# USER MANUAL

## Z-PASS1

## Z-PASS2

**SENECA s.r.l.**

Via Austria, 26 – 35127 – Z.I. CAMIN – PADOVA – ITALY

Tel. +39.049.8705359 – 8705408 Fax. +39.049.8706287

Web site: www.seneca.it

Support: supporto@seneca.it (IT), support@seneca.it (Other)

Sales: commerciale@seneca.it (IT), sales@seneca.it (Other)

Seneca Z-PC Line modules: **Z-PASS1, Z-PASS2**

# Table of Contents

# 1 Preliminary information / Informazioni preliminari

***WARNING!***

***IN NO EVENT WILL SENECA OR ITS SUPPLIERS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF CAUSE (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE Z-PASS1/Z-PASS2, EVEN IF SENECA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.***

***SENECA, ITS SUBSIDIARIES AND AFFILIATES COMPANY OR GROUP OF DISTRIBUTORS AND SENECA RETAILERS NOT WARRANT THAT THE FUNCTIONS WILL MEET YOUR EXPECTATIONS, AND THAT Z-PASS1/Z-PASS2, ITS FIRMWARE AND SOFTWARE WILL BE FREE FROM ERRORS OR IT OPERATES UNINTERRUPTED.***

***SENECA SRL CAN MODIFY THE CONTENTS OF THIS MANUAL IN ANY TIME WITHOUT NOTICE TO CORRECT, EXTEND OR INTEGRATING FUNCTION AND CHARACTERISTICS OF THE PRODUCT.***

***ATTENZIONE!***

***IN NESSUN CASO SENECA O I SUOI FORNITORI SARANNO RITENUTI RESPONSABILI PER EVENTUALI PERDITE DI DATI ENTRATE O PROFITTI, O PER CAUSE INDIRETTE, CONSEQUENZIALI O INCIDENTALI, PER CAUSE (COMPRESA LA NEGLIGENZA), DERIVANTI O COLLEGATE ALL' USO O ALL' INCAPACITÀ DI USARE Z-PASS1/Z-PASS2, ANCHE SE SENECA È STATA AVVISATA DELLA POSSIBILITÀ DI TALI DANNI.***

***SENECA, LE SUSSIDIARIE O AFFILIATE O SOCIETÀ DEL GRUPPO O DISTRIBUTORI E RIVENDITORI SENECA NON GARANTISCONO CHE LE FUNZIONI SODDISFERANNO FEDELMENTE LE ASPETTATIVE E CHE Z-PASS1/Z-PASS2, IL SUO FIRMWARE E SOFTWARE SIA ESENTE DA ERRORI O CHE FUNZIONI ININTERROTTAMENTE.***

***SENECA SRL PUO' MODIFICARE IL CONTENUTO DI QUESTO MANUALE IN QUALUNQUE MOMENTO E SENZA PREAVVISO AL FINE DI CORREGGERE, ESTENDERE O INTEGRARE FUNZIONALITA' E CARATTERISTICHE DEL PRODOTTO.***

| Date | Revision | Notes |
|---|---|---|
| 07/03/2019 | 22<br>(FW rel. SW003900_250) | -Added chapter “Timer Configuration”<br>-Added paragraphs under “Rule Management” for new logic features |
| 20/03/2019 | 23<br>(FW rel. SW003900_251) | - Paragraph “Rule Management”: added “Bitmask” condition and “Set Bits” action<br>- Paragraphs “Alarm Configuration”, “Message Configuration”: added info about export/import to/from csv file<br>- Paragraph “Configuration Management”: added type of configuration to be saved |
| 09/04/2019 | 24<br>(FW rel. SW003900_260) | -Added chapter “OPC-UA protocol”<br>-Added paragraph “OPC-UA Server Cconfiguration” |
| 23/07/2019 | 25<br>(FW rel. SW003900_270) | -Added chapter “MQTT client protocol”<br>-Changed Chapters order for new webserver menu |
| 26/07/2019 | 26<br>(FW rel. SW003900_280) | -Added OPC-UA server Security Policy<br>-Added MQTT client protocol chapter info |
| 27/08/2019 | 27<br>(FW rel. SW003900_290) | -Added the new option “Retain” in Tag Creation/Modification |
| 05/11/2019 | 28<br>(FW rel. SW003900_292) | -Max Modbus TCP-IP servers from 10 to 25<br>-Added NAT 1:1 feature<br>-Added Static Route feature |
| 19/12/2019 | 29<br>(FW rel. SW003900_293) | Added new 64 bits Tags in chapter “Tag Creation/Modification” |
| 19/12/2019 | 30 | Added info about OPC-UA Server namespace-id |
| 30/03/2020 | 31<br>(FW rel. SW003900_295) | Added “User” account |
| 23/09/2020 | 32<br>(FW rel SW003900_299) | Added “Datalogger on Trigger” new feature<br>Added “Serial Trace” new feature<br>Added “SMS command “OVPN ON” and “OVPN OFF”<br>Added new parameter MQTT “Sleep Timeout” |
| 25/01/2021 | 33 | Added new command “CLEAN LOGS” (From FW rel 313)<br>Added info on how to send commands from MQTT to the device<br>Added info on how to write a command from MQTT to the device<br>Removed all references to old Z-PASS models |

# 2 Firmware Licensing Terms

## 2.1 Firmware with Open Source GPL

The Z-PASS firmware contains Open Source software under GPL. According to Section 3b of GPL, we offer you the source code. You can obtain the source code with licensing terms of the Open Source software from Seneca s.r.l. on request. Send your request to support@seneca.it with the subject "Open Source Z-PASS ".

# 3 Upgrading the firmware by USB pen

Z-PASS firmware can be upgraded by means of a USB pen; a pen drive formatted with FAT32 file-system is needed.

The procedure is the following:

1) download the FW file from one of the following links:

   http://www.seneca.it/products/z-pass1
   http://www.seneca.it/products/z-pass2

   the downloaded file is a .zip file; extract the FW file from it;
   the FW file shall have a name like the following:

   *SW003900_xxx.bin*

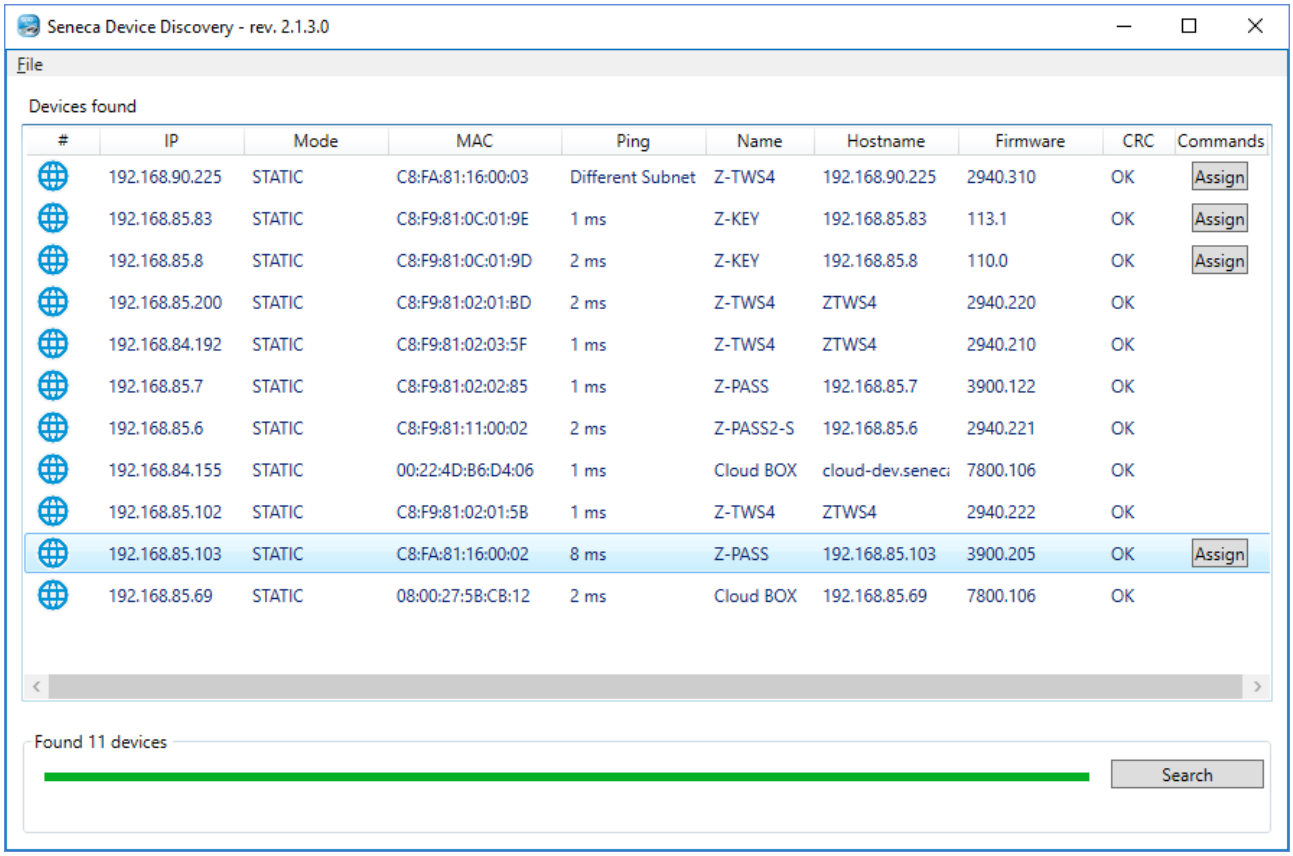
2) copy the file into the root of the USB pen
3) switch off the Z-PASS
4) insert the USB pen into the USB#1 port
5) switch on the Z-PASS; the upgrade procedure will take some minutes to be completed; during this time, the Z-PASS MUST NOT be switched off; during the procedure, the Z-PASS will be rebooted several times; also, during the procedure, several LEDS will blink simultaneously[1]
6) the upgrade procedure is ended when only the LED “RUN” is blinking[2]
7) remove the USB pen

[1] This applies only to products with HW revisions IO and R01; in details: for IO HW revision, all LEDs will blink simultaneously, except for Power, LAN/WAN, COM and modem LEDs; for R01 HW revision, RUN, VPN and SERV LEDs will blink.
[2] Also SERV and VPN LEDs might blink, depending on the Device configuration and status.

# 4 Discovering the Z-PASS IP address

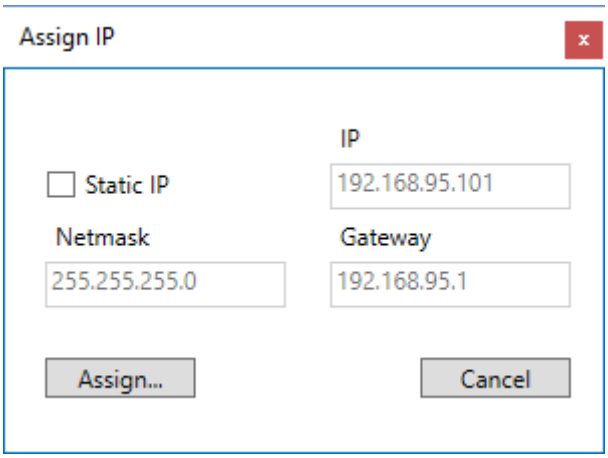
Z-PASS devices come out of the factory with the default IP address 192.168.90.101, on the Ethernet (LAN) network interface.

If this address is changed, *and forgotten*, it can be retrieved using the "Seneca Device Discovery" application (SDD), as shown in the following figure:

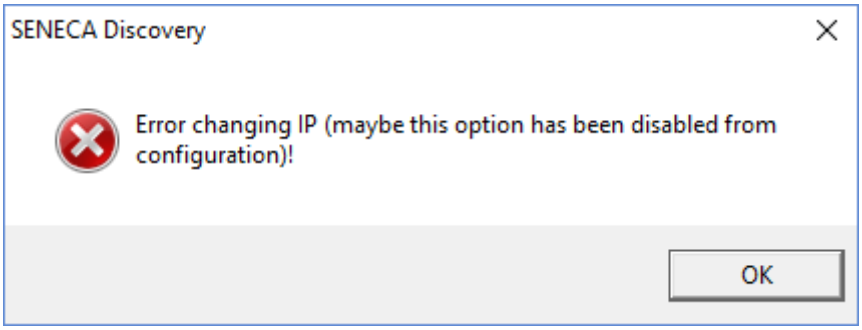



This application shows the IP address, MAC address, FW version and some other useful information, for every Z-PASS device (and other Seneca products) found in the LAN.

Moreover, by clicking on the "Assign" button, it is possible to change the network configuration parameters of a device, as shown in the following figure:




For security reasons, this feature can be disabled on the device (see paragraph 20.1.2); in this case, the following error message is shown, after clicking on the "Assign" button".




The SDD can be easily installed by running the installer program available at the following link:

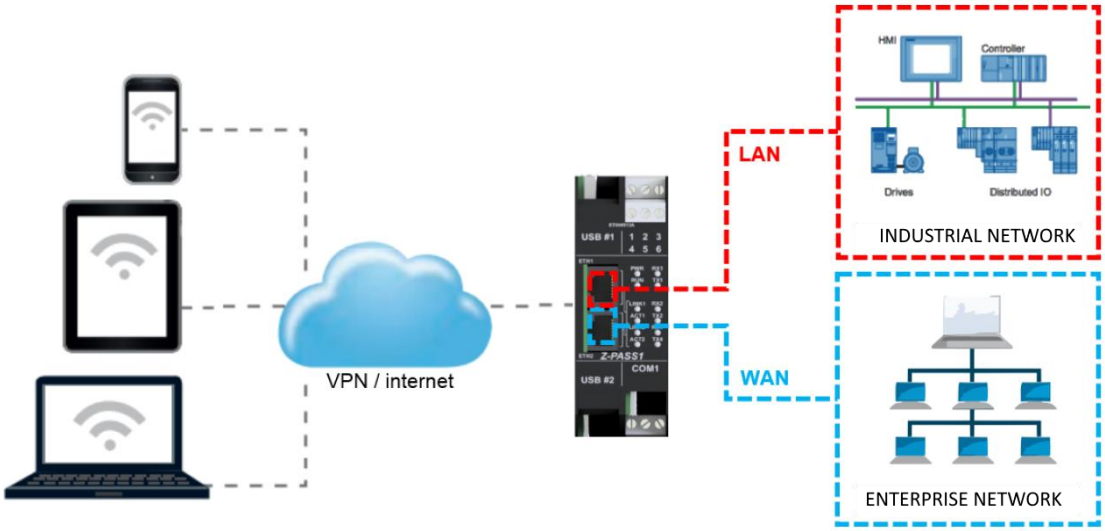
http://www.seneca.it/products/sdd

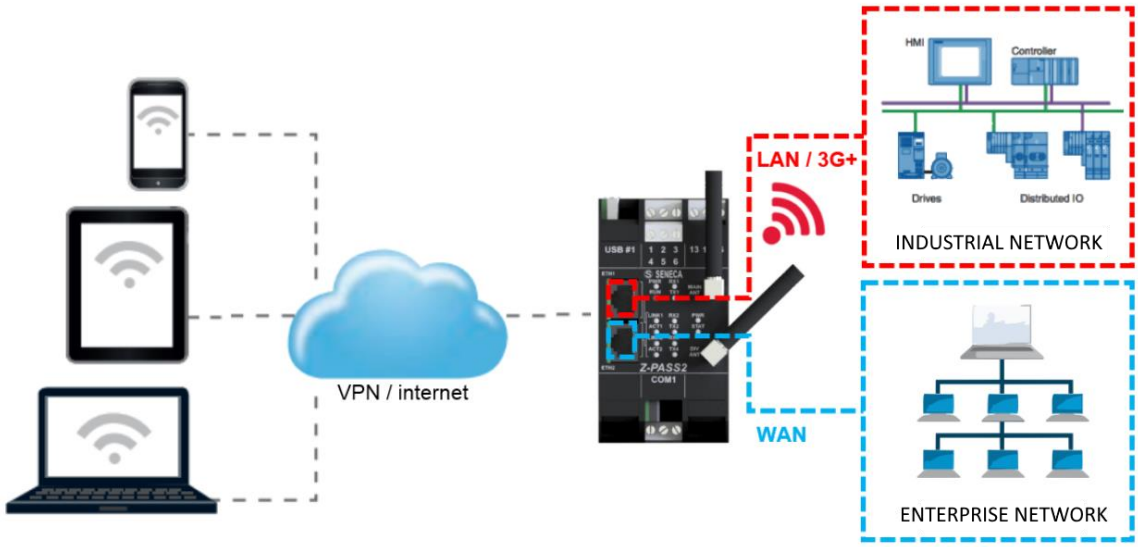
NOTE:
- when Z-PASS is working in "Switch" mode, the IP Address shown by the SDD is the same regardless of the Ethernet port which the PC running the SDD is connected to;
- when Z-PASS is working in "LAN/WAN" mode, the IP Address shown by the SDD is the LAN IP Address when the PC is connected to the LAN port, the WAN IP Address when the PC is connected to the WAN port; moreover, the network configuration parameter changes apply to the relevant port.

# 5 Ethernet Mode

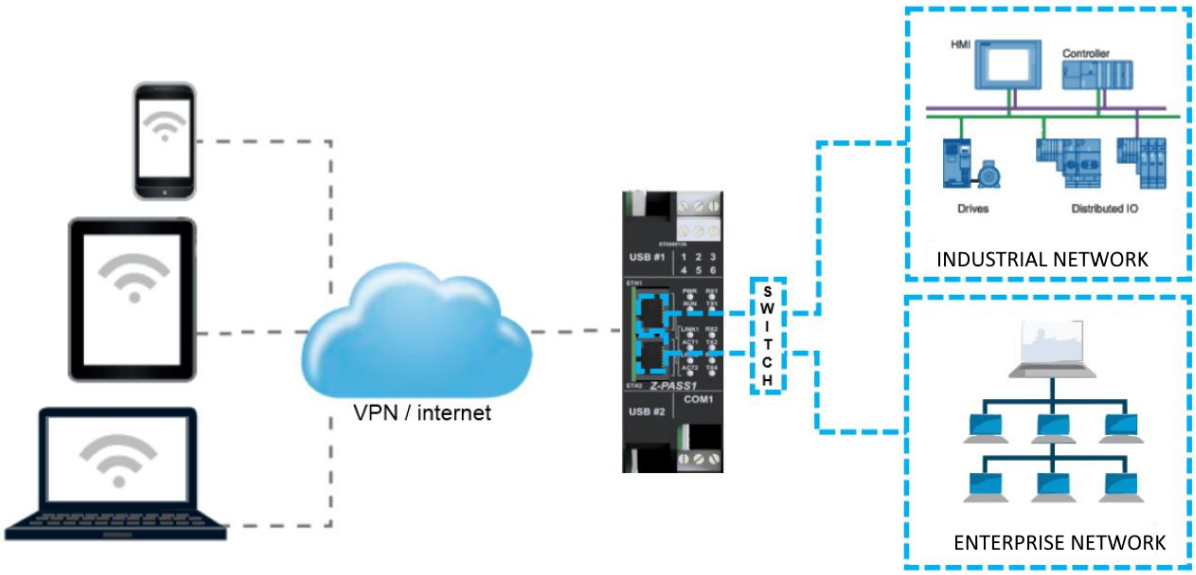
In Z-PASS products, the two available Ethernet ports can be configured as two fully separated network interfaces ("LAN" and "WAN") or, as in the older versions, they can work as ports of an Ethernet switch; the user can choose between the "LAN/WAN" mode and the "Switch" mode, by means of a new configuration parameter ("Ethernet Mode") (see paragraph 20.1.2).

The “LAN/WAN” mode is needed when the “industrial” network connected to the LAN interface (comprising e.g. HMI and PLC devices) shall be separated from the “enterprise” network connected to the WAN interface (comprising enterprise PCs and servers); when the Z-PASS is remotely accessed through the WAN interface, only devices connected to the LAN interface can be reached, while access to machines lying in the enterprise network is forbidden; this is depicted in the following two figures.




When this separation is not needed or when the Internet access is achieved only through the mobile (3G+) interface, the “Switch” mode still lets the Z-PASS to be used as an Ethernet switch, as shown in the following figure.




# 6 Modbus Ethernet to Serial Gateway

Z-PASS can be configured to run as a Modbus Ethernet to Serial Gateway: Modbus TCP requests received from the Ethernet interface (but also from the PPP [Mobile Network] and VPN interfaces) are converted into Modbus RTU requests and sent to the serial interface; in the same way, the Modbus RTU responses received from the serial interface are converted to Modbus TCP responses and sent back to the source network interface.

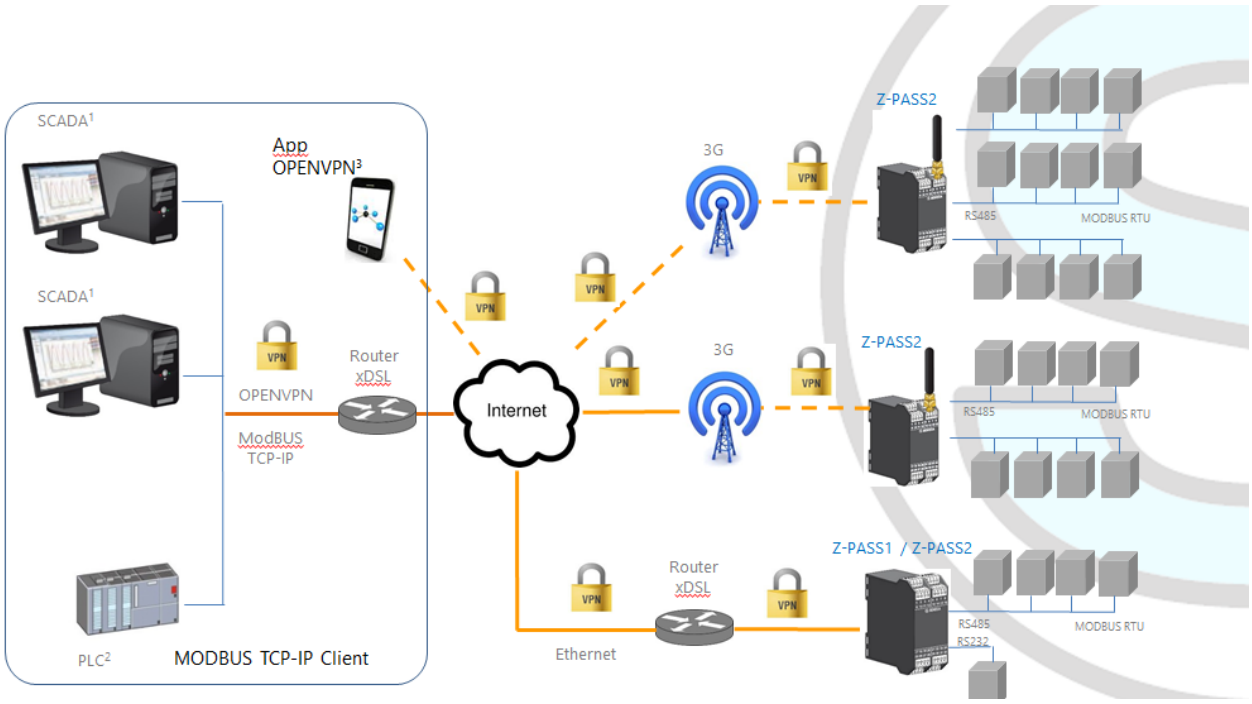
A Modbus Ethernet to Serial Gateway instance can be activated for each of the three available serial ports: COM1 (RS232/RS485), COM2 (RS485) and COM4 (RS485); each one can receive the Modbus TCP requests on a different TCP port (e.g.: 501, 502, 503).

Another possible configuration is to run a Modbus Ethernet to Serial Gateway instance, receiving Modbus TCP requests on a single TCP port (e.g.: 502) and handling two or all the three serial ports. In this case, Modbus RTU requests are simultaneously sent to all the configured ports; obviously, in this configuration, each slave module on the two or three buses shall have a distinct Modbus address;

Each Modbus Ethernet to Serial Gateway instance can support up to 32 simultaneous TCP connections.

The TCP connection can be established over a VPN tunnel, as shown in the following figure.

A detailed description of the Modbus Ethernet to Serial Gateway configuration can be found in 20.1.6.1 paragraph.



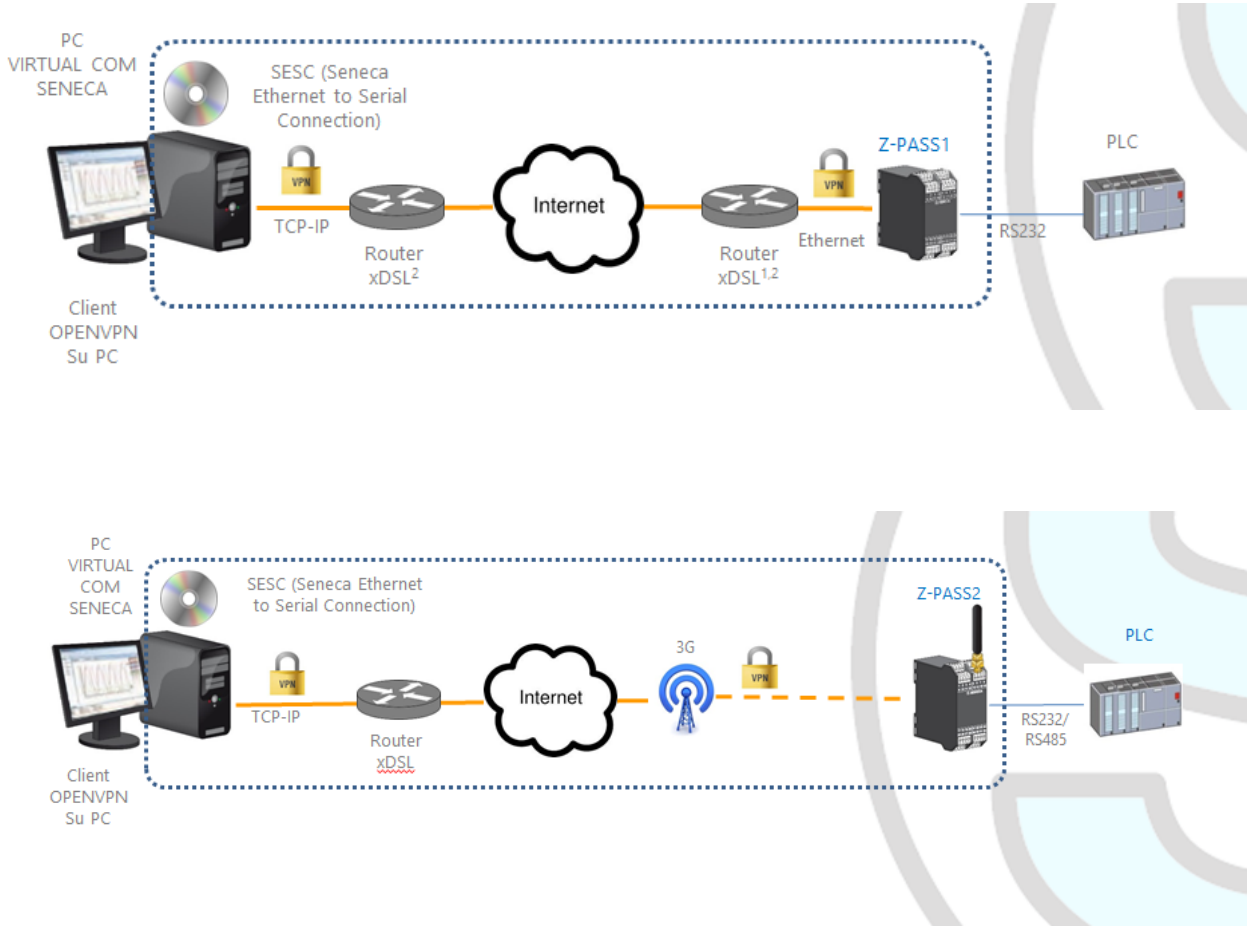

# 7 Transparent Gateway

As an alternative to Modbus Ethernet to Serial Gateway, Z-PASS can be configured to run as a "Transparent Gateway". The big difference between these two modes is that, while the first works just with the Modbus protocol, the second could virtually be applied to any serial protocol that can be transported over the TCP/IP stack.
As a Transparent Gateway, Z-PASS provides the following operating modes:

- Virtual COM (with RFC 2217 support)
- Serial Tunnel Point-to-Point on TCP
- Serial Tunnel Point-to-Point on UDP
- Serial Tunnel Point-to-Multipoint on UDP

Each mode will be fully described in a specific paragraph below.

## 7.1 Virtual COM (with RFC 2217)




The Virtual COM functionality lets to a PC Application, which transmits data only over a serial line, to communicate with a remote serial device, using Ethernet/Internet; in other word, through a Z-PASS, a PC and a serial device, placed in sites distant from each other, can communicate as they are directly connected.

In this mode, data sent over the LAN or WAN network, are received by the Z-PASS and sent to the serial port; response packets follow the reverse path.

RFC 2217 defines some features that let the PC remotely set the properties (baud rate, data bits, stop bits and parity) of the Z-PASS serial port; so, when the Virtual COM operating mode is selected for one port, the port is reconfigured regardless of the previous settings and the values configured by means of the “Serial Ports” web page are overwritten.

To let the Virtual COM work, an utility called “Seneca Ethernet to Serial Connection” shall be installed on the PC; this is explained in details in 7.1.1 paragraph.

The TCP connection can be established over a VPN tunnel, as shown in the figures at the beginning of the paragraph.

Once the connection is established, a program using the virtual COM port will transmit data to the Z-PASS serial port; for example, Modbus RTU requests sent by a Modbus Master program will reach Modbus slave devices connected to the COM2 RS485 bus.

A particular notice shall be given about the "Data Packing Interval" parameter, that can be set when Virtual COM operating mode is selected: this parameter lets you define the time interval, in milliseconds, used by Z-PASS as a criterion to pack the data bytes received from the serial port before sending them to the network; in other words, when Z-PASS does not receive any more bytes from the serial port for the given time interval, it packs the received bytes and send them over the established TCP connection; the optimal value to be set for this parameter depends on the protocol that is transparently routed from the TCP/IP network to the serial line and vice versa.

***WARNING!***

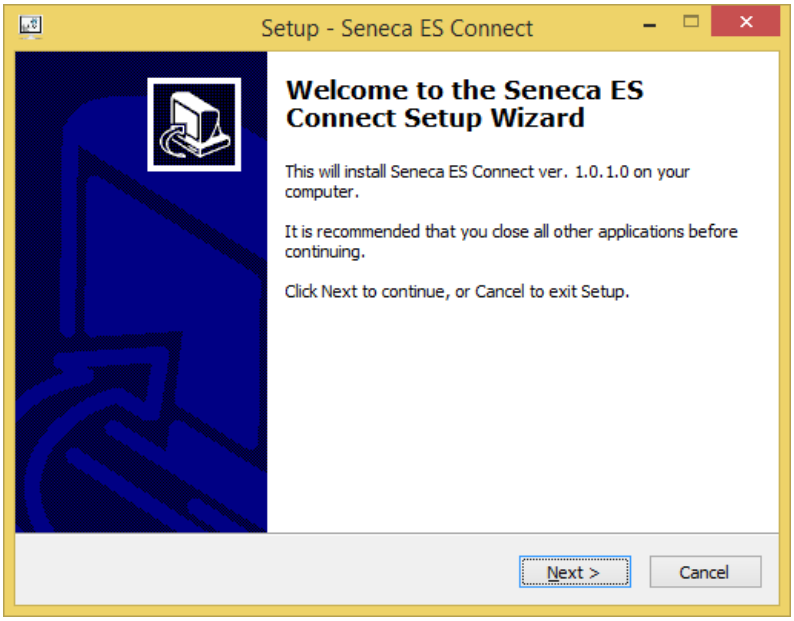
***In the Virtual COM operating mode, just one connection is accepted for a given serial port.***

### *7.1.1 Seneca Serial to Ethernet Connect*

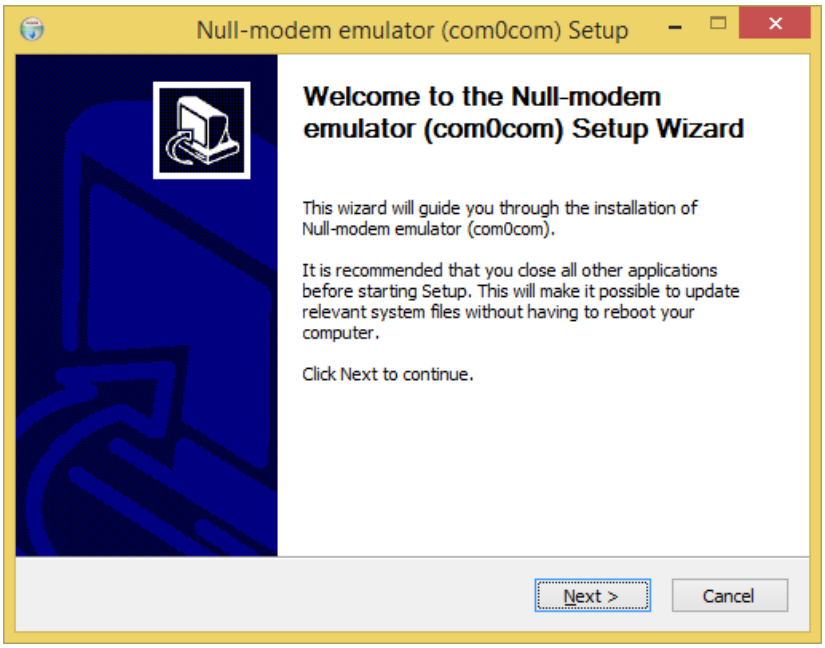
#### *7.1.1.1 Installing Seneca Serial to Ethernet Connect driver*

Seneca Ethernet to Serial Connect runs on Windows Vista™, Windows 7™ and Windows 8.1™.

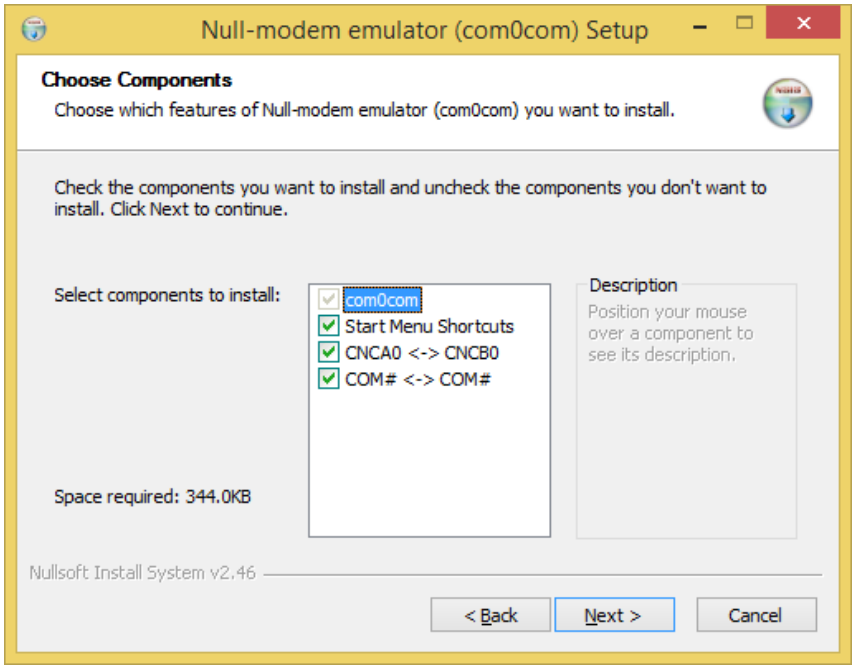
Double click the installer:



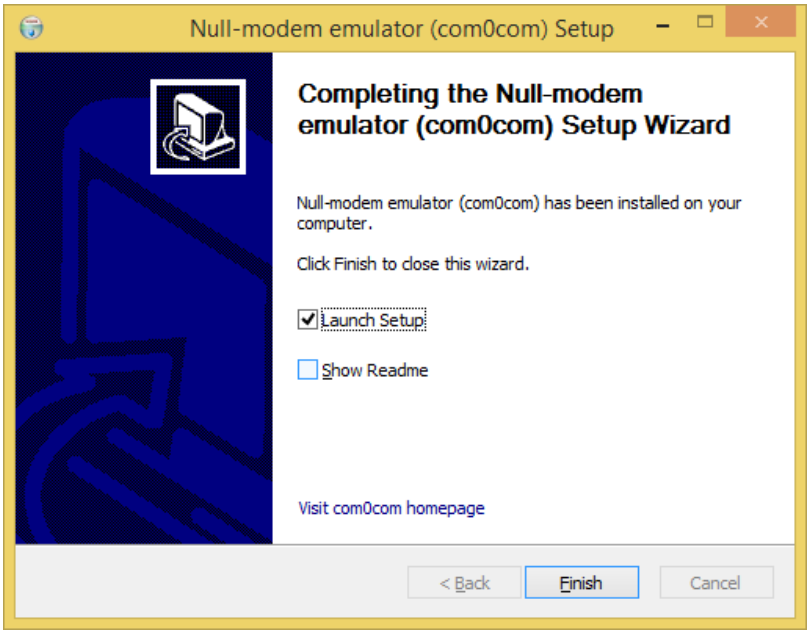

After that, the com0com driver will be installed:



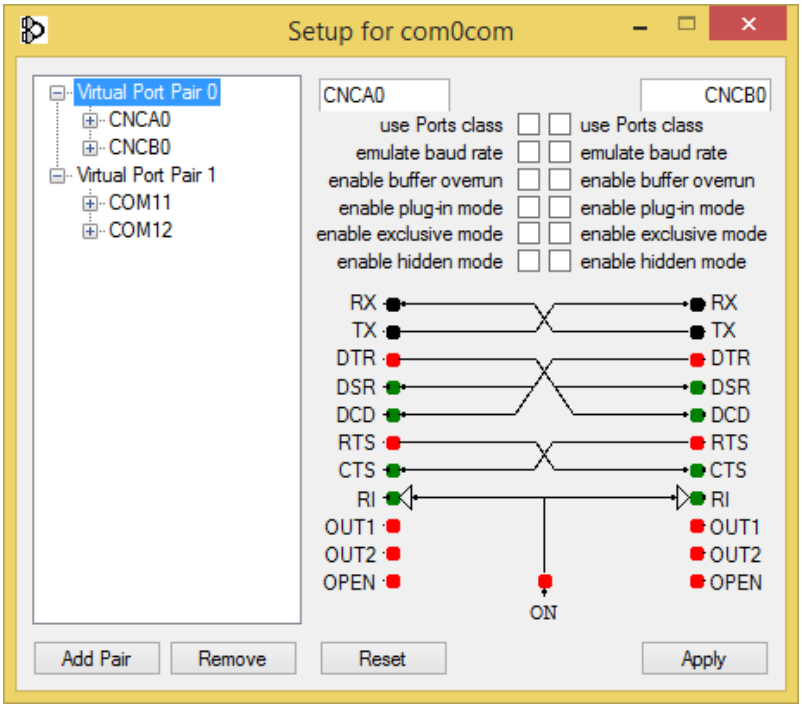

Select the CNCA0<->CNCB0 and the COM#<->COM# virtual port names:



Now Click on “Launch Setup”:




Press Finish, the com0com setup will open:



We have installed two pairs of Virtual Ports:

CNCA0, CNCB0

and also:

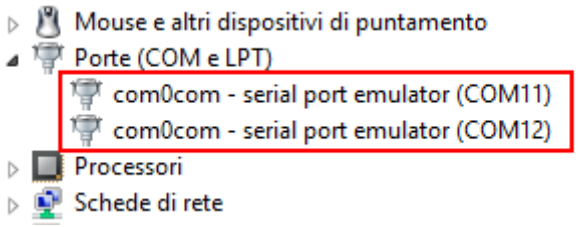
COM11, COM12 (note that in your system the com# can be different).

The first pair can be used in software that support the CNCA names, the other in software that support only the Ports class.

If you need to add more virtual ports, press the “Add Pair” button, then select if you need or not a port class.

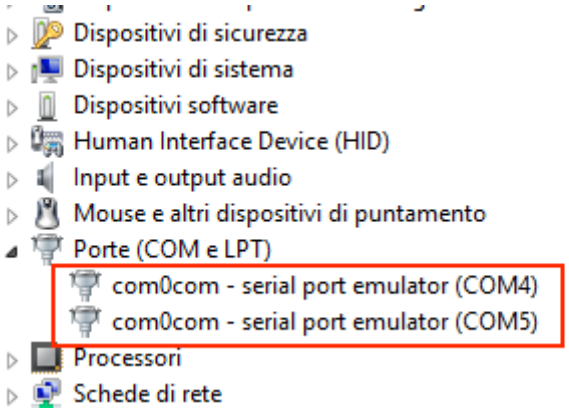
Confirm the driver installation with “Apply”.

The serial port emulator couple COM11-COM12 will be available:



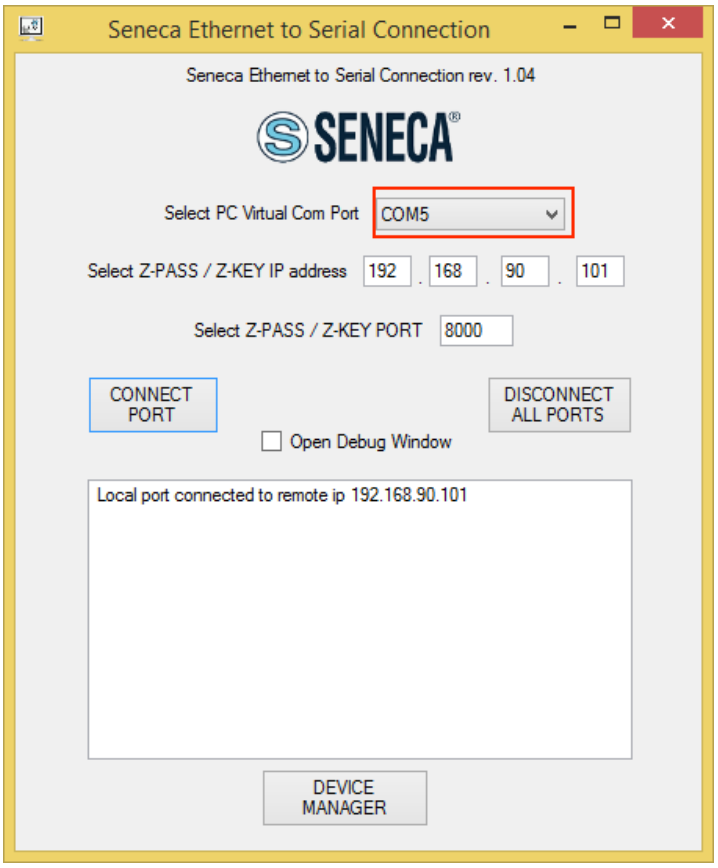

### *7.1.1.2 Select the COM port for Seneca Serial to Ethernet Connect*

The driver installation will use the first 2 serial ports that are free (in our case the driver has created the COM4 and COM5 pair):

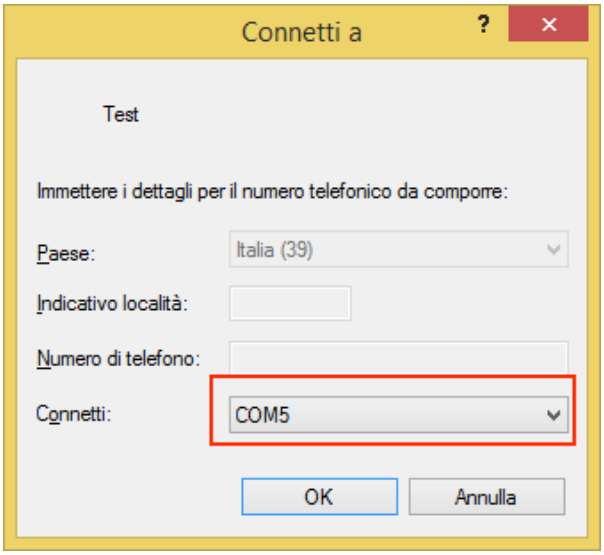



The Ethernet to Serial Connection software will use only one port (the right port in the com0com setup), only the com0com ports will be displayed.

We connect the COM5 to the Seneca ES Connector:

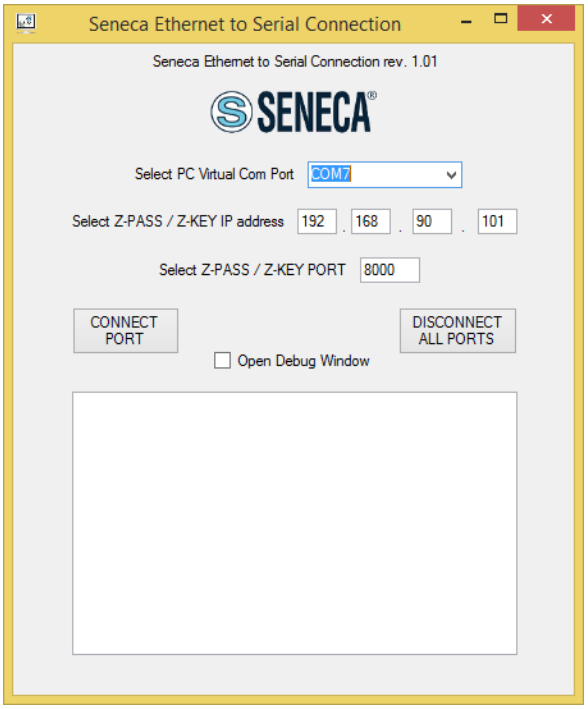



Now use the same COM5 (for example in a terminal software):




The COM5 is now connected to Z-PASS, on the TCP port 8000:

### 7.1.1.3 Configuring Seneca Serial to Ethernet Connect




- *Select the Virtual COM Port*
- *Select the Z-PASS IP address (default 192.168.90.101).*
- *Select the TCP-IP port (default 8000).*

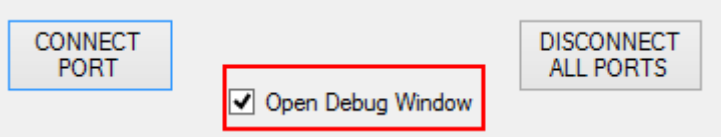
Then click on “CONNECT PORT”.

If you need to connect another serial com to another Z-PASS, configure the new com port and the new IP address, then click on “CONNECT PORT”.

To disconnect all ports, click on “DISCONNECT ALL PORTS”.

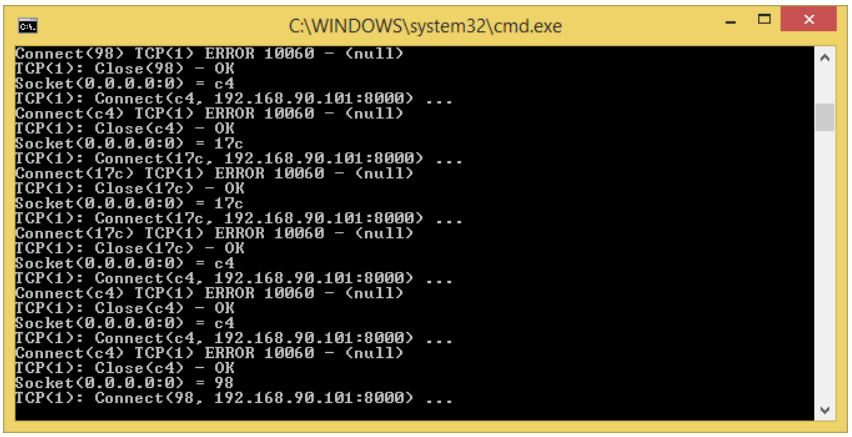
### 7.1.1.4 Debugging the Connection

Before clicking on “CONNECT PORT”, you can choose to open a debug window to verify the connection:




Then click on “CONNECT PORT”:

If you see “Connect Error” like here:



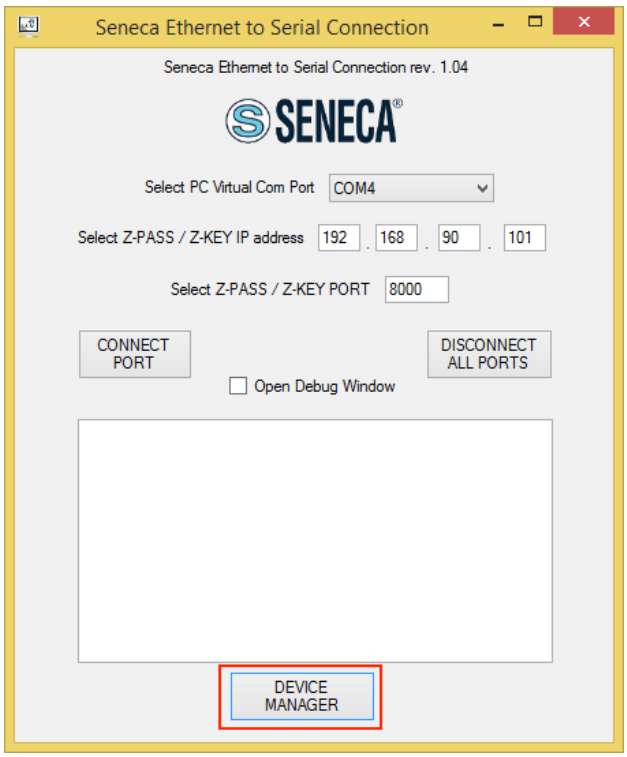

check the configuration (Z-PASS IP address and TCP port).

### *7.1.1.5 Changing the COM port number*

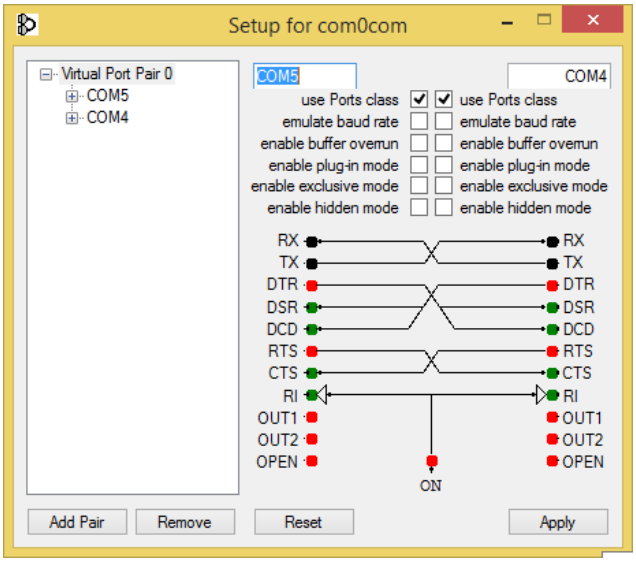
Old software applications can use only a little range of COM ports, so you may need to change the virtual COM number.

In our case the COM pair created is COM4/COM5, but we want to change it to COM2/COM3:

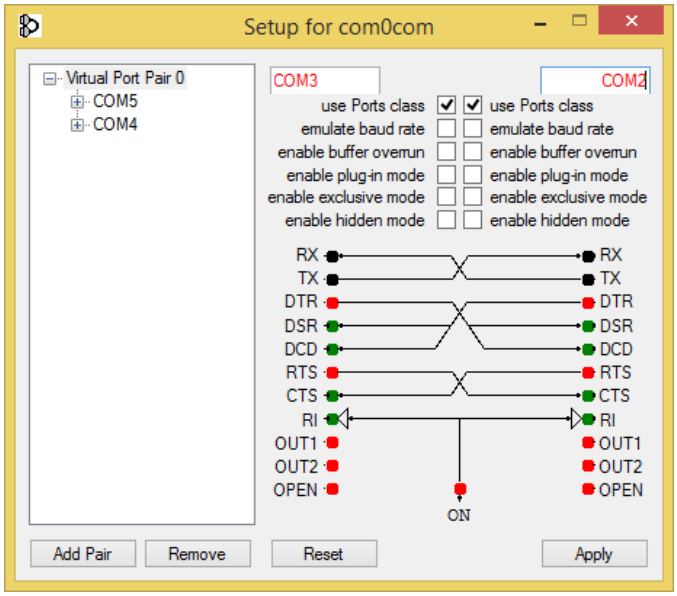
Click on “DEVICE MANAGER” button:



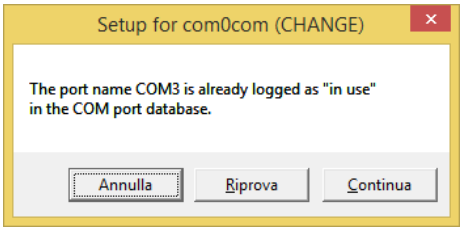
The com0com setup window will open:




Now change COM5 to COM3 and COM4 to COM2, then click “Apply”:

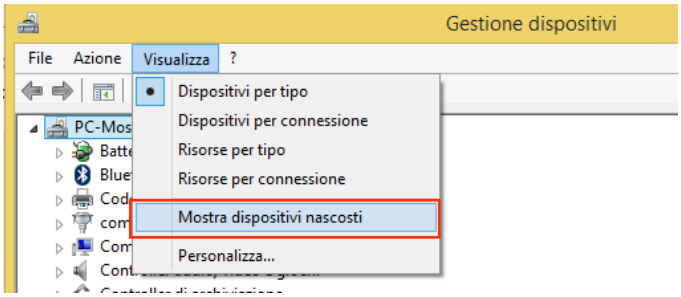


Sometimes the COM can be marked as “in use”:

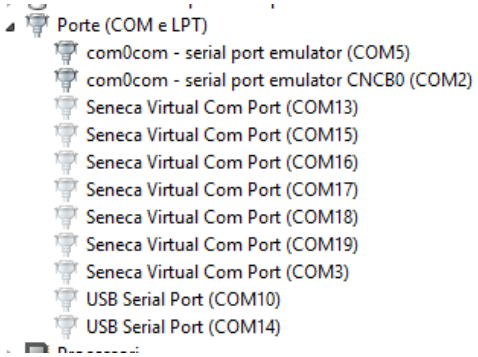



If you need to use this COM number, click on “Continue”, then go to the device manager.

