titan router topic 1. AT commands sent to this topic will be executed in the router
- AT Topic 2: Titan router topic 2. AT commands sent to this topic will be executed in the router
- AT Topic 3: Titan router topic 3. AT commands sent to this topic will be executed in the router
- AT Topic Rest: MQTT ansours to AT commands received by the Titan router will be sent to this topic also via MQTT



▶ Other ▶ MQTT Broker

Enabled:	☐	Enable MQTT broker service
TCP Port:	1883	Listening port (for example 1883)
Anonymous User:	☐	Allow anonymous user (no user / password is needed)
User:		Username (used if anonymous is not selected)
Password:		Password (used if anonymous is not selected)

▶ Other ▶ MQTT Client

Enabled:	☑	Enable MQTT client
MQTT Broker	tcp://test.mosquitto.org:1883	Destination MQTT Broker. Examples: tcp://test.mosquitto.org:1883
MQTT Username		MQTT Username (blank if not used)
MQTT Password		MQTT Password (blank if not used)
MQTT ID		Device identification
MQTT Qos	1	MQTT Quality Of Service (0 ... 2)
MQTT Keepalive	300	Seconds for keepalive (30 ... 3600)
MQTT Persistence	☐	Data persistence
MQTT AT Topic	/[IMEI]/request	This topic will be subscribed for receiving AT Commands (usefull for individual device)
MQTT AT Topic 2		This topic will be subscribed for receiving AT Commands (usefull for groups)
MQTT AT Topic 3		This topic will be subscribed for receiving AT Commands (usefull for all devices)
MQTT AT Resp Topic	/[IMEI]/response	This topic will be used for publishing the AT Command Responses.

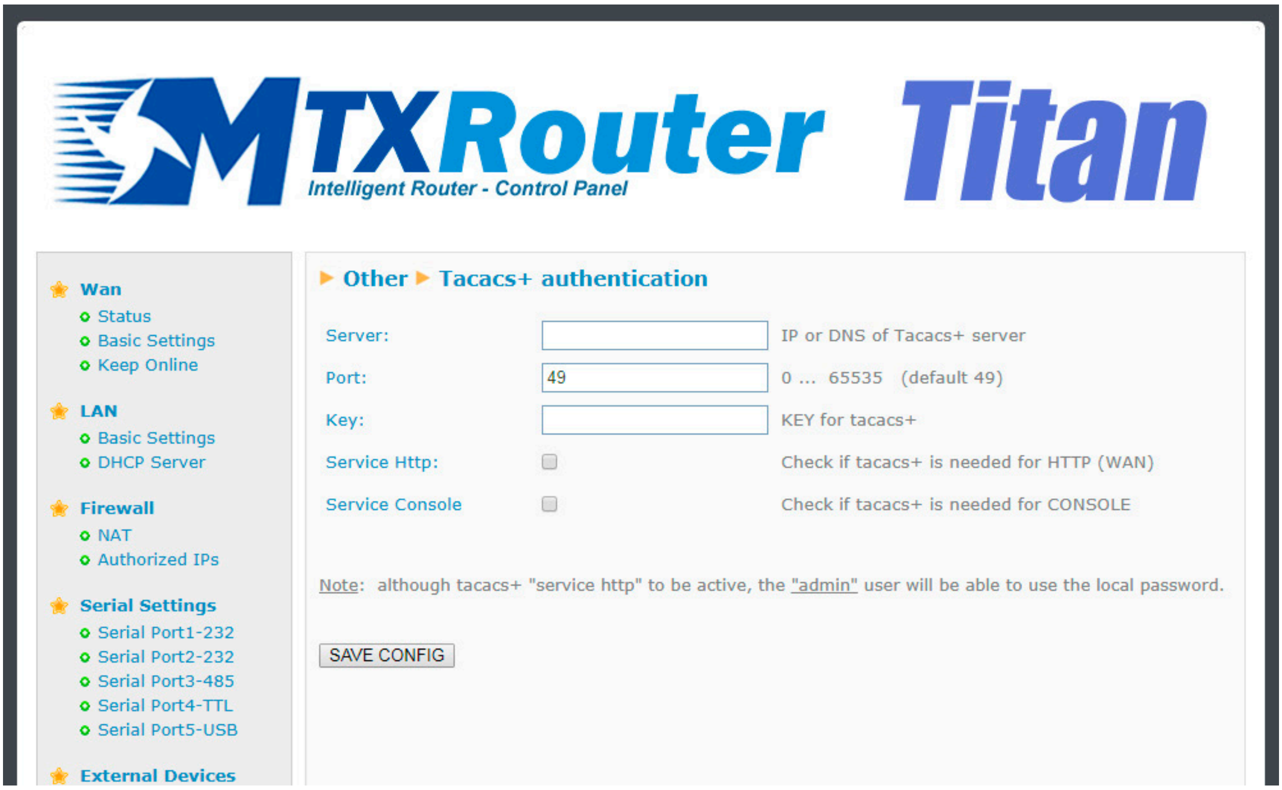
ADDITIONAL NOTES

- Once configured click on the “SAVE CONFIG” button to save changes. Restart the router so changes apply
- Note we can enter the text [IMEI] instead of the IMEI number. That is, if the IMEI is 012345678912345, we could either enter the topic /012345678912345/TEST or /[IMEI]/TEST

2.7.23 Other: Tacacs+

If an external Tacacs+ server is needed for the authentication of the HTTP and Telnet services, we need to configure in this section.

- Server: Tacacs+ server IP address or DNS
- Port: Tacacs+ tap port (default 49)
- Key: encryption password
- Service http: activate this box in case we want the access to the Titan router via HTTP to use the Tacacs+ authentication service
- Service console: activate this box in case we want the access to the Titan router via Telnet (remote console) to use Tacacs+ authentication



▶ Other ▶ Tacacs+ authentication

Server:		IP or DNS of Tacacs+ server
Port:	49	0 ... 65535 (default 49)
Key:		KEY for tacacs+
Service Http:	□	Check if tacacs+ is needed for HTTP (WAN)
Service Console	□	Check if tacacs+ is needed for CONSOLE

Note: although tacacs+ "service http" to be active, the "admin" user will be able to use the local password.

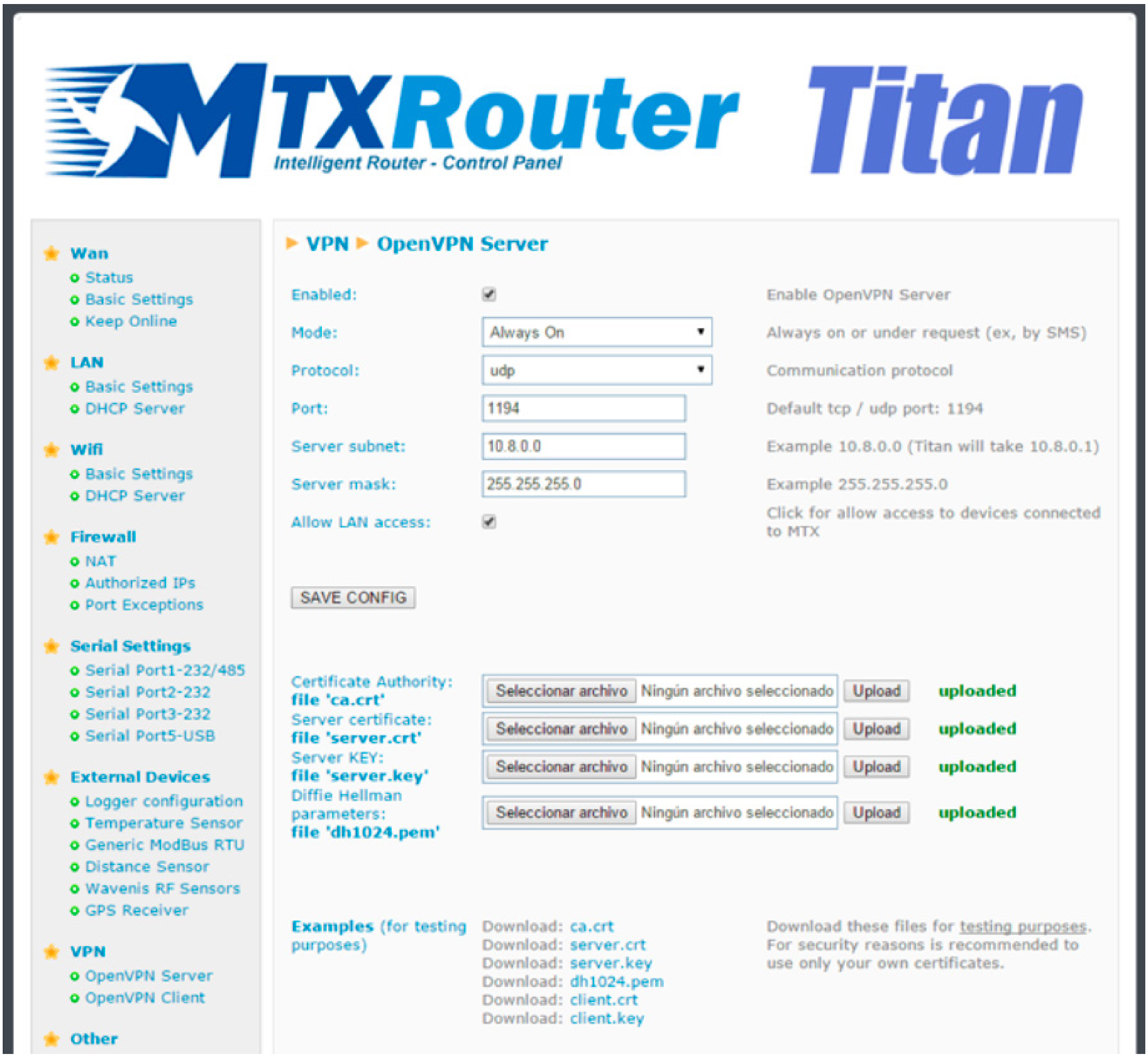
ADDITIONAL NOTES

- Once configured click on the “SAVE CONFIG” button to save changes. Restart the router so changes apply
- Note the Titan router will allow us to use the username and password assigned to the user “admin” locally, so if the router does not have Internet connectivity (operator change, etc.) it can have a way to enter the router. Save the “admin” local password securely

2.8 VPN

2.8.1 VPN: OpenVPN Server

The Titan and Titan mini can act as an OpenVPN server. By using a VPN service, all devices connected to the router’s Ethernet bus or the IP-RS232/485/USB gateways can be securely accessed from the othe rend of the VPN network. A VPN service is also useful to avoid problems generated from the use of proxies, firewalls, etc. and especially when using SIM cards that use IP addresses in the range 10.x.x.x



▶ VPN ▶ OpenVPN Server

Enabled:	☑	Enable OpenVPN Server
Mode:	Always On	Always on or under request (ex, by SMS)
Protocol:	udp	Communication protocol
Port:	1194	Default tcp / udp port: 1194
Server subnet:	10.8.0.0	Example 10.8.0.0 (Titan will take 10.8.0.1)
Server mask:	255.255.255.0	Example 255.255.255.0
Allow LAN access:	☑	Click for allow access to devices connected to MTX

Certificate Authority: **file 'ca.crt'**	Ningún archivo seleccionado	**uploaded**
Server certificate: **file 'server.crt'**	Ningún archivo seleccionado	**uploaded**
Server KEY: **file 'server.key'**	Ningún archivo seleccionado	**uploaded**
Diffie Hellman parameters: **file 'dh1024.pem'**	Ningún archivo seleccionado	**uploaded**

Examples (for testing purposes)

Download: ca.crt
Download: server.crt
Download: server.key
Download: dh1024.pem
Download: client.crt
Download: client.key

Download these files for testing purposes. For security reasons is recommended to use only your own certificates.

- Enabled: select this box if we wish to activate the OpenVN service in Server mode
- Mode: "Always On" will keep the VPN active. "Under Request" will activate the VPN for the time we require. This option could be used for maintenance. To activate the VPN service we will need to send an AT command (see Chapter 5) via SMS, Telnet, Webserver, SNMP or Modbus TCP. Once the time configured has passed, the VPN will be disconnected
- Protocol: establish the protocol for the activation of the VPN service. Either UDP or TCP
- Port: the standard port is 1194 but we can change this in this field
- Server Subnet: indicates the subnet that will be created when the VPN is activated. If a value of 10.8.0.0 is used, the device will adopt the address 10.8.0.1 once the VPN is activated

- Server Mask: indicate the server mas to be applied to the VPN
- Allow LAN access: select this option if we wish to be able to access remotely the devices connected to the router's Ethernet port. Do not activate this option if we only want to access the router and the IP/RS232/485/USB gateways controlled by the router
- Necessary files for OpenVPN
- In order to be able to use the MTX-Router-Titan devices as an OpenVPN server, we will need to create and update the following files: ca.crt (certificate of authenticity), server.crt (server certificate), server.key (server private key) and dh1024.pem (Diffie Hellman parameters)

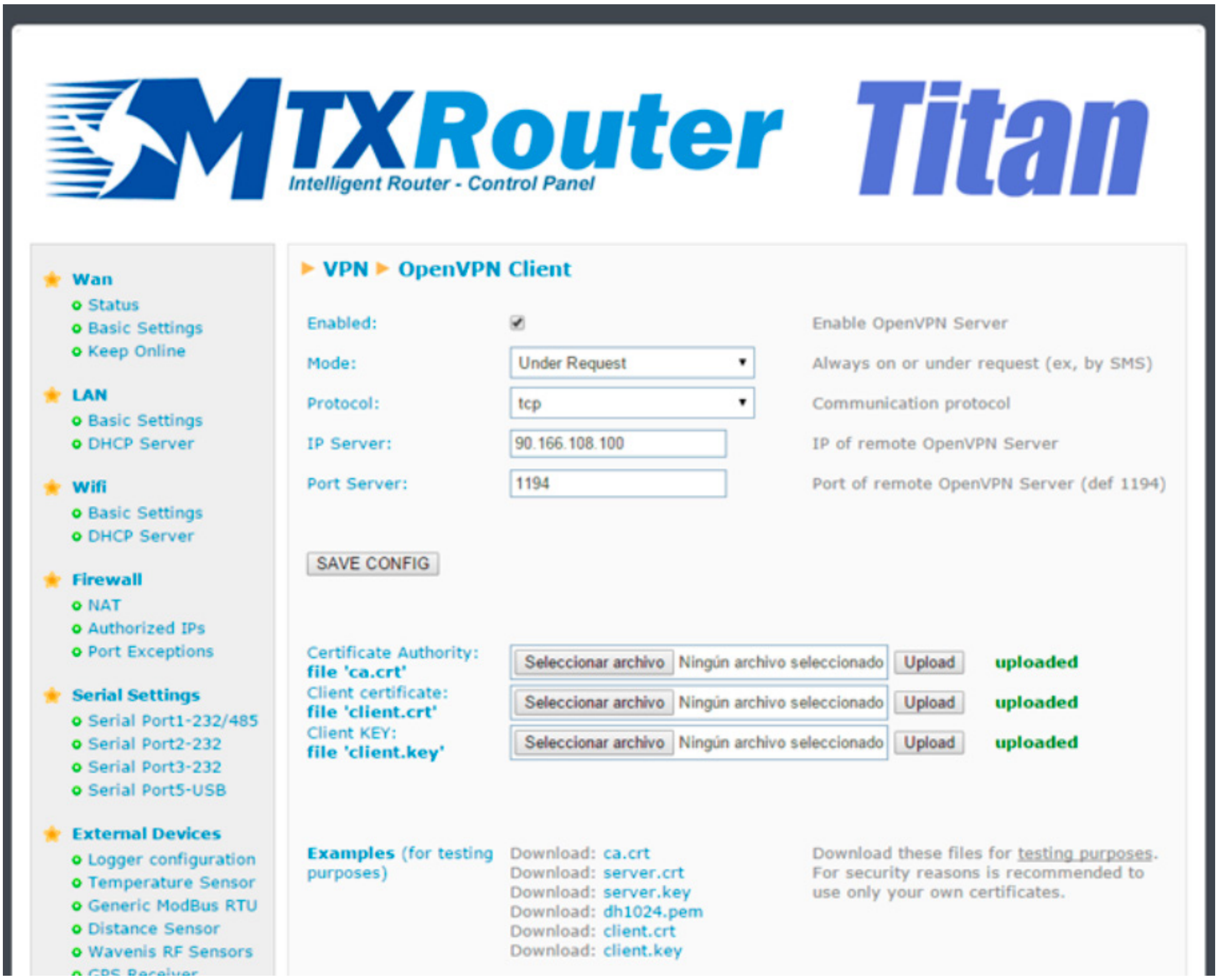
Towards the bottom of the screen we will see that we can download example files. These must only be used in test mode. In real applications we should always generate our own certificates.

ADDITIONAL NOTES

- Once the configuration is complete, press the "SAVE CONFIG" button to save the changes. Remember that the router should be reset in order for the changes to take effect

2.8.2 VPN: OpenVPN Client

The Titan and Titan mini can act as an OpenVPN client. By using a VPN service, all devices connected to the router's Ethernet bus or the IP-RS232/485/USB gateways can be securely accessed from the othe rend of the VPN network. A VPN service is also useful to avoid problems generated from the use of proxies, firewalls, etc. and especially when using SIM cards that use IP addresses in the range 10.x.x.x



▶ VPN ▶ OpenVPN Client

Enabled:	☑	Enable OpenVPN Server
Mode:	Under Request	Always on or under request (ex, by SMS)
Protocol:	tcp	Communication protocol
IP Server:	90.166.108.100	IP of remote OpenVPN Server
Port Server:	1194	Port of remote OpenVPN Server (def 1194)

Certificate Authority: file 'ca.crt'	Ningún archivo seleccionado	uploaded
Client certificate: file 'client.crt'	Ningún archivo seleccionado	uploaded
Client KEY: file 'client.key'	Ningún archivo seleccionado	uploaded

Examples (for testing purposes)

Download: ca.crt
Download: server.crt
Download: server.key
Download: dh1024.pem
Download: client.crt
Download: client.key

Download these files for testing purposes. For security reasons is recommended to use only your own certificates.

- Enabled: select this box if we wish to activate the OpenVN service in Client mode
- Mode: this option allows we to establish the connection mode for the VPN service. "Always On" will keep the VPN active at all times. "Under Request" will activate the VPN for the time we require. This option could be used in times of maintenance for example. If used, to activate the VPN service we will need to send an AT command (see Chapter 5 regarding AT commands) via SMS, Telnet, Webserver, SNMP or Modbus TCP. Once the time configured for an active service has passed, the VPN will be disconnected
- Protocol: this option allows we to establish the protocol for the activation of the VPN service. Either UDP or TCP can be used
- Port: the standard port is 1194 but we can change this in this field

- IP server: indicate the public IP address of the remote server that will act as the OpenVPN server
- Necessary files for OpenVPN
- In order to be able to use the MTX-Router-Titan devices as an OpenVPN client, we will need to create and update the following files: ca.crt (certificate of authenticity), client.crt (server certificate) and client.key (server private key)

Towards the bottom of the screen we will see that we can download example files. These must only be used in test mode. In real applications we should always generate our own certificates.

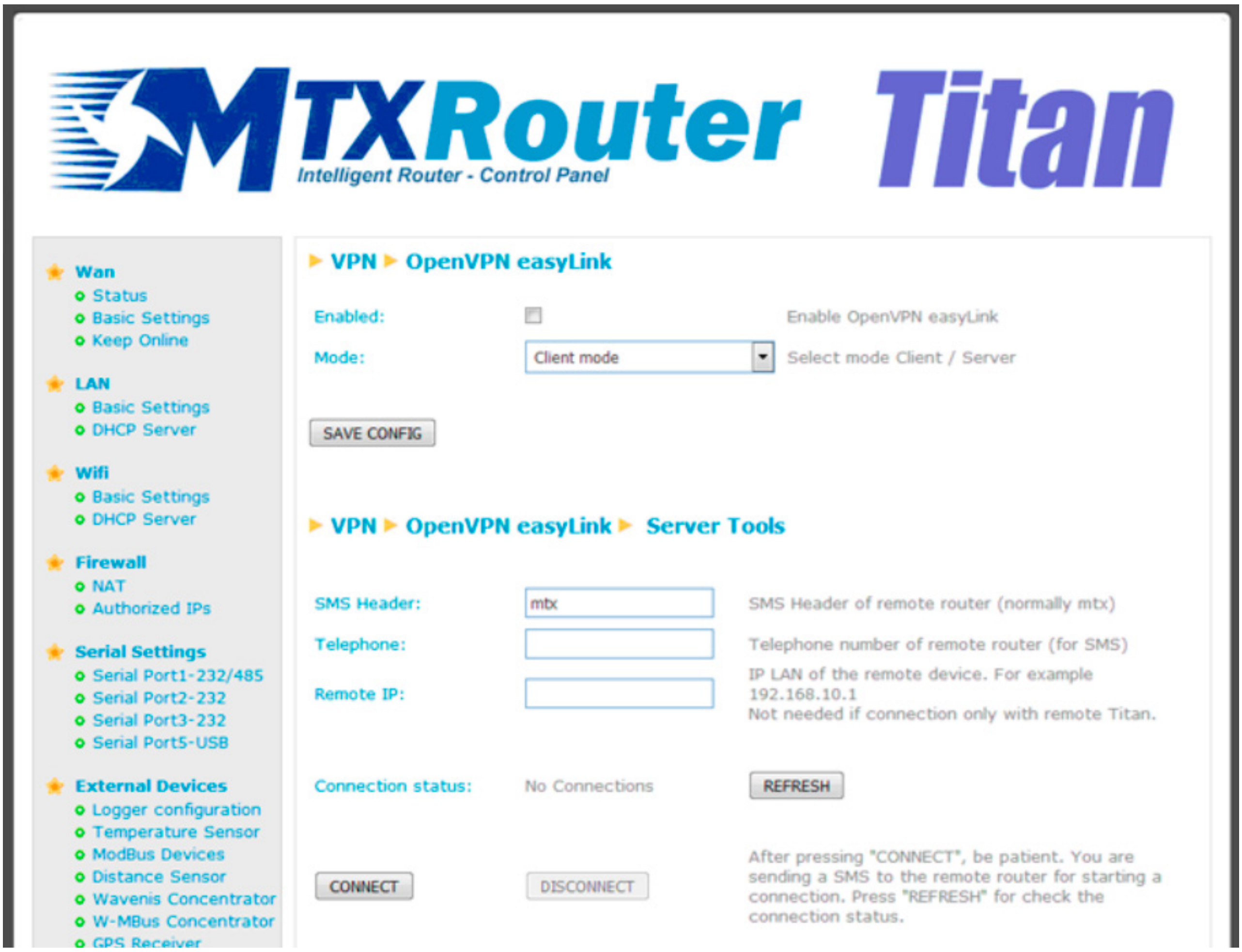
ADDITIONAL NOTES

- Once the configuration is complete, press the “SAVE CONFIG” button to save the changes. Remember that the router should be reset in order for the changes to take effect.

2.8.3 VPN: OpenVPN EasyLink

With OpenVPN EasyLink it is possible to establish an OpenVPN communication in a very simple and comfortable way in situations where it is necessary to perform a specific maintenance of a remote equipment.

In addition to its simplicity, it is very useful because it works regardless of whether the SIM cards used in remote Titan routers provide a public or private IP address. This way we do not need to worry about the GSM operator to use. What SIM cards should used is the SMS messaging service enabled. The reason is that, to start the EasyLink connection, the router acting as server will send an SMS to the remote router.



VPN ▸ OpenVPN easyLink

Enabled: □ Enable OpenVPN easyLink

Mode: Client mode Select mode Client / Server

VPN ▸ OpenVPN easyLink ▸ Server Tools

SMS Header: mtx SMS Header of remote router (normally mtx)

Telephone: Telephone number of remote router (for SMS)

Remote IP: IP LAN of the remote device. For example 192.168.10.1 Not needed if connection only with remote Titan.

Connection status: No Connections

After pressing "CONNECT", be patient. You are sending a SMS to the remote router for starting a connection. Press "REFRESH" for check the connection status.

- Enabled: check this box if we want to enable the OpenVPN EasyLink service
- Mode: we must set “Client mode” on the remote Titan routers, that is, they will be connected to the devices we want to manage. “Server mode” must be selected on the local Titan router which, connected to our PC, will use to establish the OpenVPN connection
- SMS header: here we must specify the SMS header that we configured on remote Titan routers, in the “Other -> SMS Control” configuration section
- Telephone: the SIM telephone number of the remote Titan router with which it is intended to communicate

- Remote IP: LAN IP of the remote device that we want to control

It has an application note: AN17-Router-Titan-OpenVPN-EasyLink.pdf where we will explain in a very detailed way how to use this feature.

ADDITIONAL NOTES

- Once the configuration is finished press the “SAVE CONFIG” button to save the changes. Remember to restart our router for the new changes to take effect.

3. AT Commands

The router's firmware allows AT commands to be sent directly to the internal modem via several interfaces:

1. Via a serial port
2. Via a 3G-Serial gateway (via 3G, Ethernet or WiFi)
3. Via SMS
4. Via Telnet (Remote Console, via 3G, Ethernet or WiFi)
5. Via Webserver (via 3G, Ethernet or WiFi)
6. Via Modbus TCP (via 3G, Ethernet or WiFi)

AT commands can be sent to the router under our responsibility. The accepted commands are those indicated in the Cinterior EHS5 AT Commands manual, as well as extra commands listed below:

```
AT^MTXTUNNEL=REBOOT
```

Action: resets the Titan router

```
AT^MTXTUNNEL=VERSION
```

Action: returns the Titan router's firmware version

```
AT^MTXTUNNEL=GETIP
```

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

```
AT^MTXTUNNEL=SETRELAY,1,0
```

Action: deactivates relay 1

```
AT^MTXTUNNEL=SETRELAY,1,1
```

Action: activates relay 1

```
AT^MTXTUNNEL=SETRELAY,2,0
```

Action: deactivates relay 2 (not available in Titan mini versions)

```
AT^MTXTUNNEL=SETRELAY,2,1
```

Action: activates relay 2 (not available in Titan mini versions)

```
AT^MTXTUNNEL=SETRELAY,2,1
```

Action: activates relay 2 (not available in Titan mini versions)

```
AT^MTXTUNNEL=GETTEMPERATURE
```

Action: returns the current temperature when the MTX-Temp-RS232 external device (temperature sensor) is connected

```
AT^MTXTUNNEL=GETDISTANCE
```

Action: returns the current distance when the Maxbotix external device (distance sensor) is connected

```
AT^MTXTUNNEL=TRAP,OID;myMessage;mySeverity
```

Action: allows an SNMP Trap to be sent with a specific OID and the corresponding message and severity

Example:`AT^MTXTUNNEL=TRAP,.1.3.6.1.4.1.45711.1.1.11.1.1;myMessage;5`

```
AT^MTXTUNNEL=SMS,telephoneNumber,message
```

Action: allows an SMS message to be sent to a specific number

Example: `AT^MTXTUNNEL=SMS,+34677123456,alarma de robo`

```
AT^MTXTUNNEL=EMAIL,destinationAddress,Subject
```

Action: allows an email to be sent to a specific email address. Configuration is required in the menu “Other > Email configuration”. Note that the text of the email is contained in the subject field only

Example: `AT^MTXTUNNEL=EMAIL,jgallego@matrix.es,temperature alarm`

```
AT^MTXTUNNEL=GETGPSPOSITION
```

Action: returns the GPS position when the MTX-Router-Titan-3G router includes an internal GPS module (or an external module that is connected via a USB or RS232 interface)

Example: `AT^MTXTUNNEL=GETGPSPOSITION`

```
AT^MTXTUNNEL=OVPNS,minutes
```

Action: if the VPN > OpenVPN Server section is configured as an on-demand OpenVPN service, the service can be activated in server mode for the specified time

Example: `AT^MTXTUNNEL=OVPNS,5 (This example activates the VPN for 5 minutes)`

```
AT^MTXTUNNEL=OVPNC,minutes
```

Action: if the VPN > OpenVPN Client section is configured as an on-demand OpenVPN service, the service can be activated in client mode for the specified time

Example: `AT^MTXTUNNEL=OVPNC,5 (This example activates the VPN for 5 minutes)`

```
AT^MTXTUNNEL=RESETCOUNTER,1
```

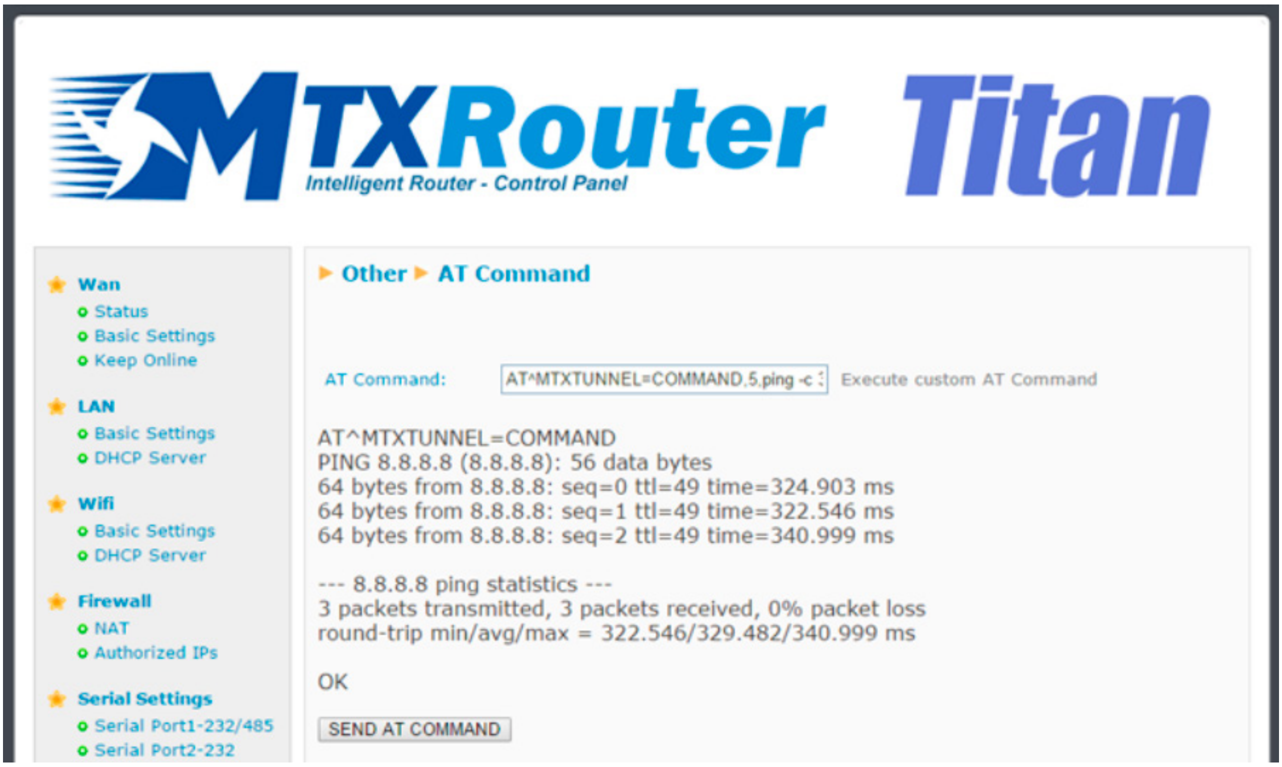
Action: if the digital input is used as a pulse counter, the count can be reset to the value specified in the command

Example: `AT^MTXTUNNEL=RESETCOUNTER,1 (This example resets the current value of the count to 1)`

```
AT^MTXTUNNEL=COMMAND,timeout,command
```

Action: this command allows we to carry out special commands in the Titan router. The commands currently available are “ping” and “traceroute”. A timeout (in seconds) can be specified as well as the command to be executed

Example: `AT^MTXTUNNEL=COMMAND,5,ping -c 3 8.8.8.8` (This example executes 3 pings to the IP 8.8.8.8 with a timeout of 5 seconds)



AT Command: AT^MTXTUNNEL=COMMAND,5,ping -c 3

```
AT^MTXTUNNEL=COMMAND
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=49 time=324.903 ms
64 bytes from 8.8.8.8: seq=1 ttl=49 time=322.546 ms
64 bytes from 8.8.8.8: seq=2 ttl=49 time=340.999 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 322.546/329.482/340.999 ms

OK
```

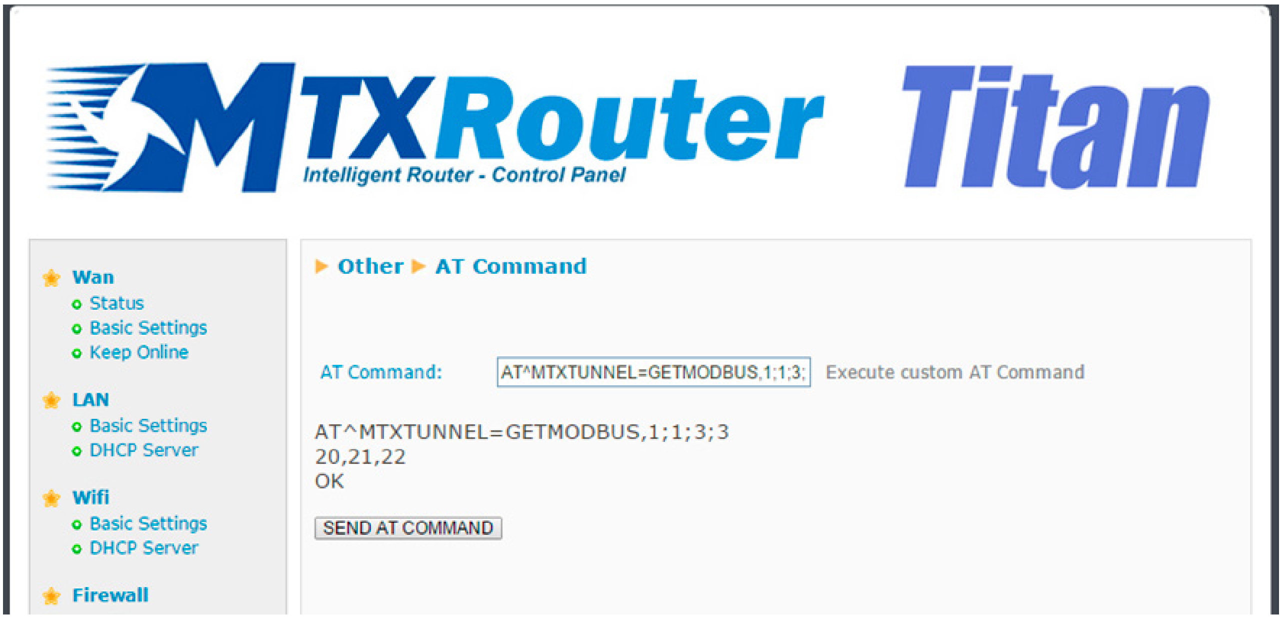
```
AT^MTXTUNNEL=GETMODBUS,ModbusAdd;FirstRegisterAdd;numWords;command
```

Action: returns the Modbus registers of a device where:

- ModbusAdd: Modbus device address (1, … , 255) or IP address:port
- FirstRegisterAdd: address of the first register to be read (0, … , 65535)
- numWords: number of Modbus registers to read (1, … , 64)
- command: command to read Modbus (3 or 4)

Example: `AT^MTXTUNNEL=GETMODBUS,192.168.1.200:502;1;1;3;3`

sent from a web configured environment (can also be sent via SMS or Remote Console (Telnet)), obtaining the values 20,21,22 as a response



AT Command: AT^MTXTUNNEL=GETMODBUS,1;1;3;

```
AT^MTXTUNNEL=GETMODBUS,1;1;3;3
20,21,22
OK
```

```
AT^MTXTUNNEL=SETMODBUS,ModbusAdd;FirstRegisterAdd;command;data1;
data2; … dataX
```

Action: establishes the Modbus registers of a device where:

- ModbusAdd: Modbus device address (1, … , 255) or IP address:port
- FirstRegisterAdd: address of the first register to be read (0, … , 65535)
- command: Modbus write command (6 or 16)
- data1,...,dataX: values of the Modbus registers to be written

Example: `AT^MTXTUNNEL=SETMODBUS,1;3;16;10;11;12;13;14;15`

sent from the configuration environment. This writes in the Modbus RTU device with address @1, starting in register 3 and using the Modbus writing command 16, the values 10, 11, 12, 13, 14 and 15.

Example:
`AT^MTXTUNNEL=SETMODBUS,192.168.1.202:502;3;16;10;11;12;13;14;15`

sent from the configuration environment. This writes in the Modbus TCP device with address and TCP port 192.168.1.202:502, starting in register 3 and using the Modbus writing command 16, the values 10, 11, 12, 13, 14 and 15.

```
AT^MTXTUNNEL=GETGSMLOCATION
```

Action: returns information of the telephony cell used. Can be useful as it obtains an approximate GPS position

```
AT^MTXTUNNEL=SETREDLED,onOff
```

Action: allow to activate / deactivate the red led from an AT command

- onOff: 0= Off/1== On

Example: `AT^MTXTUNNEL=SETREDLED,1` (This example will activate the red led of the Titan router)

```
AT^MTXTUNNEL=GETTEMPERATUREPROC
```

Action: returns the current temperature of the processor

Example:

```
AT^MTXTUNNEL=GETTEMPERATUREPROC
AT^MTXTUNNEL=GETTEMPERATUREPROC
50.75
OK
```

(This example returns the current processor temperature)

```
AT^MTXTUNNEL=GETTEMPERATUREGSM
```

Action: returns the current temperature of the Internal GSM module

Example:

```
AT^MTXTUNNEL=GETTEMPERATUREGSM
AT^MTXTUNNEL=GETTEMPERATUREGSM
40.25
OK
```

(This example returns the current GSM temperature of the module)

```
AT^MTXTUNNEL=GETTIME
```

Action: returns the current time. Useful for devices connected to the router, they will be able to use this command to synchronize their time.

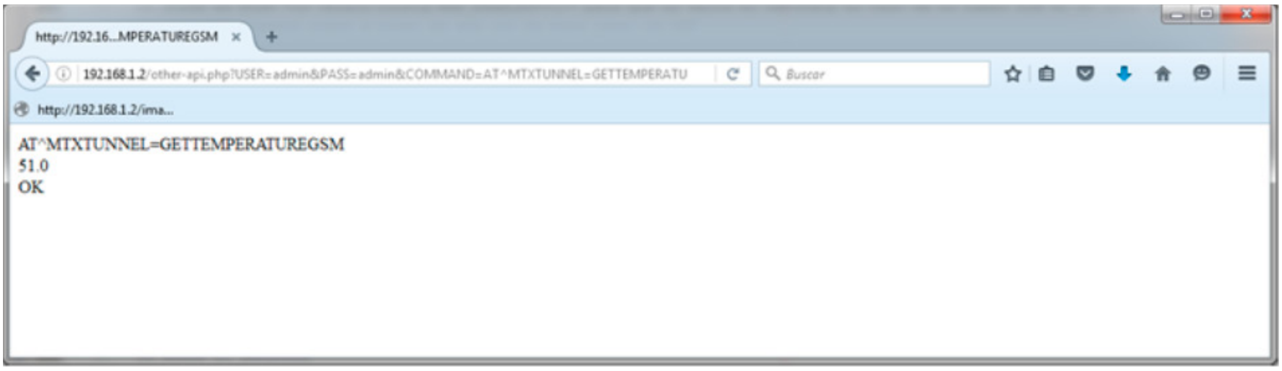
Example:

```
AT^MTXTUNNEL=GETTIME
```

```
AT^MTXTUNNEL=GETTIME
21/05/2016 10:56:52
OK
```

In addition to sending AT commands via SMS, Telnet, Modbus TCP, ... it is possible to send AT commands via HTTP GET both locally and remotely. For example, to execute a temperature read command of the GSM module, simply make a call like the following:

http://192.168.1.2/other-api.php?USER=admin&PASS=admin&COMMAND=AT^MTXTUNNEL=GETTEMPERATUREGSM


http://192.16...MPERATUREGSM
192.168.1.2/other-api.php?USER=admin&PASS=admin&COMMAND=AT^MTXTUNNEL=GETTEMPERATU
Buscar
http://192.168.1.2/ima...

```
AT^MTXTUNNEL=GETTEMPERATUREGSM
51.0
OK
```

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

Action: alows we to read the value of any configuration parameter of the Titan router. For example, we can check the configuration of each parameter of the Titan router from a Web Platform or from a device connected to the Eth or WiFi port of the Titan router. Check with Matrix Electrónica gsmsupport@matrix.es in case we want to use this command, as we will need the available parameter list.

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

Action: allows we to change the value of any configuration parameter of the Titan router. For example we can change the configuration of almost any parameter of the Titan router from a Web Platform or from a device connected to the Eth or WiFi port of the Titan router. Check with Matrix Electrónica gsmsupport@matrix.es in case we want to use this command, as we will need the available parameter list.

```
AT^MTXTUNNEL=ROUTERON,numMinutes
```

Action: in case the router is not configured for a permanent Internet connection, this command allows to activate the connection the very moment we want to during the time specified in "numMinutes." It can be from 1 to 1440. Similarly, if we want to end the Internet connection before time runs out, we can do it with the same command and specifying the value 0 in the parameter "numMinutes".

4. Plugins

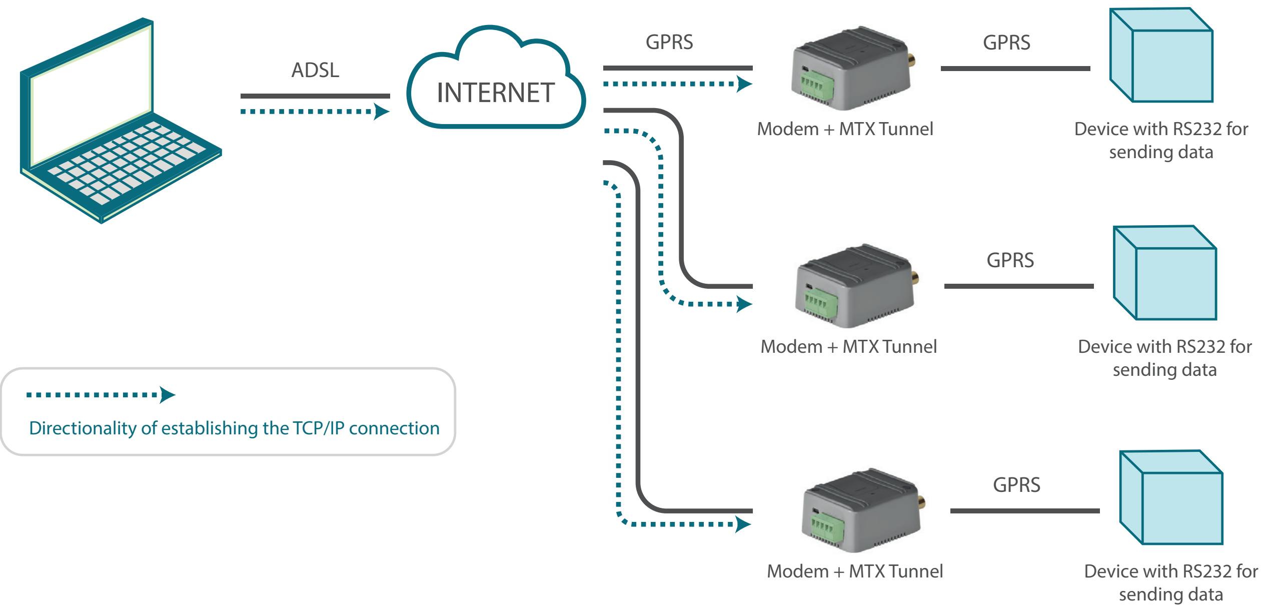
Plugins are small, independent utilities that are included in the Titan routers. If we require a peculiar characteristic that cannot be found in the current characteristics, let us know at gsmsupport@matrix.es. Depending on the size of the project, this could be included as a plugin for free.

Given that the plugins are independent utilities, when a copy of the Titan configuration is created, it is not necessary for the plugin section to be replicated

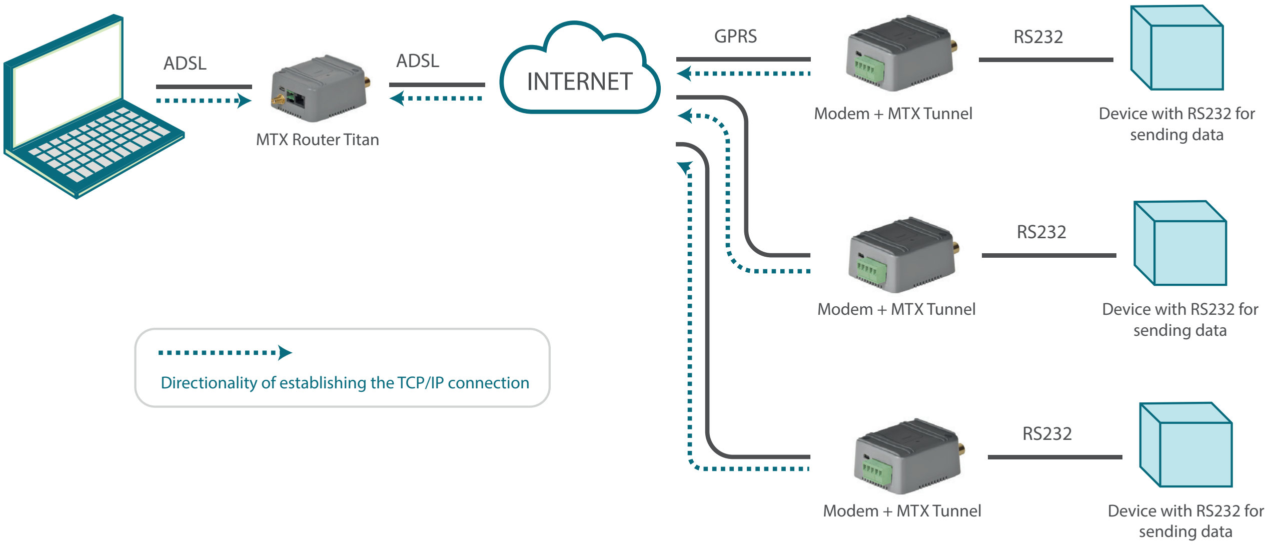
4.1 Plugin “No-Nat”

The “No-Nat” plugin is specifically designed for IP/Serial gateway situations that have NAT problems; for example, if we have a series of MTX-65i + MTX-Tunnel modems to create a GPRS-RS232 transparent gateway but we have NAT problems (for example, our telephone operator provides SIM cards with private, not public IP address), and we have a PC that uses third party software that only allows we to input IP addresses and ports of the remote devices to create the connection.

A typical representation would be as follows:


ADSL
INTERNET
GPRS
GPRS
Modem + MTX Tunnel
Device with RS232 for sending data
GPRS
Modem + MTX Tunnel
Device with RS232 for sending data
GPRS
Modem + MTX Tunnel
Device with RS232 for sending data
Directionality of establishing the TCP/IP connection

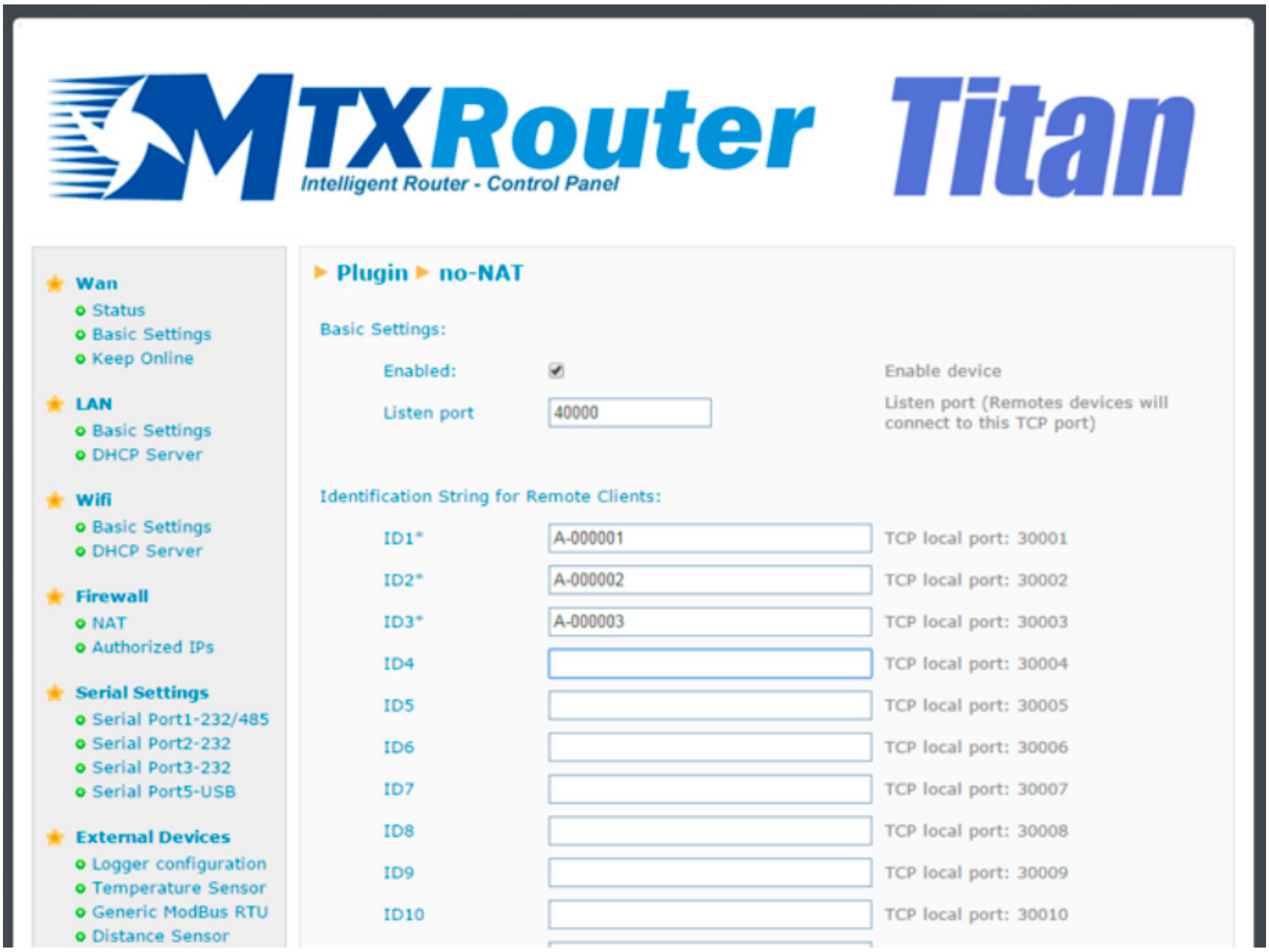
However, our GSM operator does not allow this as it blocks all incoming connections to modems. What we can do with the Titan router is the following:


ADSL
MTX Router Titan
ADSL
INTERNET
GPRS
Modem + MTX Tunnel
RS232
Device with RS232 for sending data
Modem + MTX Tunnel
RS232
Device with RS232 for sending data
Modem + MTX Tunnel
RS232
Device with RS232 for sending data
Directionality of establishing the TCP/IP connection

In other words, the MTX-Tunnel modems connect in client mode, meaning that they do not affect the NATs nor the majority of Firewalls. The connection is not made directly with with PC, yet using an intermediary, i.e. using the Titan router's No-NAT plugin.

On the other hand, our control software will also connect to the Titan's No-NAT plugin, meaning the Titan router will act as an intermediary between the PC and the different modems.

We will illustrate this with an example:



▶ Plugin ▶ no-NAT

Basic Settings:

Enabled:	☑	Enable device
Listen port	40000	Listen port (Remotes devices will connect to this TCP port)

Identification String for Remote Clients:

ID1*	A-000001	TCP local port: 30001
ID2*	A-000002	TCP local port: 30002
ID3*	A-000003	TCP local port: 30003
ID4		TCP local port: 30004
ID5		TCP local port: 30005
ID6		TCP local port: 30006
ID7		TCP local port: 30007
ID8		TCP local port: 30008
ID9		TCP local port: 30009
ID10		TCP local port: 30010

In this case, we must configure the GPRS modems (MTX-Tunnel) to work in client mode (MTX_mode: client) and so that an identificative chain is sent so that the Titan knows which MTX-Tunnel each connection corresponds to. For example, we can make MTX-Tunnel 1 send "A-000001" (MTX_IDClient: A-000001) as the identificative chain and MTX-Tunnel devices 2 and 3 will send "A-000002" and "A-000003" respectively. Each of them must connect to the TCP port 40000 in the Titan router.

On the other hand, the PC must connect to the Titan's IP address (for example the local Ethernet address 192.168.1.2) when it wishes to connect to the MTX-Tunnel 1 modem, as well as the corresponding TCP port. For example, to connect to the MTX-Tunnel 1 device, the Titan port 30001 will be used.

Once connected to a socket, the data sent by the PC will be received by the Titan an then reset by the corresponding socket to the MTX-Tunnel to which we wish to connect. Once this data reaches the MTX-Tunnel device, it will be resent by the serial port

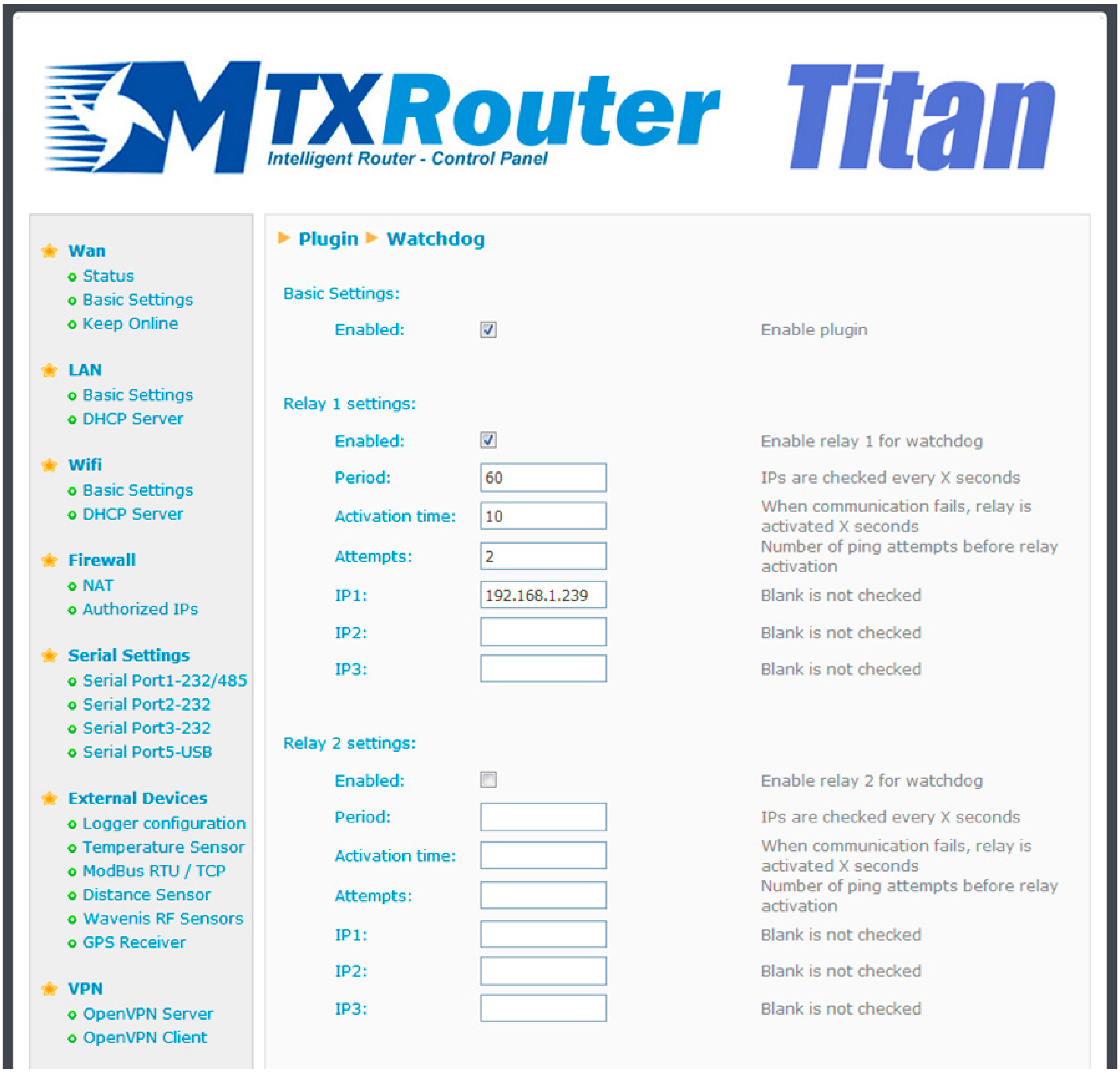
4.2 Plugin "Watchdog"

The Titan routers include watchdog hardware. In the unlikely event of severe problems, such as a blocked device, the watchdog will reset the Titan router completely. However, we must also know what happens when the block occurs in a device that is connected to the router, for example an IP camera, PLC, analyzer, meterological stations, etc.

The Watchdog plugin allows a periodic ping to be configured This will be sent by one of the Titan router's interfaces (usually Ethernet, but it could also be WiFi or 3G). If the ping fails X times (where X is a configurable variable), a relay can be configured in the Titan device that restarts the external device that has caused the failure, either by carrying out a standard reset or by cutting off its power supply for a specific period of time.

- Enable Plugin: this option activates the plugin
- Relay1 enable: this option configures Relay 1 so that it is activated when a block is detected in a connected device
- Period: this field specifies the number of seconds between pings made to the device
- Activation time: this field specifies the duration (in seconds) for which the relay should be activated in the event of a block being detected
- Attempts: this field indicates the number of ping attempts that should be made
- IP1, IP2, IP3: in this field, we should indicate the IP address of the device to be supervised

Either one or two relays can be configured, depending on the number included in our device (1 relay for the MTX-Router-Titan mini device and 2 relays for the MTX-Tunnel-Titan device).



▶ Plugin ▶ Watchdog

Basic Settings:

Enabled:	☑	Enable plugin

Relay 1 settings:

Enabled:	☑	Enable relay 1 for watchdog
Period:	60	IPs are checked every X seconds
Activation time:	10	When communication fails, relay is activated X seconds
Attempts:	2	Number of ping attempts before relay activation
IP1:	192.168.1.239	Blank is not checked
IP2:		Blank is not checked
IP3:		Blank is not checked

Relay 2 settings:

Enabled:	□	Enable relay 2 for watchdog
Period:		IPs are checked every X seconds
Activation time:		When communication fails, relay is activated X seconds
Attempts:		Number of ping attempts before relay activation
IP1:		Blank is not checked
IP2:		Blank is not checked
IP3:		Blank is not checked

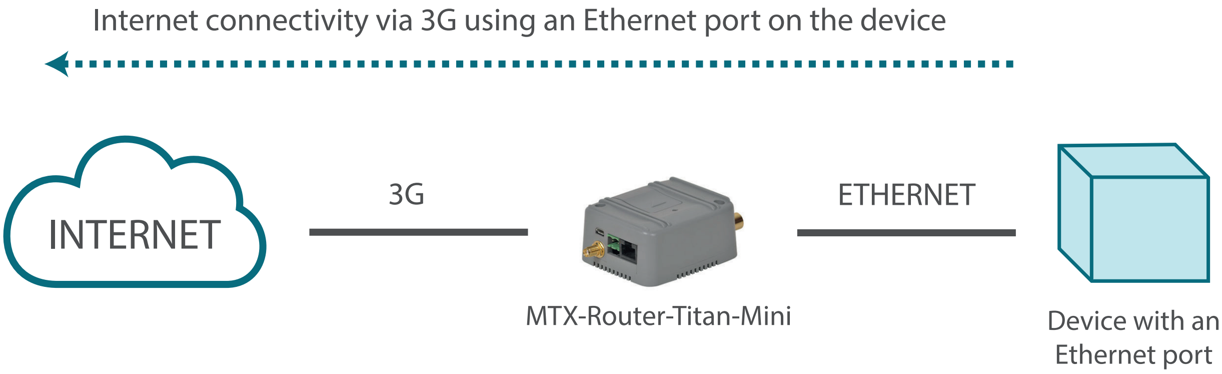
ANNEX1: BASIC EXAMPLE SCENARIOS AND CONFIGURATIONS

Example Scenario 1.1: Configuration to provide a PLC device with an Ethernet port with access to the Internet

Details of the example scenario:

- We have a PLC device with ETH port that we want to provide with Internet access in order to send data to the Cloud. The PLC has a local IP address of 192.168.1.70
- We need to be able to access the router's configuration remotely in the standard TCP port 80
- SIM cards with fixed IP address are used

Solution: MTX-Router-Titan mini router

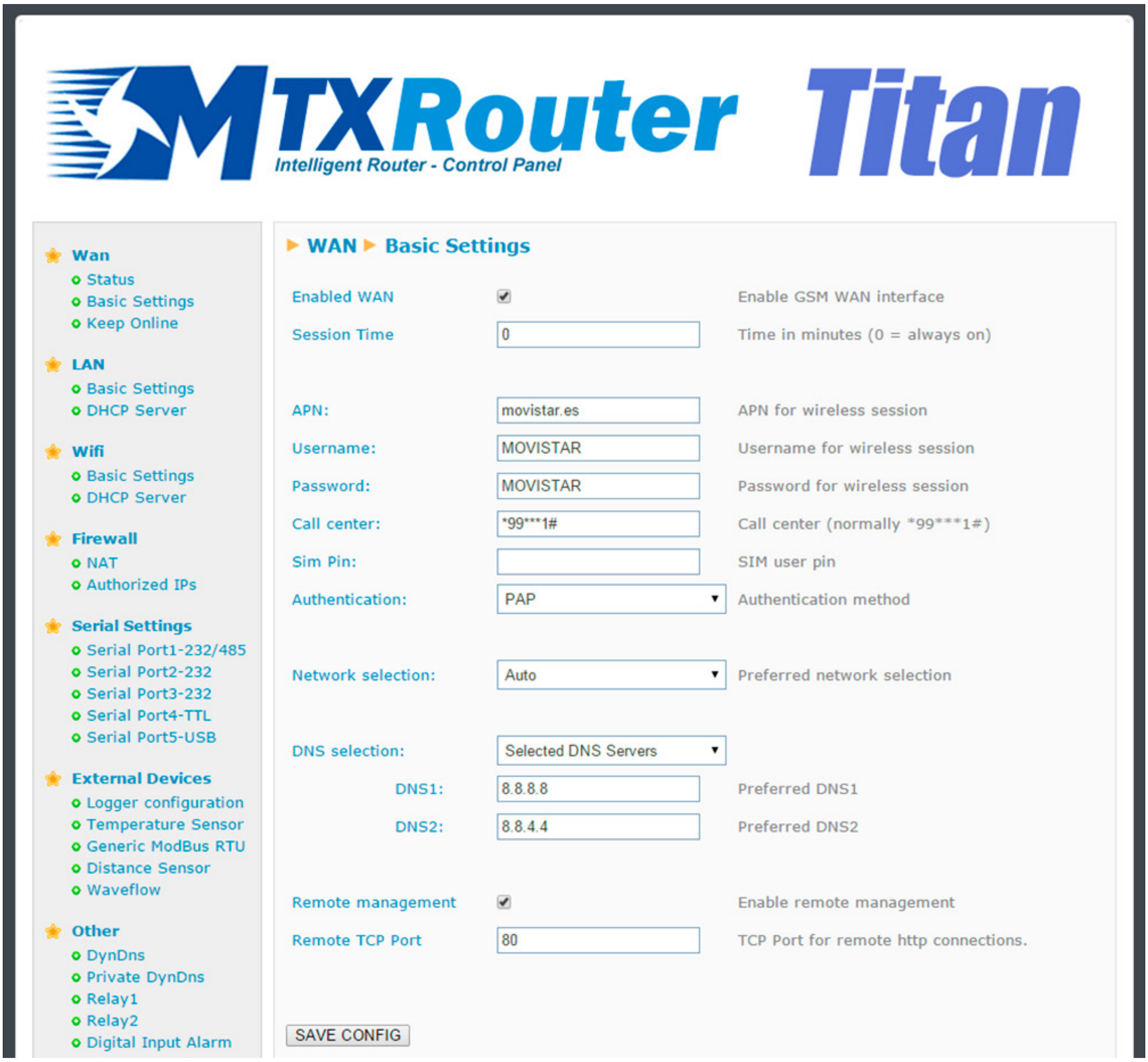

Internet connectivity via 3G using an Ethernet port on the device
INTERNET
3G
ETHERNET
MTX-Router-Titan-Mini
Device with an Ethernet port

Example configuration ready for use:

We can easily load the example from the router's web configuration environment from the menu "Other>Backup/Examples".

Details:

1. After the configuration is loaded in our router, we can access the router's configuration with the default username and password: "admin" and "admin", and the IP address"192.168.1.2"
2. Check the configuration in the menus "Wan>Basic Settings"
3. Remember that in order to work, the PLC's IP address should be in the range of the router's LAN IP address and we should specify the PLC's Gateway IP address with the router's LAN IP address. In this example, it would be 192.168.1.2



▶ WAN ▶ Basic Settings

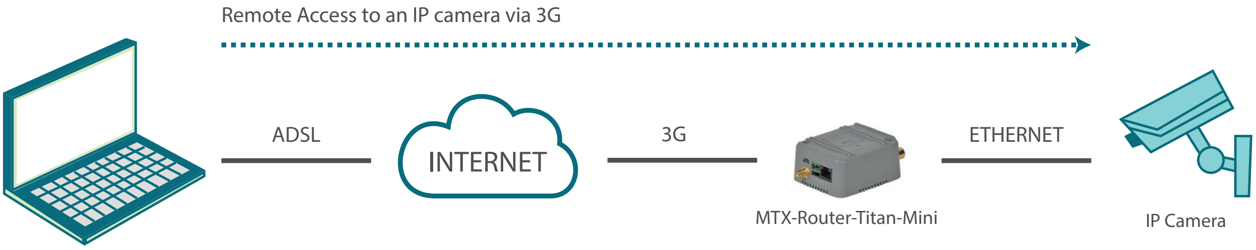
Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP ▾	Authentication method
Network selection:	Auto ▾	Preferred network selection
DNS selection:	Selected DNS Servers ▾	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	80	TCP Port for remote http connections.

Example Scenario 1.2: Configuration to provide Internet access and remotely connect an IP camera with an Ethernet port

Details of the example scenario:

- We have an IP camera with Ethernet port that we want to provide with Internet access. The camera has a local IP address of 192.168.1.70
- The IP camera has an internal webserver that we can use to access the video that is being recorded. The TCP port used by the camera is TCP80 and it cannot be changed. Since we also want to be able to remotely access the router in order to access the configuration, we must change the TCP port of the remote configuration from the TCP port 80 to the TCP port 8080 so that there are not conflicts with the camera port
- We also need the remote configuration to have access to the Internet from any IP address. Therefore, only the IP addresses 200.1.2.3 and 200.1.2.4, corresponding to the central offices, will be able to access the IP camera
- SIM cards with fixed IP address will be used

Solution: MTX-Router-Titan mini router

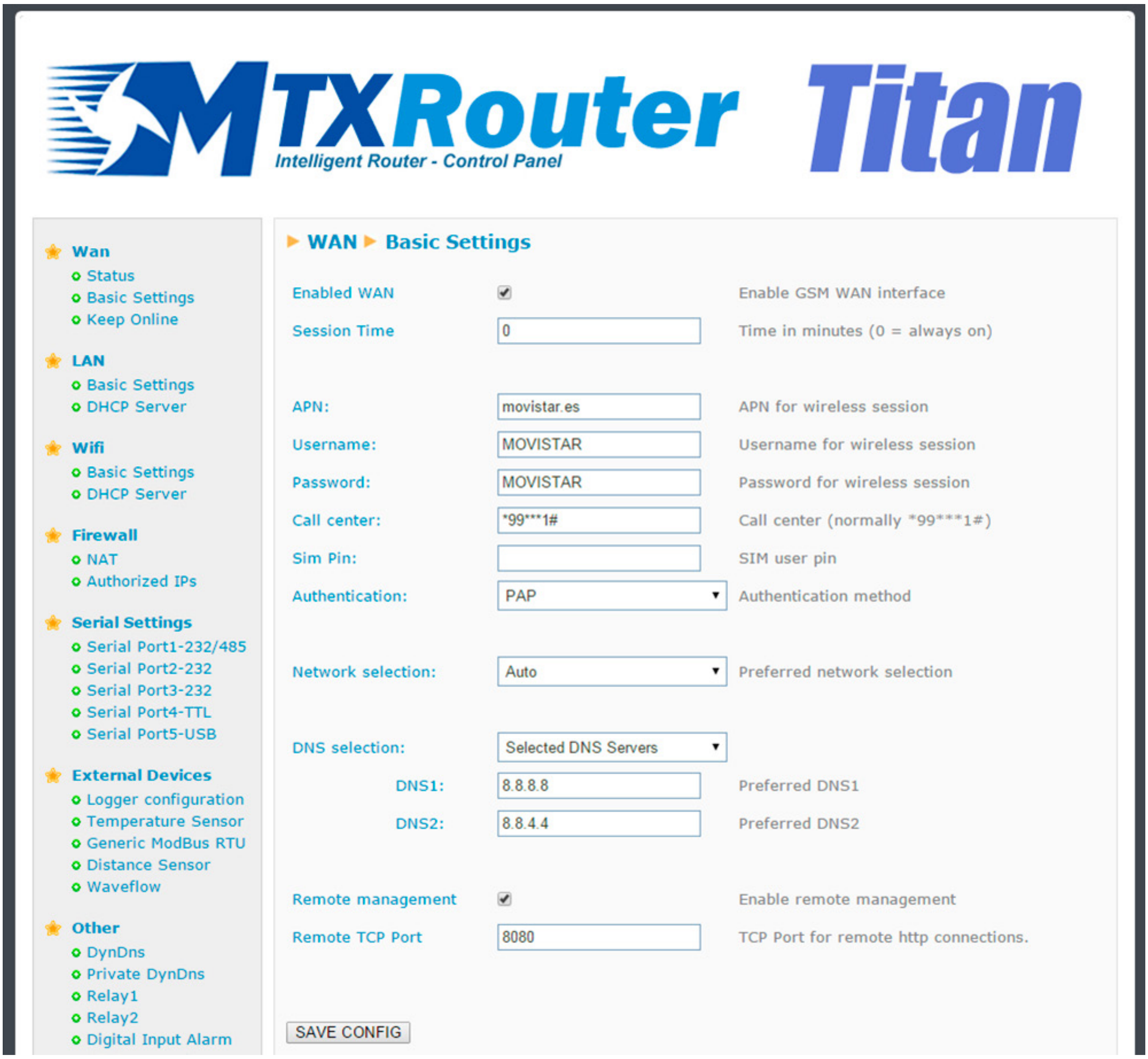


Configuration example ready for use:

Load the example from the web configuration environment from the menu “Other>Backup/Examples”.

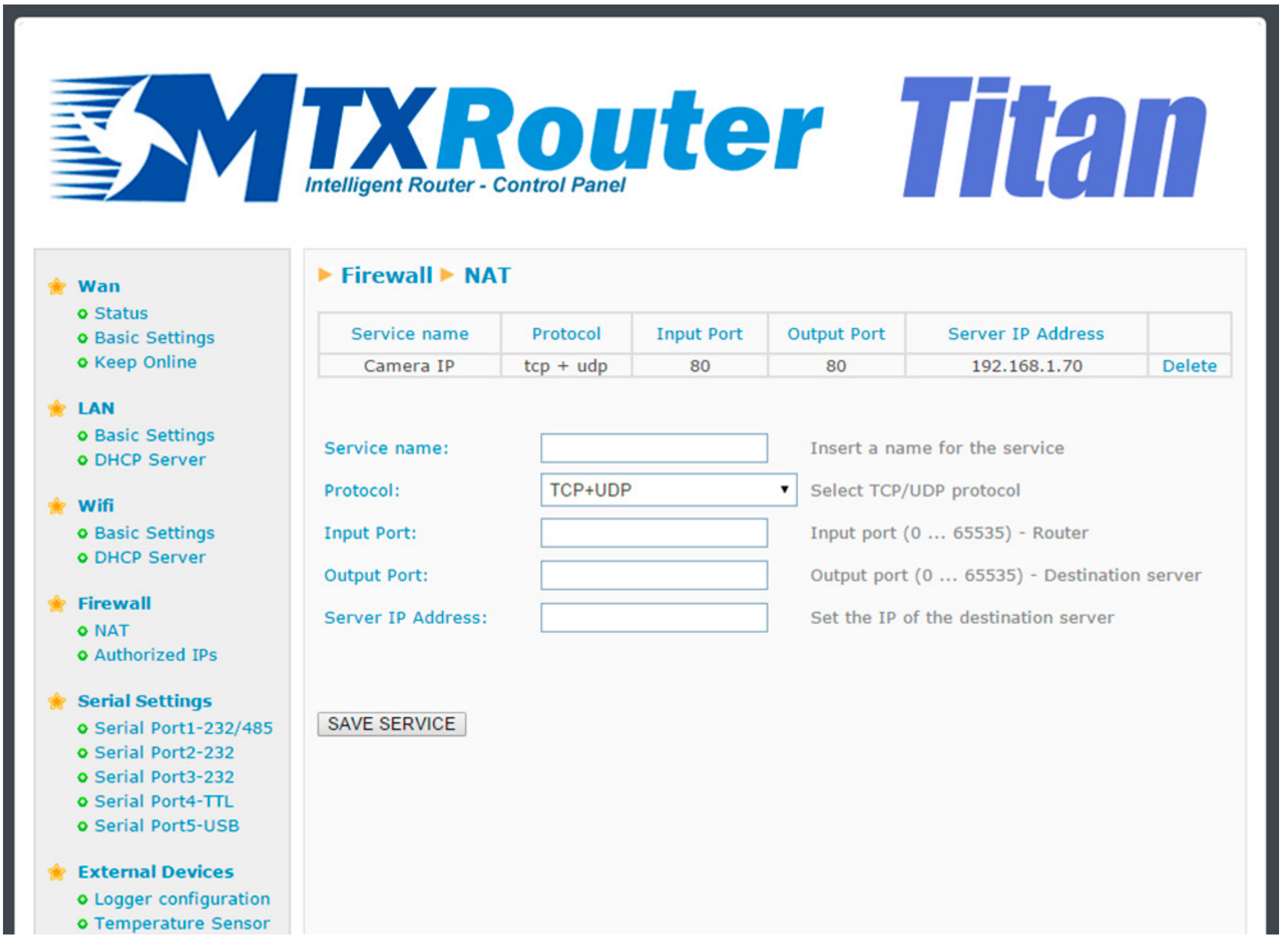
Details:

1. After the configuration is loaded in our router, we can access the router’s configuration with the default username and password: “admin” and “admin”, and the IP address“192.168.1.2”
2. Check the configuration in the menus “Wan>Basic Settings”, “Firewall > NAT”, “Firewall > Authorized IPs”
3. In order to access the TCP port 80 belonging to the camera, we need to create an NAT. In other words, we need to redirect traffic that arrives in the router’s TCP80 port to the internal IP address and TCP port belonging to the camera; i.e. to the IP 192.168.1.70
4. Remember that in order to work, the camera’s IP address should be in the range of the router’s LAN IP address and we should specify the camera’s Gateway IP address with the router’s LAN IP address. In this example, it would be 192.168.1.2



▶ WAN ▶ Basic Settings

Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP	Authentication method
Network selection:	Auto	Preferred network selection
DNS selection:	Selected DNS Servers	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	8080	TCP Port for remote http connections.

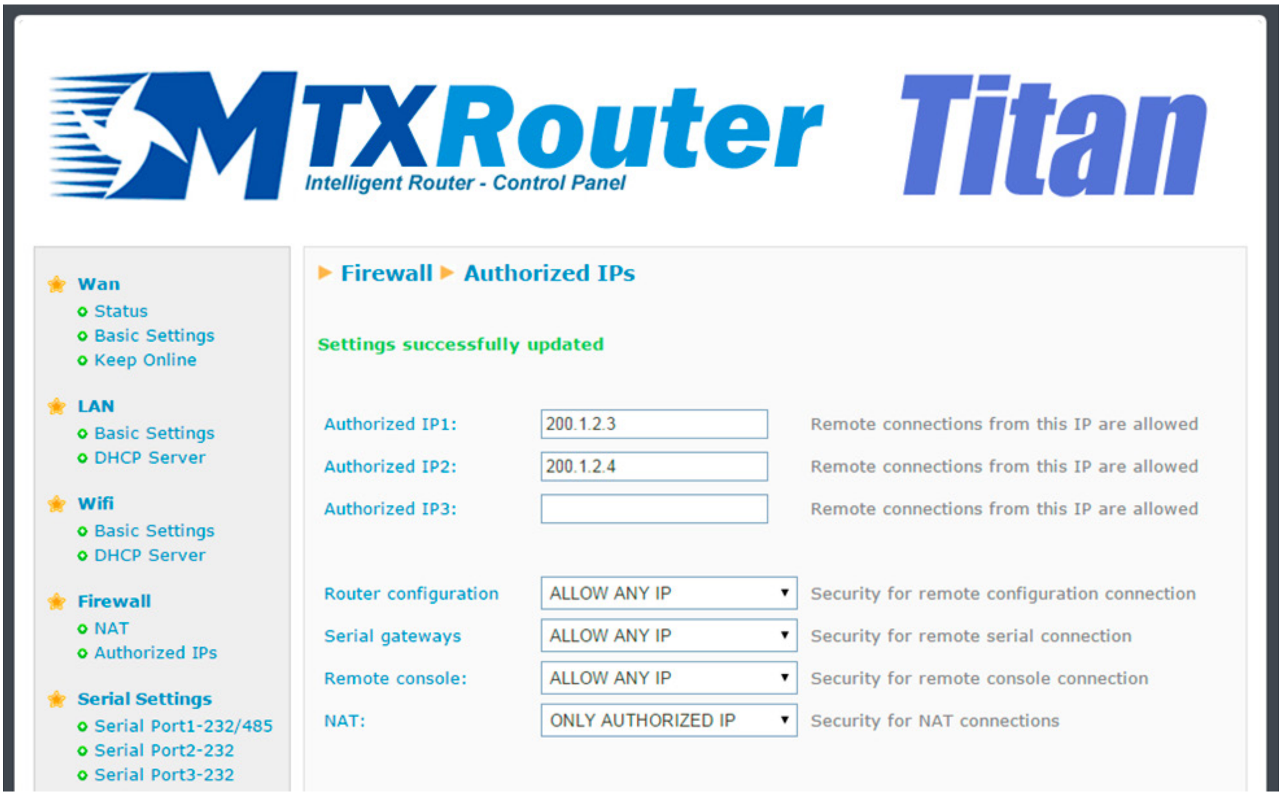


▸ Firewall ▸ NAT

Service name	Protocol	Input Port	Output Port	Server IP Address	
Camera IP	tcp + udp	80	80	192.168.1.70	Delete

Service name:		Insert a name for the service
Protocol:	TCP+UDP ▾	Select TCP/UDP protocol
Input Port:		Input port (0 ... 65535) - Router
Output Port:		Output port (0 ... 65535) - Destination server
Server IP Address:		Set the IP of the destination server

SAVE SERVICE



▸ Firewall ▸ Authorized IPs

Settings successfully updated

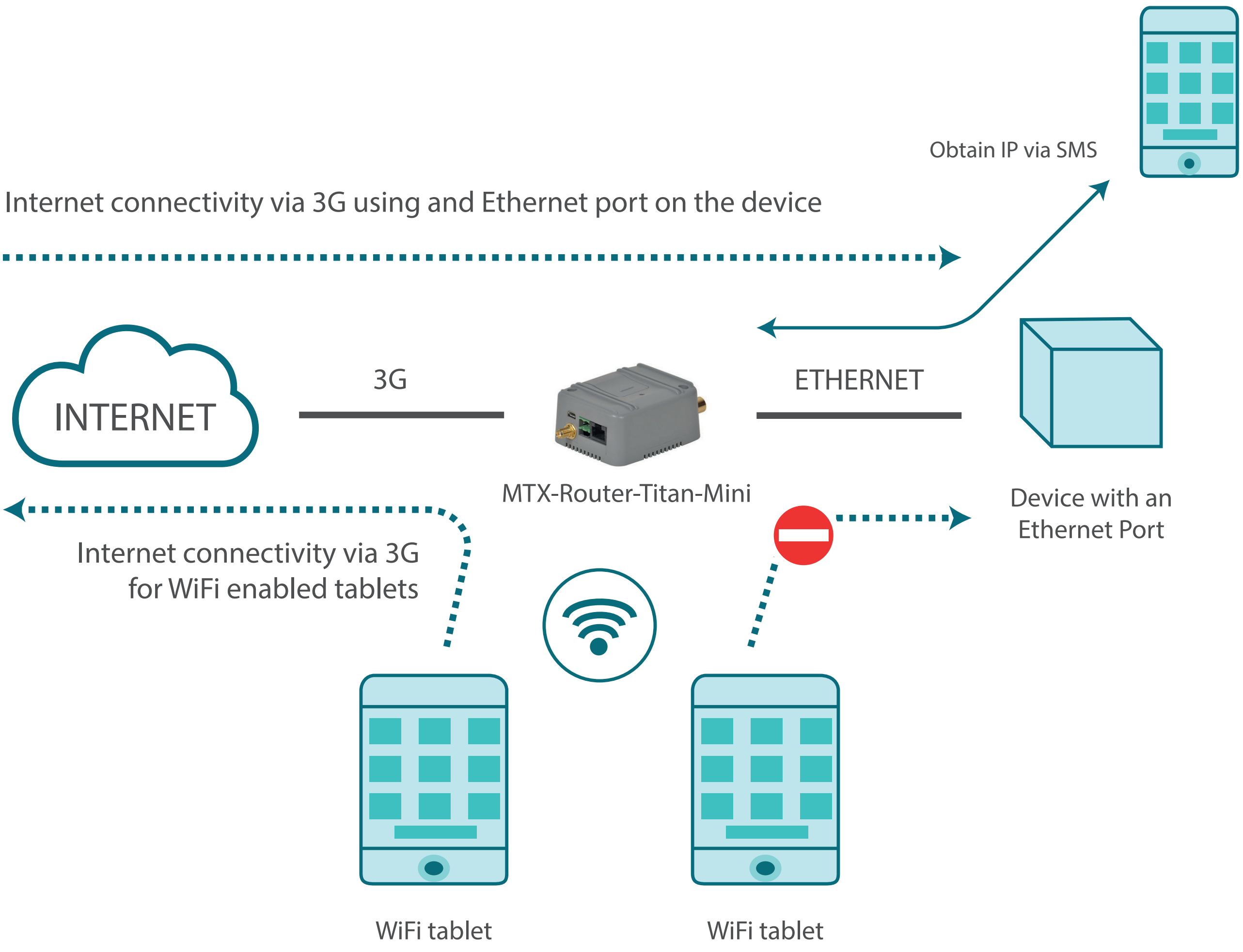
Authorized IP1:	200.1.2.3	Remote connections from this IP are allowed
Authorized IP2:	200.1.2.4	Remote connections from this IP are allowed
Authorized IP3:		Remote connections from this IP are allowed
Router configuration	ALLOW ANY IP ▾	Security for remote configuration connection
Serial gateways	ALLOW ANY IP ▾	Security for remote serial connection
Remote console:	ALLOW ANY IP ▾	Security for remote console connection
NAT:	ONLY AUTHORIZED IP ▾	Security for NAT connections

Example Scenario 1.3: Configuration to provide Internet access to a device with an Ethernet port and to several devices with WiFi connectivity

Details of the example scenario:

- We have a device with ETH port which we want to provide with Internet access to send data to the Cloud. The Ethernet device has a local IP address of 192.168.1.70
- We should also be able to provide several other WiFi devices (tablets) with Internet access. These devices will connect to the router using DHCP (given they do not have a fixed LAN IP address). The WiFi devices must not have access to the Ethernet device that is connected to the router; we must only provide them with Internet access
- We have to be able to access the router's configuration remotely in the standard TCP port 80
- A SIM card with a dynamic IP address will be used. We do not want to use services such as DynDNS or No-IP therefore we need to be able to obtain the router's IP address at any time via a missed call or SMS. Via this IP we will be able to access the router's configuration at any time

Solution: MTX-Router-Titan mini router

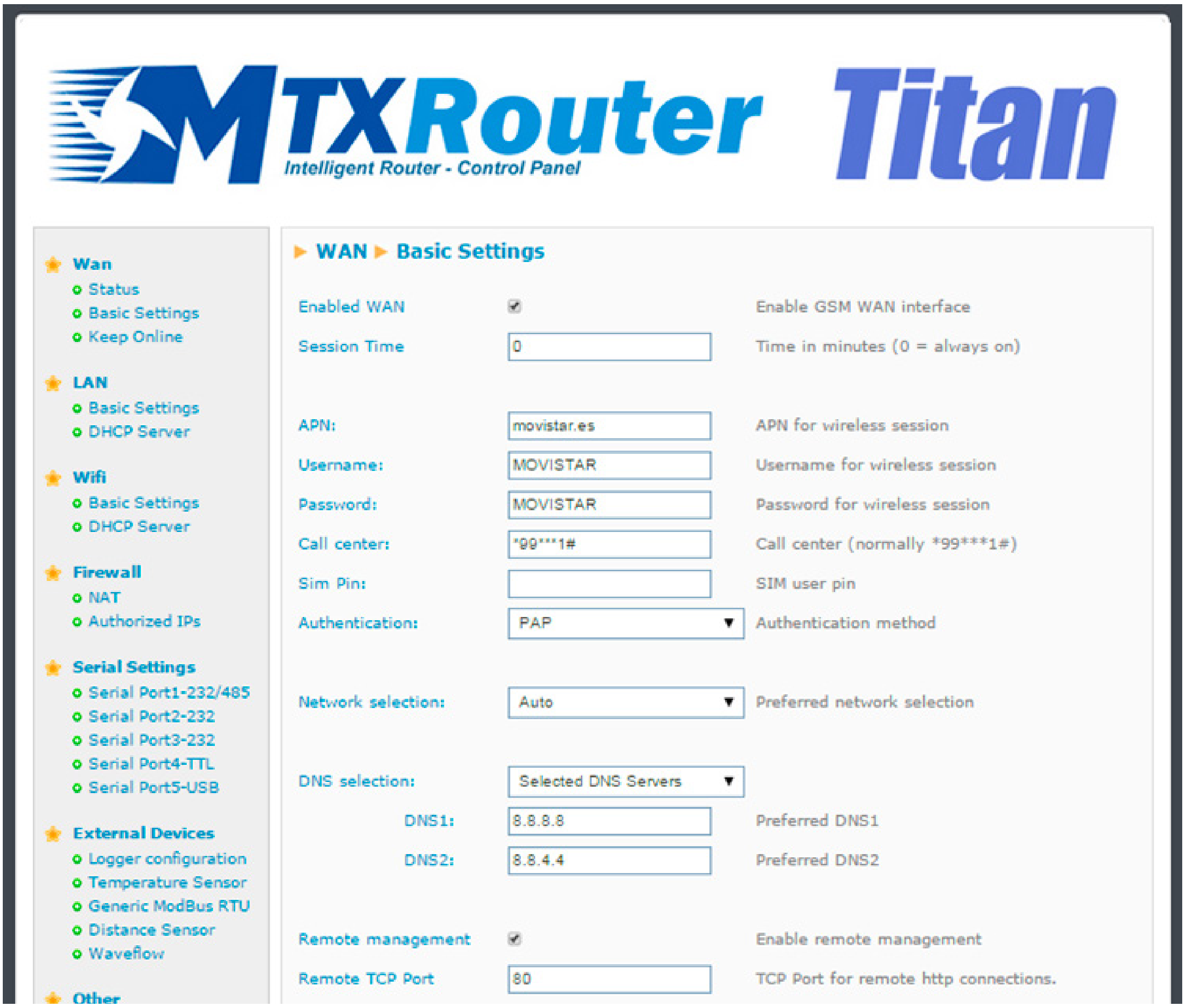

Obtain IP via SMS
Internet connectivity via 3G using and Ethernet port on the device
INTERNET
3G
ETHERNET
MTX-Router-Titan-Mini
Device with an Ethernet Port
Internet connectivity via 3G for WiFi enabled tablets
WiFi tablet
WiFi tablet

Configuration example ready for use:

Load the example from the web configuration environment from the menu “Other>Backup/Examples”.

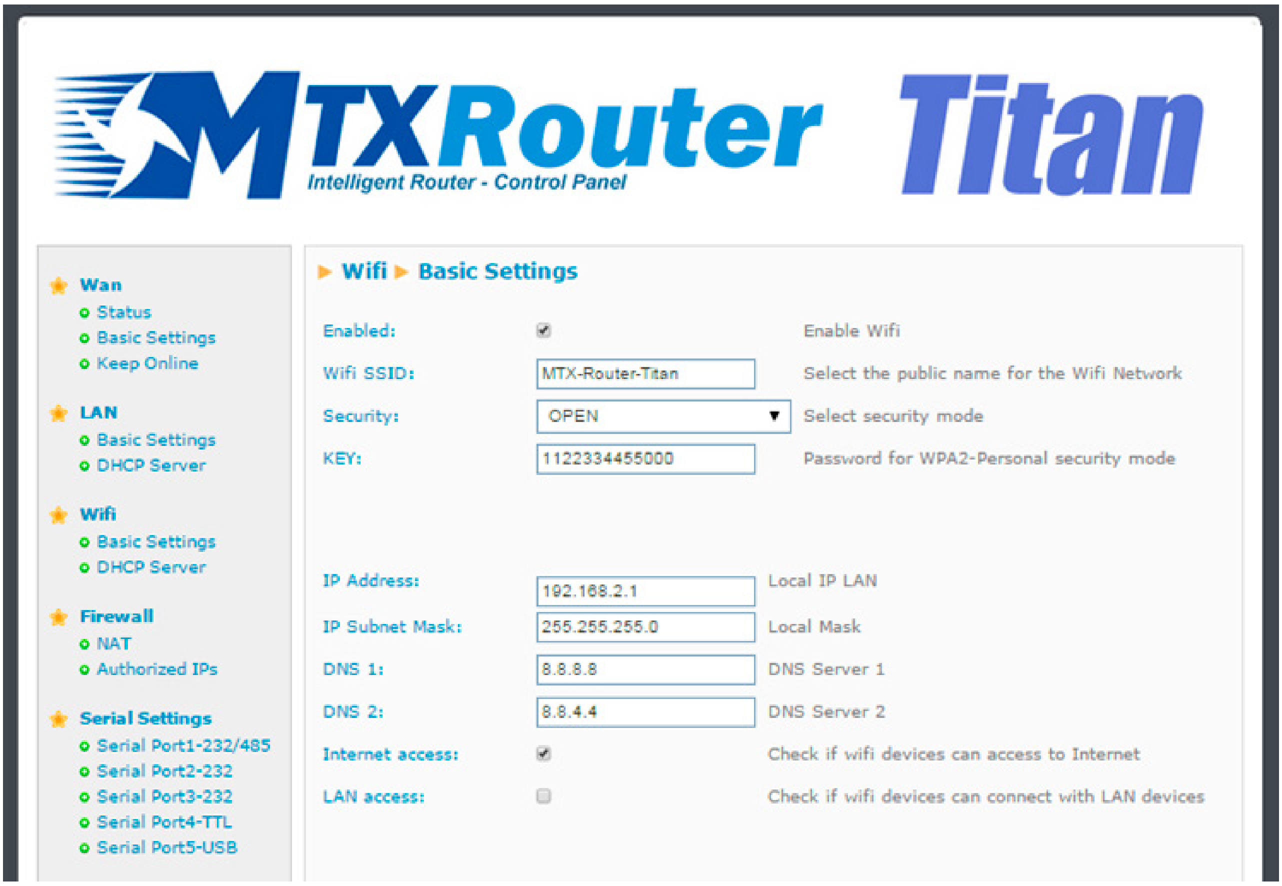
Details:

1. After the configuration is loaded in our router, we can access the router’s configuration with the default username and password: “admin” and “admin”, and the IP address“192.168.1.2”
2. Check the configuration in “Wan>Basic Settings”, “WiFi>Basic Settings”, “WiFi>DHCP Server”, “Other>Sms Control”
3. We must specify the PLC’s Gateway IP address with the router’s LAN IP address: 192.168.1.2
4. To obtain the IP address via a missed call, make sure the SIM card voice-calling services are activated. If voice-calling is restricted, it will only be possible to obtain the IP address via an SMS since these are not usually limited, although we should check this too
5. Send SMS with “mtx AT+IP” or make a missed call to obtain the MTX router’s current IP address.



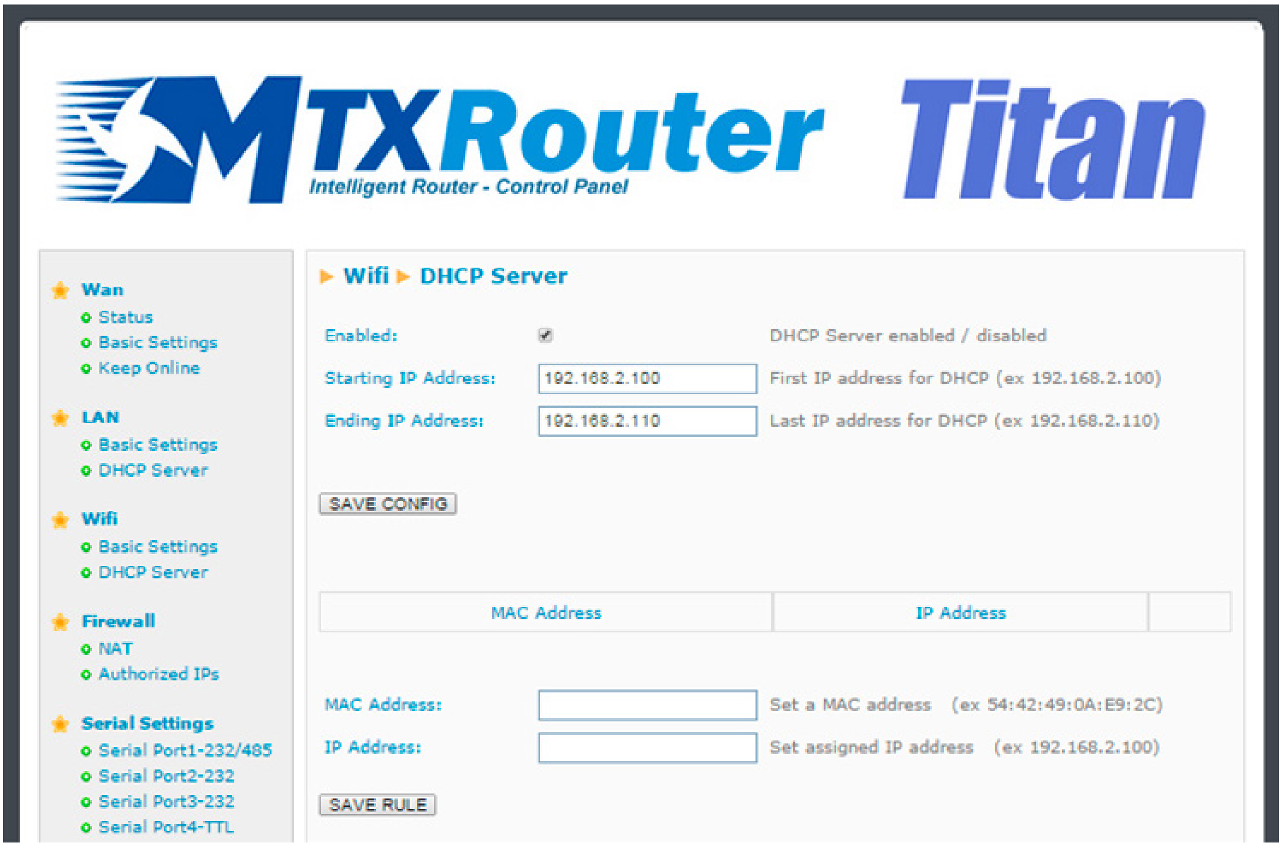
▶ WAN ▶ Basic Settings

Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP ▼	Authentication method
Network selection:	Auto ▼	Preferred network selection
DNS selection:	Selected DNS Servers ▼	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	80	TCP Port for remote http connections.



▸ Wifi ▸ Basic Settings

Enabled:	☑	Enable Wifi
Wifi SSID:	MTX-Router-Titan	Select the public name for the Wifi Network
Security:	OPEN ▾	Select security mode
KEY:	1122334455000	Password for WPA2-Personal security mode
IP Address:	192.168.2.1	Local IP LAN
IP Subnet Mask:	255.255.255.0	Local Mask
DNS 1:	8.8.8.8	DNS Server 1
DNS 2:	8.8.4.4	DNS Server 2
Internet access:	☑	Check if wifi devices can access to Internet
LAN access:	□	Check if wifi devices can connect with LAN devices

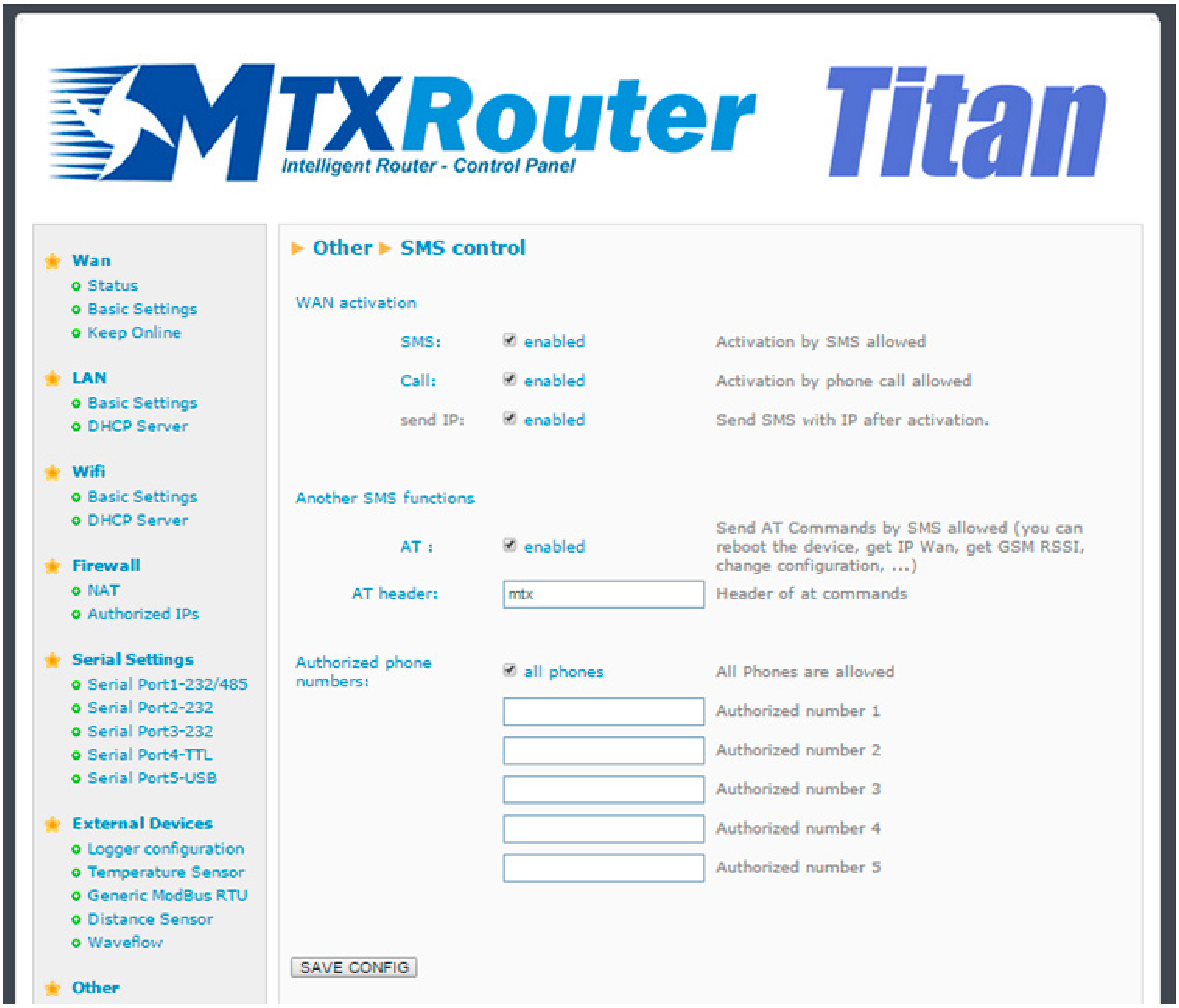


▸ Wifi ▸ DHCP Server

Enabled:	☑	DHCP Server enabled / disabled
Starting IP Address:	192.168.2.100	First IP address for DHCP (ex 192.168.2.100)
Ending IP Address:	192.168.2.110	Last IP address for DHCP (ex 192.168.2.110)

MAC Address	IP Address	

MAC Address:		Set a MAC address (ex 54:42:49:0A:E9:2C)
IP Address:		Set assigned IP address (ex 192.168.2.100)



▶ Other ▶ SMS control

WAN activation

SMS: ☑ enabled — Activation by SMS allowed

Call: ☑ enabled — Activation by phone call allowed

send IP: ☑ enabled — Send SMS with IP after activation.