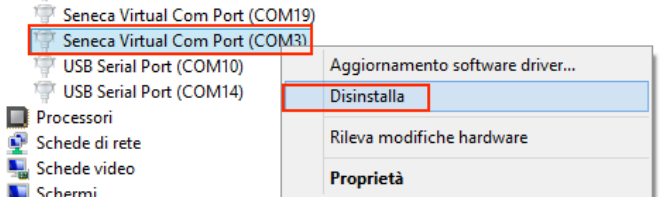
We must uncheck the “in use” flag by uninstalling the port. Since the port is not connected, click on “Show hidden peripherals”:



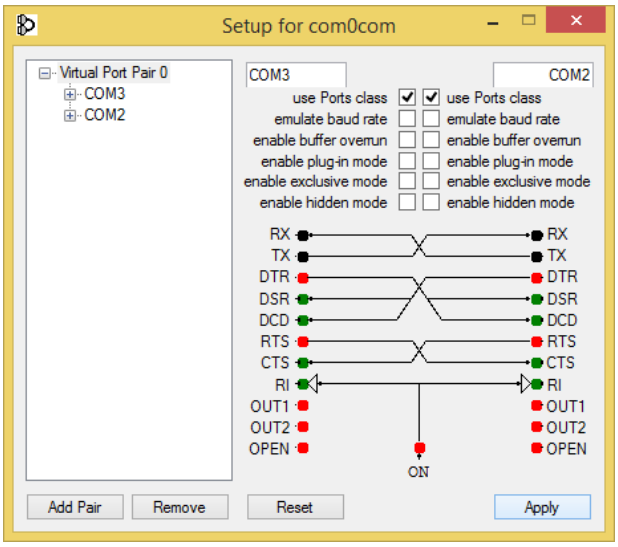

Now all the ports that are not in use are displayed in transparent (also our COM3):



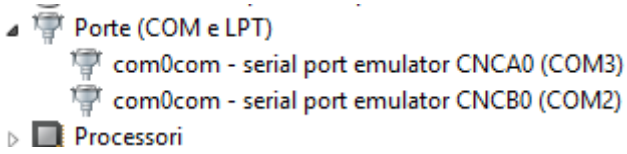

Now select the COM3 port and click on “Uninstall”:




Now the COM3 is free and we can use it on the com0com setup:

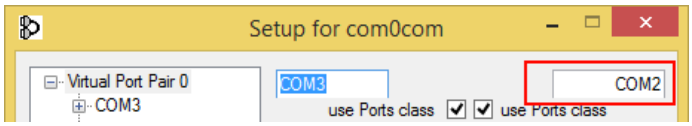



Finally click on "Apply", now the COM3/COM2 pair is created:

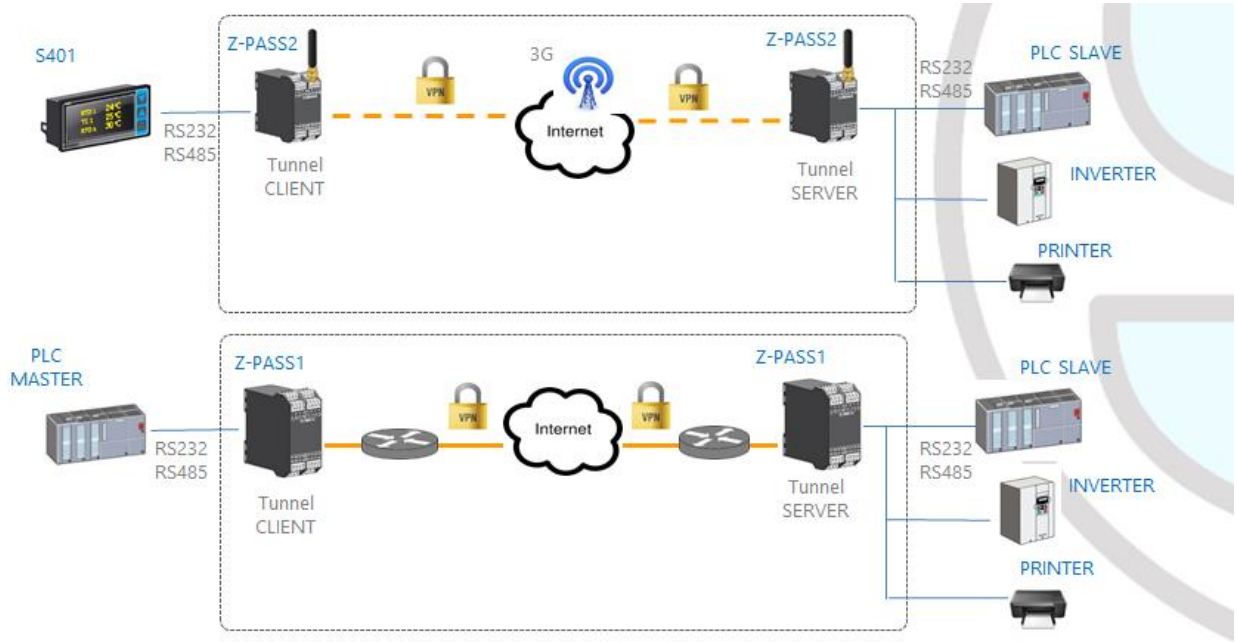



***WARNING!***

***Seneca Serial to Ethernet connector always uses the right port in the com0com setup (in our case COM2).***



## 7.2 Serial Tunnel Point-to-Point on TCP




The Serial Tunnel Point-to-Point allows to extend a serial connection between two serial devices that support the same serial protocol by a TCP/UDP connection.

In TCP operating mode, one Z-PASS is defined as the “Master” and another Z-PASS is the “Slave”: the first is a Tunnel Client, which receives data from the serial line and sends them to an outgoing TCP connection, while the second is a Tunnel Server, which receives data from an incoming TCP connection and sends them to the serial line; in this mode a “tunnel” is established between the two serial ports.

In configuration phase, on the Master it is necessary to set the Destination IP Address and the Destination Port that defines the outgoing TCP connection; on the Slave, you have to set the Listen Port on which the incoming TCP connection is accepted.

The tunnel can be established through the LAN (Ethernet) or through the WAN (Mobile Network), also exploiting VPN connectivity.

***WARNING!***

***In the Serial Tunnel Point-to-Point on TCP operating mode, just one connection is accepted for a given serial port.***

## 7.3 Serial Tunnel Point-to-Point on UDP

The Serial Tunnel Point-to-Point on UDP operating mode is much like that on TCP.

The only difference is that no TCP connection is established and serial data are transported by UDP packets.

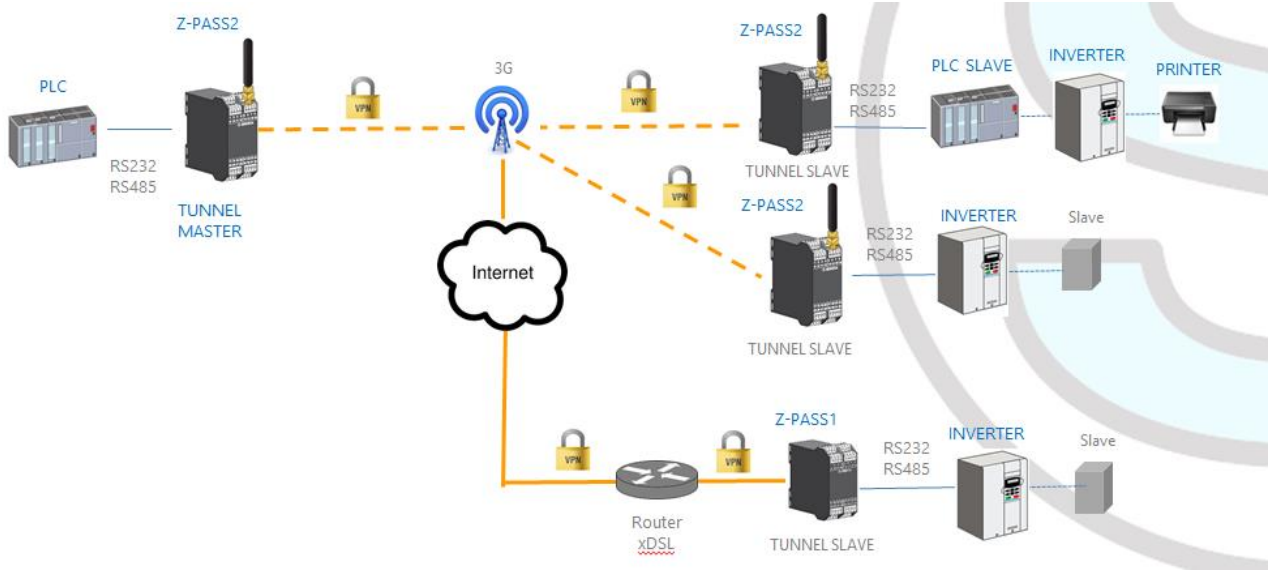
The configuration parameters are the same as those for the serial tunnel on TCP.

Also in this case, the tunnel can be established through the LAN (Ethernet) or through the WAN (Mobile Network), also exploiting VPN connectivity.

***WARNING!***

***In the Serial Tunnel Point-to-Point on UDP operating mode, just one connection is accepted for a given serial port.***

## 7.4 Serial Tunnel Point-to-Multipoint




The Serial Tunnel Point-to-Multipoint allows to create a tunnel with a master and more than one slave; on the master side, the data received from the serial line are sent to all the slaves, by means of *multicast* transmission mode, in UDP packets.

To let the multicast work, the master and the slaves shall be part of the same *multicast group*, so there is a "Multicast Group" parameter that shall be properly set; furthermore, for the Master Configuration have to be defined "Destination Port" and "Multicast Interface" parameters, the latter shall be set to select the network interface that allows to send the packets; for the slave configuration, "Listen Port" and "Multicast Interface" are requested; the latter shall be set to select the network interface which allows to receive the packets.

The tunnel can be established through the LAN (Ethernet) or through the VPN (Ethernet or 3G based).

***WARNING!***

***In the Serial Tunnel Point-to-Multipoint operating mode, just one connection is accepted for a given serial port.***

# 8 Modbus Shared Memory Gateway

Z-PASS can be configured to run as a Modbus Shared Memory Gateway: in this mode, a set of configured tags are periodically and continuously read from Modbus RTU Slaves or Modbus TCP Servers; these values are always available in a shared memory, readable via Modbus TCP/RTU.

Z-PASS Modbus Shared Memory Gateway supports up to 2000 tags and up to 32 Modbus TCP Client simultaneously.

In the Z-PASS Modbus Shared Memory Gateway, a Modbus TCP/IP Server (or slave) is always running on a configured TCP port.

As for Modbus Ethernet to Serial Gateway functionality (see chapter 6), the Modbus TCP requests can be forwarded through the Ethernet interface or through the Mobile/VPN interface.

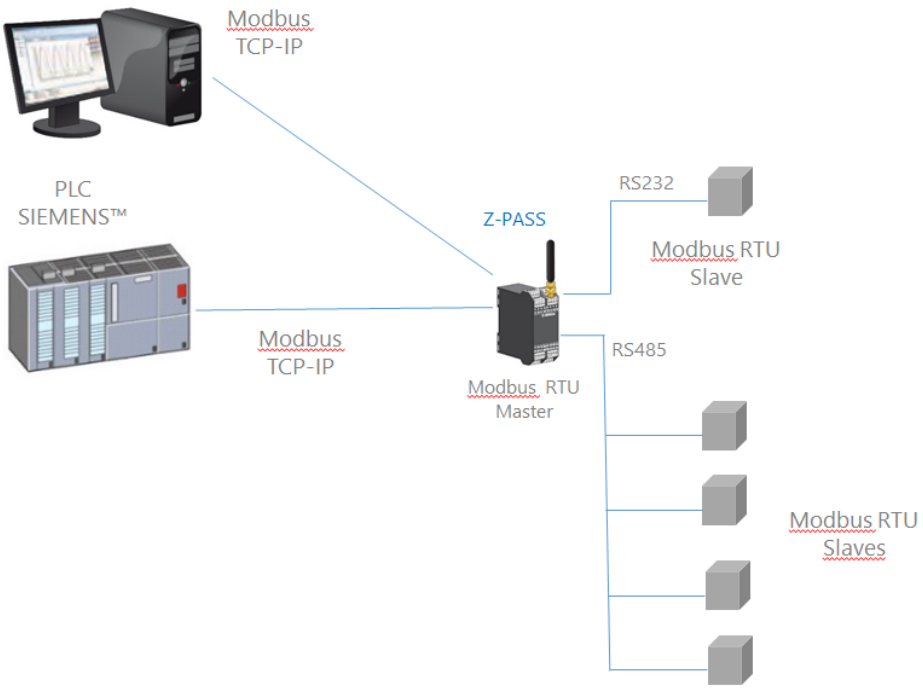
For each of the three available serial ports (COM1, COM2, COM4), the kind of "Task" can be defined: a serial port can be configured as a Modbus RTU Master or Modbus RTU Slave or not running at all.

In this manner, a number of possible combinations are available, to a maximum of three Modbus RTU Masters or three Modbus RTU Slaves; normally, a combination of the two will be chosen, for example: Modbus RTU Slave on COM1 and Modbus RTU Masters on COM2,COM4.

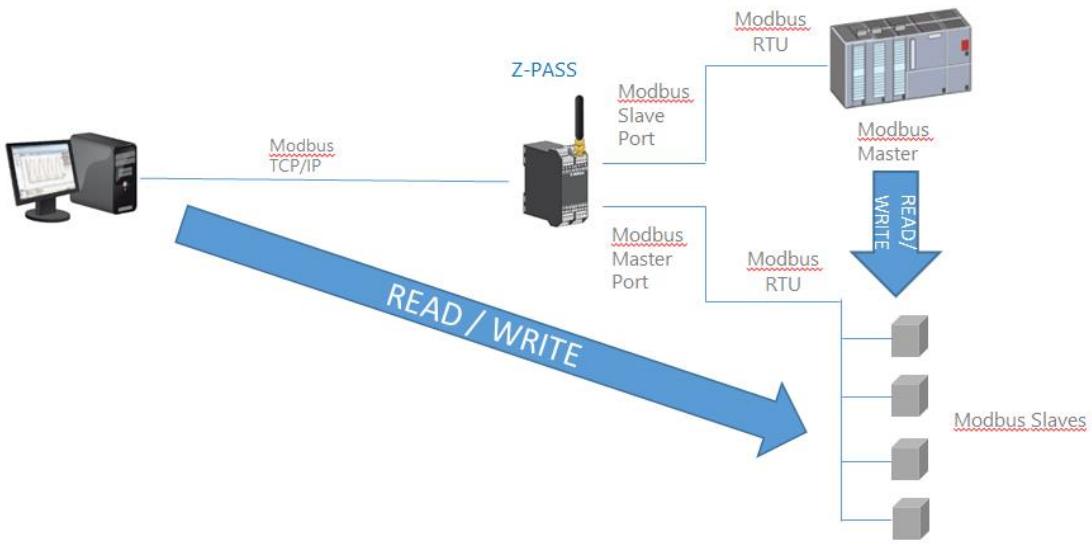
Furthermore, tags can be read from/written to up to 25 Modbus TCP Servers.

Finally, some tags can be defined which are related to "embedded" digital I/Os and to GPS information (only for Z-PASS2).

In the following pictures, some typical scenarios are shown.



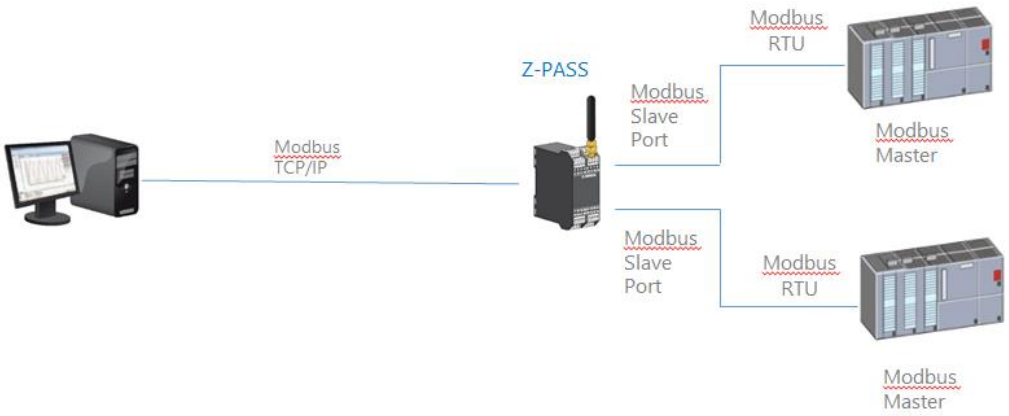

In the above picture, two serial ports (RS232 – COM1, RS485 – COM2) are configured as Modbus RTU Master.



In this case, one serial port (e.g. COM1) is configured as Modbus Slave and another (e.g. COM2) is configured as Modbus Master.

When some measures acquired from the Modbus Slaves must be available for a PLC, which supports only Modbus Master protocol, and also for a SCADA/Datalogger, the Z-PASS can be configured with one serial port defined as Modbus Slave (connected to the PLC) and another in Modbus Master (connected to the Modbus Slaves bus).

The PLC Modbus RTU Master and the Modbus TCP client(s) write/read the Z-PASS shared memory registers, while the Z-PASS Modbus Shared Memory Gateway keeps the shared memory aligned with the Modbus Slaves registers.




In the above picture, two serial ports (e.g. COM2 and COM4) are configured as Modbus Slave and connected to a PLC Modbus Master port; so, the two PLCs and the Modbus TCP Client can write/read the Z-PASS shared memory to share data among them.

The Z-PASS Modbus Shared Memory Gateway provides some interesting features as explained in the following.

Besides “classic” gateway behavior, tags can be configured to work in “Bridge” mode; this mode allows to acquire tag values from the serial side only when the gateway receives Modbus TCP/RTU Requests for those tags; this can be very useful when using RTU devices with “Fail safe” outputs[3], as explained in details in 20.3.1 paragraph.

Z-PASS Modbus Shared Memory Gateway performs requests optimization, inserting as many tags as possible in a single read/write request; the maximum number of registers in a request can be set

[3] This feature is available in many Seneca products.

independently for each serial port/TCP Server and for read and write operations; this option can be useful to connect RTU devices which support different maximum number of registers on different serial ports.

Tag configuration can be created using a Microsoft Excel™ Template provided by Seneca (see paragraph 20.3.2.4); this can largely reduce configuration time, particularly when a large number of tags shall be configured.

# 9 Data Logger

When Modbus Shared Memory Gateway functionality is enabled, Z-PASS can act as a "Data Logger": Modbus Shared Memory Gateway tag values are periodically stored into files (called "log files"), which can then be transferred.

Tags can be associated to up to four Data Logger Groups, which can have different sample periods and transfer periods.

Three "transfer" methods are currently supported; log files can be:

- copied to the SD card;
- transferred to an FTP server;
- sent to one or more email addresses, as an attachment.

One or more of the above methods can be enabled.

Log files are stored in the Z-PASS (flash) memory so, if one of the active transfer methods should temporarily fail, they can be successfully transferred later; for each data logger group, this internal log file "cache" can contain up to the limit which is reached first between the following two:

- 1000 log files
- (about) 100000/(number of enabled groups) samples (that is log file lines)

When the limit is reached, the log file "rotation" occurs, that is the oldest files are overwritten by the new ones.

Log files are standard "csv" files, which can be processed by Excel™ or other PC software.

Each log file has an "header" line containing:

- the "INDEX" string (optional)
- the "TYPE" string (optional)
- the "TIMESTAMP" string
- the tag names

The following lines contain:

- a progressive line index (optional)
- the "LOG" string (optional)

- the timestamp value
- the tag values

Here is a portion of a log file:

```
INDEX;TYPE;TIMESTAMP;ZPASS_DI;ZPASS_DO;ZPASS_DI_1;ZPASS_DI_2;ZPASS_DI_3;ZPASS_DI_4;ZPASS_DO_1;ZPASS_
DO_2;ZPASS_DO_3;ZPASS_DO_4;GPS_ERROR;GPS_HOUR;GPS_MINUTE;GPS_SECOND;GPS_DAY;GPS_MONTH;GPS_YEAR;GPS_L
ATITUDE;GPS_LONGITUDE;GPS_HDOP;GPS_ALTITUDE;GPS_COG;GPS_SPEED_KM;GPS_SPEED_KN;GPS_FIX;GPS_NUM_SAT;SH
M_TAG1;ZPASS2_105_TAG1;ZPASS2_106_TAG1;ZPASS2_106_TAG2
1;LOG;29/05/2018
09:49:00;0;0;0;0;0;0;0;0;0;0;7;48;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;5;0;32767;14;
11.5
2;LOG;29/05/2018
09:49:05;0;0;0;0;0;0;0;0;0;0;7;48;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;5;0;32767;14;
11.5
3;LOG;29/05/2018
09:49:10;0;0;0;0;0;0;0;0;0;0;7;48;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;5;0;32767;14;
11.5
4;LOG;29/05/2018
09:49:15;0;0;0;0;0;0;0;0;0;0;7;48;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;5;0;32767;14;
11.5
5;LOG;29/05/2018
09:49:20;0;0;0;0;0;0;0;0;0;0;7;48;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;5;0;32767;14;
11.5
6;LOG;29/05/2018
09:49:25;0;0;0;0;0;0;0;0;0;0;7;48;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;5;0;32767;14;
11.5
7;LOG;29/05/2018
09:49:30;0;0;0;0;0;0;0;0;0;0;7;48;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;5;0;32767;14;
11.5
8;LOG;29/05/2018
09:49:35;0;0;0;0;0;0;0;0;0;0;7;48;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;5;0;32767;14;
11.5
9;LOG;29/05/2018
09:49:40;0;0;0;0;0;0;0;0;0;0;7;49;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;4;0;32767;14;
11.5
10;LOG;29/05/2018
09:49:45;0;0;0;0;0;0;0;0;0;0;7;49;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;4;0;32767;14;
11.5
11;LOG;29/05/2018
09:49:50;0;0;0;0;0;0;0;0;0;0;7;49;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;4;0;32767;14;
11.5
12;LOG;29/05/2018
09:49:55;0;0;0;0;0;0;0;0;0;0;7;49;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;4;0;32767;14;
11.5
13;LOG;29/05/2018
09:50:00;0;0;0;0;0;0;0;0;0;0;7;49;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;4;0;32767;14;
11.5
```

If for a tag the actual value is not available (for example, if the tag corresponds to a register of a Modbus Station which is not responding to Modbus requests), the value written in the corresponding field of the log file can be (see 20.3.2.1 paragraph):

- the string "ERR!", if the "ERROR MODE" parameter for that tag is set to "LAST VALUE"
- the value defined in the "ERROR VALUE" parameter, if the "ERROR MODE" parameter for that tag is set to "ERROR VALUE"

Please note that any time a configuration change is made that affects the Data Logger functionality (from one of the pages in the "Data Logger" section), the following procedure is executed:

- the Data Logger processes are stopped
- the internal log file cache is cleaned
- the Data Logger processes are restarted

### 9.1 HTTP POST protocol

Z-PASS Data Logger is compatible with Seneca Cloud Box product[4], by means of the HTTP POST Communication protocol developed by Seneca.

This protocol features a set of HTTP POST (RESTFUL) APIs; the related documentation can be provided by Seneca to customers who wish to develop their own server-side software; for information, please contact Seneca Service & Support at support@seneca.it.

The HTTP POST protocol can be enabled along with the other transfer methods (SD, FTP, EMAIL); however, when the HTTP POST protocol is enabled, the following changes apply to the Data Logger behavior:

- only one logging group can be enabled;
- the sampling period shall be a multiple of 30 seconds;
- each sample is sent to the server (namely, the Cloud Box) in a *LOG* message, carried by an HTTP POST request.

The Seneca HTTP POST protocol also lets the server perform the following actions on the Z-PASS:

- setting the values of one or more tags
- restarting the device
- saving the device configuration on the server FTP site
- loading the device configuration from the server FTP site
- starting the FW Upgrade; the FW file is downloaded from the server FTP site
- starting the VPN Box functionality
- stopping the VPN Box functionality

There is an internal cache also for LOG messages sent via HTTP POST requests, used to store log messages while it's not possible to send them to the server; this cache can contain up to 3000 messages.

## 10 Alarms and Logic Rules

The device can be configured with a maximum of 2000 logic rules.

A logic rule is based on the following basic concept:

[4] For information about "Cloud Box" product, please see Seneca web site (www.seneca.it).

IF CONDITION(s) THEN ACTION(s) ELSE ACTION(s)

The “Then Action” is executed if the “If Condition” is true.

The “Else Action” is executed if the “If Condition” is false.

The “If Condition” can also be configured as an alarm.

A full set of parameters are available to define alarm behavior, as given in “Alarm Configuration” page (see paragraph 20.4.1); the whole alarm status can be viewed in “Alarm Summary” page (see paragraph 20.4.2) and the alarm history can be retrieved in “Alarm History” page (see paragraph 20.4.3).

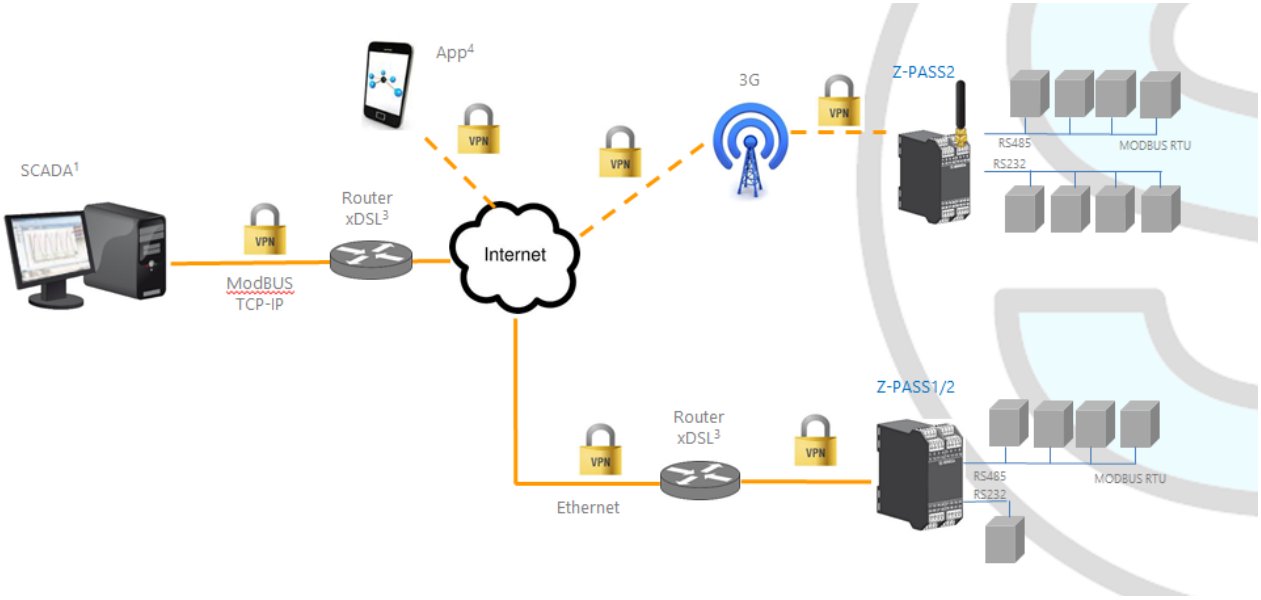
Furthermore, in the “Tag View” page, the “ALARM” and “ANALOG DANGER ALARM” columns show the current alarm status for each tag (see paragraph 20.3.2.4).

The Actions can be used for sending a SMS, EMAIL or HTTP POST;
In each rule can be configured:

- up to three logic conditions (based on alarm states) can be combined in an OR logic expression;
- up to three actions (sending alarms) can be executed.

For more info see chapter 20.6

# 11 VPN




Z-PASS supports the standard OpenVPN protocol.

The main advantages that come from using a VPN are:

- secure connections, since transported data are encrypted;

- the ability to establish connections without interfering with the corporate LAN;
- no need to have a static/public IP address on the WAN side;
- remote configurability by a built-in Web Server.

Two “VPN modes“ are available, named “OpenVPN” and “VPN Box”, respectively.

The “OpenVPN” mode can be used when the Z-PASS shall be installed in an already existing VPN. In this case, an OpenVPN server shall be available and the configuration, certificate and key files for the Z-PASS client shall be provided by the VPN administrator; the files can be uploaded to the Z-PASS using the “VPN configuration” page of Z-PASS Web Server.

If the VPN infrastructure does not exist yet, the advisable choice is to adopt the “VPN Box” solution, developed by Seneca. The “VPN Box” is an hardware appliance (or a virtual machine) which lets the user easily setup two alternative kinds of VPN:

- “Single LAN” VPN
- “Point-to-Point” VPN

In the “Single LAN” VPN, all devices and PCs (and associated local subnets) configured into VPN are always connected in the same network. In this scenario any PC Client can connect to any device (Z-PASS) and to other machines which lie in the Z-PASS LAN, but also any device/machine can connect to any other remote device/machine which belongs to the same VPN network. This VPN architecture puts some constraints on the device sub-networks definition, in fact all VPN clients must have a different IP address and different local LAN, to avoid conflicts. The software named “VPN BOX Manager” configures VPN BOX and will help you to avoid errors defining local subnet.

In the “Point-to-Point” VPN, a client PC, in a given moment, can perform a single connection, on demand, to only one device (Z-PASS) (and to machines which lie in the Z-PASS LAN) at time. Furthermore, devices can’t communicate each other also if they belong to the same VPN. The advantage of this architecture is that the same sub-network can be used in all sites. Point to point mode makes it possible to define user groups and manage them. This VPN modality must be configured on “VPN Box” by VPN BOX Manager.

There are two kinds of “Point-to-Point” VPN:

- routing Layer 3 VPN
- bridging Layer 2 VPN

In “Routing Layer 3 VPN”, only IP (Layer 3) packets are transported over the VPN tunnel and a new virtual LAN is created with a network subnet which must be different from the LAN subnets of the server and clients.

Conversely, in “Bridging Layer 2 VPN”, all Ethernet frames are transported over the VPN tunnel and the clients are inserted in the server LAN.

Each of the two kinds has benefits and drawbacks:

Layer 2 benefits/drawbacks:

- can transport any network protocol
- broadcast traffic (e.g.: DHCP) is transported

- causes much more traffic overhead on the VPN tunnel

Layer 3 benefits/drawbacks:

- can transport only IP traffic
- broadcast traffic (e.g.: DHCP) is not transported
- lower traffic overhead, transports only traffic which is destined for the VPN clients

The "VPN Box" is supplied with two Windows applications:

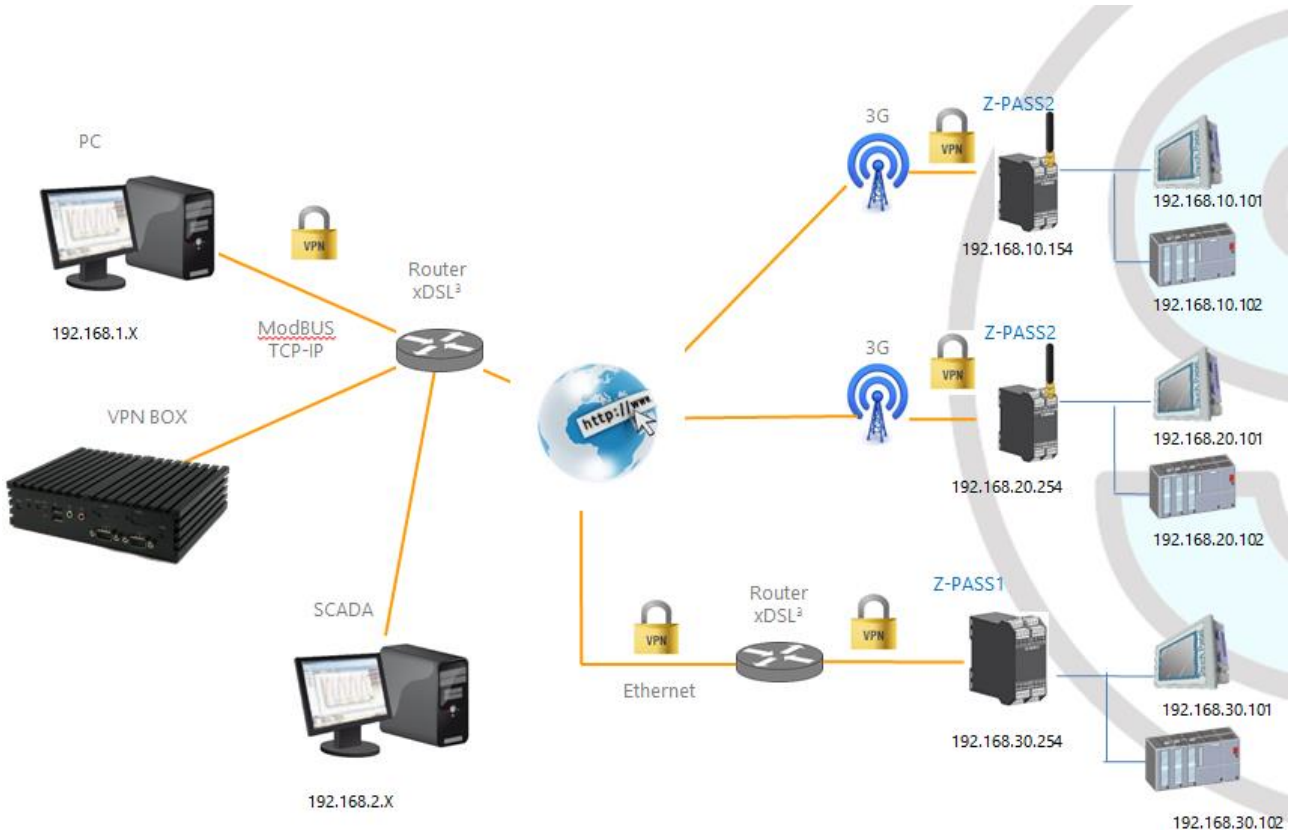
- the "VPN Box Manager", which allows to configure the VPN[5] mode on the VPN Box and manage the devices
- the "VPN Client Communicator", which lets the user connect the PC to the network (in the "Single LAN" case) or to a specific device (in the "Point-to-Point" case)

A detailed description of "VPN Box" can be found in the "VPN Box User Manual".

A detailed description of Z-PASS VPN configuration parameters is given in 20.1.7 paragraph.

The following two sub-paragraphs give some more info about the two kinds of VPN.

## *11.1 "Single LAN" VPN*




[5] Only one of the two kinds of VPN can be configured on a given VPN Box.

The above figure gives an example of a “Single LAN” VPN.

The client PC (with IP address 192.168.1.X) can connect, just as an example, to the first Z-PASS2 by using its 192.168.10.154 IP address and to the PLC in the Z-PASS LAN by using its local IP address 192.168.10.102.

Also, two devices which lie in two different LANs of the same VPN network (e.g.: 192.168.10.101 and 192.168.20.102) can connect to each other, again using their local IP addresses.

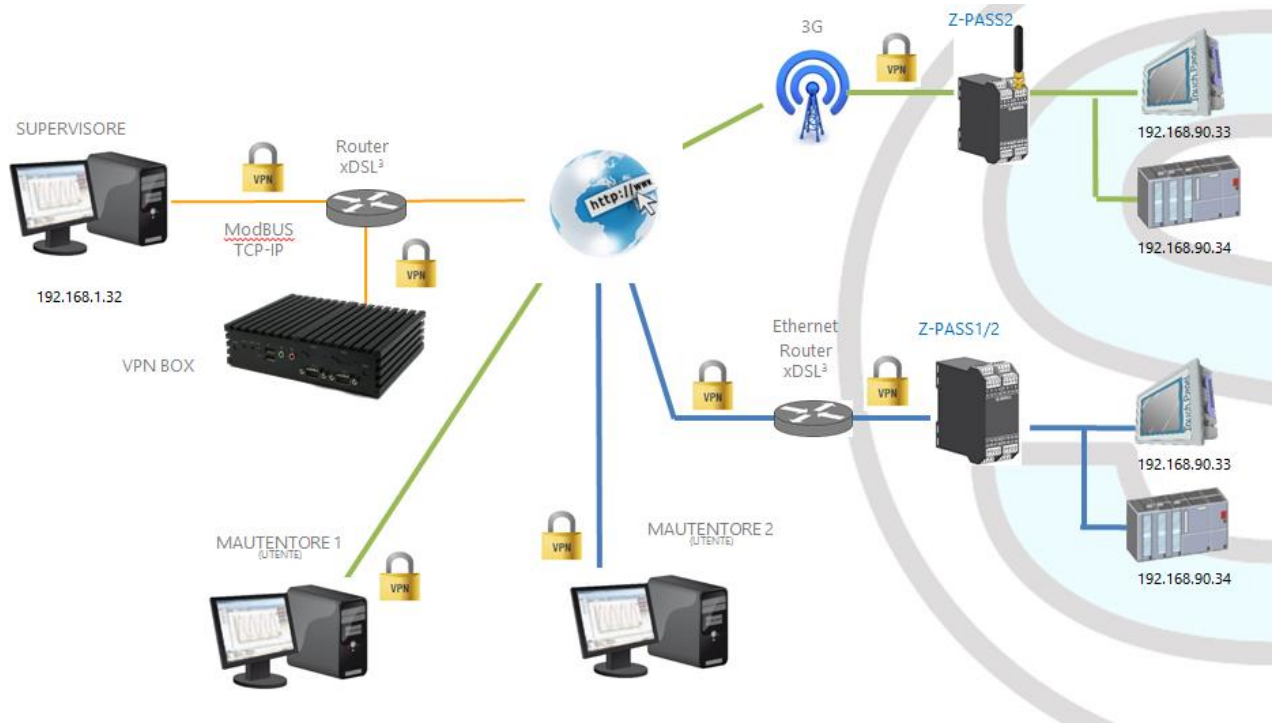
To let this scenario work correctly, an essential rule must always be followed: the Z-PASS LANs and the PC LAN shall have different and not colliding subnets; so, in the above figure, the following subnets allocation has been depicted:

| | |
|---|---|
| PC LAN | 192.168.1.0/24 |
| SCADA LAN | 192.168.2.0/24 |
| Z-PASS2 LAN | 192.168.10.0/24 |
| Z-PASS2 LAN | 192.168.20.0/24 |
| Z-PASS1 LAN | 192.168.30.0/24 |

The “VPN Box Manager” application guides you in the configuration task, checking that no subnet/IP address conflict is present in the network.

If subnet/conflicts cannot be avoided, using a “Single LAN” VPN is still possible if local IP addresses are not used; devices can be reached by means of their VPN IP addresses and machines beyond them can be reached by configuring some “port forwarding” rules on the Device Router (see 20.1.8 paragraph).

## *11.2 “Point-to-Point” VPN*



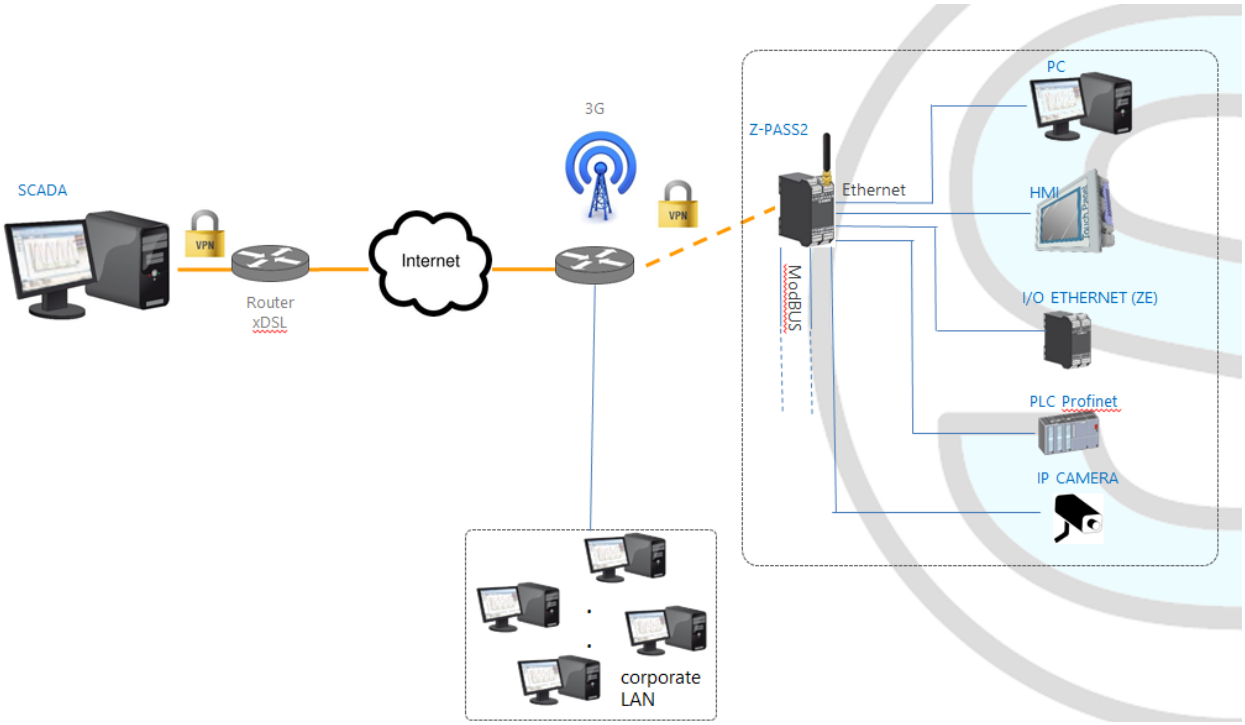
The above figure gives an example of a “Point-to-Point” VPN.

In this scenario a PC (acting as a VPN Client) can connect, on demand, to only one Z-PASS and its subnet, using local IP addresses. Since the client “sees” just one Z-PASS (and attached devices) at time, the same subnet configuration can be assigned to different sites, without creating conflicts.

For this kind of VPN, the “VPN Box Manager” application lets define group of users that can connect only to assigned devices.

The “VPN Client Communicator” application retrieves the list of devices which are available for the logged user; then the user can select one device on the list and connect to it.

# 12 Router




As already told before, “Router” functionality routes packets between the LAN (Ethernet) interface and the WAN (Mobile Network) interface; so, this functionality specially makes sense when a mobile connection is active, which needs the availability of a 3G modem (true for Z-PASS2).

More specifically, an important feature of the Router is what is known as “IP forwarding”; this means that when Z-PASS receives a packet not targeted for it, it does not discard the packet but forwards it to its actual destination; when a packet is routed from the LAN to the WAN, Z-PASS also performs what is known as “IP masquerading”, meaning that the original source IP address is replaced with the IP address of the WAN (PPP) interface.

Another important feature is the availability of a DNS server/forwarder, which can resolve names either by itself or querying the external configured DNS server.

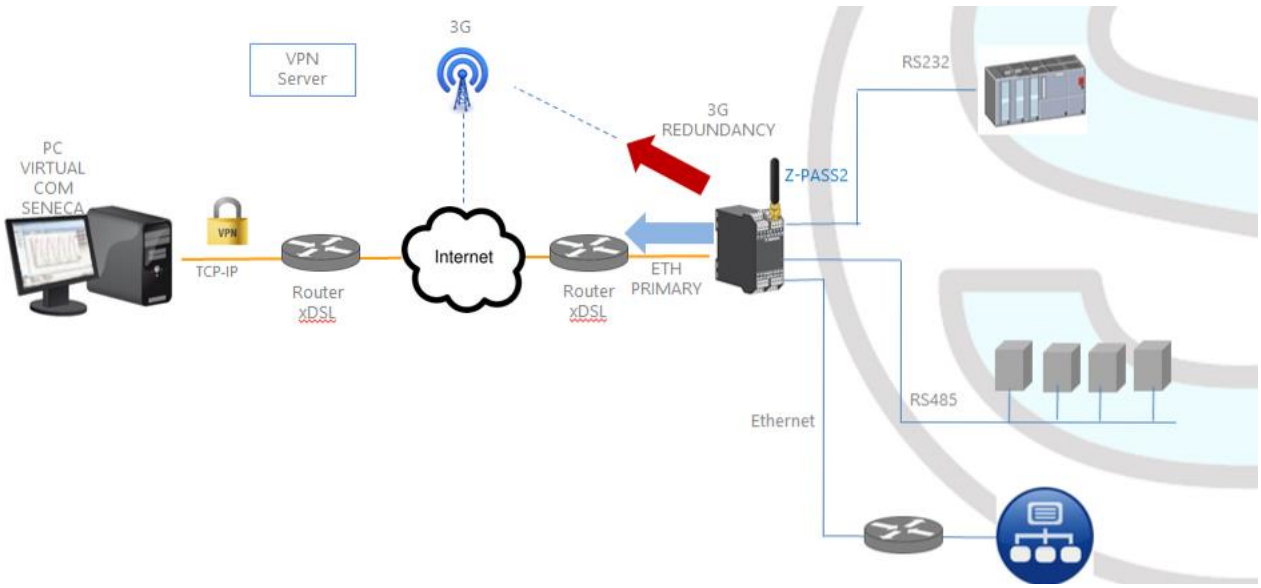
Also, a DHCP server is available which assigns IP addresses to clients connected on the Z-PASS LAN; here, you can configure the range of addresses used by the server and the lease time.

There is also the possibility to define up to five “Port Forwarding” rules or “Virtual Servers”; using these rules, you can, for example, redirect packets received from a TCP or UDP port to another Z-PASS port or to another machine, with a different IP address, on the same or another port.

As an alternative to using “Port Forwarding” rules, Router + VPN functionalities allow the use of local addresses, as shown in the previous chapter; in the router configuration, a flag is given to enable this feature.

A detailed description of the Router configuration can be found in 20.1.8 paragraph.

# 13 Network Redundancy




“Network Redundancy” is a functionality than can be enabled on Z-PASS2 devices, where a 3G modem is available.

This functionality is aimed at switching the network interface used to access the Internet from the Ethernet (“primary” interface) to the Mobile/3G (“secondary” interface), when Internet access through the primary interface becomes unavailable; when access through the primary interface become available again, the network interface is switched back to Ethernet.

The parameters provided to configure Network Redundancy are explained in paragraph 20.1.2 “Network and Services”.

# 14 Remote Connection Disable

Z-PASS1 and Z-PASS2 products provide a dedicated digital input and a dedicated digital output to control and monitor remote connection to the device.

In details:

- when “Remote Connection Disable” digital input is set to HIGH state, remote connection to the device is disabled; conversely, when “Remote Connection Disable” digital input is set to LOW state, remote connection to the device is enabled; “Remote Connection Disable” digital input state is reported by the “RCD” LED;
- “Remote Connection Active” digital output is set to HIGH state when the device is remotely accessed (VPN connection is active); it is set to LOW state when VPN connection is not active.

Four levels of security can be configured to disable remote connection:

- Level 1 (“VPN Connection”): VPN connections are disabled in any VPN mode (VPN Box Point-to-Point, VPN Box Single LAN, OpenVPN), but VPN Box Service is still running, so the device can still be monitored on VPN Box Manager;
- Level 2 (“VPN Service”): VPN Box Service is disabled, but the device can still access the Internet and send/receive SMSs;
- Level 3 (“Internet Connection”): any Internet access is disabled, but the device can still send/receive SMSs;
- Level 4 (“SMS Service”): modem is off, so SMSs can’t be sent/received.

See “Digital I/O Configuration” paragraph to learn how to set the desired security level.

# 15 Auto-APN

The Auto-APN feature lets the Z-PASS establish mobile data connections without requiring the user to configure APN data[6] for the SIM in use.

This is accomplished by using the SIM IMSI and, possibly, some other data available on the SIM, to select the proper APN record in an internal DB[7], containing APN records for all mobile operators in the world.

In some particular cases, however, when a “custom APN” shall be used, the Auto-APN feature can be disabled, setting the “APN Mode” parameter to “Manual”, in the “Mobile Network” page (see paragraph 20.2).

[6] APN data are: APN, Username, Password and Authentication Type.
[7] This DB is updated to the one used in the last Android O.S. version.

# 16 HTTP POST Communication protocol

The communication between RTU and Cloud takes place on HTTP protocol by a POST-type call. The representation of the call is REST (REpresentational State Transfer) where data are configured as those of a classical web FORM but via JSON (JavaScript Object Notation). For more info on the HTTP POST Communication Protocol refers to "Seneca HTTP POST Communication Protocol" (you can request the document from support@seneca.it).

# 17 OPC Unified Architecture (OPC-UA) server protocol

OPC Unified Architecture (OPC-UA) is a standardized machine to machine communication protocol for industrial 4.0 automation developed by the OPC Foundation.

OPC-UA is a vendor-independent communication protocol and it's based on the client-server principle.

Z-PASS devices support the OPC-UA server protocol also with security policy.

In particular, Z-PASS OPC-UA server "exports" the Modbus Shared Memory Gateway tags; so, using an OPC-UA Client software, you can read/write the tags by means of the OPC-UA protocol

# 18 MQTT client protocol

The MQTT is the most used protocol for IOT applications:

*"MQTT stands for MQ Telemetry Transport. It is a publish/subscribe, extremely simple and lightweight messaging protocol, designed for constrained devices and low-bandwidth, high-latency or unreliable networks. The design principles are to minimise network bandwidth and device resource requirements whilst also attempting to ensure reliability and some degree of assurance of delivery. These principles also turn out to make the protocol ideal of the emerging "machine-to-machine" (M2M) or "Internet of Things" world of connected devices, and for mobile applications where bandwidth and battery power are at a premium".*

For more info on MQTT protocol see http://mqtt.org/

The MQTT version supported by the Z-PASS1/2 is the 3.1.1

# 19 SMS Commands

On Z-PASS devices, a number of features can be controlled by means of “SMS commands”; such features include setting up a mobile data (PPP) connection, activating the VPN Box functionality, setting a digital output etc.

SMS Commands can be sent by phone numbers that are present in the Z-PASS Phonebook as “admin” or “manager” users; as an alternative, any phone number can send an SMS command, provided that the command contains a “password”; the password is made by the last four digits of the Z-PASS modem IMEI; so the command will have the following format (there must be a blank character between the “password” and the command text):

```
<last four IMEI digits> <command text>
```

Example:

```
6172 PPP ON
```

Please note that the command text can be written in any letter case, all uppercase, all lowercase or a mix between the two.

Any SMS command received from a number that is not recognized as an “admin” or “manager” user and does not contain the password will be discarded; as an option, these messages and all messages that are not recognized as valid commands can be “relayed” to the “admin” user (see paragraph 20.6.2).

Example:

```
PPP ON RELAYED
```

SMS commands substantially fall into two categories:

- “set” commands which execute an action
- “get” commands which ask for some information

While “get” commands always have an answer, “set commands” can be given an answer (“acknowledge”) or not, depending on a configuration parameter (see paragraph 20.6.2).

Any response to a command, both “set” or “get”, will contain the original message text, plus a result string, which can be:

“EXECUTING”
meaning that the command has been correctly processed; the “ING” form is used to tell that the procedure started by the command might not be completed yet

“FAILED”
meaning that the command could not be processed or something failed; in this case, an error string is present giving the failure reason

Examples:

```
PPP ON EXECUTING (100.70.179.88)
PPP ON FAILED (System PPP ON)
```

Obviously, the response to a “get” command also contains the requested info, if the command has been successfully processed.

Example:

```
GET DIN EXECUTING (1,0,0,0)
```

Finally, the whole SMS commands functionality can be disabled, if not needed, by means of a configuration parameter (see paragraph 20.6.2).

Obviously, SMS commands are available only in Z-PASS2 product (for all HW revisions), where a GSM model is available.

In the following paragraphs, the full list of supported commands is given along with the corresponding responses.

## *19.1 PPP ON*

This command can be used to setup the mobile data (PPP) connection; the connection is setup using system configuration parameters (APN Mode, APN, Auth Type etc.).

If the command is successfully processed, the response contains the IP address assigned to the PPP network interface.

This command is rejected in the following case:

- if “Remote Connection Disable” (RCD) digital input is HIGH and “Security Level/Service Disable” parameter is set to “Internet Connection”, the command will fail with the "Security Level error” error.

Also, if the connection setup procedure is not completed after a timeout (currently fixed to 30 seconds), the command will fail with the “Timeout error” error.

Please note that this command that does not enable the mobile data connection in a persistent way, so if the Z-PASS is restarted, the mobile data (PPP) connection is not re-established.

Example:

```
→     PPP ON
←     PPP ON EXECUTING (100.70.179.88)
```

## *19.2 PPP OFF*

This command can be used to drop down the mobile data (PPP) connection setup by a previous “PPP ON” command.

Please note that this command that does not disable the mobile data connection in a persistent way, so if the Z-PASS is restarted, the mobile data (PPP) connection is re-established.

This command is never rejected.

Example:

```
→     PPP OFF
←     PPP OFF EXECUTING
```

### 19.3 PPP IP

This command can be used to get the IP address assigned to the mobile data (PPP) connection; if the PPP connection is not active, the "dummy" IP address (0.0.0.0) will be given.

This command is never rejected.

Example:

```
→     PPP IP
←     PPP IP EXECUTING (100.70.179.88)
```

### 19.4 PPP CNF

This command can be used to change the value of the system configuration parameters related to the mobile data (PPP) connection; the changes are persistent.

The command shall have the following format, where parameter values shall be separated by a blank character:

```
PPP CNF <APN mode> <APN> <Authentication Type> <Username> <Password> <PPP Connection Testing IP Address>
```

Please note that all the parameters shall be present, in the above order; no parameter can be left empty.

For the meaning of these parameters, please see 20.2 paragraph.

<APN> and <Authentication Type> are numeric fields with the following values.

```
APN Mode
0:    Automatic
1:    Manual

Authentication Type
0:    None
1:    CHAP/PAP
2:    CHAP only
3:    PAP only
```

This command is rejected in the following case:

- if any of the command parameters is missing or invalid, the command will fail with the "Command parameter error".