Another SMS functions

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

AT header: mtx — 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

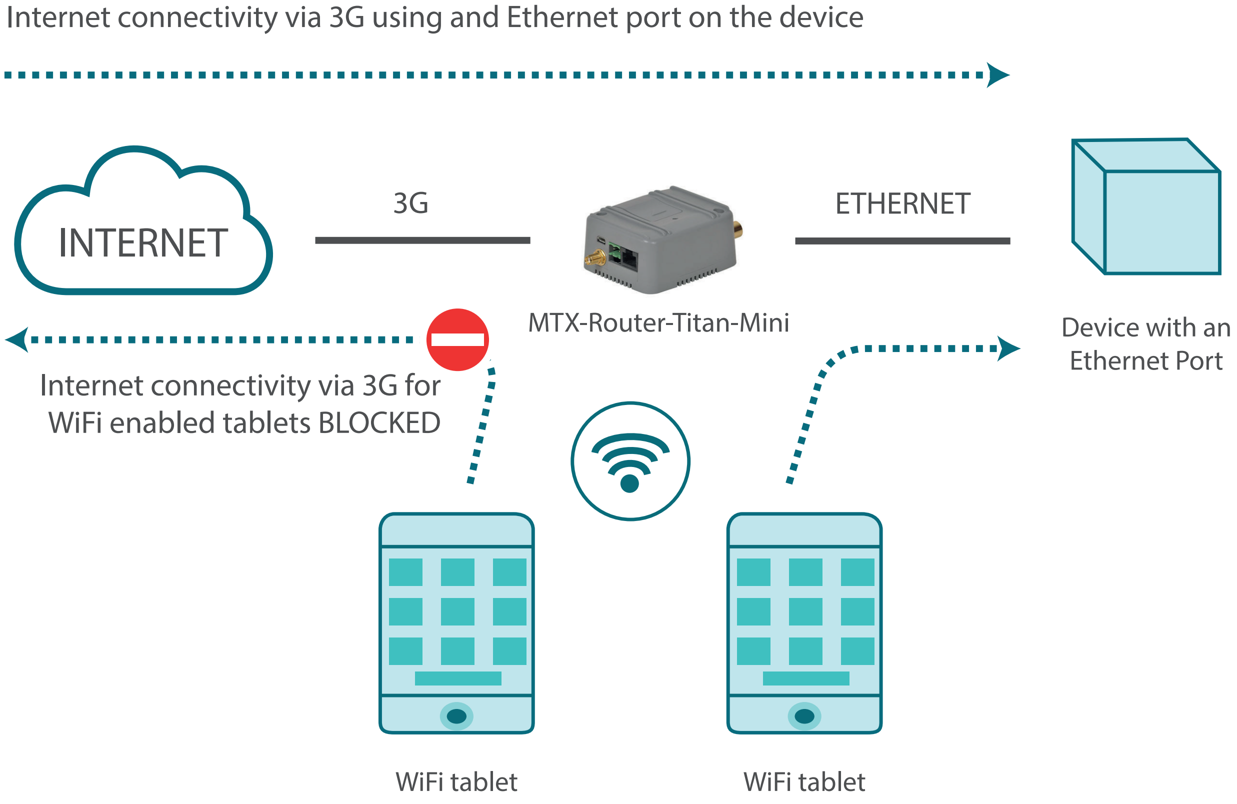
Authorized number 5

Example Scenario 1.4: Configuration to provide a PLC device with an Ethernet port with Internet access. WiFi devices will be able to access the Ethernet device but Internet access for the WiFi devices will be blocked

Details of the example scenario:

- We have a PLC device with an ETH port which we want to provide with Internet access to send data to the Cloud. The PLC has a local IP address of 192.168.1.1
- Several tablets will also connect to the router via WiFi (DHCP) which will need to be able to connect to the Ethernet device which is connected to the router for maintenance tasks, although Internet accesss must also be blocked for these. Only the Ethernet device should have Internet access

Solution: MTX-Router-Titan mini router

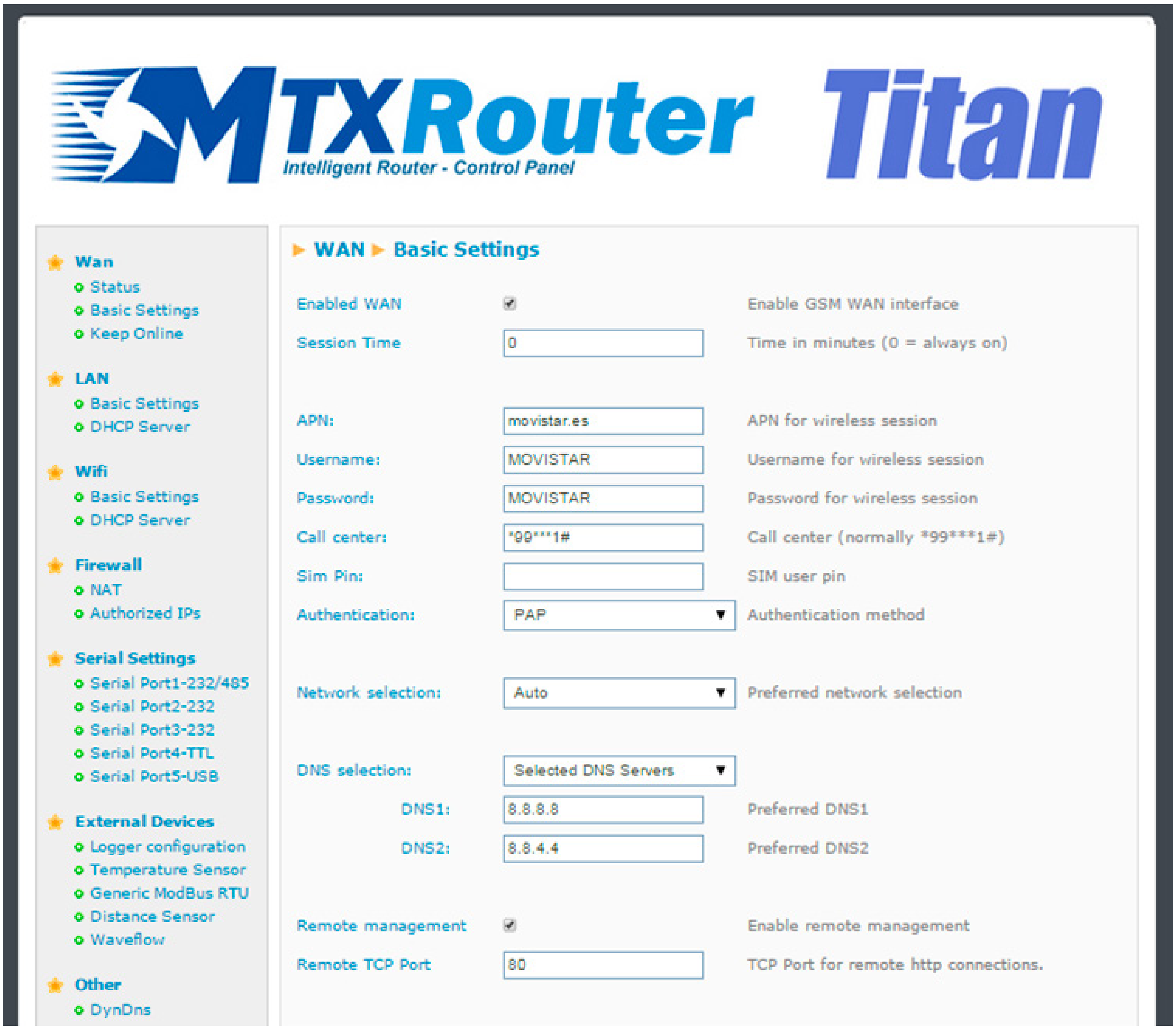

Internet connectivity via 3G using and Ethernet port on the device
INTERNET
3G
ETHERNET
MTX-Router-Titan-Mini
Device with an Ethernet Port
Internet connectivity via 3G for WiFi enabled tablets BLOCKED
WiFi tablet
WiFi tablet

Configuration example ready for use:

We can easily load the example from the router's web configuration environment from the menu "Other>Backup/Examples".

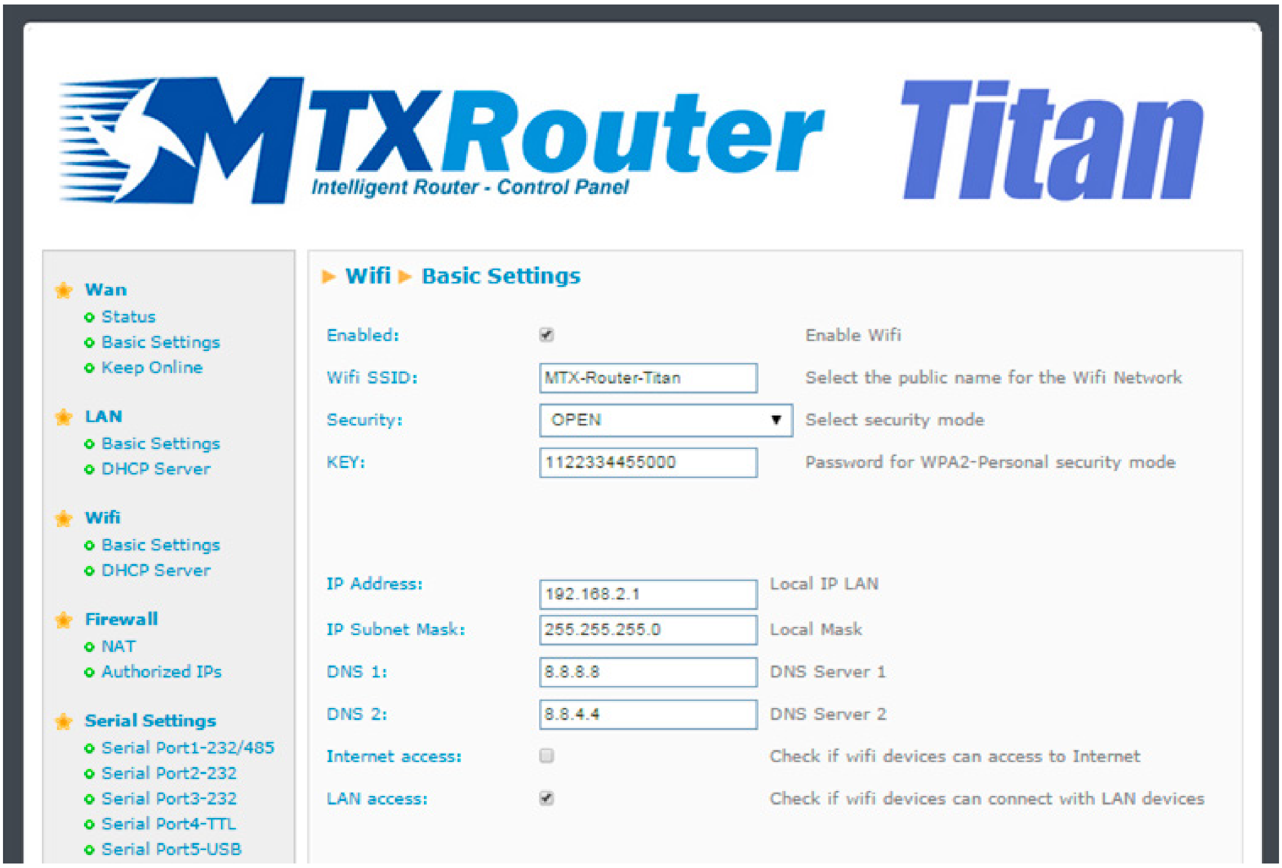
Details:

1. After the configuration is loaded in our router, we can access the router's configuration with the default username and password: "admin" and "admin", and the IP address"192.168.1.2"
2. Check the configuration in the menus "Wan>Basic Settings", "WiFi>Basic Settings", "WiFi>DHCP Server"
3. Remember that in order to work, the PLC's IP address should be in the range of the router's LAN IP address and we should specify the PLC's Gateway IP address with the router's LAN IP address. In this example, it would be 192.168.1.2



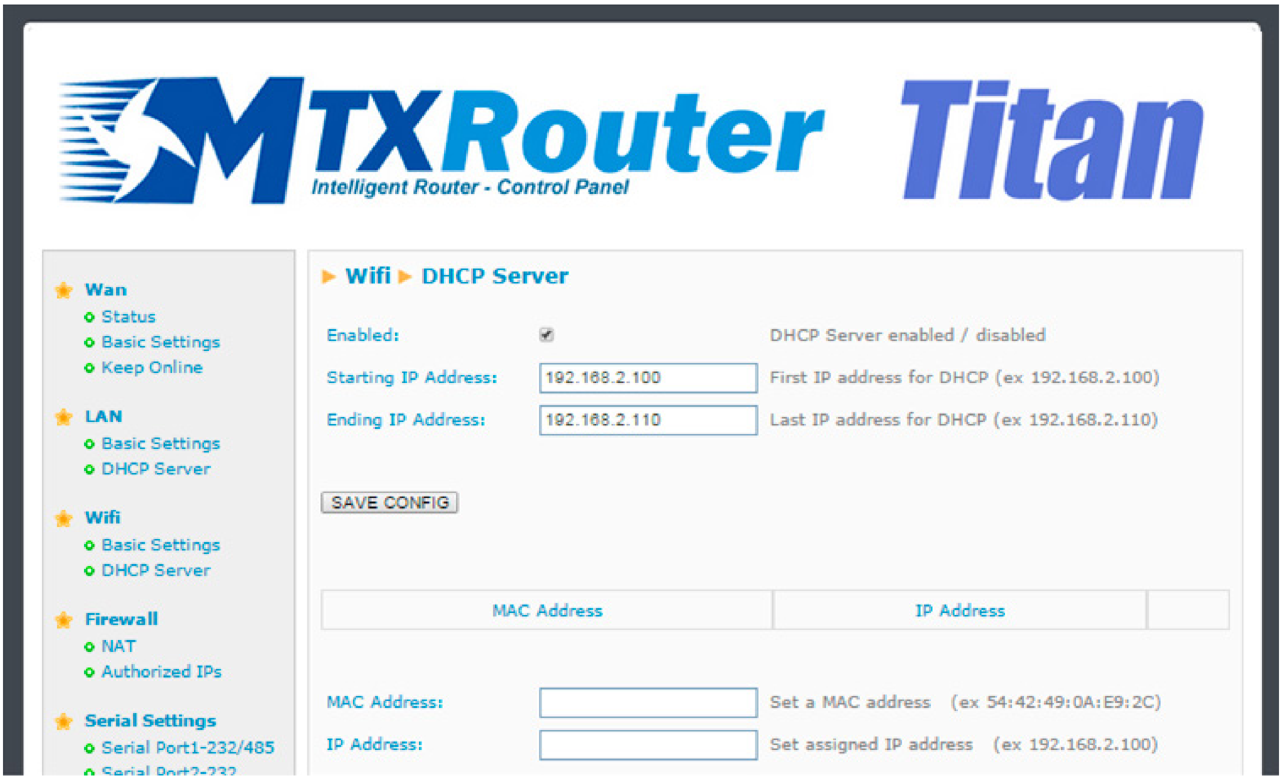
▶ WAN ▶ Basic Settings

Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP ▼	Authentication method
Network selection:	Auto ▼	Preferred network selection
DNS selection:	Selected DNS Servers ▼	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	80	TCP Port for remote http connections.



▶ Wifi ▶ Basic Settings

Enabled:	☑	Enable Wifi
Wifi SSID:	MTX-Router-Titan	Select the public name for the Wifi Network
Security:	OPEN ▼	Select security mode
KEY:	1122334455000	Password for WPA2-Personal security mode
IP Address:	192.168.2.1	Local IP LAN
IP Subnet Mask:	255.255.255.0	Local Mask
DNS 1:	8.8.8.8	DNS Server 1
DNS 2:	8.8.4.4	DNS Server 2
Internet access:	□	Check if wifi devices can access to Internet
LAN access:	☑	Check if wifi devices can connect with LAN devices



▶ Wifi ▶ DHCP Server

Enabled:	☑	DHCP Server enabled / disabled
Starting IP Address:	192.168.2.100	First IP address for DHCP (ex 192.168.2.100)
Ending IP Address:	192.168.2.110	Last IP address for DHCP (ex 192.168.2.110)

MAC Address	IP Address	

MAC Address:		Set a MAC address (ex 54:42:49:0A:E9:2C)
IP Address:		Set assigned IP address (ex 192.168.2.100)

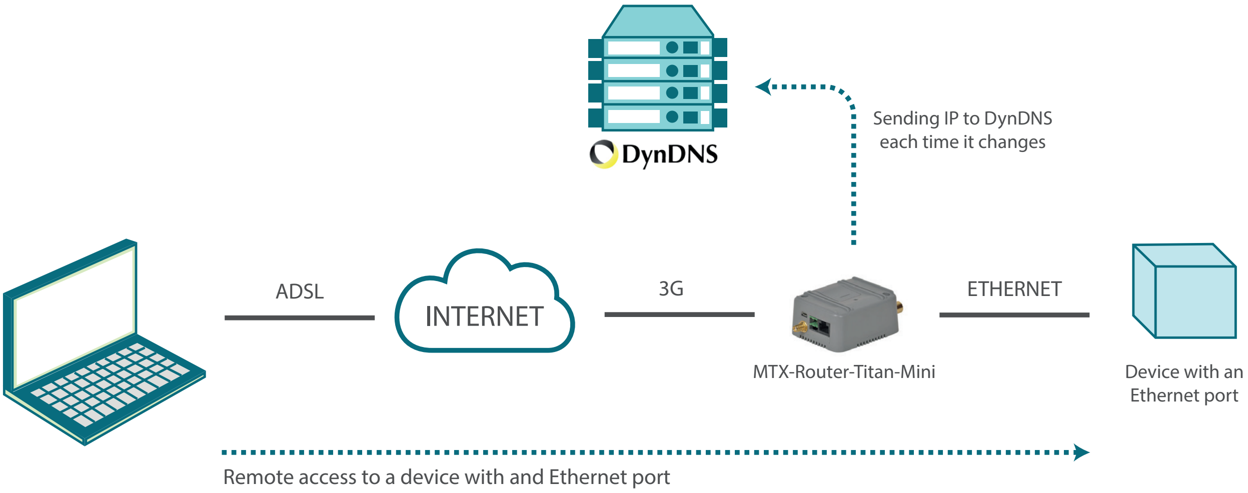
ANNEX2: ADVANCED EXAMPLE SCENARIOS AND CONFIGURATIONS

Example Scenario 2.1: Configuration to give Internet access to a device with an Ethernet port we want to access remotely with a SIM card and a dynamic IP address along with the DynDNS or No-IP service

Details of the example scenario:

- We have a device with an ETH port which we want to access remotely via Internet along the TCP port 502. The Ethernet device has a local IP address of 192.168.1.70
- We have to be able to access the router's configuration remotely in the standard TCP port 80
- We want to be able to remotely access the device. SIM cards with a dynamic IP address will be used, therefore we will use the DynDNS or No-IP services

Solution: MTX-Router-Titan mini router

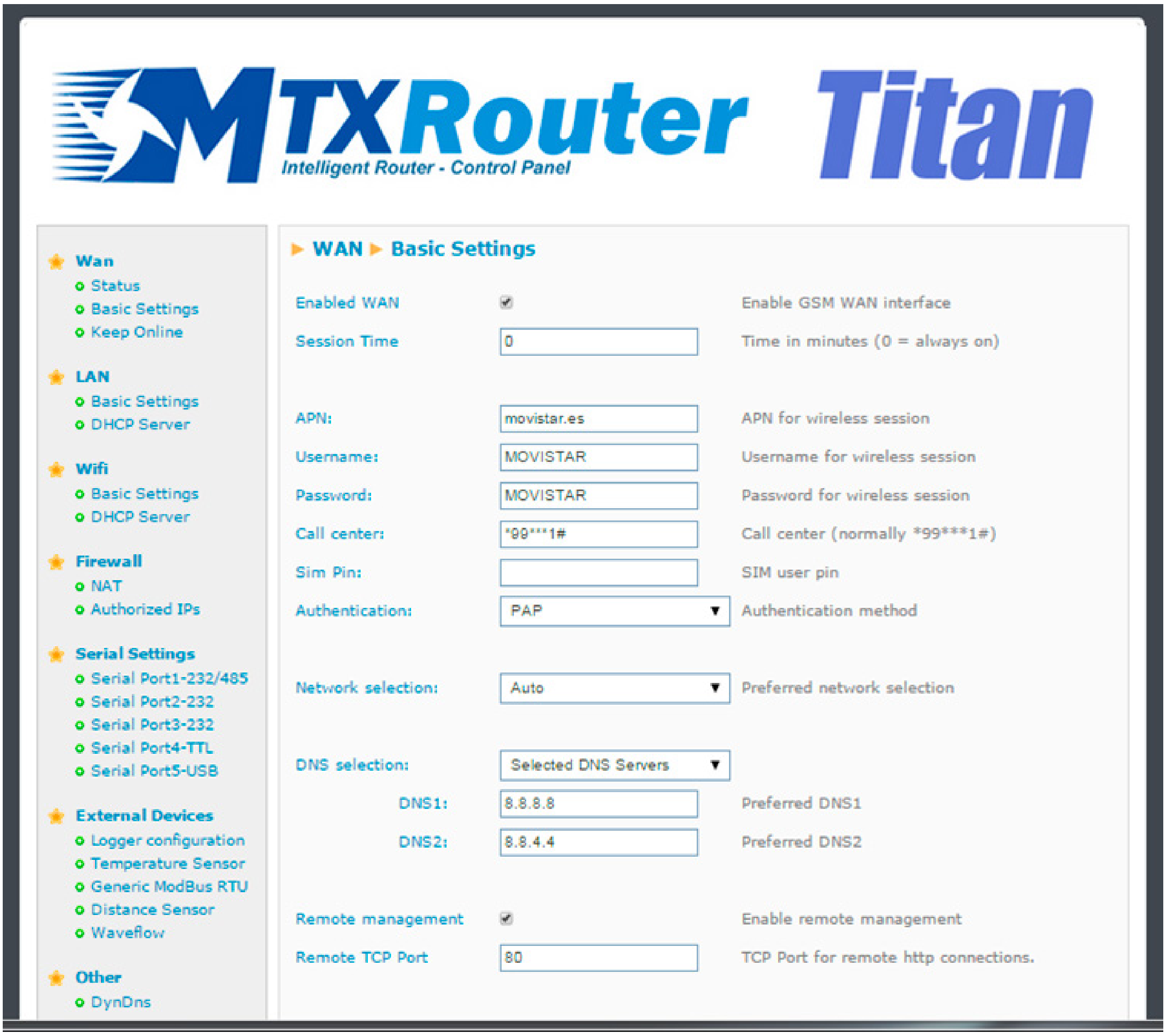

DynDNS
Sending IP to DynDNS each time it changes
ADSL
INTERNET
3G
ETHERNET
MTX-Router-Titan-Mini
Device with an Ethernet port
Remote access to a device with and Ethernet port

Configuration example ready for use:

We can easily load the example from the router's web configuration environment from the menu "Other>Backup/Examples".

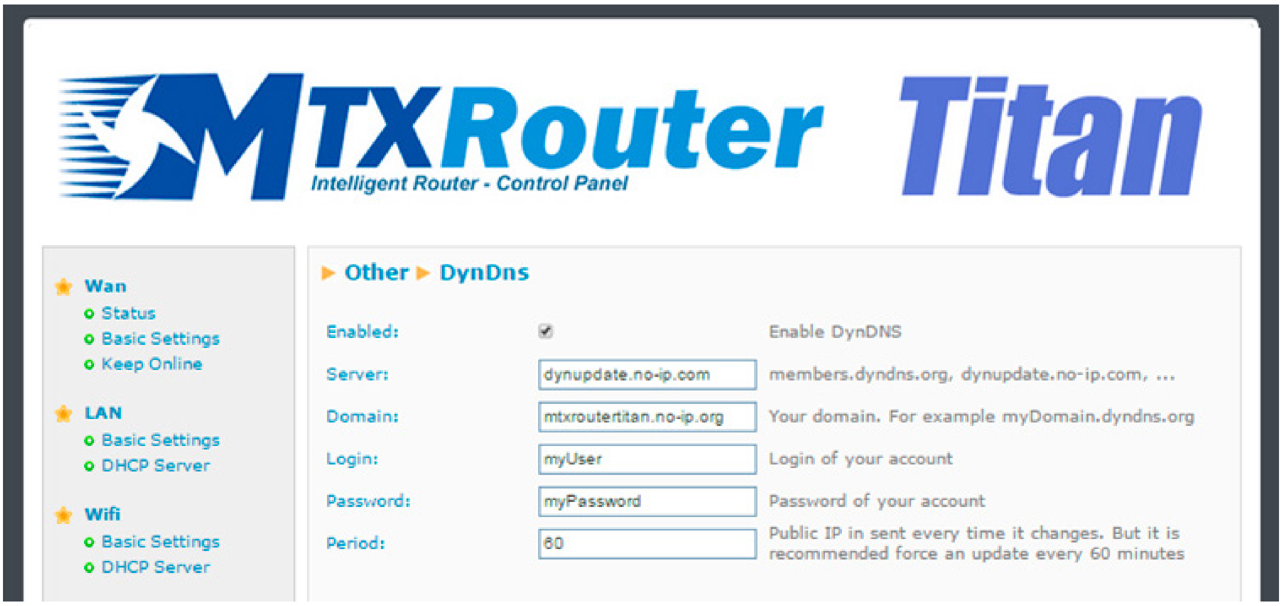
Details:

- After the configuration is loaded in our router, we can access the router's configuration with the default username and password: "admin" and "admin", and the IP address"192.168.1.2"
- Check the configuration in the menus "Wan>Basic Settings","Firewall>Nat", "Other>DynDNS"
- Remember that in order to work, the Gateway IP address of the Ethernet device should be specified along with the router's LAN IP address. In this example, it would be 192.168.1.2



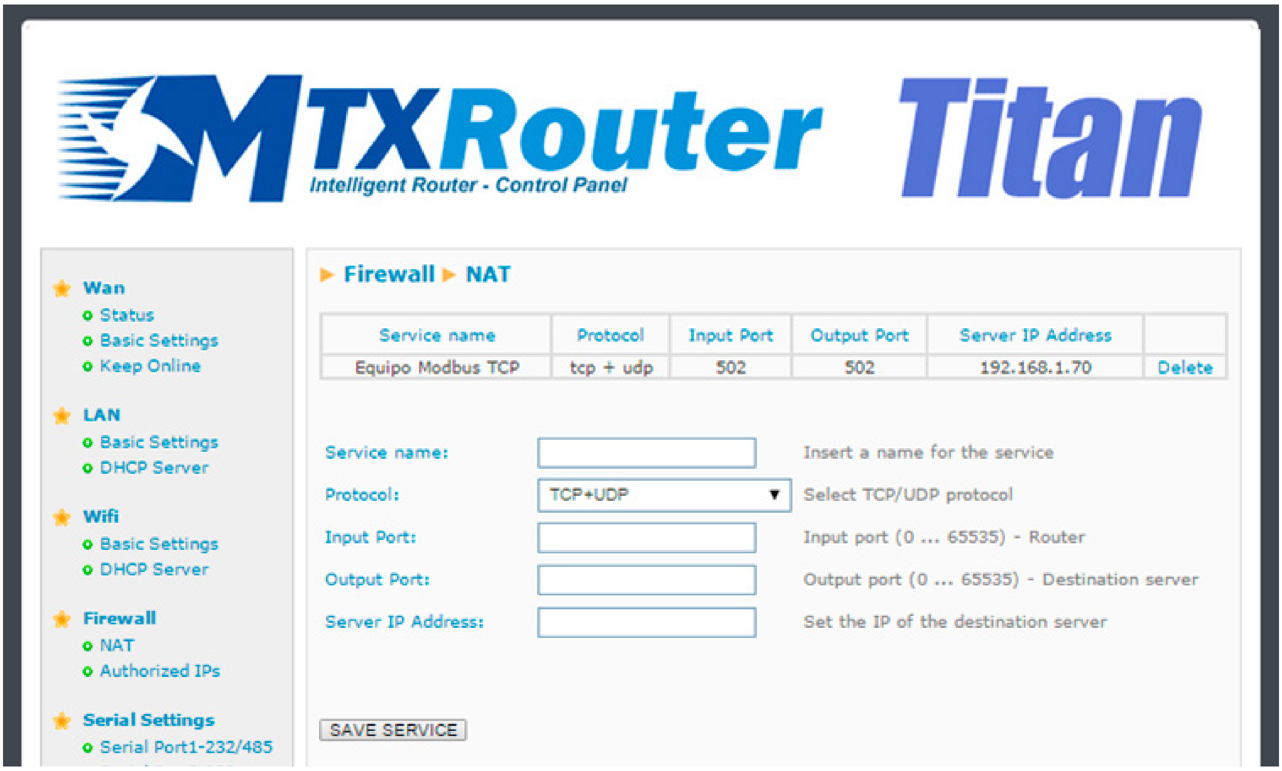
WAN ▶ Basic Settings

Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP ▼	Authentication method
Network selection:	Auto ▼	Preferred network selection
DNS selection:	Selected DNS Servers ▼	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	80	TCP Port for remote http connections.



▶ Other ▶ DynDns

Enabled:	☑	Enable DynDNS
Server:	dynupdate.no-ip.com	members.dyndns.org, dynupdate.no-ip.com, ...
Domain:	mtxroutertitan.no-ip.org	Your domain. For example myDomain.dyndns.org
Login:	myUser	Login of your account
Password:	myPassword	Password of your account
Period:	60	Public IP in sent every time it changes. But it is recommended force an update every 60 minutes



▶ Firewall ▶ NAT

Service name	Protocol	Input Port	Output Port	Server IP Address	
Equipo Modbus TCP	tcp + udp	502	502	192.168.1.70	Delete

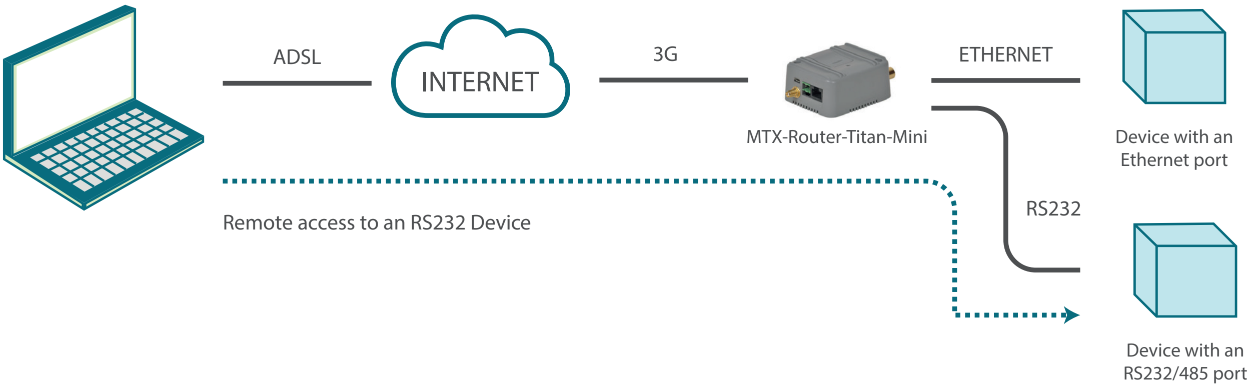
Service name:		Insert a name for the service
Protocol:	TCP+UDP ▼	Select TCP/UDP protocol
Input Port:		Input port (0 ... 65535) - Router
Output Port:		Output port (0 ... 65535) - Destination server
Server IP Address:		Set the IP of the destination server

● Example Scenario 2.2: Configuration to be able to access a serial device with a 3G-RS232 gateway whilst Internet access is given to a device with an Ethernet port

Details of the example scenario:

- We have a device with an Ethernet port which we want to provide with Internet access to send data to the Cloud. The device does not have a fixed LAN IP address, therefore we want to use DHCP in the Ethernet port
- We need to be able to access the router's configuration remotely via the standard TCP port 80
- The router will be listening in the TCP port 20010 to create a transparent 3G-RS232 gateway and to be able to remotely access the device via the serial port RS232 with the configuration 115200,8,N,1

Solution: MTX-Router-Titan mini

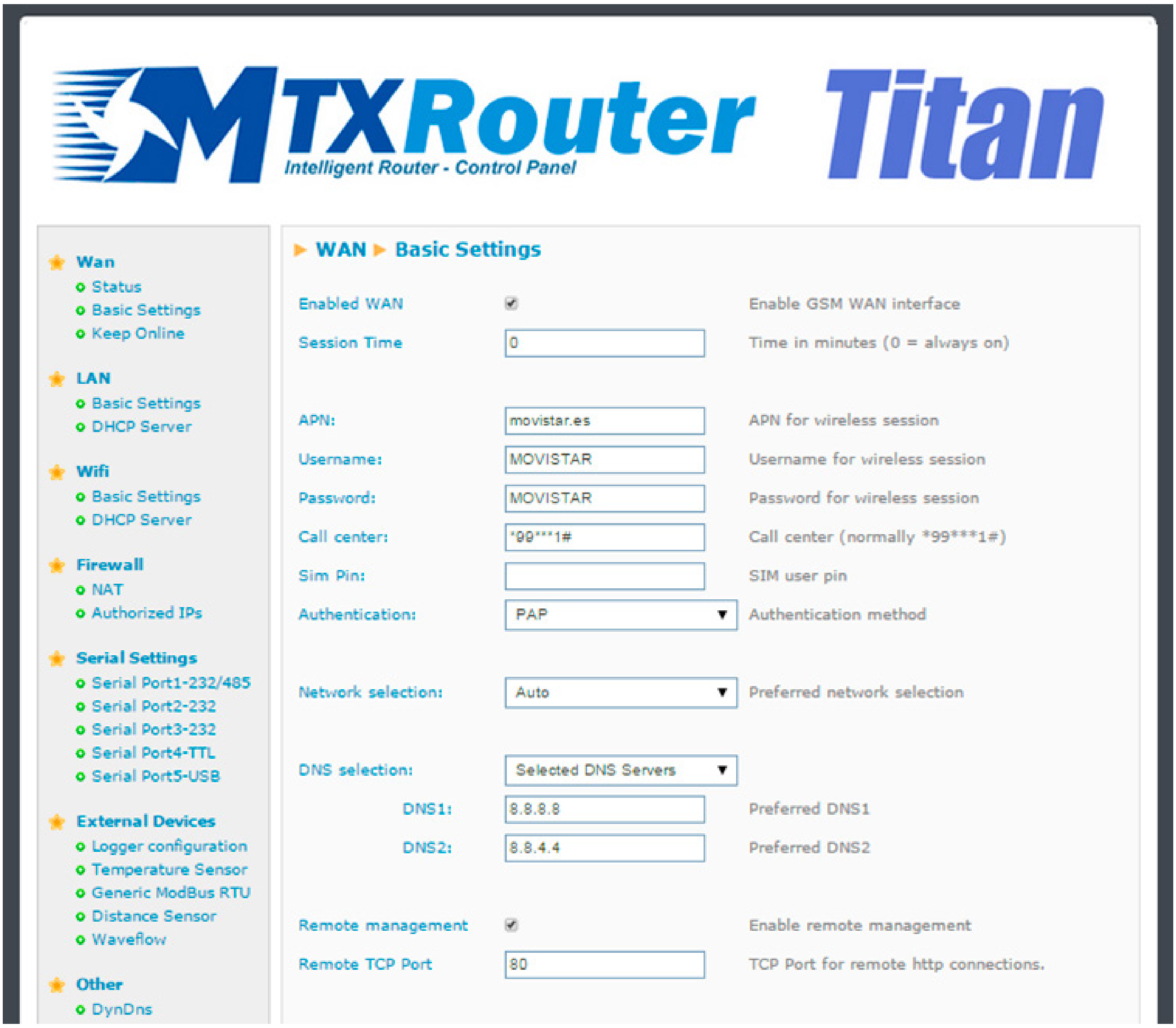

ADSL
INTERNET
3G
ETHERNET
MTX-Router-Titan-Mini
Device with an Ethernet port
RS232
Remote access to an RS232 Device
Device with an RS232/485 port

Configuration example ready for use:

We can easily load the example from the router's web configuration environment from the menu "Other>Backup/Examples".

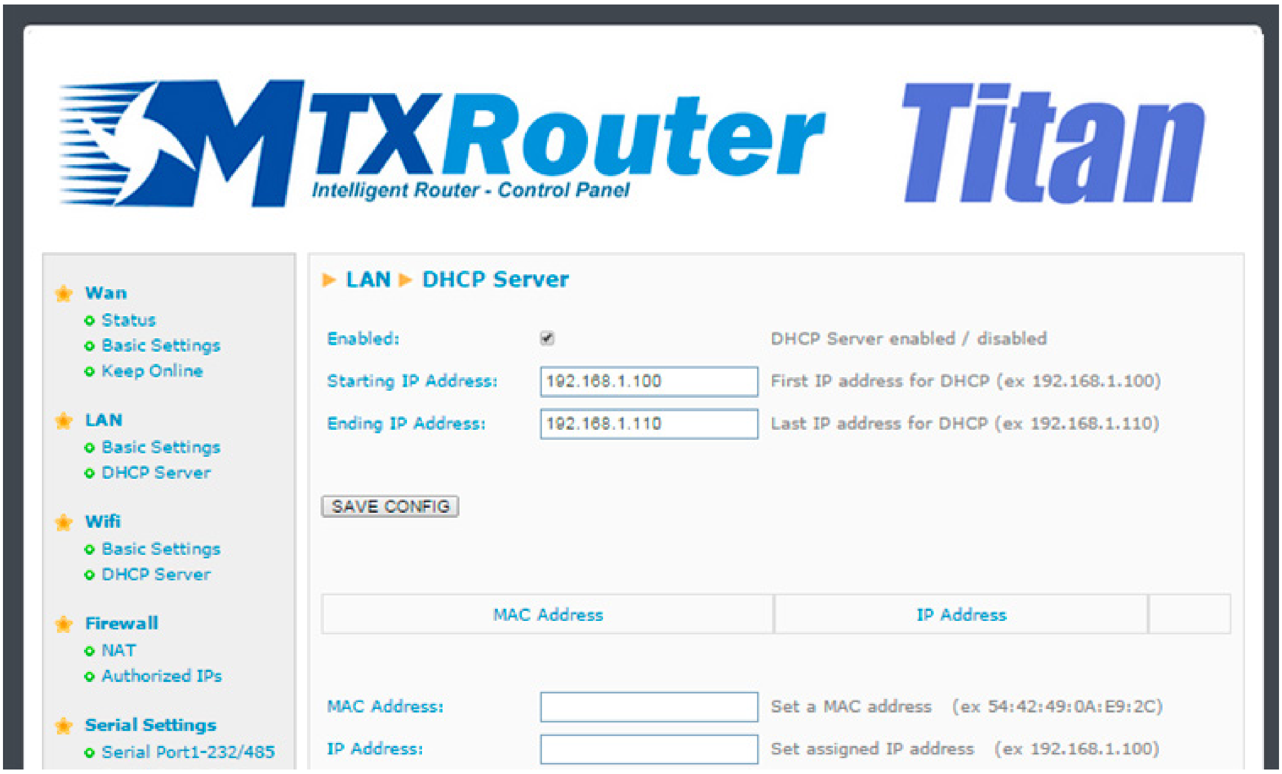
Details:

1. After the configuration is loaded in our router, we can access the router's configuration with the default username and password: "admin" and "admin", and the IP address"192.168.1.2"
2. Check the configuration in the menus "Wan>Basic Settings", "LAN>DHCP", "Serial Settings>Serial Port 1"
3. With the 3G-RS232 gateway, everything that is sent to the router's TCP port 20010 will be redirected to the device's serial port RS232 and vice versa



▶ WAN ▶ Basic Settings

Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP ▼	Authentication method
Network selection:	Auto ▼	Preferred network selection
DNS selection:	Selected DNS Servers ▼	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	80	TCP Port for remote http connections.

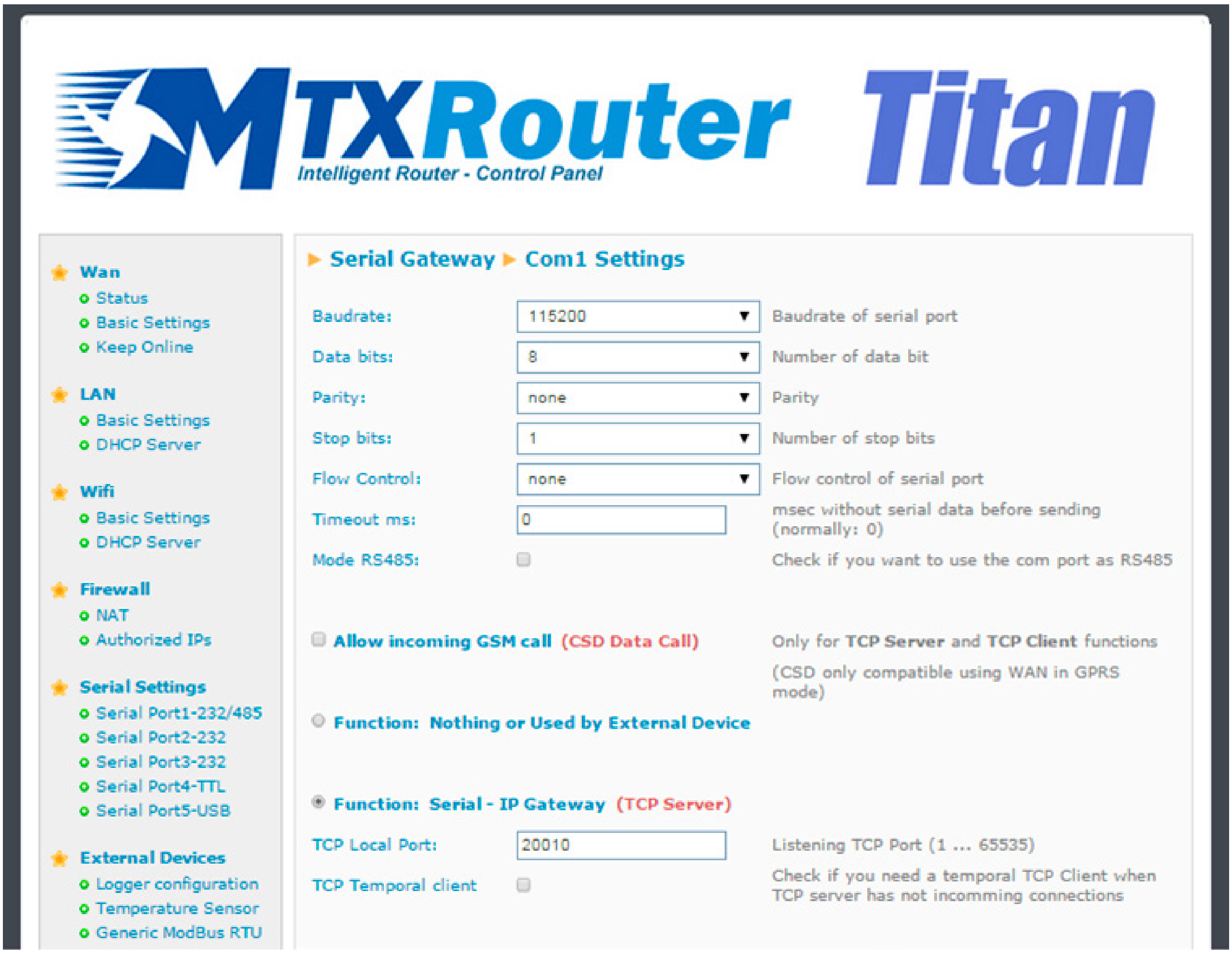


▶ LAN ▶ DHCP Server

Enabled:	☑	DHCP Server enabled / disabled
Starting IP Address:	192.168.1.100	First IP address for DHCP (ex 192.168.1.100)
Ending IP Address:	192.168.1.110	Last IP address for DHCP (ex 192.168.1.110)

MAC Address	IP Address	

MAC Address:		Set a MAC address (ex 54:42:49:0A:E9:2C)
IP Address:		Set assigned IP address (ex 192.168.1.100)



▶ Serial Gateway ▶ Com1 Settings

Baudrate:	115200	Baudrate of serial port
Data bits:	8	Number of data bit
Parity:	none	Parity
Stop bits:	1	Number of stop bits
Flow Control:	none	Flow control of serial port
Timeout ms:	0	msec without serial data before sending (normally: 0)
Mode RS485:	□	Check if you want to use the com port as RS485

□ **Allow incoming GSM call** (CSD Data Call) — Only for **TCP Server** and **TCP Client** functions (CSD only compatible using WAN in GPRS mode)

○ **Function: Nothing or Used by External Device**

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

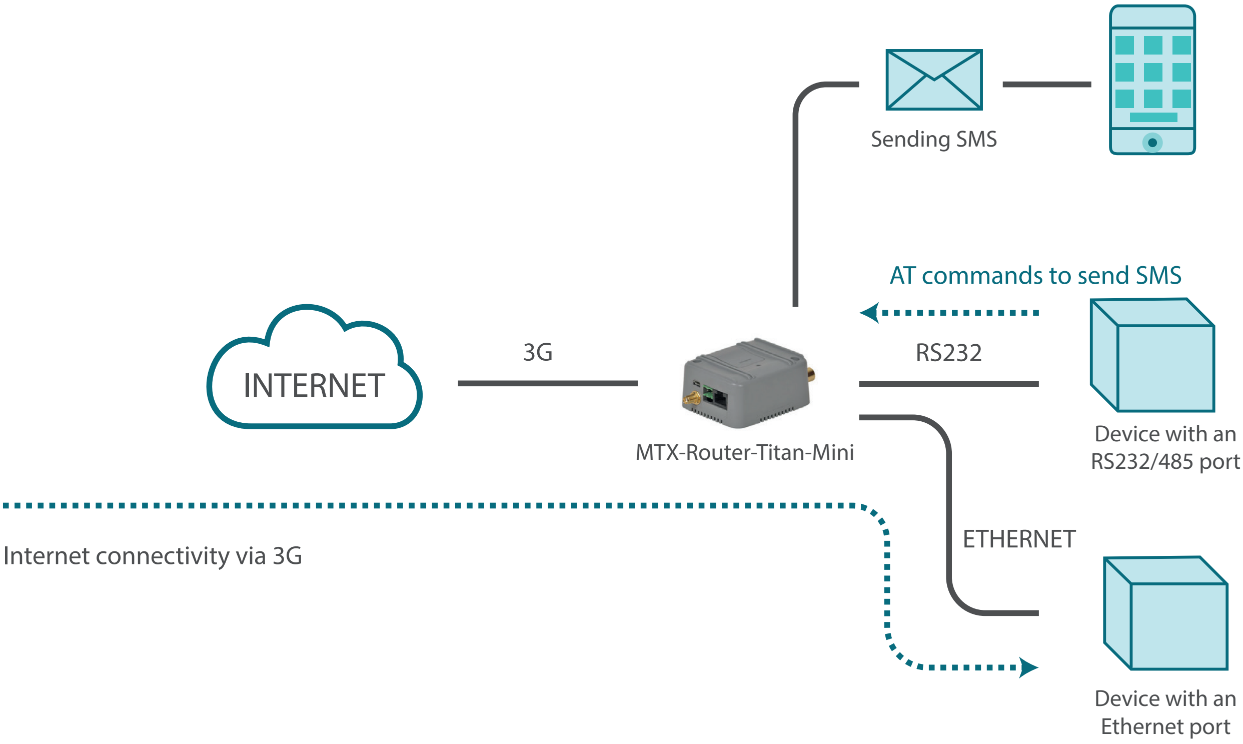
TCP Local Port:	20010	Listening TCP Port (1 ... 65535)
TCP Temporal client	□	Check if you need a temporal TCP Client when TCP server has not incomming connections

● Example Scenario 2.3: Configuration to provide Internet access to a device with an Ethernet port. Another serial device will be connected to the router via an RS232 port in order to send SMS messages via AT commands

Details of the example scenario:

- We have a device with an ETH port which we want to provide with Internet access for it to send data to the Cloud. The Ethernet device has the LAN IP address 192.168.1.70
- Another device, in this case with an RS232 serial port, will be connected to the router's RS232 port. This device will manage a series of alarms and must be able to send them via SMS using standard AT commands from any GSM modem

Solution: MTX-Router-Titan mini

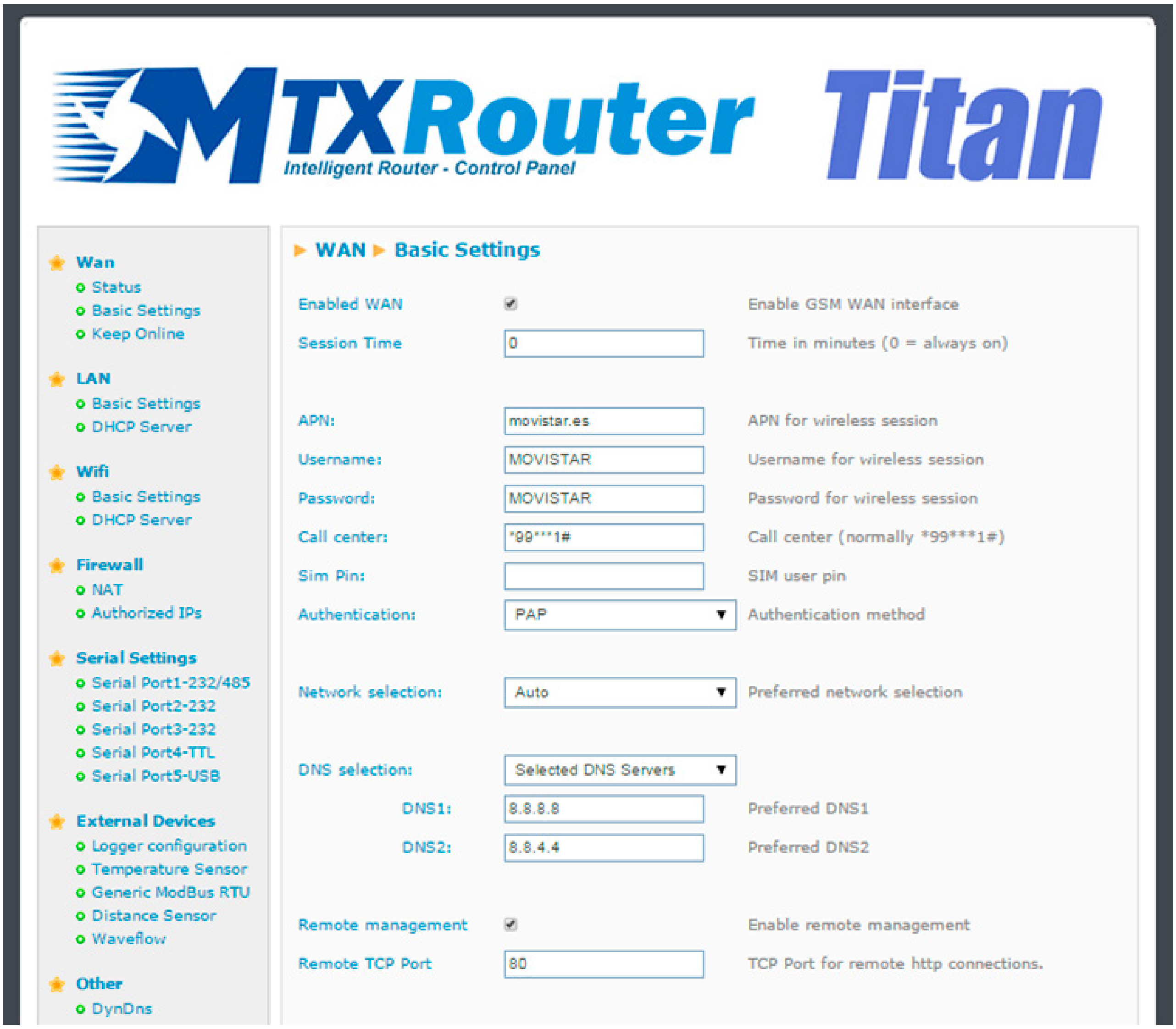

Sending SMS
AT commands to send SMS
INTERNET
3G
RS232
MTX-Router-Titan-Mini
Device with an RS232/485 port
Internet connectivity via 3G
ETHERNET
Device with an Ethernet port

Configuration example ready for use:

We can easily load the example from the router's web configuration environment from the menu "Other>Backup/Examples".

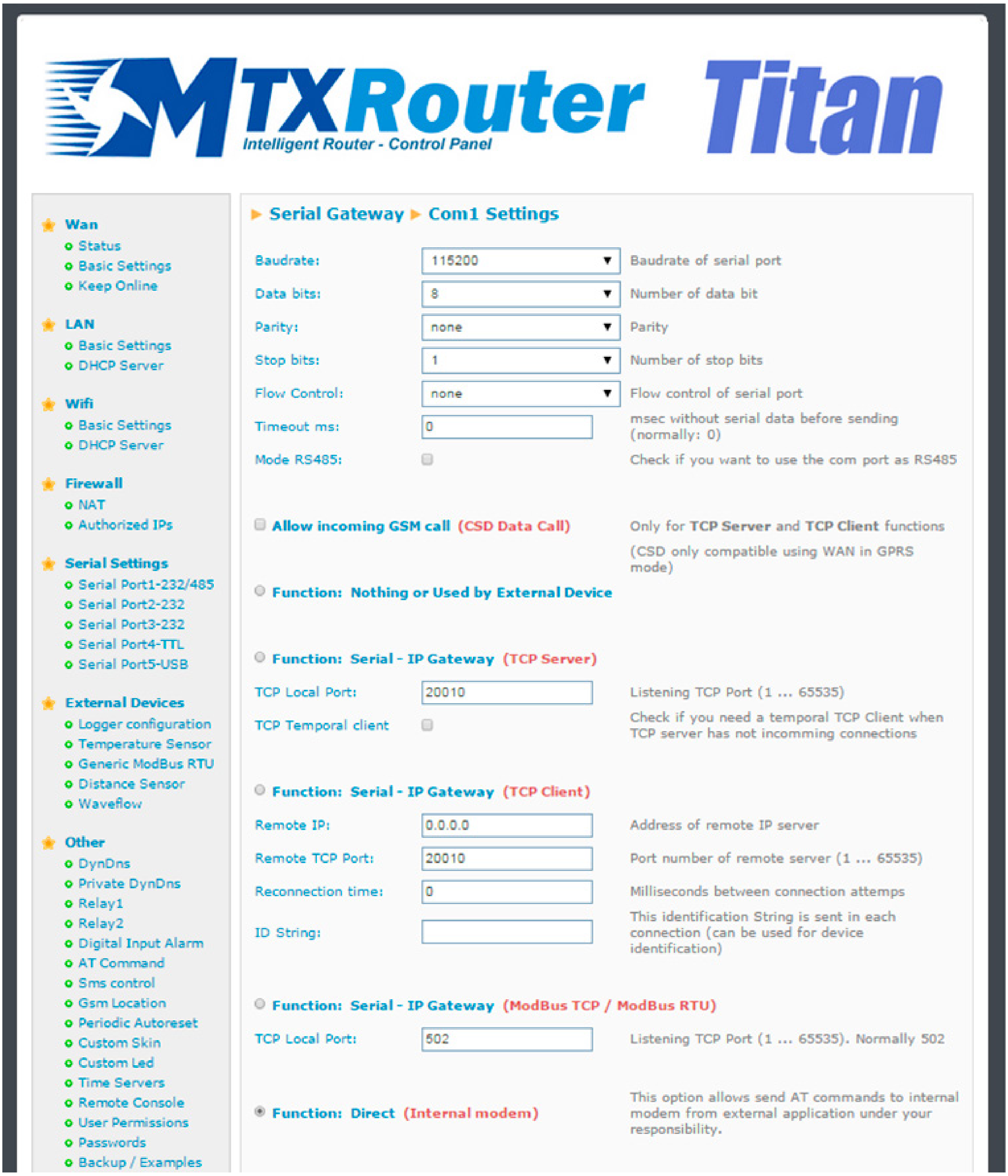
Details:

1. After the configuration is loaded in our router, we can access the router's configuration with the default username and password: "admin" and "admin", and the IP address"192.168.1.2"
2. Check the configuration in the menus "Wan>Basic Settings", "LAN>DHCP", "Serial Settings>Serial Port 1"
3. Look carefully at the configuration in "Serial Settings > Serial Port 1". We will see that the router redirects all traffic received in the serial port to the internal GSM module, therefore the AT commands that are sent through it must be appropriate for the Cinterion EHS5 module. Consult the commands AT+CMGF and AT+CMGS of the manual, which can be requested from us at gsmsupport@matrix.es, to know about the sending of SMS



▶ WAN ▶ Basic Settings

Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP ▼	Authentication method
Network selection:	Auto ▼	Preferred network selection
DNS selection:	Selected DNS Servers ▼	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	80	TCP Port for remote http connections.



▶ Serial Gateway ▶ Com1 Settings

Baudrate:	115200 ▼	Baudrate of serial port
Data bits:	8 ▼	Number of data bit
Parity:	none ▼	Parity
Stop bits:	1 ▼	Number of stop bits
Flow Control:	none ▼	Flow control of serial port
Timeout ms:	0	msec without serial data before sending (normally: 0)
Mode RS485:	□	Check if you want to use the com port as RS485

□ **Allow incoming GSM call (CSD Data Call)** — Only for **TCP Server** and **TCP Client** functions (CSD only compatible using WAN in GPRS mode)

○ **Function: Nothing or Used by External Device**

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

TCP Local Port:	20010	Listening TCP Port (1 ... 65535)
TCP Temporal client	□	Check if you need a temporal TCP Client when TCP server has not incomming connections

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

Remote IP:	0.0.0.0	Address of remote IP server
Remote TCP Port:	20010	Port number of remote server (1 ... 65535)
Reconnection time:	0	Milliseconds between connection attemps
ID String:		This identification String is sent in each connection (can be used for device identification)

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

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

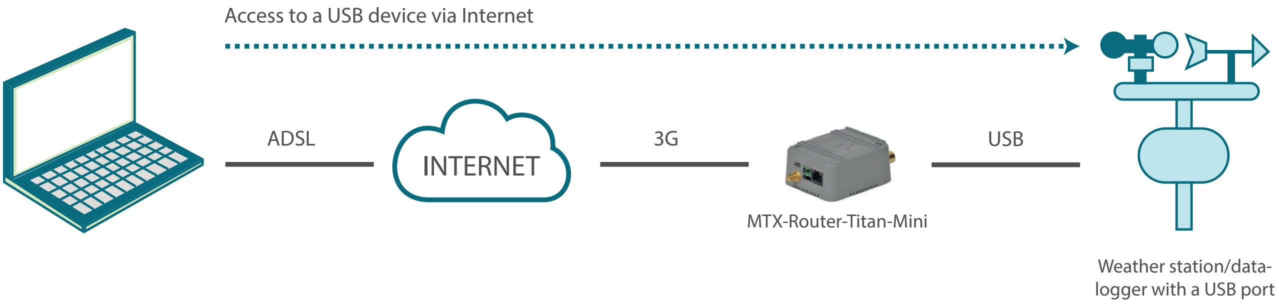
● **Function: Direct (Internal modem)** — This option allows send AT commands to internal modem from external application under your responsibility.

Example Scenario 2.4: Configuration to remotely access a USB device via Internet using a 3G router

Details of the example scenario:

- We have a device with a USB port (a weather station) which we want to access remotely to extract the data from the internal datalogger. The driver is of the standard USB FTDI type
- The router will be listening in the TCP port 20014 to create a 3G-USB gateway and remotely access the device via USB port
- For simplicity, a SIM card with fixed IP address will be used in this example, although the IP address can be obtained via SMS, or we can use a missed call as seen in previous examples

Solution: MTX-Router-Titan mini

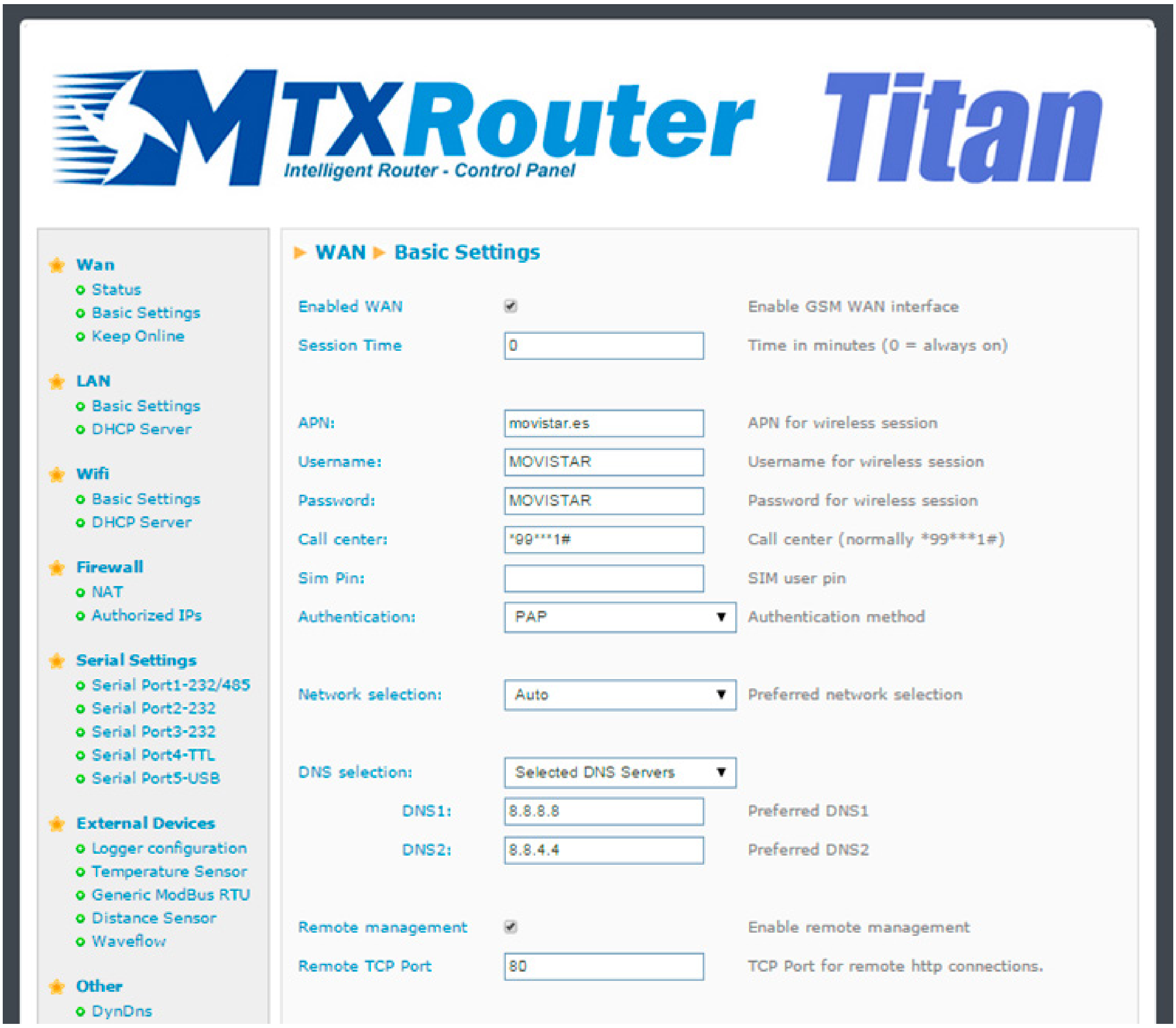

Access to a USB device via Internet
ADSL
INTERNET
3G
USB
MTX-Router-Titan-Mini
Weather station/data-logger with a USB port

Configuration example ready for use003A:

We can easily load the example from the router’s web configuration environment from the menu “Other>Backup/Examples”.

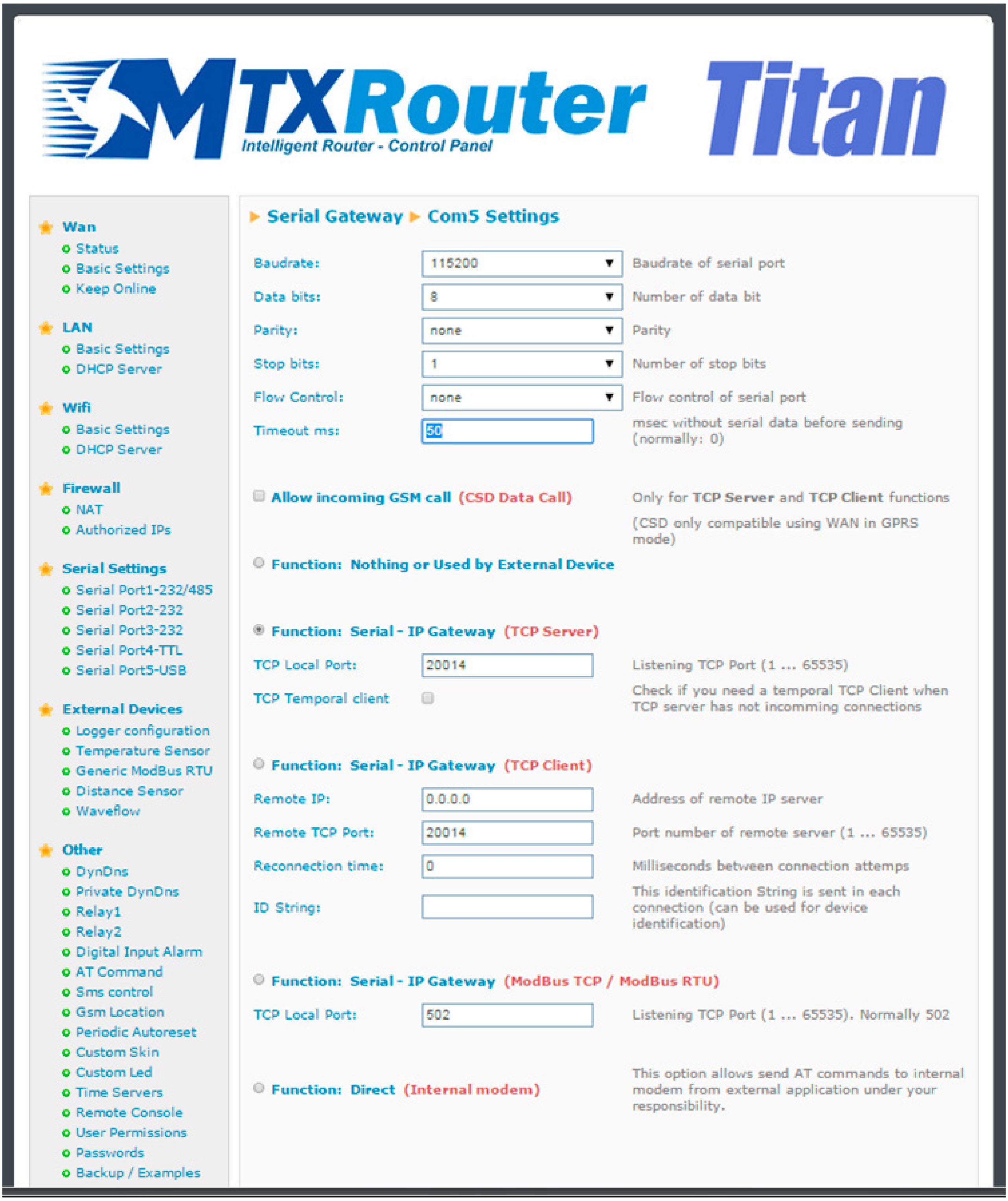
Details:

1. After the configuration is loaded in our router, we can access the router’s configuration with the default username and password: “admin” and “admin”, and the IP address“192.168.1.2”
2. Check the configuration in the menus “Wan>Basic Settings”, “Serial Settings>Serial Port 5”
3. Remember that in order for the gateway to work, the driver that the device uses must be USB FTDI or ACM. For other USB devices, get in touch with us at gsmsupport@matrix.es
4. A USB FTDI device emulates a serial device via USB. It is very important that we check the section “Serial Settings>Serial Port 5>Timeout ms” and the timeouts section, if this exists, in our control software
5. If we use the MTX-Router-Titan mini device, we will likely need to use a miniUSB-USB adaptor
6. Remember that the USB device must be connected to the router before the MTX router is connected to a power source. The MTX router will not detect the USB device correctly if it is connected after the power supply



▶ WAN ▶ Basic Settings

Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP ▼	Authentication method
Network selection:	Auto ▼	Preferred network selection
DNS selection:	Selected DNS Servers ▼	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	80	TCP Port for remote http connections.



▸ Serial Gateway ▸ Com5 Settings

Baudrate:	115200 ▾	Baudrate of serial port
Data bits:	8 ▾	Number of data bit
Parity:	none ▾	Parity
Stop bits:	1 ▾	Number of stop bits
Flow Control:	none ▾	Flow control of serial port
Timeout ms:	50	msec without serial data before sending (normally: 0)

□ Allow incoming GSM call (CSD Data Call) — Only for TCP Server and TCP Client functions (CSD only compatible using WAN in GPRS mode)

○ Function: Nothing or Used by External Device

● Function: Serial - IP Gateway (TCP Server)

TCP Local Port:	20014	Listening TCP Port (1 ... 65535)
TCP Temporal client	□	Check if you need a temporal TCP Client when TCP server has not incomming connections

○ Function: Serial - IP Gateway (TCP Client)

Remote IP:	0.0.0.0	Address of remote IP server
Remote TCP Port:	20014	Port number of remote server (1 ... 65535)
Reconnection time:	0	Milliseconds between connection attemps
ID String:		This identification String is sent in each connection (can be used for device identification)

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

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

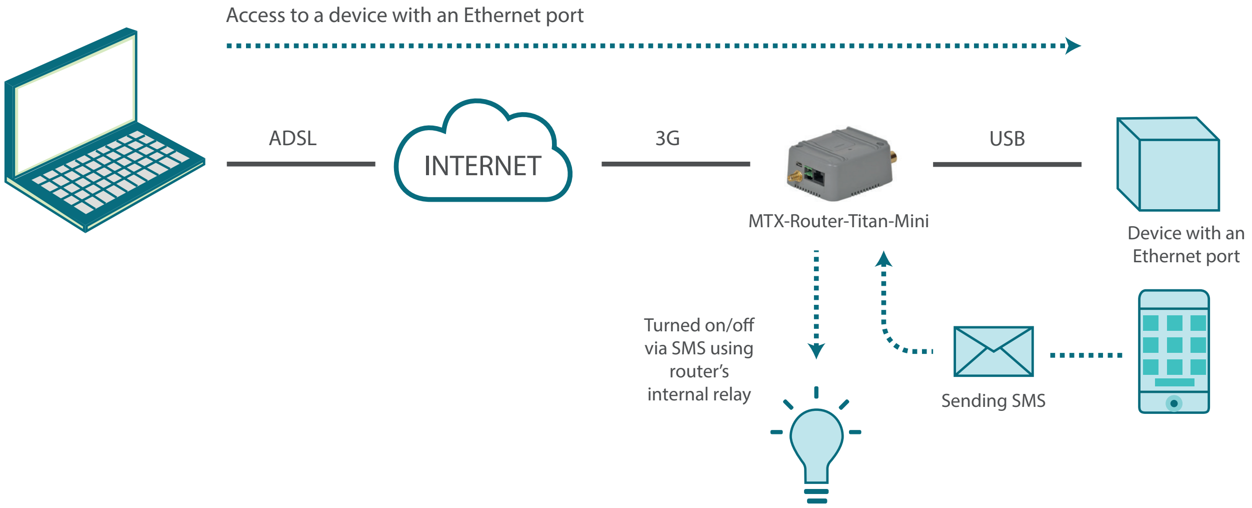
○ Function: Direct (Internal modem) — This option allows send AT commands to internal modem from external application under your responsibility.

Example Scenario 2.5: Configuration to provide remote access to a device with an Ethernet port as well as to change a relay via SMS to activate/deactivate the power supply of a third device

Details of the example scenario:

- We have a device with an ETH port which we want to provide with Internet access to send data to the Cloud. The Ethernet device has the IP address 192.168.1.70
- We have to be able to remotely access the router's configuration in the standard TCP port 80 as well as the Ethernet device via the TCP port 8080
- The router must also be configured so we can use the internal relay to activate/deactivate the power supply of an additional device. This activation/deactivation can be done via the router's webserver or via SMS. The text will be "ON" to activate the relay and "OFF" to deactivate it. Finally, we need to be able to carry out a reset of the external device's power supply without needing to send two SMSs. For this, we will send the text "RESET" which will deactivate the relay for three seconds

Solution: MTX-Router-Titan mini

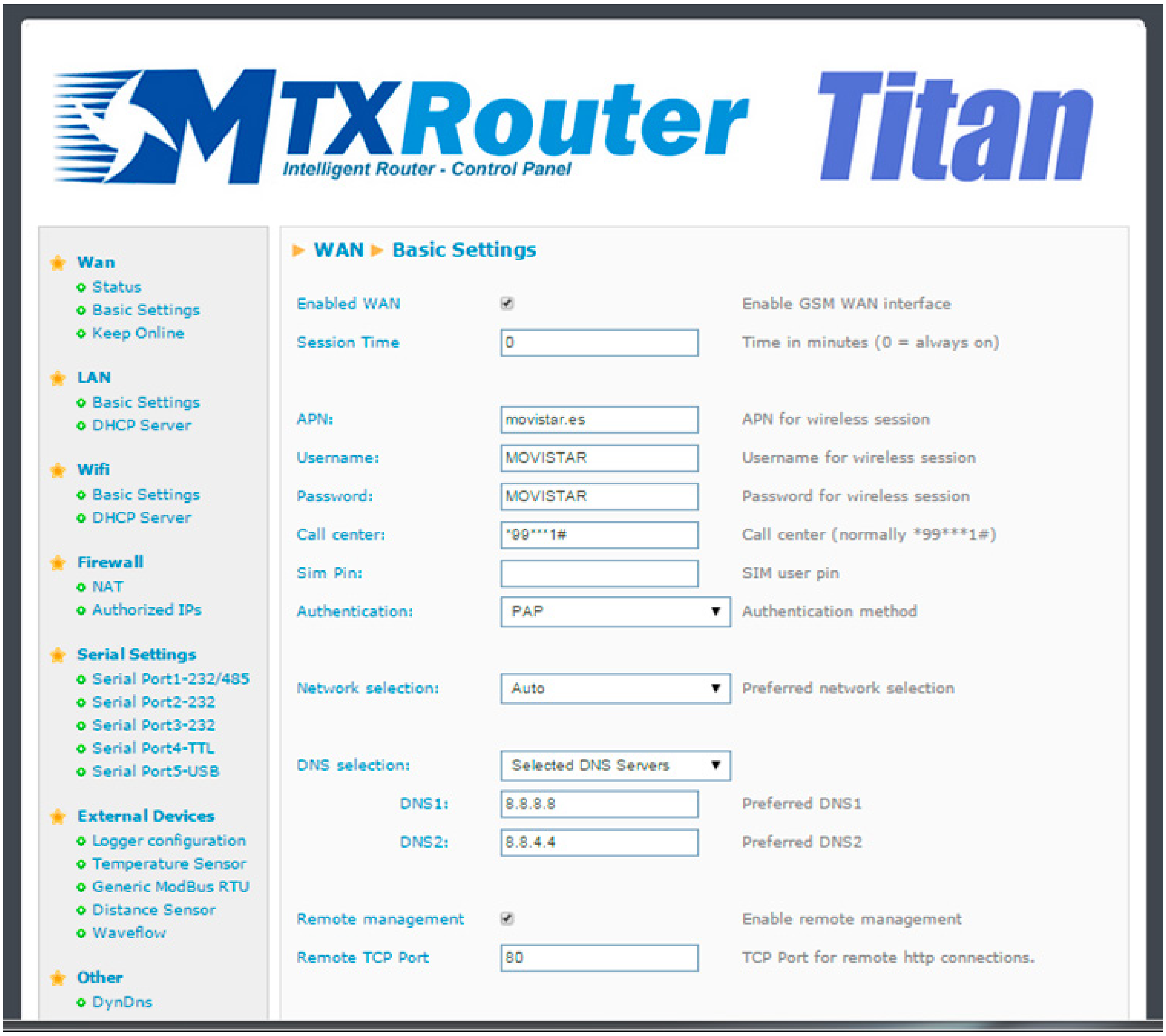

Access to a device with an Ethernet port
ADSL
INTERNET
3G
USB
MTX-Router-Titan-Mini
Device with an Ethernet port
Turned on/off via SMS using router's internal relay
Sending SMS

Configuration example ready for use:

We can easily load the example from the router's web configuration environment from the menu "Other>Backup / Examples".

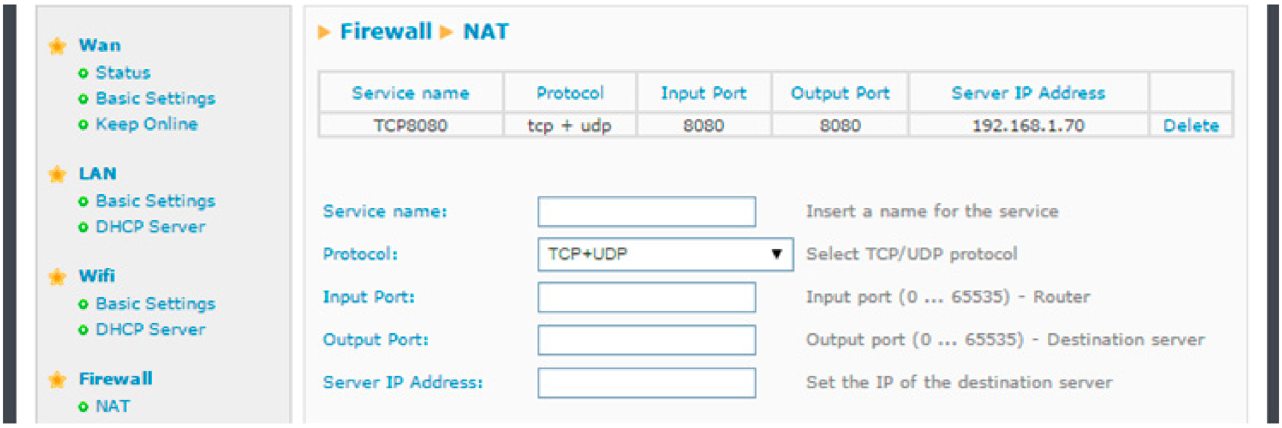
Details:

1. After the configuration is loaded in our router, we can access the router's configuration with the default username and password: "admin" and "admin", and the IP address"192.168.1.2"
2. Check the configuration in the menus "Wan>Basic Settings", ,"Firewall>Nat", "Other>Relay 1"



WAN ▶ Basic Settings

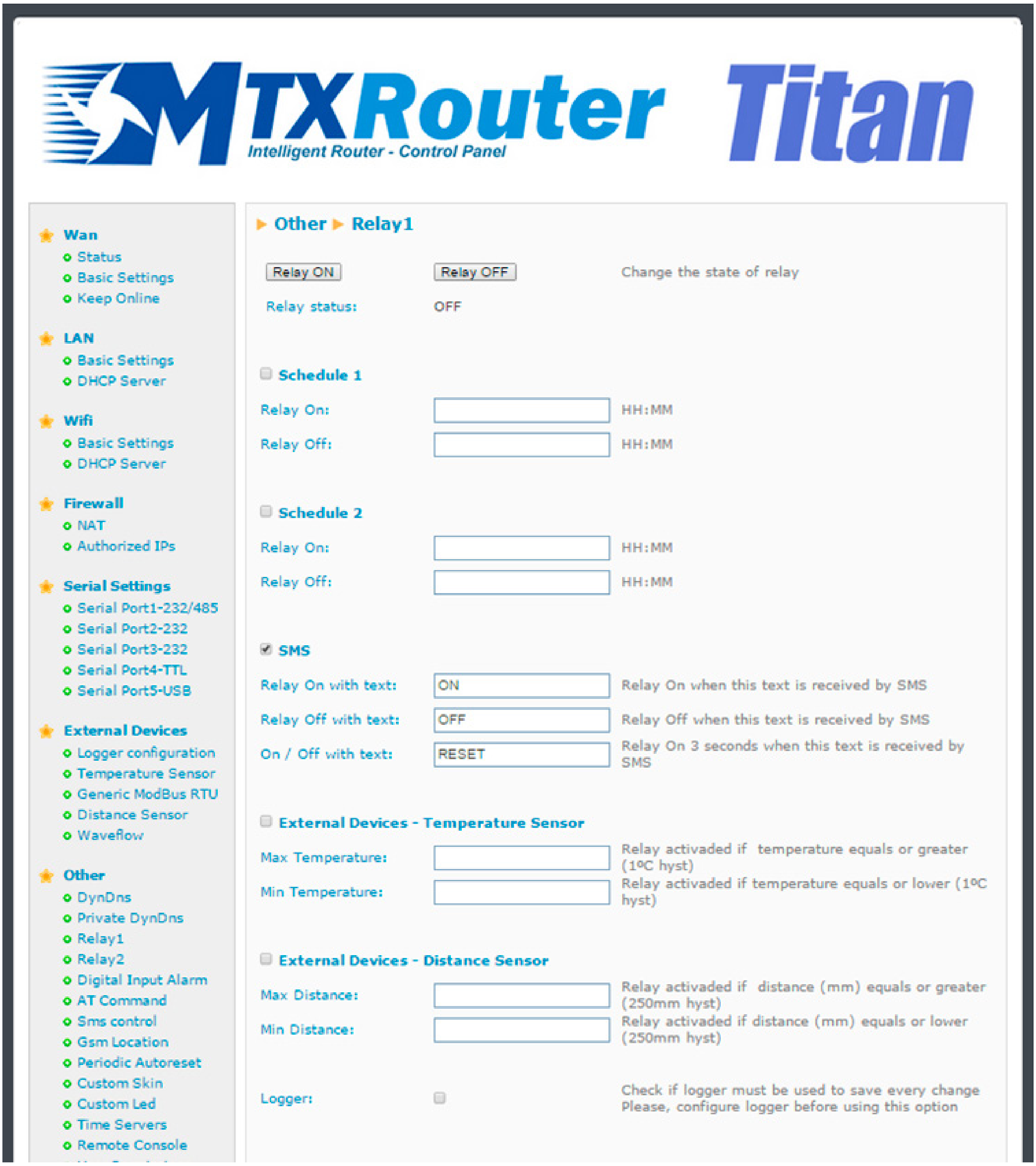
Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP ▼	Authentication method
Network selection:	Auto ▼	Preferred network selection
DNS selection:	Selected DNS Servers ▼	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	80	TCP Port for remote http connections.



Firewall ▶ NAT

Service name	Protocol	Input Port	Output Port	Server IP Address	
TCP8080	tcp + udp	8080	8080	192.168.1.70	Delete

Service name:		Insert a name for the service
Protocol:	TCP+UDP ▼	Select TCP/UDP protocol
Input Port:		Input port (0 ... 65535) - Router
Output Port:		Output port (0 ... 65535) - Destination server
Server IP Address:		Set the IP of the destination server



Other ▸ Relay1

Relay ON | Relay OFF — Change the state of relay

Relay status: OFF

□ Schedule 1

Relay On: ____ HH:MM

Relay Off: ____ HH:MM

□ Schedule 2

Relay On: ____ HH:MM

Relay Off: ____ HH:MM

☑ SMS

Relay On with text: ON — Relay On when this text is received by SMS

Relay Off with text: OFF — Relay Off when this text is received by SMS

On / Off with text: RESET — Relay On 3 seconds when this text is received by SMS

□ External Devices - Temperature Sensor

Max Temperature: ____ Relay activaded if temperature equals or greater (1ºC hyst)

Min Temperature: ____ Relay activaded if temperature equals or lower (1ºC hyst)

□ External Devices - Distance Sensor

Max Distance: ____ Relay activaded if distance (mm) equals or greater (250mm hyst)

Min Distance: ____ Relay activaded if distance (mm) equals or lower (250mm hyst)

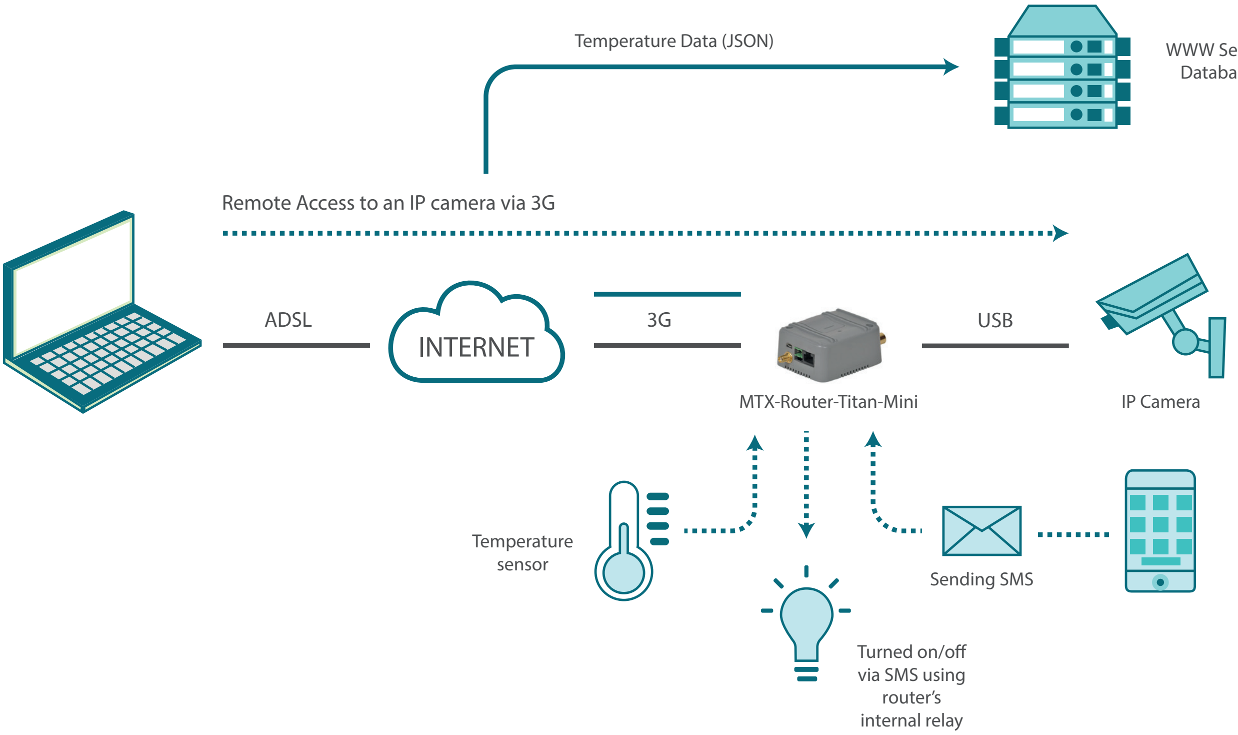
Logger: □ Check if logger must be used to save every change Please, configure logger before using this option

Example Scenario 2.6: Configuration to periodically send data from an RS232 temperature sensor to a Web server, as well as sending SMS alerts about the temperature, providing remote access to an IP camera and changing the router's internal relay according to a given timetable or SMS in order to activate/deactivate another device

Details of the example scenario:

- We have an IP camera with an Ethernet port which we want to provide with Internet access. The camera has a local IP address of 192.168.1.1
- The IP camera has an internal webserver that we can use to access the video that is being recorded. We must configure the router to access the internal webserver (in the TCP port 80), redirecting the external TCP port 8080 since we need to be able to access the router's webserver configuration also located in the TCP port 80
- SIM cards with fixed IP address will be used
- The temperature that is read must be send every 15 minutes to a webserver. The webpage to which it will be sent is http://www.metering.es/json/set.asp?data=
- In the event that the temperature that is read is greater than 30 degrees or loour than 10 degrees, a relay must be changed that will activate a light-up alarm or sound alarm as well as sending an SMS alarm to three telephone numbers
- The modem's internal relay should be programmed to activate itself at certain times of the day, as well as being activated via webserver and SMS

Solution: MTX-Router-Titan mini+MTX-Temp-RS232 sensor



Configuration example ready for use:

We can easily load the example from the router's web configuration environment from the menu "Other>Backup/Examples".

Details:

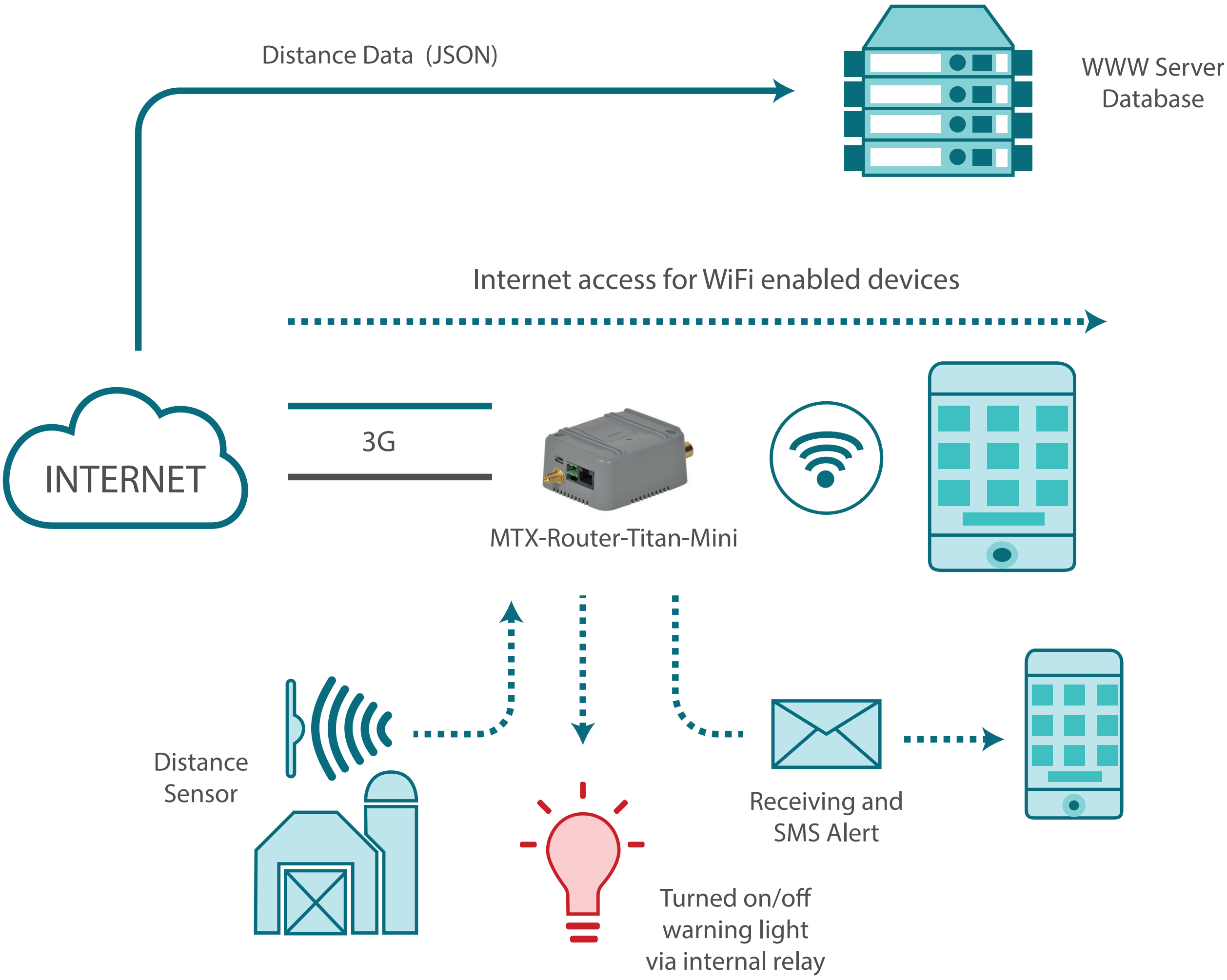
1. After the configuration is loaded in our router, we can access the router's configuration with the default username and password: "admin" and "admin", and the IP address"192.168.1.2"
2. Check the configuration in the menus "Wan>Basic Settings" y "Firewall > NAT", "Serial Settings>SerialPort1","ExternalDevices>LoggerConfiguration","ExternalDevices>Temperatura Sensor", "Other>Time Servers".
3. If we need a webserver to carry out testing, write to us at gsmsupport@matrix.es and request a testing account in the test server site www.metering.es.
4. Remember that in section 4.5.2 of this manual, we have the exact format of the data (JSON object) that is sent to the webserver.

Example Scenario 2.7: Configuration of the Titan to periodically send data from a distance sensor to a web server and planning to send SMS alerts according to the distance measured activating a warning light via relay. How to provide Internet access to WiFi enabled tablets

Details of the example scenario:

- We want to control the level of a grain silo for animal feed. For this, the router will have the distance sensor Maxbotix connected to its serial port with an RS232 output. The Maxbotix output will be installed at the top of the grain silo to measure the distance
- When a distance greater than 6m. is detected, the volume is very low and an SMS alert must be sent to three different telephone numbers as well as activating a warning light via a relay
- Additionally, the grain silo level must be sent every 12 hours to a webserver. The web address will be http://www.metering.es/json/set.asp?data=
- The router must provide Internet access to tablets via WiFi to carry out maintenance tasks

Solution: MTX-Router-Titan mini + Maxbotix sensor



Configuration example ready for use:

We can easily load the example from the router’s web configuration environment from the menu “Other>Backup / Examples”.

Details:

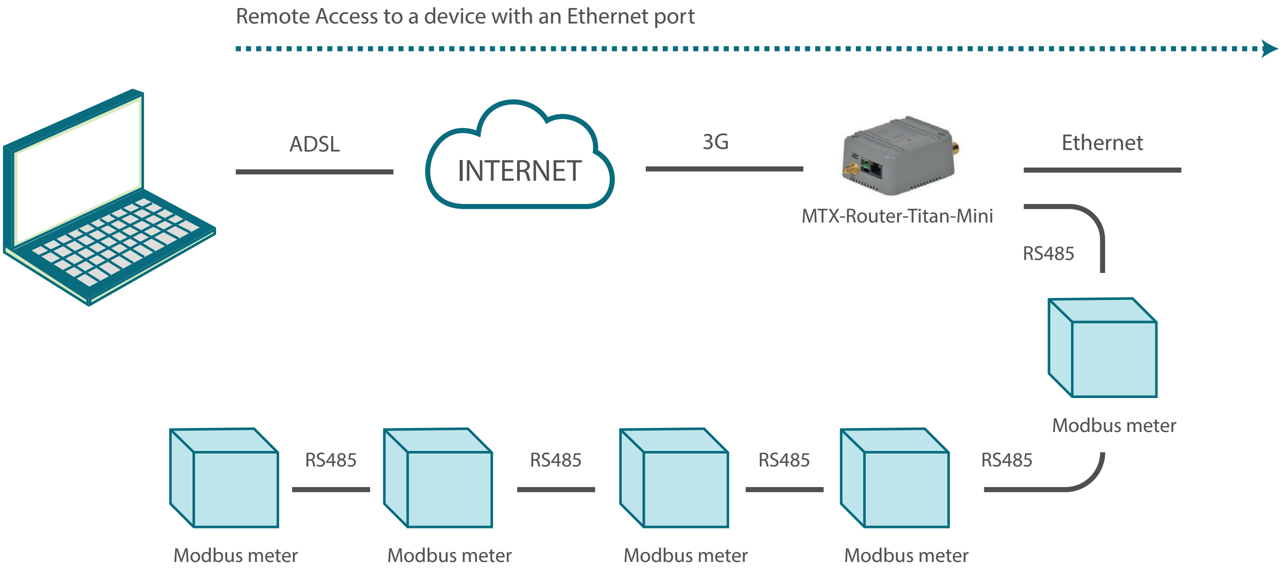
1. After the configuration is loaded in our router, we can access the router’s configuration with the default username and password: “admin” and “admin”, and the IP address“192.168.1.2”
2. Check the configuration in the menus “Wan>Basic Settings”, “WiFi>Basic Settings”, “WiFi>DHCP Server”, “Serial Settings>Serial Port1”, “External Devices>Logger Configuration”,“External Devices>DistanceTemperatura Sensor”, “Other>Relay1”, “Other>Time Servers”
3. If we need a webserver to carry out testing, write to us at gsmsupport@matrix.es and request a testing account in the test server site www.metering.es
4. Remember that in section 4.5.3 of this manual, we have the exact format of the data (JSON object) that is sent to the webserver

Example Scenario 2.8: Configuration to send to a webserver the Modbus readings of 5 Modbus RS485 devices, as well as providing Internet access to an Ethernet network analyzer

Details of the example scenario:

- We have five electric meters with Modbus RTU protocol. These meters have a series of variables/ registers (for example, current consumption and average consumption) in its internal memory which should be periodically read and sent to a webserver.
- The router should request this data from the meter every 15 minutes. The registers to be read for the current consumption is register 20, and the average consumption is register 21.
- The router should send the value of registers to a webserver via HTTP GET using a JSON object after each reading, but it must be able to store up to 1000 readings in its flash memory in case of GPRS communication failure. These will be send upon restoration of the service. For each meter, a JSON string will be sent where the meter that is read will be indicated with an identifier (the Modbus address).
- Finally, the router should provide Internet access to a network analyzer with an Ethernet interface. The IP address of the analyzer is 192.168.1.1. The router must also map the TCP port 8080 to the TCP port 80 to be able to remotely access it.
- The router will use a SIM card with a dynamic IP address. Therefore, the IP address must be send each time it is changed to the webserver.

Solution: MTX-Router-Titan mini



Configuration example ready for use:

We can easily load the example from the router's web configuration environment from the menu "Other>Backup/Examples".

Details:

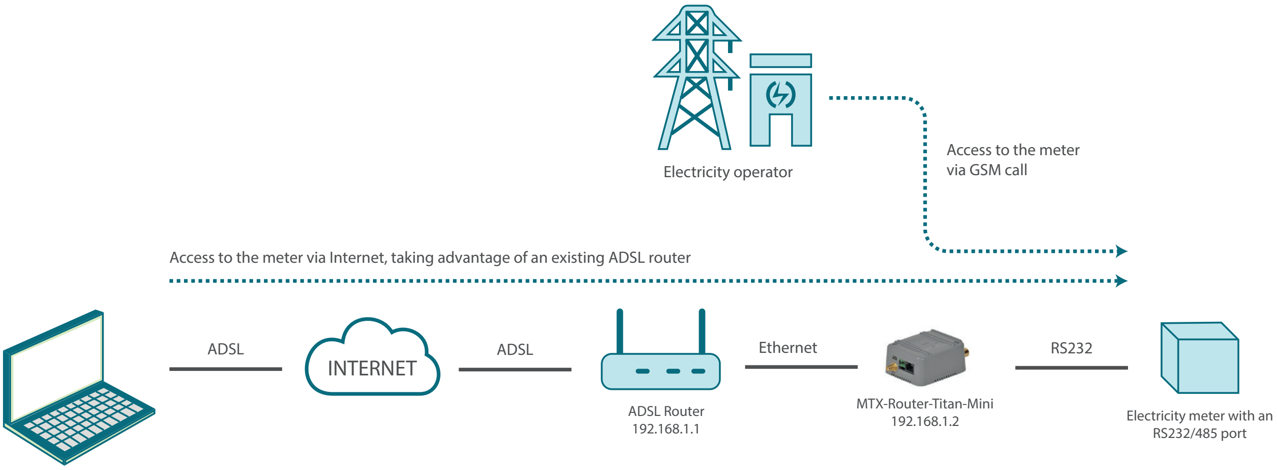
1. After the configuration is loaded in our router, we can access the router’s configuration with the default username and password: “admin” and “admin”, and the IP address“192.168.1.2”
2. Check the configuration in the menus “Wan>Basic Settings”, “Lan>Basic Settings”, “Firewall>Nat”,“SerialSettings>SerialPort1”,“ExternalDevices>LoggerConfiguration”,“External Devices>Generic Modbus RTU”, “Other>Time Servers”.
3. If we need a webserver to carry out testing, write to us at gsmsupport@matrix.es and request a testing account in the test server site www.metering.es.
4. Remember that in section 4.5.4 of this manual, we have the exact format of the data (JSON object) that is sent to the webserver when the Modbus devices are read.
5. Remember that in section 4.6.2 of this manual, we have the exact format of the data (JSON object) that is sent to the webserver when the IP address is read.

Example Scenario 2.9: Access to an electricity meter’s data via a GSM data call (from the energy supplier such as Iberdrola, Endesa, etc.) as well as via Internet using an existing ADSL router, giving priority to the GSM data call from the company

Details of the example scenario:

- We need to be able to access the data of an electricity meter remotely. The electricity meter will have an RS232 serial port with the configuration 9600 and 8N1
- We want to access the meter in real time and in a continuous way using an Internet connection that is already available in the company where the meter is installed. Therefore, we will take advantage of the client’s ADSL router, which has a fixed IP address, to access the meter’s data. The ADSL router’s LAN IP address is 192.168.1.1 and the port to be used is the TCP 20010 port
- The energy provider (Iberdrola, Endesa, etc.) should also be able to access the meter via a GSM data call. This call with take priority over the IP connection made with the ADSL router. This means that if a GSM call is received, any access via Ethernet must be stopped so the GSM call can be attended to. Once the GSM call is terminated by the energy provider, the Ethernet connection must be restored

Solution: MTX-Router-Titan mini

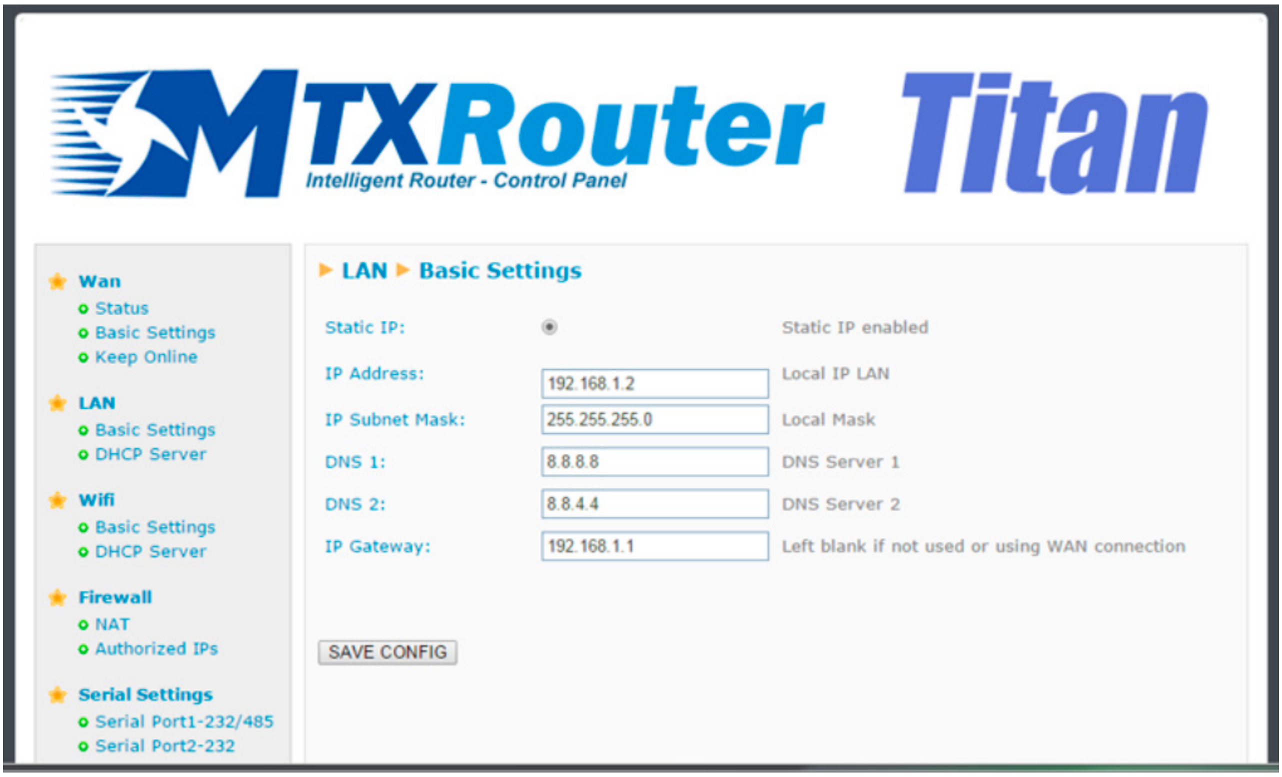

Electricity operator
Access to the meter via GSM call
Access to the meter via Internet, taking advantage of an existing ADSL router
ADSL
INTERNET
ADSL
ADSL Router 192.168.1.1
Ethernet
MTX-Router-Titan-Mini 192.168.1.2
RS232
Electricity meter with an RS232/485 port

Configuration example ready for use:

We can easily load the example from the router’s web configuration environment from the menu “Other>Backup / Examples”.