Example:

```
→     PPP CNF 0 mobile.vodafone.it 0 user pass www.google.com
←     PPP CNF EXECUTING
```

## *19.5 VPN ON*

This command can be used to activate the VPN Box functionality; the functionality is activated using system configuration parameters (Server, Password, Tag Name).

The command has two optional parameters, so its format is the following:

`VPN ON [PPP] [NOFWL]`[8]

"PPP"
if this parameter is present, the mobile data (PPP) connection is setup (if it's not already active), before activating the VPN Box functionality

"NOFWL"
if this parameter is present, the "Mobile Network Firewall" is disabled, in the system configuration

This command is rejected in the following cases:

- if the "custom" VPN functionality is enabled in the system configuration (parameter "VPN/Enable" = ON, "VPN Mode" = "OpenVPN"), the command will fail with the "System VPN ON" error;
- if "Remote Connection Disable" (RCD) digital input is HIGH and "Security Level/Service Disable" parameter is set to "VPN Connection" or "VPN Service" or "Internet Connection", the command will fail with the "Security Level error" error.

Please note that this command that does not activate the VPN Box functionality in a persistent way, so if the Z-PASS is restarted, the functionality is not re-activated.

Examples:

```
→     VPN ON
←     VPN ON EXECUTING

→     VPN ON PPP
←     VPN ON PPP EXECUTING

→     VPN ON NOFWL
←     VPN ON NOFWL EXECUTING

→     VPN ON PPP NOFWL
←     VPN ON PPP NOFWL EXECUTING
```

[8] Square brackets tell that parameter is optional.

### 19.6 VPN OFF

This command can be used to deactivate the VPN Box functionality activated by a previous "VPN ON" command; it also drops down the mobile data (PPP) connection setup by a previous "VPN ON PPP" command or "PPP ON" command.

This command is never rejected.

Please note that this command that does not de-activate the VPN Box functionality in a persistent way, so if the Z-PASS is restarted, the functionality is re-activated.

Example:

```
→     VPN OFF
←     VPN OFF EXECUTING
```

### 19.7 VPN CNF

This command can be used to change the value of the system configuration parameters related to the VPN Box; the changes are persistent.

The command shall have the following format, where parameter values shall be separated by a blank character:

```
VPN CNF <Server> <Password> <Tag Name>
```

Please note that all the parameters shall be present, in the above order; no parameter can be left empty.

For the meaning of these parameters, please see 20.1.7.2 paragraph.

This command is rejected in the following case:

- if any of the command parameters is missing or invalid, the command will fail with the "Command parameter error".

Example:

```
→     VPN CNF myvpnbox.seneca.it myvpnbox zpass2-GSP
←     VPN CNF EXECUTING
```

### 19.8 FWL ON

This command can be used to enable the "Mobile Network Firewall" in the system configuration (parameter "Mobile Network Firewall/Enable" = ON).

This command is never rejected.

Example:

```
→     FWL ON
←     FWL ON EXECUTING
```

## 19.9 FWL OFF

This command can be used to disable the "Mobile Network Firewall" in the system configuration (parameter "Mobile Network Firewall/Enable" = OFF).

This command is never rejected.

Example:

```
→     FWL OFF
←     FWL OFF EXECUTING
```

## 19.10 GET DIN

This command can be used to get the status of one or all of the four digital inputs; if a digital input is not available (since it is used as an output)[9], the "0" value is given.

The command can have two formats:

| | | |
|---|---|---|
| `GET DIN<n>` | with <n>=1..4 | get the status of a single digital input |
| `GET DIN` | | get the status of all the digital inputs |

This command is rejected in the following cases:

- if the command is received on a Z-PASS2, Z-PASS2-R01 device, which has no digital I/Os, the command will fail with the "Digital I/O not available" error;
- if the digital I/O number in the command is out of range (e.g.: 0 or 5), the command will fail with the "Command parameter error" error.

Examples:

```
→     GET DIN
←     GET DIN EXECUTING (1,0,0,0)

→     GET DIN1
←     GET DIN1 EXECUTING (1)

→     GET DIN2
←     GET DIN2 EXECUTING (0)
```

## 19.11 GET DOUT

This command can be used to get the status of one or all of the four digital outputs; if a digital output is not available (since it is used as an input)[10], the "0" value is given.

[9] This can be true for DI3 an DI4.
[10] This can be true for DO3 an DO4.

The command can have two formats:

| | | |
|---|---|---|
| `GET DOUT<n>` | with <n>=1..4 | get the status of a single digital output |
| `GET DOUT` | | get the status of all the digital outputs |

This command is rejected in the following cases:

- if the command is received on a Z-PASS2, Z-PASS2-R01 device, which has no digital I/Os, the command will fail with the "Digital I/O not available" error;
- if the digital I/O number in the command is out of range (e.g.: 0 or 5), the command will fail with the "Command parameter error" error.

Examples:

```
→     GET DOUT
←     GET DOUT EXECUTING (0,1,0,0)

→     GET DOUT1
←     GET DOUT1 EXECUTING (0)

→     GET DOUT2
←     GET DOUT2 EXECUTING (1)
```

## 19.12 SET DOUT

This command can be used to set the status of one of the four digital outputs.

The command can have two formats:

| | | |
|---|---|---|
| `SET DOUT<n>.CLOSE` | with <n>=1..4 | set the digital output to the HIGH state |
| `SET DOUT<n>.OPEN` | with <n>=1..4 | set the digital output to the LOW state |

This command is rejected in the following cases:

- if the command is received on a Z-PASS2, Z-PASS2-R01 device, which has no digital I/Os, the command will fail with the "Digital I/O not available" error;
- if the digital output is not configured as "General output" or the digital I/O is used as an input[11], the command will fail with the "Digital I/O mode error" error;
- if the digital I/O number in the command is out of range (e.g.: 0 or 5), the command will fail with the "Command parameter error" error;
- if the requested state is neither ".CLOSE", nor ".OPEN", the command will fail with the "Command parameter error" error.

Example:

```
→     SET DOUT2.CLOSE
```

[11] This can be true for DO3 and DO4.

```
←     SET DOUT2.CLOSE EXECUTING
```

## 19.13 SET PULSE

This command can be used to generate a pulse on one of the four digital outputs.

The command can have two formats:

`SET PULSE<n>.CLOSE <duration>` with <n>=1..4
to generate a LOW-HIGH-LOW pulse, with the HIGH state set for the number of seconds given by the <duration> parameter

`SET PULSE<n>.OPEN <duration>` with <n>=1..4
to generate a HIGH-LOW-HIGH pulse, with the LOW state set for the number of seconds given by the <duration> parameter

This command is rejected in the following cases:

- if the command is received on a Z-PASS2, Z-PASS2-R01 device, which has no digital I/Os, the command will fail with the "Digital I/O not available" error;
- if the digital output is not configured as "General output" or the digital I/O is used as an input[12], the command will fail with the "Digital I/O mode error" error;
- if the digital I/O number in the command is out of range (e.g.: 0 or 5), the command will fail with the "Command parameter error" error;
- if the requested state is neither ".CLOSE", nor ".OPEN", the command will fail with the "Command parameter error" error;
- if the <duration> parameter is missing or invalid, the command will fail with the "Command parameter error" error;
- if the ".CLOSE" parameter is given and the digital output is already in the HIGH state, the command will fail with the "No pulse generated" error;
- if the ".OPEN" parameter is given and the digital output is already in the LOW state, the command will fail with the "No pulse generated" error.

Example:

```
→     SET PULSE2.CLOSE 10
←     SET PULSE2.CLOSE 10 EXECUTING
```

## 19.14 SET USER.PHONE

This command can be used to insert a user with the specified telephone number, type and group list into the Phonebook; it can also be used to change the type and/or group list of an already existing user.

[12] This can be true for DO3 and DO4.

The command has the following format:

`SET USER.PHONE +<number> <type> <group list>,` with <type>=`ADM|MGR|USR`

Please note that the telephone number shall always be given in the "international format", so the initial '+' character shall always be present.

The "group list" is a list of non-negative integer numbers, separated by the "-" character, defining the groups which the user belongs to. Example of valid group lists are:

"1-2-3"
"1-4"
"1"
"0"

The "0" value means that the user is part of any group.

This command is rejected in the following cases:

- if the specified <number> already exists in the Phonebook, with the specified <type> and <group list>, the command will fail with the "Item already exists" error;
- if the <number> parameter is missing or invalid (including the case when the '+' character is missing), the command will fail with the "Command parameter error" error;
- if the <type> parameter is missing or invalid, the command will fail with the "Command parameter error" error;
- if the <group list> parameter is missing or invalid, the command will fail with the "Command parameter error" error.

Example:

```
→     SET USER.PHONE +390123456789 ADM 1-2-3
←     SET USER.PHONE +390123456789 ADM 1-2-3 EXECUTING
```

## *19.15 RESET PHONE*

This command can be used to delete a user with the specified telephone number from the Phonebook.

The command has the following format:

`RESET PHONE +<number>`

Please note that the telephone number shall always be given in the "international format", so the initial '+' character shall always be present.

This command is rejected in the following cases:

- if the specified <number> does not exist in the Phonebook, the command will fail with the "Item does not exist" error;

- if the <number> parameter is missing or invalid (including the case when the '+' character is missing), the command will fail with the "Command parameter error" error.

Example:

```
→     RESET PHONE +390123456789
←     RESET PHONE +390123456789 EXECUTING
```

Please note that, if the Phonebook user with the specified telephone number also has an email address, this will be deleted by the command too.

## 19.16 SET USER.EMAIL

This command can be used to insert a user with the specified email address, type and group list into the Phonebook; it can also be used to change the type and/or group list of an already existing user.

The command has the following format:

`SET USER.EMAIL <email address> <type> <group list>`, with <type>=ADM|MGR|USR

The "group list" is a list of non-negative integer numbers, separated by the "-" character, defining the groups which the user belongs to. Example of valid group lists are:

"1-2-3"
"1-4"
"1"
"0"

The "0" value means that the user is part of any group.

This command is rejected in the following cases:

- if the specified <email address> already exists in the Phonebook, with the specified <type> and <group list>, the command will fail with the "Item already exists" error;
- if the <email address> parameter is missing or invalid, the command will fail with the "Command parameter error" error;
- if the <type> parameter is missing or invalid, the command will fail with the "Command parameter error" error;
- if the <group list> parameter is missing or invalid, the command will fail with the "Command parameter error" error.

Example:

```
→     SET USER.EMAIL admin@zpass.it ADM 1-2-3
←     SET USER.EMAIL admin@zpass.it ADM 1-2-3 EXECUTING
```

## 19.17 RESET EMAIL

This command can be used to delete a user with the specified email address from the Phonebook.

The command has the following format:

```
RESET EMAIL <email address>
```

This command is rejected in the following cases:

- if the specified <email address> does not exist in the Phonebook, the command will fail with the "Item does not exist" error;
- if the < email address > parameter is missing or invalid, the command will fail with the "Command parameter error" error.

Example:

```
→     RESET EMAIL admin@zpass.it
←     RESET EMAIL admin@zpass.it EXECUTING
```

Please note that, if the Phonebook user with the specified email address also has a telephone number, this will be deleted by the command too.

### *19.18 STATUS*

This command can be used to get some status information from the device.

The status info given in the response has the following format:

```
Z-PASS2<hwrev>     <date>     <time>     RUNNING     <service     status>,<vpn     status>
<DI1>,<DI2>,<DO1>,<DO2>,<DIDO1>,<DIDO2>
```

where:

<hwrev>: "", "-R01", "-IO"
<date> is in the form "yyyy/mm/dd"
<hour> is in the form "hh:mm:ss"
<service status> reports the status of the "SERV" LED[13] ("OFF"|"ON"|"FAIL")
<vpn status> reports the status of the "VPN" LED ("OFF"|"ON"|"FAIL")
<DI1>,<DI2>,<DO1>,<DO2>,<DIDO1>,<DIDO2> status ("LO"|"HI") of the digital I/Os (only for Z-PASS2–IO)

This command is never rejected.

Example:

```
→     STATUS
←     STATUS  EXECUTING  (Z-PASS2-IO  2018/03/09  08:01:31  RUNNING  OFF,OFF
HI,LO,HI,LO,LO,LO)
```

[13] See Chapter "LEDs signaling".

### 19.19 GET GPS

This command can be used to get GPS location info from the device.

The response is given as an URL to Google Maps™:
https://www.google.com/maps/?q=<latitude>,<longitude>

This command is rejected in the following cases:

- if the command is received on a Z-PASS2, Z-PASS2-R01 device, which does not have a GPS module, the command will fail with the "GPS not available" error;
- If the GPS signal is not available, the command will fail with the "GPS not fixed" error.

Example:

```
→     GET GPS
←     GET GPS EXECUTING (https://www.google.com/maps/?q=45.3742,11.94557)
```

### 19.20 RESET

This command can be used to restart ("reboot") the device.

This command is never rejected.

Example:

```
→     RESET
←     RESET EXECUTING
```

### 19.21 GET TAG

This command can be used to get the value of a tag (see "Modbus Shared Memory Gateway" functionality in chapter 8).

The command has the following format:

```
GET TAG <tag name>
```

Please note that the "tag name" is case-sensitive; also note that this command assumes that each tag has a distinct name; if more tags exist with the same name, this command returns the value of the first tag found with the given name.

The value is given in the response with the following format:

```
<tag value>,VALID
```

or:

```
<tag value>,INVALID
```

The “INVALID” status may occur for tags with “GATEWAY MODE”=”GATEWAY”, when the last Modbus read request has failed.

This command is rejected in the following cases:

- if no serial port has “Gateway Mode”=”Modbus Shared Memory”, the command will fail with the “Modbus Gateway not active” error;
- if no tag is found with the given name, the command will fail with the “Tag does not exist” error;
- if the requested tag has “GATEWAY MODE”=”BRIDGE” and the Modbus read request fails, the command will fail with the “Tag operation failed” error.

Example:

```
→     GET TAG GPS_LONGITUDE
←     GET TAG GPS_LONGITUDE EXECUTING (11.94528,VALID)
```

## *19.22 SET TAG*

This command can be used to set the value of a tag (see “Modbus Shared Memory Gateway” functionality in chapter 8).

The command has the following format:

```
SET TAG <tag name> <tag value>
```

Please note that the “tag name” is case-sensitive; also note that this command assumes that each tag has a distinct name; if more tags exist with the same name, this command tries to set the value of the first tag found with the given name.

For non-integer tag values, the decimal point character ‘.’ shall be used.

This command is rejected in the following cases:

- if no serial port has “Gateway Mode”=”Modbus Shared Memory”, the command will fail with the “Modbus Gateway not active” error;
- if no tag is found with the given name, the command will fail with the “Tag does not exist” error;
- if the given value does not fit the “Data Type” of the target tag (e.g. the “2” value for a “BOOL” tag), the command will fail with the “Invalid value for tag” error;
- if, for any reason, the write operation fails, the command will fail with the “Tag operation failed” error; this includes the following cases:
    - the Modbus write request fails, for “GATEWAY” or “BRIDGE” tags;
    - the tag value cannot be changed, since it is not a “General output”, for Digital I/Os (“EMBEDDED”) tags;
    - the tag value cannot be changed, since it is a “GPS info” (“EMBEDDED”) tag.

Example:

→ SET TAG ZPASS_DO 10

← SET TAG ZPASS_DO 10 EXECUTING

### 19.23 OVPN ON

This command can be used to activate the standard OPEN VPN functionality; the functionality is activated using system configuration parameters (Server, Password, Tag Name).

Please note that this command that does not activate the OPEN VPN functionality in a persistent way, so if the Z-PASS is restarted, the functionality is not re-activated.

Examples:

→ VPN ON

### 19.24 OVPN OFF

This command can be used to deactivate the OPEN VPN functionality activated by a previous "OVPN ON" command.

Please note that this command that does not de-activate the OPEN VPN functionality in a persistent way, so if the Z-PASS is restarted, the functionality is re-activated.

Example:

→ OVPN OFF

### 19.25 CLEAN LOGS

This command will delete all logs.

### 19.26 Initial Configuration

This paragraph describes a possible procedure to configure a new Z-PASS device, starting from "factory default" situation.

Firstly, a SIM with PIN check disabled is needed; this SIM shall also be usable with Auto-APN feature (that is it should not require a private custom APN); obviously, the SIM shall support SMS service.

Since no user is present in the Phonebook yet, SMS commands shall be sent with the password, so the modem IMEI shall be known.

If the previous conditions are satisfied, only two commands are needed to let the device connect to the VPN Box; these are:

```
<password> VPN CFG <parameters>
<password> VPN ON PPP
```

Once these commands are successfully processed, the new device appears in the device list presented by the VPN Box Manager SW; after inserting the device in a user's group (in case of Point-to-Point VPN Box) or applying the device configuration (in case of Single-LAN VPN Box), the device will be reachable via the VPN, letting the user fully configure it.

# 20 Web Configuration Pages

Z-PASS can be fully configured by means of a set of web configuration pages.

To access Z-PASS configuration site, you have to connect the browser to the Z-PASS IP address on port 8080, e.g.:

http://192.168.90.101:8080

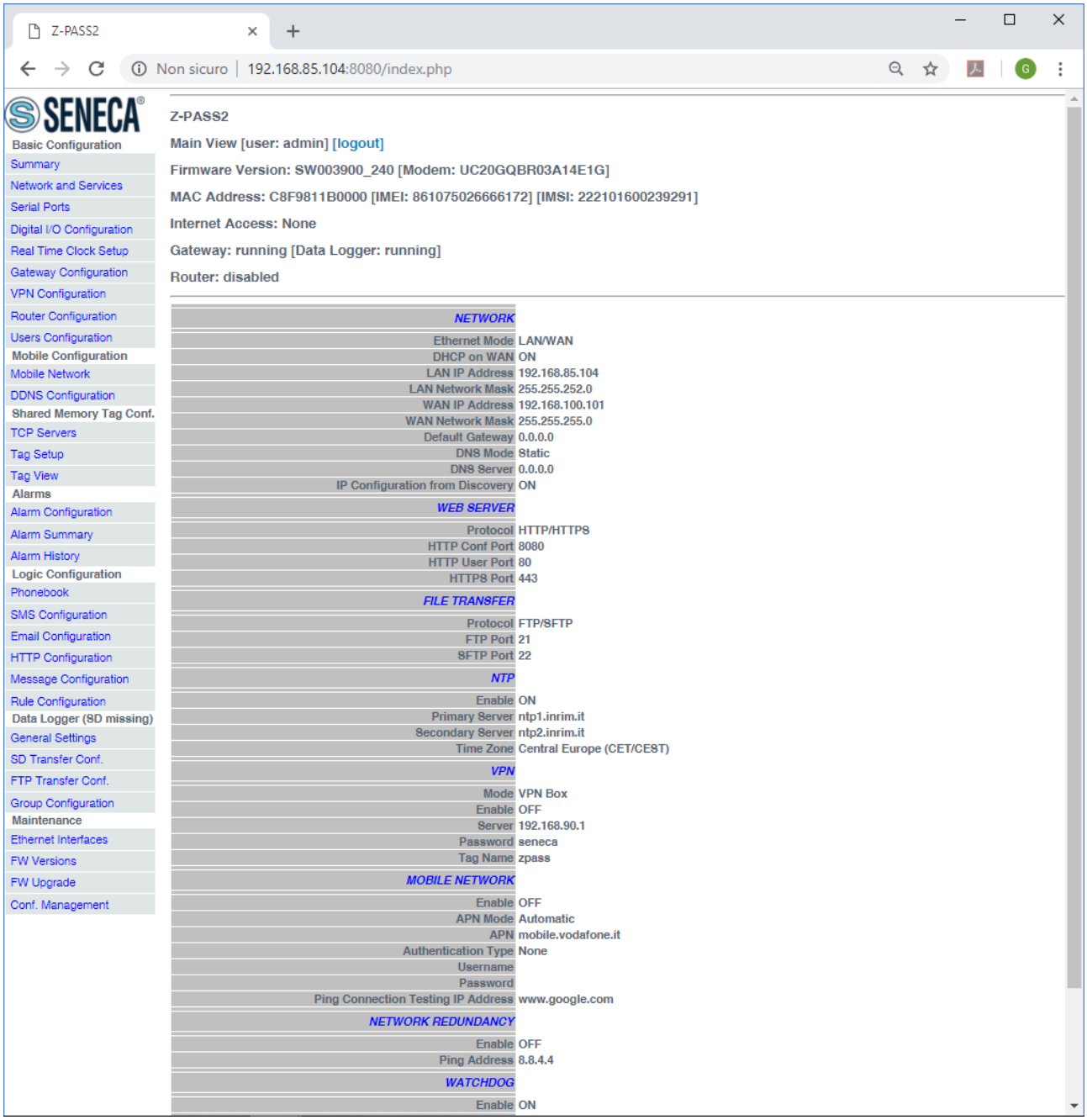
and, when asked, provide the following credentials (default values):

Username: admin
Password: admin

You come to the "Summary" page, described in the following paragraph.

## 20.1 Basic Configuration

### 20.1.1 Summary




In this page, main Z-PASS configuration parameters are shown, with their current values.

On the left side of the page, like in any other page, a menu is shown which lets you access all the configuration pages; the menu is divided in several sections:

- Basic Configuration
- Mobile Configuration (not available on Z-PASS1)

- Shared Memory Tag Configuration (when Gateway Mode is set to Modbus Shared Memory Gateway, see paragraph 20.1.4)
- Alarms
- Logic Configuration
- Data Logger
- Maintenance

Furthermore, in this like in any other page, the following information are shown:

- the page name
- the Z-PASS FW version along with the modem FW revision, for Z-PASS2
- the Z-PASS MAC address; the modem IMEI, for Z-PASS2; the SIM IMSI, for Z-PASS2, when a SIM is present
- the network interface used for Internet Access (i.e.: “Ethernet” or “Mobile”)
- the Modbus Ethernet to Serial/Transparent/Modbus Shared Memory Gateway status (i.e.: “running” or “stopped”) along with the Data Logger status (i.e.: “running” or “stopped”)
- the Router status (i.e.: “running” or “disabled”)

The currently logged user (e.g.: “admin”) and the “Logout” link are also present, near the page name.

In this page, two buttons are available:

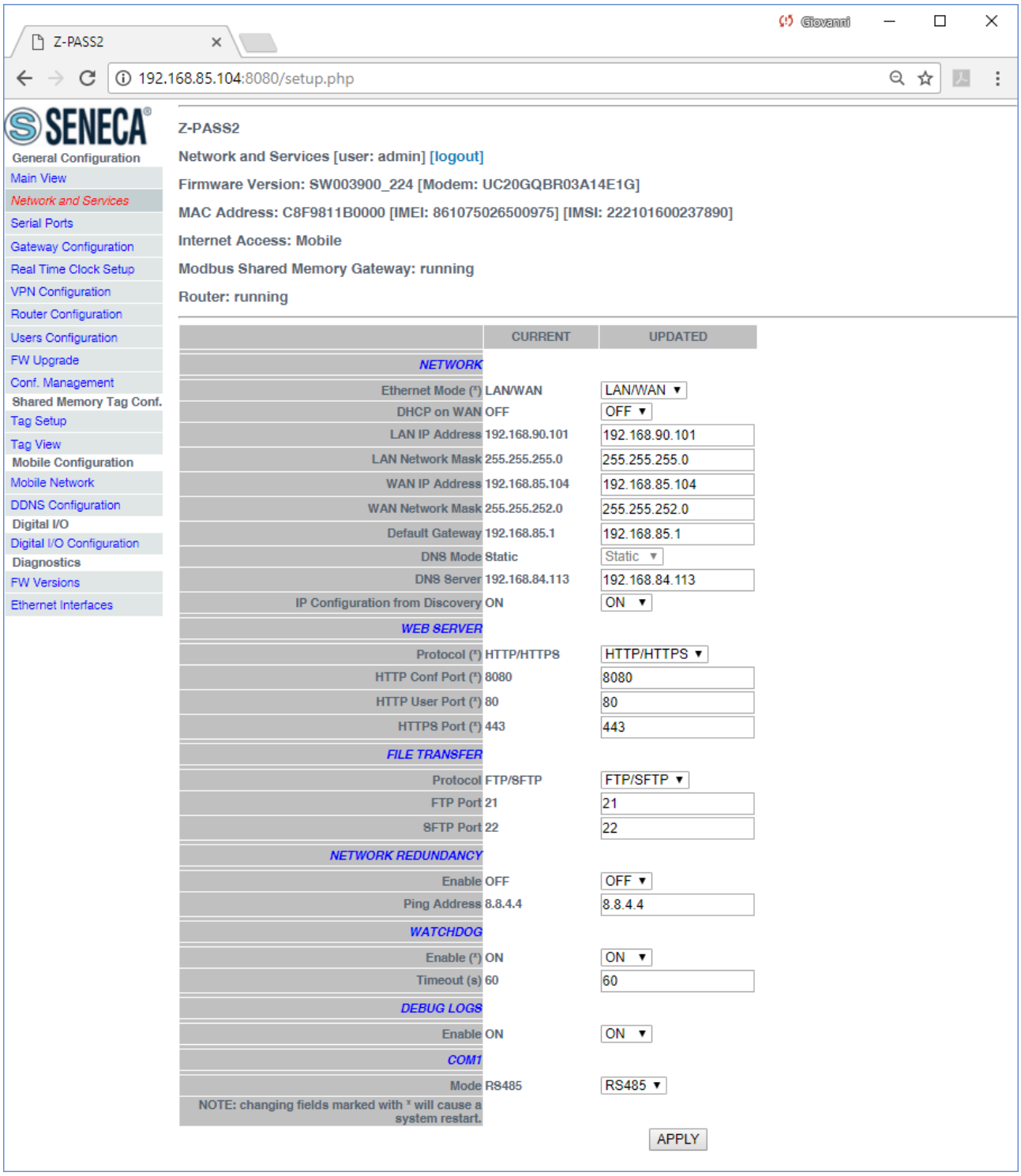
- “RESTART”, to perform Z-PASS reboot;
- “FACTORY DEFAULT”, to reset Z-PASS to its factory state.

Probably, the first parameters you need to change when setting up a new Z-PASS device are those related to its network configuration.

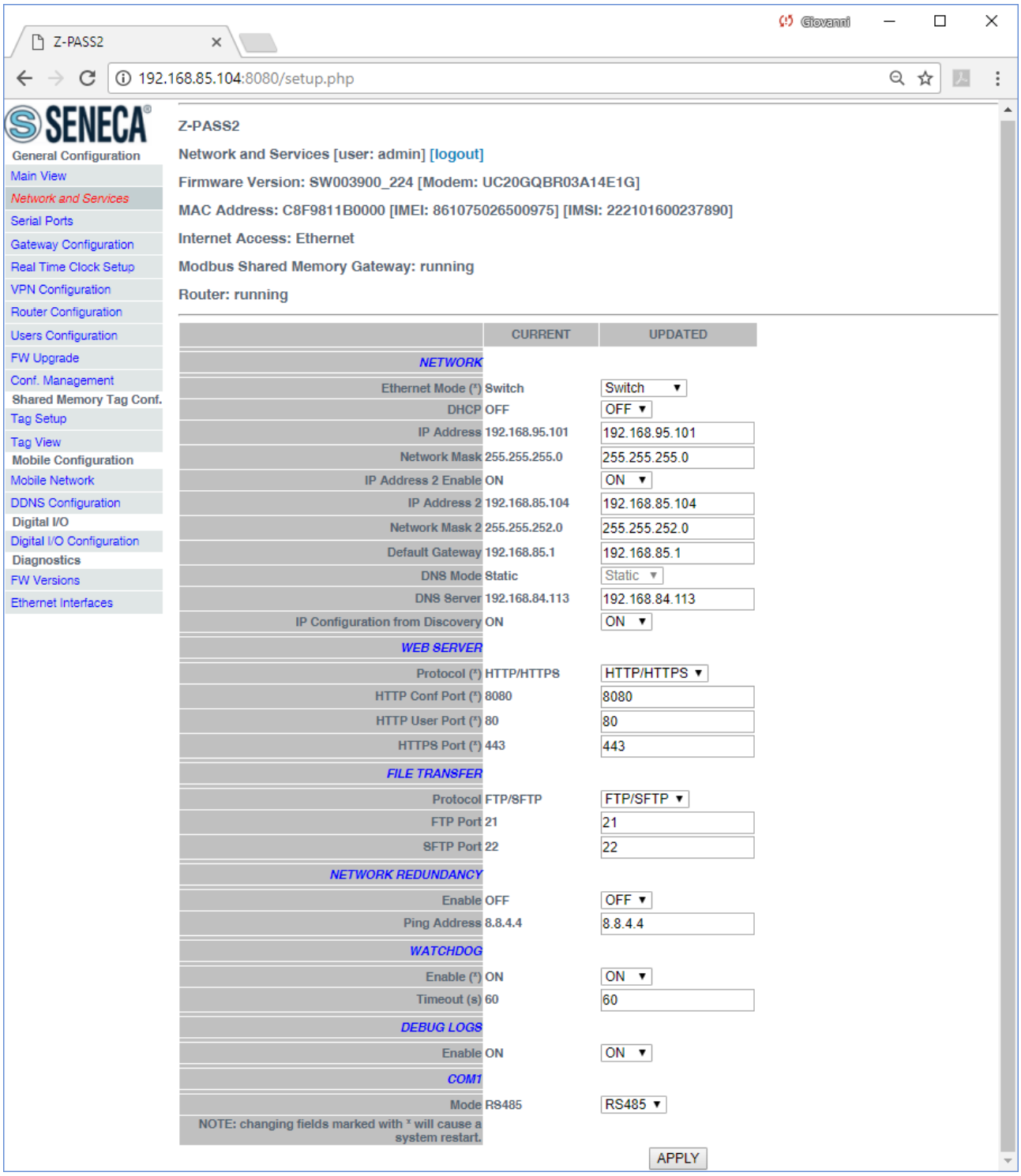
You can accomplish this in the “Network and Services” page, described in the following paragraph.

### *20.1.2 Network and Services*

The parameters shown in this page slightly change, depending on the HW version of the product and, for new HW versions, on the selected “Ethernet Mode”; this is shown in the following figures.




The previous figure shows the “Network and Services” page for a Z-PASS2, when the “Ethernet Mode” parameter is set to “LAN/WAN”; it also applies to a Z-PASS1 in “LAN/WAN” mode.




The previous figure shows the “Network and Services” page for a Z-PASS2, when the “Ethernet Mode” parameter is set to “Switch”; it also applies to a Z-PASS1 in “Switch” mode.


The previous figure shows the “Network and Services” page for a Z-PASS2-R01, when the “Ethernet Mode” parameter is set to “LAN/WAN”; it also applies to a Z-PASS1-R01 in “LAN/WAN” mode.


The previous figure shows the “Network and Services” page for a Z-PASS2-R01, when the “Ethernet Mode” parameter is set to “Switch”; it also applies to a Z-PASS1-R01 in “Switch” mode.


The previous figure shows the “Network and Services” page for a Z-PASS2 (old version); it also applies to a Z-PASS1 (old version).

There is an important difference between the parameter values shown in this page and those shown in the “Summary” page: the former are configured values, whereas the latter are actual values.

To better explain this difference, let's consider the case when the DHCP parameter is set to ON; in the "Network and Services" page, you may see the 192.168.90.101 default value for the "IP Address" parameter, whereas the "Summary" page shows the actual IP Address, assigned by the DHCP server.

In the following table, all configuration parameters available in this page are listed, with a short explanation and the parameter default value for each of them.

| Field | Meaning | Default value |
|---|---|---|
| NETWORK/Ethernet Mode | This parameter determines if the two Ethernet ports work as two fully separated network interfaces ("LAN/WAN") or as the ports of an Ethernet switch ("Switch"); depending on the value of this parameter, some other network parameters are hidden/shown or renamed as described below. | LAN/WAN |
| Ethernet Mode = "Switch" | | |
| NETWORK/DHCP | Flag to enable/disable the DHCP functionality on the Ethernet interface. | OFF |
| NETWORK/IP Address | IP address of the Ethernet interface (disabled when "DHCP" is set to "ON") | 192.168.90.101 |
| NETWORK/Network Mask | Network mask of the Ethernet interface (disabled when "DHCP" is set to "ON") | 255.255.255.0 |
| NETWORK/IP Address 2 Enable | Flag to enable/disable the second IP address on the Ethernet interface.<br>Note that the second IP address can be enabled also when the DHCP functionality is active. | OFF |
| NETWORK/IP Address 2 | Second IP address of the Ethernet interface | 192.168.100.101 |
| NETWORK/Network Mask 2 | Second network mask of the Ethernet interface | 255.255.255.0 |
| Ethernet Mode = "LAN/WAN" | | |
| NETWORK/DHCP on WAN | Flag to enable/disable the DHCP functionality on the WAN Ethernet interface | ON |
| NETWORK/LAN IP Address | IP address of the LAN Ethernet | 192.168.90.101 |

| | | |
|---|---|---|
| | interface | |
| NETWORK/LAN Network Mask | Network mask of the LAN Ethernet interface | 255.255.255.0 |
| NETWORK/WAN IP Address | IP address of the WAN Ethernet interface (disabled when “DHCP on WAN” is set to “ON”) | 192.168.100.101 |
| NETWORK/WAN Network Mask | Network mask of the WAN Ethernet interface (disabled when “DHCP on WAN” is set to “ON”) | 255.255.255.0 |
| | | |
| NETWORK/Default Gateway | Default Gateway IP address (disabled when DHCP functionality is enabled).<br>When “Ethernet Mode” is set to “LAN/WAN”, the Default Gateway shall be in the WAN subnet. | 192.168.100.1 , for Z-PASS1-R0x and Z-PASS2-R0x (x=1,2)<br>192.168.90.1, for all other products |
| NETWORK/DNS Mode | Tells if the DNS Server shall be set statically (value: “Static”) or dinamically assigned by the DHCP Server (value: “DHCP”) | DHCP, for Z-PASS1-R0x and Z-PASS2-R0x (x=1,2)<br>Static, for Z-PASS1 and Z-PASS2 |
| NETWORK/DNS Server | DNS server IP address (disabled when DHCP functionality is enabled and DNS Mode = DHCP) | 192.168.100.1 , for Z-PASS1-R0x and Z-PASS2-R0x (x=1,2)<br>192.168.90.1, for all other products |
| NETWORK/IP Configuration from Discovery | Flag to enable/disable the possibility of changing some of the network configuration parameters by means of the SDD application (see chapter 4) | ON |
| WEB SERVER/Protocol | Protocol used to access the web pages:<br>HTTP/HTTPS, HTTPS, HTTP | HTTP/HTTPS |
| WEB SERVER/HTTP Conf Port | TCP port to access the configuration pages, using HTTP protocol.<br>Please note that if this parameter is set to 80 (standard HTTP port), the web user site won’t be available anymore. | 8080<br>Default URL for conf pages:<br>**Errore. Riferimento a collegamento ipertestuale non valido.** |
| WEB SERVER/HTTP User Port | TCP port to access the user pages, using HTTP protocol. | 80<br>Default URL for user pages:<br>**Errore. Riferimento a** |

| | | |
|---|---|---|
| | | **collegamento ipertestuale non valido.**> |
| WEB SERVER/HTTPS Port | TCP port to access the configuration and user pages, using HTTPS protocol. | 443<br>Default URL for conf pages:<br>**Errore. Riferimento a collegamento ipertestuale non valido.**<br>Default URL for user pages:<br>**Errore. Riferimento a collegamento ipertestuale non valido.** |
| FILE TRANSFER/Protocol | Protocol used for File Transfer: FTP/SFTP, SFTP, FTP | FTP/SFTP |
| FTP Port | TCP Port for FTP protocol | 21 |
| SFTP Port | TCP Port for SFTP protocol | 22 |
| NETWORK REDUNDANCY/Enable | Flag to enable/disable the "Network Redundancy" functionality, that is using the Ethernet interface as the primary interface to access the Internet and the Mobile interface as the secondary interface, if the access through the primary interface becomes unavailable | OFF |
| NETWORK REDUNDANCY/Ping Address | IP Address used as ping destination to check if access to the Internet through the primary interface (Ethernet) is available.<br>This address shall be different from the one set for "DNS Server" parameter, otherwise an error is shown (see figure below). | 8.8.4.4 |
| WATCHDOG/Enable | Flag to enable/disable the watchdog functionality | ON |
| WATCHDOG/Timeout (s) | Watchdog timeout, in seconds; when watchdog is enabled, if it's not refreshed for this amount of seconds, the system will be rebooted.<br>Possible values are in the range [30..3600]. | 60 |

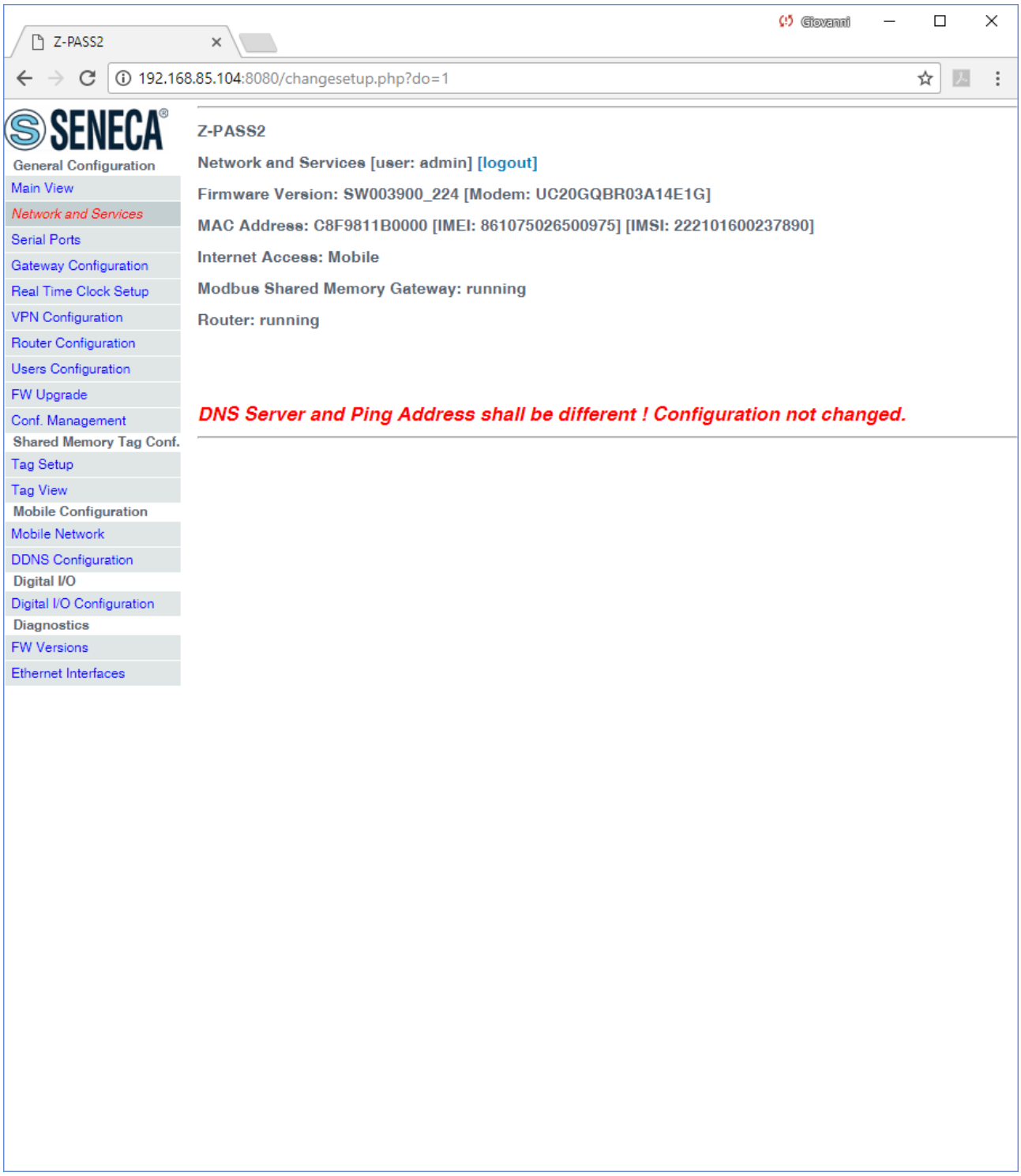
| | | |
|---|---|---|
| DEBUG LOGS/Enable | Flag to enable/disable the debug logs | OFF |
| COM1/Mode | Operating mode of the COM1 serial port<br>Possible values: RS485 \| RS232 | RS485 |

One note about the “DHCP” parameters:

- the “DHCP” parameter can be set to “ON” only if the “DHCP Server” parameter of the “Router Configuration” page is set to “OFF” (see paragraph 20.1.8).

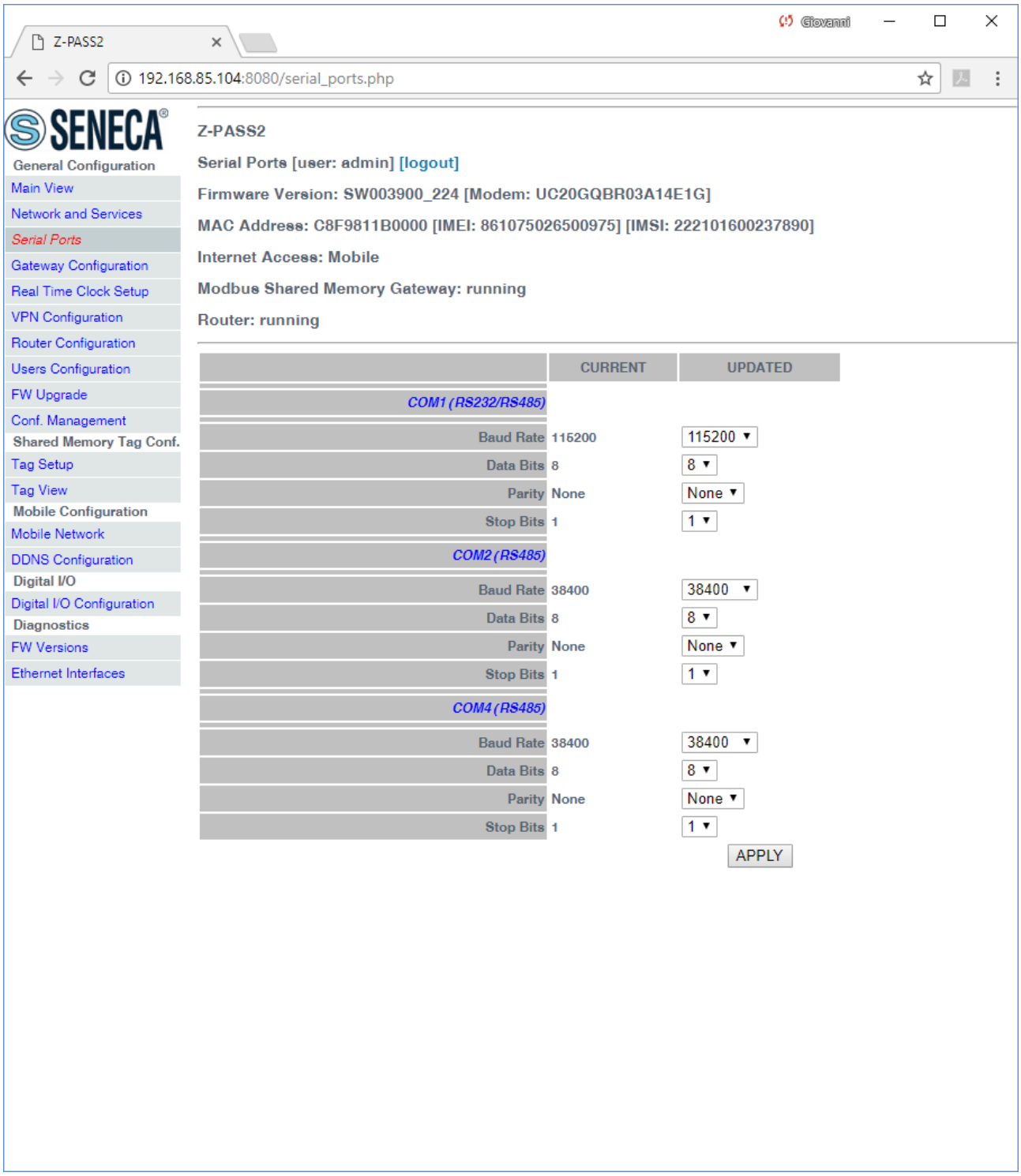
In the “Network and Services” page, you can change any of the above parameters; to apply the changes, press the “APPLY” button; as warned by the note on the page, only for some parameters, the parameter change requires rebooting the Z-PASS; these parameters are:

- NETWORK/Ethernet Mode
- WEB SERVER/Port
- WATCHDOG/Enable, only when changing ON -> OFF
- DEBUG LOGS/Enable, only when changing ON -> OFF




### *20.1.3 Serial Ports*

By clicking on the “Serial Ports” link, in the “Basic Configuration” section, you come to the following page:




This page is made up of three sections, corresponding to the three serial ports available in Z-PASS devices:

- COM1 RS232 or RS485[14]

[14] Depending on the position of the SW2 DIP switch.

- COM2 RS485
- COM4 RS485

For each serial port, the following configuration parameters are available:

| Field | Meaning | Default value |
|---|---|---|
| Baud Rate | Baud rate (in bps); possible values are:<br>200<br>300<br>600<br>1200<br>2400<br>4800<br>9600<br>19200<br>38400<br>57600<br>115200 | 38400 |
| Data Bits | Data bits; possible values are: 5/6/7/8 | 8 |
| Parity | Parity; possible values are: None/Even/Odd | None |
| Stop Bits | Stop bits; possible values are: 1/2 | 1 |

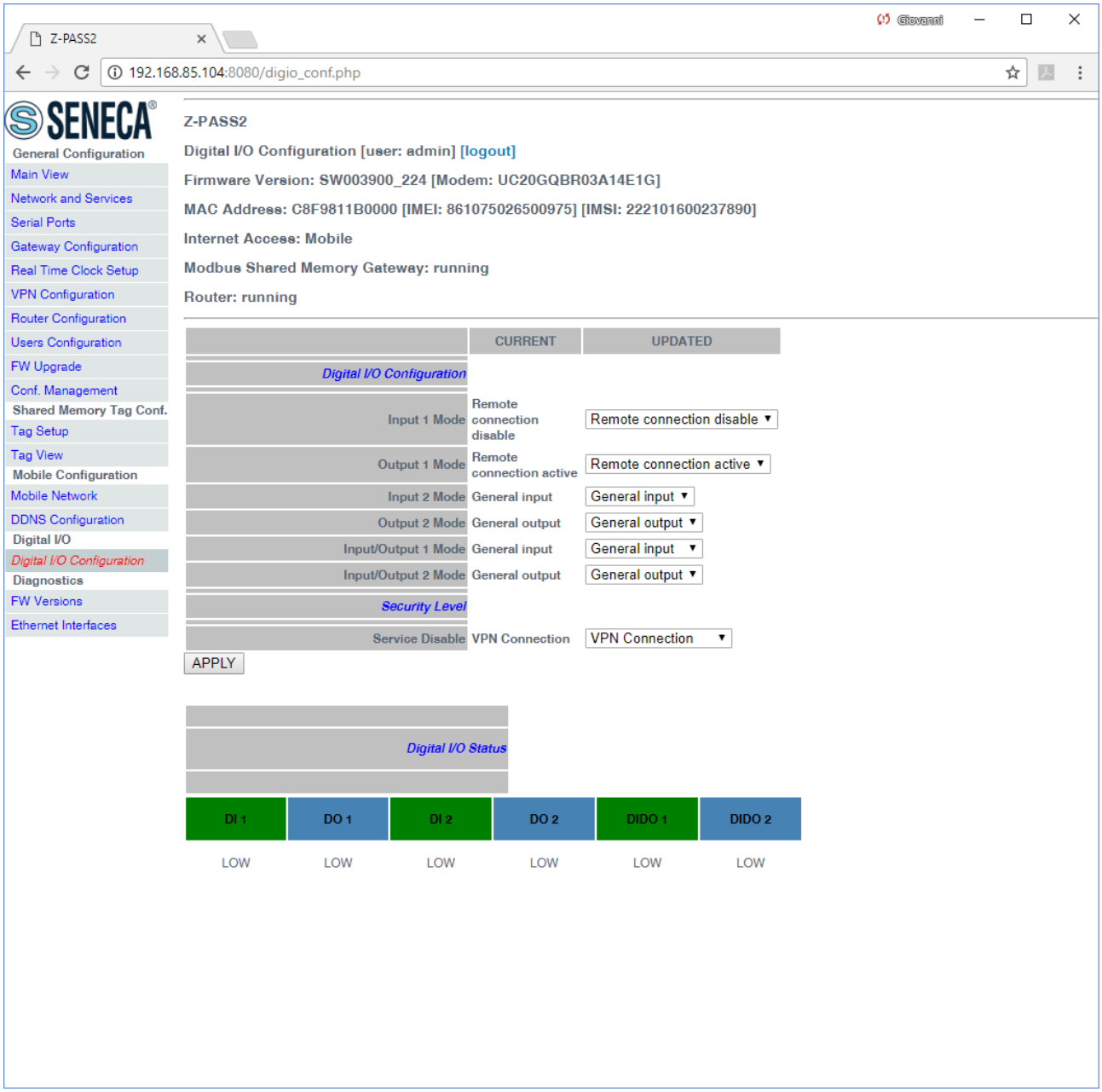
In the “Serial Ports” page, you can change any of the above parameters; to apply the changes, press the “APPLY” button.

Note that when you change the serial ports configuration, the Gateway services are automatically restarted, to actually apply the changes.

### *20.1.4 Digital I/O Configuration*

By clicking on the “Digital I/O Configuration” link, in the “Basic Configuration” section, you come to the page described in the following sub-paragraphs; the page differs between Z-PASS1 and Z-PASS2:

### *20.1.4.1 Z-PASS2*




In this page, you can configure the operating modes of the Digital I/Os and the security level applied by the "Remote Connection Disable" feature (see chapter 14).

| Field | Meaning | Default value |
|---|---|---|
| Input 1 Mode | This parameter represents the operating mode of the Digital Input 1 (DI 1).<br>Since this is the digital input used for "Remote Connection Disable" | Remote connection disable |

| | | |
|---|---|---|
| | feature, its value ("Remote connection disable") cannot be changed. | |
| Output 1 Mode | This parameter represents the operating mode of the Digital Output 1 (DO 1).<br>Since this is the digital output used to monitor remote connection, its value ("Remote connection active") cannot be changed. | Remote connection active |
| Input 2 Mode | This parameter represents the operating mode of the Digital Input 2 (DI 2).<br>Possible modes are: "General input" \| "Local alarm". | General input |
| Output 2 Mode | This parameter represents the operating mode of the Digital Output 2 (DO 2).<br>Possible modes are: "General output" \| "Remote toggle"[15]. | General output |
| Input/Output 1 Mode | This parameter represents the operating mode of the Digital Input/Output 1 (first configurable digital I/O) (DIDO 1).<br>Possible modes are: "General input" \| "General output". | General input |
| Input/Output 2 Mode | This parameter represents the operating mode of the Digital Input/Output 2 (second configurable digital I/O) (DIDO 2).<br>Possible modes are: "General input" \| "General output". | General output |
| Service Disable | This parameter determines which access services are disabled when "Remote Connection Disable" digital input is HIGH.<br>Possible values are: "VPN Connection" \| "VPN Service" \| "Internet Connection" \| "SMS | VPN Connection |

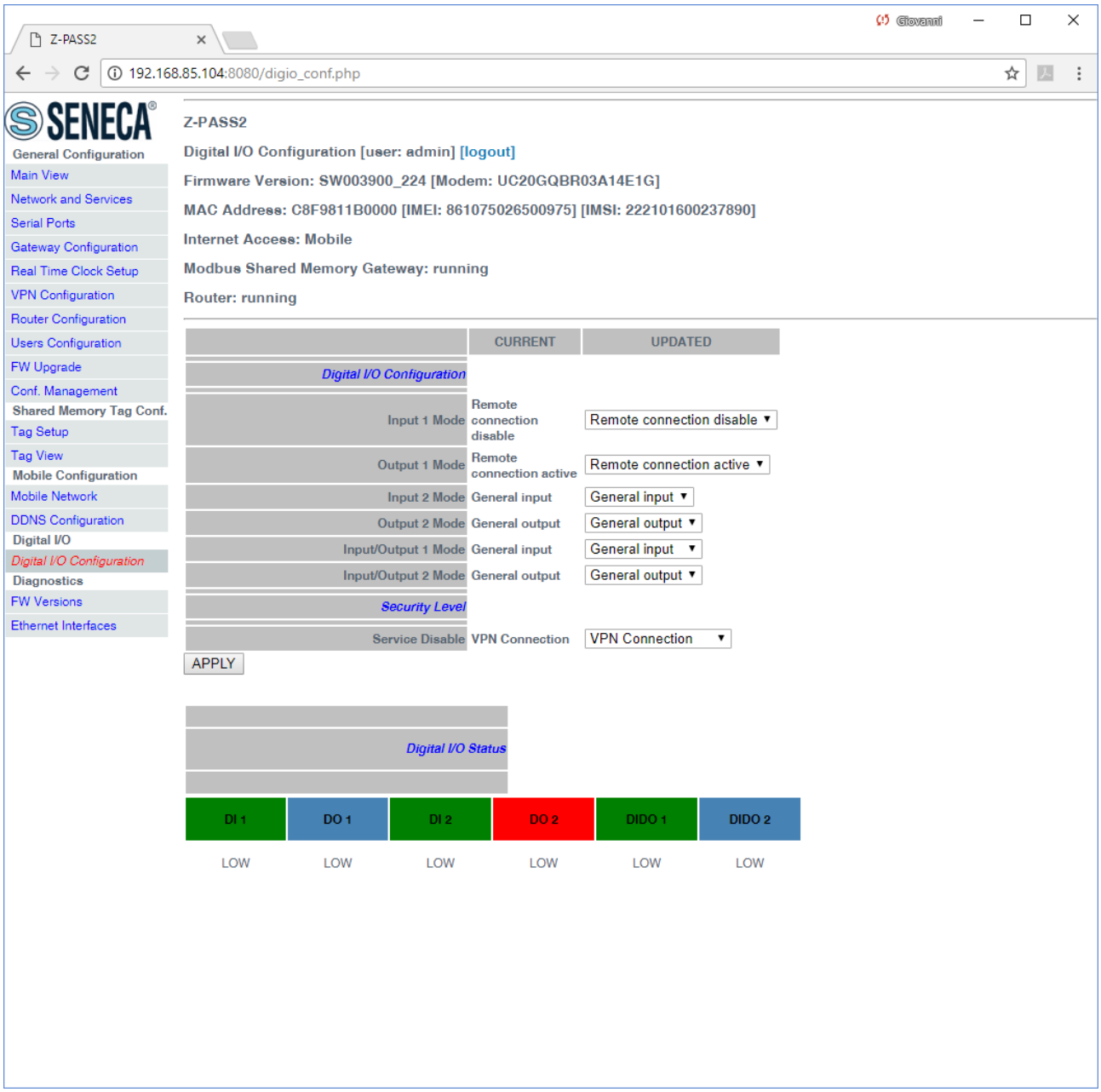
[15] "Remote toggle" function is still to be defined.

| | | |
|---|---|---|
| | Service".<br>See chapter 14, for a detailed description of these values. | |

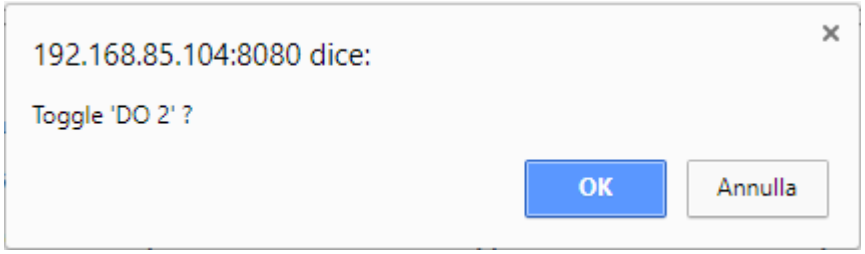
The "Digital I/O Status" section of the page gives the current status values ("LOW"/"HIGH") for each of the six available digital I/Os.