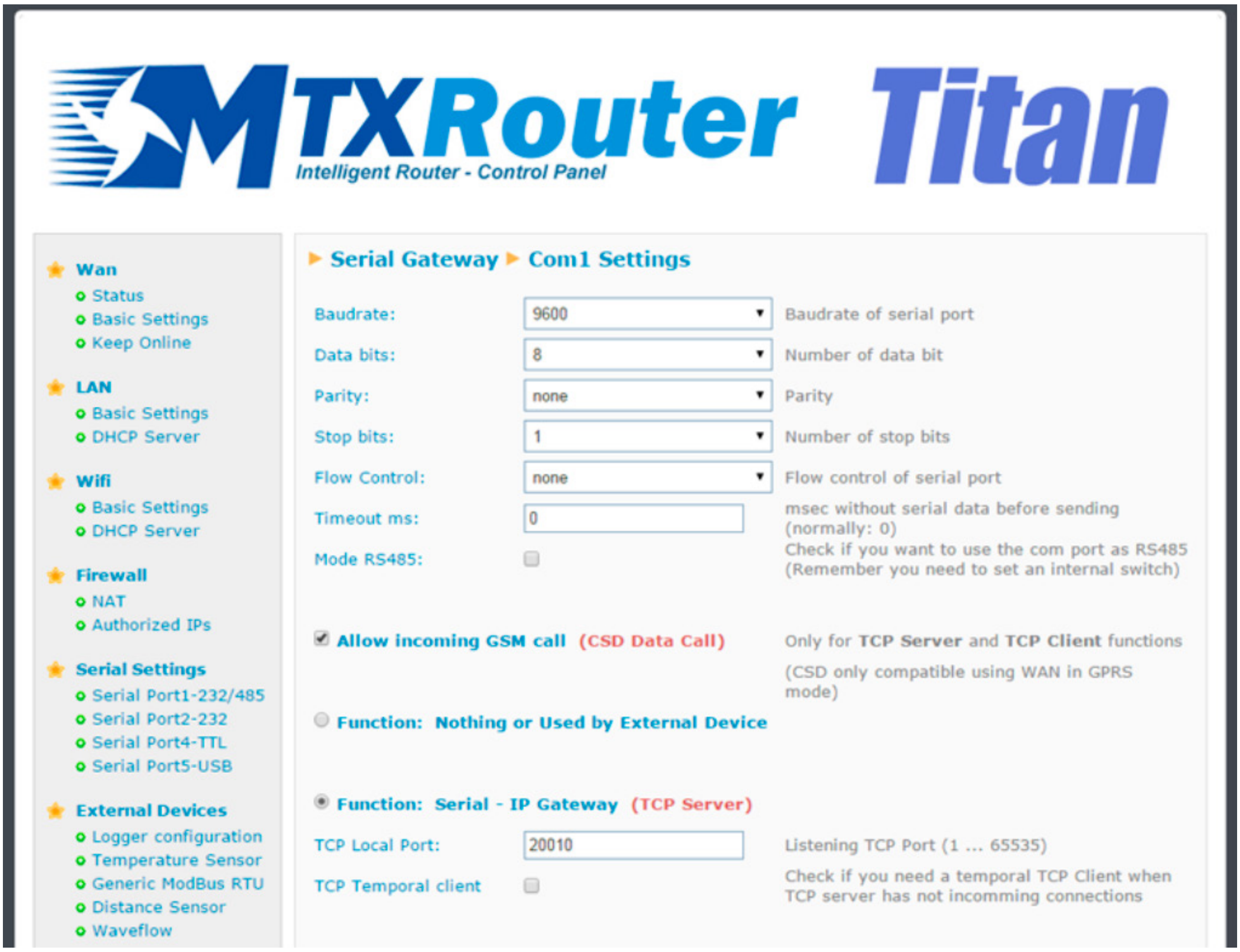
Details:

1. After the configuration is loaded in our router, we can access the router's configuration with the default username and password: "admin" and "admin", and the IP address"192.168.1.2"
2. Check the configuration in the menus "Wan>Basic Settings", "LAN>Basic Settings", "Firewall>NAT", "Serial Settings>Serial Port 1"
3. Remember that the router must be configured only to accept CSD calls when the router is in fixed GPRS mode. It will not be possible when it is working in 3G mode
4. Since we want to use an existing ADSL router, we must create an NAT (mapped from at least one TCP port) from the ADSL router to the MTX-Router-Titan mini. In this example case, the MTX-Router-Titan mini is listening out to create an IP-RS232 gateway in the TCP20010 port. A NAT should be created (in the ADSL router's configuration menus) from the ADSL router's TCP20010 port to the TCP20010 port of the device with IP address 192.168.1.2, which is the LAN IP address of the MTX-Router-Titan mini device as in the example. Remember that in order for the NAT to function correctly, the ADSL router's local IP address must be specified as the Gateway IP address in the MTX's LAN configuration. In this case, it would be 192.168.1.1



▶ LAN ▶ Basic Settings

Static IP:	●	Static IP enabled
IP Address:	192.168.1.2	Local IP LAN
IP Subnet Mask:	255.255.255.0	Local Mask
DNS 1:	8.8.8.8	DNS Server 1
DNS 2:	8.8.4.4	DNS Server 2
IP Gateway:	192.168.1.1	Left blank if not used or using WAN connection



▶ Serial Gateway ▶ Com1 Settings

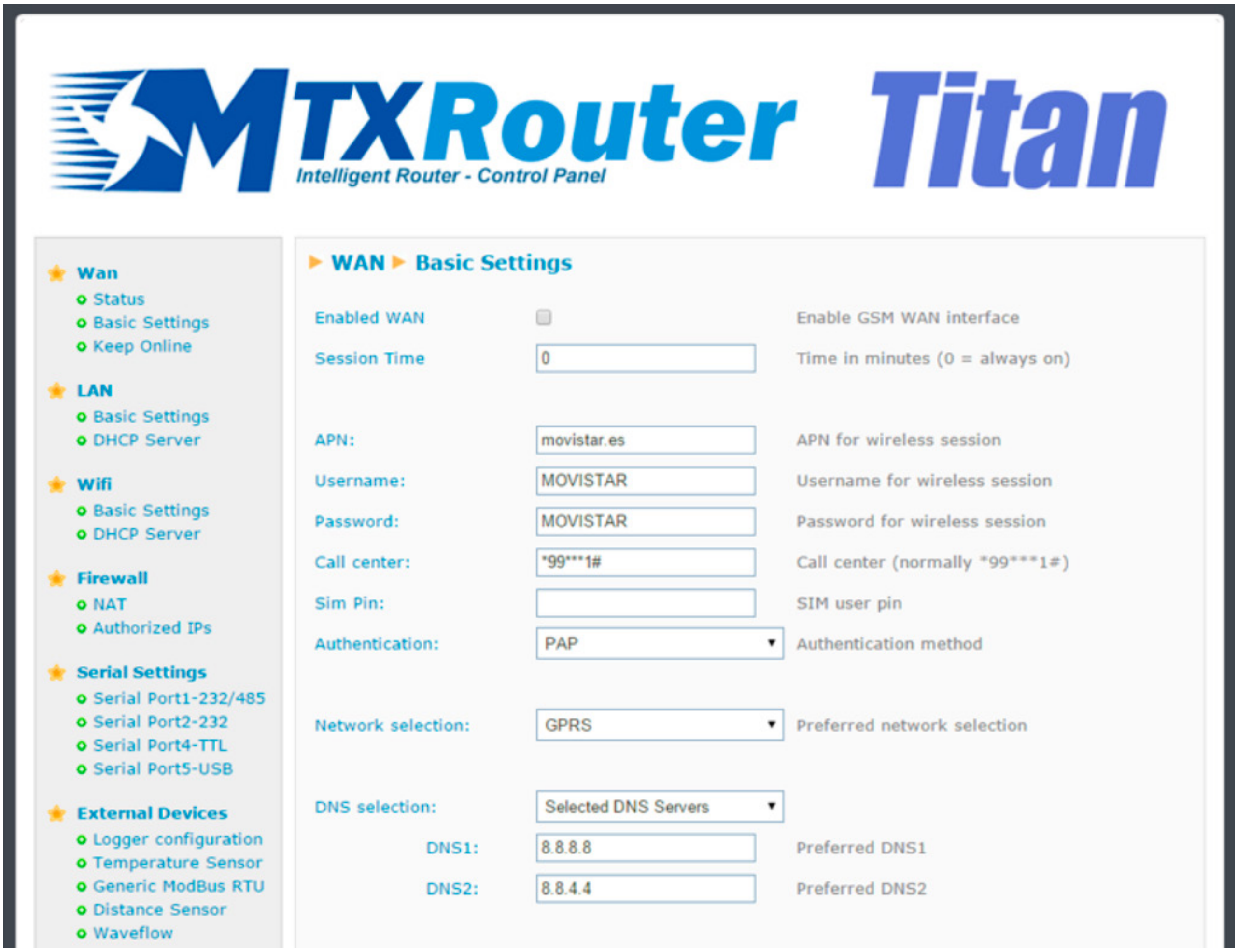
Baudrate:	9600 ▾	Baudrate of serial port
Data bits:	8 ▾	Number of data bit
Parity:	none ▾	Parity
Stop bits:	1 ▾	Number of stop bits
Flow Control:	none ▾	Flow control of serial port
Timeout ms:	0	msec without serial data before sending (normally: 0)
Mode RS485:	□	Check if you want to use the com port as RS485 (Remember you need to set an internal switch)

☑ **Allow incoming GSM call** **(CSD Data Call)** — Only for **TCP Server** and **TCP Client** functions (CSD only compatible using WAN in GPRS mode)

○ **Function: Nothing or Used by External Device**

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

TCP Local Port:	20010	Listening TCP Port (1 ... 65535)
TCP Temporal client	□	Check if you need a temporal TCP Client when TCP server has not incomming connections



▸ WAN ▸ Basic Settings

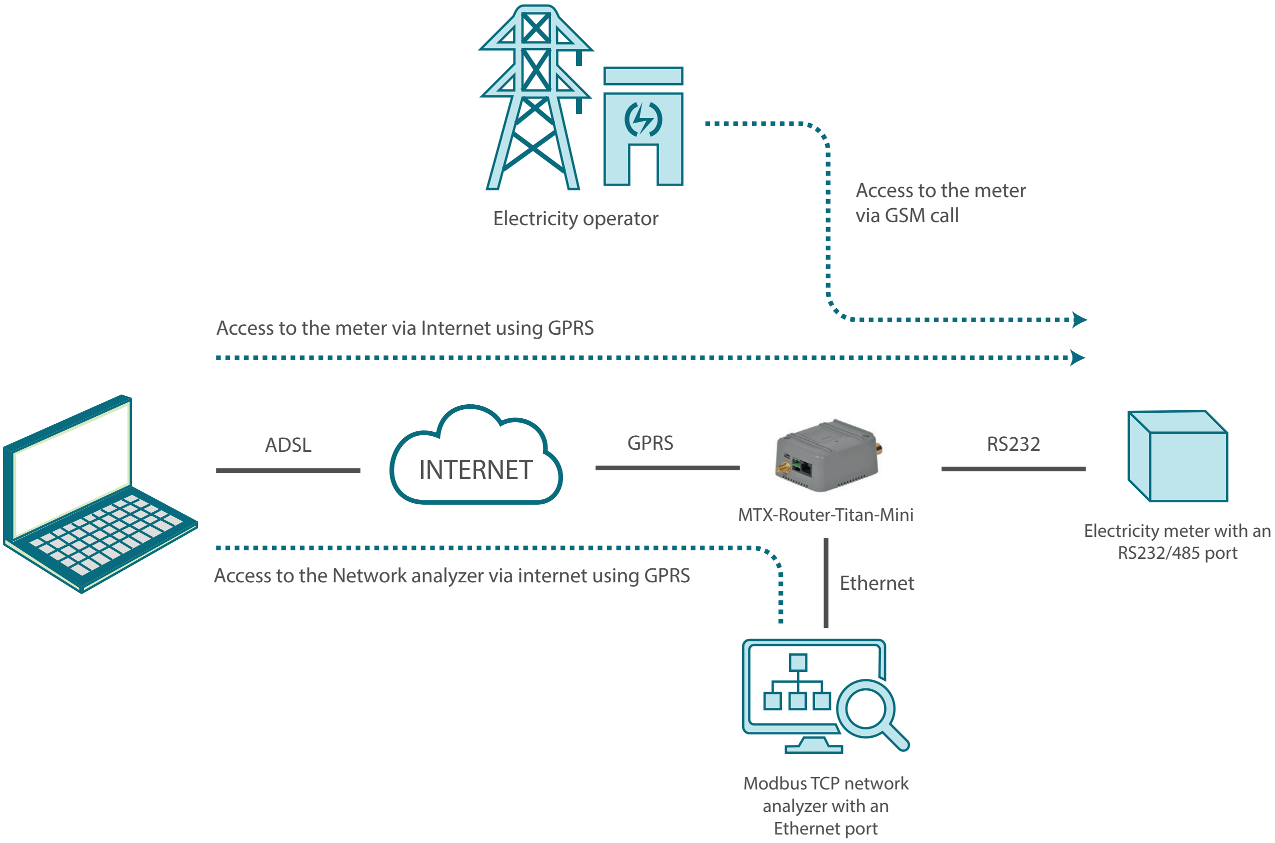
Enabled WAN	□	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP ▾	Authentication method
Network selection:	GPRS ▾	Preferred network selection
DNS selection:	Selected DNS Servers ▾	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2

Example Scenario 2.10: Accessing data from an electronic meter via a GSM data call (Iberdrola, Endesa, etc.) and via GPRS, giving priority to the GSM call made by the company. Also, obtaining remote access to a network analyzer using an Ethernet port via Modbus TCP

Details of the example scenario:

- We need to provide Internet access to a network analyzer with an Ethernet interface. We must be able to access it in the TCP502 port given that it is a Modbus TCP meter. The meter's LAN IP address is 192.168.1.70
- On the other hand, we have an electricity meter with an RS232 port with the configuration 9600bps 8N1. The data from this meter should be accessed using a transparent GPRS-RS232 gateway, for which we will use the TCP20010 port
- The energy provider (Iberdrola, Endesa, etc.) must also be able to access the electricity meter via a typical GSM (CSD) data call. When the operator access the data, the GPRS connection will be suspended until the call is terminated

Solution: MTX-Router-Titan router

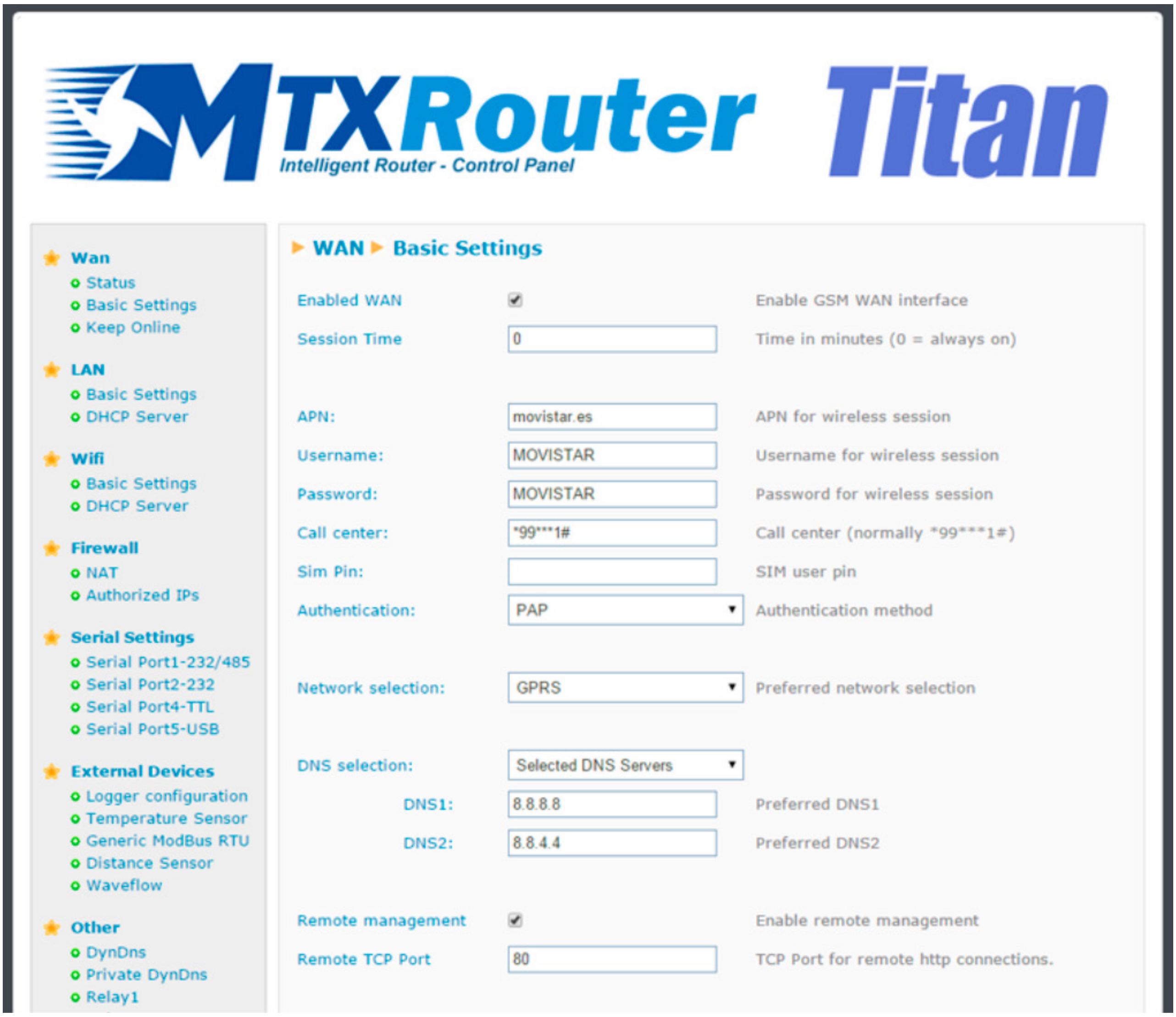

Electricity operator
Access to the meter via GSM call
Access to the meter via Internet using GPRS
ADSL
INTERNET
GPRS
RS232
MTX-Router-Titan-Mini
Electricity meter with an RS232/485 port
Access to the Network analyzer via internet using GPRS
Ethernet
Modbus TCP network analyzer with an Ethernet port

Configuration example ready for use:

We can easily load the example from the router's web configuration environment from the menu "Other>Backup/Examples".

Details:

1. After loading the configuration on our router, we can access the router's configuration with the default username and password: "admin" and "admin" and the IP address "192.168.1.2"
2. Check the configuration in the menus "Wan>Basic Settings", "LAN>Basic Settings", "Firewall>NAT", "Serial Settings>Serial Port 1"
3. Remember that the router can only be configured to accept CSD calls when the router is in fixed GPRS mode. It is not possible when in 3G mode



▶ WAN ▶ Basic Settings

Enabled WAN ☑ Enable GSM WAN interface

Session Time 0 Time in minutes (0 = always on)

APN: movistar.es APN for wireless session

Username: MOVISTAR Username for wireless session

Password: MOVISTAR Password for wireless session

Call center: *99***1# Call center (normally *99***1#)

Sim Pin: SIM user pin

Authentication: PAP Authentication method

Network selection: GPRS Preferred network selection

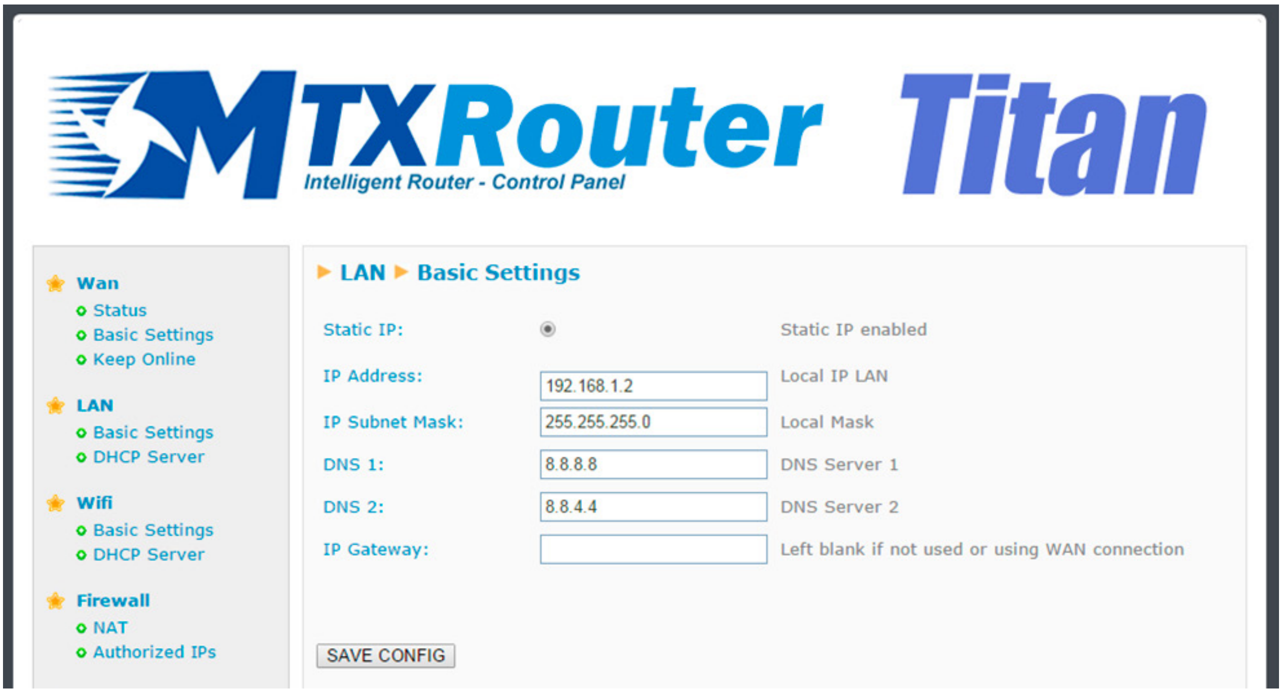
DNS selection: Selected DNS Servers

DNS1: 8.8.8.8 Preferred DNS1

DNS2: 8.8.4.4 Preferred DNS2

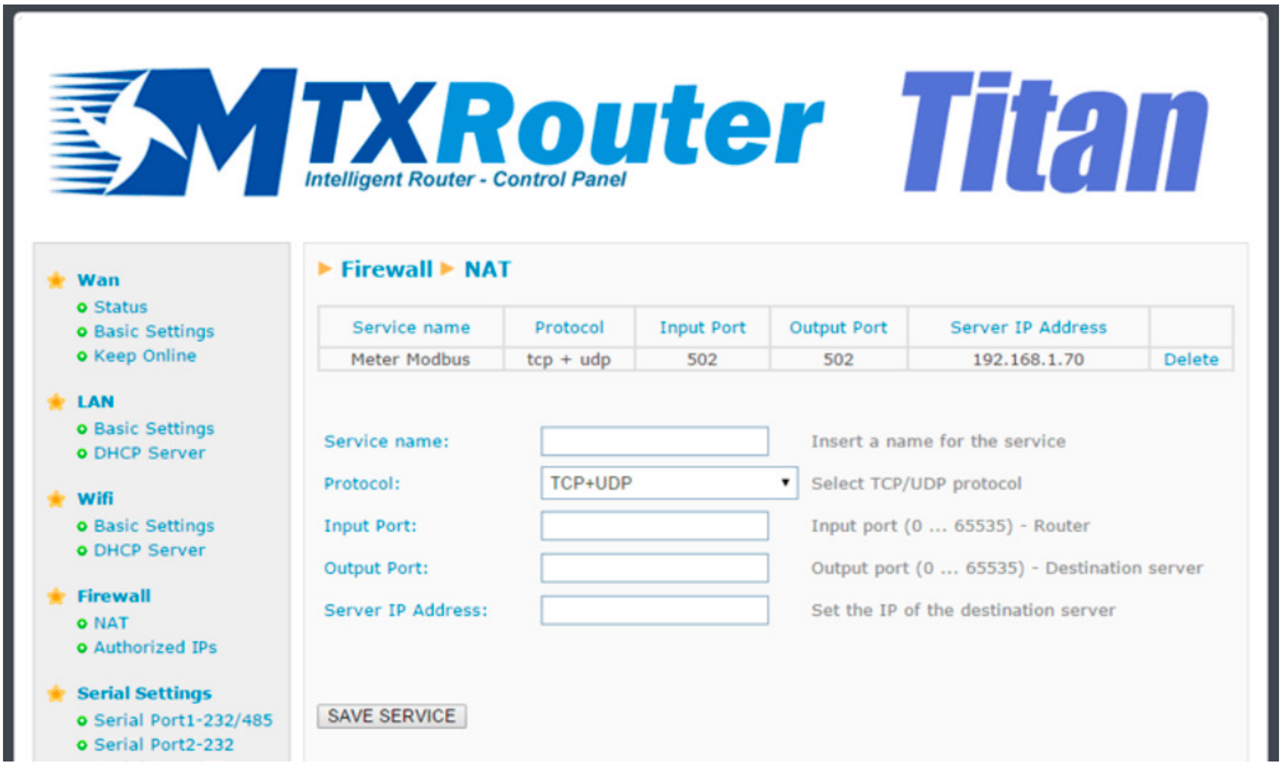
Remote management ☑ Enable remote management

Remote TCP Port 80 TCP Port for remote http connections.



▶ LAN ▶ Basic Settings

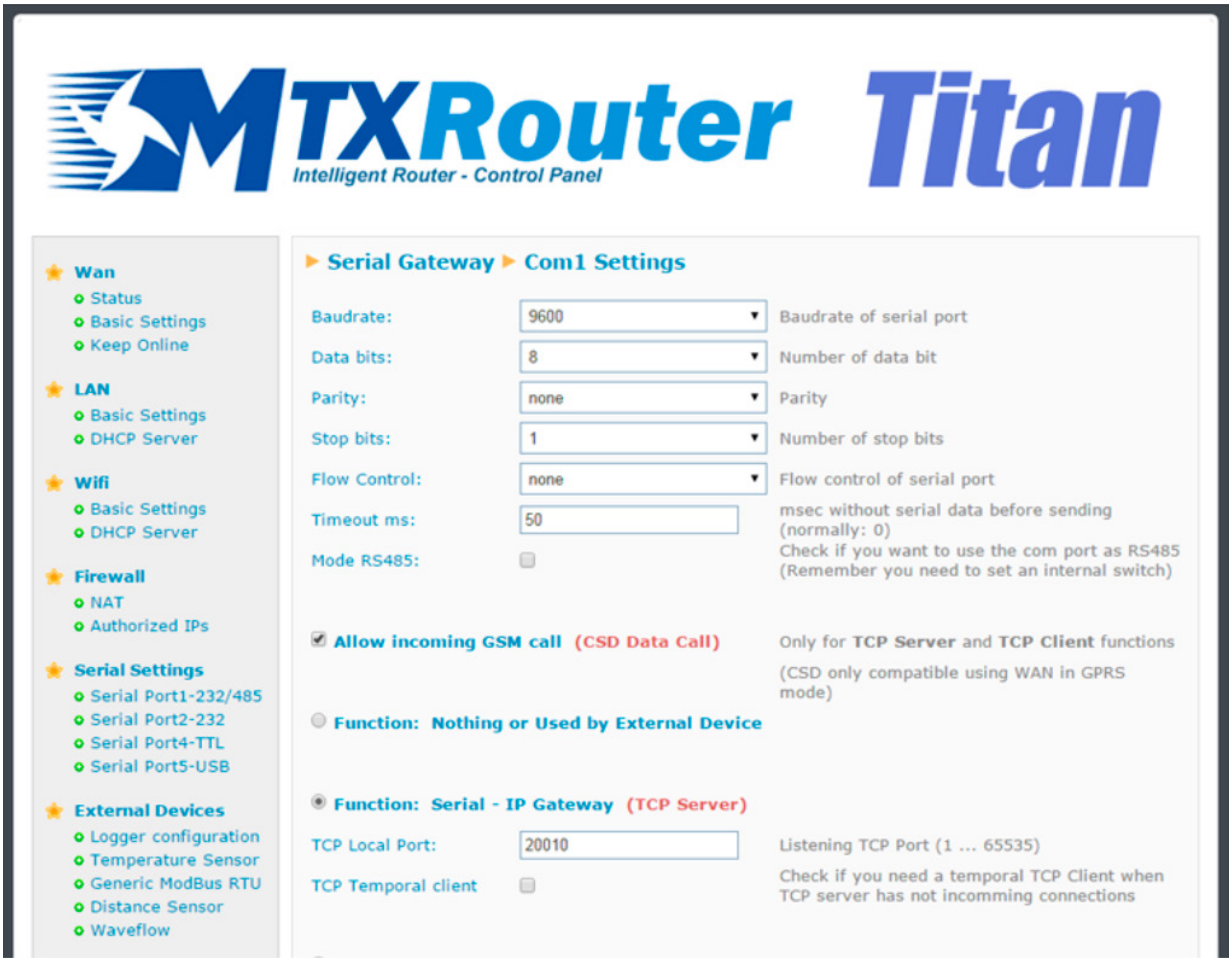
Static IP:	●	Static IP enabled
IP Address:	192.168.1.2	Local IP LAN
IP Subnet Mask:	255.255.255.0	Local Mask
DNS 1:	8.8.8.8	DNS Server 1
DNS 2:	8.8.4.4	DNS Server 2
IP Gateway:		Left blank if not used or using WAN connection



▶ Firewall ▶ NAT

Service name	Protocol	Input Port	Output Port	Server IP Address	
Meter Modbus	tcp + udp	502	502	192.168.1.70	Delete

Service name:		Insert a name for the service
Protocol:	TCP+UDP ▾	Select TCP/UDP protocol
Input Port:		Input port (0 … 65535) - Router
Output Port:		Output port (0 … 65535) - Destination server
Server IP Address:		Set the IP of the destination server



▸ 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
Flow Control:	none ▾	Flow control of serial port
Timeout ms:	50	msec without serial data before sending (normally: 0)
Mode RS485:	□	Check if you want to use the com port as RS485 (Remember you need to set an internal switch)

☑ Allow incoming GSM call (CSD Data Call) — Only for **TCP Server** and **TCP Client** functions (CSD only compatible using WAN in GPRS mode)

○ Function: Nothing or Used by External Device

● Function: Serial - IP Gateway (TCP Server)

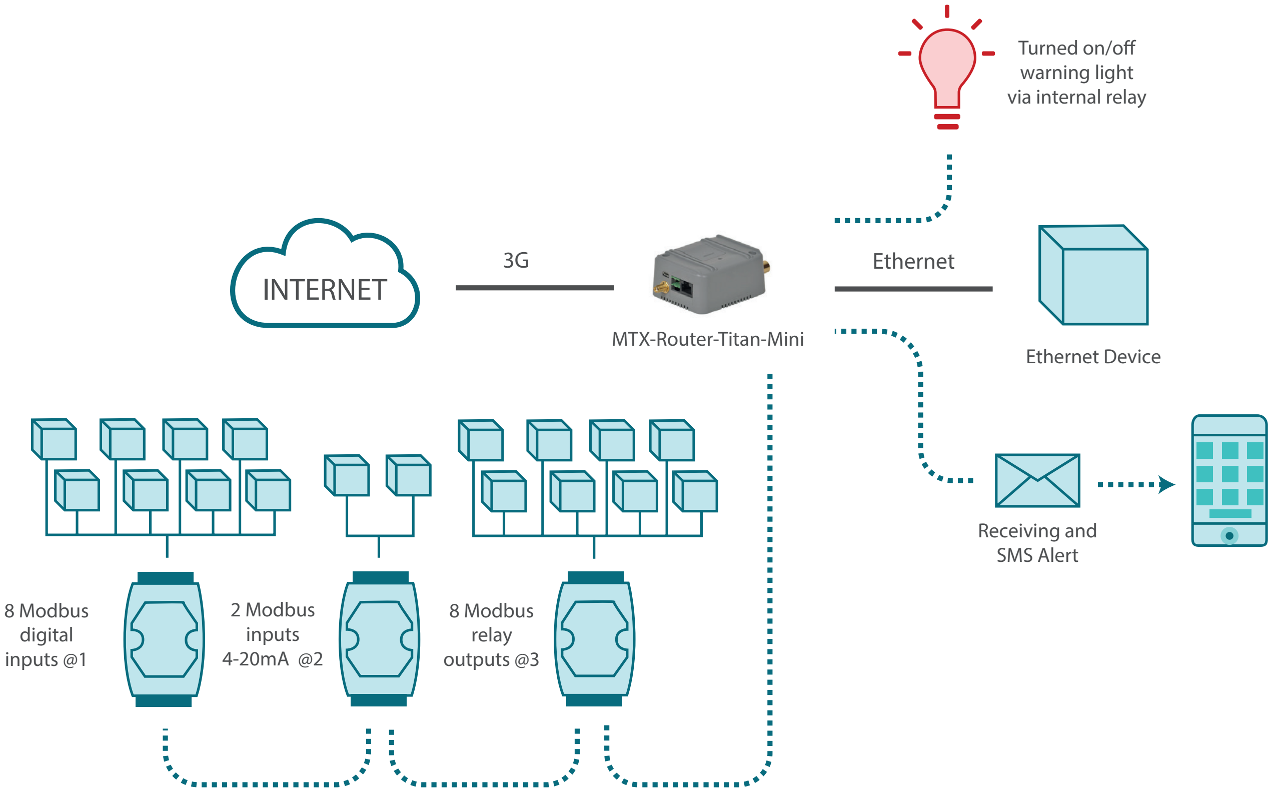
TCP Local Port:	20010	Listening TCP Port (1 ... 65535)
TCP Temporal client	□	Check if you need a temporal TCP Client when TCP server has not incomming connections

Example Scenario 2.11: Example of how Titan Scripts are used. Updating registers in a Modbus device according to the Modbus registers in a different device. Sending SMS and changing the Titan's relays according to the values in these registers

Details of the example scenario:

- We need to provide Internet connectivity to a network analyzer with an Ethernet interface. The LAN IP address of the Ethernet device 192.168.1.70
- We also have 3 Modbus RTU modules. One of them, with address Modbus1, is to ready 8 digital inputs. The module with address 2 allows us to read 2 analog inputs (4-20mA). The module with address 3 has 8 relay outputs
- We can change Relay1 in module 3 (by writing "1" in register 1) when the digital inputs 1, 2 and 3 (registers 1, 2 and 3) in module 1 are activated (all three of them have the value "1"). Also, Relay2 in module 3 will be changed (writing 1 in register 2) when the digital entries 4 or 5 (registers 4 and 5) in module 1 are not activated or when the analog input 1 in module 2 has a value of 10mA or less. Finally, an SMS alert should be sent and an internal relay in the Titan minidevice should be changed when the second analog input in module 2 has a value greater than 18mA

Solution: MTX-Router-Titan mini router

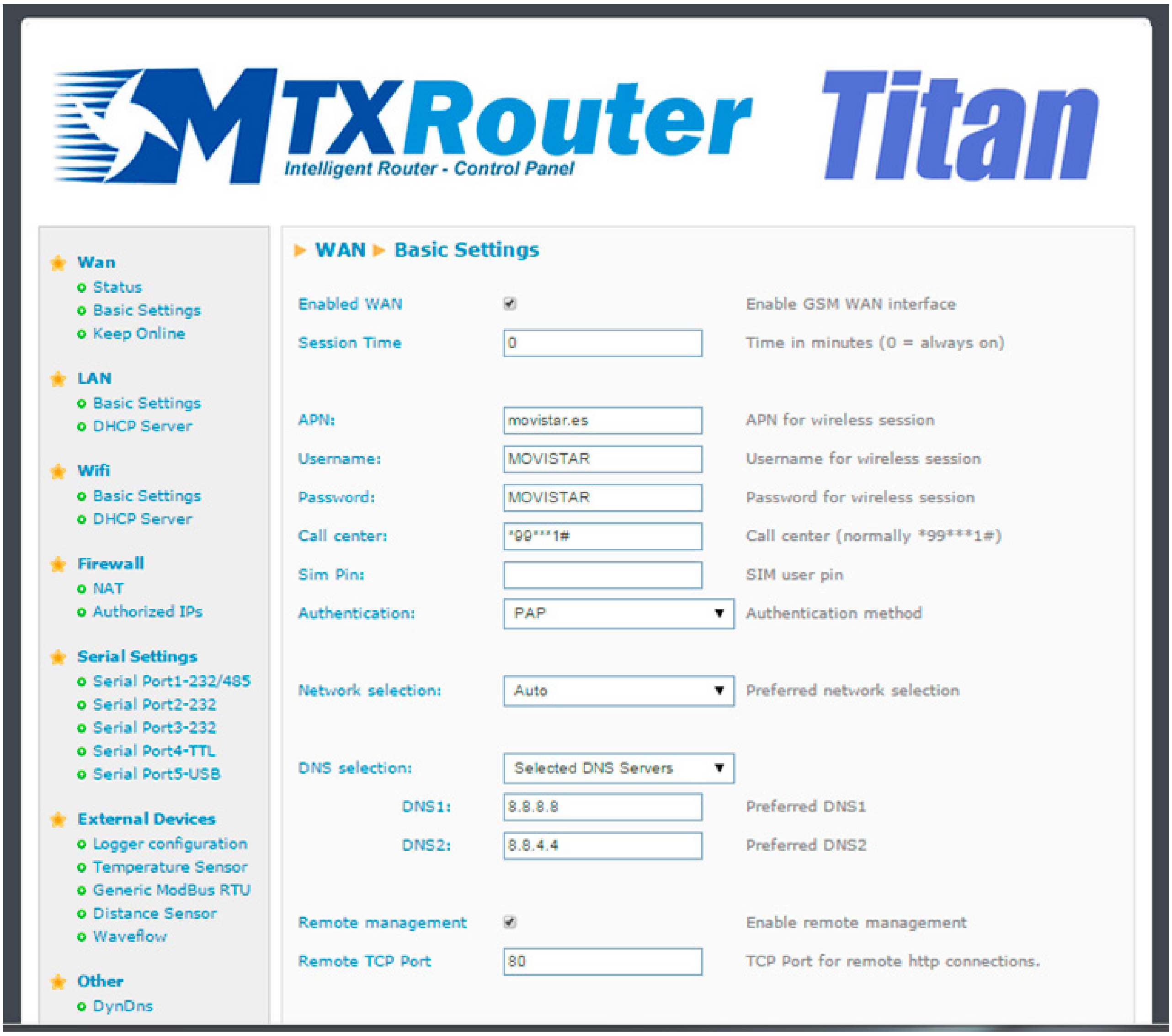


Configuration example ready for use:

We can easily load the example from the router’s web configuration environment from the menu “Other>Backup / Examples”.

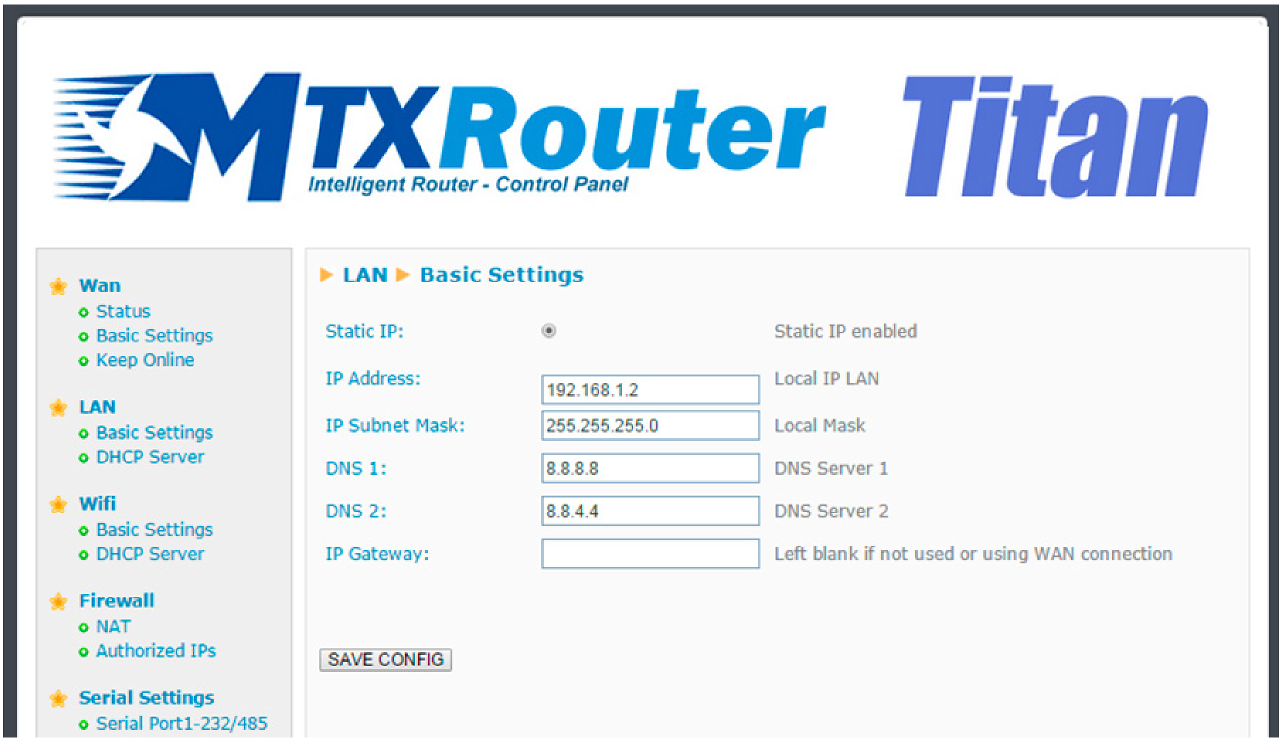
Details:

1. After loading the configuration on our router, we can access the router’s configuration with the default username and password: “admin” and “admin” and the IP address “192.168.1.2”
2. Check the configuration in the menus “Wan>Basic Settings”, “LAN>Basic Settings”, “Serial Settings>Serial Port 1”, “Other>Titan Scripts”



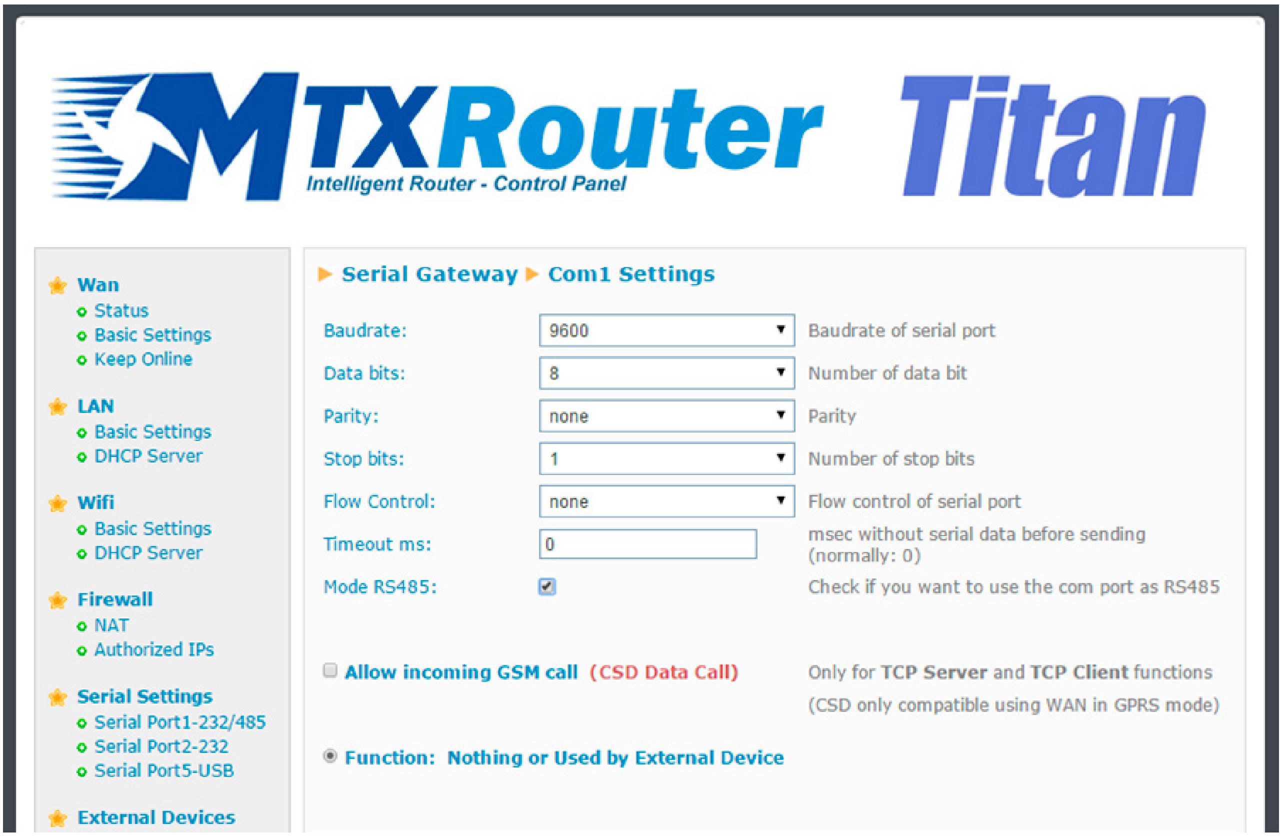
▶ WAN ▶ Basic Settings

Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP	Authentication method
Network selection:	Auto	Preferred network selection
DNS selection:	Selected DNS Servers	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	80	TCP Port for remote http connections.



▶ LAN ▶ Basic Settings

Static IP:	●	Static IP enabled
IP Address:	192.168.1.2	Local IP LAN
IP Subnet Mask:	255.255.255.0	Local Mask
DNS 1:	8.8.8.8	DNS Server 1
DNS 2:	8.8.4.4	DNS Server 2
IP Gateway:		Left blank if not used or using WAN connection

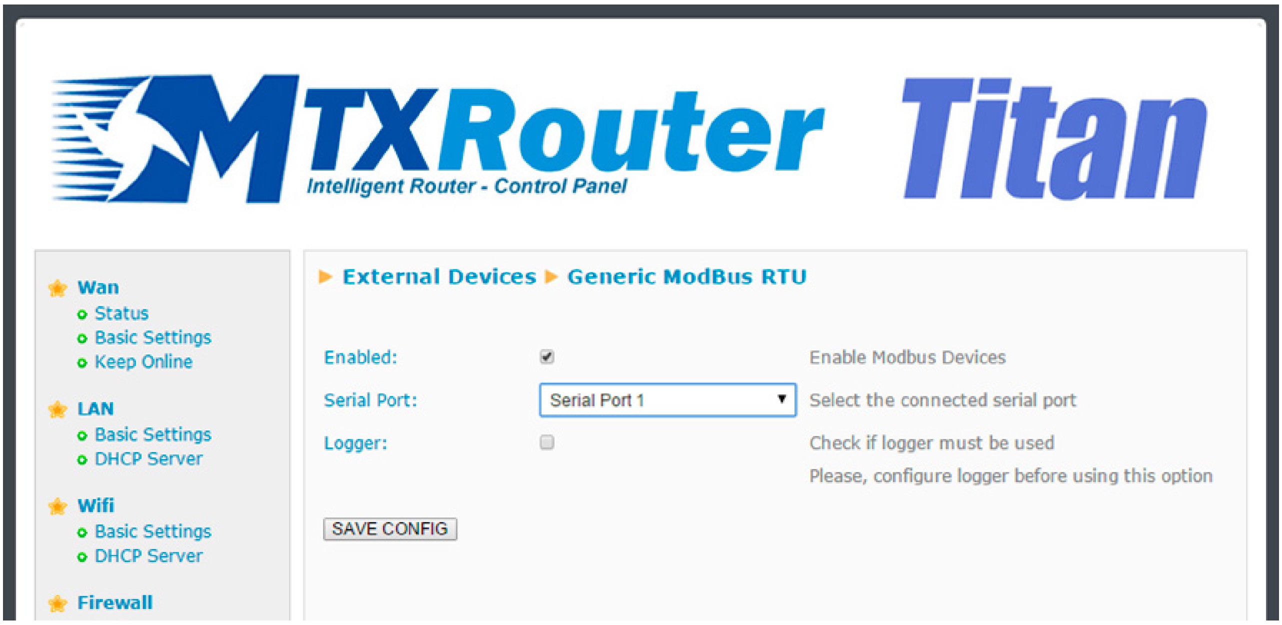


▶ Serial Gateway ▶ Com1 Settings

Baudrate:	9600	Baudrate of serial port
Data bits:	8	Number of data bit
Parity:	none	Parity
Stop bits:	1	Number of stop bits
Flow Control:	none	Flow control of serial port
Timeout ms:	0	msec without serial data before sending (normally: 0)
Mode RS485:	☑	Check if you want to use the com port as RS485

☐ **Allow incoming GSM call (CSD Data Call)** — Only for **TCP Server** and **TCP Client** functions (CSD only compatible using WAN in GPRS mode)

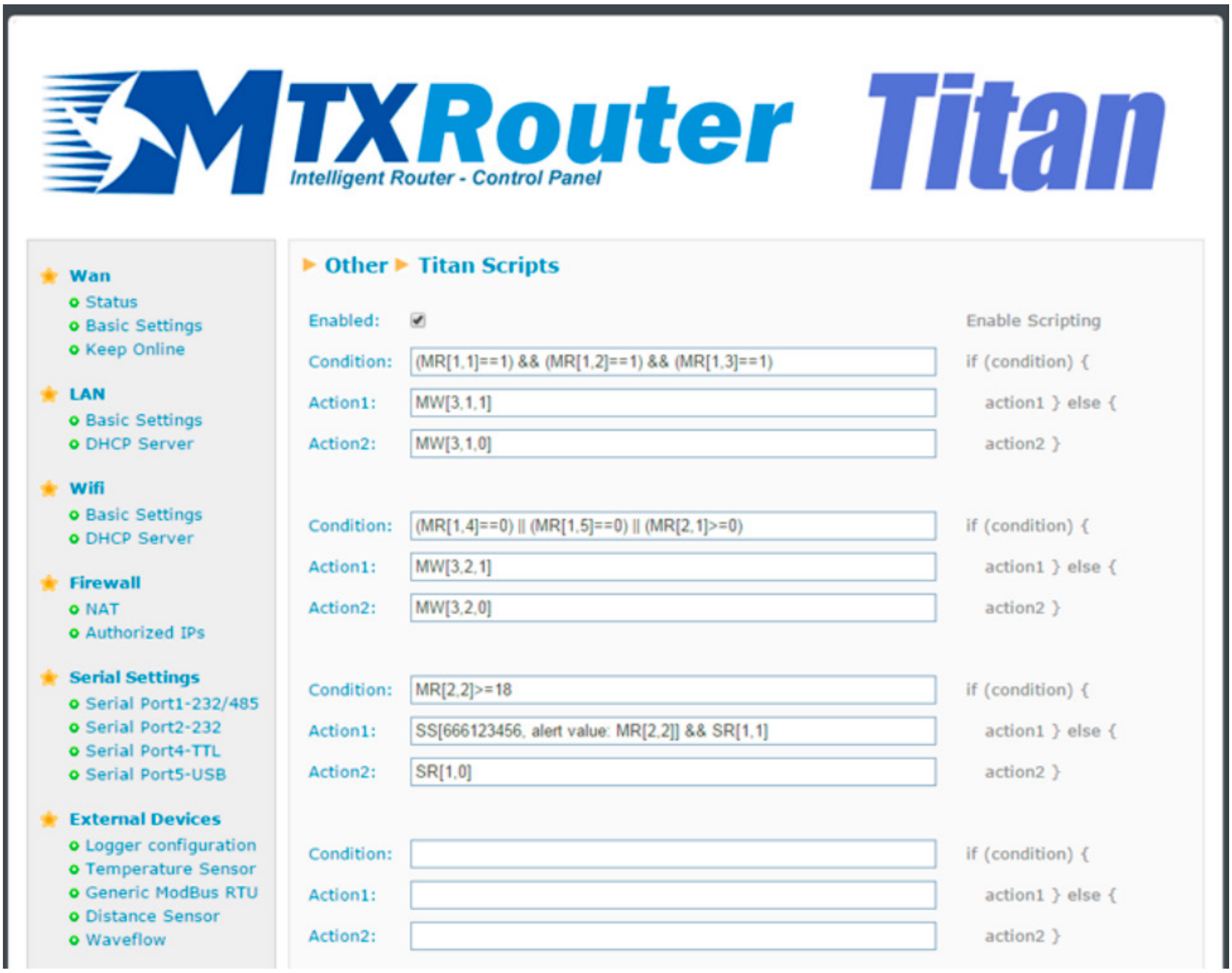
● **Function: Nothing or Used by External Device**



External Devices ▶ Generic ModBus RTU

Enabled:	☑	Enable Modbus Devices
Serial Port:	Serial Port 1 ▾	Select the connected serial port
Logger:	□	Check if logger must be used Please, configure logger before using this option

SAVE CONFIG

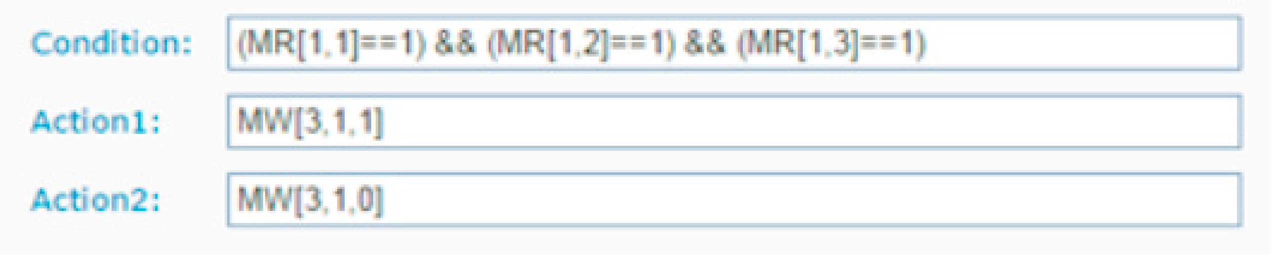


Other ▶ Titan Scripts

Enabled:	☑	Enable Scripting
Condition:	(MR[1,1]==1) && (MR[1,2]==1) && (MR[1,3]==1)	if (condition) {
Action1:	MW[3,1,1]	action1 } else {
Action2:	MW[3,1,0]	action2 }
Condition:	(MR[1,4]==0) || (MR[1,5]==0) || (MR[2,1]>=0)	if (condition) {
Action1:	MW[3,2,1]	action1 } else {
Action2:	MW[3,2,0]	action2 }
Condition:	MR[2,2]>=18	if (condition) {
Action1:	SS[666123456, alert value: MR[2,2]] && SR[1,1]	action1 } else {
Action2:	SR[1,0]	action2 }
Condition:		if (condition) {
Action1:		action1 } else {
Action2:		action2 }

Details (2):

The exact meaning of the scripts is:



Condition: (MR[1,1]==1) && (MR[1,2]==1) && (MR[1,3]==1)