From this page, you can also change the status of the digital outputs working as "General Output"; the procedure is the following:

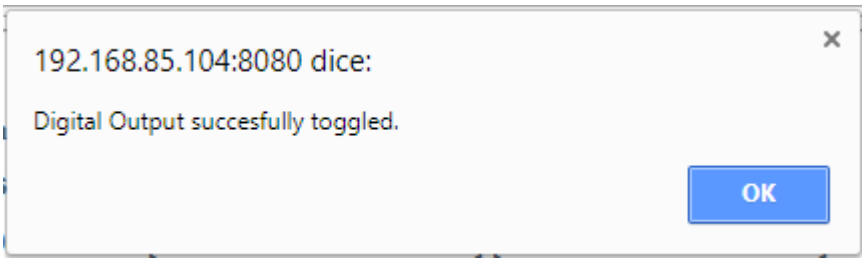
- when you move the mouse over one of the rectangles containing the digital I/O label (in the following figure, "DO 2"), the rectangle becomes red:




- when you click on the rectangle (only when I/O mode is “General Output”), a confirm pop-up is shown:

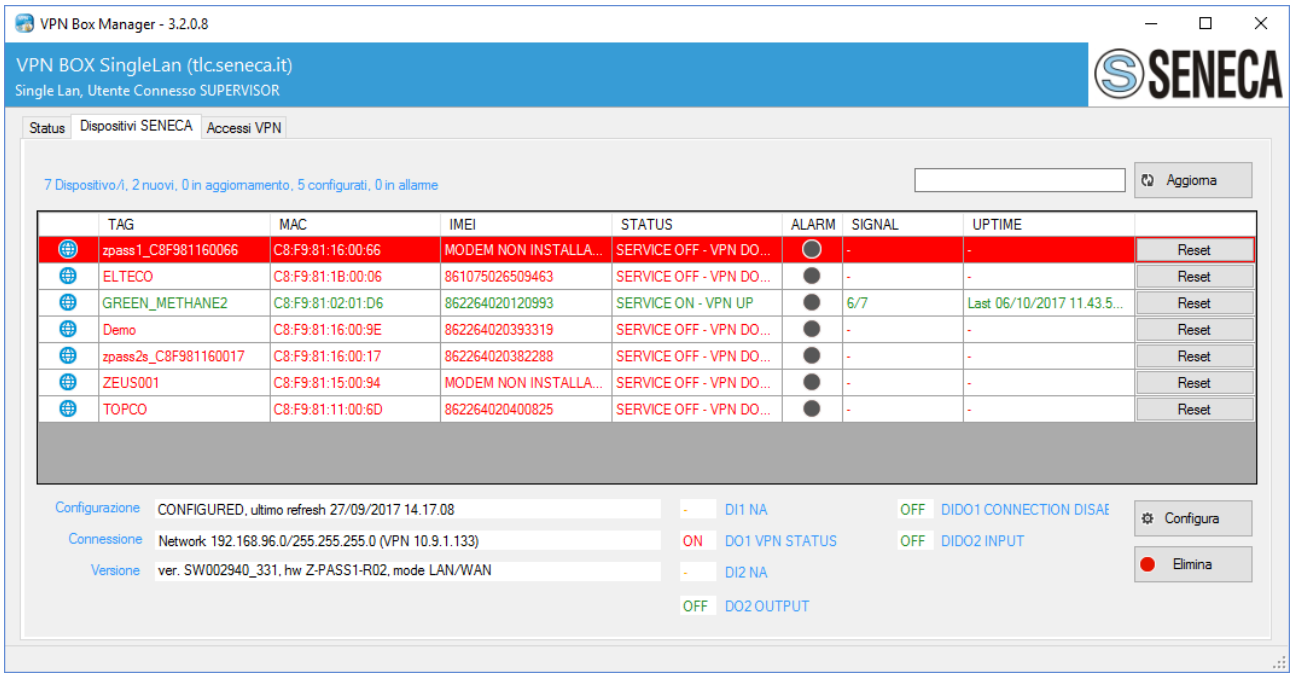



- if you click on “Cancel” button, no action is performed; if you click on “OK” button, the digital output status is toggled and a new pop-up is shown:

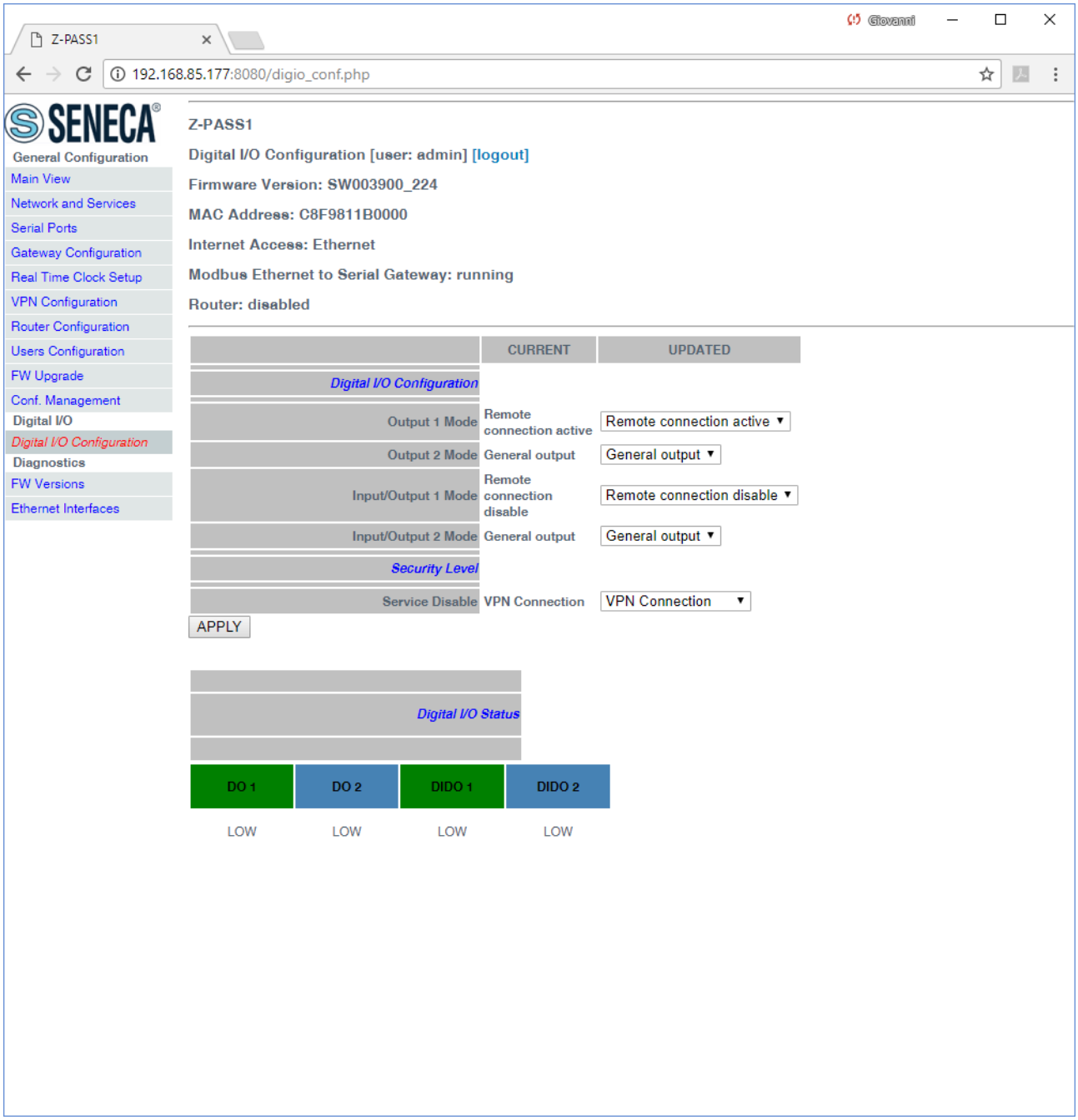



Please note that the above procedure applies also to Z-PASS1.

The status of the digital input configured as “Local Alarm” is reported in the “ALARM” column in the “Devices” tab of the “Seneca VPN Box Manager” and “Seneca VPN Client Communicator” applications.



### *20.1.4.2 Z-PASS1*




In this page, you can configure the operating modes of the Digital I/Os and the security level applied by the "Remote Connection Disable" feature (see chapter 14).

| Field | Meaning | Default value |
|---|---|---|
| Output 1 Mode | This parameter represents the operating mode of the Digital Output 1 (DO 1). | Remote connection active |

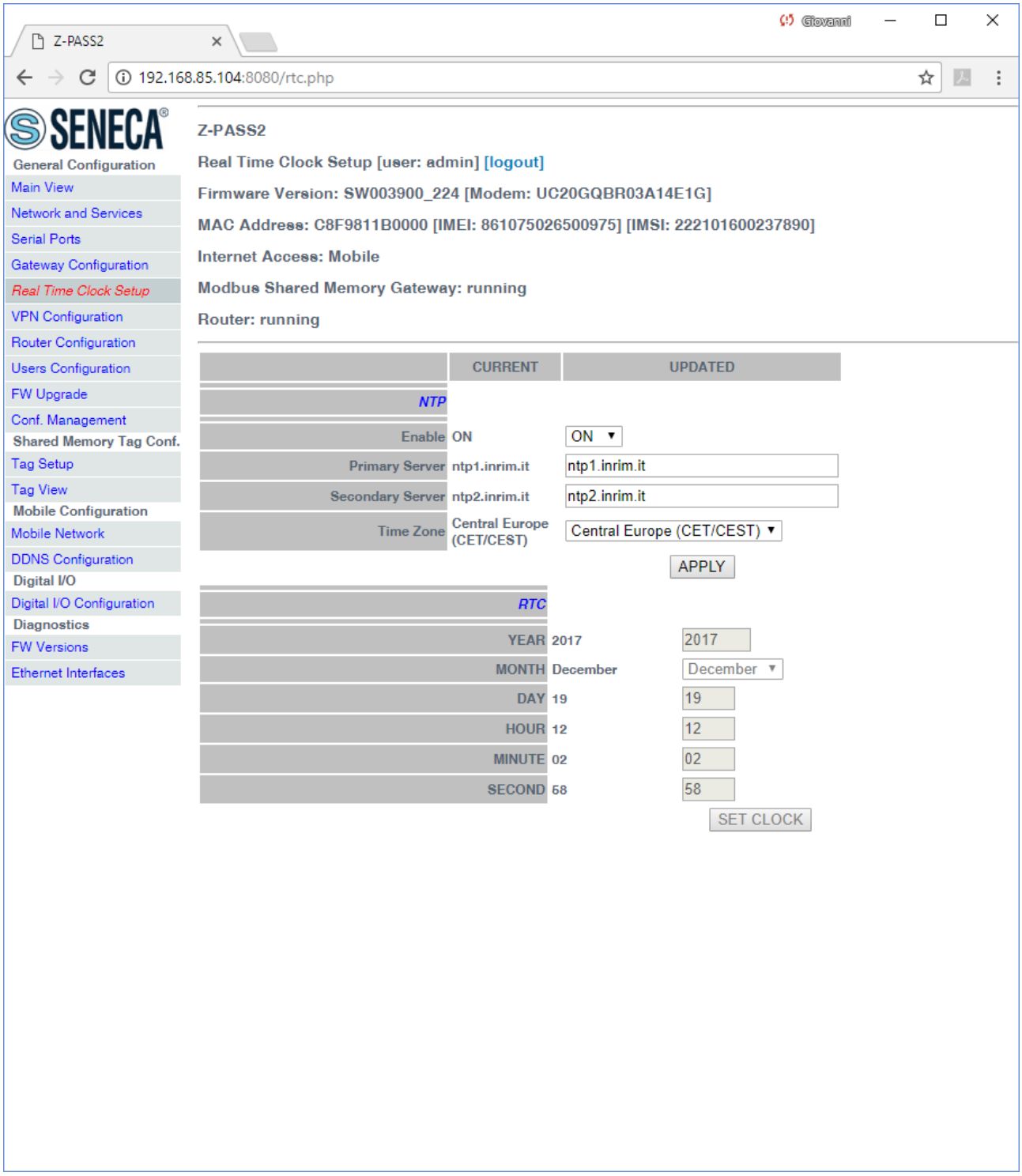
| | | |
|---|---|---|
| | Since this is the digital output used to monitor remote connection, its value ("Remote connection active") cannot be changed. | |
| Output 2 Mode | This parameter represents the operating mode of the Digital Output 2 (DO 2).<br>Possible modes are: "General output" \| "Remote toggle"[16]. | General output |
| Input/Output 1 Mode | This parameter represents the operating mode of the Digital Input/Output 1 (first configurable digital I/O) (DIDO 1).<br>Since this is used as an input for "Remote Connection Disable" feature, its value ("Remote connection disable") cannot be changed. | Remote connection disable |
| Input/Output 2 Mode | This parameter represents the operating mode of the Digital Input/Output 2 (second configurable digital I/O) (DIDO 2).<br>Possible modes are: "General input" \| "General output" \| "Local alarm". | General output |
| Service Disable | This parameter determines which access services are disabled when "Remote Connection Disable" digital input is HIGH.<br>Possible values are: "VPN Connection" \| "VPN Service" \| "Internet Connection" \| "SMS Service".<br>See chapter 14, for a detailed description of these values. | VPN Connection |

The "Digital I/O Status" section of the page gives the current status values ("LOW"/"HIGH") for each of the four available digital I/Os.

[16] "Remote toggle" function is still to be defined.

### 20.1.5 Real Time Clock Setup

By clicking on the “Real Time Clock Setup” link, in the “Basic Configuration” section, you come to the following page:




This page is made up of two sections: “NTP” and “RTC”.

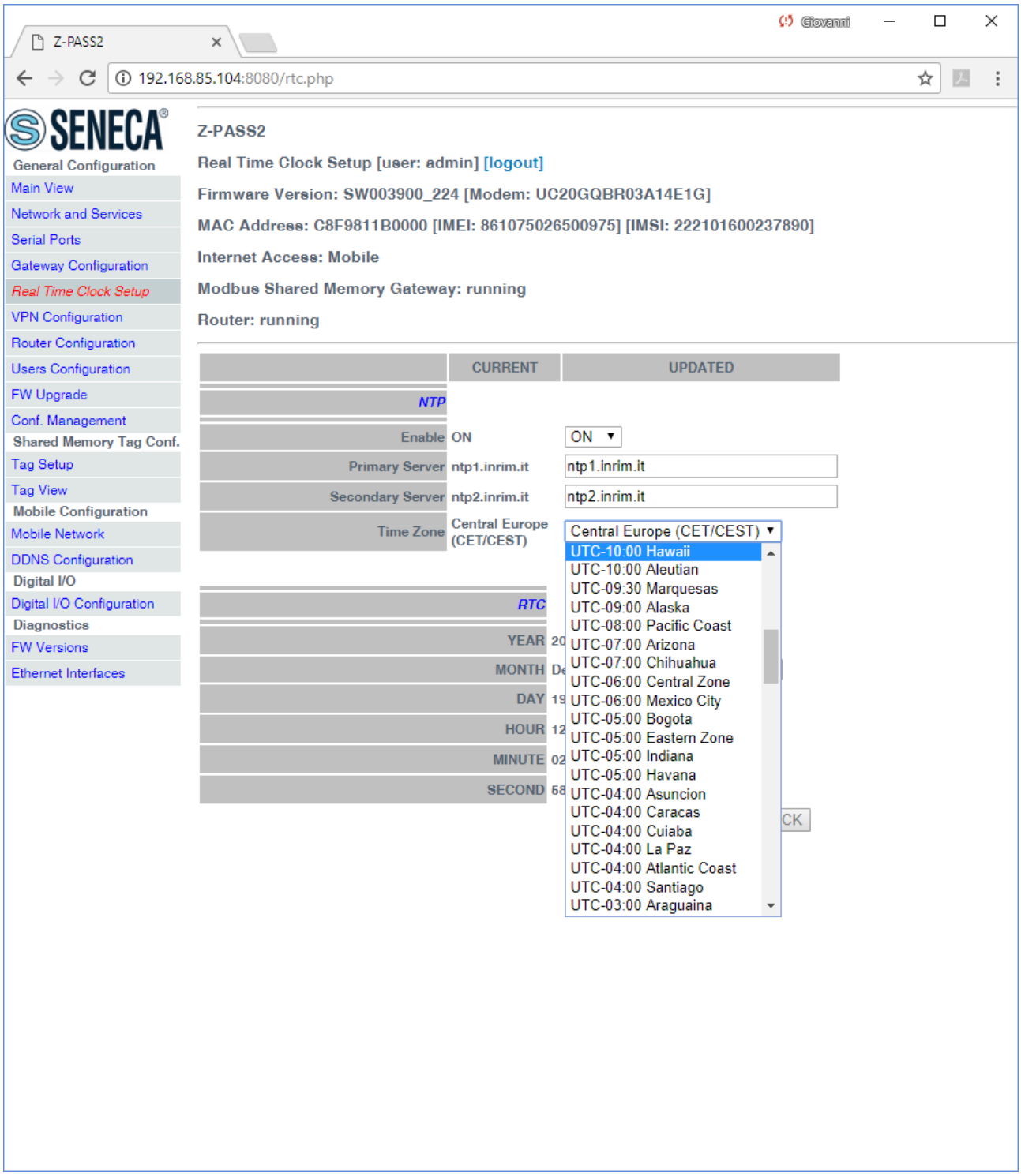
In the “NTP” section, you can change the parameters related to the Network Time Protocol and to the Time Zone, as listed in the following table:

| Field | Meaning | Default value |
|---|---|---|
| NTP/Enable | Flag to enable/disable time synchronization by means of NTP protocol | ON |
| NTP/Primary Server | IP address or FQDN[17] of the Primary NTP Server | ntp1.inrim.it |
| NTP/Secondary Server | IP address or FQDN of the Secondary NTP Server | ntp2.inrim.it |
| NTP/Time Zone | Time Zone | Central Europe (CET/CEST) |

When the “Time Zone” parameter is set to “Central Europe (CET/CEST)” value, the Device automatically enables (CEST) / disables (CET) the “Daylight Saving Time” setting.

A large number of Time Zones are available, as partially shown in the following figure:

[17] FQDN: Fully Qualified Domain Name, e.g.: “pool.ntp.org”.

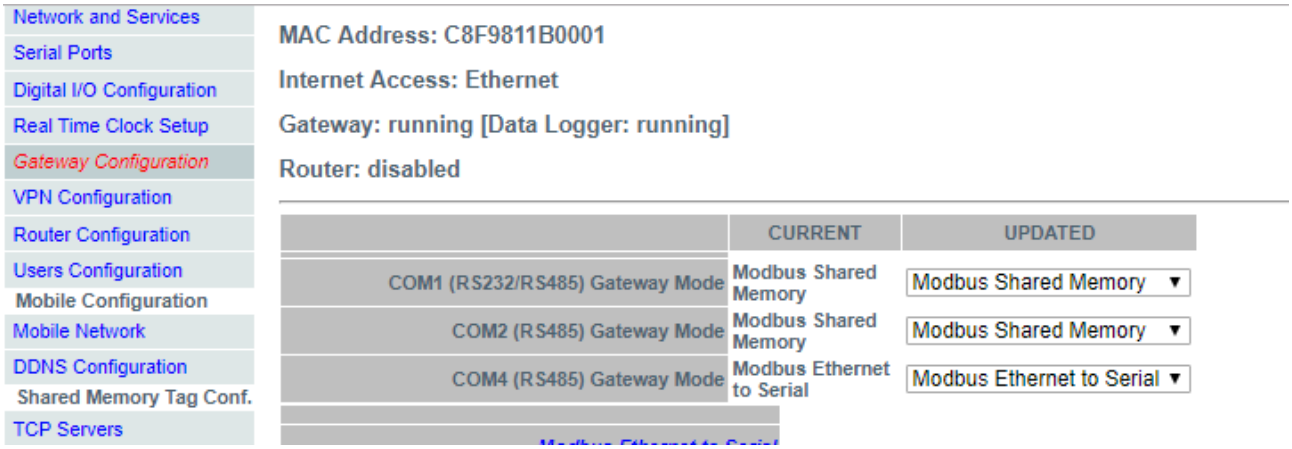



The “RTC” section of the page lets you manually change the Z-PASS date/time settings; since this makes sense only if NTP time synchronization is not enabled, when “NTP/Enable” parameter is “ON” the input fields and the “SET CLOCK” button are disabled and the parameters are only for viewing.

Instead, when “NTP/Enable” parameter is “OFF”, the input fields in the “NTP” section are still enabled; this lets you change and save the parameter values, even if they are not actually used.

### 20.1.6 Gateway Configuration

By clicking on the "Gateway Configuration" link, in the "Basic Configuration" section, you come to the following page:




The first thing you have to do in this page is to select, for each serial port, the type of gateway bound to the port, by means of the corresponding "Gateway Mode" parameter; the possible modes are "Modbus Ethernet to Serial", "Transparent" and "Modbus Shared Memory".

The page is substantially made up of three sections, corresponding to the three serial ports available in Z-PASS devices.

The configuration parameters available in each of these sections depend on the selected mode, as described in the following sub-paragraphs.

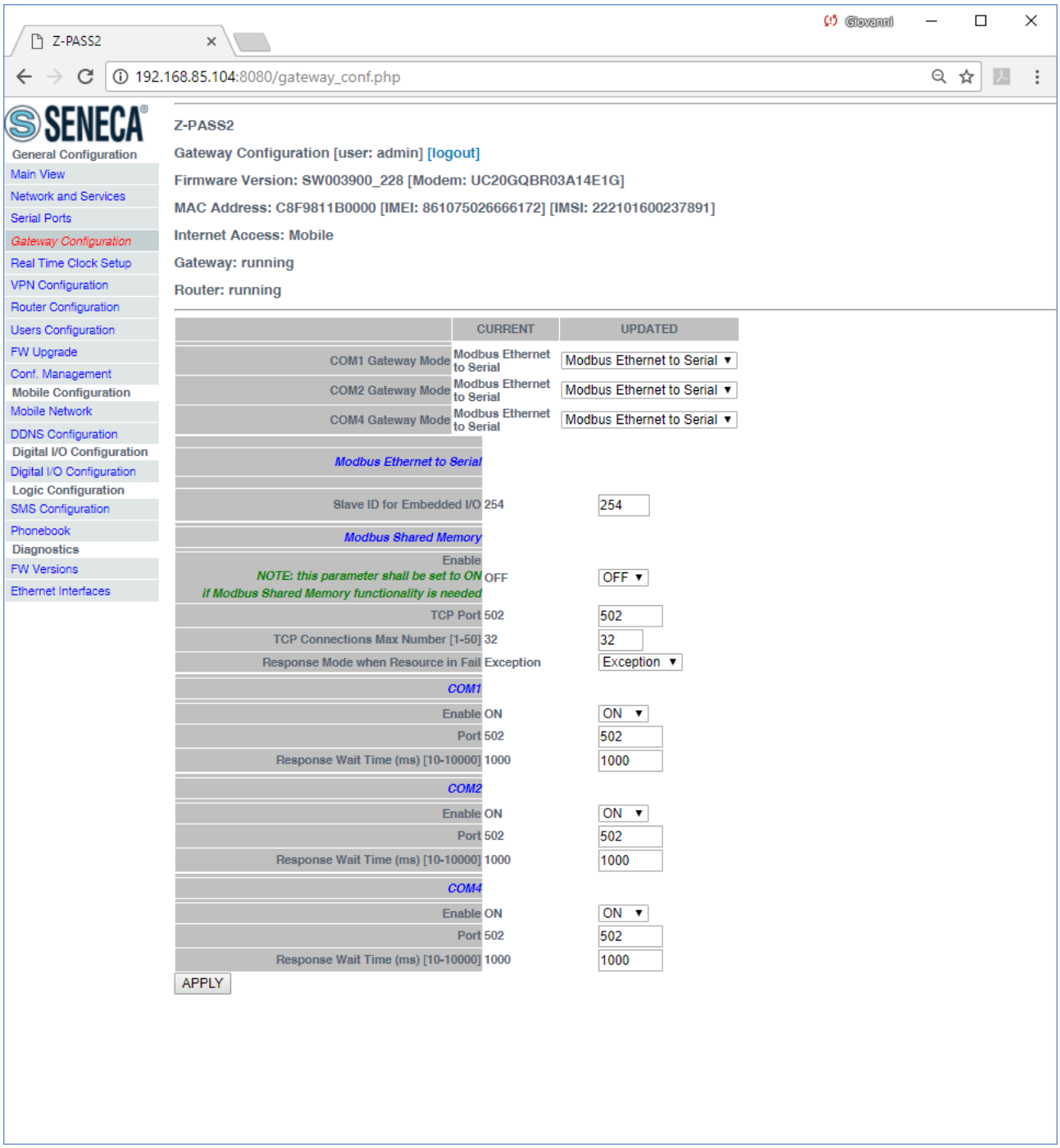
#### 20.1.6.1 Modbus Ethernet to Serial Gateway

For each serial port with "Gateway Mode" = "Modbus Ethernet to Serial", the following configuration parameters are available:

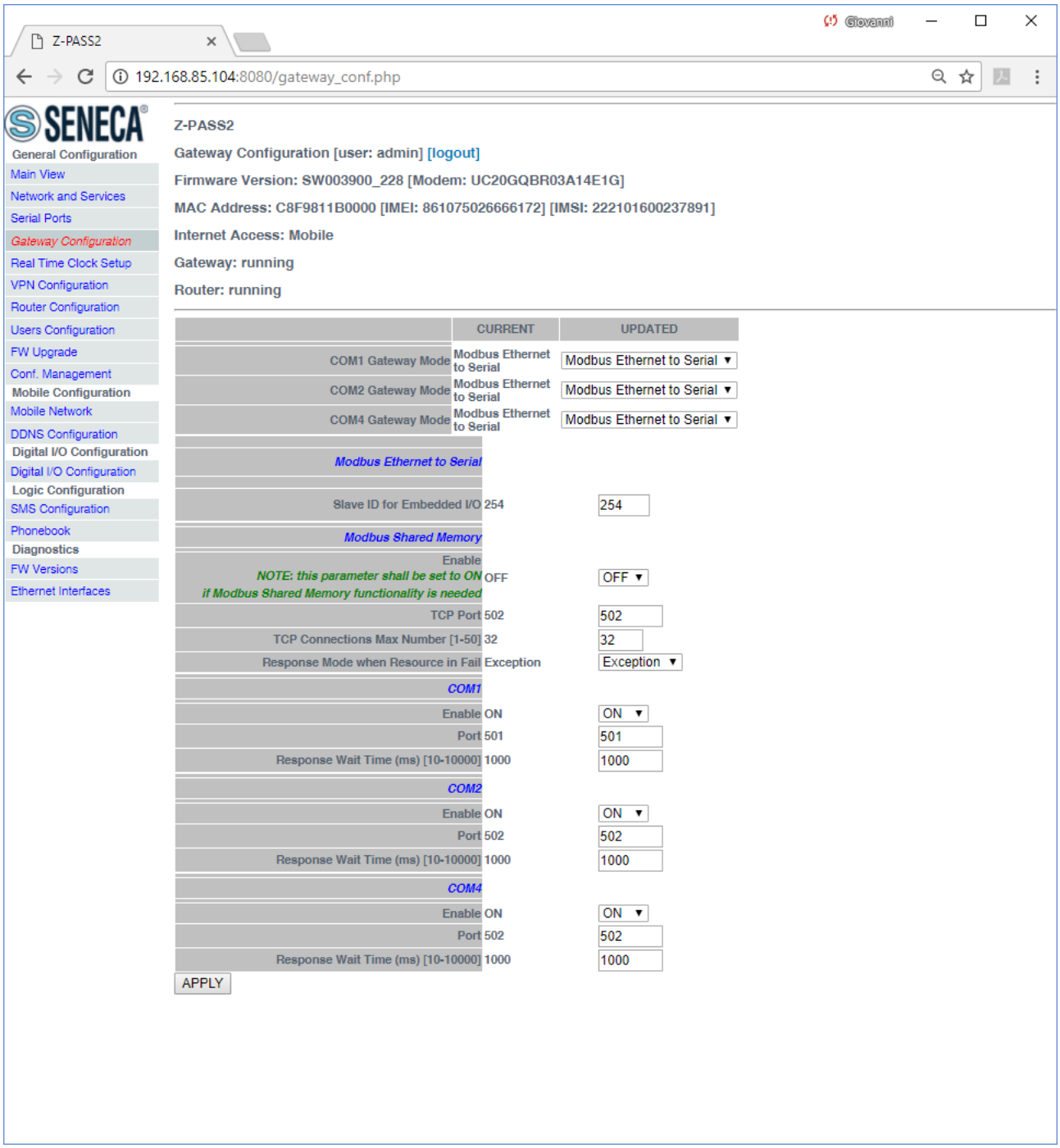
| Field | Meaning | Default value |
|---|---|---|
| Enable | Flag to enable/disable the Modbus Ethernet to Serial Gateway functionality on the port | ON |
| Port | TCP port to access the Modbus Ethernet to Serial Gateway<br>If three distinct values are set, three Modbus Ethernet to Serial Gateway instances are run, each handling a | COM1: 501<br>COM2: 502<br>COM4: 503 |

| | | |
|---|---|---|
| | single serial port.<br>If the same port value is set for more than one serial port, the same Modbus Ethernet to Serial Gateway instance will handle two or three serial ports, that is the Modbus RTU requests will be simultaneously sent to the serial ports. | |
| Response Wait Time | Timeout on the reception of the Modbus RTU responses<br>The value is in milliseconds; possible values are in the range [10 - 10000]. | 1000 |

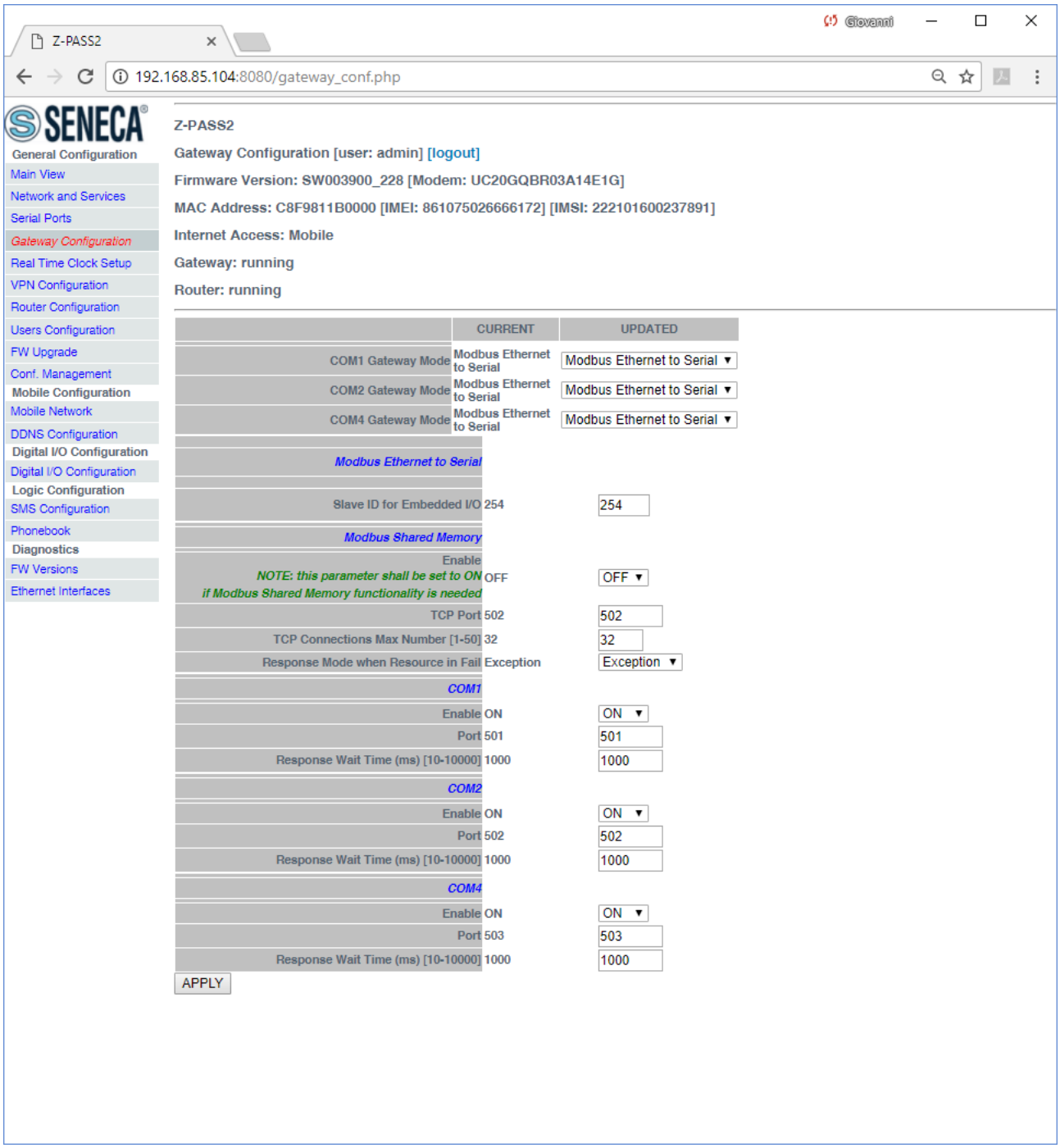
The following screen-shots give some examples of Modbus Ethernet to Serial Gateway configurations.




In the above configuration, all the Modbus requests received on the 502 TCP port will be sent to all the three serial ports (COM1, COM2 and COM4); the communication parameters on the serial ports are those set in the “Serial Ports” page (see 20.1.3).

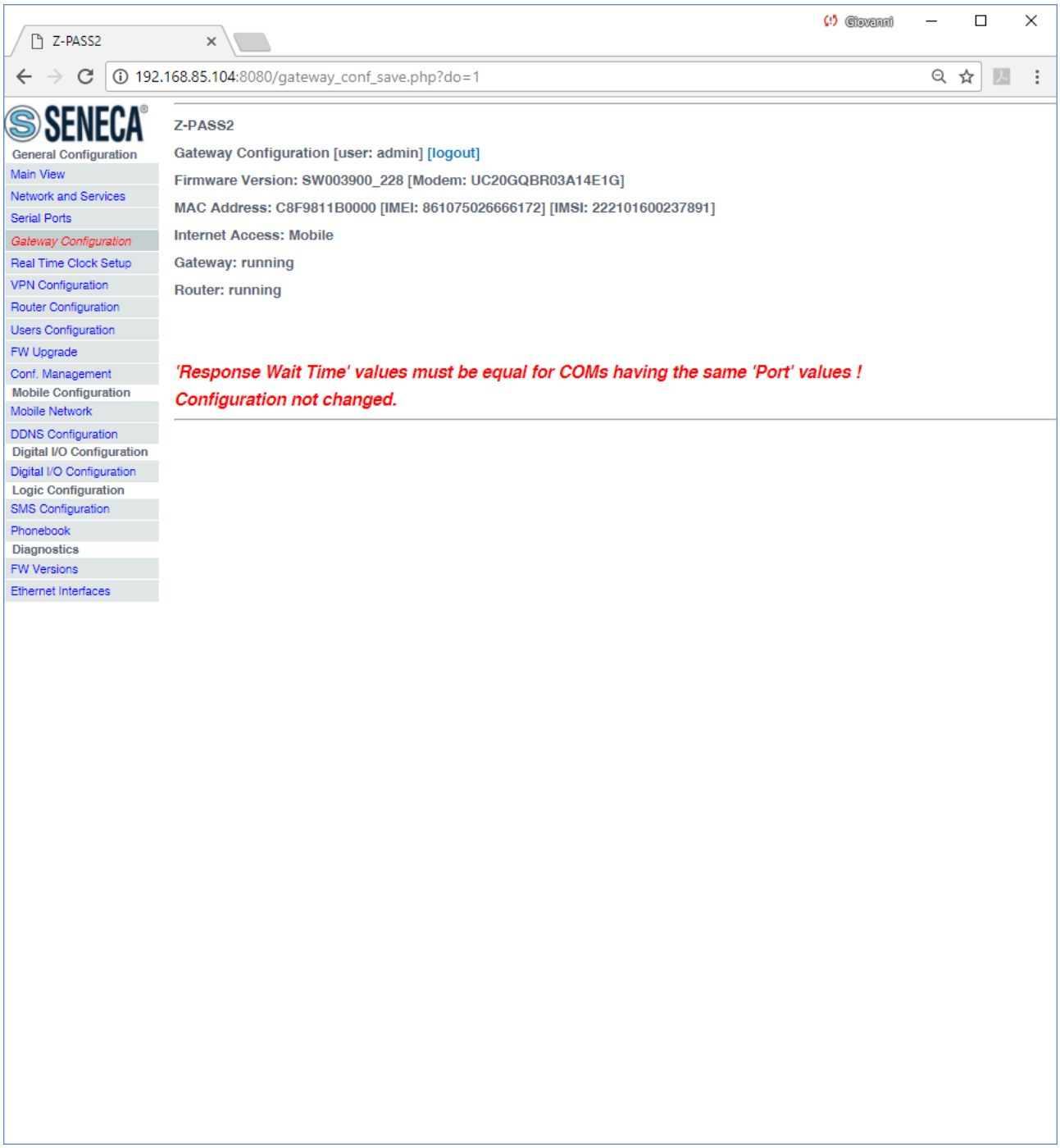



In the above configuration, the Modbus requests received on the 501 TCP port will be sent to the COM1 port, while those received on the 502 TCP port will be sent to the COM2 and COM4 ports.




Finally, in the above configuration, each TCP port corresponds to a single serial port, that is Modbus requests received on a TCP port are sent to a single serial port.

Please note that if you set the same TCP port value for more than one serial port, the “Response Wait Time” values shall also be the same for those serial ports; otherwise, clicking on the “APPLY” button, the following error message is shown.




#### 20.1.6.1.1 Embedded I/O

As shown in the above figures, when at least one port has “Gateway Mode” = “Modbus Ethernet to Serial”, the “Gateway Configuration” page contains the following parameter:

| Field | Meaning | Default value |
|---|---|---|
| Slave ID for Embedded I/O | Slave ID used to access the Modbus Registers corresponding to the | 254 |

| | | |
|---|---|---|
| | "embedded" digital I/Os (for "IO" HW revision).<br>In Z-PASS2, this id can also be used to access Modbus Registers containing GPS information.<br>Possible values: [1..255]. | |

The Modbus Registers representing the Digital I/Os are given in the following table:

| **Data Type** | **Digital I/Os** | **Address** |
|---|---|---|
| Holding Registers | Bit 0: DI1 (LSB)<br>Bit 1: DI2<br>Bit 2: DI3<br>Bit 3: DI4 | 0 (40001) |
| Holding Registers | Bit 0: DO1 (LSB)<br>Bit 1: DO2<br>Bit 2: DO3<br>Bit 3: DO4 | 0 (40002) |
| Discrete Inputs | DI1 | 0 (10001) |
| Discrete Inputs | DI2 | 1 (10002) |
| Discrete Inputs | DI3 | 2 (10003) |
| Discrete Inputs | DI4 | 3 (10004) |
| Coils | DO1 | 0 |
| Coils | DO2 | 1 |
| Coils | DO3 | 2 |
| Coils | DO4 | 3 |

The mapping between DI1..DI4, DO1..DO4 and the Digital I/O names described in the "Digital I/O Configuration" paragraph is as follows:

| | |
|---|---|
| DI1 | DI 1 |
| DI2 | DI 2 |
| DI3 | DIDO 1, if input |
| DI4 | DIDO 2, if input |
| DO1 | DO 1 |
| DO2 | DO 2 |
| DO3 | DIDO 1, if output |
| DO4 | DIDO 2, if output |

If DIx or DOx is not available (e.g.: DI4, when DIDO 2 is configured as an output), the corresponding bit value is always 0.

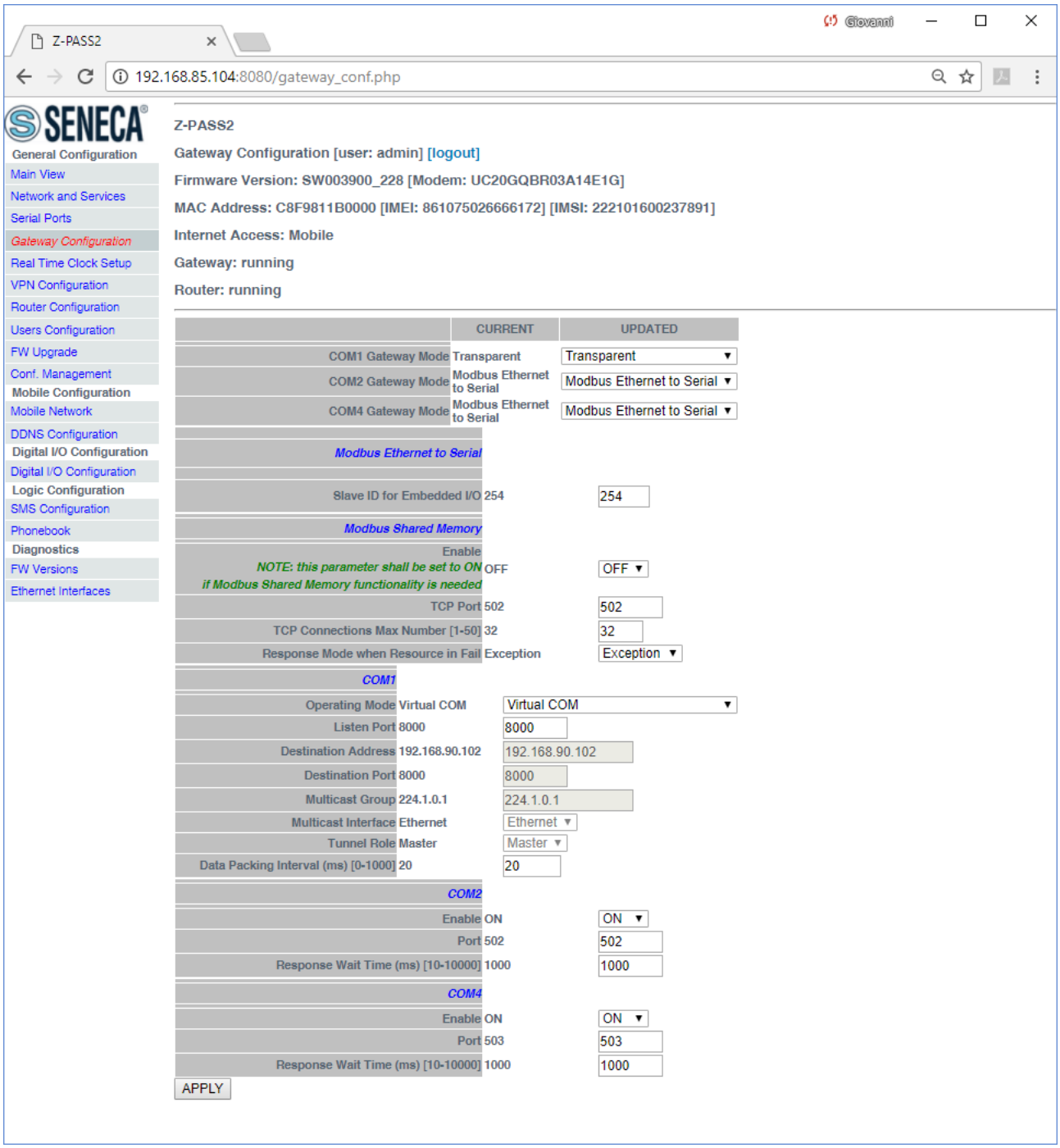
DOx can be actually set only if the corresponding Digital I/O Mode is "General Output" (see "Digital I/O Configuration" paragraph); otherwise, the write request will have no effect.

The Modbus Registers containing the GPS information are given in the following table (all Holding Registers):

| Info | Address | Data Type |
|---|---|---|
| GPS_ERROR | 9 (40010) | INT<br>(0: OK,<br>-1: Not fixed<br>-2: Internal error) |
| GPS_UTC_HH | 10 (40011) | UINT |
| GPS_UTC_MM | 11 (40012) | UINT |
| GPS_UTC_SS | 12 (40013) | UINT |
| GPS_DATE_DD | 13 (40014) | UINT |
| GPS_DATE_MM | 14 (40015) | UINT |
| GPS_DATE_YY | 15 (40016) | UINT |
| GPS_LATITUDE | 16 – 19 (40017 – 40020) | LREAL |
| GPS_LONGITUDE | 20 – 23 (40021 – 40024) | LREAL |
| GPS_HDOP | 24 – 27 (40025 – 40028) | LREAL |
| GPS_ALTITUDE | 28 – 31 (40029 – 40032) | LREAL |
| GPS_COG | 32 – 35 (40033 – 40036) | LREAL |
| GPS_SPEED_KM | 36 – 39 (40037 – 40040) | LREAL |
| GPS_SPEED_KN | 40 - 43 (40041 – 40044) | LREAL |
| GPS_FIX | 44 (40045) | UINT |
| GPS_NSAT | 45 (40046) | UINT |

#### *20.1.6.2 Transparent Gateway*

Selecting “Transparent” as the gateway mode for one of the serial ports, e.g. “COM1”, the “Gateway Configuration” page will change to look like the one shown in the following figure:




For each serial port with “Gateway Mode” = “Transparent”, the available configuration parameters depend on the value of the “Operating Mode” parameter selected for the port.

The possible values for the “Operating Mode” parameter are:

- None (default value)
- Virtual COM
- Serial Tunnel Point-to-Point on TCP

- Serial Tunnel Point-to-Point on UDP
- Serial Tunnel Point-to-Multipoint

Furthermore, for the "Serial Tunnel" operating modes, the available parameters depend on the selected "Tunnel Role" (Master or Slave).

The following tables describe the relevant parameters for the various operating modes.

Virtual COM

| Field | Meaning | Default value |
|---|---|---|
| Listen Port | TCP port to access the transparent gateway | COM1: 8000<br>COM2: 8001<br>COM4: 8002 |
| Data Packing Interval | Time interval used as a criterion to pack data bytes received from the serial port, before sending them to the network; that is, if no byte is received for this time, available bytes are sent to the network.<br>The value is in milliseconds; possible values are in the range [0 - 1000]. | 20 |

Serial Tunnel Point-to-Point on TCP (Slave)
Serial Tunnel Point-to-Point on UDP (Slave)

| Field | Meaning | Default value |
|---|---|---|
| Listen Port | TCP/UDP port to access the transparent gateway | COM1: 8000<br>COM2: 8001<br>COM4: 8002 |

Serial Tunnel Point-to-Point on TCP (Master)
Serial Tunnel Point-to-Point on UDP (Master)

| Field | Meaning | Default value |
|---|---|---|
| Destination Address | The IP Address which the transparent gateway will connect to | COM1: 192.168.90.102<br>COM2: 192.168.90.103<br>COM4: 192.168.90.104 |
| Destination Port | The TCP/UDP port which the transparent gateway will connect to | COM1: 8000<br>COM2: 8001<br>COM4: 8002 |

Serial Tunnel Point-to-Multipoint (Master)

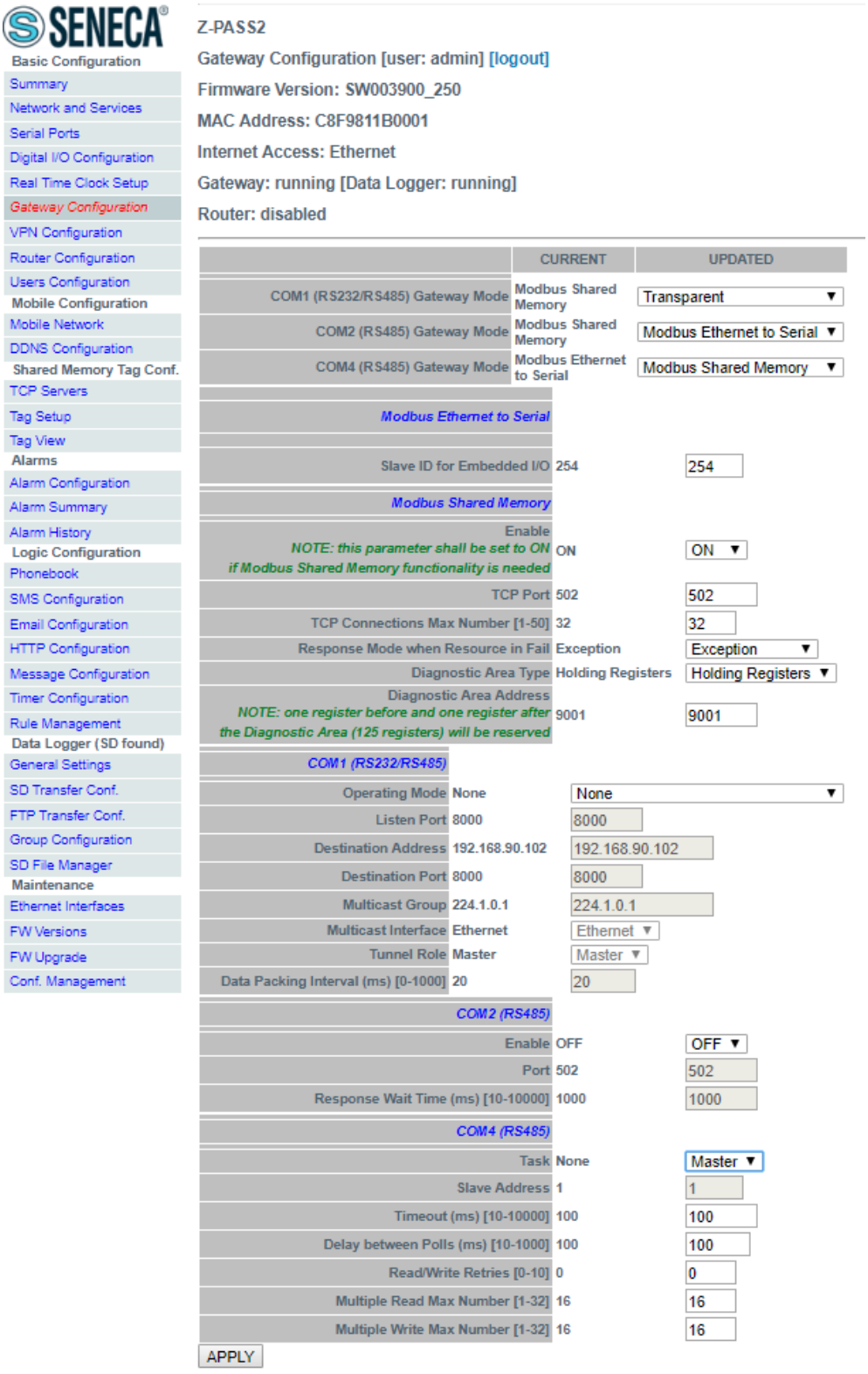
| Field | Meaning | Default value |
|---|---|---|
| Destination Port | The UDP port which the packets will be sent to | COM1: 8000<br>COM2: 8001<br>COM4: 8002 |
| Multicast Group | IP Address which identifies the Multicast Group | 224.1.0.1 |
| Multicast Interface | Network Interface which the UDP packets are sent to; possible values: Ethernet\|VPN; "VPN" option is available only when VPN is active | Ethernet |

Serial Tunnel Point-to-Multipoint (Slave)

| Field | Meaning | Default value |
|---|---|---|
| Listen Port | The UDP port which the packets will be received from | COM1: 8000<br>COM2: 8001<br>COM4: 8002 |
| Multicast Group | IP Address which identifies the Multicast Group | 224.1.0.1 |
| Multicast Interface | Network Interface which the UDP packets are received from; possible values: Ethernet\|VPN; "VPN" option is available only when VPN is active | Ethernet |

### *20.1.6.3 Modbus Shared Memory Gateway (Use for Datalogging and Logic Rules)*

Selecting "Modbus Shared Memory" as the gateway mode for one of the serial ports, e.g. "COM4", the "Gateway Configuration" page will change to look like the one shown in the following figure:




As shown in the previous figures, the “Gateway Configuration” page always contains the following parameters, related to the “Modbus Shared Memory Gateway” mode; these parameters are always shown

since this functionality makes sense even when no serial port is assigned to it, that is using only Modbus TCP protocol.

| Field | Meaning | Default value |
|---|---|---|
| Enable | This parameter enables/disables the Modbus Shared Memory Gateway service.<br>It is important to note that, when this parameter is set to OFF, the service is not running even if some serial ports are assigned to it. | OFF |
| TCP Port | Listening port for the Modbus TCP server | 502 |
| TCP Connections Max Number [1-50] | Maximum number of TCP connections that can be accepted by the Modbus TCP server | 32 |
| Response Mode when Resource in Fail | This parameter defines how the response to a Modbus (read) request is built for a tag corresponding to a Modbus station which is not responding; when mode is “Tag error value”, the value in the Modbus response is given according to the “Error Mode”/”Error Value” parameters in the tag definition; when mode is “Exception”, the response contains an exception with the value 11 (“Gateway target device failed to respond”). | Exception |
| Diagnostic Area Type | Select if the diagnostic are can be accessed by Holding or Input Modbus Registers. | |
| Diagnostic Area Address | The diagnostic area reserve a bit for each tag (125 registers):<br>Bit value to 0 -> means Tag Reading Error (or tag not configured)<br>Bit value to 1 -> means Tag Reading OK<br><br>So if you need to check the fail status of the first 10 tags using the default Area (9001 Holding Registers) you | |

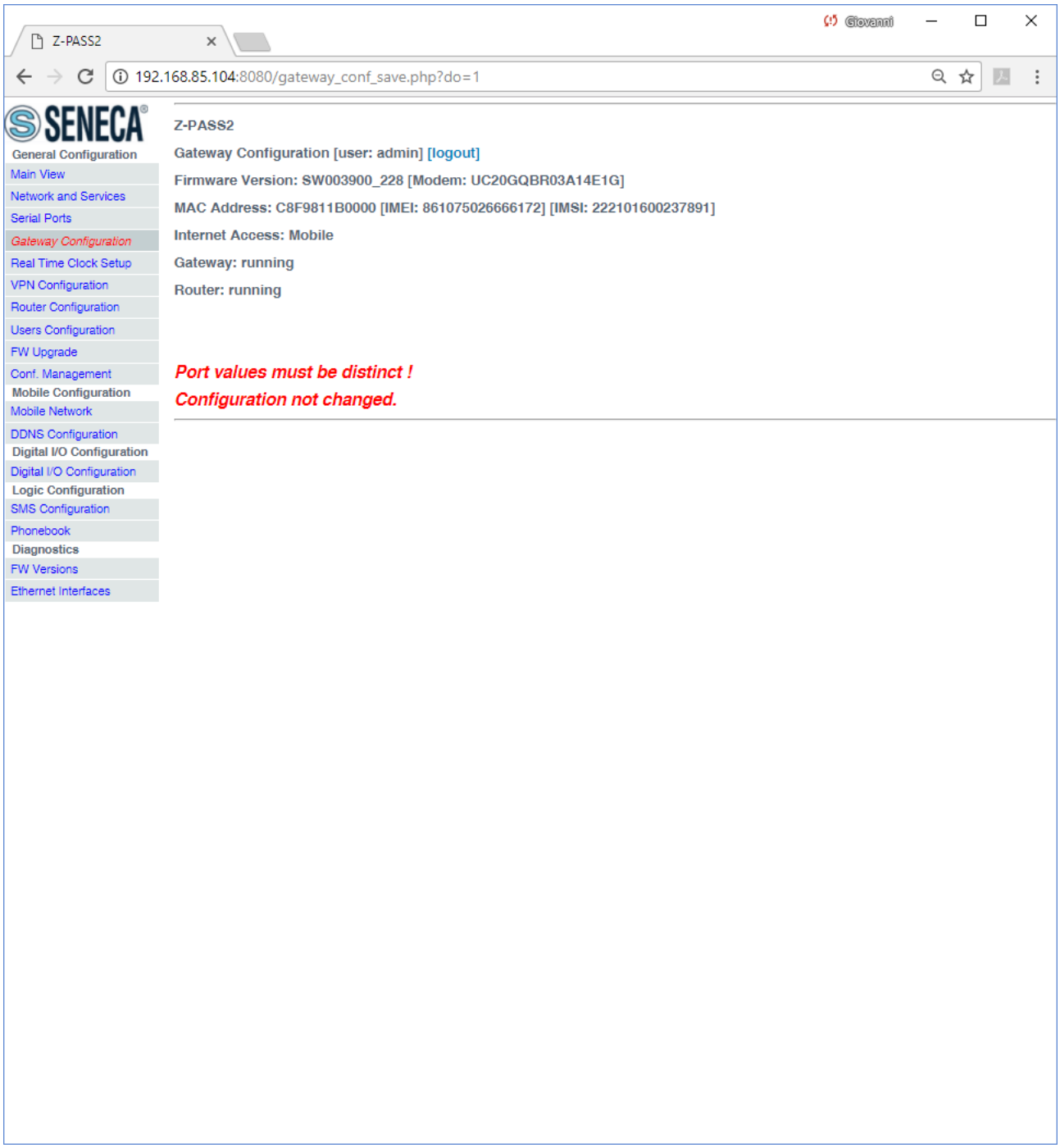
| | | |
|---|---|---|
| | must read the register 49001.<br><br>For example if the regsiter value is:<br><br>0x3DB = 987 = 0000 0011 1101 1011<br><br>Tag 1 = OK<br><br>Tag 2 = OK<br><br>Tag 3 = FAIL<br><br>Tag 4 = OK<br><br>Tag 5 = OK<br><br>Tag 6 = FAIL<br><br>…<br><br>Note that one register before and one register after the Diagnostic Area will be reserved (by default the register 49000 and 49126). | |

Then, for each serial port with “Gateway Mode” = “Modbus Shared Memory”, the parameters described in the following table are available.

| **Field** | **Meaning** | **Default value** |
|---|---|---|
| Task | This parameter defines which Modbus Shared Memory Gateway task is running on the serial port; possibile values are: None, Master, Slave | None |
| Slave Address | Modbus Address for the RTU Slave; this is the only parameter available when Task=Slave | 1 |
| Timeout (ms) [10 – 10000] | Response timeout for Modbus RTU requests, in milliseconds (available only when Task=Master) | 100 |
| Delay between Polls (ms) [10 – 1000] | Interval between Modbus RTU requests, in milliseconds (available only when Task=Master) | 100 |
| Read/Write Retries [0 – 10] | Maximum number of retries for Modbus RTU requests; this always | 0 |

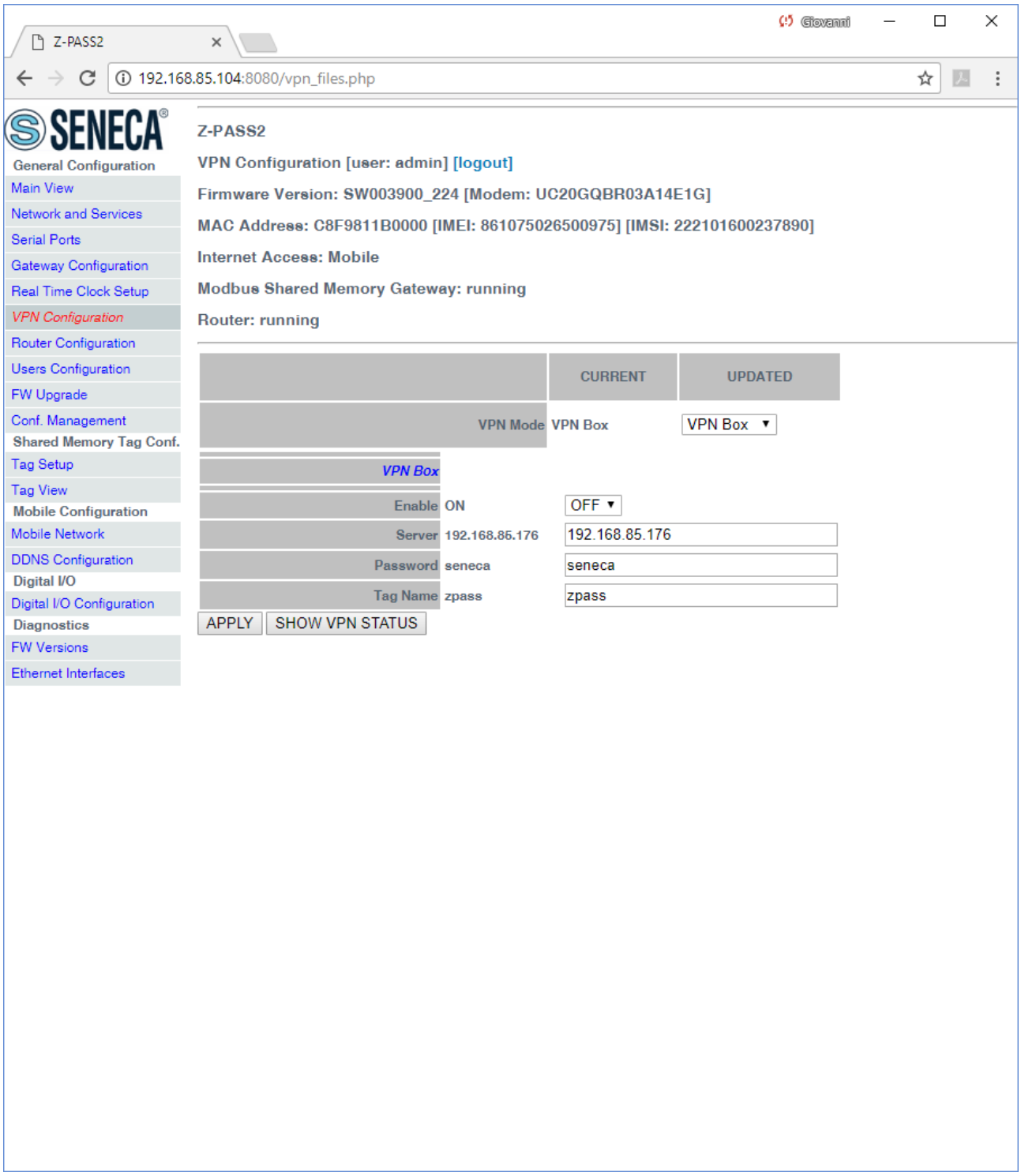
| | | |
|---|---|---|
| | applies to write requests; for read requests, it applies only to tags with “Gateway Tag Mode”=”BRIDGE” (see 20.3.2.1 paragraph) | |
| Multiple Read Max Number [1 – 32] | Maximum number of Modbus registers that can be read in a single Modbus RTU request; this is used to reduce the number of read requests sent on the serial bus, thus performing optimization | 16 |
| Multiple Write Max Number [1 – 32] | Maximum number of Modbus registers that can be written in a single Modbus RTU request; this is used to reduce the number of write requests sent on the serial bus, thus performing optimization | 16 |

Please note that, if any of the configured TCP/UDP port values collide, the configuration is not applied and the following error message is shown:




### 20.1.7 VPN Configuration

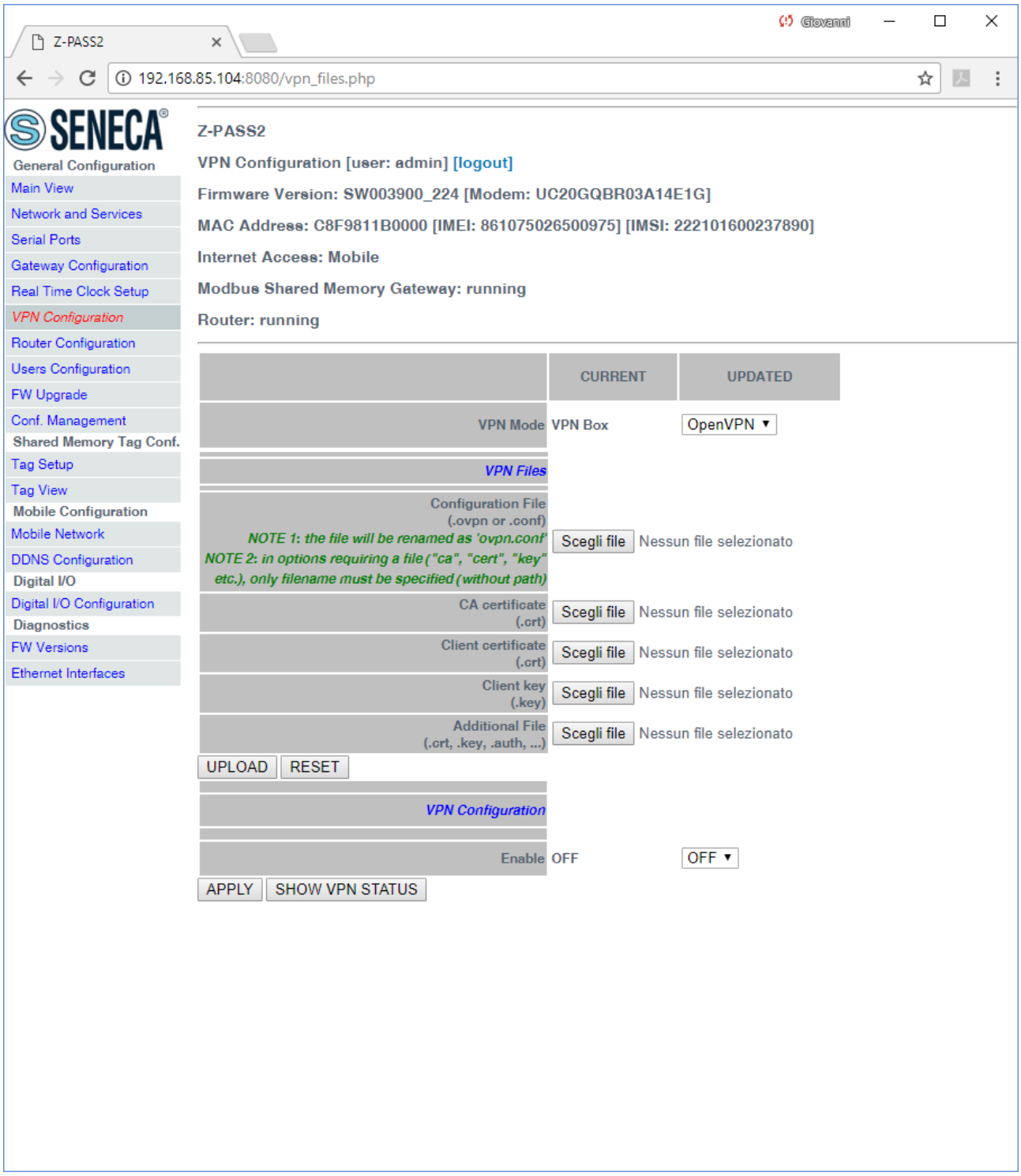
By clicking on the “VPN Configuration” link, in the “Basic Configuration” section, you come to the following page:




The page has a different layout depending on the value of the “VPN Mode” parameter, which can be “OpenVPN” or “VPN Box”.

#### *20.1.7.1 OpenVPN*

The page is made up of two sections: “VPN Files” and “VPN Configuration”.




The “VPN Files” section lets you load the files needed to configure Open VPN and establish a secure VPN connection on the Z-PASS; these files are described in the following.

#### 20.1.7.1.1 Configuration File

This file shall contain all the information needed to configure the Open VPN behaviour; the main configuration options are[18]:

- if Z-PASS shall act as a client or a server (typically, it will be a client)
- the transport protocol (UDP or TCP)
- the server IP address/host name and port
- the files needed to perform authentication procedures
- etc.

This file has the *.ovpn* extension (in Windows systems) or *.conf* extension (in Linux systems); regardless of the original name, it will be renamed as *ovpn.conf* on the Z-PASS.

This is the only mandatory file, that is if this file has not been loaded on the Z-PASS, VPN can't be enabled.

As reminded in the web page, in options requiring a file argument, only the file name shall be given, with no path, as in the following example:

`ca ca.crt` **OK**

`ca /home/config/vpn/ca.crt` **KO !**

Other two important rules that shall be followed are:

- the "dev" option shall be: "`dev tun0`" or "`dev tap0`"
- the "log" option shall be omitted (so that, logs are written to syslog)

An example of a client configuration file is given in paragraph 20.1.7.1.7.

#### 20.1.7.1.2 CA certificate

This file shall contain the Certification Authority (CA) certificate and has the *.crt* extension.

It is needed when the configuration file contains the *"ca"* option.

#### 20.1.7.1.3 Client certificate

This file shall contain the client certificate and has the *.crt* extension.

It is needed when the configuration file contains the *"cert"* option.

#### 20.1.7.1.4 Client key

This file shall contain the client key and has the *.key* extension.

[18] For more information about configuration options, please refer to the OpenVPN web page ("openvpn.net").

It is needed when the configuration file contains the *"key"* option.

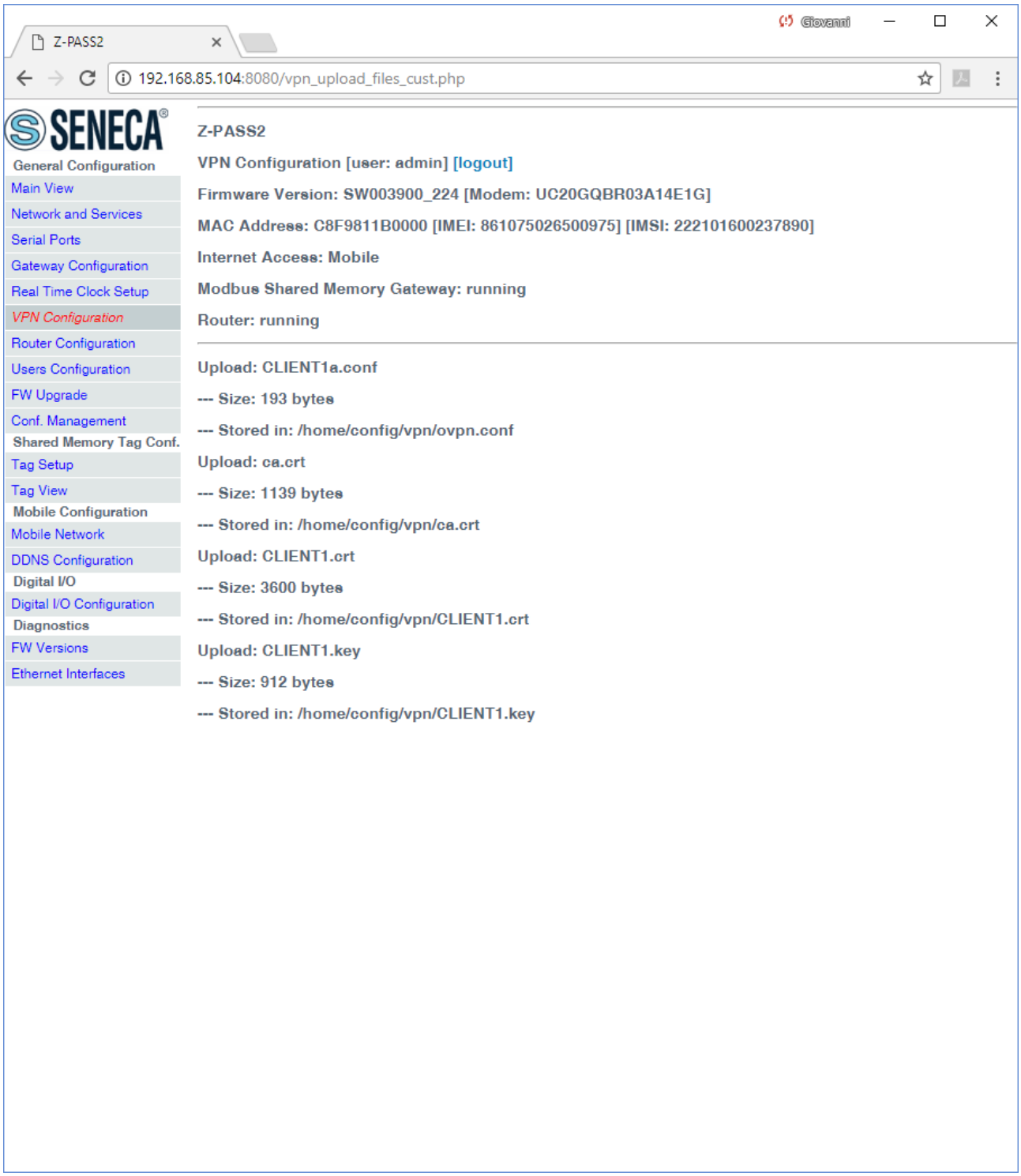
#### 20.1.7.1.5 Additional file

This file can be of any type and may be needed for configuration options other than *"ca"*, *"cert"* and *"key*".

Please note that more than one additional file can be loaded.

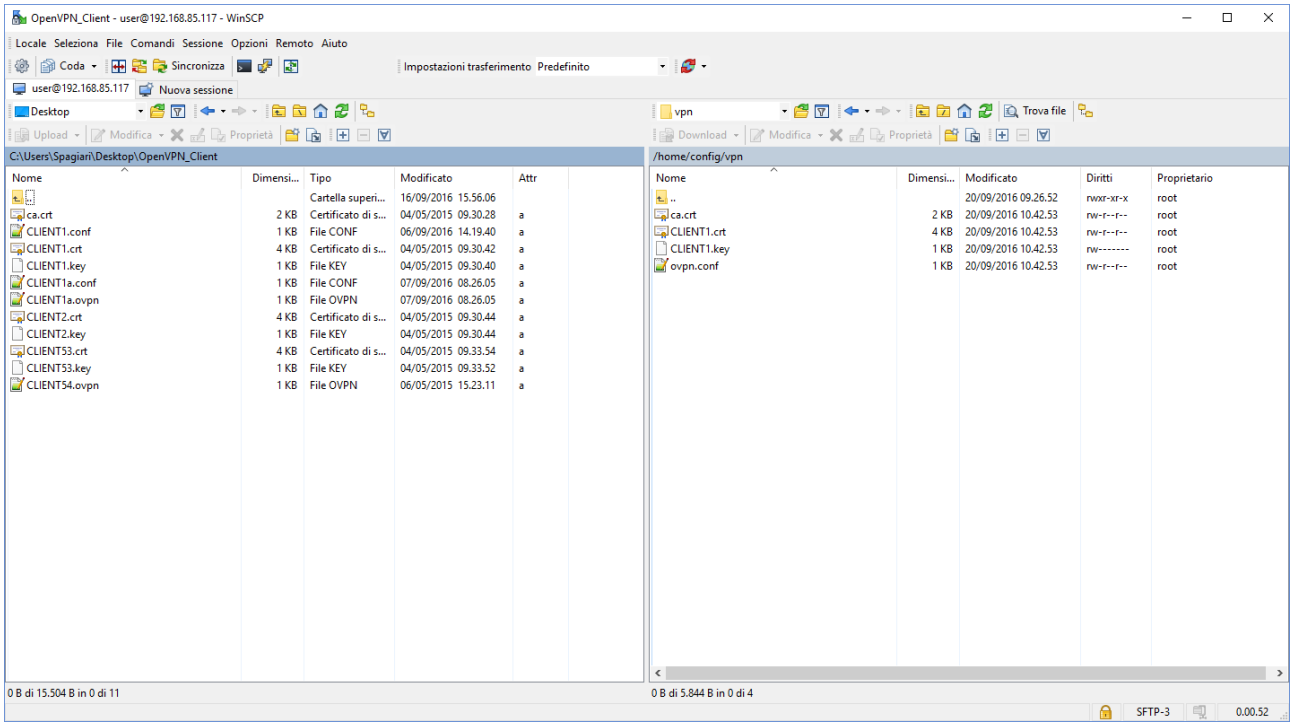
You can browse your PC to select the above files and send them to the Z-PASS by pressing the "UPLOAD" button.

Once the upload is done, a result page is shown like in the following figure.

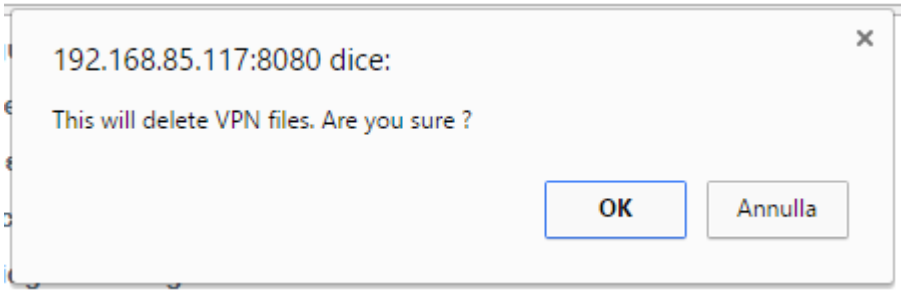

Giovanni
Z-PASS2
192.168.85.104:8080/vpn_upload_files_cust.php
SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces
Z-PASS2
VPN Configuration [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Mobile
Modbus Shared Memory Gateway: running
Router: running
Upload: CLIENT1a.conf
--- Size: 193 bytes
--- Stored in: /home/config/vpn/ovpn.conf
Upload: ca.crt
--- Size: 1139 bytes
--- Stored in: /home/config/vpn/ca.crt
Upload: CLIENT1.crt
--- Size: 3600 bytes
--- Stored in: /home/config/vpn/CLIENT1.crt
Upload: CLIENT1.key
--- Size: 912 bytes
--- Stored in: /home/config/vpn/CLIENT1.key

You can check which VPN files are stored on the Z-PASS by clicking on the “SHOW VPN STATUS” button, as shown in the following figure (remember that the configuration file is renamed as “ovpn.conf”):

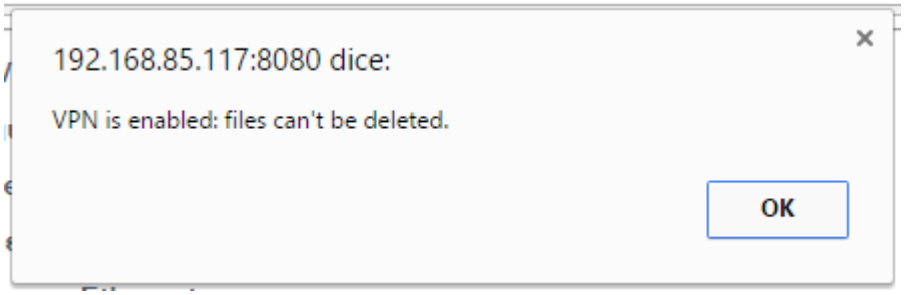
As reminded by the web page, the VPN files can be downloaded from the Z-PASS, if needed, via FTP/SFTP; they can be found in the */home/config/vpn* directory, as shown in the following figure.




Is is possible to clear all the VPN files, by clicking on the "RESET" button; a pop-up will appear, requiring a confirmation:



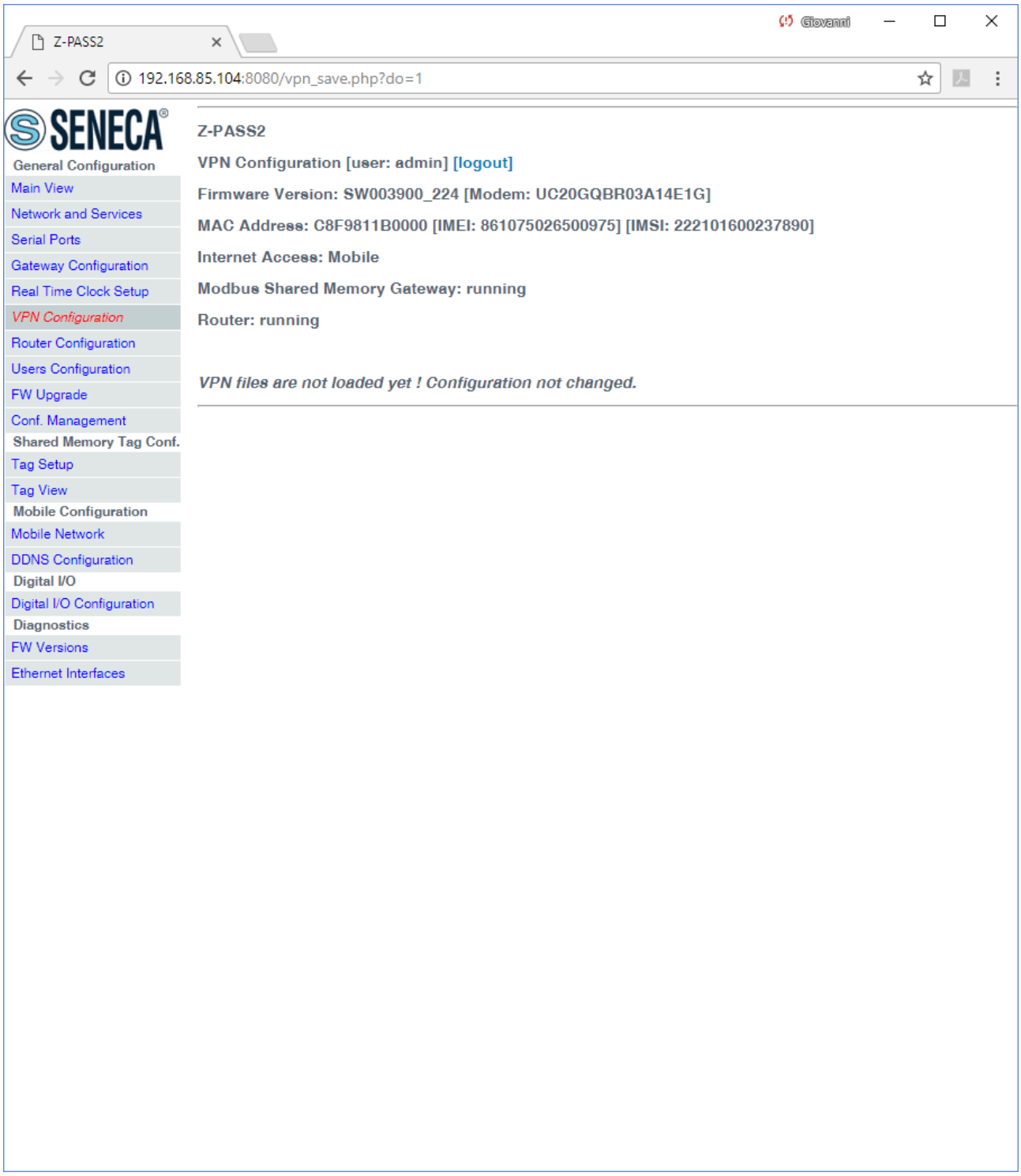

If VPN is enabled, the user is not allowed to delete VPN files, as warned by the following pop-up:



In the “VPN Configuration” section, there is only one parameter, as described in the following table:

| Field | Meaning | Default value |
|---|---|---|
| VPN Configuration/Enable | Flag to enable/disable the VPN connectivity; when enabled, Z-PASS will run the Open VPN process with the loaded configuration | OFF |

As already told above, if you try to enable the VPN connectivity, but no configuration file has been uploaded to the Z-PASS yet, an error is given as shown in the following figure:



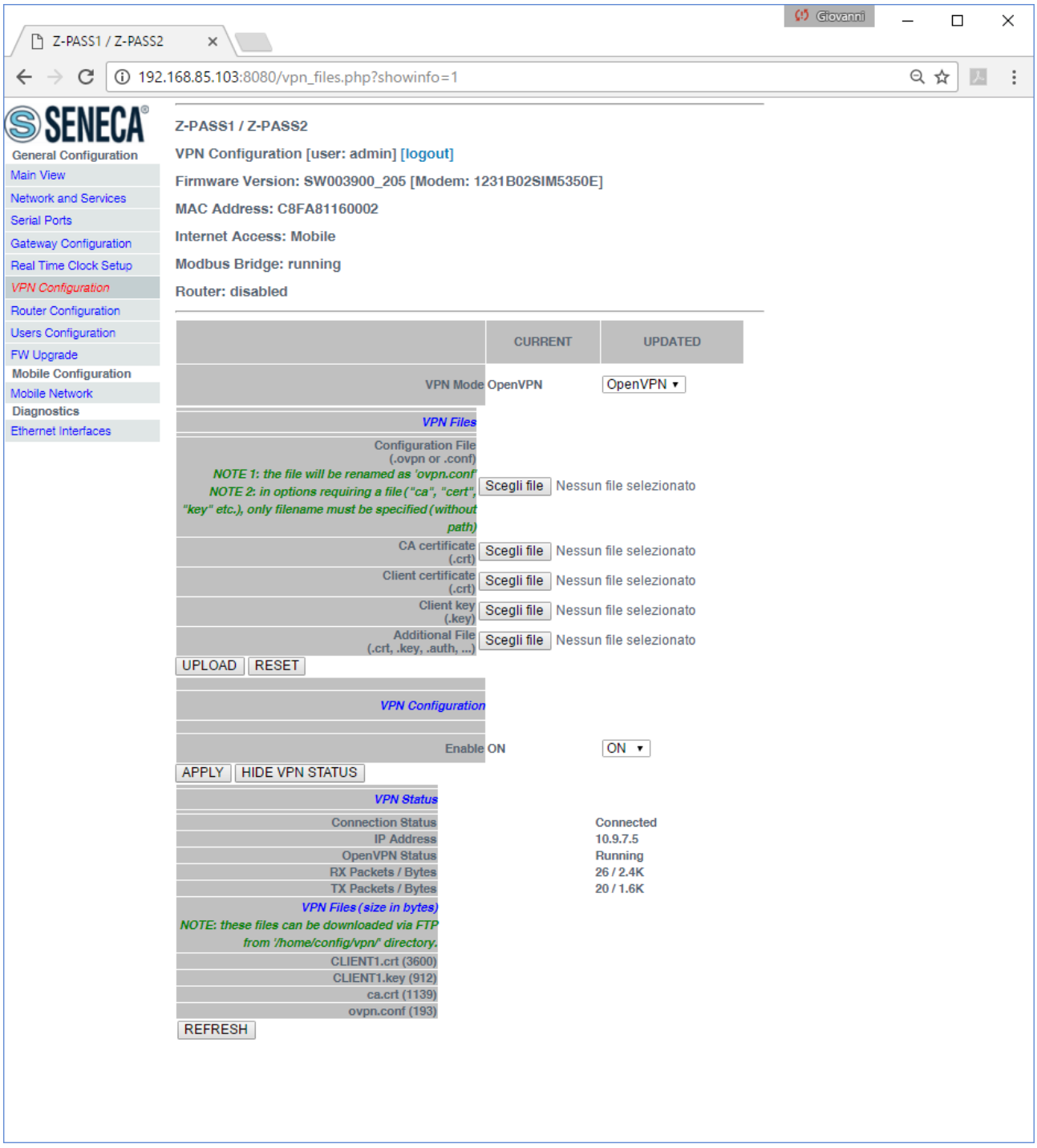

When you click on the “SHOW VPN STATUS” button, a third section appears, named “VPN Status”, showing:

- the VPN “Connection Status” (i.e.: “Disconnected” or “Connected”)
- the IP address assigned to the VPN interface when “Connected”, the “dummy” IP address “0.0.0.0” when “Disconnected”
- the “OpenVPN Status” (i.e.: “Stopped” or “Running”)

- the number of packets/bytes received from the VPN interface, when connected; “0/0” when disconnected
- the number of packets/bytes sent to the VPN interface, when connected; “0/0” when disconnected
- the VPN files stored on the Z-PASS (see above)

as shown in the following couple of figures:


Giovanni
Z-PASS2
192.168.85.104:8080/vpn_files.php?showinfo=1
SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces
Z-PASS2
VPN Configuration [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Mobile
Modbus Shared Memory Gateway: running
Router: running
CURRENT
UPDATED
VPN Mode
OpenVPN
OpenVPN
VPN Files
Configuration File (.ovpn or .conf)
NOTE 1: the file will be renamed as 'ovpn.conf'
NOTE 2: in options requiring a file ("ca", "cert", "key" etc.), only filename must be specified (without path)
Scegli file
Nessun file selezionato
CA certificate (.crt)
Client certificate (.crt)
Client key (.key)
Additional File (.crt, .key, .auth, ...)
UPLOAD
RESET
VPN Configuration
Enable
OFF
OFF
APPLY
HIDE VPN STATUS
VPN Status
Connection Status
Disconnected
IP Address
0.0.0.0
OpenVPN Status
Stopped
RX Packets / Bytes
0 / 0
TX Packets / Bytes
0 / 0
VPN Files (size in bytes)
NOTE: these files can be downloaded via FTP from '/home/config/vpn/' directory.
CLIENT1.crt (3600)
CLIENT1.key (912)
ca.crt (1139)
ovpn.conf (218)
REFRESH




An important status information is given by the “OpenVPN Status” field; if VPN is enabled (“ON”), but this status is “Stopped”, this means that Open VPN process could not be correctly started: probably, the configuration file contains some errors or, maybe, some options not supported by the Z-PASS Open VPN implementation.

You can refresh the VPN status, by clicking on the “REFRESH” button.

Finally, you can hide the “VPN Status” section, by clicking on the “HIDE VPN STATUS” button.

#### 20.1.7.1.6 OpenVPN Server configuration file

This paragraph gives an example of OpenVPN server configuration; this is the server configuration typically used with Z-PASS devices.

```
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server 10.9.7.0 255.255.255.0
ifconfig-pool-persist ipp.txt
client-config-dir ccd
client-to-client
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
verb 3
```

#### 20.1.7.1.7 OpenVPN Client configuration file

This paragraph gives an example of OpenVPN client configuration; this is the client configuration typically loaded on Z-PASS devices.

```
client
dev tun
port 1194
proto udp
remote 2.192.5.105 1194
nobind
ca ca.crt
cert tws4.crt
key tws4.key
comp-lzo
persist-key
persist-tun
script-security 3 system
verb 3
```

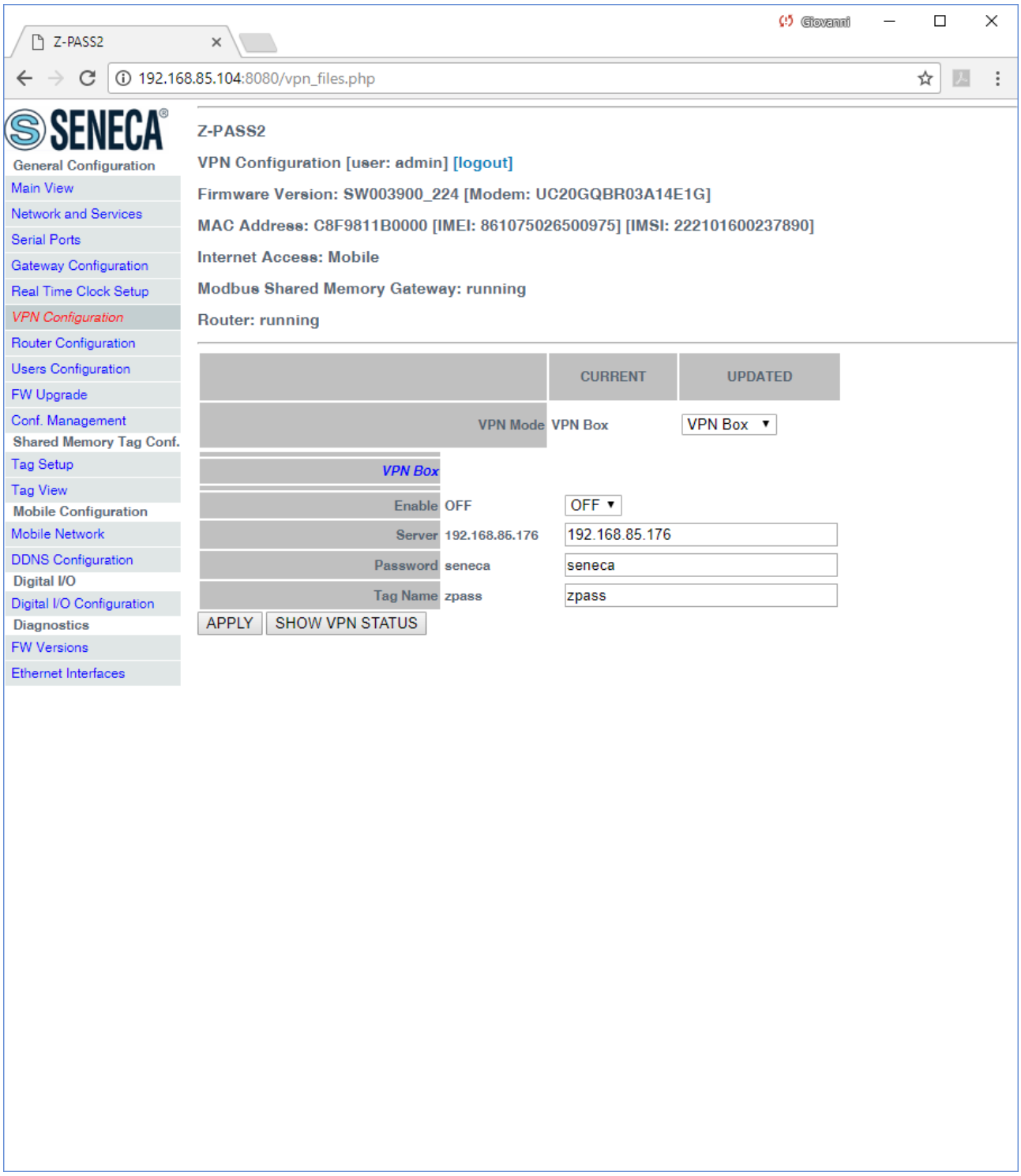
#### 20.1.7.1.8 LED signalling

In Z-PASS products, when VPN functionality is enabled in “OpenVPN” mode, the “SERV” and “VPN“ LEDs give the following status information (see paragraph **Errore. L'origine riferimento non è stata trovata.**):

| LED | Status | Meaning |
|---|---|---|
| VPN Yellow | ON<br><br>Blinking<br><br>OFF | VPN connection is working properly<br><br>VPN connection is not working properly<br><br>VPN functionality is disabled |
| SERV Green | - | Not used |

#### *20.1.7.2 VPN Box*

The page contains only ony section: “VPN Box”, as shown in the following figure.




The “VPN Box” section contains the following parameters:

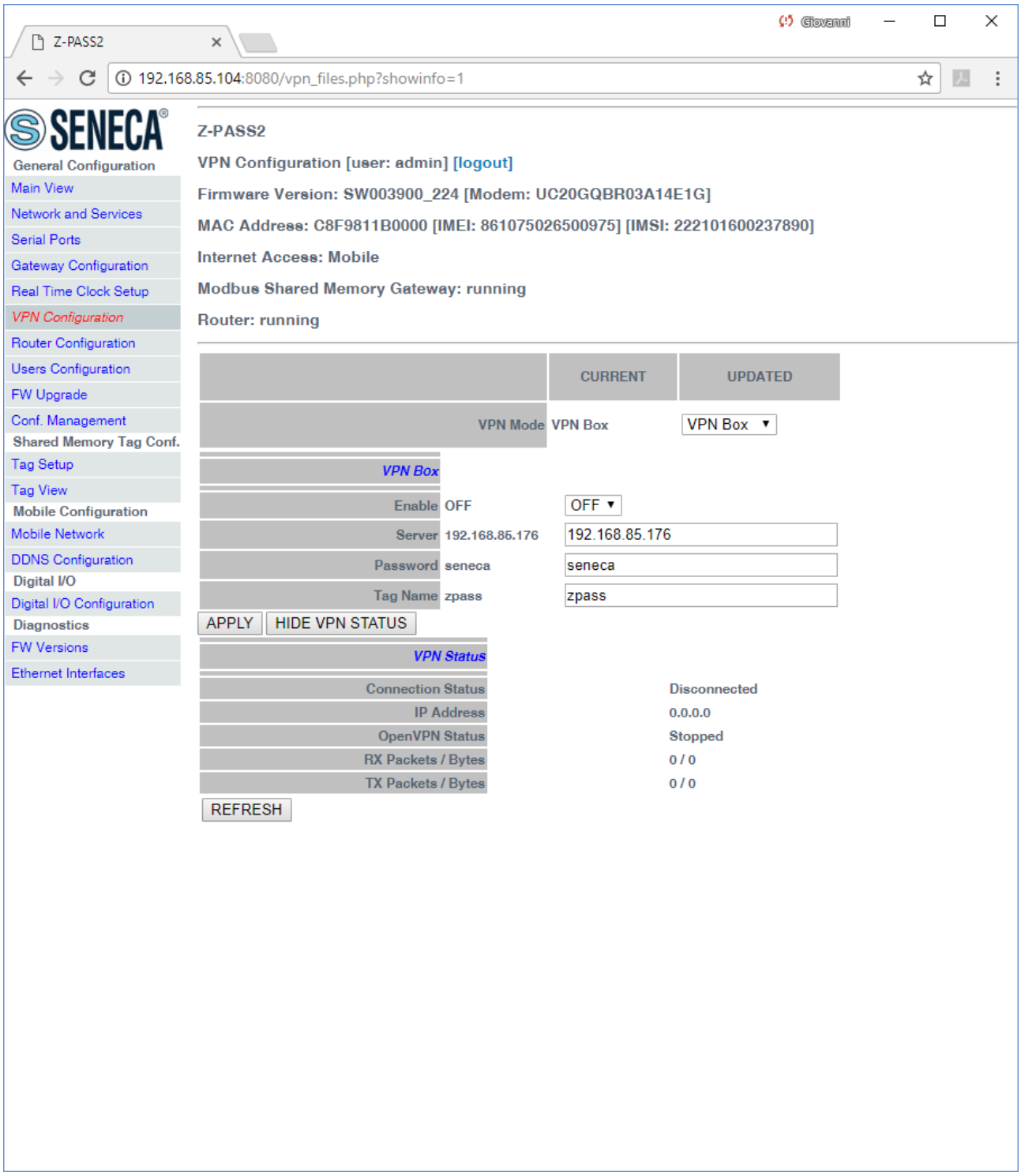
| Field | Meaning | Default value |
|---|---|---|
| VPN BOX/Enable | Flag to enable/disable the “VPN Box” functionality, that is the procedure/protocol that lets the Z- | OFF |

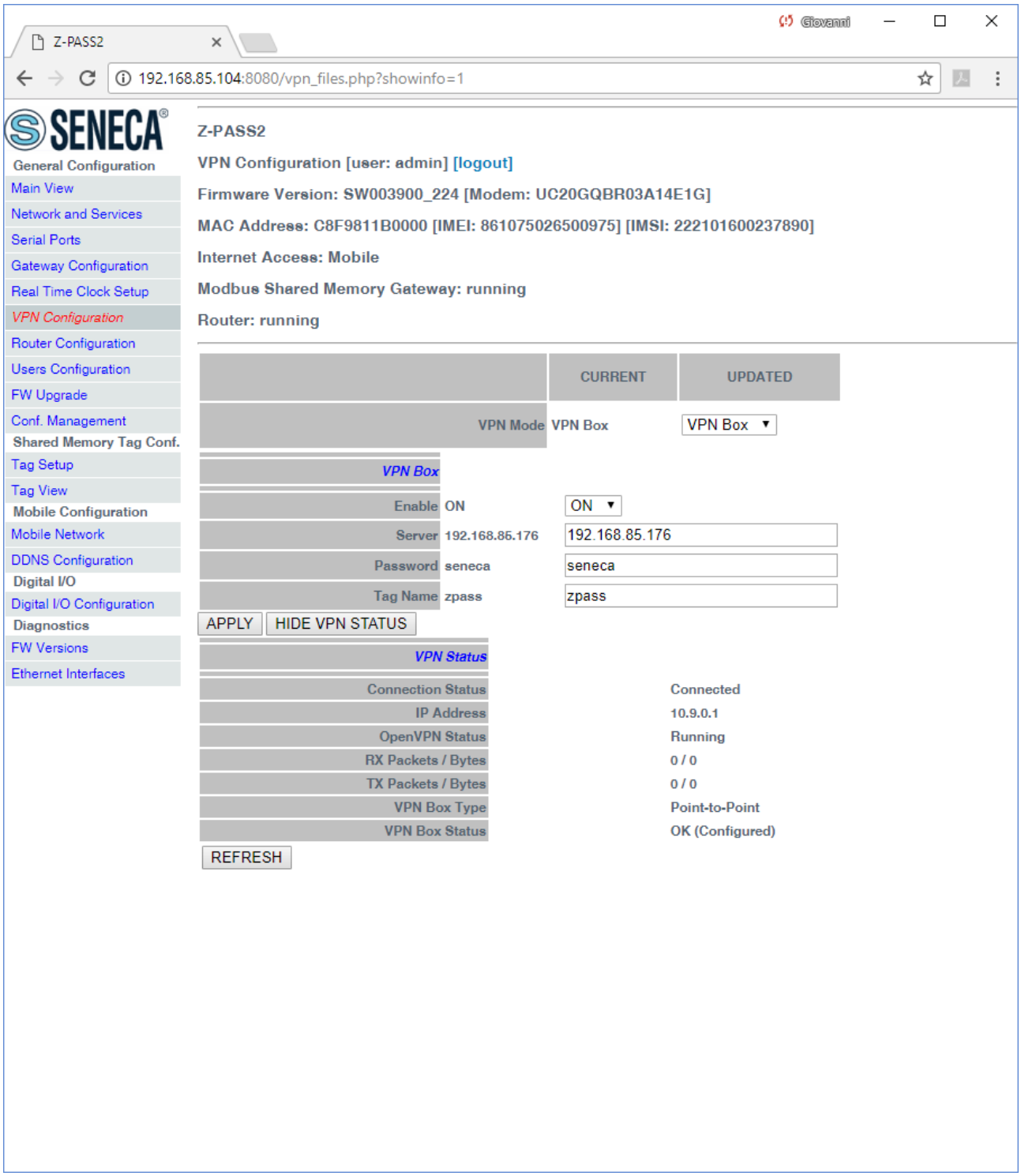
| | | |
|---|---|---|
| | PASS setup the VPN, by interacting with the “VPN Box” server (see “VPN Box User Manual”) | |
| VPN BOX/Server | IP address or FQDN of the “VPN Box” server | 192.168.90.1 |
| VPN BOX/Password | Password to access the “VPN Box” server | seneca |
| VPN BOX/Tag Name | Mnemonic name used to uniquely identify the Z-PASS; if the default (“zpass”) value is left, the Device will register as “zpass_<MACAddress>” on the VPN Box | zpass |

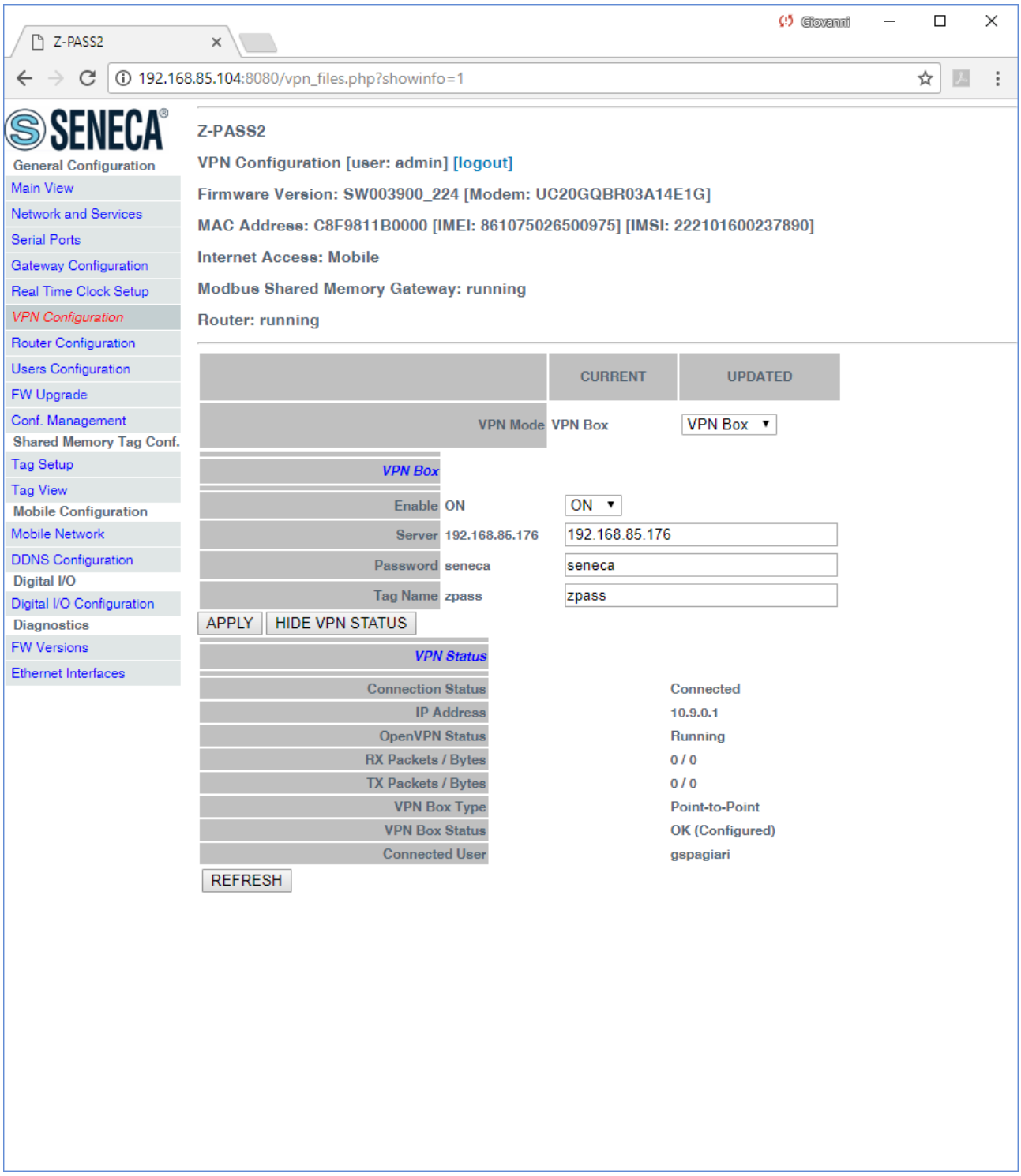
When you click on the “SHOW VPN STATUS” button, a new section appears, named “VPN Status”, showing:

- the VPN “Connection Status” (i.e.: “Disconnected” or “Connected”)
- the VPN IP address assigned to the Z-PASS when “Connected”, the “dummy” IP address “0.0.0.0” when “Disconnected”; this row is not shown for “Point-to-Point (L2)” VPN Box, since no IP address is assigned to the VPN interface
- the “OpenVPN Status” (i.e.: “Stopped” or “Running”)
- the number of packets/bytes received from the VPN interface, when connected; “0/0” when disconnected
- the number of packets/bytes sent to the VPN interface, when connected; “0/0” when disconnected
- the “VPN Box Type”, which can be “Point-to-Point”, “Point-to-Point (L2)” or “Single LAN”, if VPN Box is enabled
- the “VPN Box Status”, if VPN Box is enabled
- the username of the connected user, if any

as shown in the following three figures:


Giovanni
Z-PASS2
192.168.85.104:8080/vpn_files.php?showinfo=1
SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces
Z-PASS2
VPN Configuration [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Mobile
Modbus Shared Memory Gateway: running
Router: running
CURRENT
UPDATED
VPN Mode
VPN Box
VPN Box
Enable
OFF
OFF
Server
192.168.85.176
192.168.85.176
Password
seneca
seneca
Tag Name
zpass
zpass
APPLY
HIDE VPN STATUS
VPN Status
Connection Status
Disconnected
IP Address
0.0.0.0
OpenVPN Status
Stopped
RX Packets / Bytes
0 / 0
TX Packets / Bytes
0 / 0
REFRESH


Giovanni
Z-PASS2
192.168.85.104:8080/vpn_files.php?showinfo=1
SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces
Z-PASS2
VPN Configuration [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Mobile
Modbus Shared Memory Gateway: running
Router: running
CURRENT
UPDATED
VPN Mode
VPN Box
VPN Box
VPN Box
Enable
ON
ON
Server
192.168.85.176
192.168.85.176
Password
seneca
seneca
Tag Name
zpass
zpass
APPLY
HIDE VPN STATUS
VPN Status
Connection Status
Connected
IP Address
10.9.0.1
OpenVPN Status
Running
RX Packets / Bytes
0 / 0
TX Packets / Bytes
0 / 0
VPN Box Type
Point-to-Point
VPN Box Status
OK (Configured)
REFRESH




For an explanation of the differences between a “Single LAN” VPN and a “Point-to-Point” VPN, see chapter 9.