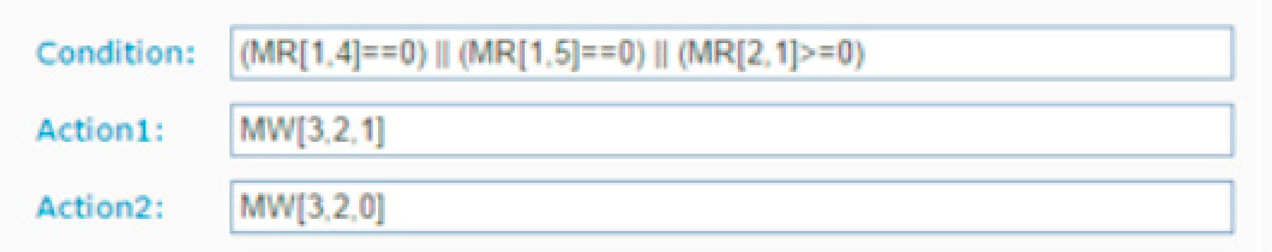
Action1: MW[3,1,1]

Action2: MW[3,1,0]

Condition: [If register 1 of the device with address 1 is equal to 1] AND [If register 2 of the device with address 1 is equal to 1] AND [If register 3 of the device with address 1 is equal to 1]

If true: write “1” in register 1 of the device with address 3

If false: write “0” in register 1 of the device with address 3



Condition: (MR[1,4]==0) || (MR[1,5]==0) || (MR[2,1]>=0)

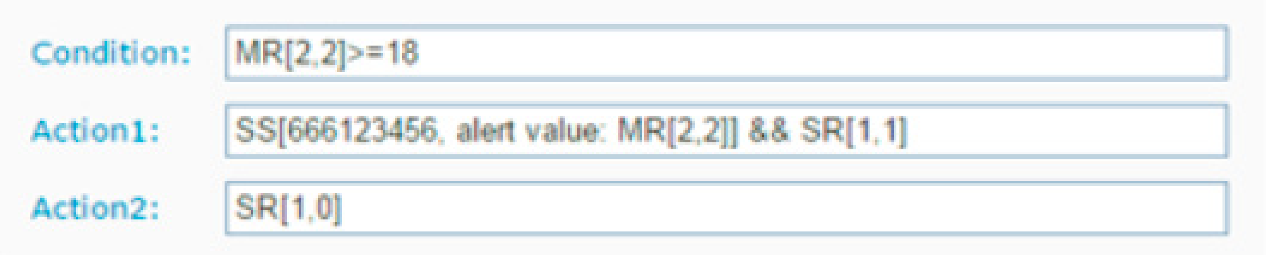
Action1: MW[3,2,1]

Action2: MW[3,2,0]

Condition: [If register 4 of the device with address 1 is equal to 0] OR [If register 5 of the device with address 1 is equal to 1] OR [If register 1 of the device with address 2 is greater than or equal to 1]

If true: write “1” in register 2 of the device with address 3

If false: write “0” in register 2 of the device with address 3



Condition: MR[2,2]>=18

Action1: SS[666123456, alert value: MR[2,2]] && SR[1,1]

Action2: SR[1,0]

Condition: [If register 2 of the device with address 2 is greater than or equal to 18]

If true: send an SMS to the telephone 666274646 with the text “alert value: [the current value of register 2 in the device with address 2]” AND activate the Titan device’s relay 1

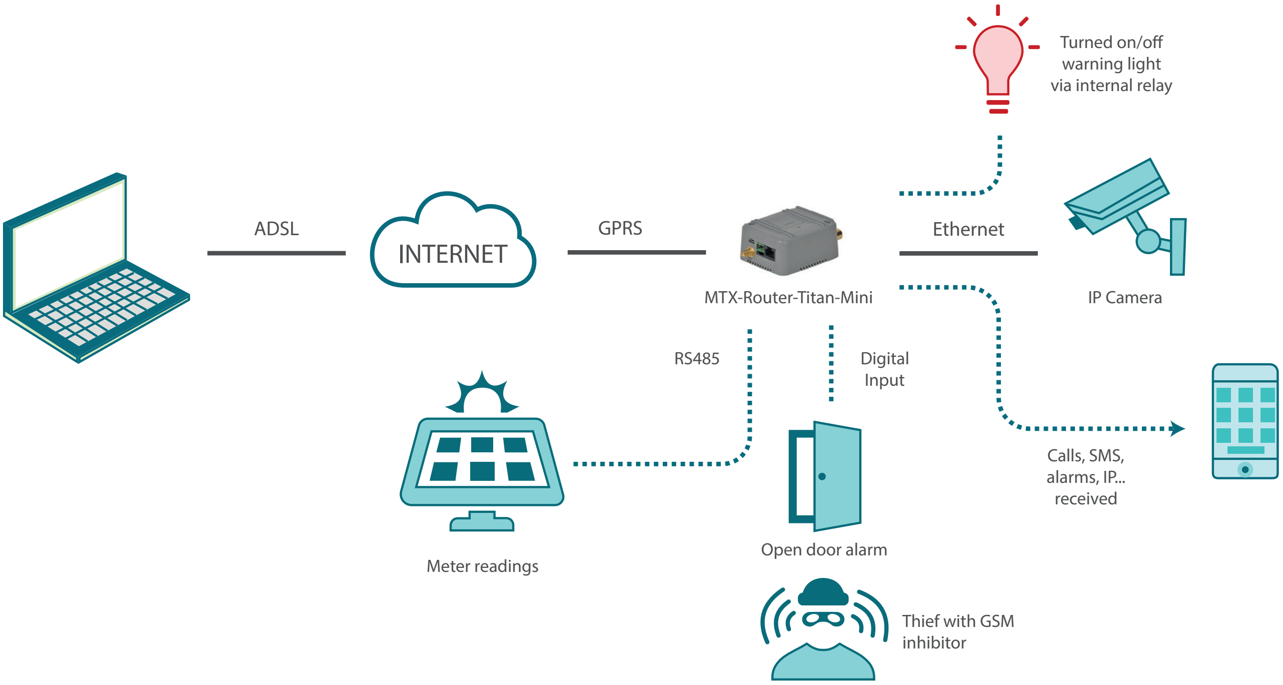
If false: desactivate the Titan device’s relay 1

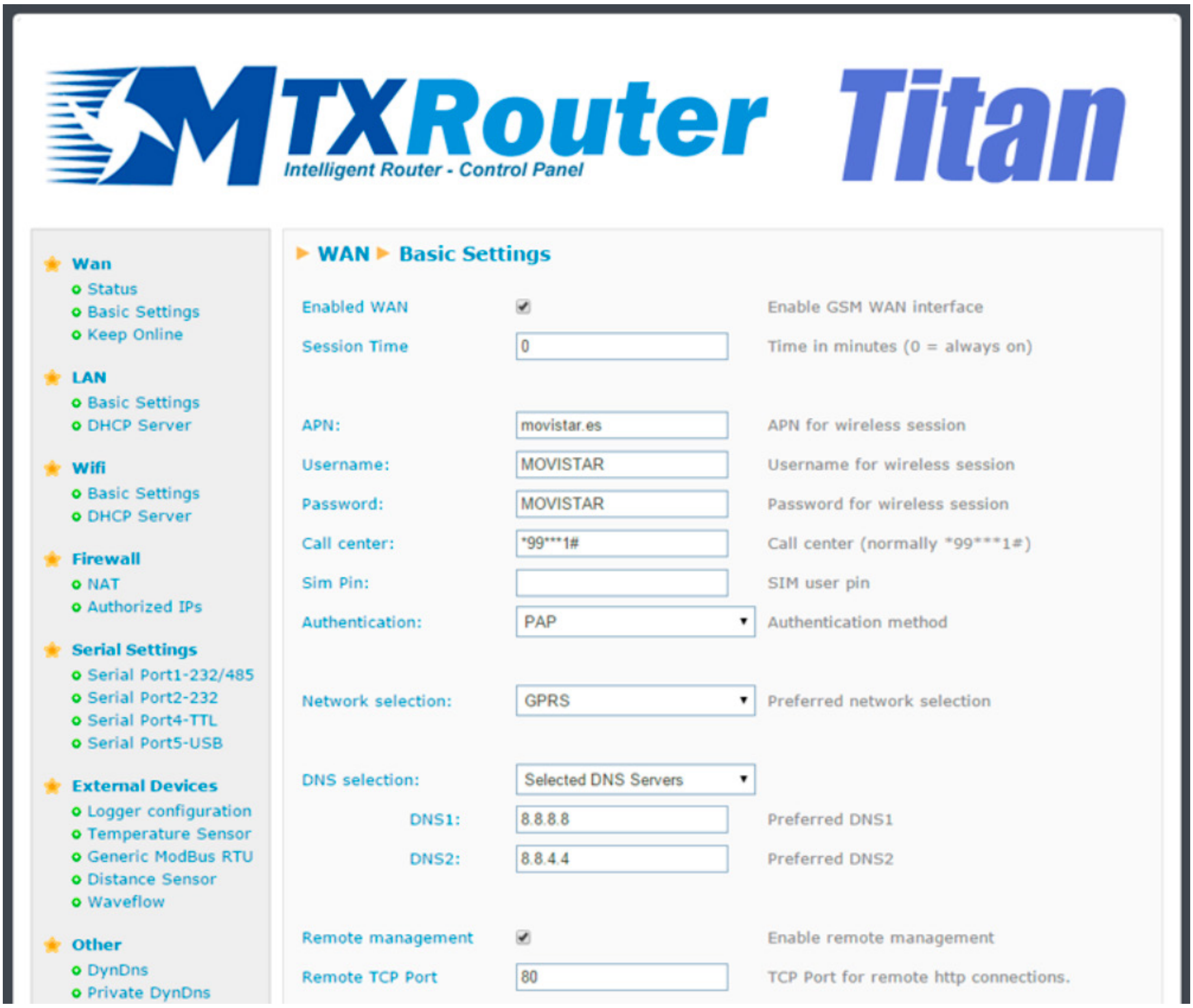
● Example Scenario 2.12: Example of an alarm after detecting Jamming (GSM inhibitor). Remote control of an IP camera via GPRS. Changing a relay and making a warning call when possible Jamming is detected. Sending SMS alerts when an open gate is detected

Details of the example scenario:

- We need to be able to remotely access, via GPRS, an IP camera that is located in a solar farm to monitor neglected equipment
- The camera has an IP address of 192.168.1.70 and the webserver to which we need to connect is located in the TCP port 8080
- To economize, a SIM card with a dynamic public IP address will be used. We must be able to obtain the router's IP address via a missed call from either of the following numbers: 666123456 and 666123457
- The router must be configured to detected possible GSM inhibitors. When a possible detection is made, a relay connected to a siren must be activated and, if the inhibitor signal is weak given it is not too close, an SMS alert must be sent and a GSM call made to the number 666123456
- The router should supervise a gate and if opened, an SMS alert must be sent to the numbers 666123456 and 666123457
- We will also use the router to take daily readings of an RS485 electricity meter (configuration 9600bps, 8N1) via a transparent GPRS/RS485 gateway

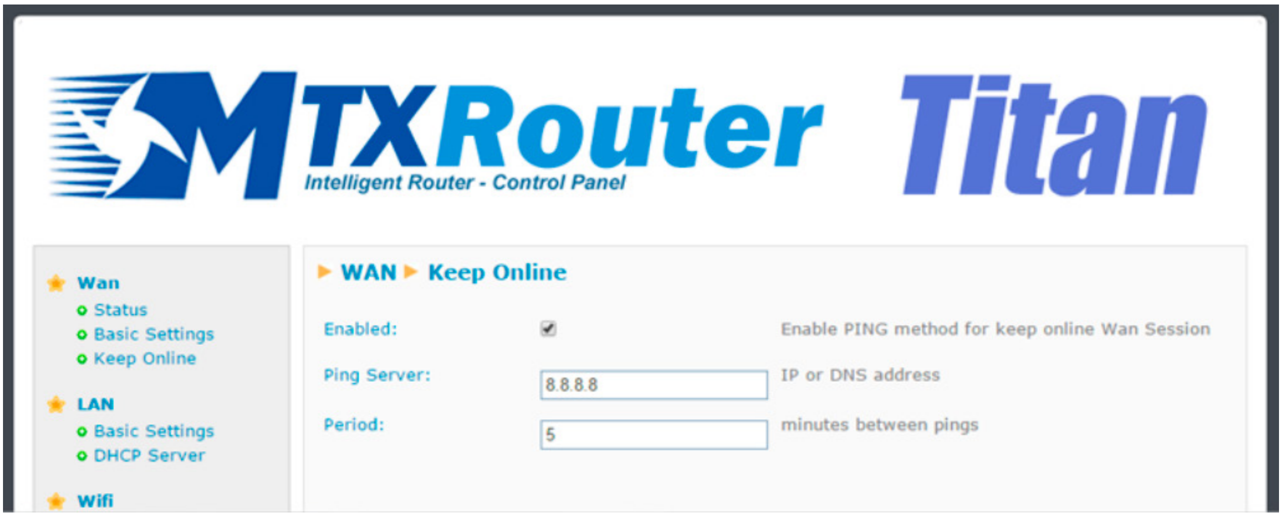
Solution: MTX-Router-Titan mini router





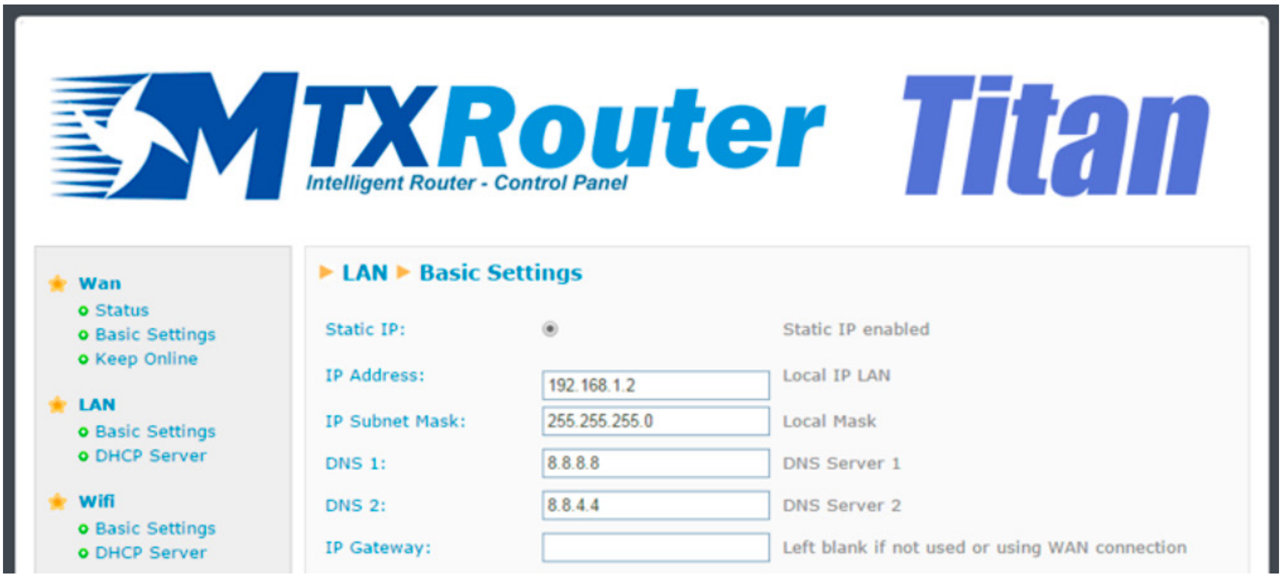
▶ WAN ▶ Basic Settings

Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP	Authentication method
Network selection:	GPRS	Preferred network selection
DNS selection:	Selected DNS Servers	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	80	TCP Port for remote http connections.



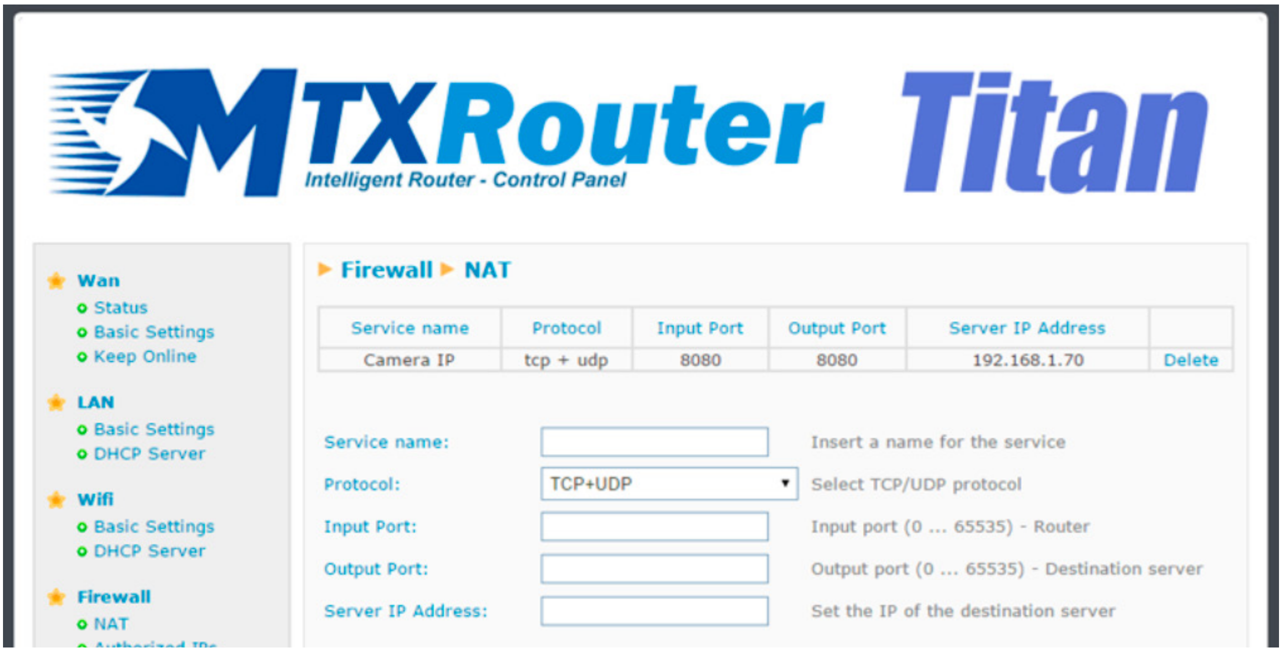
▶ WAN ▶ Keep Online

Enabled:	☑	Enable PING method for keep online Wan Session
Ping Server:	8.8.8.8	IP or DNS address
Period:	5	minutes between pings



▶ LAN ▶ Basic Settings

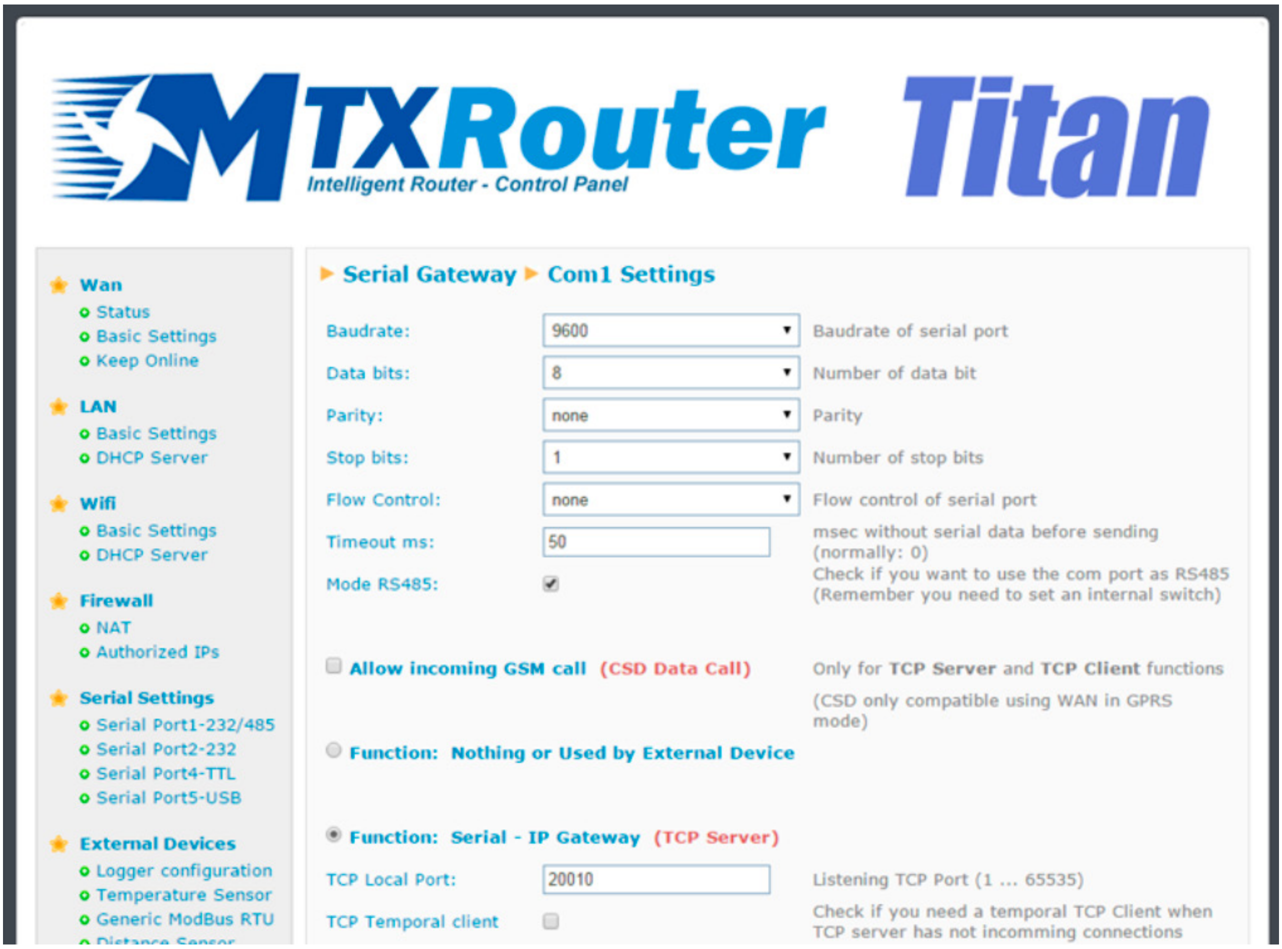
Static IP:	●	Static IP enabled
IP Address:	192.168.1.2	Local IP LAN
IP Subnet Mask:	255.255.255.0	Local Mask
DNS 1:	8.8.8.8	DNS Server 1
DNS 2:	8.8.4.4	DNS Server 2
IP Gateway:		Left blank if not used or using WAN connection



▶ Firewall ▶ NAT

Service name	Protocol	Input Port	Output Port	Server IP Address	
Camera IP	tcp + udp	8080	8080	192.168.1.70	Delete

Service name:		Insert a name for the service
Protocol:	TCP+UDP ▾	Select TCP/UDP protocol
Input Port:		Input port (0 ... 65535) - Router
Output Port:		Output port (0 ... 65535) - Destination server
Server IP Address:		Set the IP of the destination server



▶ Serial Gateway ▶ Com1 Settings

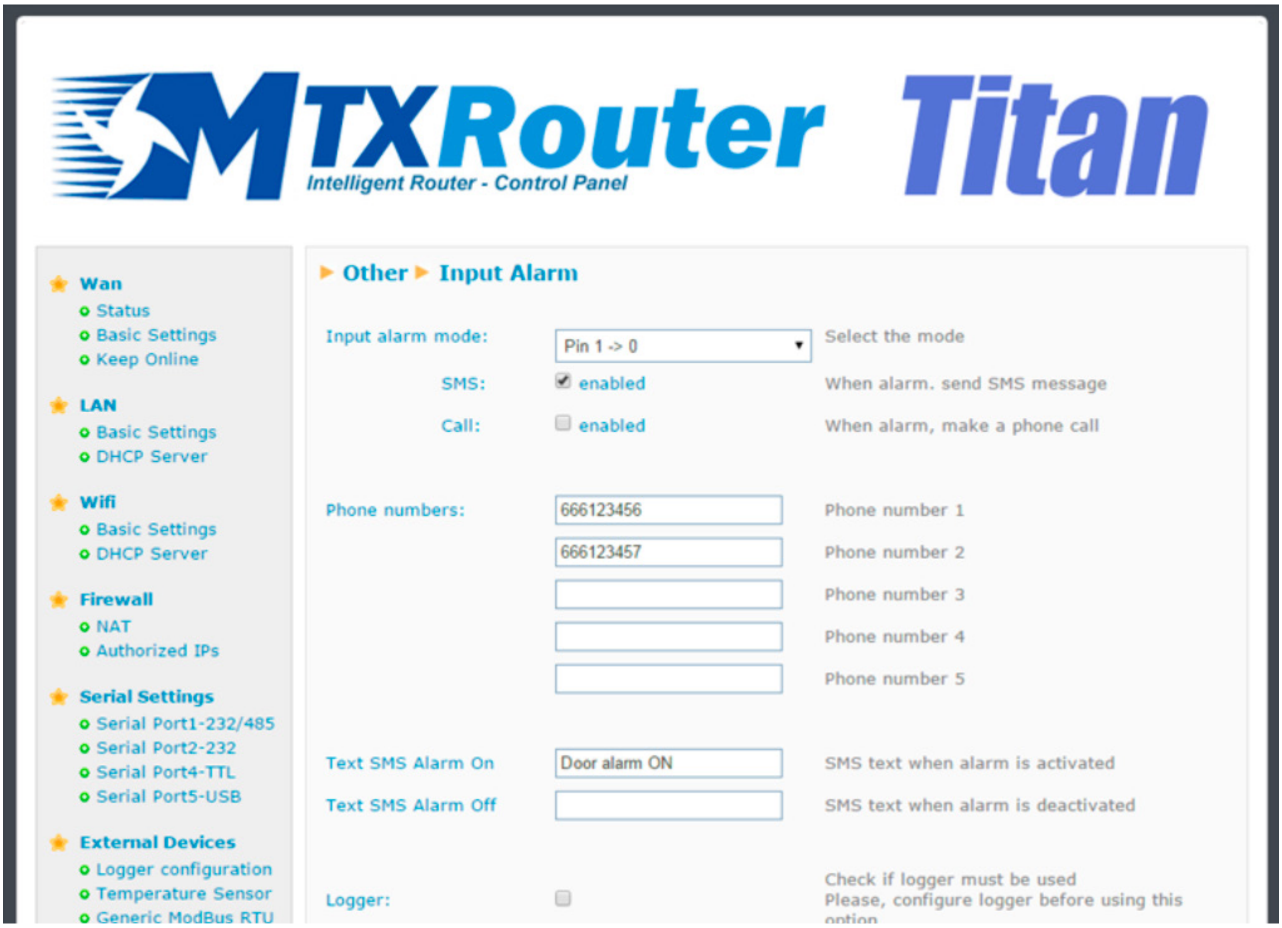
Baudrate:	9600	Baudrate of serial port
Data bits:	8	Number of data bit
Parity:	none	Parity
Stop bits:	1	Number of stop bits
Flow Control:	none	Flow control of serial port
Timeout ms:	50	msec without serial data before sending (normally: 0)
Mode RS485:	☑	Check if you want to use the com port as RS485 (Remember you need to set an internal switch)

□ **Allow incoming GSM call** **(CSD Data Call)** — Only for **TCP Server** and **TCP Client** functions (CSD only compatible using WAN in GPRS mode)

○ **Function: Nothing or Used by External Device**

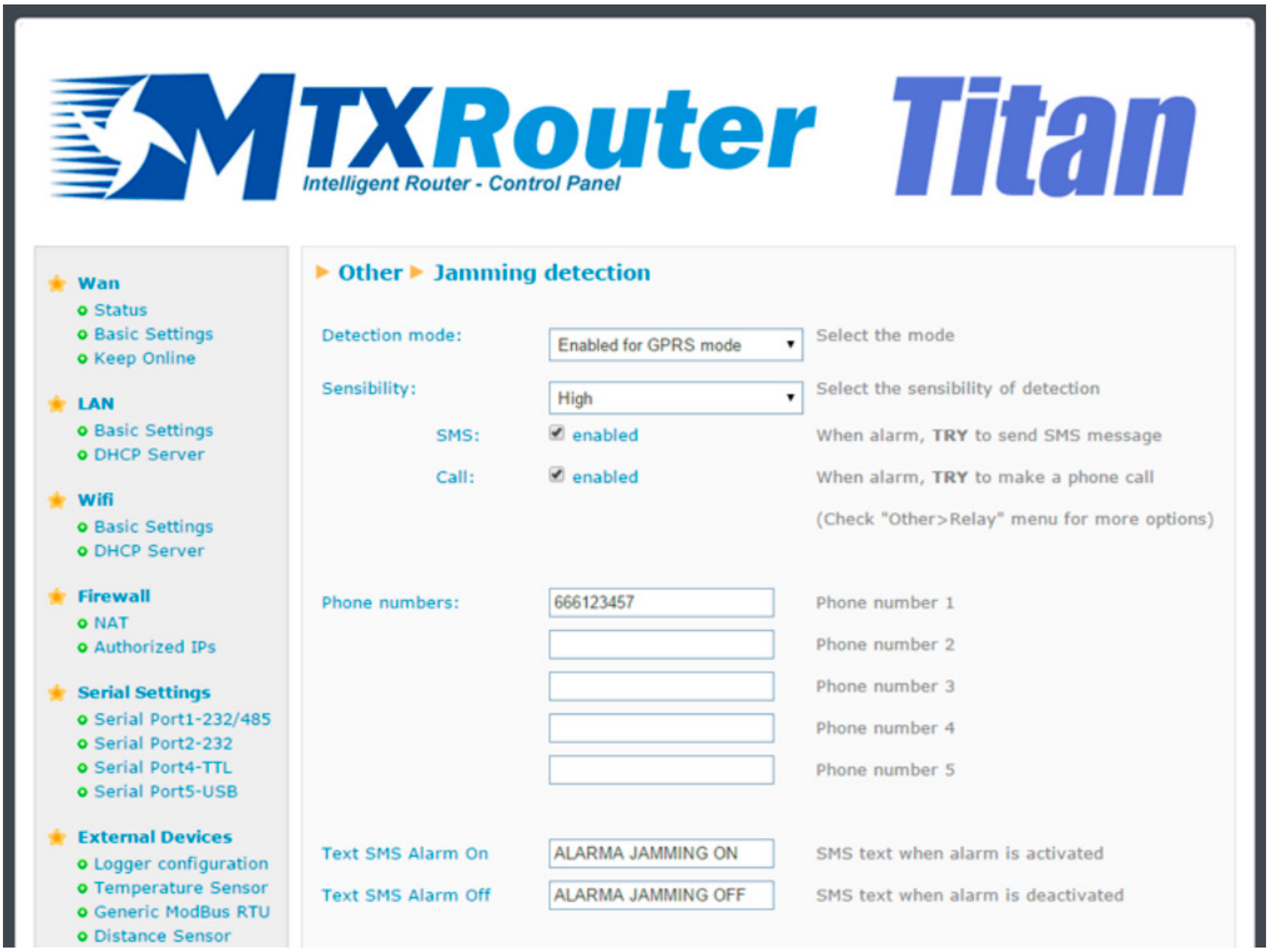
● **Function: Serial - IP Gateway** **(TCP Server)**

TCP Local Port:	20010	Listening TCP Port (1 ... 65535)
TCP Temporal client	□	Check if you need a temporal TCP Client when TCP server has not incomming connections



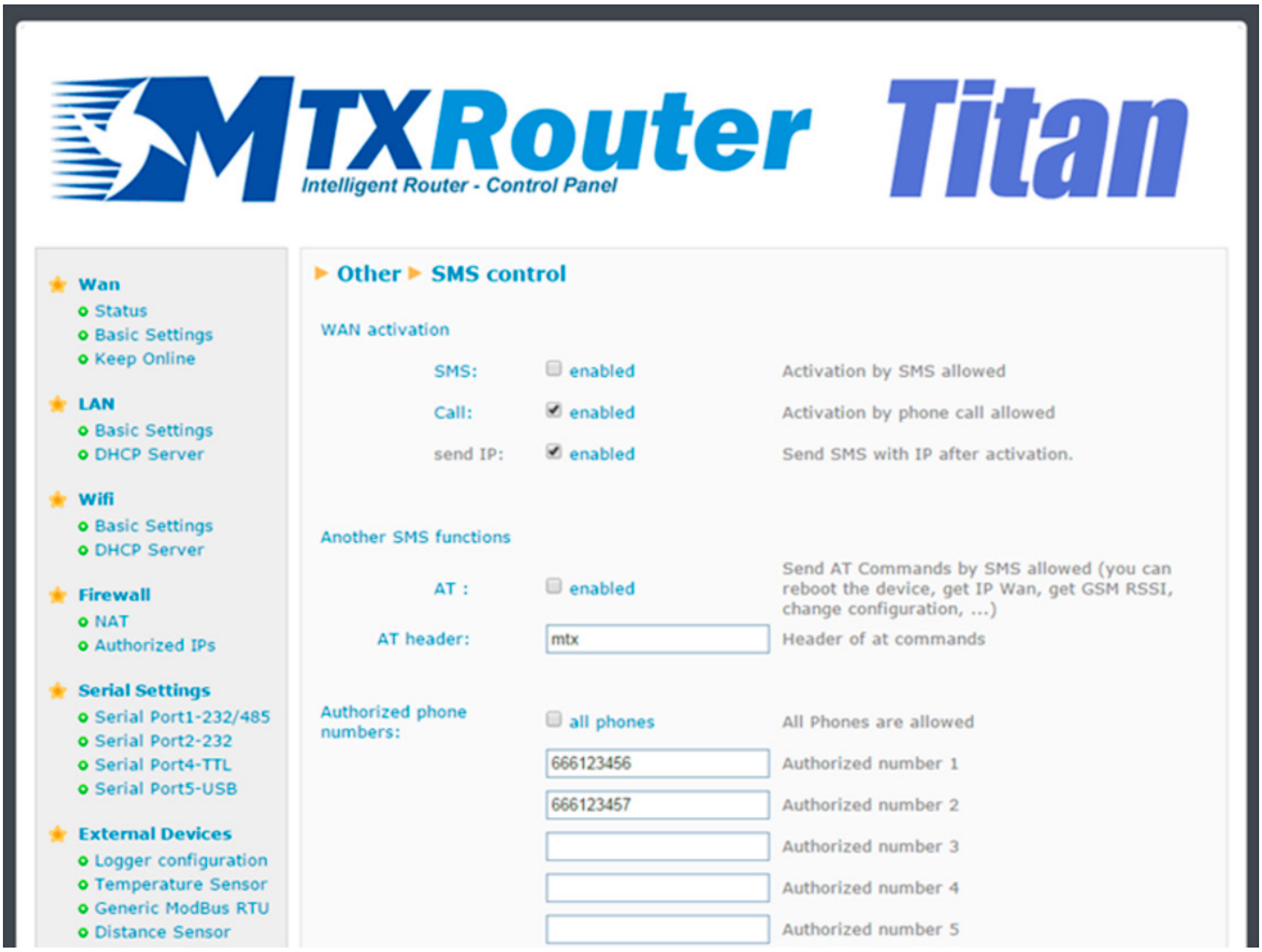
► Other ► Input Alarm

Input alarm mode:	Pin 1 -> 0	Select the mode
SMS:	☑ enabled	When alarm. send SMS message
Call:	□ enabled	When alarm, make a phone call
Phone numbers:	666123456	Phone number 1
	666123457	Phone number 2
		Phone number 3
		Phone number 4
		Phone number 5
Text SMS Alarm On	Door alarm ON	SMS text when alarm is activated
Text SMS Alarm Off		SMS text when alarm is deactivated
Logger:	□	Check if logger must be used Please, configure logger before using this option



► Other ► Jamming detection

Detection mode:	Enabled for GPRS mode ▾	Select the mode
Sensibility:	High ▾	Select the sensibility of detection
SMS:	☑ enabled	When alarm, **TRY** to send SMS message
Call:	☑ enabled	When alarm, **TRY** to make a phone call
		(Check "Other>Relay" menu for more options)
Phone numbers:	666123457	Phone number 1
		Phone number 2
		Phone number 3
		Phone number 4
		Phone number 5
Text SMS Alarm On	ALARMA JAMMING ON	SMS text when alarm is activated
Text SMS Alarm Off	ALARMA JAMMING OFF	SMS text when alarm is deactivated



▶ Other ▶ SMS control

WAN activation

SMS:	□ enabled	Activation by SMS allowed
Call:	☑ enabled	Activation by phone call allowed
send IP:	☑ enabled	Send SMS with IP after activation.

Another SMS functions

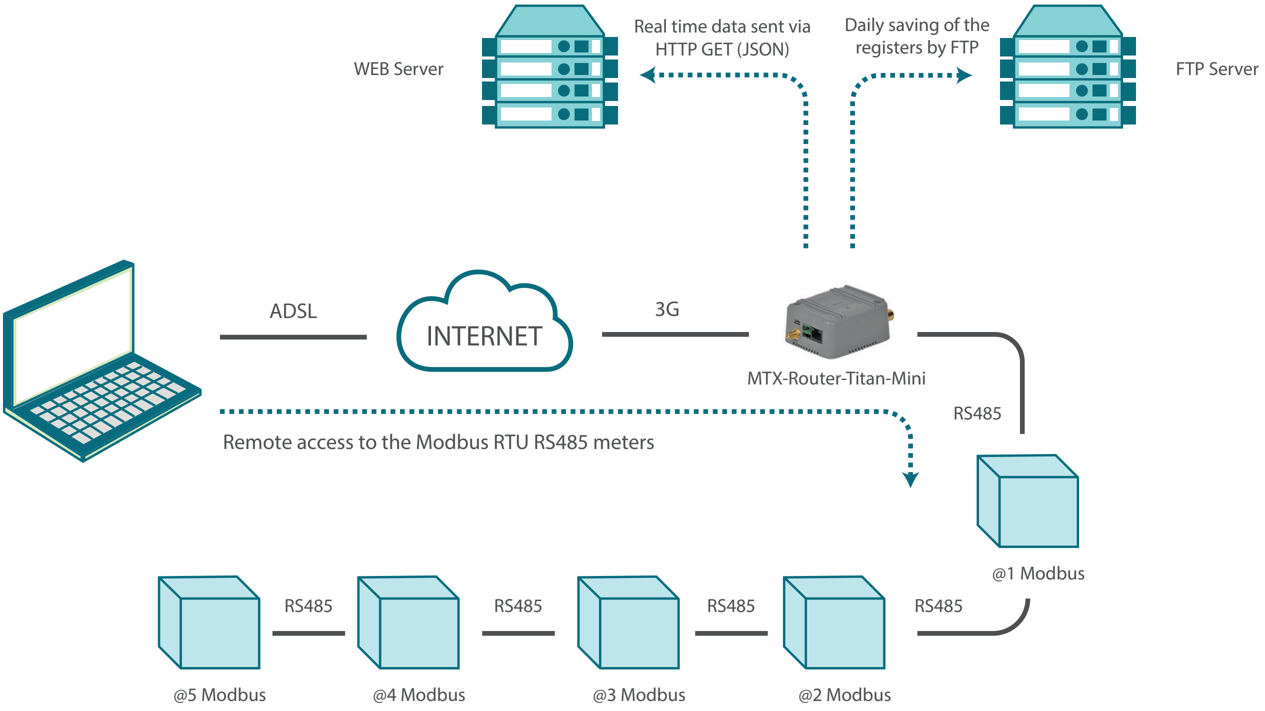
AT :	□ enabled	Send AT Commands by SMS allowed (you can reboot the device, get IP Wan, get GSM RSSI, change configuration, ...)
AT header:	mtx	Header of at commands

Authorized phone numbers:	□ all phones	All Phones are allowed
	666123456	Authorized number 1
	666123457	Authorized number 2
		Authorized number 3
		Authorized number 4
		Authorized number 5

Example Scenario 2.13: Autonomous reading of Modbus registers and automatic sending to two web platforms. HTTP GET will be used to send the registers to one platform, and to the other we will send the data via FTP

Details of the example scenario:

- We need to read several Modbus registers of 5 Modbus RTU devices. The data should be read every 10 minutes
- The router must send the readings to two web platforms. On the one hand, we will send the readings in real time (in JSON format) via HTTP GET to Platform 1. On the other hand, the router will send a file once a day with the readings to Platform 2 via FTP. The file will have a name of the format "IMEI-year-month-day.txt"
- Registers: @1: registers 1-10, @2: register 20 and 30, @3: registers 21-25, @4: registers 100-105 and @5:registers 1-5 and 20-25. All will use the Modbus read command 0x03
- We also need to remotely access each of the Modbus devices, and change registers remotely via a Telnet console and webserver

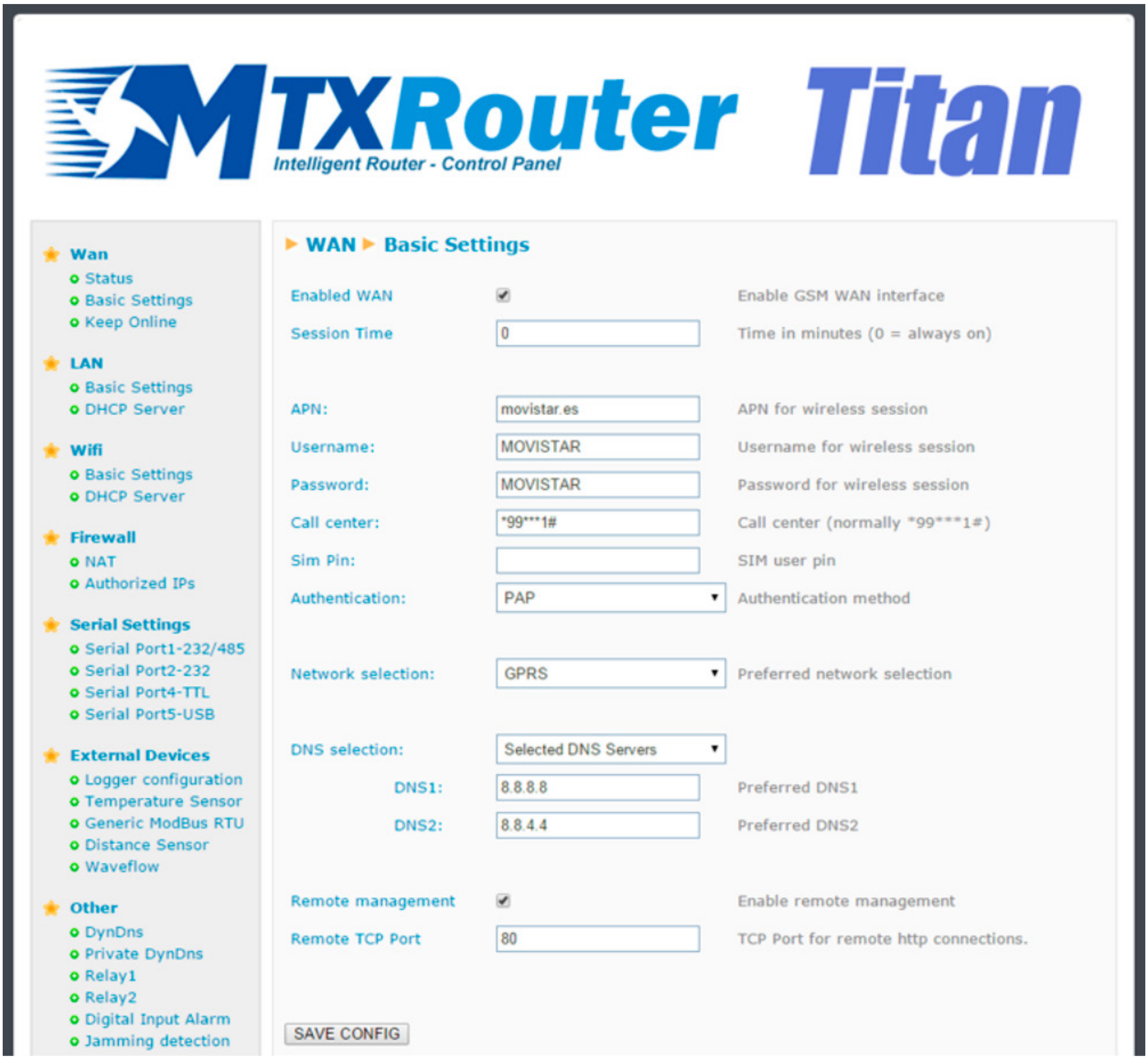


Configuration example ready for use:

We can easily load the example from the router's web configuration environment from the menu "Other>Backup/Examples".

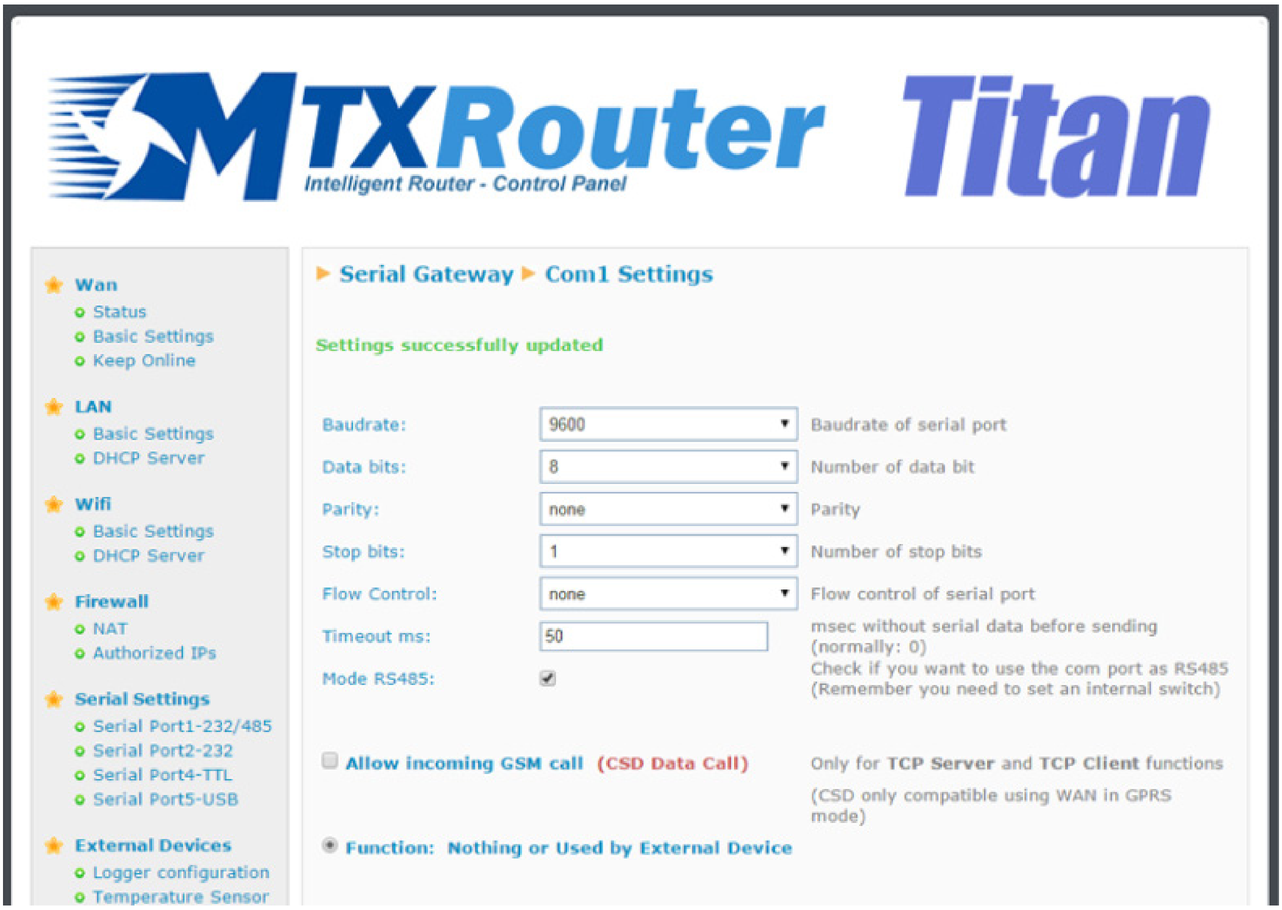
Details:

1. After loading the configuration on our router, we can access the router's configuration with the default username and password: "admin" and "admin" and the IP address "192.168.1.2"
2. Check the configuration in the menus "Wan>Basic Settings", "Serial Settings > Serial Port 1", "External devices > Logger Configuration", "External Devices>Modbus RTU"
3. Remember that readings are not taken immediately upon start-up, but at xx:00, xx:10, xx:20, xx:30, xx:40, etc. (i.e. every 10 minutes)



▶ WAN ▶ Basic Settings

Enabled WAN	☑	Enable GSM WAN interface
Session Time	0	Time in minutes (0 = always on)
APN:	movistar.es	APN for wireless session
Username:	MOVISTAR	Username for wireless session
Password:	MOVISTAR	Password for wireless session
Call center:	*99***1#	Call center (normally *99***1#)
Sim Pin:		SIM user pin
Authentication:	PAP	Authentication method
Network selection:	GPRS	Preferred network selection
DNS selection:	Selected DNS Servers	
DNS1:	8.8.8.8	Preferred DNS1
DNS2:	8.8.4.4	Preferred DNS2
Remote management	☑	Enable remote management
Remote TCP Port	80	TCP Port for remote http connections.



▶ Serial Gateway ▶ Com1 Settings

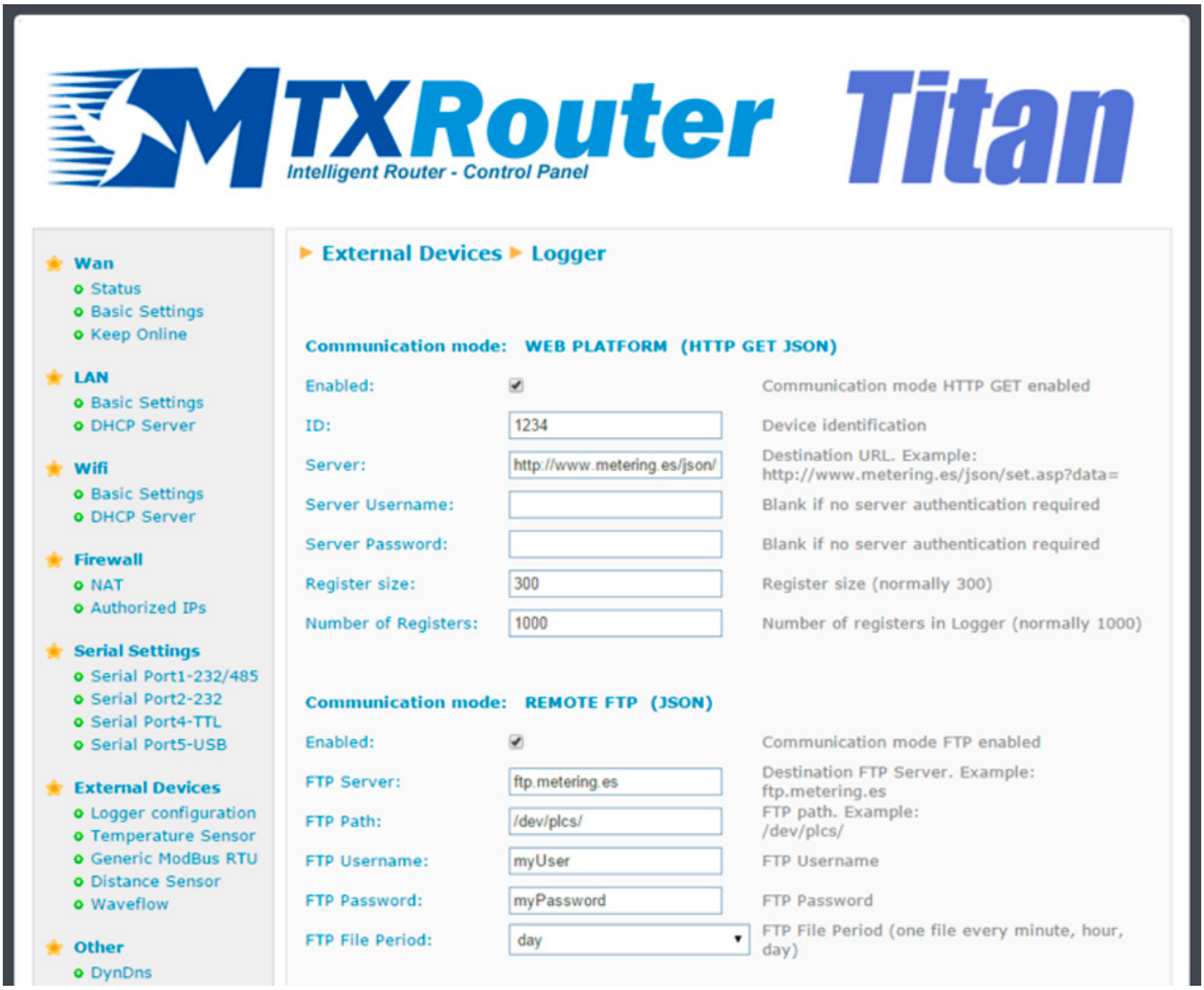
Settings successfully updated

Baudrate:	9600	Baudrate of serial port
Data bits:	8	Number of data bit
Parity:	none	Parity
Stop bits:	1	Number of stop bits
Flow Control:	none	Flow control of serial port
Timeout ms:	50	msec without serial data before sending (normally: 0)
Mode RS485:	☑	Check if you want to use the com port as RS485 (Remember you need to set an internal switch)

☐ Allow incoming GSM call (CSD Data Call) — Only for **TCP Server** and **TCP Client** functions

(CSD only compatible using WAN in GPRS mode)

● Function: Nothing or Used by External Device



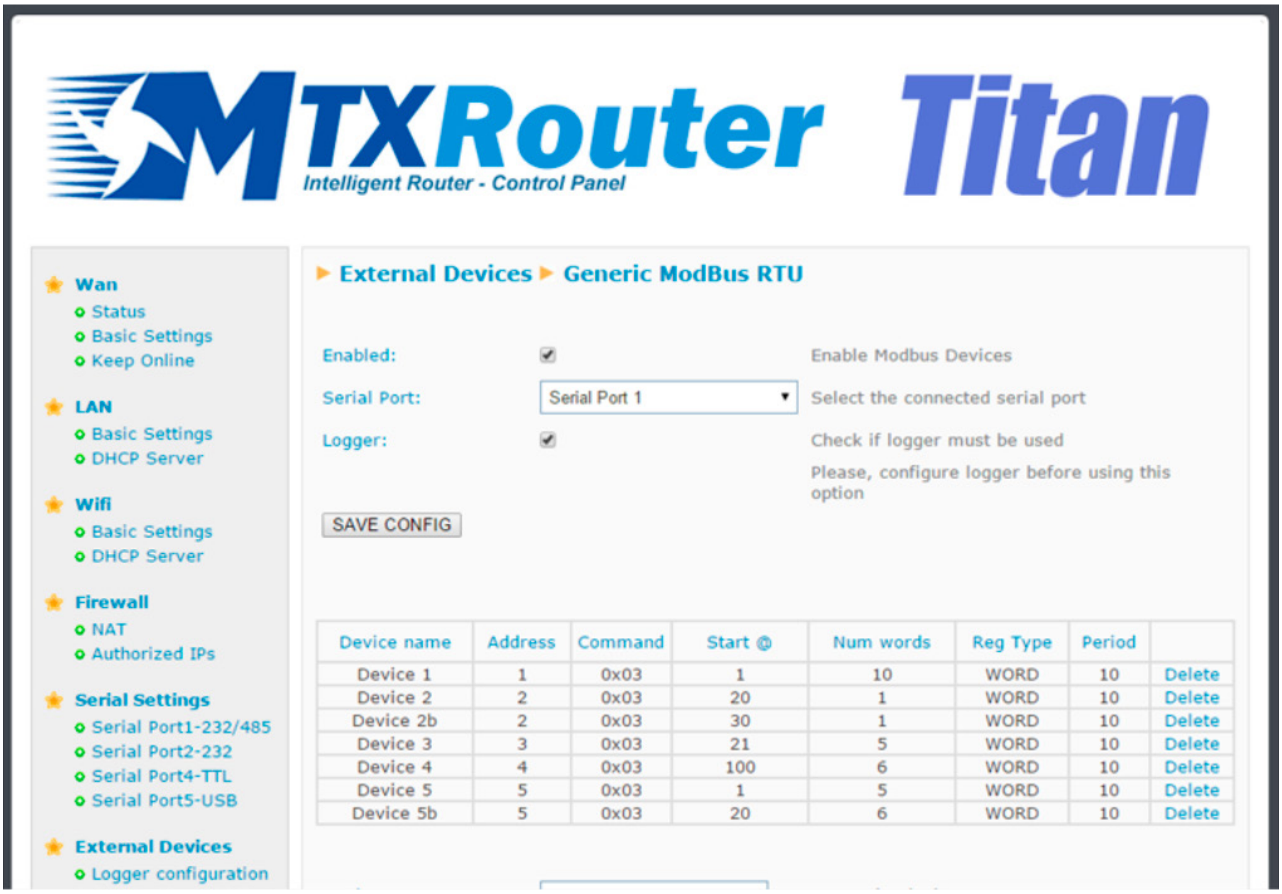
▸ External Devices ▸ Logger

Communication mode: WEB PLATFORM (HTTP GET JSON)

Enabled:	☑	Communication mode HTTP GET enabled
ID:	1234	Device identification
Server:	http://www.metering.es/json/	Destination URL. Example: http://www.metering.es/json/set.asp?data=
Server Username:		Blank if no server authentication required
Server Password:		Blank if no server authentication required
Register size:	300	Register size (normally 300)
Number of Registers:	1000	Number of registers in Logger (normally 1000)

Communication mode: REMOTE FTP (JSON)

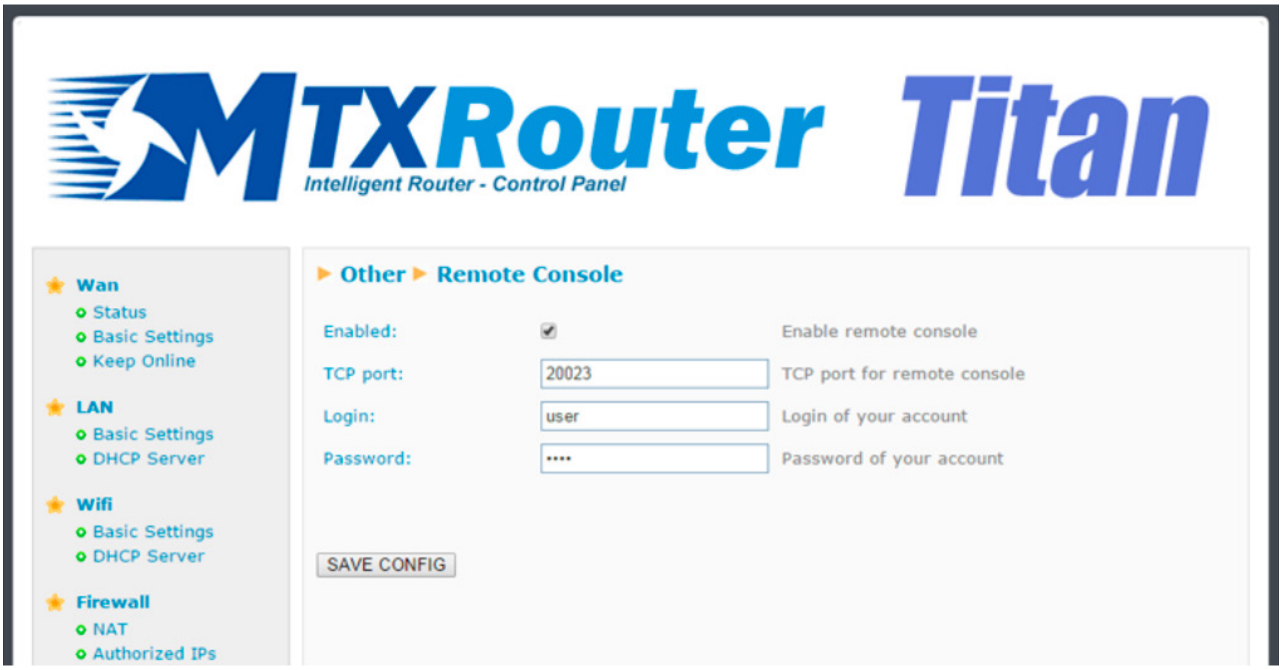
Enabled:	☑	Communication mode FTP enabled
FTP Server:	ftp.metering.es	Destination FTP Server. Example: ftp.metering.es
FTP Path:	/dev/plcs/	FTP path. Example: /dev/plcs/
FTP Username:	myUser	FTP Username
FTP Password:	myPassword	FTP Password
FTP File Period:	day ▾	FTP File Period (one file every minute, hour, day)



External Devices ▸ Generic ModBus RTU

Enabled:	☑	Enable Modbus Devices
Serial Port:	Serial Port 1	Select the connected serial port
Logger:	☑	Check if logger must be used Please, configure logger before using this option

Device name	Address	Command	Start @	Num words	Reg Type	Period	
Device 1	1	0x03	1	10	WORD	10	Delete
Device 2	2	0x03	20	1	WORD	10	Delete
Device 2b	2	0x03	30	1	WORD	10	Delete
Device 3	3	0x03	21	5	WORD	10	Delete
Device 4	4	0x03	100	6	WORD	10	Delete
Device 5	5	0x03	1	5	WORD	10	Delete
Device 5b	5	0x03	20	6	WORD	10	Delete

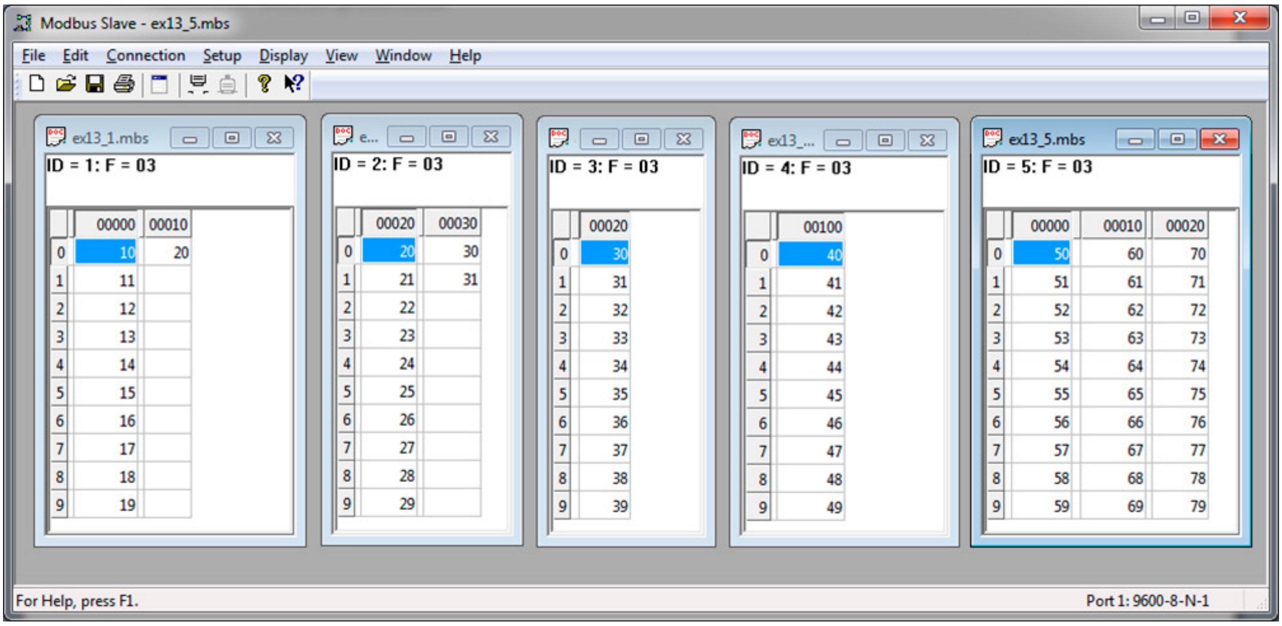


Other ▸ Remote Console

Enabled:	☑	Enable remote console
TCP port:	20023	TCP port for remote console
Login:	user	Login of your account
Password:	••••	Password of your account

Details (2):

1. To test this example, we can use a simple Slave Modbus simulator. For example, the following figure shows the creation of this example's 5 devices, with addresses 1 to 5 and the corresponding registers.


Modbus Slave - ex13_5.mbs
File Edit Connection Setup Display View Window Help
ex13_1.mbs
e...
ex13_...
ex13_5.mbs
For Help, press F1.
Port 1: 9600-8-N-1

ID = 1: F = 03

	00000	00010
0	10	20
1	11	
2	12	
3	13	
4	14	
5	15	
6	16	
7	17	
8	18	
9	19	

ID = 2: F = 03

	00020	00030
0	20	30
1	21	31
2	22	
3	23	
4	24	
5	25	
6	26	
7	27	
8	28	
9	29	

ID = 3: F = 03

	00020
0	30
1	31
2	32
3	33
4	34
5	35
6	36
7	37
8	38
9	39

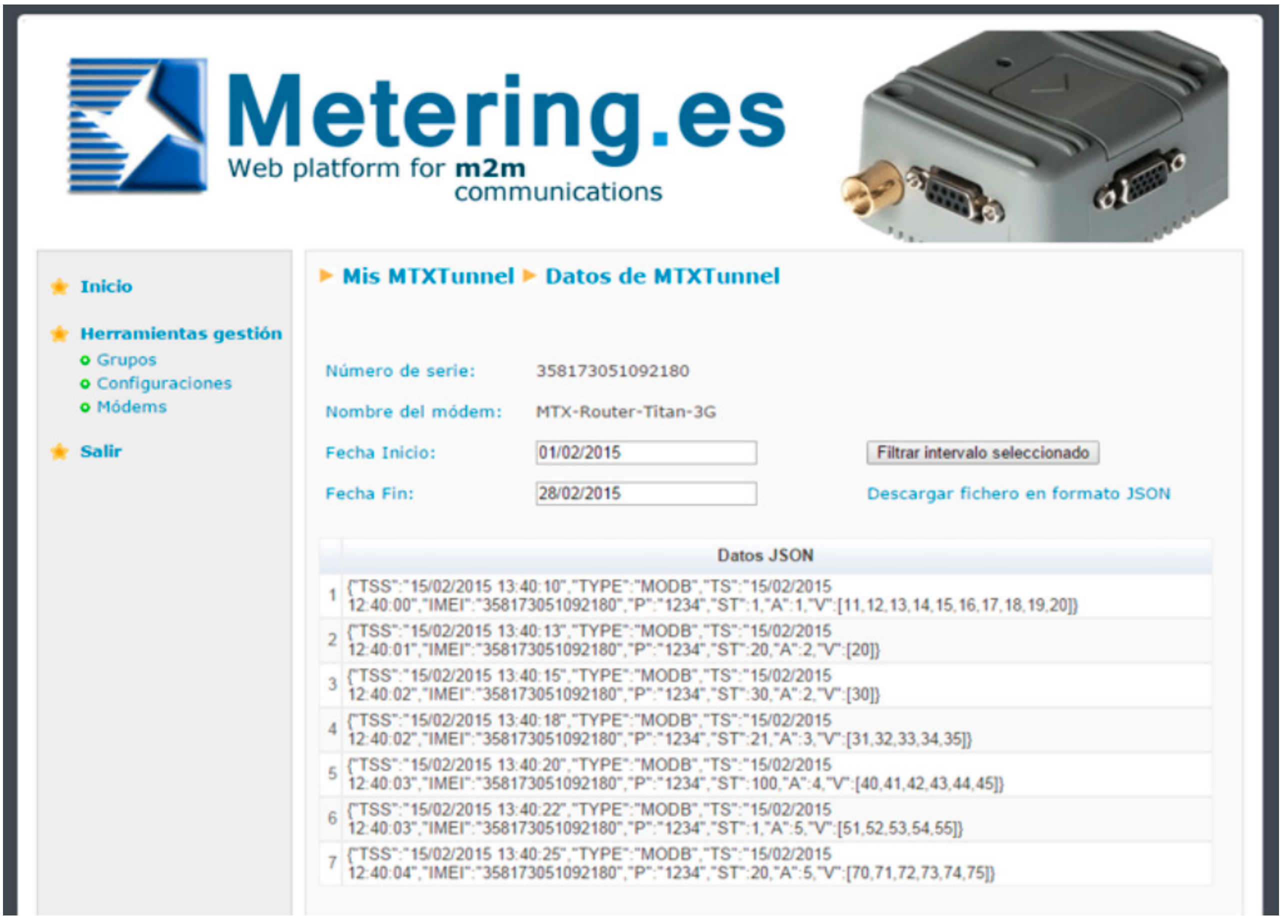
ID = 4: F = 03

	00100
0	40
1	41
2	42
3	43
4	44
5	45
6	46
7	47
8	48
9	49

ID = 5: F = 03

	00000	00010	00020
0	50	60	70
1	51	61	71
2	52	62	72
3	53	63	73
4	54	64	74
5	55	65	75
6	56	66	76
7	57	67	77
8	58	68	78
9	59	69	79

The responses read and collected by the Titan device and then sent to a Web platform (in this example, the test platform www.metering.es) will have the following format, as shown in the "External Modbus RTU" section of this manual.


Metering.es
Web platform for m2m communications
Inicio
Herramientas gestión
Grupos
Configuraciones
Módems
Salir
Mis MTXTunnel ▸ Datos de MTXTunnel
Filtrar intervalo seleccionado
Descargar fichero en formato JSON

Número de serie: 358173051092180

Nombre del módem: MTX-Router-Titan-3G

Fecha Inicio: 01/02/2015

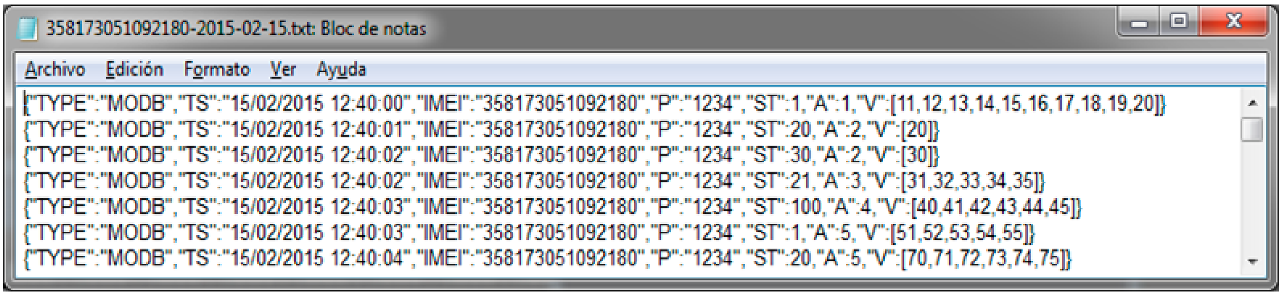
Fecha Fin: 28/02/2015

	Datos JSON
1	{"TSS":"15/02/2015 13:40:10","TYPE":"MODB","TS":"15/02/2015 12:40:00","IMEI":"358173051092180","P":"1234","ST":1,"A":1,"V":[11,12,13,14,15,16,17,18,19,20]}
2	{"TSS":"15/02/2015 13:40:13","TYPE":"MODB","TS":"15/02/2015 12:40:01","IMEI":"358173051092180","P":"1234","ST":20,"A":2,"V":[20]}
3	{"TSS":"15/02/2015 13:40:15","TYPE":"MODB","TS":"15/02/2015 12:40:02","IMEI":"358173051092180","P":"1234","ST":30,"A":2,"V":[30]}
4	{"TSS":"15/02/2015 13:40:18","TYPE":"MODB","TS":"15/02/2015 12:40:02","IMEI":"358173051092180","P":"1234","ST":21,"A":3,"V":[31,32,33,34,35]}
5	{"TSS":"15/02/2015 13:40:20","TYPE":"MODB","TS":"15/02/2015 12:40:03","IMEI":"358173051092180","P":"1234","ST":100,"A":4,"V":[40,41,42,43,44,45]}
6	{"TSS":"15/02/2015 13:40:22","TYPE":"MODB","TS":"15/02/2015 12:40:03","IMEI":"358173051092180","P":"1234","ST":1,"A":5,"V":[51,52,53,54,55]}
7	{"TSS":"15/02/2015 13:40:25","TYPE":"MODB","TS":"15/02/2015 12:40:04","IMEI":"358173051092180","P":"1234","ST":20,"A":5,"V":[70,71,72,73,74,75]}

Regarding the FTP – having selected one file per day, a file with the name:

358173051092180-2015-02-15.txt (IMEI-year-month-day.txt)

will be created in the remote FTP server, and the following content shown below (the previous JSON registers, grouped together in an easy-to-mange.txt file).

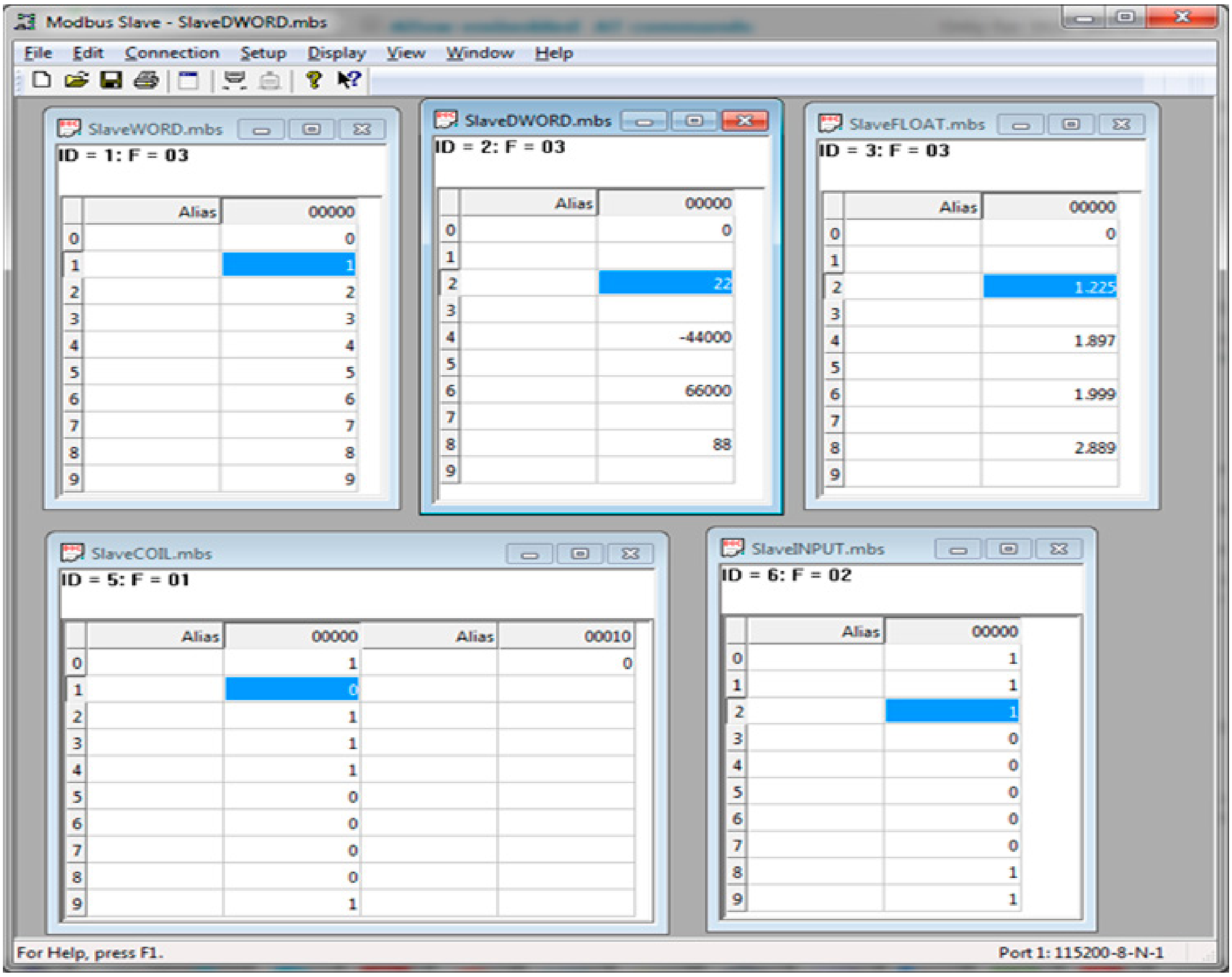


```
{"TYPE":"MODB","TS":"15/02/2015 12:40:00","IMEI":"358173051092180","P":"1234","ST":1,"A":1,"V":[11,12,13,14,15,16,17,18,19,20]}
{"TYPE":"MODB","TS":"15/02/2015 12:40:01","IMEI":"358173051092180","P":"1234","ST":20,"A":2,"V":[20]}
{"TYPE":"MODB","TS":"15/02/2015 12:40:02","IMEI":"358173051092180","P":"1234","ST":30,"A":2,"V":[30]}
{"TYPE":"MODB","TS":"15/02/2015 12:40:02","IMEI":"358173051092180","P":"1234","ST":21,"A":3,"V":[31,32,33,34,35]}
{"TYPE":"MODB","TS":"15/02/2015 12:40:03","IMEI":"358173051092180","P":"1234","ST":100,"A":4,"V":[40,41,42,43,44,45]}
{"TYPE":"MODB","TS":"15/02/2015 12:40:03","IMEI":"358173051092180","P":"1234","ST":1,"A":5,"V":[51,52,53,54,55]}
{"TYPE":"MODB","TS":"15/02/2015 12:40:04","IMEI":"358173051092180","P":"1234","ST":20,"A":5,"V":[70,71,72,73,74,75]}
```

Details (3):

For firmware versions up to 1.07, Titan routers can read data types UNSIGNED WORD (2 bytes). For versions 1.08 or later, they can also read data types DOUBLE WORD (4 bytes), FLOAT (4 bytes), COIL (1 bit) and INPUTS (1 bit).

For example, we can configure the emulator with five Modbus slaves, each of which with a different data types.



SlaveWORD.mbs

ID = 1: F = 03

	Alias	00000
0		0
1		1
2		2
3		3
4		4
5		5
6		6
7		7
8		8
9		9

SlaveDWORD.mbs

ID = 2: F = 03

	Alias	00000
0		0
1		
2		22
3		
4		-44000
5		
6		66000
7		
8		88
9		

SlaveFLOAT.mbs

ID = 3: F = 03

	Alias	00000
0		0
1		
2		1.225
3		
4		1.897
5		
6		1.999
7		
8		2.889
9		

SlaveCOIL.mbs

ID = 5: F = 01

	Alias	00000	Alias	00010
0		1		0
1		0		
2		1		
3		1		
4		1		
5		0		
6		0		
7		0		
8		0		
9		1		

SlaveINPUT.mbs

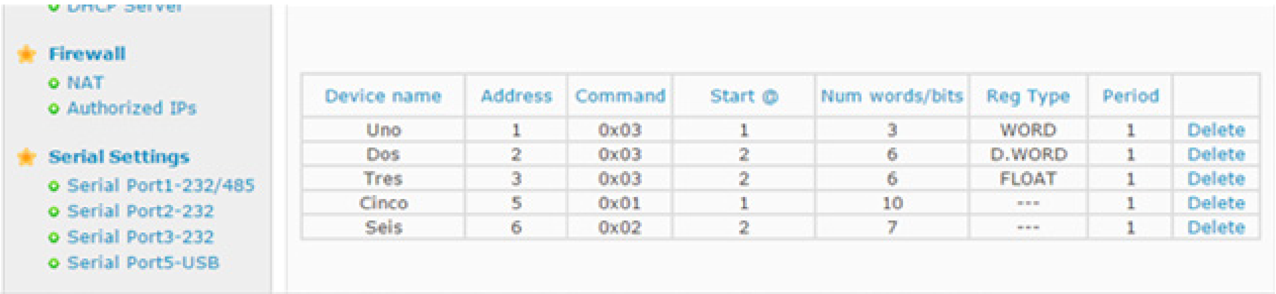
ID = 6: F = 02

	Alias	00000
0		1
1		1
2		1
3		0
4		0
5		0
6		0
7		0
8		1
9		1

For Help, press F1.

Port 1: 115200-8-N-1

If we wish to read registers 1, 2 and 3 from device @1 (SlaveWORD), registers 2, 4 and 6 from device @2 (SlaveDWORD), and registers 2, 4 and 6 from device @3 (SlaveFLOAT), as well as 10 bits, starting from bit 1, from device @5 (SlaveCOIL) and 7 bits, starting from bit 2, from device @6 (INPUTS), the configuration would be as follows:



Device name	Address	Command	Start @	Num words/bits	Reg Type	Period	
Uno	1	0x03	1	3	WORD	1	Delete
Dos	2	0x03	2	6	D.WORD	1	Delete
Tres	3	0x03	2	6	FLOAT	1	Delete
Cinco	5	0x01	1	10	---	1	Delete
Seis	6	0x02	2	7	---	1	Delete

RELEASE NOTES OF FIRMWARE VERSIONS

V1.01

- First version of the firmware

V1.02

- Improvements in the backup configuration section
- Improvements in the NAT. It allows NAT in the TCP port 80 (HTTP)
- The Internet blocking option is added to WiFi devices and option blocking for devices connected to the Ethernet port in WiFi devices
- New examples added in the configuration section

V1.03

- The temporary client option is added for when a 3G-RS232/485 gateway is created
- New firewall options. The IP filter for access to the configuration interface, 3G/Serial gateways, remote consoles and NAT is added
- Improvements in the changing of relays via SMS
- Allows an access port to the router's web configuration interfaces from the WAN interface (3G). This means that a different port can be specified, which allows NAT to be carried out from the TCP port 80 to internal devices that use this port

V1.04

- Allows the WiFi channel to be chosen to improve performance depending on location
- Sending data via FTP is added as an option to the logger
- Improvements in the IP-Serial gateway performance

V1.05

- Use of the Hardware watchdog is included
- New pre-installed examples in the web configuration environment
- GSM data calls (CSD) can be received for GSM/RS232-485 gateways with preference over IP

V1.06

- Digital input added to control the alarm for the Titan mini device
- The option of RS485, as well as RS232, for serial port 1 is added
- The AT^MTXTUNNEL=GETMODBUS and AT^MTXTUNNEL =SETMODBUS commands are added to read and write Modbus registers via AT commands
- Jamming detection added, allowing for the detection of possible intrusion using GSM inhibitors. At the moment, Jamming detection is only available for GSM/GPRS networks

V1.07

- The status of the digital entry is shown in the webserver
- More examples are included
- Wavenis and Wavetherm (temperature radio sensors) devices added
- Added characteristic to allow the device to act as a Modbus TCP Slave, through which the firmware version, GSM coverage, etc. can be read

V1.08

- Embedded AT Commands included in the IP-Serial gateways
- Generic AT commands can be send to the router via Modbus TCP protocol

V1.09

- FTDI and ACM connections to USB devices permitted

V1.10

- Added control to the internal GPS module in the MTX-Router-Titan-3G device
- Added possibility of sending emails either by AT command from external devices or automatically using Titan Scripts
- Improvements in the Logger to be able to send data to third party platforms (GroveStreams, for example)

V1.11

- Improvements in the periodic autoreset
- SNMP protocol incorporated
- Possibility of creating a second digital input in the MTX-Router-Titan mini device
- Added characteristic of a pulse counter for metering applications

V1.12

- OpenVPN service in client and server mode incorporated
- “WiFi Client” mode added (as well as the existing WiFi access point)

V1.13

- DHCP incorporated for WiFi client mode
- New relay control by astronomical clock option
- New relay control by GPS cell position option
- Alarms (SMS, calls and relays) upon the detection of movement in the router via an internal inclinometer

V1.14

- Option of receiving SMS message via Modbus TCP
- Improvements in Titan Scripts
- Improvements in firewall allowing specific IP addresses to be authorized

V2.00

- Improvements in OpenVPN (faster speeds)

V2.01

- “No-NAT” plug-in included
- Improvements in Titan Scripts (new commands)

V2.02

- New MTX-Router-Titan models (only ETH and Wi Fi), as well as new MTX-Router-Titan mini models (only ETH and Wi Fi); i.e. new devices without the GSM communication module.
- Improvements in Titan Scripts, supporting Modbus TCP

V2.03

- Improvements in NTP time servers

V2.05

- Support for the new MTX-Router-Titan-3G-mini-GPS device
- New “Watchdog” plug-in, allowing pings to be carried out to external devices that change an internal relay when a response is not received in order to reset the device

V3.00.3.0

- New firmware version format (v3.xx.3.xx)
- Improvements in the time format. New time zones added, allowing a different zone to UTC (the current option)
- Support for the 4G model (MTX-Router-Titan-4G-mini-GPS)
- Improvements in the Modbus Slave support (up to 5 simultaneous connections)
- Reading and datalogging for Modbus RTU devices allowed, incorporating support for Modbus TCP devices

V3.00.3.02

- Introduction to alias for SMS commands (Other > SMS control)
- Serial device datalogger. The Titan router allows data that is received through one of its serial ports or USB ports to be collected, stored and sent (via HTTP or FTP)

V3.00.3.03

- For greater security, the 3G/4G module (depending on the version of the Titan router) is reset after each start up by cutting the internal power supply. In this way, there is a complete guarantee that the GSM network will be reached after restarting. The process could however take a few seconds longer than normal as a result
- IP-Serial gateways can be established at the same time as an External Modbus RTU device or script. For example, the Titan router can be configured to take readings from a Modbus RTU device via a serial port as well as connect remotely to the same Modbus RTU device via a 3G-Serial gateway. When the socket is established, the readings are temporarily suspended to avoid collisions in the BUS. Once the 3G-Serial gateway is terminated, the readings are reestablished

V3.00.3.04

- NTP time servers are added for the MTX-Router-Titan (only Ethernet & Wi Fi) and MTX-Router-Titan mini (only Ethernet & Wi Fi) models (i.e. the routers without the 2G/4G communication model)
- The configuration back-up includes the plug-ins and is now encrypted

V3.00.3.05

- Improvements in the Wavenis sensor concentrator services
- New button to read the internal battery status of the Wavenis radio sensors
- New button to read the RSSI link level via boosters for the Wavenis radio sensor concentrator
- Reconfigured internal LEDs on the miniPCI card; green indicates good 3G communications; blue indicates that the router has a public IP address
- Improvements for receiving CSD calls (GSM calls). For future versions, CSD data calls made from analog modems are accepted as well as those made via GSM modems
- Improved IP-RS232 gateway speeds (multiplied by 4). Increased from 115200 bauds to 460800 bauds

V3.00.3.06

- Added a Modbus-SNMP protocol converter, including traps, allowing an SNMP network to be integrated into almost any Modbus device
- Sending of TRAPS via AT commands and Modbus TCP now available
- Sending of TRAPS from Titan Scripts now available. Application Note available for this feature

V3.00.3.07

- Increased possibilities to send the internal logger to web platforms. Now available: TCP socket, HTTP GET, HTTPS GET, HTTP PUT, HTTPS PUT and GroveStreams
- Improvements in the internal SNMP server. New, more complete MIB
- Added a timeout of 900 seconds to the IP-Serial gateways in client moode. If there is no traffic in this time, the socket is reset for secuity reasons

V3.00.3.08

- New funcionalities for IP-Serial gateways, in particular in TCP Server mode
- New funcionality for GPS enabled Titan routers, through which it is possible to open a socket to obtain NMEA frames via the Titan router as well as via the serial port. The GPS NMEA frames are updated every second

V3.00.3.09

- Improvements in the DynDNS service

V3.00.3.10

- New command AT ^ MTXTUNNEL = SETREDLED to turn on the red led by AT commands
- New command AT ^ MTXTUNNEL = GETTEMPERATUREPROC to read the processor temperature
- New command AT ^ MTXTUNNEL = GETTEMPERATUREGSM to read the temperature of the internal GSMmodule
- Backup improvements (custom header included)

V3.00.3.11

- Added: supports for temperature probe 1-Wire

V3.00.3.12

- Titan 4G enhancements related to connectivity

V3.00.3.14

- Improvements in OpenVPN. It creates utility to automatically create all the certificates
- HTTPS support for the configuration interface

V3.00.3.15

- Improvements in OpenVPN to be activated by SMS
- New OpenVPN feature EasyLink
- New command AT ^ MTXTUNNEL = GETTIME to be able to synchronize external equipment
- Improvements in SNMP. Continuous forwarding of traps is allowed until an alert has been completed

V3.00.3.16

- New TitanLink plugin, which allows we to manage up to 50 remote MTX-Tunnel
- New feature “Automatic APN”. The router is able to search the appropriate APN, username and password in a list based on the inserted SIM
- New Remote Console feature. On this occasion the option of “client mode” is added. A very interesting option to control the router centrally from a Web platform

V3.00.3.17

- New feature to convert the Router Titan into a Concentrator (data collector) W-MBus

V3.00.3.18

- New feature to block WAN PING
- Improvements in the management of plugins

V3.00.3.19

- New Modbus read commands 0x01 and 0x02
- The MW command is added to the Titan Scripts [dir, posi, value, command]
- The DI1 command for reading the digital input of the Titan mini is added to the Titan Scripts
- AES support for W-MBus devices and export of readings to CSV

V3.00.3.20

- Improvements in reading speed of remote devices W-MBus

V3.00.3.21

- New NAT_Interface option for the NAT section. The “auto” mode (the current one so far) but also the interface “Ethernet”, “WiFi” and “OpenVPN”

V3.00.3.22

- New option to send logger data. Possibility of sending data using MQTT
- Improvements in the management of incoming CSD calls

V3.00.3.23

- New option to send logger data. Possibility of sending data via HTTP POST and HTTPS POST
- Improvement in ALIAS SMS. It is possible to hide the AT command in response to an SMS command
- Improvements in the stability of the OpenVPN service when the router is configured as Client and a configuration failure occurs in the Server

V3.00.3.24

- Added the custom HTTP headers option in the OTHER> Private DNS
- SSID names (router running as WiFi AP) are supported with spaces and the titan reconnectivity is improved in case of acting as WiFi Client

V3.00.3.25

- New option of traffic control of the SIM, being able to send an SMS when it exceeds 90% of the traffic consumed or even cutting the connection once exceeded the maximum predicted
- New MQTT parameters

V3.00.3.26

- Modbusno consecutive registries can be read separated by “,”
- Titan can function as a RTU slave devide (as well as Modbus TCP slave)
- Following modbus registries added to the Titan modbus map: day, month, year, hours, minutes, seconds

V3.00.3.27

- New features to be able to use Telnet (remote console) as SSH
- New user “guest” that allows to visualize the same configuration than “user” but without permissions to make modifications
- AES128 encryption of the logger JSON data
- Ability to use MQTT in DNS
- Improvement of NTP internal services
- New logs to monitor the activity of users and services

V3.00.3.28

- SNMPv3 service added
- Tacacs+ service added (just authentication)
- New command AT^MTXTUNNEL=ROUTERON,xxx to be able to activate the Internet connection via an AT command

V3.00.3.29

- Improvement of the MQTT service. ID field added
- GPS parameters added to the Titan router modbus registry map
- Ability to activate the Internet connection by changing a digital input

V3.00.3.30

- Failover option added
- DynDNS use allowed when the Internet output is made via Ethernet or WiFi

V4.00.4.01

- Compatibility with the new MTX-Router-Titan II-S added
- Correction of a DNS problem that happened when using private range DNS in a router configuration without GSM module (just with Ethernet or WiFi)

GENERIC EMULATION SOFTWARE FOR VIRTUAL SERIAL PORTS

1. Emulation software for serial ports: VSPE

Quick quide to the emulation software for serial ports.

Introduction:

One of the most used software nowadays to emulate serial ports is VSPE. It is a free piece of software for 32 bit Windows Operating Systems and a pay service for 64 bit platforms.

Emulation software for serial ports to TCP/IP must be used if we have old software for connecting serial devices that only allows we to connect to these devices via a COM serial port. This software allows we to create virtual COMs (COM1, COM2, COM3, etc.) on our PC that, in reality, are directed to a specific IP address or TCP port.

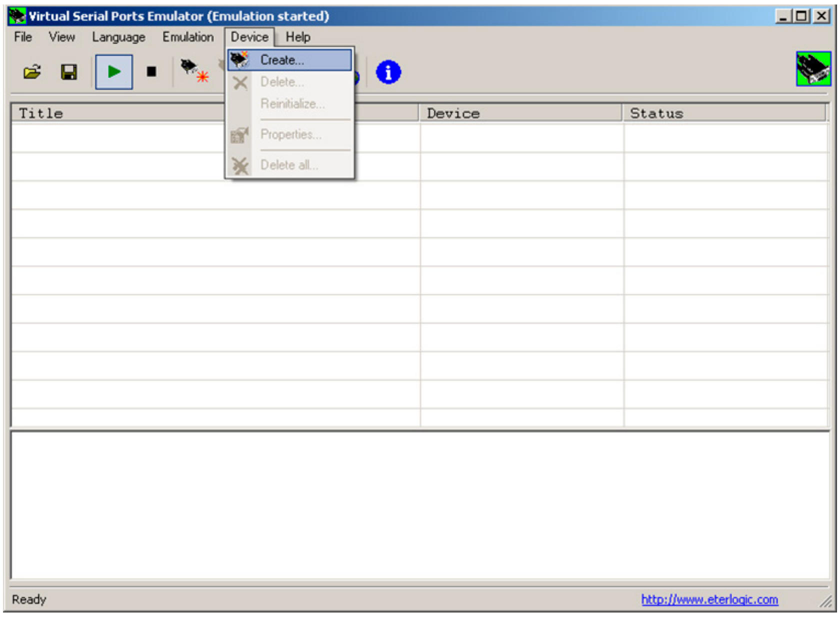
We can download the software from the following link:

http://www.eterlogic.com/downloads/SetupVSPE.zip

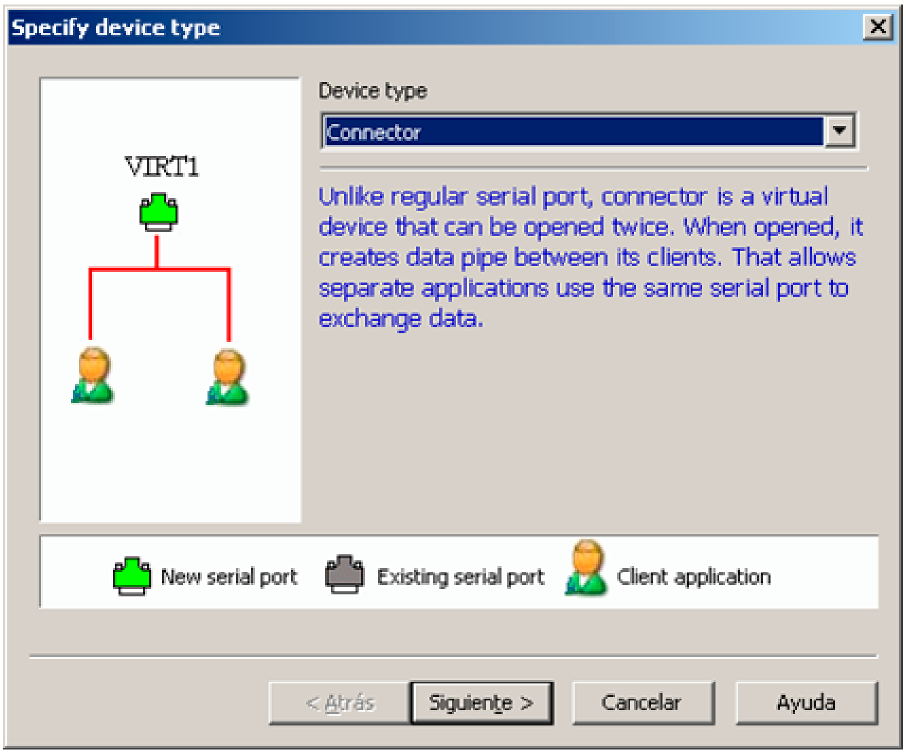
Usage example:

The following steps show how to configure a virtual COM port that directs to a specific IP address or TCP port.

- Menu: Device > Create



- Select the option “Connector”



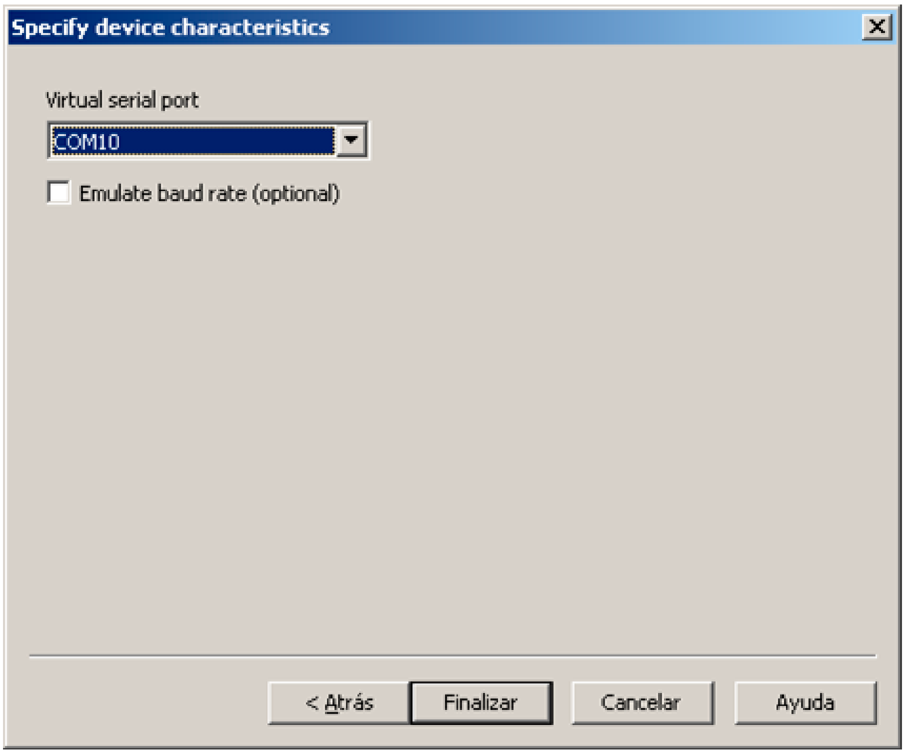
Specify device type

Device type

Connector

Unlike regular serial port, connector is a virtual device that can be opened twice. When opened, it creates data pipe between its clients. That allows separate applications use the same serial port to exchange data.

- Select the number of the virtual COM that we want to use. For example, COM10



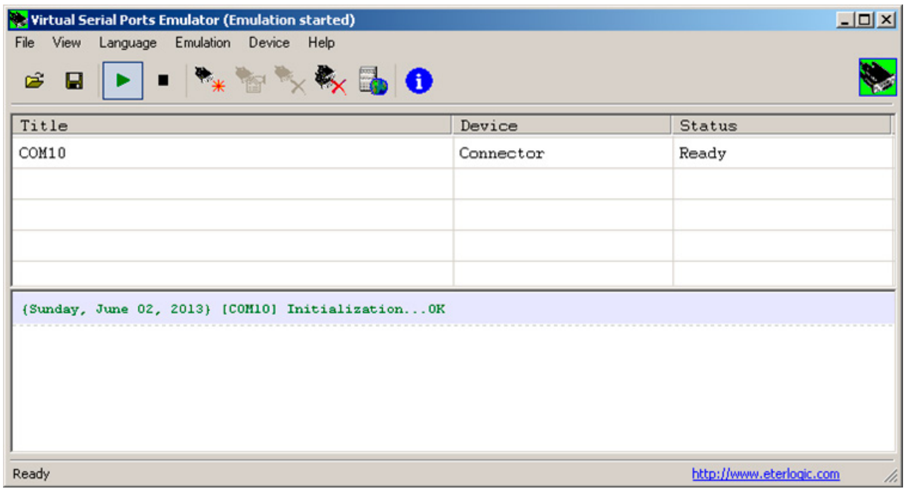
Specify device characteristics

Virtual serial port

COM10

□ Emulate baud rate (optional)

- Click Finish. The virtual COM that has been created will appear in the list

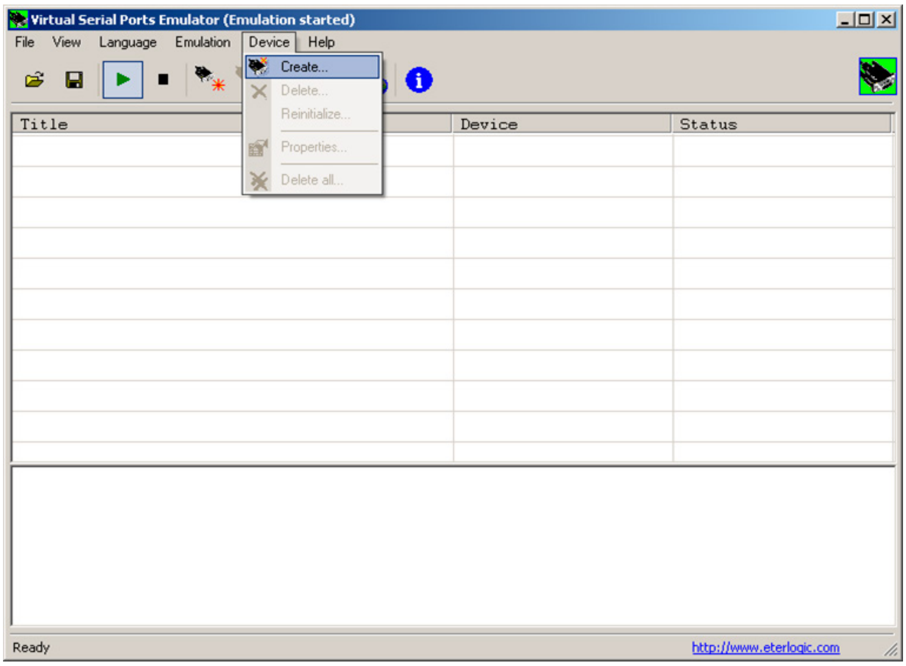

Virtual Serial Ports Emulator (Emulation started)
File View Language Emulation Device Help

Title	Device	Status
COM10	Connector	Ready

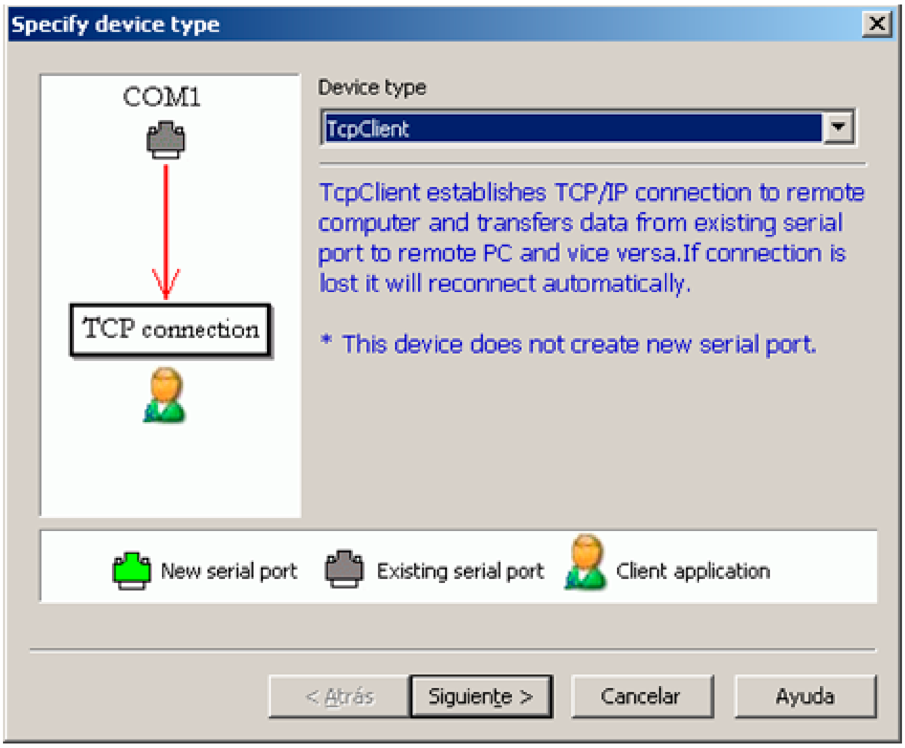
```
(Sunday, June 02, 2013) [COM10] Initialization...OK
```

Ready
http://www.eterlogic.com

- Return to the menu: Device > Create



- Select the option TCPClient from the drop-down menu



Device type: TcpClient

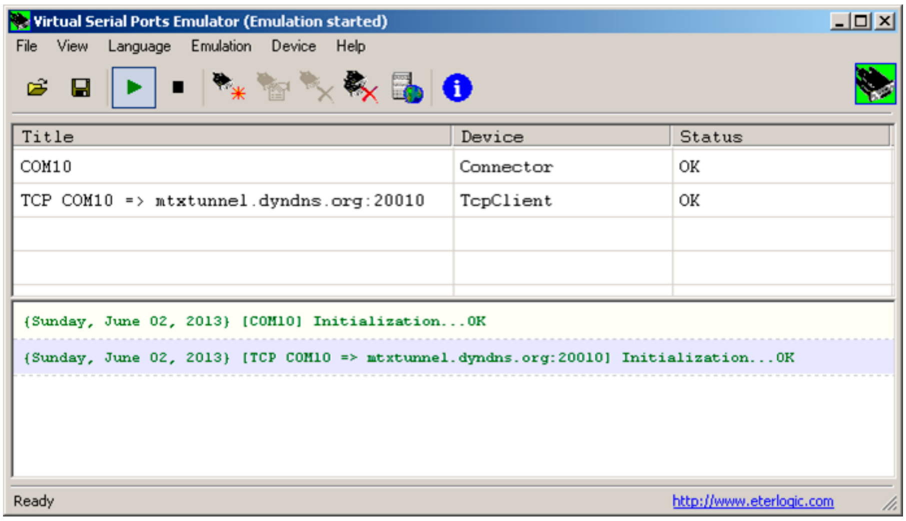
TcpClient establishes TCP/IP connection to remote computer and transfers data from existing serial port to remote PC and vice versa.If connection is lost it will reconnect automatically.