The “VPN Box Status” string has the following format:

Result (Status)

The following table gives a short explanation of the possible “Result” and “Status” strings:

| Result | Status | Meaning |
|---|---|---|
| Error (Unexpected response) | | A response code has been received that is not handled by the Z-PASS (it should never occur) |
| Error (No response from VPN Box) | | No response has been received from the VPN Box (response timeout) |
| Error (Invalid response from VPN Box) | | A response has been received whose content is not valid for the Z-PASS (it should never occur) |
| Error (Wrong password) | | The password set on Z-PASS is wrong |
| Error (License Limit Reached) | | The maximum number of devices allowed by the license are already registered on VPN Box |
| Error (VPN Box not configured) | | The VPN Box has not been configured yet |
| Error (Generic error) | | A generic error has occurred on the VPN Box |
| OK | | The Z-PASS has just been registered on the VPN Box |
| OK | New | The Z-PASS is registered on the VPN Box, but it is not configured yet (“Single LAN” only) |
| OK | Configuration updated | The Z-PASS configuration has just been updated |
| OK | Configured | The Z-PASS is properly configured and available for VPN connection |
| OK | Ban | The Z-PASS has been banned |
| OK | Not found | The Z-PASS is unknown for the VPN Box; this happens when Z-PASS registration is deleted on the VPN Box |
| OK | Unknown | The Z-PASS has an “unknown” status in the VPN Box (it should never occur) |
| OK | Not bound | The “tunnel” between the Z-PASS and the VPN Box is not up; this may occur when the tunnel port is blocked (“not open”) in the ADSL router on the VPN Box side (“Point-to-Point” only) |
| OK | Unexpected status | A status code has been received that is not handled by the Z-PASS (it should never occur) |

You can refresh the VPN status, by clicking on the “REFRESH” button.

Finally, you can hide the “VPN Status” section, by clicking on the “HIDE VPN STATUS” button.

#### 20.1.7.2.1 LED signalling

In Z-PASS products, when VPN functionality is enabled in “VPN Box/Single LAN” mode, the “SERV” and “VPN“ LEDs give the following status information (see paragraph **Errore. L'origine riferimento non è stata trovata.**):

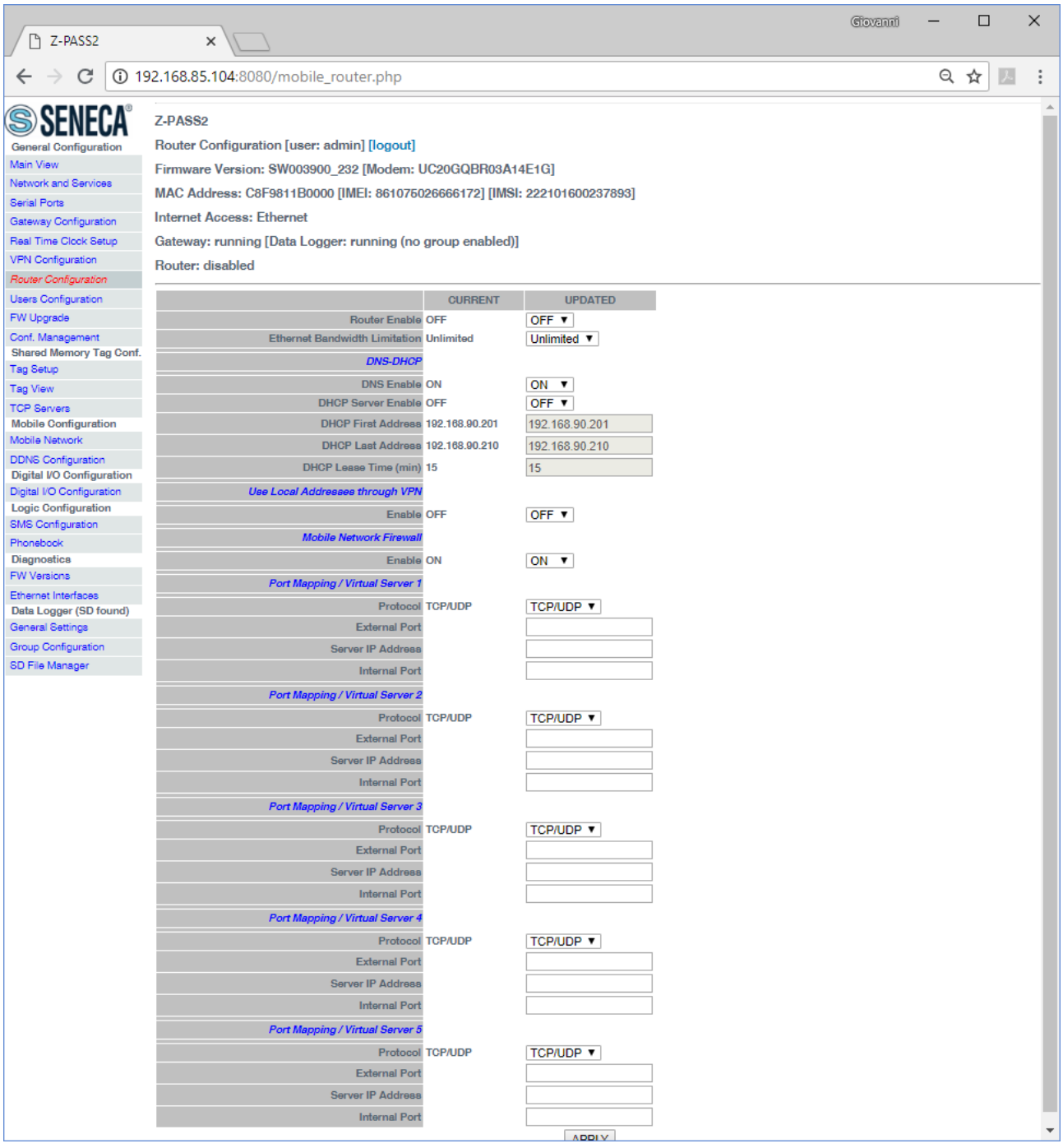
| LED | Status | Meaning |
|---|---|---|
| VPN Yellow | ON | VPN connection is working properly |
| | Blinking | VPN connection is not working properly |
| | OFF | The Device has not been configured by the VPN Box yet or VPN Box functionality is disabled |
| SERV Green | ON | VPN Box "SERVICE" connection is working properly |
| | Blinking | VPN Box "SERVICE" connection is not working properly |
| | OFF | VPN Box functionality is disabled |

Similarly, when VPN functionality is enabled in "VPN Box/Point-to-Point" mode, the "SERV" and "VPN" LEDs give the following status information (see paragraph **Errore. L'origine riferimento non è stata trovata.**):

| LED | Status | Meaning |
|---|---|---|
| VPN Yellow | ON | A VPN client is connected to the Device |
| | OFF | No VPN client is connected to the Device or VPN Box functionality is disabled |
| SERV Green | ON | VPN Box "SERVICE" connection is working properly |
| | Blinking | VPN Box "SERVICE" connection is not working properly |
| | OFF | VPN Box functionality is disabled |

### *20.1.8 Router Configuration*

By clicking on the "Router Configuration" link, in the "Basic Configuration" section, you come to the following page:




In this page, you can change the parameters related to the Z-PASS Router functionality.

First, you have a set of general parameters, as listed in the following table:

| Field | Meaning | Default value |
|---|---|---|
| Router Enable | Flag to enable/disable the Router functionality | OFF |
| Ethernet Bandwidth Limitation | This parameter can be used to limit | Unlimited |

| | | |
|---|---|---|
| | the bandwidth on the ethernet interfaces; this may be needed to avoid overloading the CPU, when a large amount of data is forwarded from one interface to the other (LAN ↔ WAN).<br>Since this does not occur when the two ethernet interfaces work in "switch" mode, the parameter is not shown when "Ethernet Mode" parameter is set to "Switch" (see paragraph 20.1.2).<br>Possible values are:<br>Unlimited<br>20 Mbit/s<br>10 Mbit/s<br>1 Mbit/s | |
| DNS Enable | Flag to enable/disable the DNS forwarding service | ON |
| DHCP Server Enable | Flag to enable/disable the DHCP service (DHCP server)<br>NOTE: this parameter can be set to "ON" only if the "DHCP" parameter of the "Network and Services" page is set to "OFF". | OFF |
| DHCP First Address<br>DHCP Last Address | These parameters define the range of IP addresses assigned by the DHCP server to requesting clients | 192.168.90.201<br>192.168.90.210 |
| DHCP Lease Time (min) | Validity time interval for the IP address assignment, in minutes.<br>Possible values are in the range [1..60]. | 15 |

Then, you have the parameter shown in the following table.

| **Field** | **Meaning** | **Default value** |
|---|---|---|
| Use Local Addresses Through VPN/Enable | Flag to enable/disable the access to the Z-PASS and other devices which are in the Z-PASS LAN, by using their local (LAN) IP addresses | OFF |

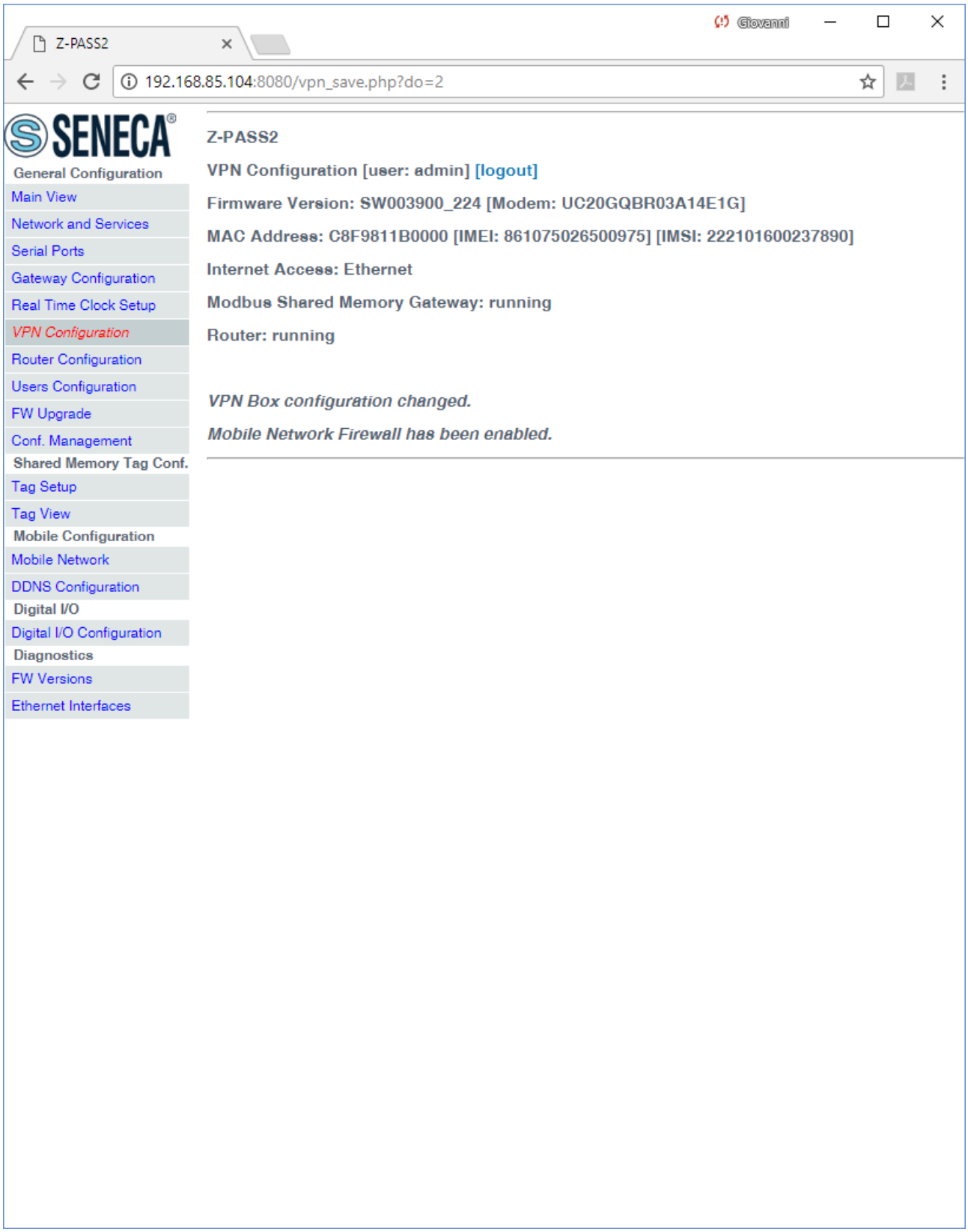
Then, you have another important parameter, which is shown in the following table.

| Field | Meaning | Default value |
|---|---|---|
| Mobile Network Firewall/Enable | Flag to enable/disable the "Mobile Network Firewall", that is disable/enable access to the Z-PASS and other devices which are in the Z-PASS LAN, by using the IP address assigned to the Mobile Network (3G) interface.<br>To open a port in the firewall, a "Port Mapping / Virtual Server" rule shall be defined. | OFF |

The above parameter shall be set to ON, to protect the Z-PASS against undesired (maybe malicious) accesses.

This is the only parameter in the "Router Configuration" page that is working also when the Router functionality is disabled (Router Enable = OFF).

It is important to note that, when the VPN is activated (see 20.1.7 paragraph), the parameter is automatically set to ON, as warned by the message shown in the following figure.


Giovanni
Z-PASS2
192.168.85.104:8080/vpn_save.php?do=2
SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces
Z-PASS2
VPN Configuration [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Ethernet
Modbus Shared Memory Gateway: running
Router: running
VPN Box configuration changed.
Mobile Network Firewall has been enabled.

Finally, there are 5 sections which let you define up to 5 “Port Mapping” rules (also known as “Virtual Servers”); for each section, the available parameters are the following:

| **Field** | **Meaning** | **Default value** |
|---|---|---|
| Protocol | This parameter defines the transport protocol (or kind of port) which is affected by the rule: TCP, UDP or both | TCP/UDP |
| External Port | TCP or UDP port which a packet was originally sent to | *Empty* |
| Server IP Address | IP address which the received packet is forwarded to | *Empty* |
| Internal Port | TCP or UDP port which the received packet is forwarded to | *Empty* |

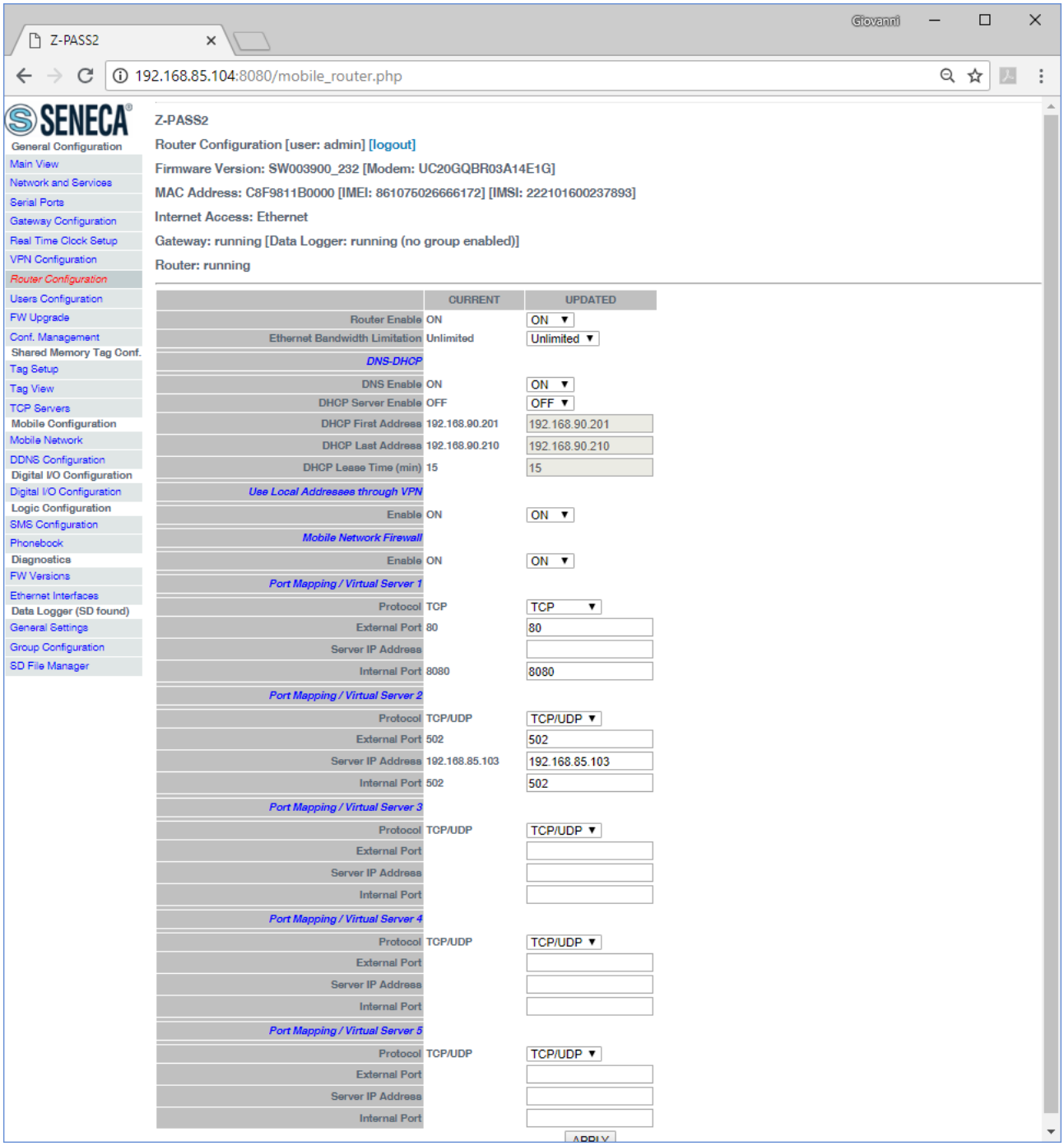
If Router is left disabled (Router Enabled = OFF), you can still change parameters; changes will be saved without actually applying them (except for the “Mobile Network Firewall” parameter, as told before); the following message will be given, after clicking the “APPLY” button:


Giovanni
Z-PASS2
192.168.85.104:8080/mobile_router_save.php?do=1
SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces
Z-PASS2
Router Configuration [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Ethernet
Modbus Shared Memory Gateway: running
Router: disabled
Router Configuration changed (router not active).

If you try to enable the DHCP server functionality (DHCP Enable = ON), but the “DHCP First Address” and “DHCP Last Address” parameters define an address range that is not congruent with the Ethernet configuration (IP address and network mask), an error is given, as shown in the following figure:


As already told before, the Router configuration page lets you define up to 5 “Port Forwarding” rules or “Virtual Servers”.

An example is given in the following figure:

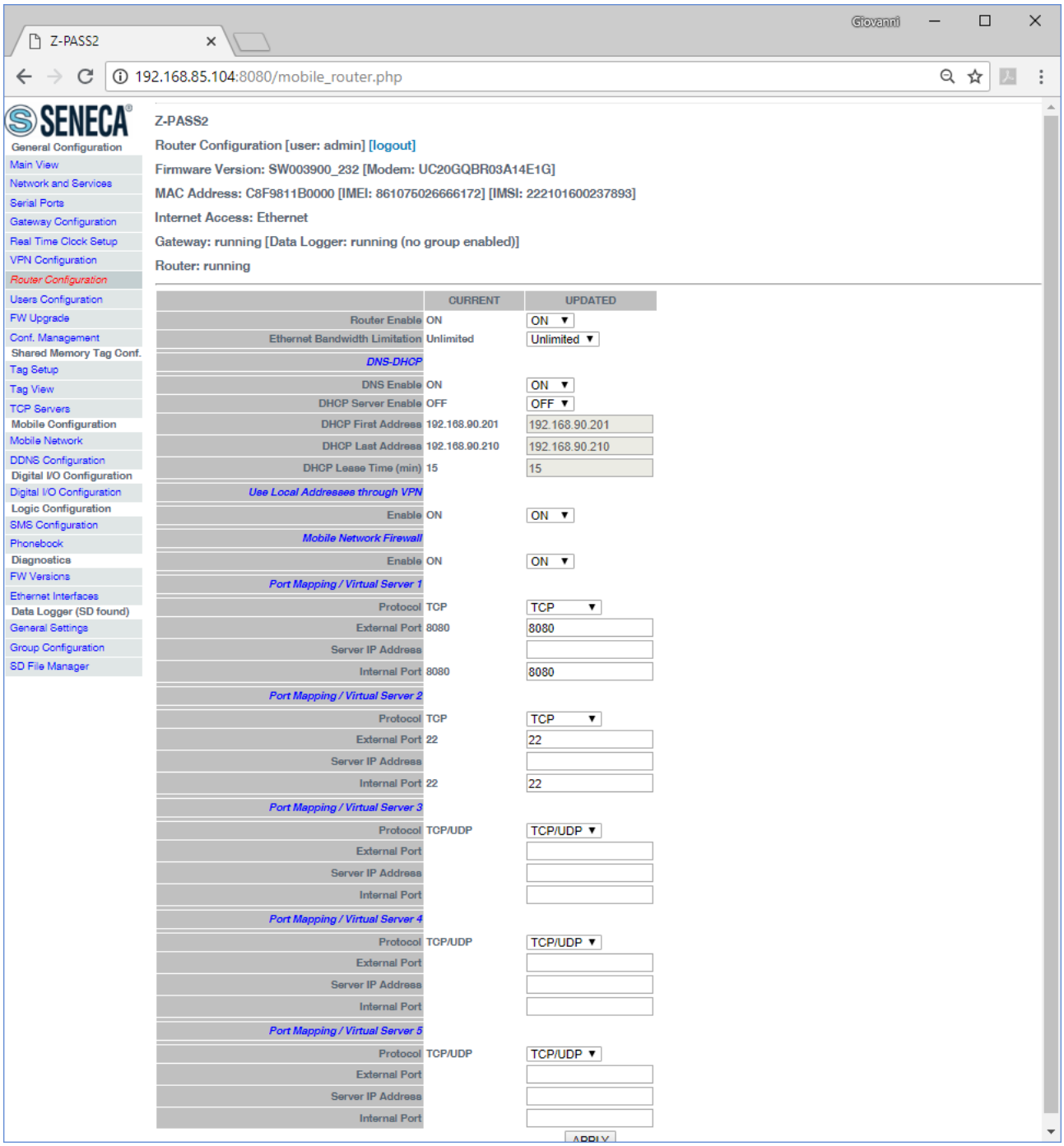



In this example, 2 rules have been set:

- the first rule tells Z-PASS that any TCP packet received on the 80 (HTTP) port has to be forwarded to the 8080 port, leaving the original destination IP address unchanged; so, this rule lets you access the Z-PASS configuration web site on the standard HTTP port;

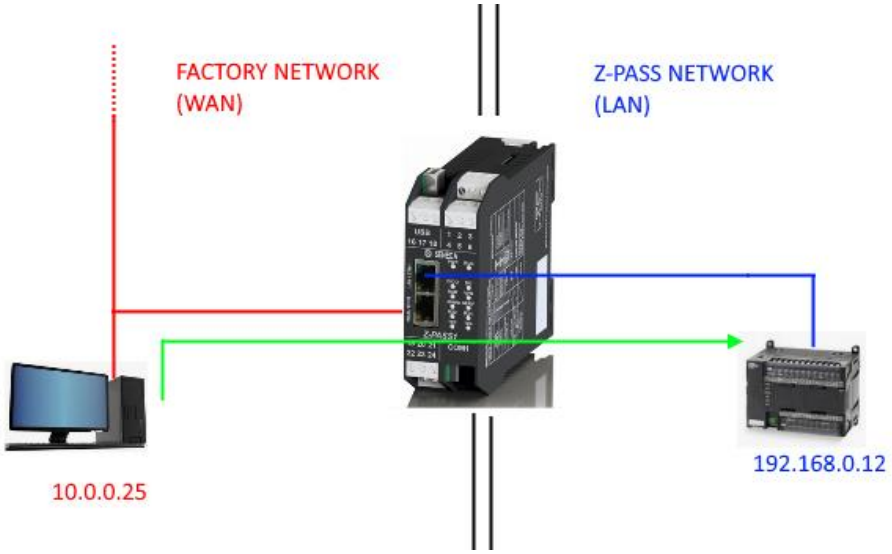
- the second rule tells Z-PASS that any TCP or UDP packet received on the 502 port (which is often used for Modbus TCP protocol) shall be forwarded to the 192.168.85.103 IP address (which corresponds to another device) on the same (502) destination port.

Another important aspect of “Port Mapping / Virtual Server” rules is that they let define which ports are open in the “Mobile Network Firewall”; for example, if you want to connect to the web configuration site and to the SSH console, through the public IP address assigned to the 3G interface, the 8080 and 22 TCP ports shall be open; this can be done as shown in the following figure.

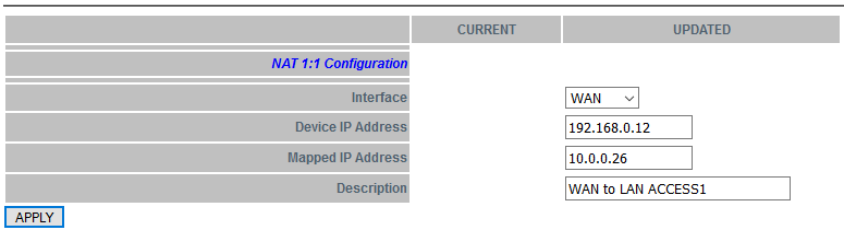


### 20.1.9 NAT 1:1 RULES

You can use this feature for access a device (for example) from WAN to the LAN (a PC in the WAN network that must obtain data from a PLC in the LAN network):




For to do this you must create a new address (10.0.0.26) that is in a compatible network with the PC (10.0.0.25) so:




Now the PLC 192.168.0.12 is accessible from the WAN using the 10.0.0.26 address.

***WARNING!***

***In SWITCH mode this feature is not available (only in LAN/WAN mode)!***

### 20.1.10 STATIC ROUTES

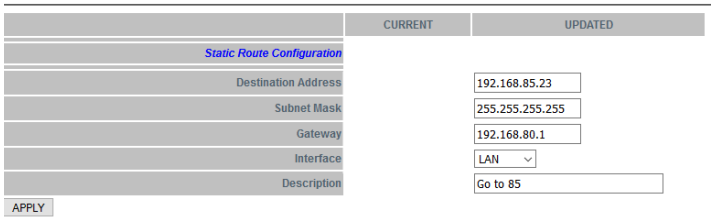
Use this function for route an address or a range of addresses to different gateways.

For example if you must reach 2 different addresses: 192.168.85.23 and 192.168.82.56 but you need to pass from 2 different gateways.

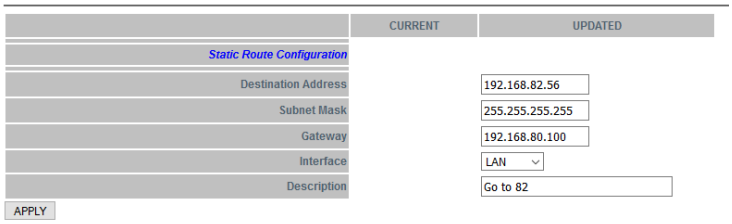
1) For access to the 192.168.85.23 you must pass from the 192.168.80.1 Gateway

2) For access to the 192.168.82.56 you must pass from the 192.168.80.100 Gateway

So you must configure:

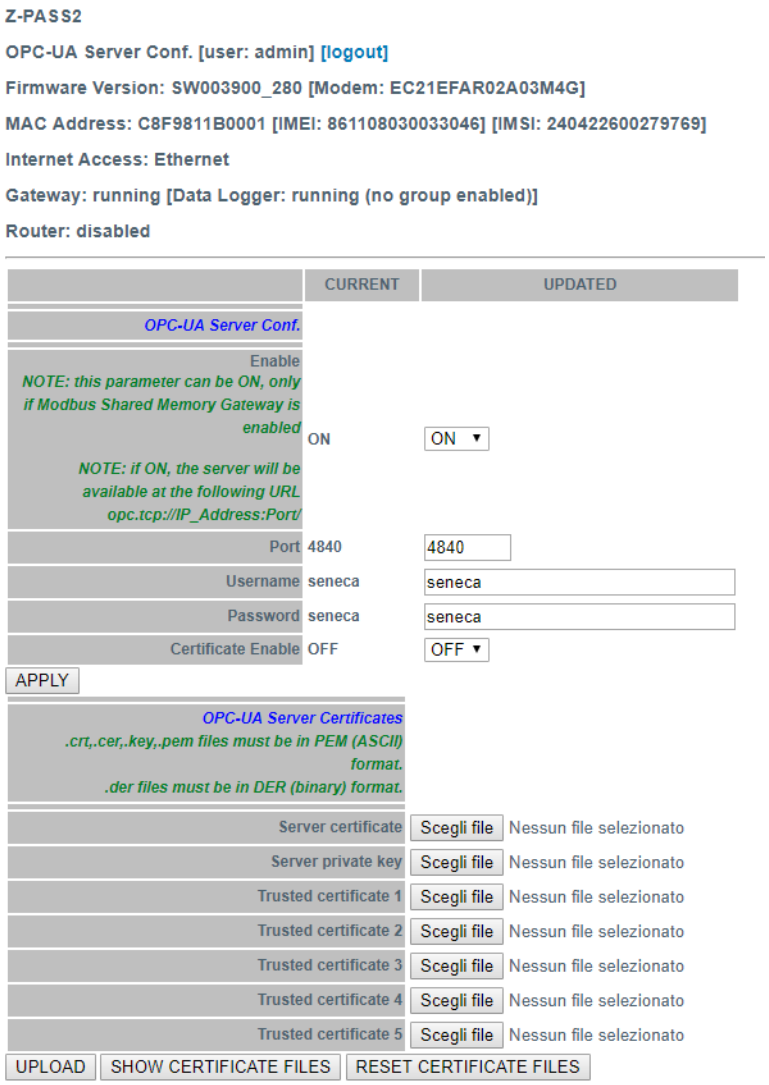



And then:




### 20.1.11 OPC-UA Server Configuration

By clicking on the “OPC-UA Server Conf.” link, in the “Basic Configuration” menu, you come to the following page:




In this page, you can set the parameters related to the OPC Unified Architecture (OPC-UA) server, as listed in the following table:

| Field | Meaning | Default value |
|---|---|---|
| Enable | Flag to enable/disable the OPC-UA server functionality | OFF |
| Port | OPC-UA server TCP port | 4840 |
| Username | Username that an OPC-UA Client shall use to connect to the server | empty |
| Password | Password that an OPC-UA Client shall use to connect to the server | empty |
| Security Policy | Select between “None” Or “None, Basic128Rsa15, Basic256Sha256” | “None” |

| | | |
|---|---|---|
| | Note: A predefined couple of certifates are inlcuded in the Z-PASS. | |

You can add yours certificates with the buttons

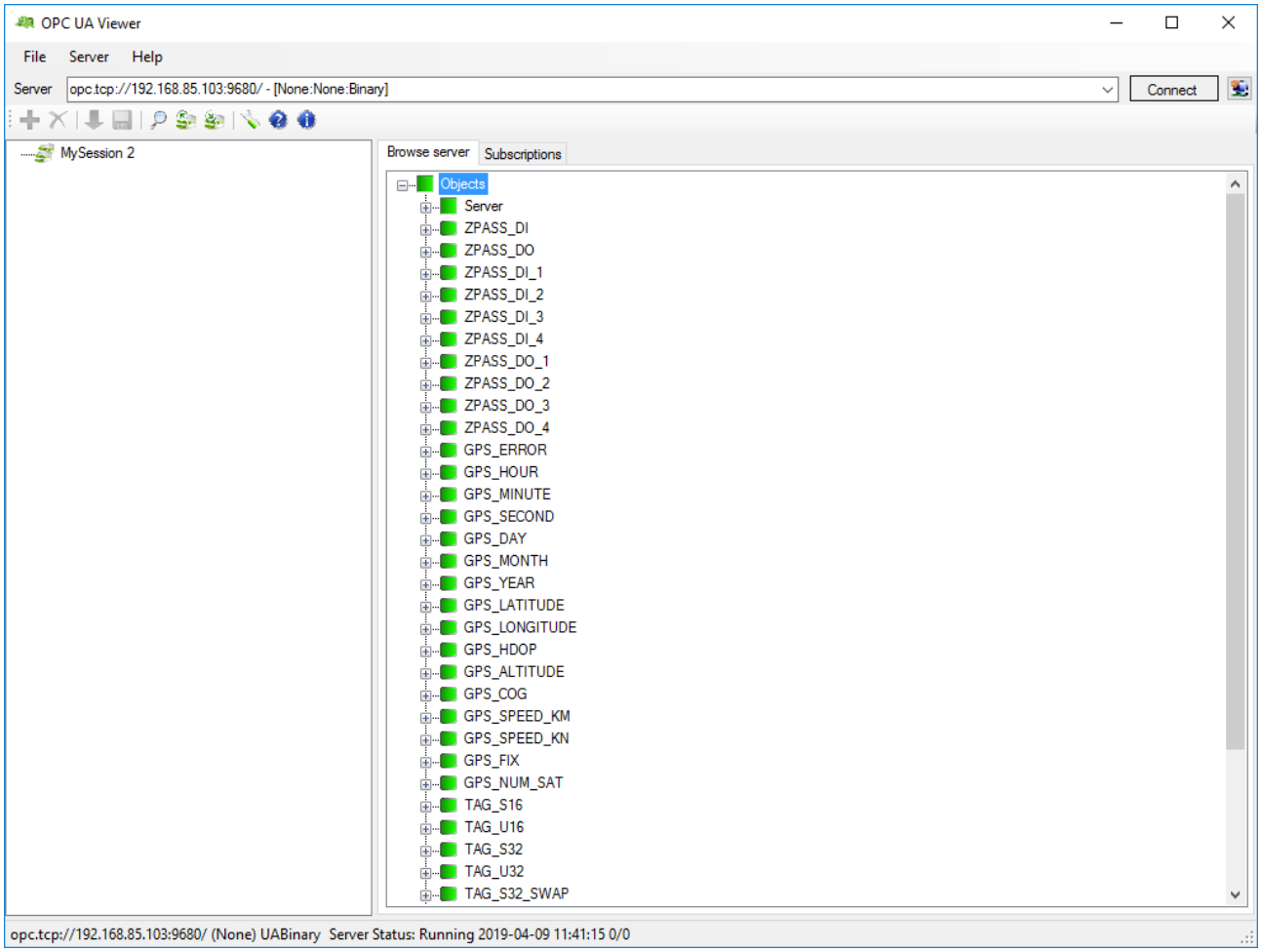
Note that, to access the Z-PASS OPC-UA server, a client shall use the following URL:

opc.tcp://IP_ADDR:PORT/

where:
IP_ADDR is the Z-PASS IP address
PORT is the TCP port configured for the OPC-UA server

Z-PASS OPC-UA server “exports” the Modbus Shared Memory Gateway tags; so, using an OPC-UA Client software, you can read/write the tags by means of the OPC-UA protocol.

The following figure shows the Z-PASS Modbus Shared Memory Gateway tags as seen by the Comm Server OPC UA Viewer SW.



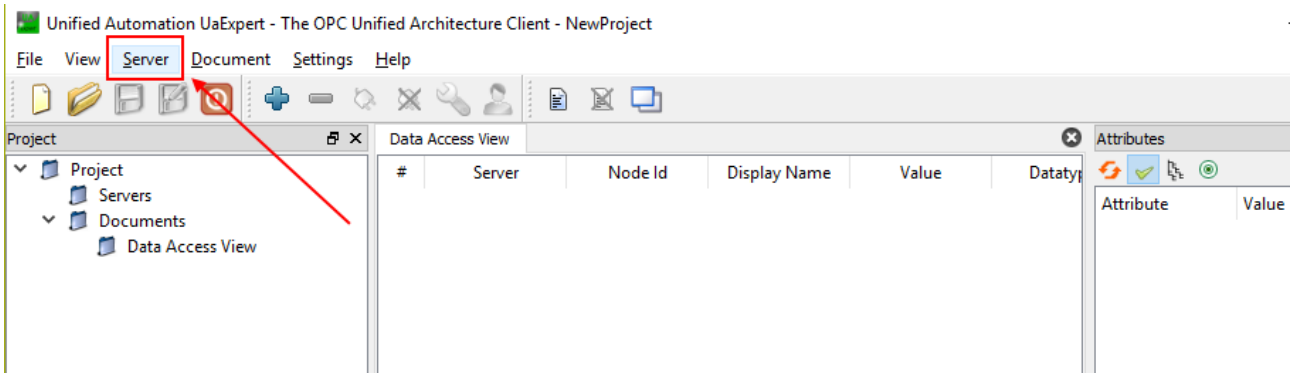
Since the Z-PASS OPC-UA server is used to “export” the Modbus Shared Memory Gateway tags, when Modbus Shared Memory Gateway is not active, also the OPC-UA server is disabled (the Enable flag is set to OFF and can’t be changed to ON).

***NOTE: For all Z-PASS OPC-UA Server variables the namespace-id is fixed to “1”.***

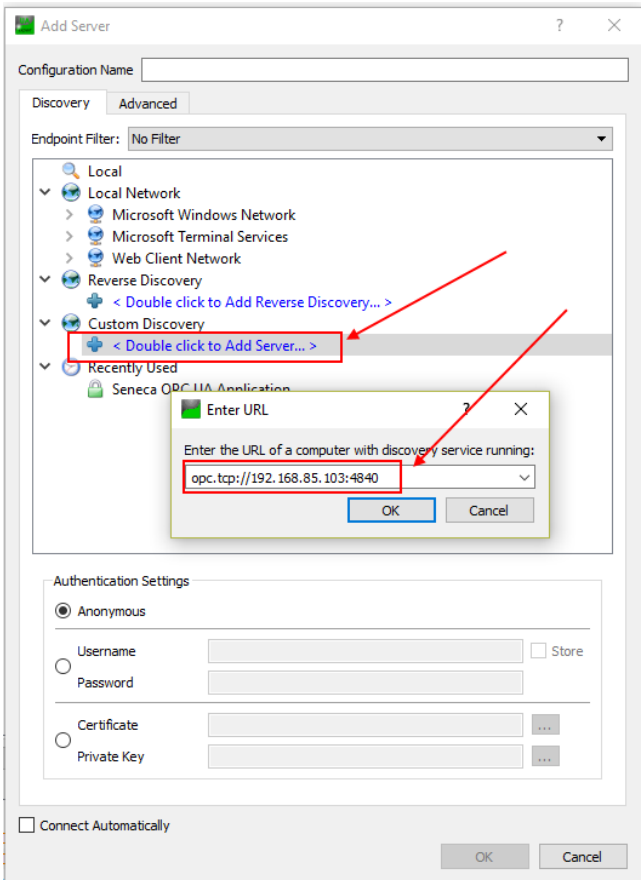
#### *20.1.11.1 UA Expert Client Configuration*

This chapter will help you to configure the connection and the correct Security Policy with the UA Expert Client

Click Select Server-> add

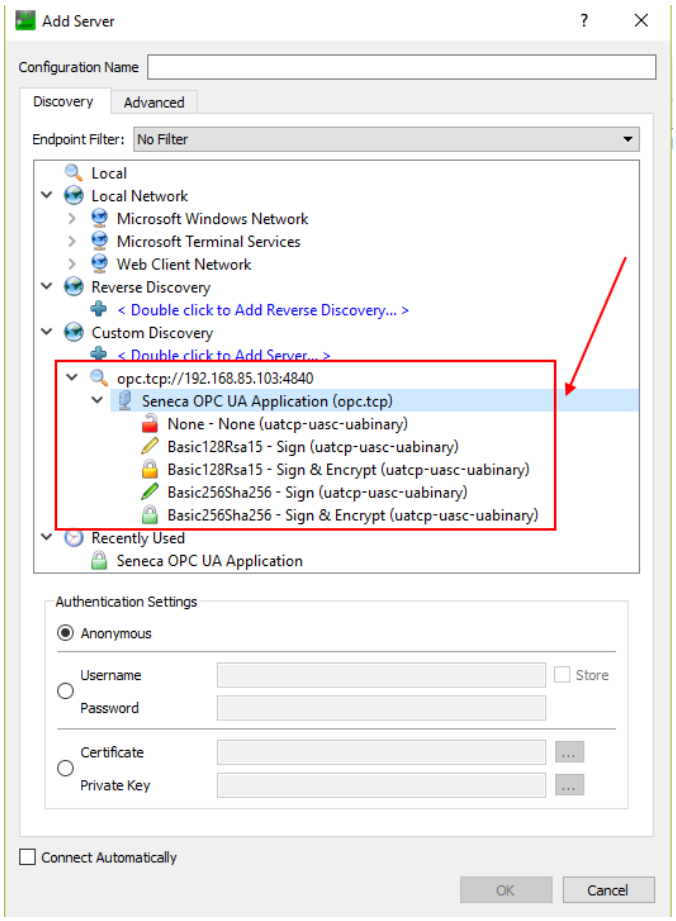



Go to Custom Discovery then enter the string to connect to the Z-PASS OPC-UA server:

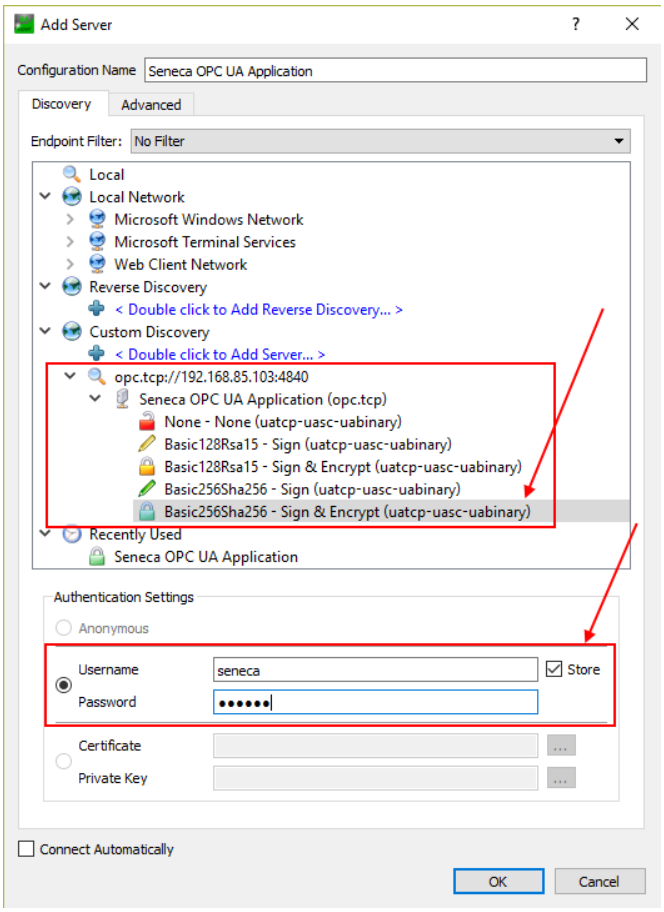



Then press OK.

Now the server capability are shown:

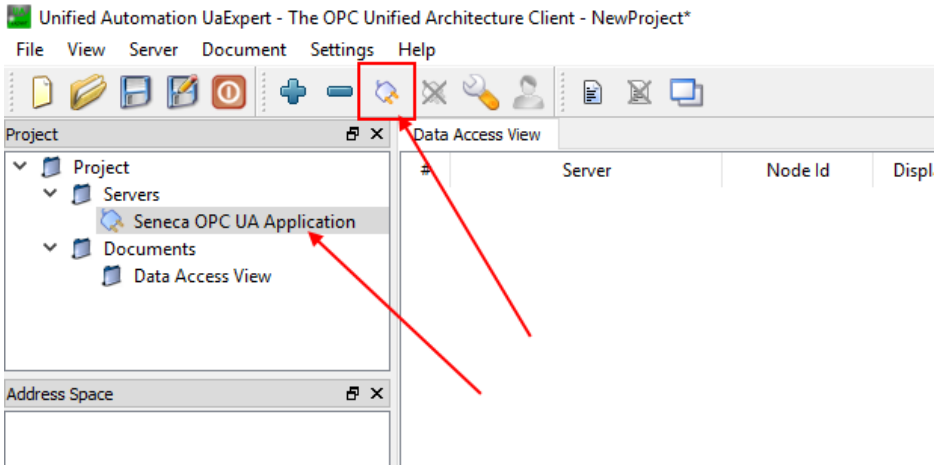



Set Security Policy that you want to use and then the Aythentication settings:



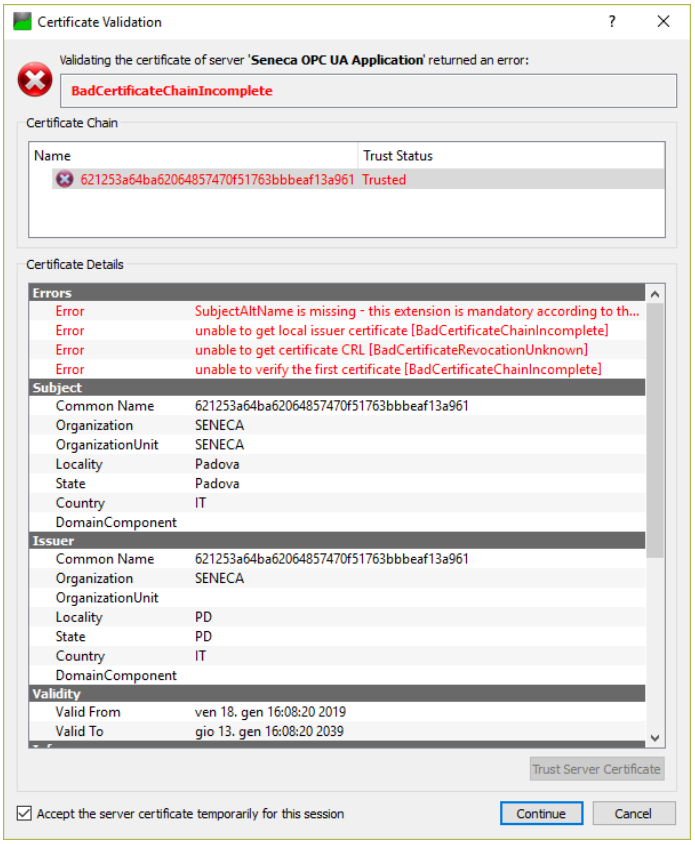

Then press OK:

Now we can connect to the server by using the plug icon:

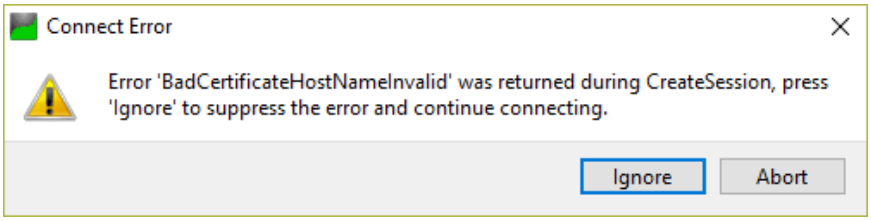



A new dialog window for validating the Server's certificate will open. After examining the certificate, choose Trust Server Certificate to permanently add the certificate to UaExpert's trust list. It is also possible

to check the box at Accept the server certificate temporarily for this session and choose Continue to not save the certificate in the trust list, or to choose Cancel to reject the certificate.

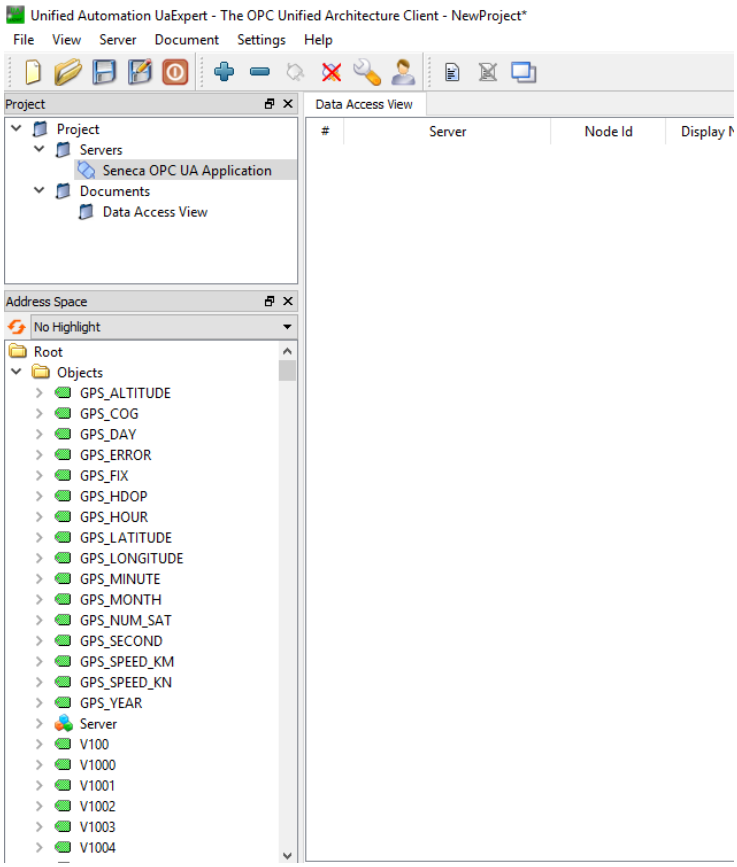



Now the Certificate Error Window will shown:

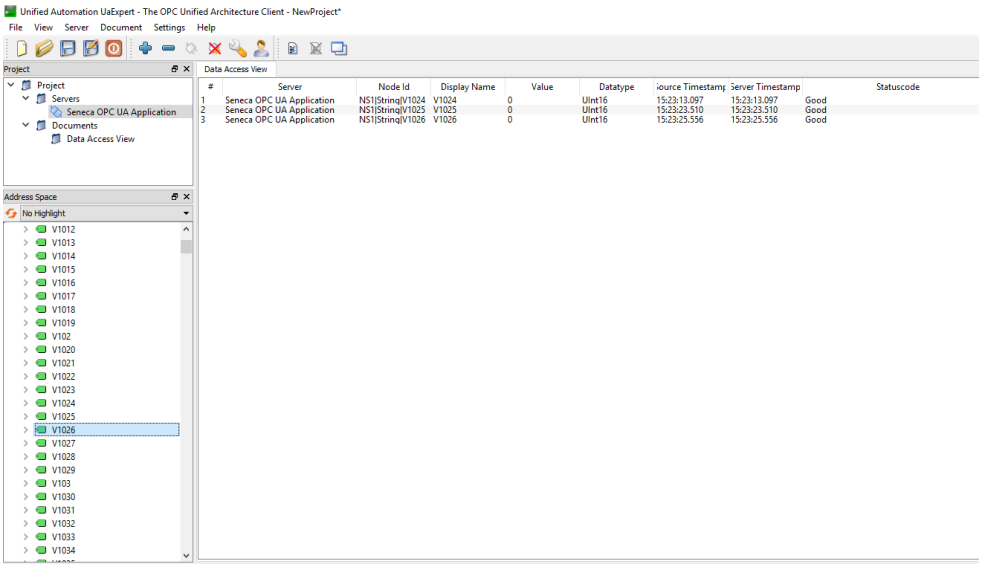



Click “Ignore” to continue.