* This device does not create new serial port.

- On the following screen, we indicate the remote IP address of our MTX device. We can input a numeric IP (if we use a SIM with fixed IP address, or because we have obtained the current IP address via SMS or missed call), or a DNS (if we use the DynDNS service).

  We also select the TCP port that the MTX is listening in (20010 by default). Finally, we select the virtual COM port that we have previously created. In this example, it would be COM10.

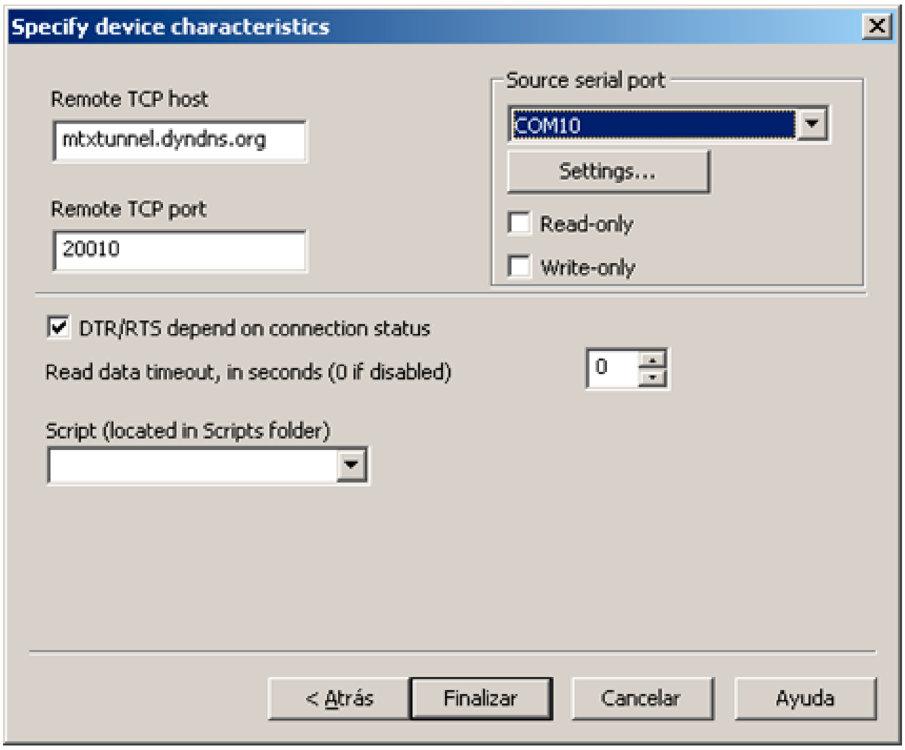
  Click “Finish”



Title	Device	Status
COM10	Connector	OK
TCP COM10 => mtxtunnel.dyndns.org:20010	TcpClient	OK

```
{Sunday, June 02, 2013} [COM10] Initialization...OK
{Sunday, June 02, 2013} [TCP COM10 => mtxtunnel.dyndns.org:20010] Initialization...OK
```

- Now we have the COM10 port connected to our MTX device



Specify device characteristics

Remote TCP host: mtxtunnel.dyndns.org

Remote TCP port: 20010

Source serial port: COM10

☐ Read-only

☐ Write-only

☑ DTR/RTS depend on connection status

Read data timeout, in seconds (0 if disabled): 0

Script (located in Scripts folder):

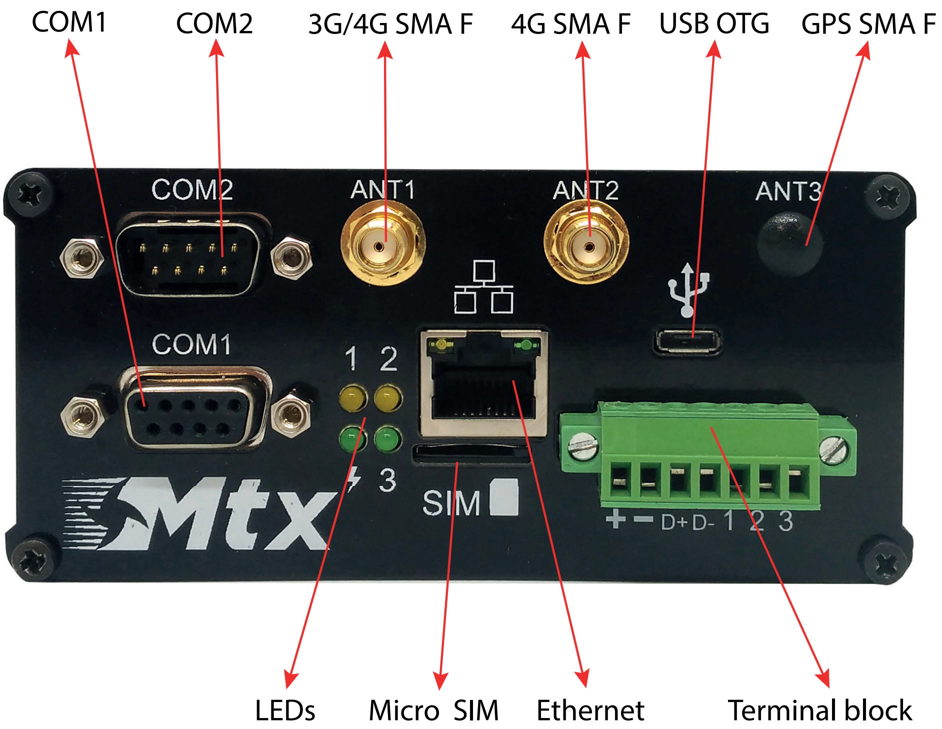
- The last step is to access our control application and select the COM10 port as the communication port. Now we can remotely access our serial devices. Remember that the modem's serial port configuration (bauds, data bits, etc.) must be established in the "config.txt" file as explained in this manual

HARDWARE

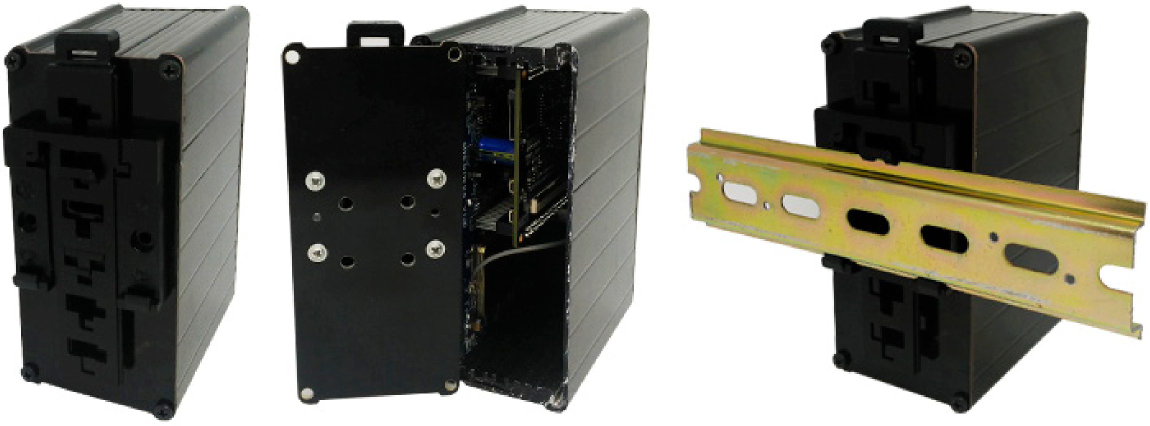
1. Quick guide to the MTX-Router-Titan II-S

Introduction:

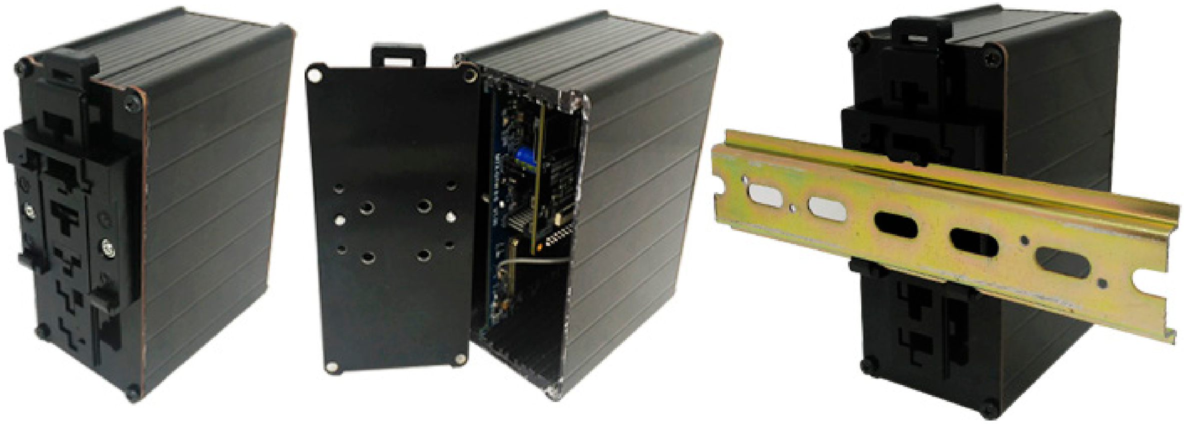
Below we see a basic connection diagram showing the MTX-Router-Titan II-S device's connection terminals. VCC can have a value between 9 and 30Vdc. The power supply needs to allow 1.5A consumption peaks.



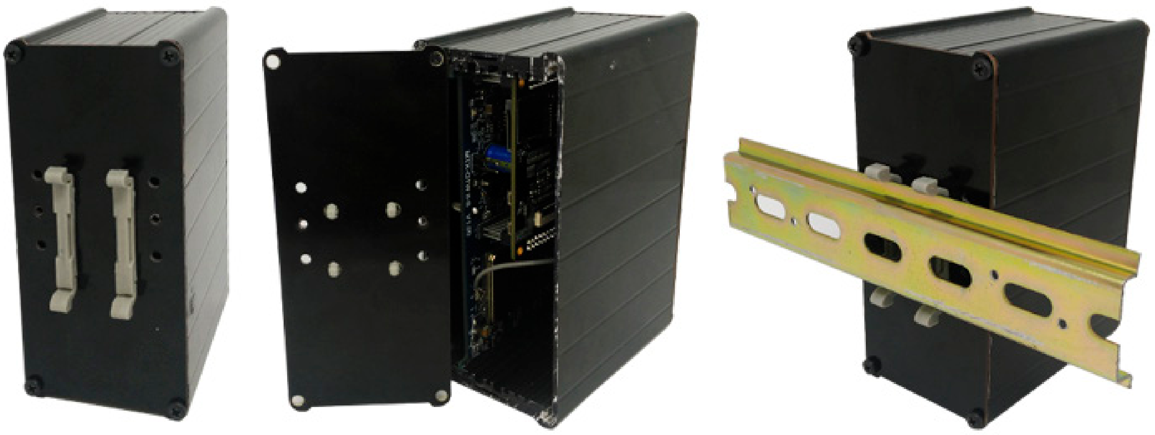
DIN rail with four screws:



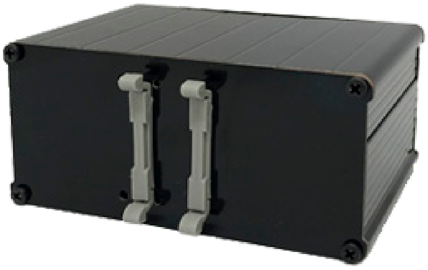
DIN rail with two screws:

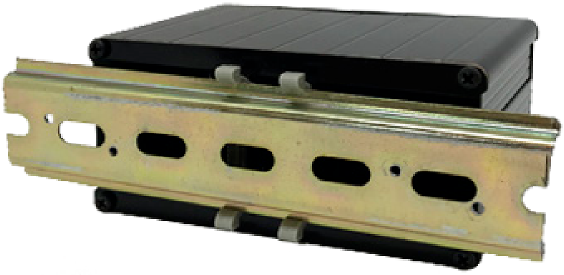


DIN rail with clip handles:



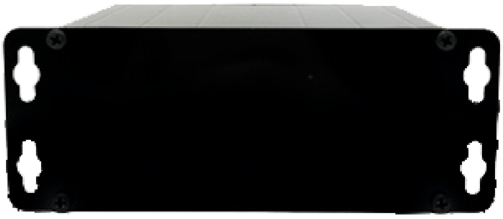
DIN rail with plastic clip horizontal:

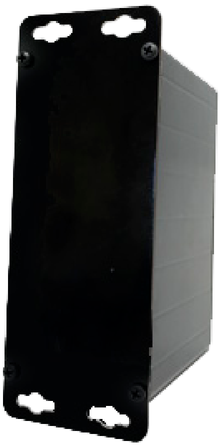




Wall mount:

MTX-T ACC wall mounting plate (Titan II/GTW II/BGS2T): 000427108





In the following table, the available connections in the MTX-Router-Titan II-S's terminal block connector are shown:

TERMINAL BLOCK	USE
1	VCC
2	GND
3	RS485_D+
4	RS485_D-
5	Digital input 1
6	Digital input 2
7	Digital input 3 (for default config)

- To activate a digital input we need to connect it to GND (dry contact). Activating a digital input the Titan will read "1 lógico). Without activating a digital input the Titan will read a "0" logic
- The third digital input should be used only when we need to reestablish the router default parameters, as this user guide explains on the section 2.7.13

Packaging:

Individual box: 5.5cm high x 12cm wide x 16cm long, 0.390Kg

60 boxes: 55cm high x 35cm wide x 35cm long. 25Kg

MTX-ROUTER-TITAN II-S

	MTX-ROUTER-TITAN II-S 4G	MTX-ROUTER-TITAN II-S 3G
	EUROPE: Penta-Band LTE: Bands 1, 3, 8, 20, 28* (700*, 800, 900, 1800, 2100 MHz), Dual-Band GSM 900 & 1800 MHz **US**: Quad-Band LTE: Bands 2, 4, 5, 12 (700, 850, 1700/2100 (AWS) & 1900 MHz), Tri-Band UMTS: Bands 5, 4, 2 (WCDMA/FDD 850, 1700/2100 (AWS) & 1900 MHz)	WORLDWIDE: Five Bands UMTS (WCDMA/FDD); Bands: 800, 850, 900, 1900 & 2100 MHz. Quad-Band GSM; Bands: 850, 900, 1800 & 1900 MHz
4G	LTE Cat.1 (3GPP Release 9): DL 10.2Mbps, UL 5.2Mbps	
3G		HSDPA Cat.8/HSUPA Cat.6 data rates: DL max. 7.2 Mbps, UL max. 5.76 Mbps
2G	GPRS Class 12: DL max. 85.6 kbps, UL max 85.6 kbps	EDGE Class 12 data rates: DL max. 237 kbps, UL max. 237 kbps GPRS Class 12 data rates: DL max. 85.6 kbps, UL max. 85.6 kbps
CSD		CSD data transmission up to 9.6 kbps, V.110, non-transparent
SMS	SMS text and PDU mode	SMS text and PDU mode

Interfaces

Ethernet 10/100 BaseT (RJ45 connector)

USB 2.0 (micro AB connector), 2x RS232 DB9M connectors, RS485 terminal block

Operating LEDs

Micro SIM card interface 1.8V/3V

Power supply (2-way plug-in terminal block)

SMA radio connectors 4G/3G/2G

WiFi 802.11 b/g/n (SMA-F RP)

Pa

Customization

Externals: temperature, distance, any Modbus RTU/TCP device

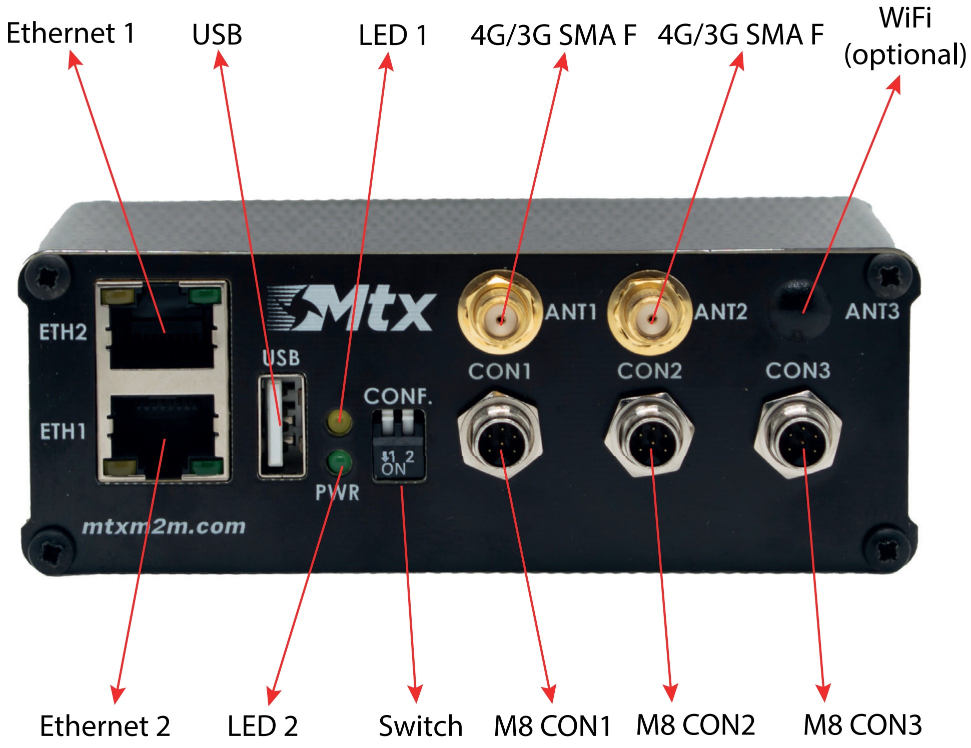
Compatible with Wavenis RF sensors using an internal wavecard (optional module)

GPS (optional module)

2. Quick guide to the MTX-Router-Titan II-R

Introduction:

Below we see a basic connection diagram showing the MTX-Router-Titan II-R device's connection terminals. VCC can have a value between 9 and 36Vdc.



In the following table, the available connections in the MTX-Router-Titan II-R's M8 connectors are shown:

M8	CON1	CON2	CON3
1	CAN0_P	CAN1_P	RS232_RTS1
2	CAN0_N	CAN1_N	RS232_CTS1
3	VIN+	-	-
4	VIN-	GND	GND
5	RS485_A	RS232_TX0	RS232_TX1
6	RS485_B	RS232_RX0	RS232_RX1

MTX-ROUTER-TITAN II-R

	OPTIONAL miniPCIe SPECIFICATIONS	
	MTX-ROUTER-TITAN II-R 4G	MTX-ROUTER-TITAN II-R 3G
	Penta-Band LTE: Bands 1, 3, 8, 20, 28* (700*, 800, 900, 1800, 2100 MHz), Dual-Band GSM 900 & 1800 MHz	UMTS/HSPA+: five band (800, 850, 900, 1900, 2100MHz), GSM/GPRS/EDGE quad band (850, 900, 1800, 1900MHz)
4G	LTE Cat.1 (3GPP Release 9): DL 10.2Mbps, UL 5.2Mbps	
3G	HSPA: DL 7.2Mbps, UL 5.7Mbps UMTS PS: DL 384Mbps, UL 384 Mbps, CS: DL 64Mbps, UL 64Mbps	HSPA (3GPP release 6, 7): DL 7.2Mbps, UL 5.7Mbps; HSDPA Cat.8/HSUPA Cat.6 data rates; compressed mode (CM) according to 3GPP TS25.212 UMTS (3GPP release 4): PS data rate 384kbps DL, UL 384kbps; CS data rate 64kbps DL, UL 64kbps
2G	GPRS Class 12: DL max. 85.6 kbps, UL max 85.6 kbps	GPRS: GPRS class 12; mobile station class B; PBCCH support; coding schemes CS 1-4 EGPRS: multislot class 12; EDGE E2 power class for 8PSK
CSD		CSD data transmission: up to 9.6kbps; V.110; non-transparent mode
SMS	SMS text and PDU mode	SMS text and PDU mode

Interfaces

- 4G/3G/2G connectivity (optional)
- 2x Ethernet 10/100 BaseT
- USB 2.0 OTG
- 2x RS232
- 1x RS485
- 2x operating LEDs
- WiFi 802.11 b/g/n (optional)
- Rail DIN
- Rugged connectors
- SIM card interface 1.8/3V
- 2x configuration switches
- Mini PCIe
- GPS (optional)

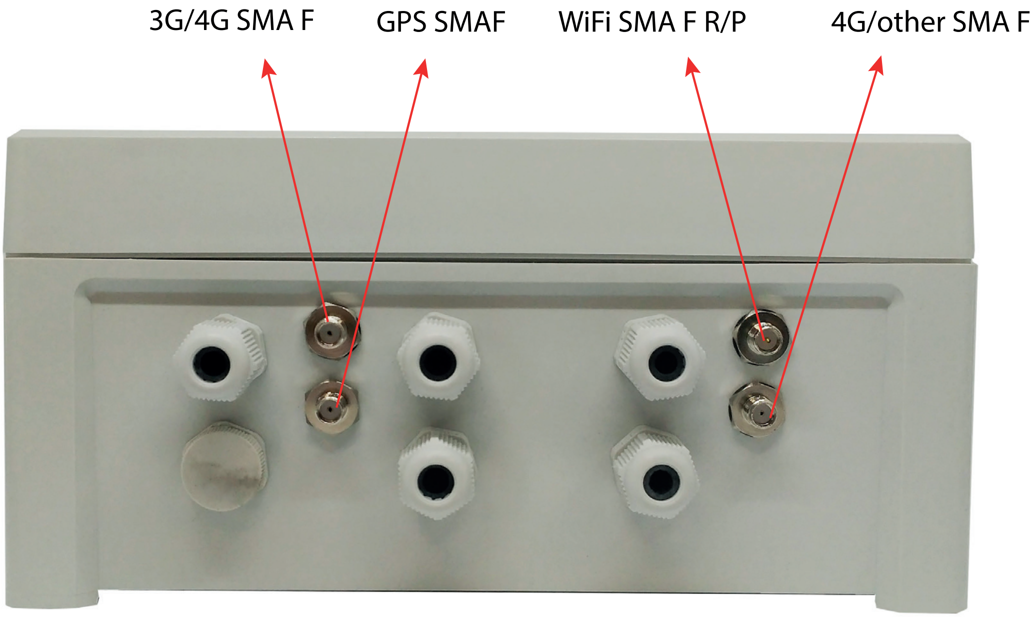
Connectors

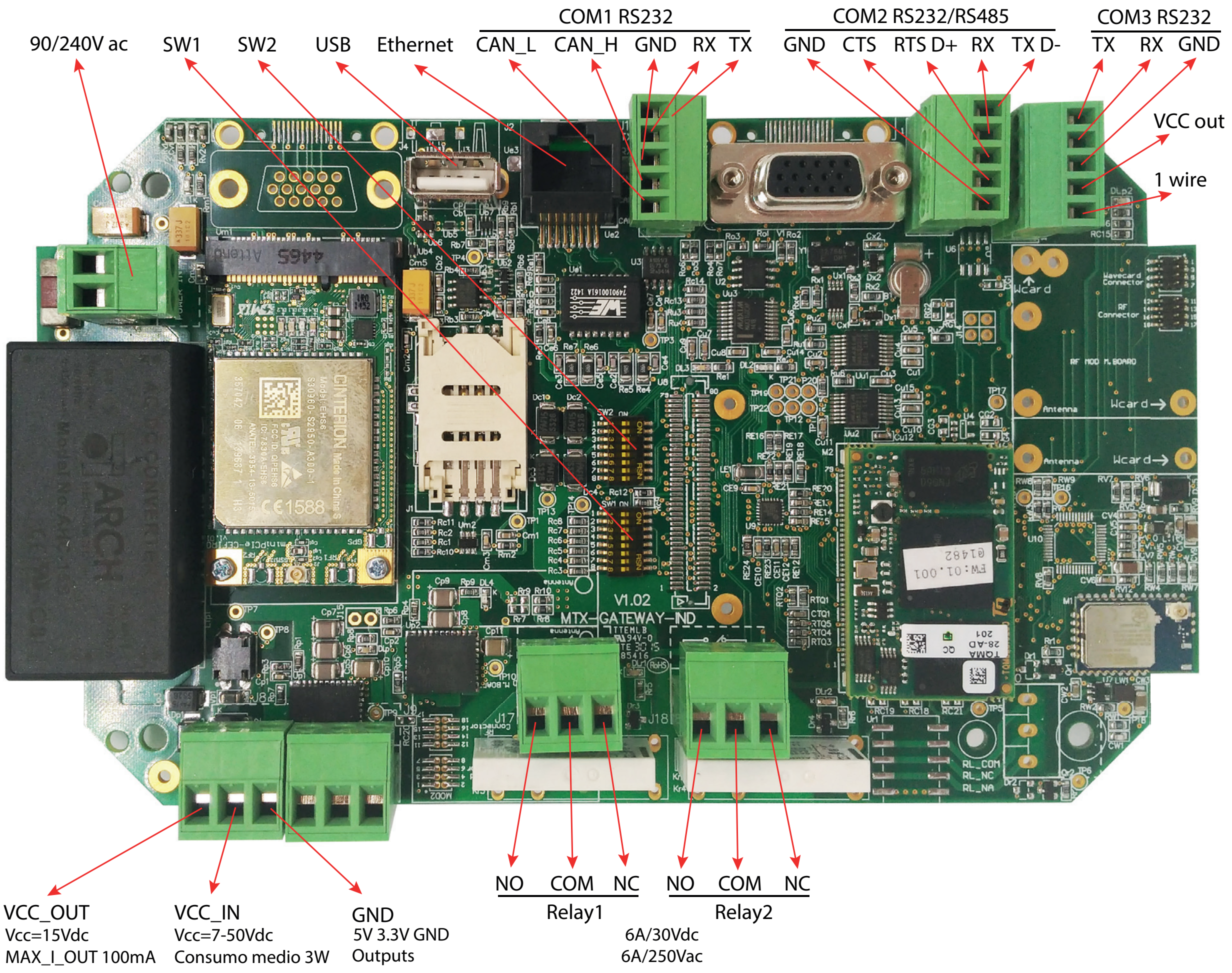
- 2x RJ45: Ethernet 10/100 BaseT
- USB A-type: USB 2.0
- 3x M8 6 pins rugged connectos: 2x RS232, 1x RS485, 2x CAN, power supply
- Micro SIM
- 3x SMA F antenna connectors: 2x 4G/3G, 1x WiFi (optional)

3. Quick guide to the MTX-Router-Titan

Introduction:

Below we will see a basic connection diagram showing the MTX-Router-Titan device's connection terminals. Note that we can power the router with both alternating voltage (90-240VaC) or direct voltage (7-50Vdc).




90/240V ac
SW1
SW2
USB
Ethernet
COM1 RS232
CAN_L
CAN_H
GND
RX
TX
COM2 RS232/RS485
GND
CTS
RTS D+
RX
TX D-
COM3 RS232
TX
RX
GND
VCC out
1 wire
VCC_OUT
Vcc=15Vdc
MAX_I_OUT 100mA
VCC_IN
Vcc=7-50Vdc
Consumo medio 3W
GND
5V 3.3V GND
Outputs
NO
COM
NC
Relay1
NO
COM
NC
Relay2
6A/30Vdc
6A/250Vac

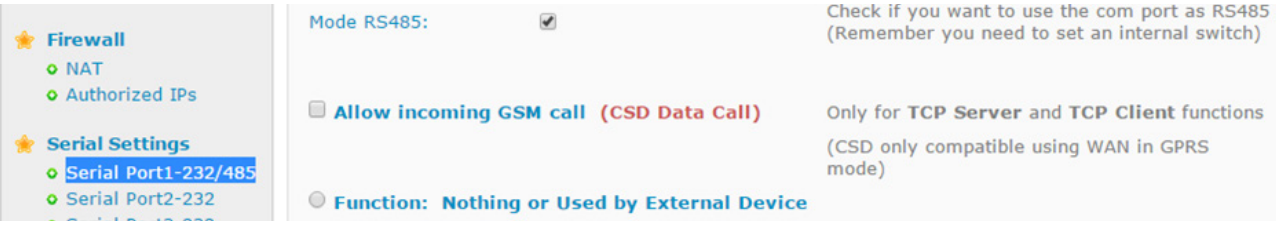
In the following table, the available connections in the MTX-Router-Titan's internal DB15 connector are shown:

FEMALE DB15	USE
1	CANH
2	COM1__RX
3	COM1__TX/RS485_- (*1)
4	COM3__TX
5	1-WIRE BUS
6	CANL
7	COM1__RTS/RS485_D+
8	COM1__CTS
9	COM3__RX
10	VCC_OUT (*2)
11	RELAY1_COM
12	COM2__TX
13	COM2__RX/DIGITAL__INPUT (*.3)
14	GND
15	RELAY1__NA

(*1) The COM1 port can be configured as an RS232 or RS485 port. By default it is configured as an RS232 port. To change this to an RS485 port, we must:

1. Place switches 3 and 4 to the ON position

2. Specify "RS485" in the environment configuration



Mode RS485: ☑ Check if you want to use the com port as RS485 (Remember you need to set an internal switch)

□ **Allow incoming GSM call (CSD Data Call)** Only for **TCP Server** and **TCP Client** functions (CSD only compatible using WAN in GPRS mode)

○ **Function: Nothing or Used by External Device**

(*2) The Titan mini device has an output (VCC_OUT, PIN_10) that can be configured to a 3.3V or 5V output.

(*3) The Titan mini device has a digital input that is shared with the RX pin belonging to the COM2 port. As a result, if we wish to use the digital input, we cannot use the COM2 port, and vice versa. TO use the digital input, ensure that switch 5 is in the ON position. The digital input will change status if PIN_13 is disconnected (in which case it will read a value of “0”), or connected to PIN_10 (in which case it will read a value of “1”).

MTX-ROUTER-TITAN

	MTX-ROUTER-TITAN 4G	MTX-ROUTER-TITAN 3G
	EUROPE: Penta Band LTE: 800/900/1800 /2100/2600 MHz; FDD-Band (20,8,3,7,1); Tri Band UMTS (WCDMA): 900/1800/2100 MHz; FDD-Band (8,3,1); Dual Band GSM/GPRS/ EDGE: 900/1800 MHz **US**: Quad Band LTE: 700/850/AWS (1700/2100)/1900 MHz; FDD-Band (17,5,4,2); Tri Band UMTS (WCDMA): 850/ AWS (1700/2100)/1900 MHz; FDD-Band (5,4,2); Quad Band GSM/GPRS/EDGE: 850/900/1800/1900 MHz)	WORLDWIDE: Five Bands UMTS (WCDMA/FDD); Bands: 800, 850, 900, 1900 & 2100 MHz. Quad-Band GSM; Bands: 850, 900, 1800 & 1900 MHz
4G	LTE Cat. 3: DL max. 100 Mbps, UL max. 50 Mbps, 2x2 DL MIMO	
3G	HSPA+ DL Cat.24 / UL Cat. 6, Dual Carrier: DL max. 42 Mbps, UL max. 5.76 Mbps	HSDPA Cat.8 / HSUPA Cat.6 data rates: DL max. 7.2 Mbps, UL max. 5.76 Mbps
2G	EDGE Class 12 data rates: DL max. 237 kbps, UL max. 237 kbps GPRS Class 12 data rates: DL max. 85.6 kbps, UL max. 85.6 kbps	EDGE Class 12 data rates: DL max. 237 kbps, UL max. 237 kbps GPRS Class 12 data rates: DL max. 85.6 kbps, UL max. 85.6 kbps
		CSD data transmission up to 9.6 kbps, V.110, non-transparent
SMS	SMS text messages	SMS text messages

Features and Interfaces

- IP65 enclosure
- Ethernet 10/100 BaseT (RJ45 connector)
- USB 2.0 (micro AB connector), RS232 2-wire and 4-wire, RS485, digital input
- Out 3.3V, 5V, 24V
- Relay with plug-in type terminal blocks: 2x 8A/250VAC relays
- 2 operating LEDs
- SIM card interface 1.8V/3V
- Power supply (internal terminal block)
- WiFi 802.11 b/g/n (SMA-F RP)
- SMA antenna connectors 4G/3G/2G

Customization

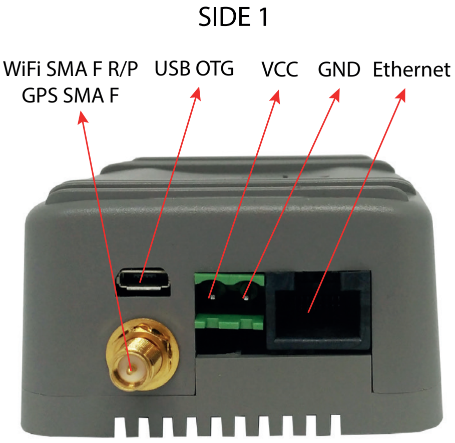
- Externals: temperature, distance, any Modbus RTU/TCP device
- Compatible with Wavenis RF sensors using an internal wavecard (optional module)
- GPS (optional module)

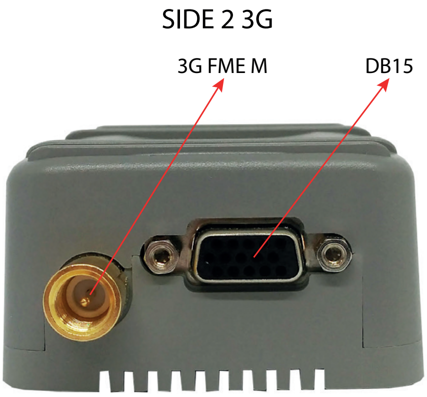
4. Quick guide to the MTX-Router-Titan mini

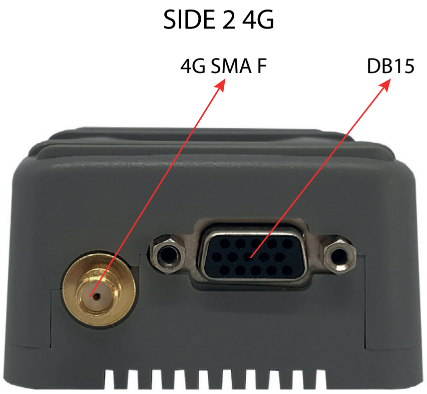
Introduction:

Below we will see a basic connection diagram showing the MTX-Router-Titan device's connection terminals. VCC can have a value between 7 and 50Vdc. Maximum device power consumption depends on different conditions and should be obtained on field. Some of the parameters that can increase the power consumption are:

- GSM status (Upload/Download/Idle) used band (2G,3G,4G) and signal quality
- WiFi status, mode (AP, managed..) and signal quality
- USB external devices connected
- DB9 external devices connected (as they can be supplied directly from the MTX)







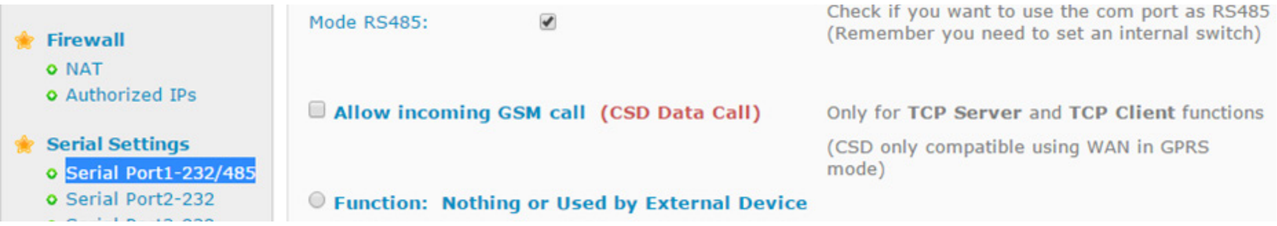
In the following table, the available connections in the MTX-Router-Titan mini's DB15 connector are shown:

FEMALE DB15	USE
1	CANH
2	COM1__RX
3	COM1__TX/RS485_- (*1)
4	COM3__TX
5	1-WIRE BUS
6	CANL
7	COM1__RTS/RS485_D+
8	COM1__CTS
9	COM3__RX
10	VCC_OUT (*2)
11	RELAY1_COM
12	COM2__TX
13	COM2__RX/DIGITAL__INPUT (*·3)
14	GND
15	RELAY1__NA

(*1) The COM1 port can be configured as an RS232 or RS485 port. By default it is configured as an RS232 port. To change this to an RS485 port, we must:

1. Place switches 3 and 4 to the ON position

2. Specify "RS485" in the environment configuration



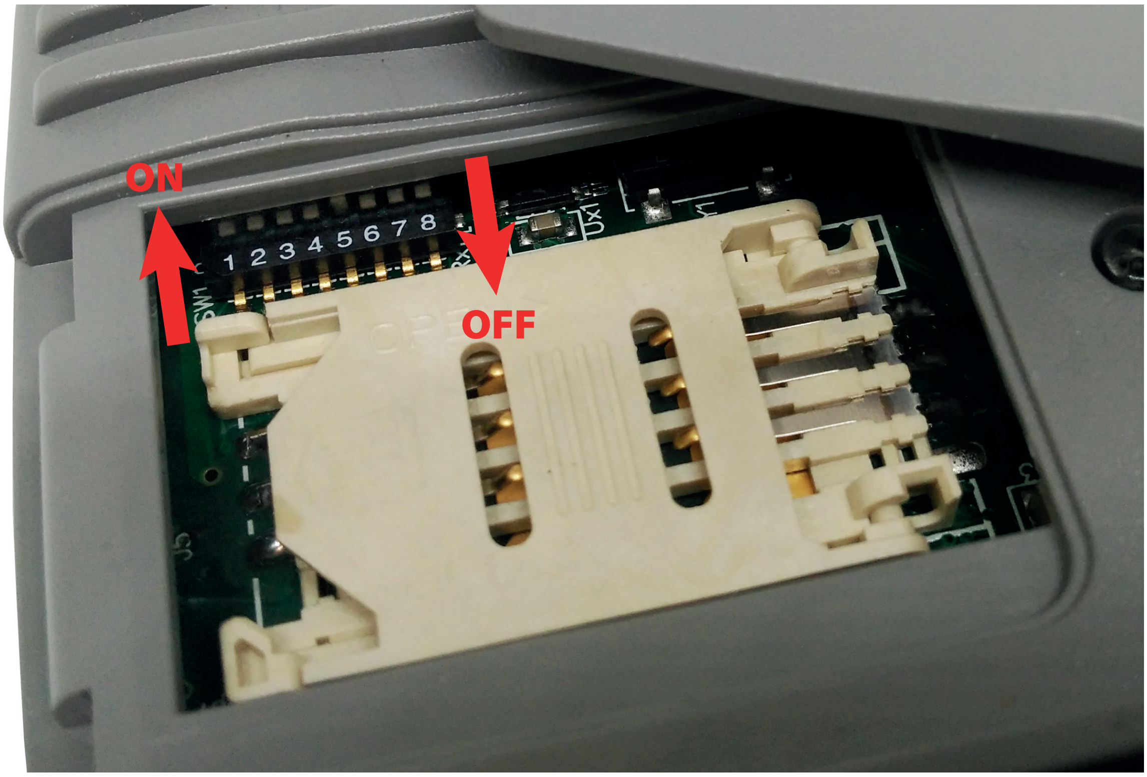
Mode RS485: ☑ Check if you want to use the com port as RS485 (Remember you need to set an internal switch)

□ Allow incoming GSM call (CSD Data Call) Only for TCP Server and TCP Client functions (CSD only compatible using WAN in GPRS mode)

○ Function: Nothing or Used by External Device

(*2) The Titan mini device has an output (VCC_OUT, PIN_10) that can be configured to a 3.3V or 5V output.

(*3) The Titan mini device has a digital input that is shared with the RX pin belonging to the COM2 port. As a result, if we wish to use the digital input, we cannot use the COM2 port, and vice versa. TO use the digital input, ensure that switch 5 is in the ON position. The digital input will change status if PIN_13 is disconnected (in which case it will read a value of “0”), or connected to PIN_10 (in which case it will read a value of “1”).



Note: any changes to the position of the microswitches must be done only when the device is switched off.

MTX-ROUTER-TITAN mini

	MTX-ROUTER-TITAN mini 4G	MTX-ROUTER-TITAN mini 3G
	EUROPE: Penta Band LTE: 800/900/1800 /2100/2600 MHz; FDD-Band (20,8,3,7,1); Tri Band UMTS (WCDMA): 900/1800/2100 MHz; FDD-Band (8,3,1); Dual Band GSM/GPRS/ EDGE: 900/1800 MHz **US**: Quad Band LTE: 700/850/AWS (1700/2100)/1900 MHz; FDD-Band (17,5,4,2); Tri Band UMTS (WCDMA): 850/ AWS (1700/2100)/1900 MHz; FDD-Band (5,4,2); Quad Band GSM/GPRS/EDGE: 850/900/1800/1900 MHz)	WORLDWIDE: Five Bands UMTS (WCDMA/FDD); Bands: 800, 850, 900, 1900 & 2100 MHz. Quad-Band GSM; Bands: 850, 900, 1800 & 1900 MHz
4G	LTE Cat. 3: DL max. 100 Mbps, UL max. 50 Mbps, 2x2 DL MIMO	
3G	HSPA+ DL Cat.24 / UL Cat. 6, Dual Carrier: DL max. 42 Mbps, UL max. 5.76 Mbps	HSDPA Cat.8 / HSUPA Cat.6 data rates: DL max. 7.2 Mbps, UL max. 5.76 Mbps
2G	EDGE Class 12 data rates: DL max. 237 kbps, UL max. 237 kbps GPRS Class 12 data rates: DL max. 85.6 kbps, UL max. 85.6 kbps	EDGE Class 12 data rates: DL max. 237 kbps, UL max. 237 kbps GPRS Class 12 data rates: DL max. 85.6 kbps, UL max. 85.6 kbps
		CSD data transmission up to 9.6 kbps, V.110, non-transparent
SMS	SMS text messages	SMS text messages

Interfaces

Ethernet 10/100 BaseT (RJ45 connector)

USB 2.0 (micro AB connector), RS232 DB9M connector, RS485 terminal block

2 operating LEDs

SIM card interface 1.8V/3V

Power supply (2-way plug-in terminal block)

WiFi 802.11 b/g/n (SMA-F RP)

SMA antenna connectors 4G/3G/2G

Customization

Externals: temperature, distance, any Modbus RTU/TCP device

Compatible with Wavenis RF sensors using an internal wavecard (optional module)

GPS (optional module)

CERTIFICATIONS: CONFORMITY AND ROHS

1. MTX-Router-Titan II-S

1.1 RED 2014/53/EU Conformity assessment

RED Declaration of Conformity (DoC)

Unique identification of this DoC: MTX-TITAN-II RED DoC

MATRIX ELECTRONICA S.L.U., C/ Alejandro Sanchez 109, 28019 Madrid, Spain

Standards of European Type Approval

We declare under our sole responsibility that the MTX-TITAN II-S family product, in all its variants

MTX-Router-Titan II-S	MTX-Router-Titan II-SC
MTX-Router-Titan II-S-3G	MTX-Router-Titan II-SC-3G
MTX-Router-Titan II-S-3G-GPS	MTX-Router-Titan II-SC-3G-GPS
MTX-Router-Titan II-S-4G-C1	MTX-Router-Titan II-SC-4G-C1
MTX-Router-Titan II-S-4G-GPS C1	MTX-Router-Titan II-SC-4G-GPS C1
MTX-Router-Titan II-S-4G-C4	MTX-Router-Titan II-SC-4G-C4
	MTX-Router-Titan II-SC
	MTX-Router-Titan II-SC-3G

Object of the declaration described above are in conformity with the relevant Union harmonization Legislation: RED Directive 2014/53/EU and R&TTE Directive 99/5/EC.

The following harmonized standards and/or other normative documents were applied: are labeled with the CE conformity mark.

CE

- EMC (art 3.1.b): EN 301 489-1 V2.2.0 EN 301 489-52 V1.1.0, EN 301 489-3 V2.1.1
- RADIO SPECTRUM (art 3. 2): EN 301 511 V12.5.1, EN 301 908-1 V11.1.1, EN 301 908-2 V11.1.1, EN 300 440 V2.1.1
- SAFETY (art 3.1.a): EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
- RF SAFETY: EN62311:2008

The technical documentation relevant to the above equipment will be held at

MATRIX ELECTRONICA S.L., Alejandro Sanchez 109, 28019 Madrid, Spain

Madrid, 5/30/2018

Mr. J. Vicente

Managing Board

2. MTX-Router-Titan II-R

2.1 RED 2014/53/EU Conformity assessment

RED Declaration of Conformity (DoC)

Unique identification of this DoC: MTX-TITAN-II RED DoC

MATRIX ELECTRONICA S.L.U., C/ Alejandro Sanchez 109, 28019 Madrid, Spain

Standards of European Type Approval

We declare under our sole responsibility that the MTX-TITAN II-R family product, in all its variants

MTX-Router-Titan II-R
MTX-Router-Titan II-R-3G
MTX-Router-Titan II-R-4G-C1
MTX-Router-Titan II-R-4G-C1-W
MTX-Router-Titan II-R-4G-C3
MTX-Router-Titan II-R-4G-C6
MTX-Router-Titan II-R
MTX-Router-Titan II-R-3G

Object of the declaration described above are in conformity with the relevant Union harmonization Legislation: RED Directive 2014/53/EU and R&TTE Directive 99/5/EC.

The following harmonized standards and/or other normative documents were applied: are labeled with the CE conformity mark.

CE

- EMC (art 3.1.b): EN 301 489-1 V2.2.0 EN 301 489-52 V1.1.0, EN 301 489-3 V2.1.1
- RADIO SPECTRUM (art 3. 2): EN 301 511 V12.5.1, EN 301 908-1 V11.1.1, EN 301 908-2 V11.1.1, EN 300 440 V2.1.1
- SAFETY (art 3.1.a): EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
- RF SAFETY: EN62311:2008

The technical documentation relevant to the above equipment will be held at

MATRIX ELECTRONICA S.L., Alejandro Sanchez 109, 28019 Madrid, Spain

Madrid, 5/30/2018

Mr. J. Vicente

Managing Board

3. MTX-Router-Titan

3.1 RED 2014/53/EU Conformity assessment

We, MATRIX ELECTRÓNICA S.L.U.: C/ Alejandro Sánchez 109, 28019 Madrid, Spain
declare under our sole responsibility that the products MTX-Router-Titan based on MTX-Gateway:

PRODUCTS			
MTX-Router-Titan (only ETH+WiFi)	199802133	MTX-GATEWAY	199802101
MTX-Router-Titan-3G (EHS6)	199802117	MTX-GATEWAY-3G (EHS6)	199802121
MTX-Router-Titan-3G (-36 to -72Vdc)	199802145	MTX-GATEWAY-3G-GPS (EHS8)	199802144
MTX-Router-Titan-3G-GPS (EHS8)	199802139	MTX-GATEWAY-4G-GPS (PLS8-E)	199802104
MTX-Router-Titan-4G-GPS (PLS8-E)	199802141	MTX-GATEWAY-OEM	199802106
MTX-Router-Titan-3G-WMBUS	199802156	MTX-GATEWAY-LC	199802111
MTX-Router-Titan-4G-WMBUS-GPS	199802157	MTX-GATEWAY-LC-OEM	199802107
MTX-Router-Titan-TC	199802132		

object of the declaration described above is in conformity with the relevant Union harmonization Legislation: RED Directive 2014/53/EU and R&TTE Directive 99/5/EC.

The following harmonized standards and/or other normative documents were applied: are labeled with the CE conformity mark.

CE

- EMC (art 3.1.b): EN 301 489-1 V2.2.0 EN 301 489-52 V1.1.0, EN 301 489-3 V2.1.1
- RADIO SPECTRUM (art 3. 2): EN 301 511 V12.5.1, EN 301 908-1 V11.1.1, EN 301 908-2 V11.1.1, EN 300 440 V2.1.1
- SAFETY (art 3.1.a):EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
- RF SAFETY: EN62311:2008
- RED Directive 2014/53/EU

The technical documentation relevant to the above equipment will be held at:

MATRIX ELECTRÓNICA S.L.U.: C/ Alejandro Sánchez 109, 28019 Madrid, Spain

Madrid, 30/05/2017

Mr. J. Vicente

Managing Board

4. MTX-Router-Titan mini

4.1 RED 2014/53/EU Conformity assessment

We, MATRIX ELECTRÓNICA S.L.U.: C/ Alejandro Sánchez 109, 28019 Madrid, Spain
declare under our sole responsibility that the products MTX-Router-Titan mini based on MTX-GTW:

PRODUCTS			
MTX-Router-Titan-mini (only ETH-WiFi)	199802134	MTX-GTW-3G (EHS5-E)	199802119
MTX-Router-Titan-3G-mini (EHS5-E)	199802115	MTX-GTW-3G (EHS6)	199802120
MTX-Router-Titan-3G-mini (EHS6)	199802118	MTX-GTW-3G (pila RTC)	199802163
MTX-Router-Titan-3G-GPS-mini (EHS8)	199802140	MTX-GTW-3G-BT (EHS6)	199802170
MTX-Router-Titan-4G-GPS-mini (PLS8-E)	199802142	MTX-GTW-3G-GPS (EHS8)	199802143
MTX-GTW	199802110	MTX-GTW-3G-GPS (PHS8-P)	199802124
MTX-GTW (pila RTC)	199802162	MTX-GTW-4G-GPS (PLS8-E)	199802123
MTX-GTW-LC	199802152		
MTX-GTW-IO	199802153		
MTX-GTW-IO (pila RTC)	199802155		

object of the declaration described above is in conformity with the relevant Union harmonization Legislation: RED Directive 2014/53/EU and R&TTE Directive 99/5/EC.

The following harmonized standards and/or other normative documents were applied: are labeled with the CE conformity mark.

CE

- EMC (art 3.1.b): EN 301 489-1 V2.2.0 EN 301 489-52 V1.1.0, EN 301 489-3 V2.1.1
- RADIO SPECTRUM (art 3. 2): EN 301 511 V12.5.1, EN 301 908-1 V11.1.1, EN 301 908-2 V11.1.1, EN 300 440 V2.1.1
- SAFETY (art 3.1.a):EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
- RF SAFETY: EN62311:2008
- RED Directive 2014/53/EU

4.2 RoHS Compliant

MTX-Router-Titan mini compliances with Directive of the European Parliament and of the Council revised on 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS).

The technical documentation relevant to the above equipment will be held at:

MATRIX ELECTRÓNICA S.L.U.: C/ Alejandro Sánchez 109, 28019 Madrid, Spain

Madrid, 12/06/2015

Mr. J. Vicente

Managing Board