Now the connection is done, you can read the tags from the left side:

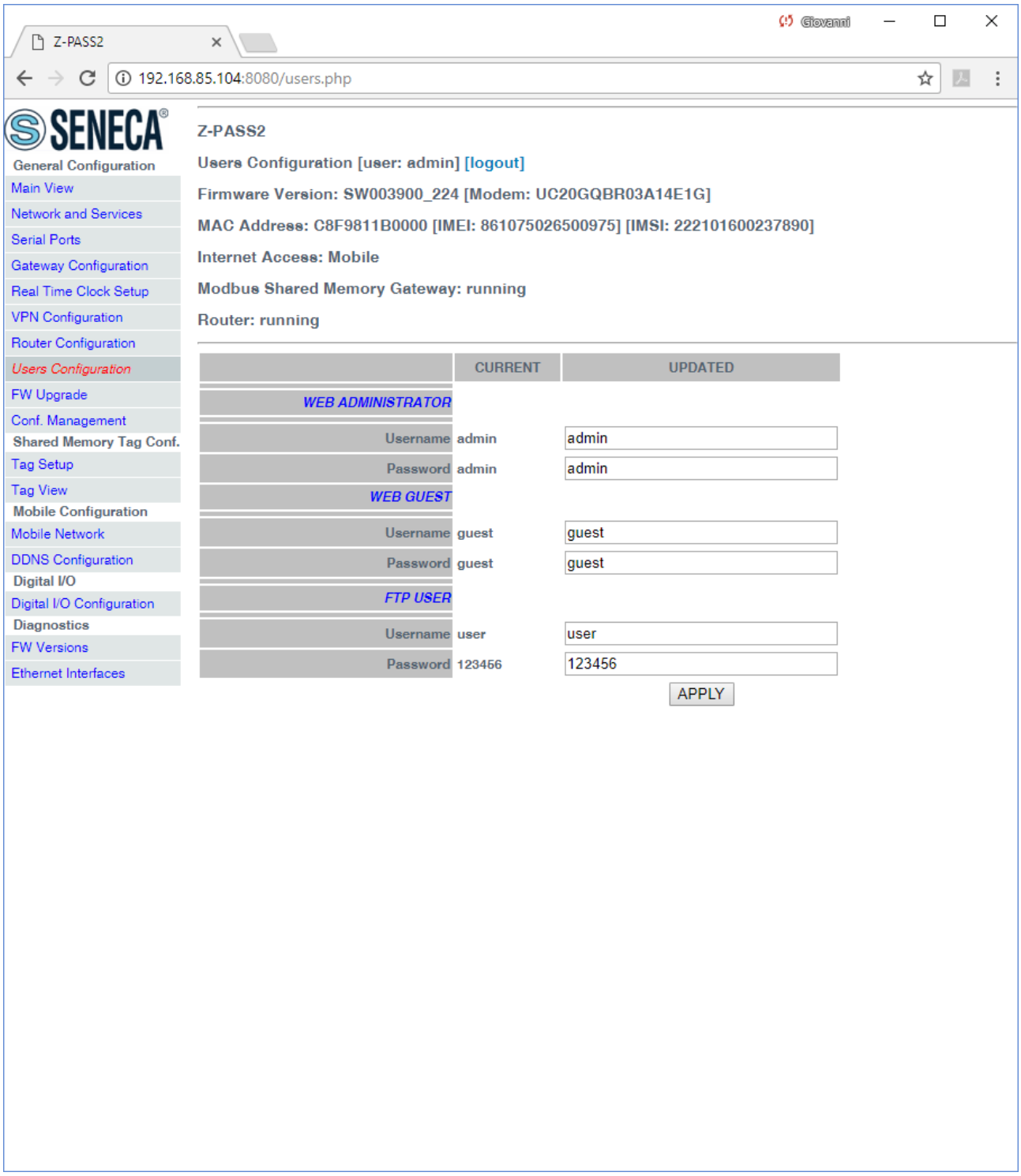



To update in real time the tags value drag and drop the Tags that you want to monitor:




### 20.1.12 Users Configuration

By clicking on the “Users Configuration” link, in the “Basic Configuration” section, you come to the following page:




In this page, you can change the “Web Administrator”, “Web Guest” and “FTP User” credentials, as explained in the following table:

| Field | Meaning | Default value |
|---|---|---|
| WEB ADMINISTRATOR/Username | Username to access the web configuration site (full access) | admin |

| | | |
|---|---|---|
| WEB ADMINISTRATOR/Password | Password to access the web configuration site (full access) | admin |
| WEB GUEST/Username | Username to access the web configuration site, in "view-only mode" (see paragraph 20.7.2) | guest |
| WEB GUEST/Password | Password to access the web configuration site, in "view-only mode" (see paragraph 20.7.2) | guest |
| FTP USER/Username | Username to access the Device FTP/SFTP site | user |
| FTP USER/Password | Password to access the Device FTP/SFTP site | 123456 |

For all the fields in this page, the following characters are allowed:

`a-zA-Z0-9-_|!@$%^&*?+{}<>;,:.`

each field can contain up to 100 characters.

The same rules apply to the other "Username" and "Password" fields of the web pages and to the "Tag Name" field of the "VPN Configuration" page.

Please note that, after changing the Web Administrator credentials, a new login will be required to access any page.

## *20.2 Mobile Configuration*

### *20.2.1 Mobile Network*

By clicking on the "Mobile Network" link, in the "Mobile Configuration" section, you come to the following page:


The above figure shows the “Mobile Network” page for Z-PASS2.


In this page, you can change the parameters related to the Mobile Network, as listed in the following table:

| Field | Meaning | Default value |
|---|---|---|
| SIM/PIN (if required by SIM) | PIN needed to unlock the SIM card, if PIN locking functionality is enabled on it[19] | 1234 |
| Operator Selection/Mode<br>(only on Z-PASS2) | This parameter tells if the modem shall select the Mobile Network Operator:<br>- automatically (Mode=Automatic)<br>- as selected by the user (Mode=Manual)<br>- reverting to "automatic" mode, if "manual" selection fails (Mode = Manual/ Automatic) | Automatic |
| Operator Selection/Operator<br>(only on Z-PASS2) | This parameter contains the list of the Mobile Network Operators currently available, that is detected by the modem.<br>The list items are strings with the following format:<br>- the MCC+MNC[20] code in square brackets (e.g.: "[22201]")<br>- the string identifying the operator (e.g.: "I TIM")<br>- the access technology, that is "GSM" or "UMTS", in brackets<br>This list is initially empty: it shall be filled by clicking on the "GET OPERATOR LIST" button. | "[22201] I TIM (UMTS)" |
| Data Connection/Enable | Flag to enable/disable the Mobile Network connectivity | OFF |
| Data Connection/APN Mode | This parameter tells if the APN and related parameters are automatically retrieved (based on SIM IMSI) (Mode=Automatic) or the values given in this page are used | Automatic |

[19] Please note that the procedure to enable/disable the PIN locking functionality on the SIM is not performed by the Device.
[20] MCC = Mobile Country Code, MNC = Mobile Network Code

| | | |
|---|---|---|
| | (Mode=Manual).<br>When APN Mode = Automatic, APN, Authentication Type, Username and Password parameters are disabled. | |
| Data Connection/APN | Access Point Name, as given by the Mobile Network Operator | ibox.tim.it |
| Data Connection/Authentication Type | Type of authentication required; possible values are: “None”, “CHAP/PAP”, “CHAP only”, “PAP only” | None |
| Data Connection/Username | Username needed for UMTS/GPRS connectivity, as given by the Mobile Network Operator; it may be empty, if “Authentication Type” parameter is “None” | user |
| Data Connection/Password | Password needed for UMTS/GPRS connectivity, as given by the Mobile Network Operator; it may be empty, if “Authentication Type” parameter is “None” | pass |
| Data Connection/Ping Connection Testing IP Address (if empty, testing is disabled) | FQDN or IP address used to periodically check, by means of “ping” packets, if the mobile connection is actually working; if the field is lefty empty, the check is not performed.<br>It is important to note that the FQDN or IP address specified must be reachable from the Z-PASS mobile network, otherwise the Z-PASS will detect that the mobile connection is not working and will drop it. | www.google.com |

In the “Mobile Network” page, when you click on the “SHOW MOBILE STATUS” button, a new section appears, named “Mobile Status”, showing:

- the SIM/PIN Status; if an error in PIN setting has occurred or PUK/PUK2 setting is needed, this status is shown in red color
- the number of remaining attempts for PIN setting; when this value is less than 3 (shown in red color), it means that PIN setting has failed, that is the configured PIN value is wrong
- the radio “Signal Level”, in the range [0..7]
- the selected operator (only for Z-PASS2)

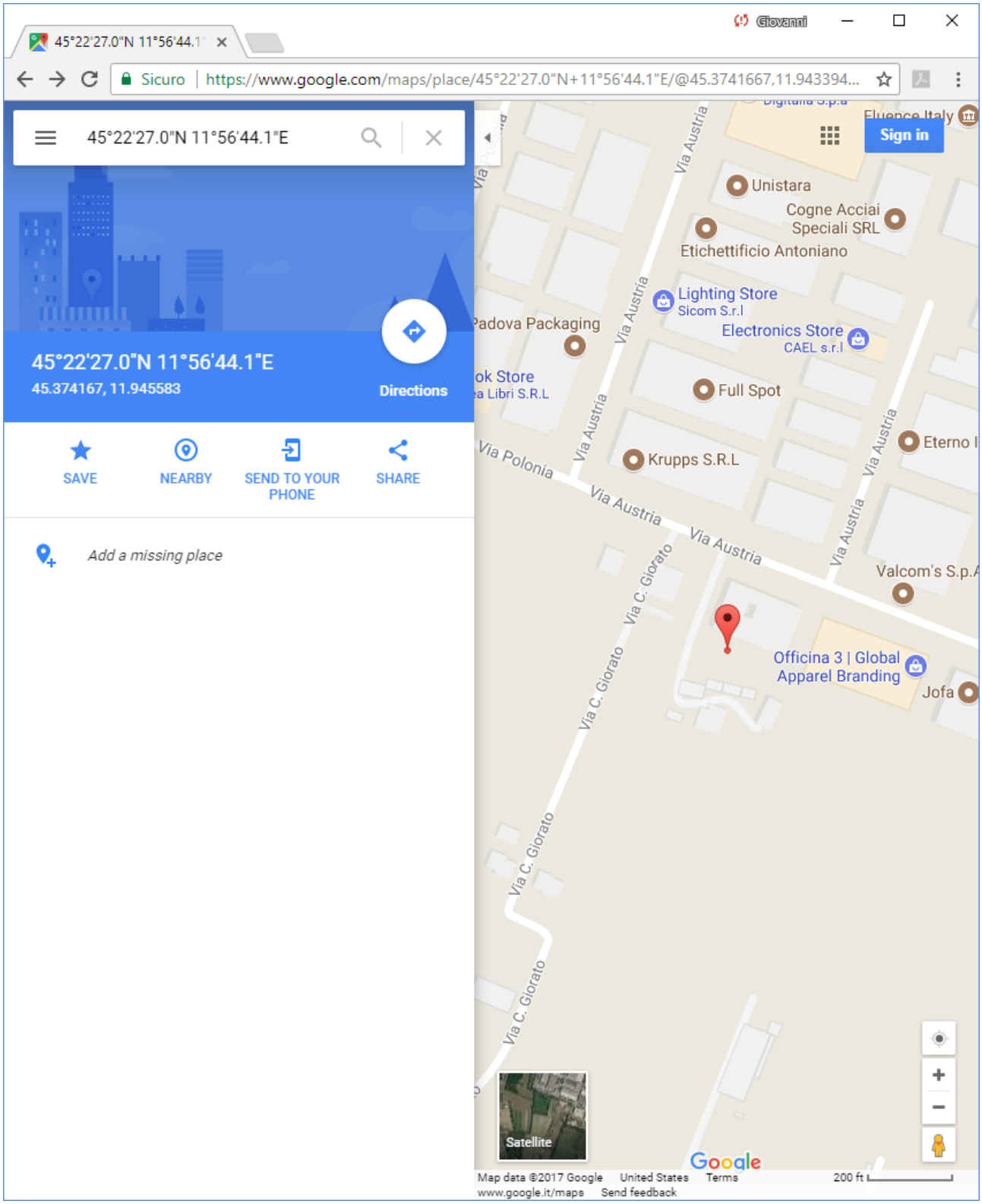
- the GSM “Registration Status”
- the Mobile Network “Connection Status” (i.e.: “Disconnected” or “Connected”)
- the IP address assigned to the Mobile Network interface when connected, the “dummy” IP address “0.0.0.0” when disconnected
- the number of packets/bytes received from the Mobile Network interface, when connected; “0/0” when disconnected
- the number of packets/bytes sent to the Mobile Network interface, when connected; “0/0” when disconnected

as shown in the following couple of figures:


Z-PASS2
Giovanni
192.168.85.104:8080/mobile_network.php?showinfo=1
SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces
Z-PASS2
Mobile Network [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Ethernet
Modbus Shared Memory Gateway: running
Router: running
CURRENT
UPDATED
SIM
PIN (if required by SIM) 8342 8342
Operator Selection
Mode Automatic Automatic
Operator [22201] I TIM (UMTS) Operator list not available
Data Connection
Enable OFF OFF
APN Mode Automatic Automatic
APN ibox.tim.it ibox.tim.it
Authentication Type None None
Username user user
Password pass pass
Ping Connection Testing IP Address (if empty, testing is disabled) www.google.com www.google.com
APPLY
HIDE MOBILE STATUS
GET OPERATOR LIST
Mobile Status
SIM/PIN Status PIN required
PIN Remaining Attempts 3
Signal Level [0..7] 5
Selected Operator "vodafone IT" (UMTS)
Registration Status Registered (home network)
Connection Status Disconnected
IP Address 0.0.0.0
RX Packets / Bytes 0 / 0
TX Packets / Bytes 0 / 0
GPS Location 45.37421,11.94562 [Map]
REFRESH


Giovanni
Z-PASS2
192.168.85.104:8080/mobile_network.php?showinfo=1
SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces
Z-PASS2
Mobile Network [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Mobile
Modbus Shared Memory Gateway: running
Router: running
CURRENT
UPDATED
SIM
PIN (if required by SIM) 8342 8342
Operator Selection
Mode Automatic Automatic
Operator [22201] I TIM (UMTS) Operator list not available
Data Connection
Enable ON ON
APN Mode Automatic Automatic
APN ibox.tim.it ibox.tim.it
Authentication Type None None
Username user user
Password pass pass
Ping Connection Testing IP Address (if empty, testing is disabled) www.google.com www.google.com
APPLY
HIDE MOBILE STATUS
GET OPERATOR LIST
Mobile Status
SIM/PIN Status PIN required
PIN Remaining Attempts 3
Signal Level [0..7] 5
Selected Operator "vodafone IT" (UMTS)
Registration Status Registered (home network)
Connection Status Connected
IP Address 10.211.101.167
RX Packets / Bytes 6 / 65
TX Packets / Bytes 6 / 98
GPS Location 45.37421,11.94562 [Map]
REFRESH

As shown in the above figures, only for Z-PASS2, the last row of the “Mobile Status” gives the “GPS Location” as `Latitude,Longitude` values; clicking on the Map link, the Google Maps™ on the current position are shown.



If the GPS signal is not available, the “GPS Location” row contains the string “Not fixed” and the Map link is not shown.

The following figure shows the situation when an error in PIN setting has occurred, due to a wrong value of the PIN parameter.


Giovanni
Z-PASS2
192.168.85.104:8080/mobile_network.php?showinfo=1
SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces
Z-PASS2
Mobile Network [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Ethernet
Modbus Shared Memory Gateway: running
Router: running
CURRENT
UPDATED
SIM
PIN (if required by SIM) 1234
1234
Operator Selection
Mode Automatic
Automatic
Operator [22201] I TIM (UMTS)
Operator list not available
Data Connection
Enable OFF
OFF
APN Mode Automatic
Automatic
APN ibox.tim.it
ibox.tim.it
Authentication Type None
None
Username user
user
Password pass
pass
Ping Connection Testing IP Address (if empty, testing is disabled) www.google.com
www.google.com
APPLY
HIDE MOBILE STATUS
GET OPERATOR LIST
Mobile Status
SIM/PIN Status PIN error
PIN Remaining Attempts 2
Signal Level [0..7] 4
Selected Operator No operator
Registration Status Searching for network
Connection Status Disconnected
IP Address 0.0.0.0
RX Packets / Bytes 0 / 0
TX Packets / Bytes 0 / 0
GPS Location Not fixed
REFRESH

It should be noted that, when the PIN is set during procedures automatically performed by the Z-PASS firmware, if the number of remaining attempts is 1, no more attempt is done to avoid blocking the SIM.

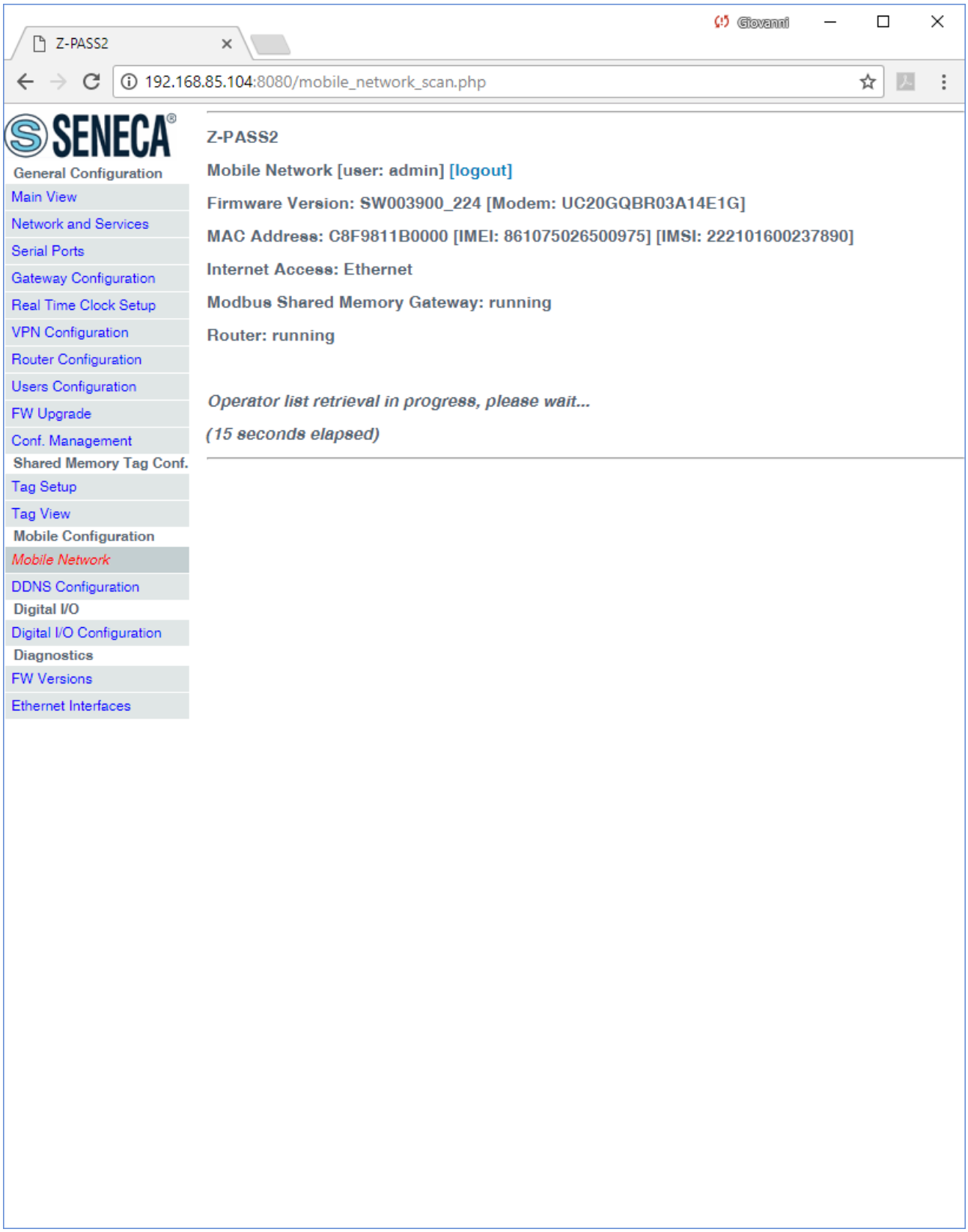
You can refresh the Mobile Network status, by clicking on the “REFRESH” button.

You can hide the “Mobile Status” section, by clicking on the “HIDE MOBILE STATUS” button.

As already told above, the “GET OPERATOR LIST” button lets you retrieve the list of the operators currently available, that is detected by the modem (only on Z-PASS2).

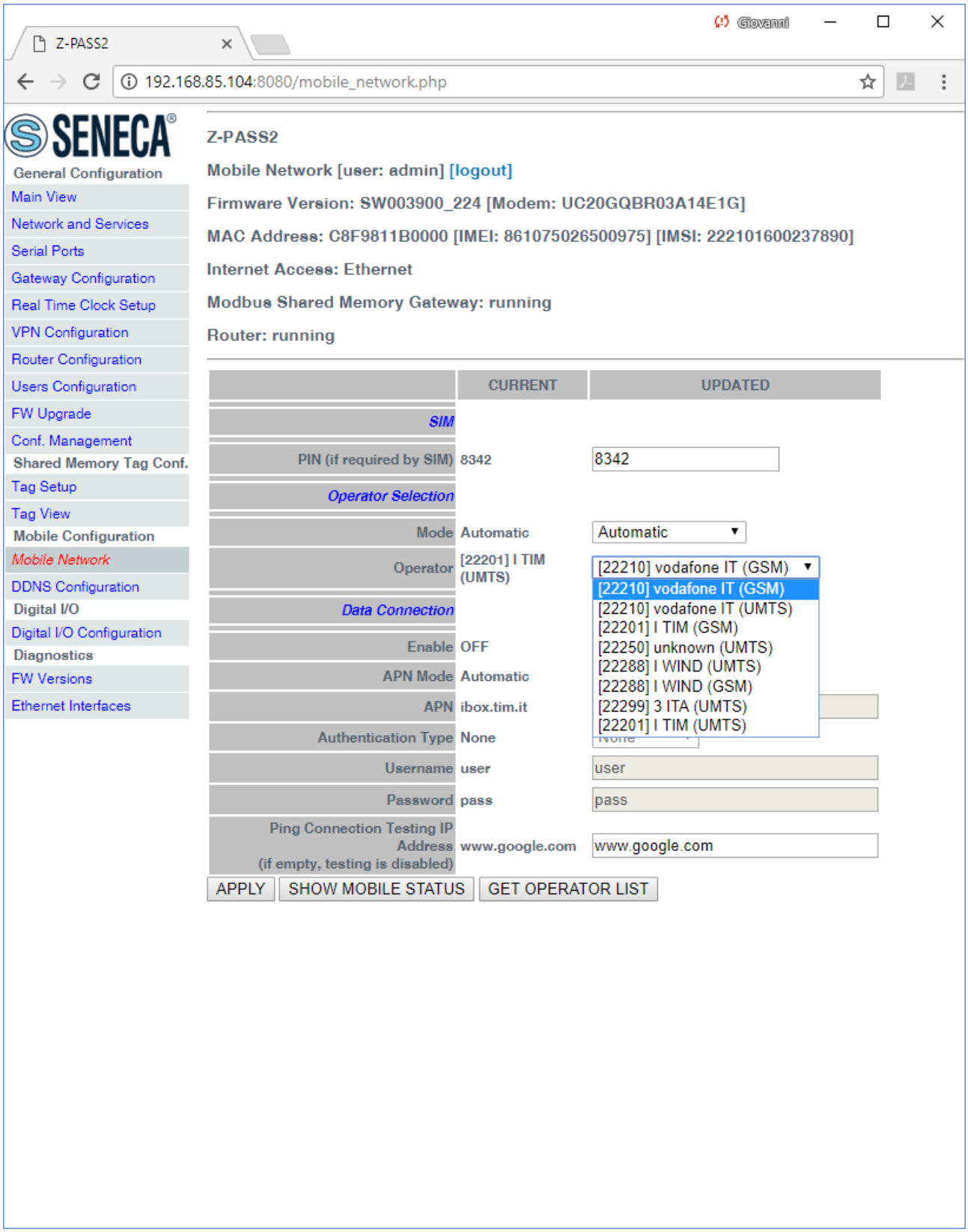
When you click on the button, the following page is shown.


Tipically, it takes about 1 minute to get the list, so the page shows the number of seconds elapsed.




When the procedure is completed, the following page is shown.


After some seconds, the page automatically evolves to the “Mobile Network” page, with the operator list filled, as shown in the following figure.




You can choose an operator from the list, to perform “Manual” or “Manual/Automatic” selection.

### *20.2.2 DDNS Configuration*

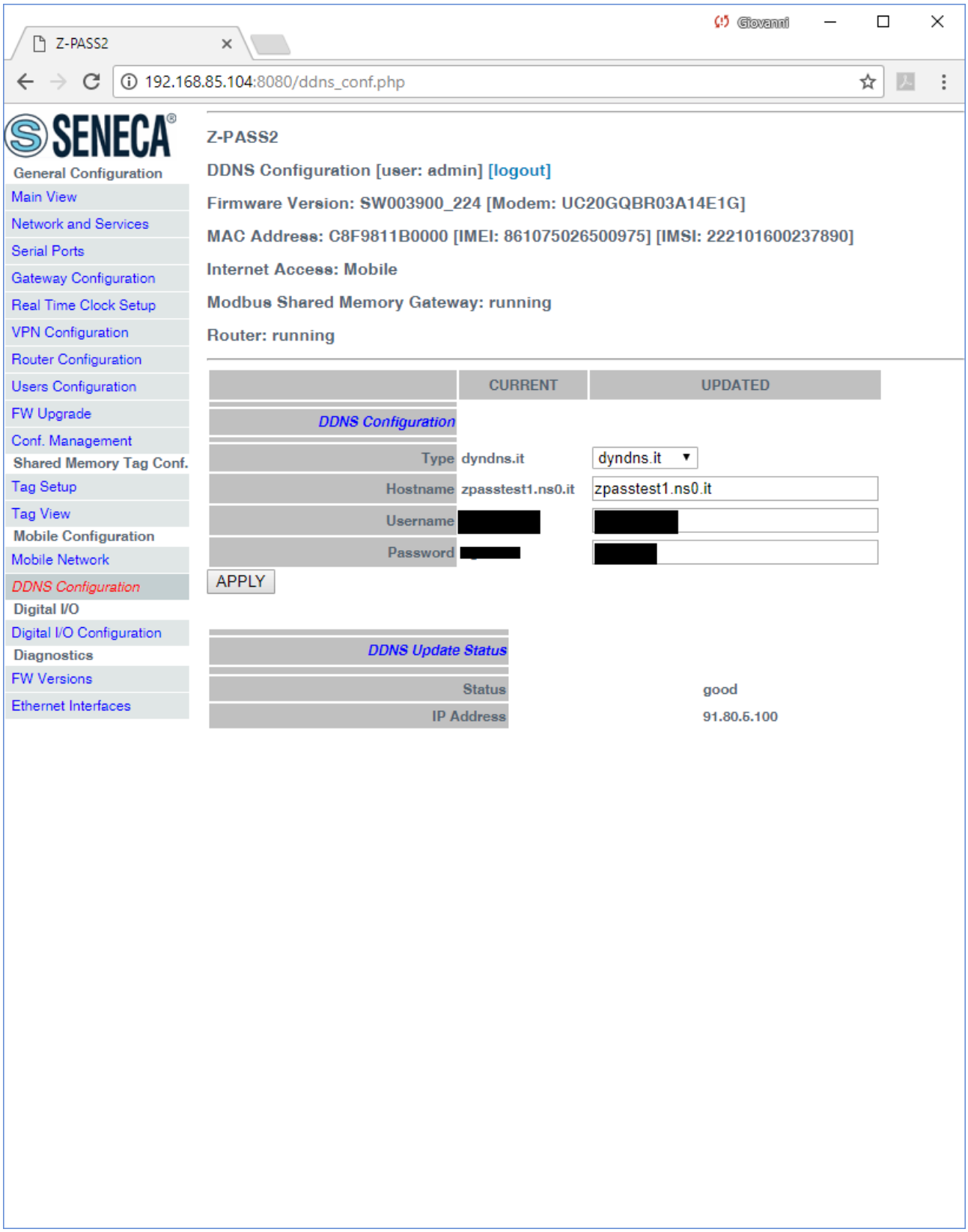
By clicking on the “DDNS Configuration” link, in the “Mobile Configuration” section, you come to the following page:


In this page, you can set the parameters related to the Dynamic DNS service, as listed in the following table:

| Field | Meaning | Default value |
|---|---|---|
| Type | Type of Dynamic DNS service;<br>possible values are:<br>- None<br>- dyndns.it<br>- dyndns.org<br>- no-ip.com | None |
| Hostname | The hostname provided with the service subscription | empty |
| Username | The username provided with the service subscription | empty |
| Password | The password provided with the service subscription | empty |

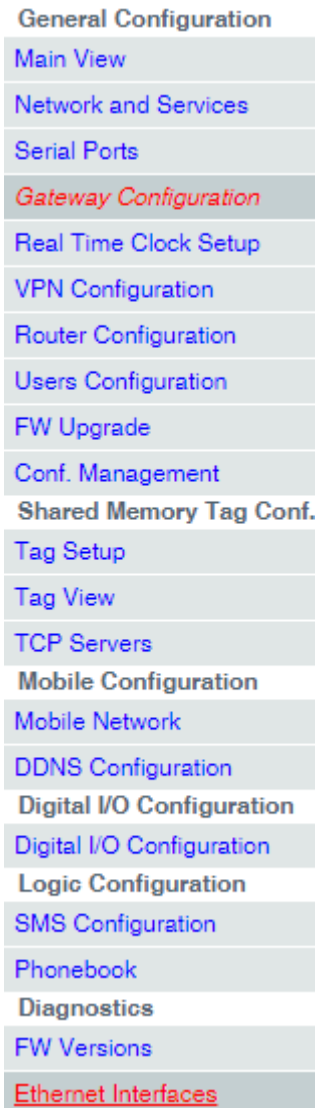
The parameters shall be set according to the DDNS service subscription; an example is given in the following figure.


When an IP address assigned to the Mobile Network Interface has been bound with the hostname, the “DDNS Update Status” section appears like in the following figure.


Giovanni
Z-PASS2
192.168.85.104:8080/ddns_conf.php
SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces
Z-PASS2
DDNS Configuration [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Mobile
Modbus Shared Memory Gateway: running
Router: running
CURRENT
UPDATED
DDNS Configuration
Type
dyndns.it
dyndns.it
Hostname
zpasstest1.ns0.it
zpasstest1.ns0.it
Username
Password
APPLY
DDNS Update Status
Status
good
IP Address
91.80.5.100

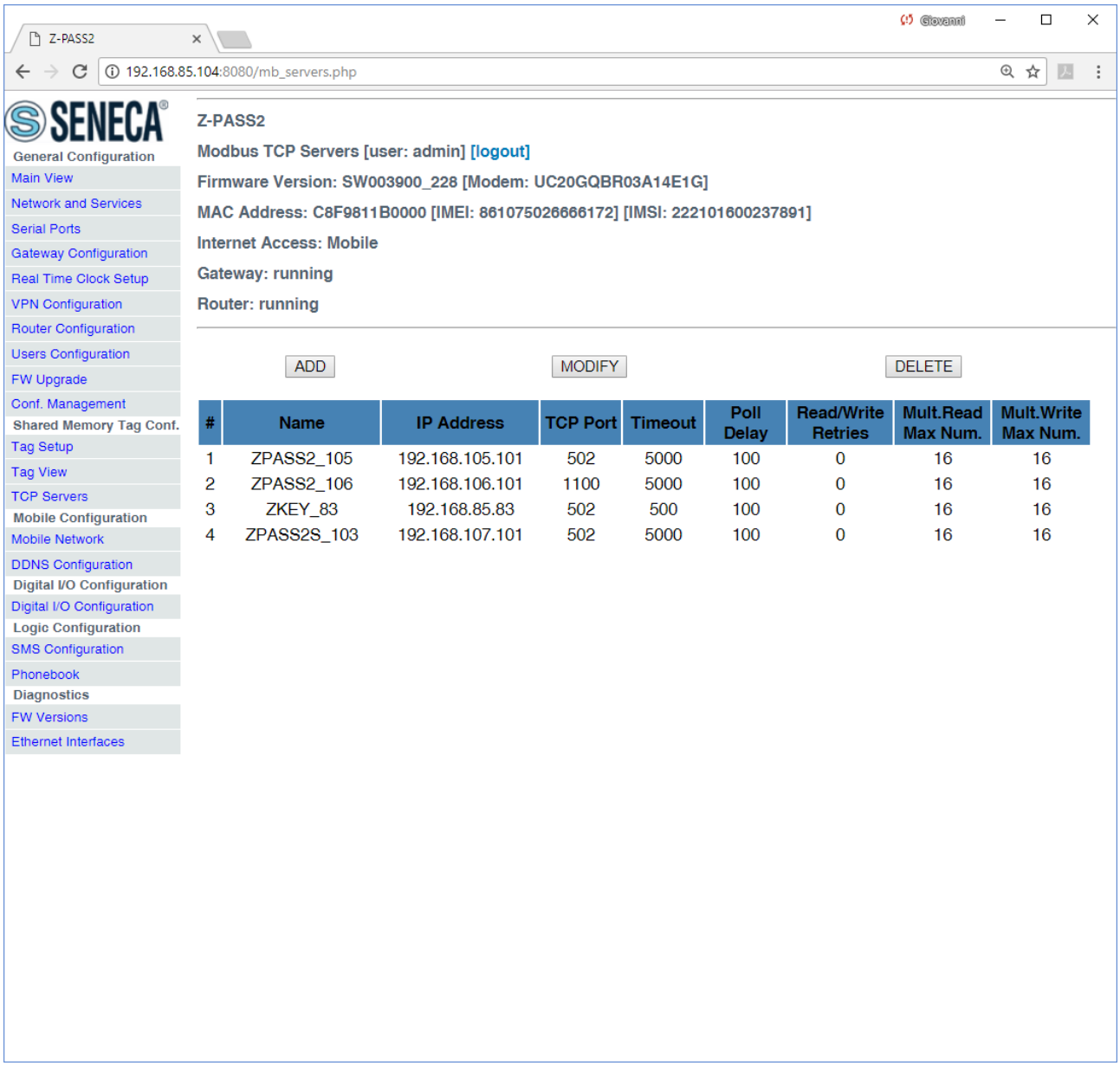
## 20.3 Shared Memory Tag Configuration

When the “Modbus Shared Memory/Enable” parameter, in the “Gateway Configuration” page, is set to “ON”, in the left side menu, a new section named “Shared Memory Tag Configuration” is available, containing three links, as shown in the following figure.



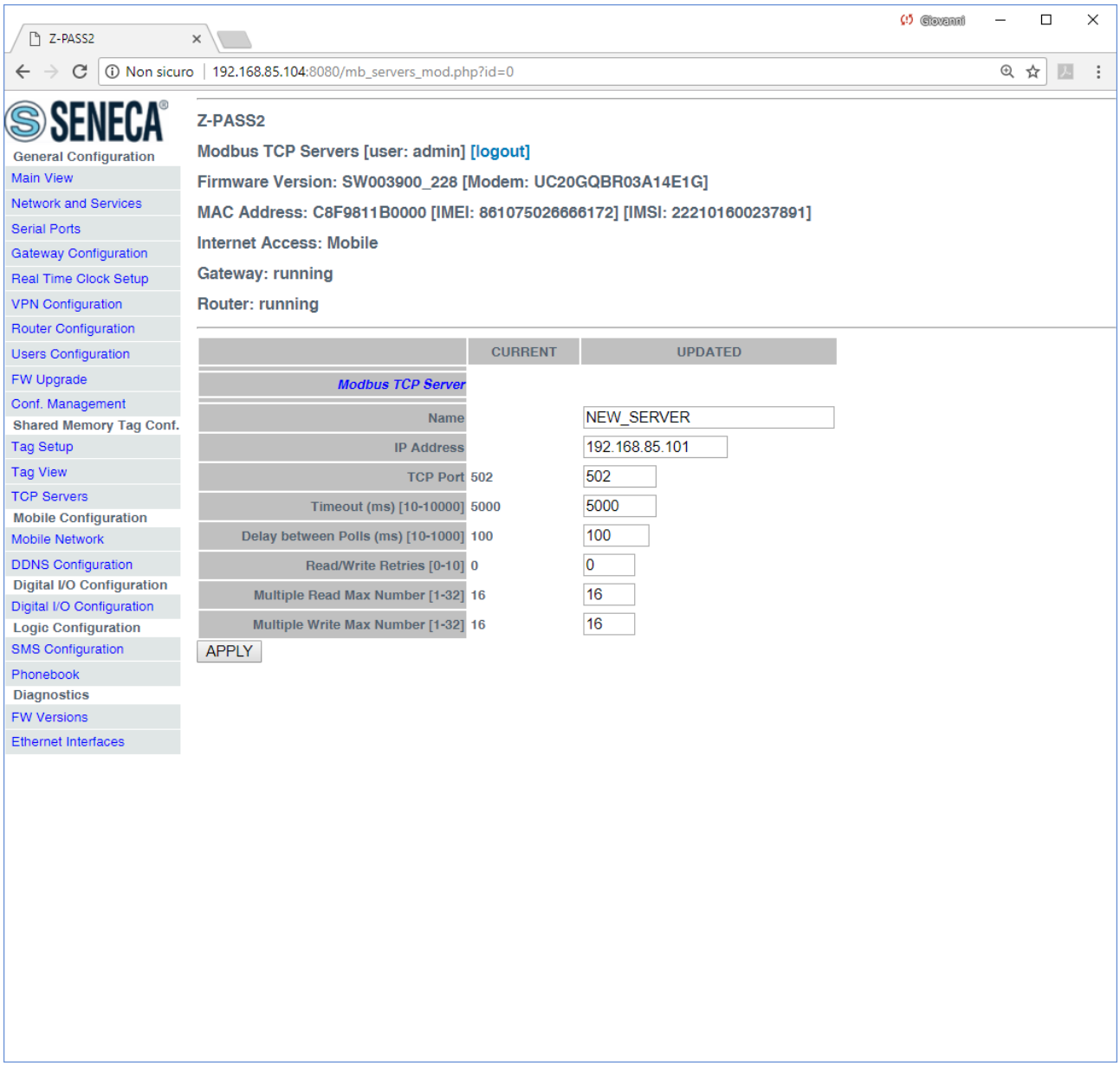

### 20.3.1 TCP Servers

By clicking on the “TCP Servers” link, in the “Shared Memory Tag Conf.” section, you come to the following page:




In this page, the list of the TCP Servers, used for Modbus Shared Memory Gateway functionality, is shown.

By clicking on the “ADD” button, a new TCP Server can be configured, as in the following figure.

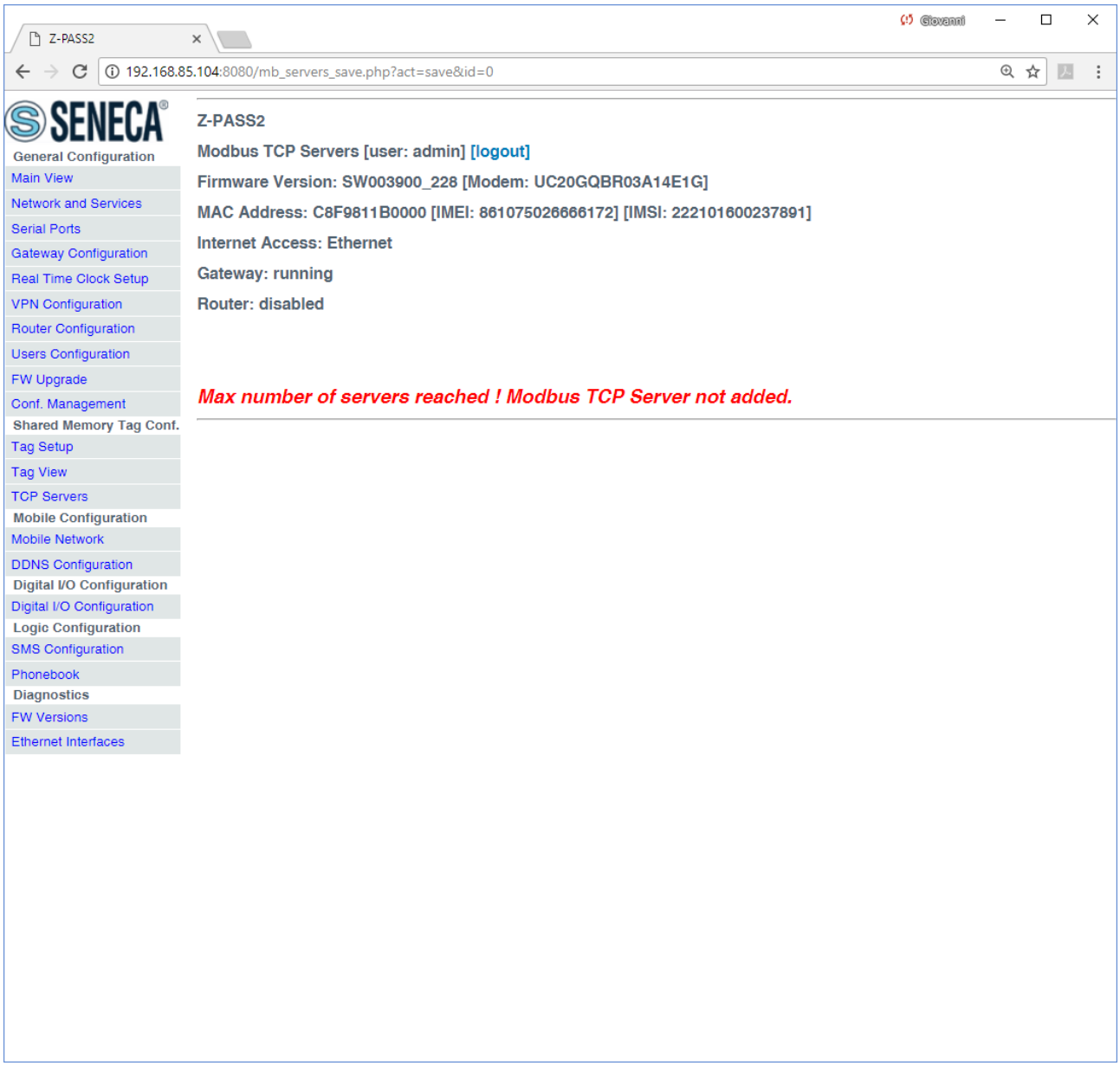



The following table explains the meaning of the parameters related to a TCP Server.

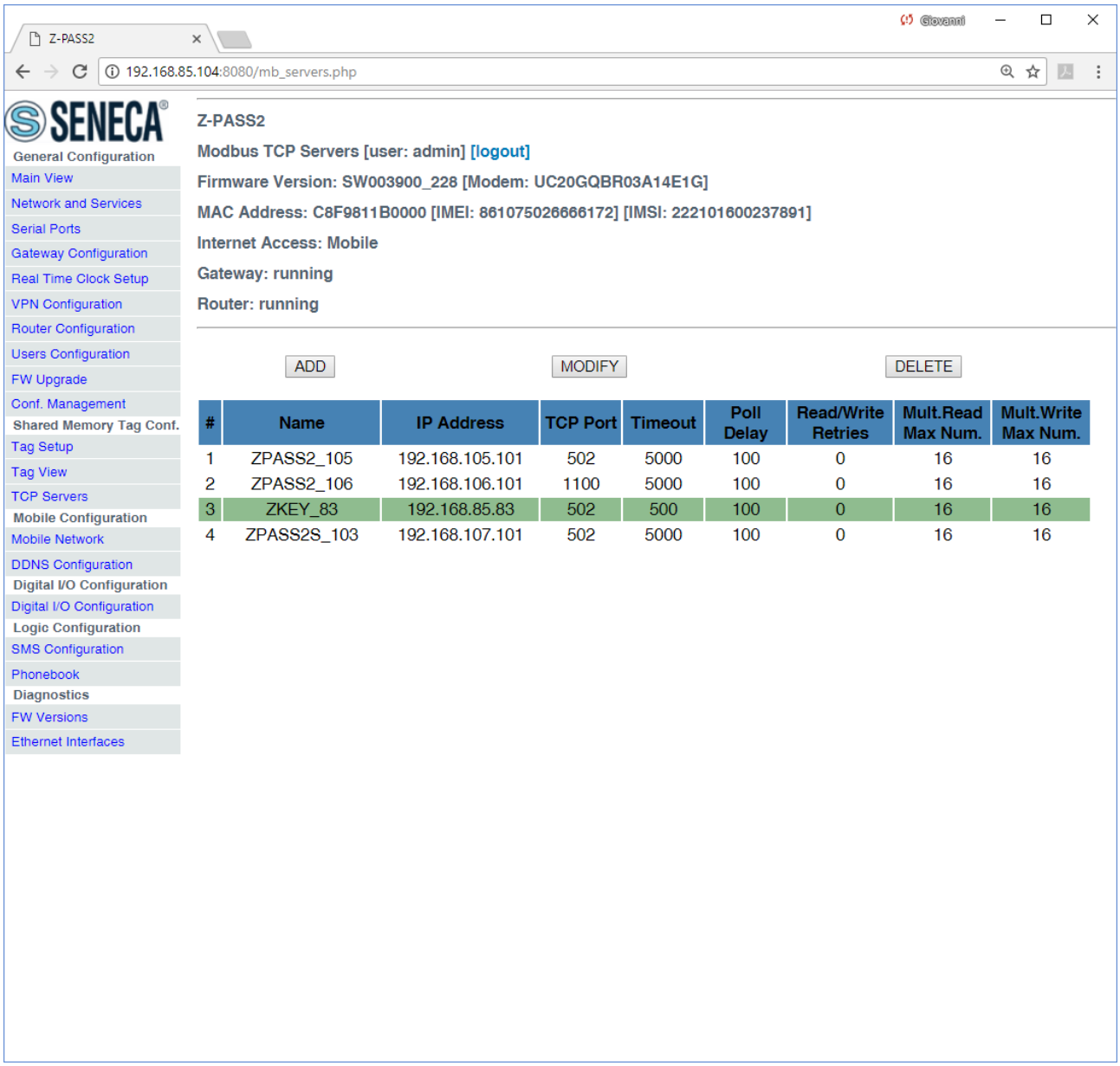
| Field | Meaning | Default value |
|---|---|---|
| Name | Mnemonic name of the TCP Server This name is used to identify the TCP Server in the “Tag Setup” and “Tag View” pages. | empty |
| IP Address | IP Address of the TCP Server | empty |
| TCP Port | Modbus TCP Server port | 502 |
| Timeout (ms) [10-10000] | Connection/Response timeout for Modbus TCP requests, in milliseconds | 5000 |
| Delay between Polls (ms) [10-1000] | Interval between Modbus TCP requests, | 100 |

| | | |
|---|---|---|
| | in milliseconds | |
| Read/Write Retries [0-10] | Maximum number of retries for Modbus TCP requests; this always applies to write requests; for read requests, it applies only to tags with “Gateway Tag Mode”=”BRIDGE” (see 20.3.2.1 paragraph) | 0 |
| Multiple Read Max Number [1-32] | Maximum number of Modbus registers that can be read in a single Modbus TCP request; this is used to reduce the number of read requests sent over the TCP connection, thus performing optimization | 16 |
| Multiple Write Max Number [1-32] | Maximum number of Modbus registers that can be written in a single Modbus TCP request; this is used to reduce the number of write requests sent over the TCP connection, thus performing optimization | 16 |

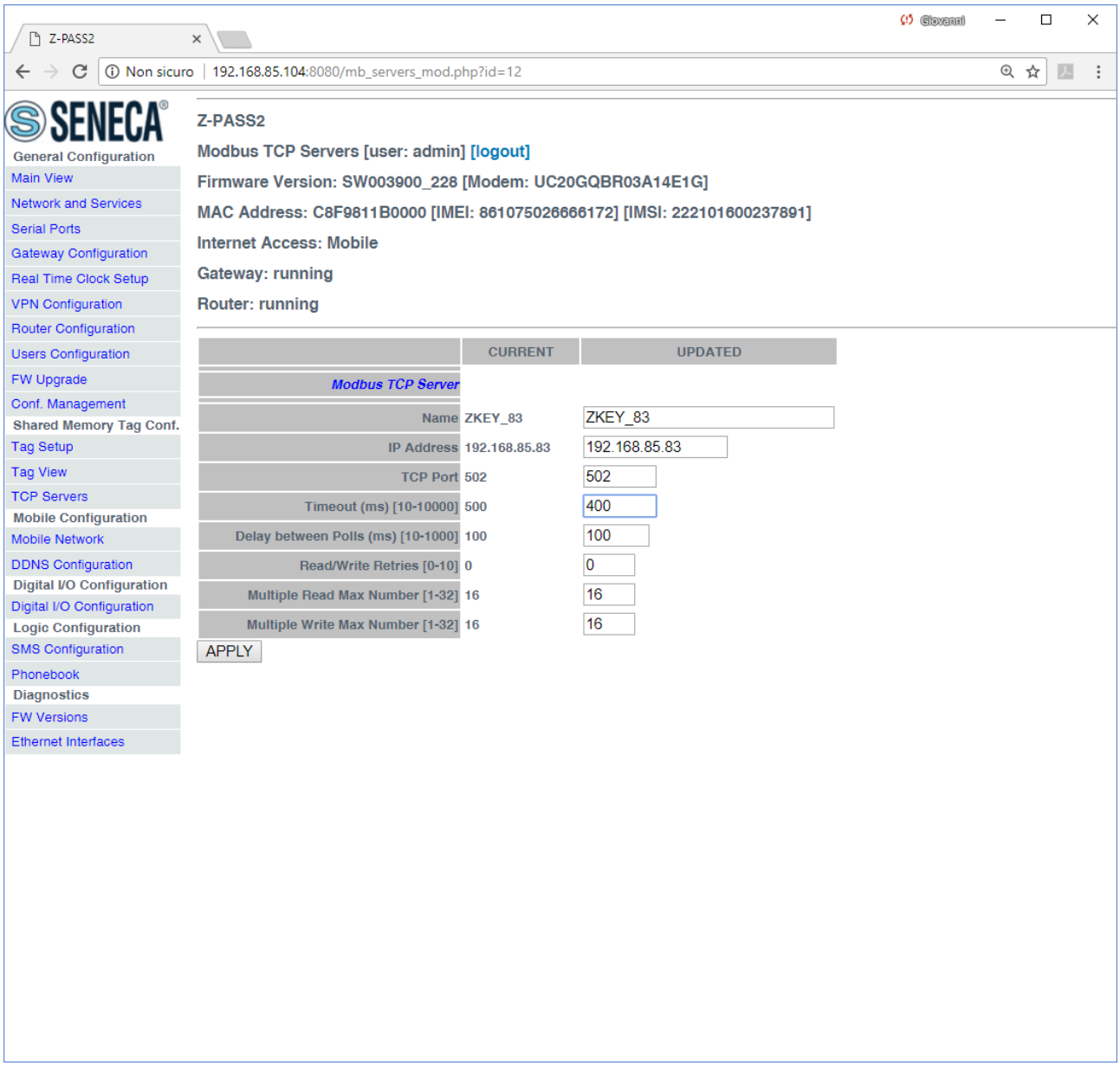
A maximum of 25 TCP Servers can be configured; so, when trying to add the eleventh server, the following error message is shown.




Selecting a TCP Server in the list and clicking on the “MODIFY” button, you can modify the TCP Server parameters, as in the following figures.



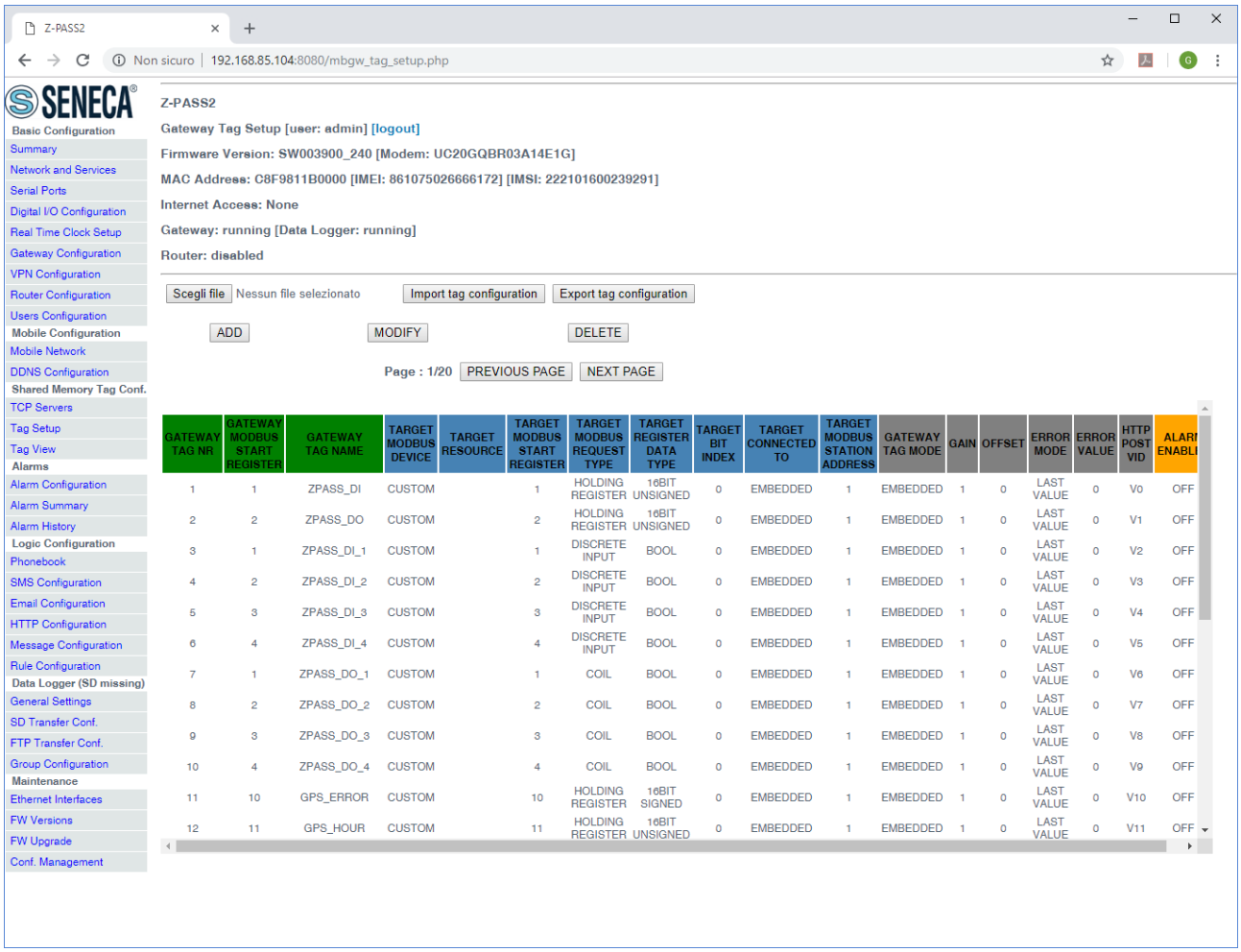

| # | Name | IP Address | TCP Port | Timeout | Poll Delay | Read/Write Retries | Mult.Read Max Num. | Mult.Write Max Num. |
|---|---|---|---|---|---|---|---|---|
| 1 | ZPASS2_105 | 192.168.105.101 | 502 | 5000 | 100 | 0 | 16 | 16 |
| 2 | ZPASS2_106 | 192.168.106.101 | 1100 | 5000 | 100 | 0 | 16 | 16 |
| 3 | ZKEY_83 | 192.168.85.83 | 502 | 500 | 100 | 0 | 16 | 16 |
| 4 | ZPASS2S_103 | 192.168.107.101 | 502 | 5000 | 100 | 0 | 16 | 16 |




Finally, selecting a TCP Server in the list and clicking on the “DELETE” button, you can remove it from the configuration.

### *20.3.2 Tag Setup*

This page is used to configure the Modbus Shared Memory Gateway tags.




| GATEWAY TAG NR | GATEWAY MODBUS START REGISTER | GATEWAY TAG NAME | TARGET MODBUS DEVICE | TARGET RESOURCE | TARGET MODBUS START REGISTER | TARGET MODBUS REQUEST TYPE | TARGET REGISTER DATA TYPE | TARGET BIT INDEX | TARGET CONNECTED TO | TARGET MODBUS STATION ADDRESS | GATEWAY TAG MODE | GAIN | OFFSET | ERROR MODE | ERROR VALUE | HTTP POST VID | ALARM ENABLE |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | ZPASS_DI | CUSTOM | | 1 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | V0 | OFF |
| 2 | 2 | ZPASS_DO | CUSTOM | | 2 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | V1 | OFF |
| 3 | 1 | ZPASS_DI_1 | CUSTOM | | 1 | DISCRETE INPUT | BOOL | 0 | EMBEDDED | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | V2 | OFF |
| 4 | 2 | ZPASS_DI_2 | CUSTOM | | 2 | DISCRETE INPUT | BOOL | 0 | EMBEDDED | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | V3 | OFF |
| 5 | 3 | ZPASS_DI_3 | CUSTOM | | 3 | DISCRETE INPUT | BOOL | 0 | EMBEDDED | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | V4 | OFF |
| 6 | 4 | ZPASS_DI_4 | CUSTOM | | 4 | DISCRETE INPUT | BOOL | 0 | EMBEDDED | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | V5 | OFF |
| 7 | 1 | ZPASS_DO_1 | CUSTOM | | 1 | COIL | BOOL | 0 | EMBEDDED | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | V6 | OFF |
| 8 | 2 | ZPASS_DO_2 | CUSTOM | | 2 | COIL | BOOL | 0 | EMBEDDED | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | V7 | OFF |
| 9 | 3 | ZPASS_DO_3 | CUSTOM | | 3 | COIL | BOOL | 0 | EMBEDDED | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | V8 | OFF |
| 10 | 4 | ZPASS_DO_4 | CUSTOM | | 4 | COIL | BOOL | 0 | EMBEDDED | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | V9 | OFF |
| 11 | 10 | GPS_ERROR | CUSTOM | | 10 | HOLDING REGISTER | 16BIT SIGNED | 0 | EMBEDDED | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | V10 | OFF |
| 12 | 11 | GPS_HOUR | CUSTOM | | 11 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | V11 | OFF |

In this page, the following buttons (i.e. functionalities) are available.

Import tag configuration

This button allows the user to upload a binary file containing the tag configuration to the Z-PASS; this file shall have been exported from the “Microsoft Excel™ Template” (see 20.3.2.4 paragraph).
When a configuration is loaded which does not contain valid VIDs, the message *“NOTE: HTTP POST have been automatically set.”* is shown (as in the above figure).

Export tag configuration

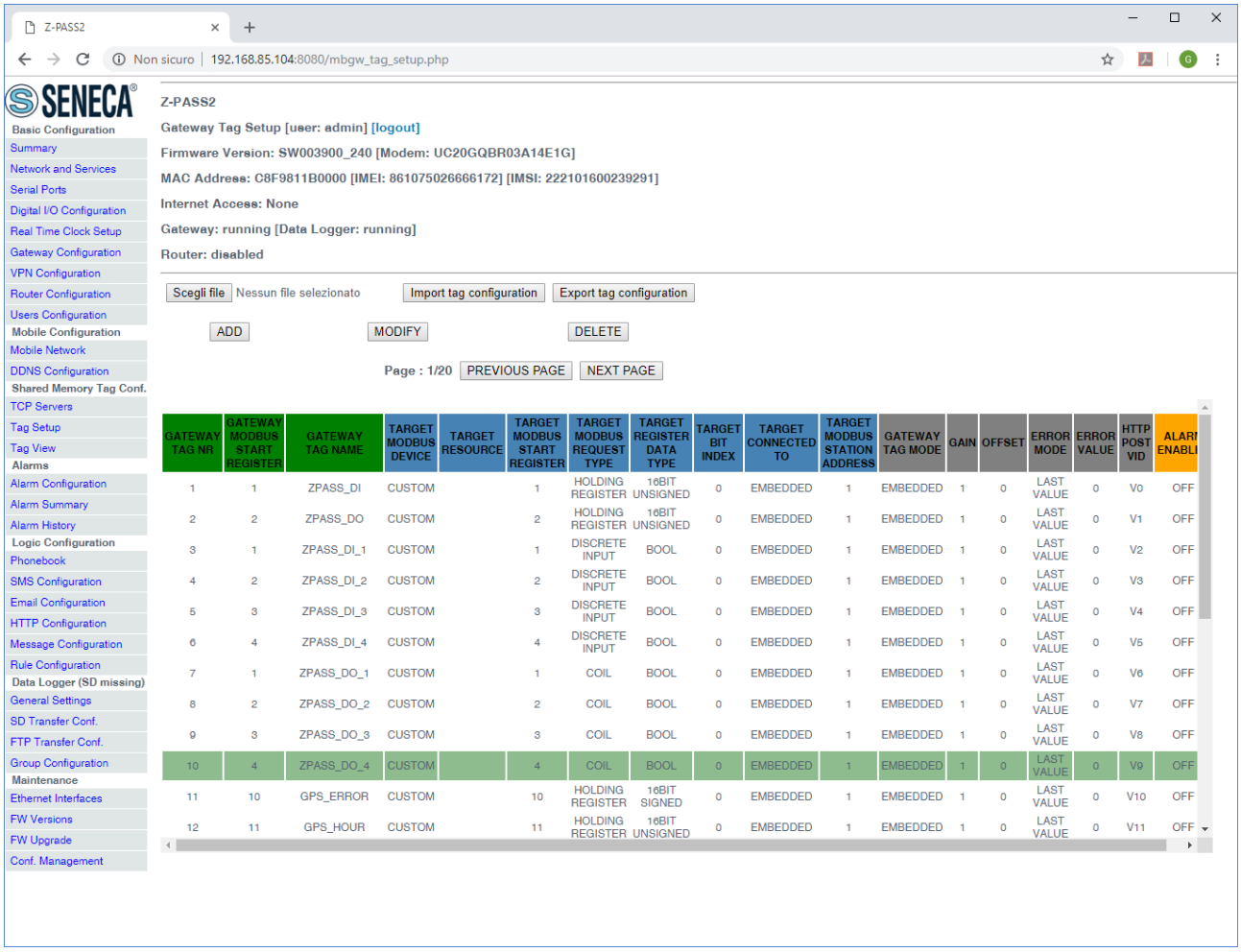
This button allows the user to download a binary file containing the tag configuration from the Z-PASS; this file can be imported into the “Microsoft Excel™ Template” (see 20.3.2.4 paragraph).

ADD

This button allows the user to add a new tag (see paragraph below); up to 2000 tags can be configured.

MODIFY

This button allows the user to modify an existing tag (see paragraph below); the tag shall have been previously selected, by clicking on the corresponding table row, as shown in the following figure.

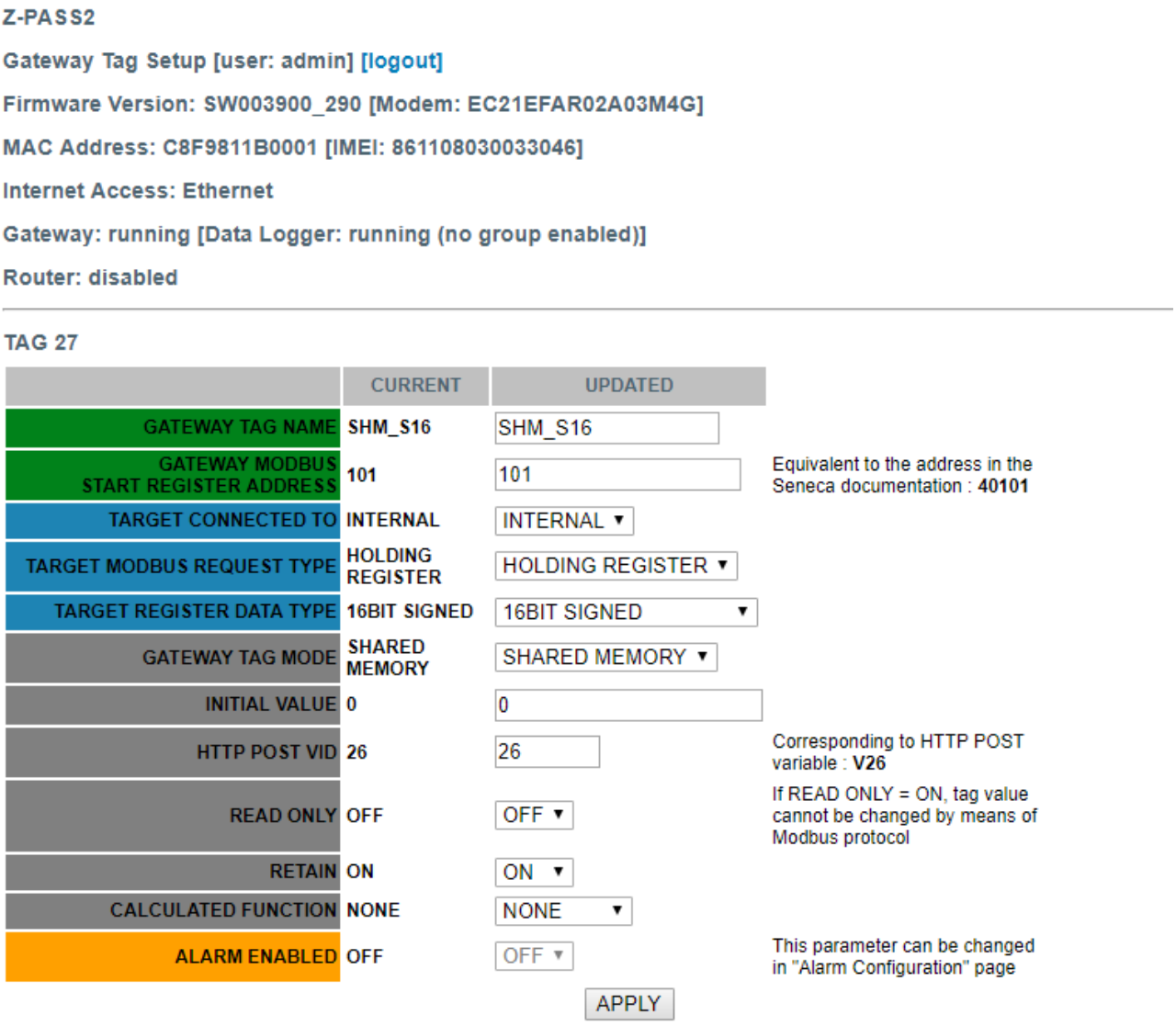




This button allows the user to delete a tag; the tag shall have been previously selected, by clicking on the corresponding table row.

### *20.3.2.1 Tag Creation/Modification*

By clicking on the “ADD” or “MODIFY” button, you come to the following page.




The following table describes the available parameters.

| Field | Meaning | Default value |
|---|---|---|
| Gateway Tag Name | Mnemonic name to identify the tag | TAG |
| Gateway Modbus Start Register Address | Start Register Address of the tag | 1 |
| Target Modbus Device | Type of Modbus device: “CUSTOM” or one of the following Seneca devices:<br>"Z-D-IN"<br>"Z-10-D-IN"<br>"Z-D-OUT"<br>"Z-10-D-OUT"<br>"Z-D-IO" | CUSTOM |

| | | |
|---|---|---|
| | "ZC-24-DI"<br>"ZC-24-DO"<br>"ZC-16DI-8DO"<br>"Z-4-AI-1"<br>"Z-8-AI-1"<br>"Z-3-AO"<br>"Z-4-TC"<br>"Z-8-TC"<br>"Z-203"<br>"Z-4RTD-2"<br>"Z-SG"<br>"Z-DAQ-PID"<br>"S-203T"<br>"S-203TA"<br>"ZE-4DI-2AI-2DO"<br>"ZE-2AI"<br>"Z-4DI-2AI-2DO"<br>"S203TA-D"<br>"S203RC-D"<br>“Z-PASS-IO”<br>“Z-PASS-GPS” | |
| Target Resource | This field identifies a particular resource (tag) on one of Seneca devices; possibile values depend on the selected device, in “Target Modbus Device” field; if that field is set to “CUSTOM”, “Target Resource” field is empty; when “Target Resource” field is set, “Target Modbus Start Register Address”, “Target Modbus Request Type” and “Target Register Data Type” fields are automatically set | *Empty* |
| Target Connected To | This field identifies the serial port the target device is connected to; possible values are: COM1, COM2, COM4 (only if the ports are configured as master), INTERNAL or the Modbus TCP-IP Server name. | The first available serial port, that is the first port with “Task” other than “None” |
| Target Modbus Station Address | Modbus Address of the target device | 1 |
| Target Modbus Start Register | Start Register Address of the tag on | 1 |

| | | |
|---|---|---|
| Address | the Modbus device | |
| Target Modbus Request Type | Possible Modbus data types:<br>COIL<br>DISCRETE INPUT<br>HOLDING REGISTER<br>INPUT REGISTER | HOLDING REGISTER |
| Target Register Data Type | Possible data types:<br>16BIT SIGNED<br>16BIT UNSIGNED<br>32BIT SIGNED MSW<br>32BIT UNSIGNED MSW<br>32BIT SIGNED LSW<br>32BIT UNSIGNED LSW<br>32BIT REAL MSW<br>32BIT REAL LSW<br>64BIT UNSIGNED MSW<br>64BIT UNSIGNED LSW<br>64BIT SIGNED MSW<br>64BIT SIGNED LSW<br>64BIT REAL LSW<br>BOOL<br>For more information about the above data types, see table below | 16 BIT SIGNED |
| Target Bit Index | This parameter defines the position, in the [0..16] interval, of the bit to be extracted from the tag value.<br>0 means no bit shall be extracted and the tag value shall be taken as a whole.<br>This parameter is meaningful only when the tag “Target Register Data Type” is set to “16 BIT UNSIGNED” | 0 |
| Gateway Tag Mode | This field defines how the tag will be handled by the gateway processes; possible values are: GATEWAY, BRIDGE, SHARED MEMORY or EMBEDDED.<br><br>The difference between Gateway and Bridge is that the Bridge tags are updated only when requested. | |

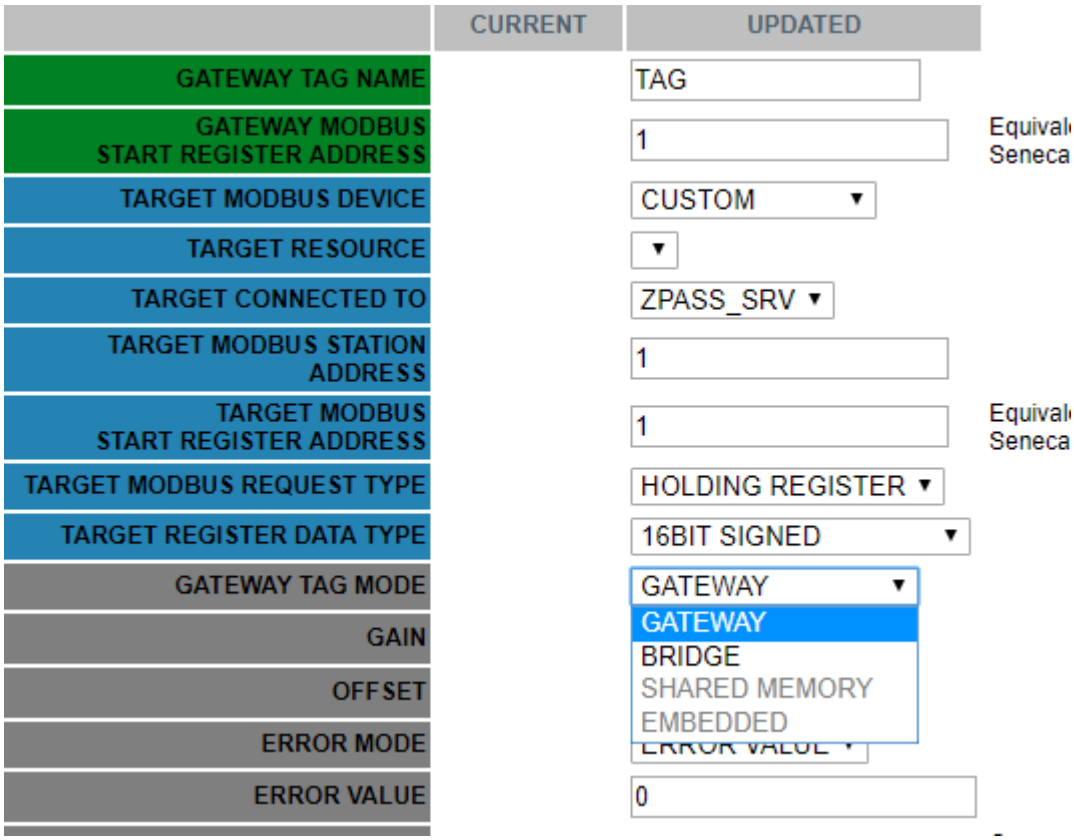
| | | |
|---|---|---|
| | SHARED MEMORY are tags that can be written from Modbus RTU/Modbus TCP-IP or from the Logic Rules. These type of tags can be used also for the Calculated Tags.<br><br>EMBEDDED<br>for embedded Digital I/Os and GPS Info tags (see next paragraphs) | |
| Gain | This field corresponds to the *m* coefficient value in the<br>m*val + q<br>formula applied to the *val* value read from the device | 1 |
| Offset | This field corresponds to the *q* factor value in the<br>m*val + q<br>formula applied to the *val* value read from the device | 0 |
| Initial Value | This filed is available only if "Gateway Tag mode" is configured in "Shared Memory" and define the TAG staring value. | 0 |
| Error Mode | This field defines which value is given in the response to a Modbus (read) request, when the value from the target device is not available.<br>Possible modes are:<br>LAST VALUE: the last available value is given<br>ERROR VALUE: the value specified in the "ERROR VALUE" field is given | LAST VALUE |
| Error Value | This field defines which value is given in the response to a Modbus (read) request, when the value from the target device is not available and the "ERROR MODE" field is set to "ERROR VALUE" | Empty |
| HTTP POST VID | This field is used to build the "Variable ID" (VID) which identifies the tag in HTTP POST requests | "V" + tag index, e.g. "V0" for the first tag, "V1" for the second and so on |

| | | |
|---|---|---|
| | (useful only when HTTP POST protocol is enabled).<br>The VID string is given by "V" character plus the number contained in the field | |
| Read Only | If selected the tag can only be written from an external protocol (for example Modbus RTU or TCP-IP) and not from a logic rule. | DISABLED |
| Retain | If selected the tag is saved in a retain memory (feRAM), when you reboot the device the last value is loaded from the memory.<br>This option is available only for SHARED MEMORY Tags. | OFF |
| Calculated Function | Active only if Gatway Tag mode is "Shared Memory". Can be used for calculate the MIN/MAX/AVG value of a tag.<br>Note that the calculation is enabled only if the datalogger is enabled. The calculation time is the acquisition time. | NONE |
| Alarm Enabled | This field is a read-only flag telling if an alarm is defined for the tag (see "Alarm Configuration" paragraph) | OFF |

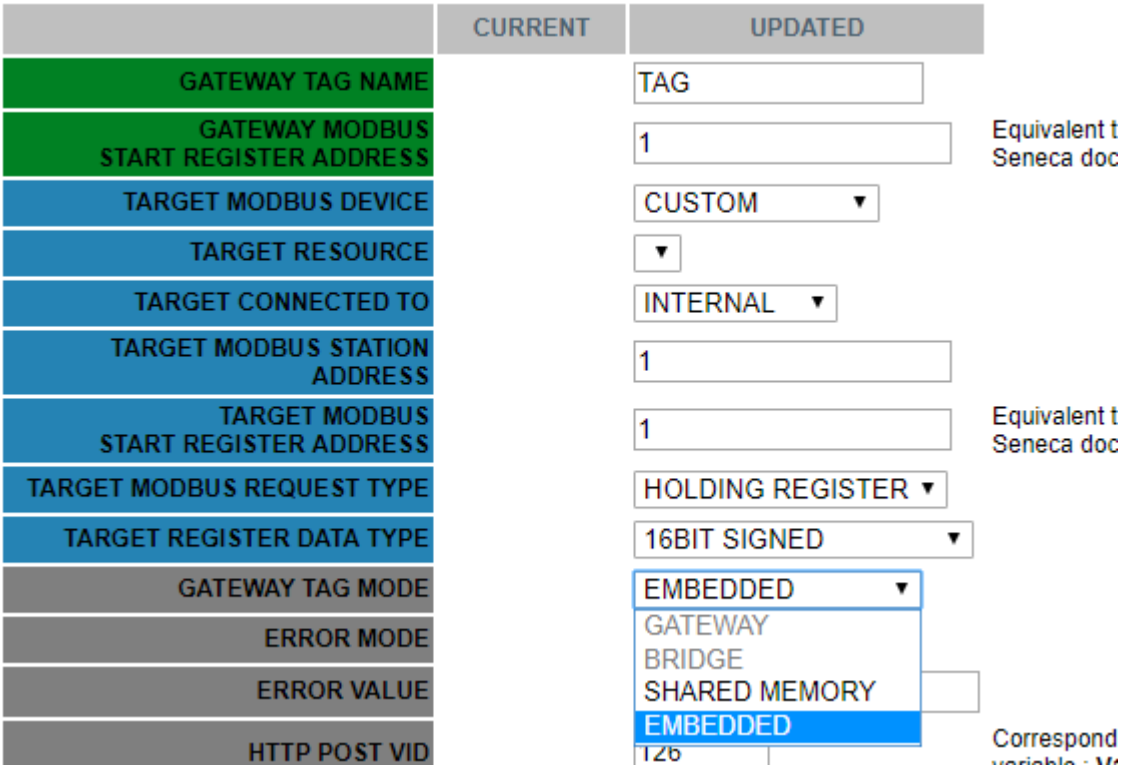
| **Data Type** | **Meaning** |
|---|---|
| 16BIT SIGNED | 1 register, from -32768 to +32767 |
| 16BIT UNSIGNED | 1 register, from 0 to 65535 |
| 32BIT SIGNED MSW | 2 registers with the lowest address register holding the Most Significant Word, from -2147483648 to +2147483647 |
| 32BIT UNSIGNED MSW | 2 registers with the lowest address register holding the Most Significant Word, from 0 to 4294967295 |
| 32BIT SIGNED LSW | 2 registers with the lowest address register holding the Least Significant Word, from -2147483648 to +2147483647 |
| 32BIT UNSIGNED LSW | 2 registers with the lowest address register holding the Least Significant Word, from 0 to 4294967295 |
| 32BIT REAL MSW | 2 registers with the lowest address register holding the Most Significant Word, Floating Point single precision (IEEE 754-2008) |

| | |
|---|---|
| 32BIT REAL LSW | 2 registers with the lowest address register holding the Least Significant Word, Floating Point single precision (IEEE 754-2008) |
| 64 BIT REAL LSW | 4 registers, Floating Point double precision (IEEE 754-2008) |
| 64BIT UNSIGNED MSW | 4 with the lowest address register holding the Most Significant Word, from 0 to 18446744073709551616 |
| 64BIT UNSIGNED LSW | 4 with the lowest address register holding the Least Significant Word, from 0 to 18446744073709551616 |
| 64BIT SIGNED MSW | 4 with the lowest address register holding the Most Significant Word, from -9223372036854775808 to +9223372036854775807 |
| 64BIT SIGNED LSW | 4 with the lowest address register holding the Least Significant Word, from -9223372036854775808 to +9223372036854775807 |
| BOOL | 1 Boolean Coil or Discrete Input register |

The following figure shows the case when no serial port is used for Modbus Shared Memory Gateway and a TCP Server named “Z-PASS2_SRV” is configured; so the possible values for “GATEWAY TAG MODE” parameter are “GATEWAY” and “BRIDGE”.




The following figure shows the case when “TARGET CONNECT TO” parmeter is “Internal” so the possible values for “GATEWAY TAG MODE” parameter are “SHARED MEMORY” and “BRIDGE”.



Some more explanations are needed for “Gateway Tag Mode” parameter.

Tags with Mode=GATEWAY are handled in the “classic” Modbus Shared Memory Gateway way, that is tags are read periodically, even if no Modbus read request is received for those tags.

Tags with Mode=BRIDGE are read only when a Modbus read request is received for those tags.

Instead, for write operations, tags with Mode=GATEWAY and tags with Mode=BRIDGE are handled in the same way, that is tags are written only when a Modbus write request is received for those tags.

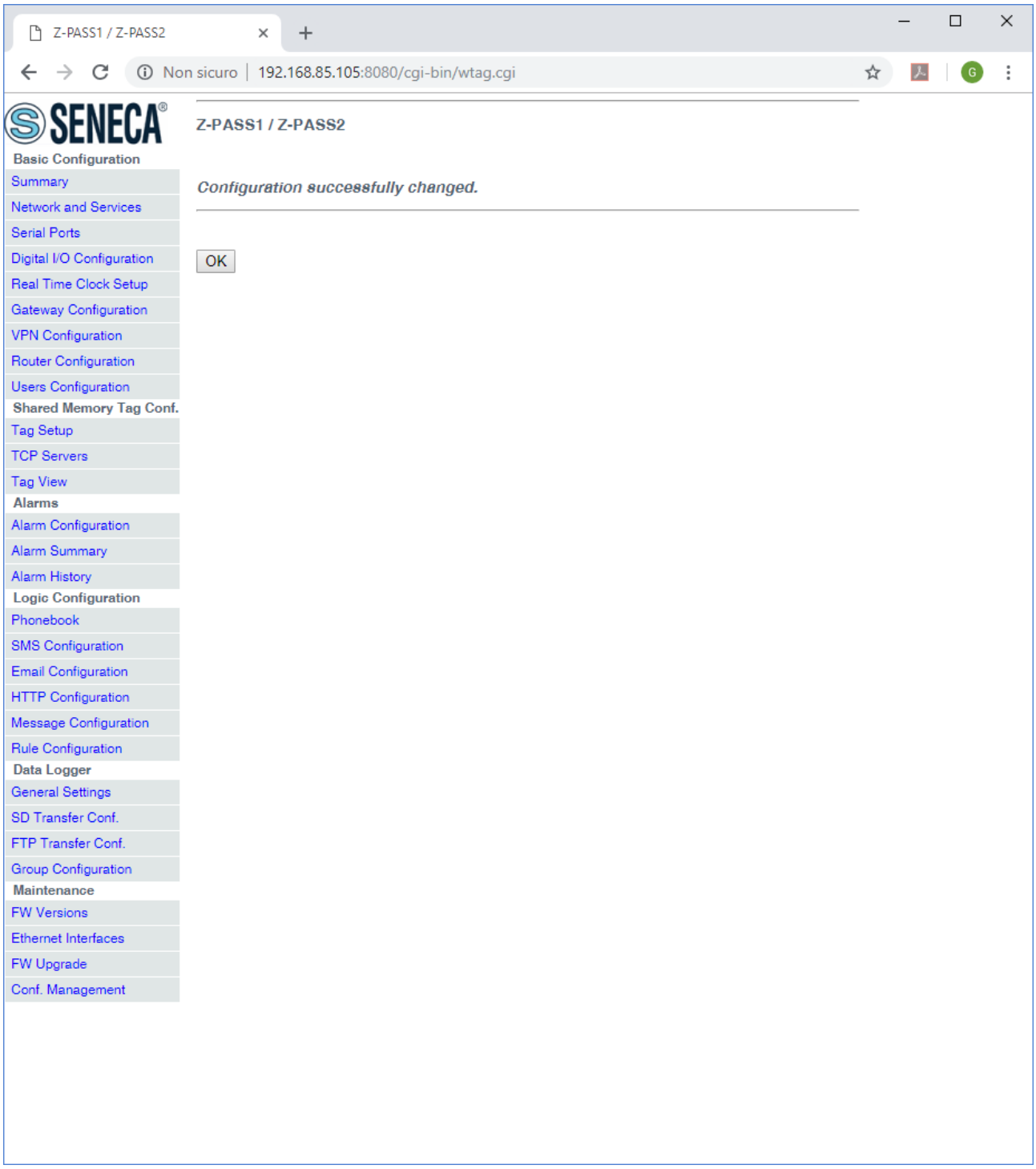
The Mode=BRIDGE option is particularly useful for Modbus RTU devices with the “Fail Safe” feature available for output lines, as for many Seneca devices; normally, those devices are designed to put their output lines to “fail safe” value, when the connection to the master (e.g. a SCADA system) goes down; since the criterion to detect the “connection failure” is that no Modbus (write and read) request is received, the “fail safe” mode can’t be entered with “classic” gateway behaviour.

Tags with Mode=SHARED MEMORY are stored only in CPU memory, not in any device, so their values are written/read only when a Modbus write/read request is received for those tags.

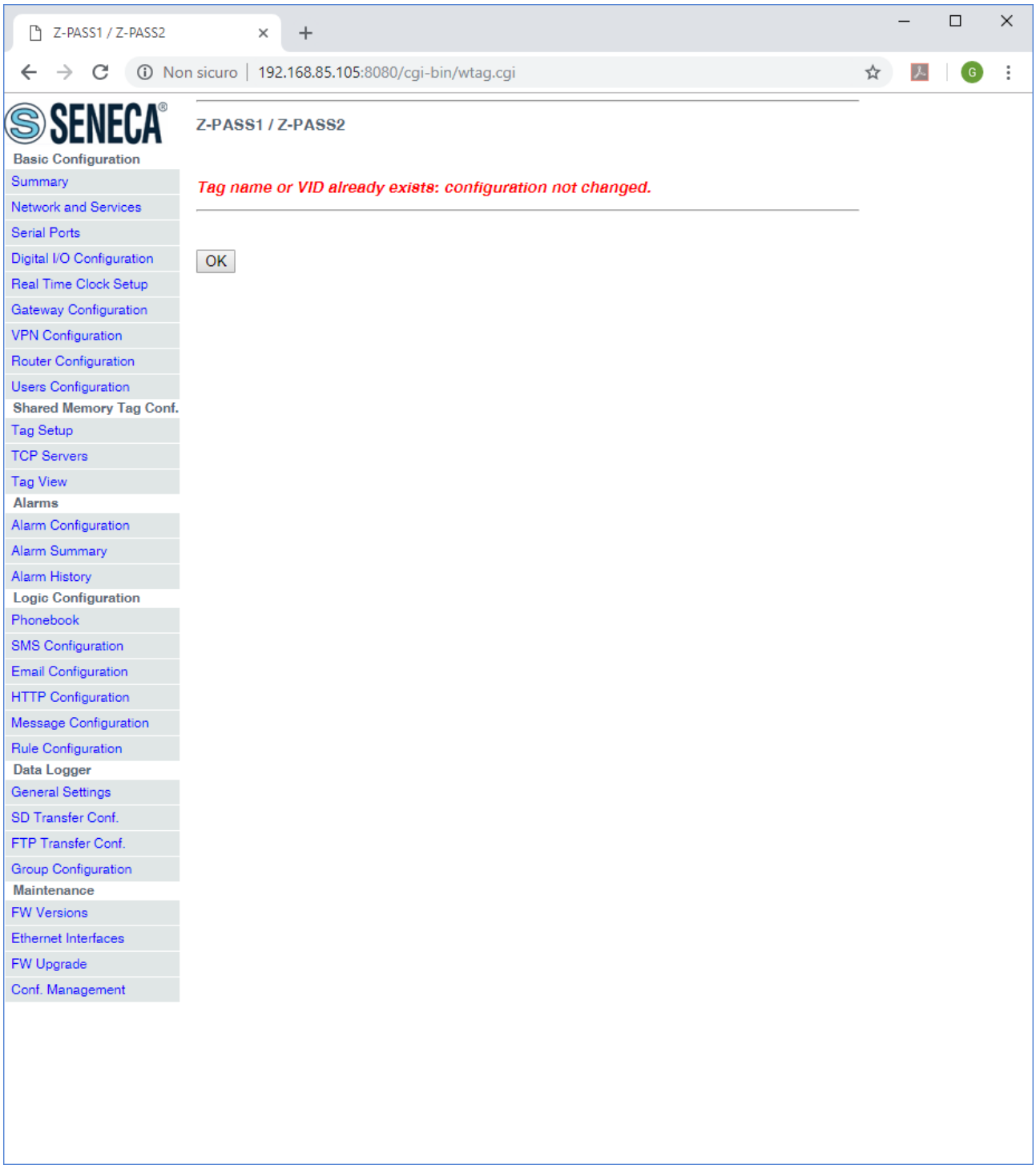
Tags Embedded are used for embedded I/O and GPS.

NOTE: all considerations related to requests received on the Modbus TCP/IP side identically apply to requests received on a serial port configured as Modbus RTU Slave.

By clicking on the “APPLY” button, the tag is added/modified and the following page is shown.



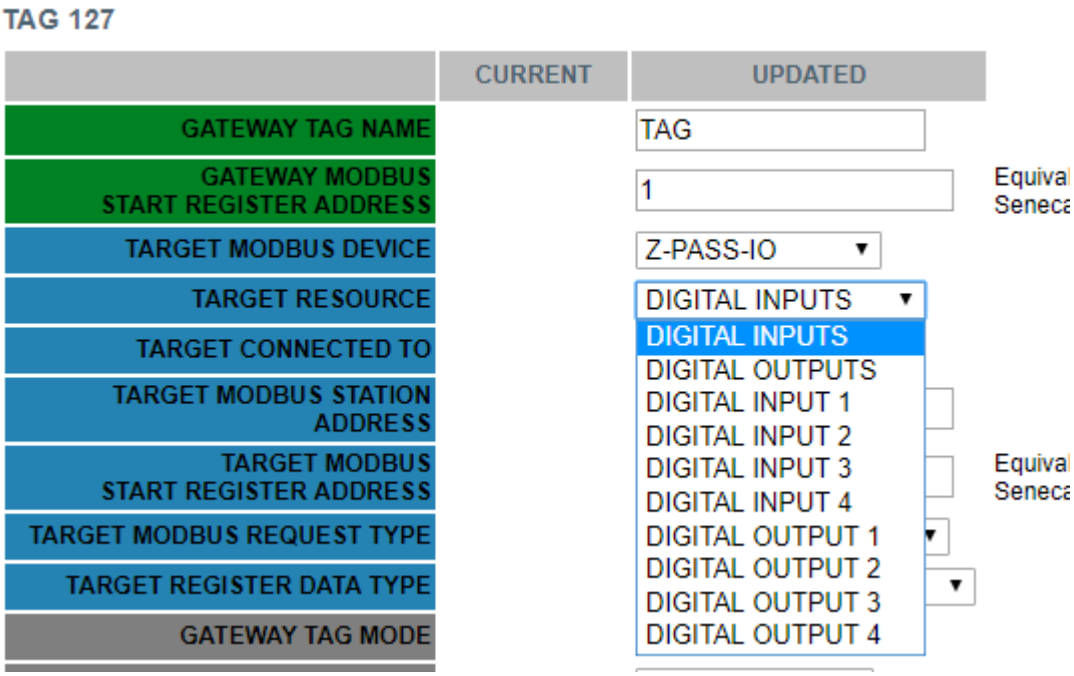

To let the Data Logger functionality work properly, the tag names shall be distinct; so if you add/modify a tag and its name is already assigned to another tag, the following error message is shown.




By clicking on the “OK” button, you go back to the “Gateway Tag Setup” page.

### *20.3.2.2 Tags for Embedded I/O*

Tags corresponding to the Z-PASS embedded digital I/Os, as shown in the following figure:




Depending on the value of the "TARGET RESOURCE" parameter, the other parameters are set to the values shown in the following table:

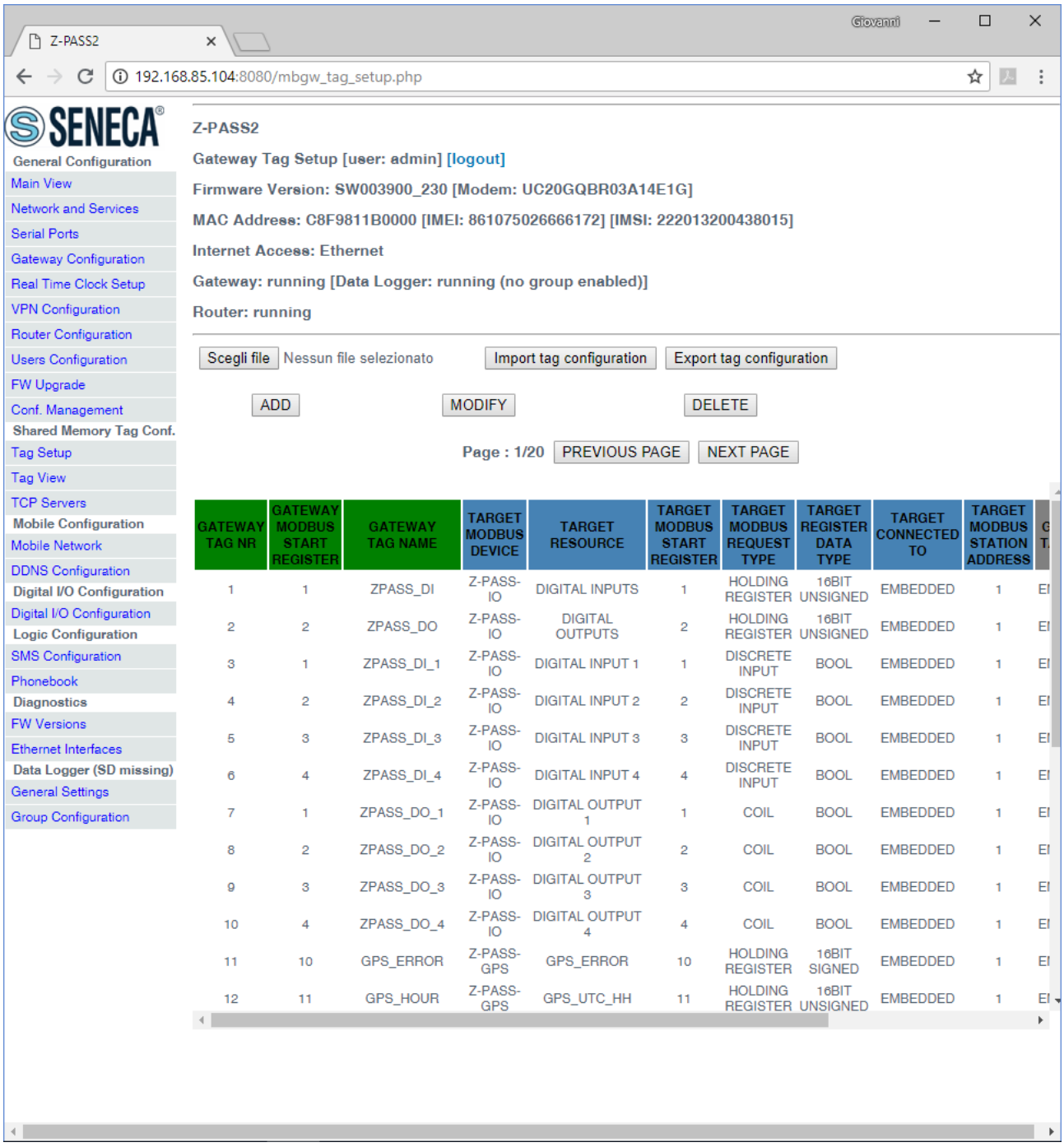
| TARGET RESOURCE | TARGET MODBUS RTU START REGISTER ADDRESS | TARGET MODBUS REQUEST TYPE | TARGET REGISTER DATA TYPE |
|---|---|---|---|
| DIGITAL INPUTS | 1 (40001) | HOLDING REGISTER | 16BIT UNSIGNED |
| DIGITAL OUTPUTS | 2 (40002) | HOLDING REGISTER | 16BIT UNSIGNED |
| DIGITAL INPUT 1 | 1 (10001) | DISCRETE INPUT | BOOL |
| DIGITAL INPUT 2 | 2 (10002) | DISCRETE INPUT | BOOL |
| DIGITAL INPUT 3 | 3 (10003) | DISCRETE INPUT | BOOL |
| DIGITAL INPUT 4 | 4 (10004) | DISCRETE INPUT | BOOL |
| DIGITAL OUTPUT 1 | 1 (1) | COIL | BOOL |
| DIGITAL OUTPUT 2 | 2 (2) | COIL | BOOL |
| DIGITAL OUTPUT 3 | 3 (3) | COIL | BOOL |
| DIGITAL OUTPUT 4 | 4 (4) | COIL | BOOL |

You can easily check that these tags correspond to Modbus Registers defined in paragraph 20.1.6.1.1.

For these tags, other parameter values are fixed:

- TARGET MODBUS SLAVE STATION ADDRESS 1
- TARGET CONNECTED TO SERIAL PORT EMBEDDED
- GATEWAY TAG MODE EMBEDDED

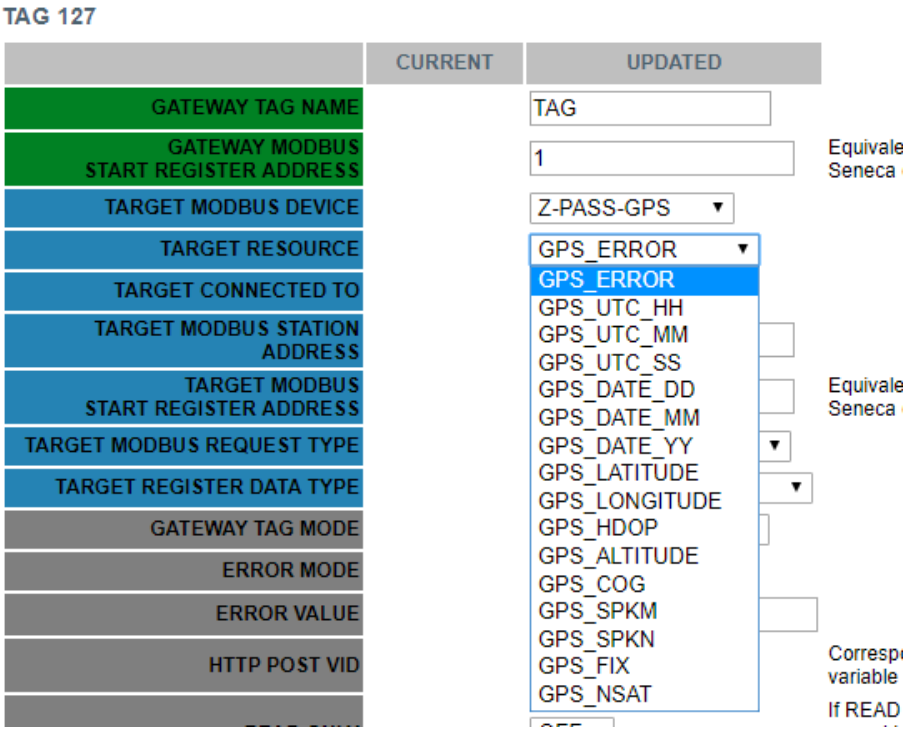
The default configuration for Z-PASS1 and Z-PASS2 already contain tags for embedded I/Os, as shown in the following figure.




| GATEWAY TAG NR | GATEWAY MODBUS START REGISTER | GATEWAY TAG NAME | TARGET MODBUS DEVICE | TARGET RESOURCE | TARGET MODBUS START REGISTER | TARGET MODBUS REQUEST TYPE | TARGET REGISTER DATA TYPE | TARGET CONNECTED TO | TARGET MODBUS STATION ADDRESS | G T |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | ZPASS_DI | Z-PASS-IO | DIGITAL INPUTS | 1 | HOLDING REGISTER | 16BIT UNSIGNED | EMBEDDED | 1 | EI |
| 2 | 2 | ZPASS_DO | Z-PASS-IO | DIGITAL OUTPUTS | 2 | HOLDING REGISTER | 16BIT UNSIGNED | EMBEDDED | 1 | EI |
| 3 | 1 | ZPASS_DI_1 | Z-PASS-IO | DIGITAL INPUT 1 | 1 | DISCRETE INPUT | BOOL | EMBEDDED | 1 | EI |
| 4 | 2 | ZPASS_DI_2 | Z-PASS-IO | DIGITAL INPUT 2 | 2 | DISCRETE INPUT | BOOL | EMBEDDED | 1 | EI |
| 5 | 3 | ZPASS_DI_3 | Z-PASS-IO | DIGITAL INPUT 3 | 3 | DISCRETE INPUT | BOOL | EMBEDDED | 1 | EI |
| 6 | 4 | ZPASS_DI_4 | Z-PASS-IO | DIGITAL INPUT 4 | 4 | DISCRETE INPUT | BOOL | EMBEDDED | 1 | EI |
| 7 | 1 | ZPASS_DO_1 | Z-PASS-IO | DIGITAL OUTPUT 1 | 1 | COIL | BOOL | EMBEDDED | 1 | EI |
| 8 | 2 | ZPASS_DO_2 | Z-PASS-IO | DIGITAL OUTPUT 2 | 2 | COIL | BOOL | EMBEDDED | 1 | EI |
| 9 | 3 | ZPASS_DO_3 | Z-PASS-IO | DIGITAL OUTPUT 3 | 3 | COIL | BOOL | EMBEDDED | 1 | EI |
| 10 | 4 | ZPASS_DO_4 | Z-PASS-IO | DIGITAL OUTPUT 4 | 4 | COIL | BOOL | EMBEDDED | 1 | EI |
| 11 | 10 | GPS_ERROR | Z-PASS-GPS | GPS_ERROR | 10 | HOLDING REGISTER | 16BIT SIGNED | EMBEDDED | 1 | EI |
| 12 | 11 | GPS_HOUR | Z-PASS-GPS | GPS_UTC_HH | 11 | HOLDING REGISTER | 16BIT UNSIGNED | EMBEDDED | 1 | EI |

### *20.3.2.3 Tags for GPS Info (Z-PASS2)*

Tags corresponding to the Z-PASS2 GPS are shown in the following figure:




Depending on the value of the "TARGET RESOURCE" parameter, the other parameters are set to the values shown in the following table:

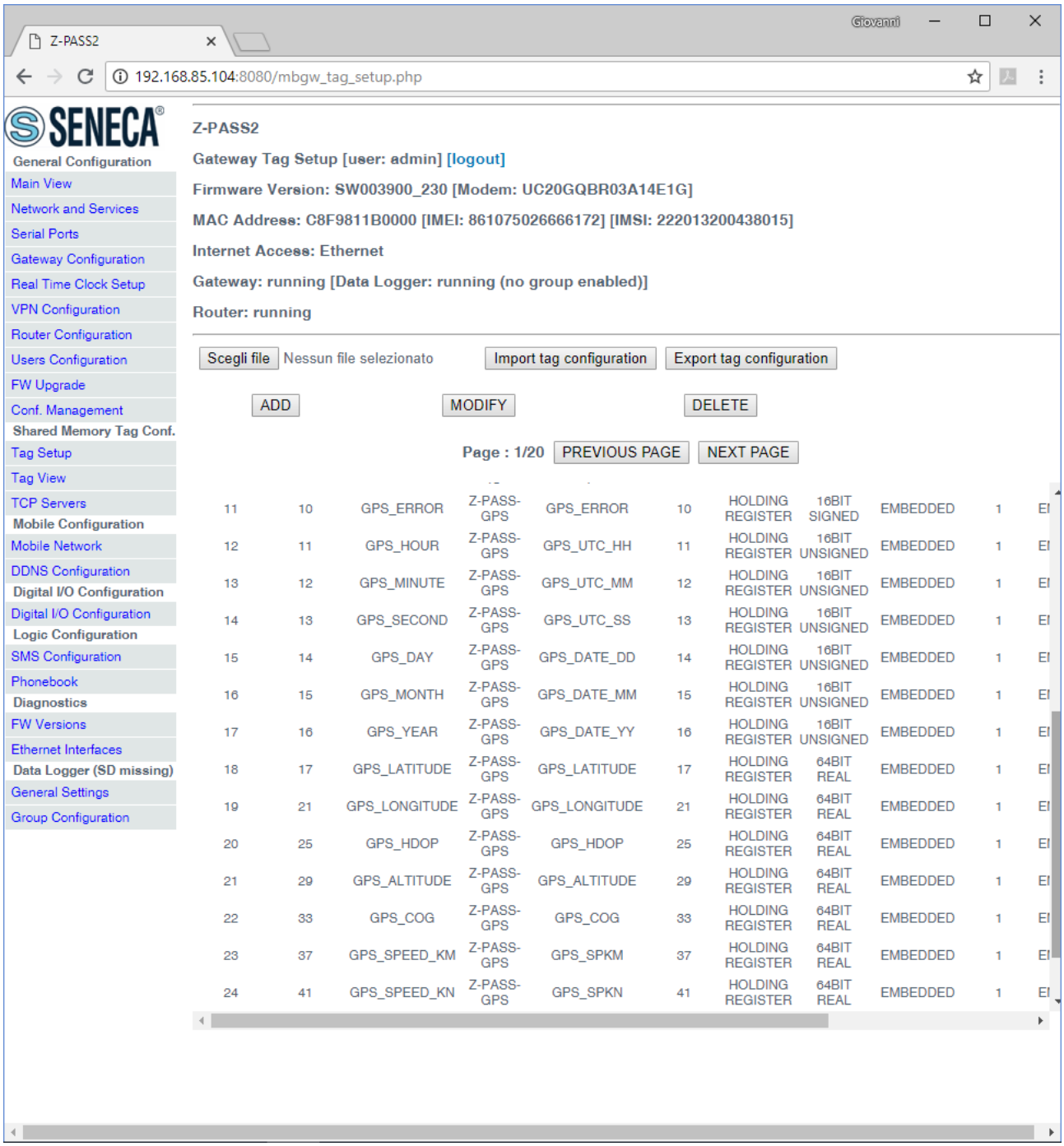
| TARGET RESOURCE | TARGET MODBUS RTU START REGISTER ADDRESS | TARGET MODBUS REQUEST TYPE | TARGET REGISTER DATA TYPE |
|---|---|---|---|
| GPS_ERROR | 10 (40010) | HOLDING REGISTER | 16BIT SIGNED |
| GPS_UTC_HH | 11 (40011) | HOLDING REGISTER | 16BIT UNSIGNED |
| GPS_UTC_MM | 12 (40012) | HOLDING REGISTER | 16BIT UNSIGNED |
| GPS_UTC_SS | 13 (40013) | HOLDING REGISTER | 16BIT UNSIGNED |
| GPS_DATE_DD | 14 (40014) | HOLDING REGISTER | 16BIT UNSIGNED |
| GPS_DATE_MM | 15 (40015) | HOLDING REGISTER | 16BIT UNSIGNED |
| GPS_DATE_YY | 16 (40016) | HOLDING REGISTER | 16BIT UNSIGNED |
| GPS_LATITUDE | 17 – 20 (40017 – 40020) | HOLDING REGISTER | 64BIT REAL |
| GPS_LONGITUDE | 21 – 24 (40021 – 40024) | HOLDING REGISTER | 64BIT REAL |
| GPS_HDOP | 25 – 28 (40025 – 40028) | HOLDING REGISTER | 64BIT REAL |
| GPS_ALTITUDE | 29 – 32 (40029 – 40032) | HOLDING REGISTER | 64BIT REAL |
| GPS_COG | 33 – 36 (40033 – 40036) | HOLDING REGISTER | 64BIT REAL |
| GPS_SPEED_KM | 37 – 40 (40037 – 40040) | HOLDING REGISTER | 64BIT REAL |
| GPS_SPEED_KN | 41 – 44 (40041 – 40044) | HOLDING REGISTER | 64BIT REAL |
| GPS_FIX | 45 (40045) | HOLDING REGISTER | 16BIT UNSIGNED |
| GPS_NSAT | 46 (40046) | HOLDING REGISTER | 16BIT UNSIGNED |

For these tags, other parameter values are fixed:

- TARGET MODBUS STATION ADDRESS 1
- TARGET CONNECTED TO EMBEDDED

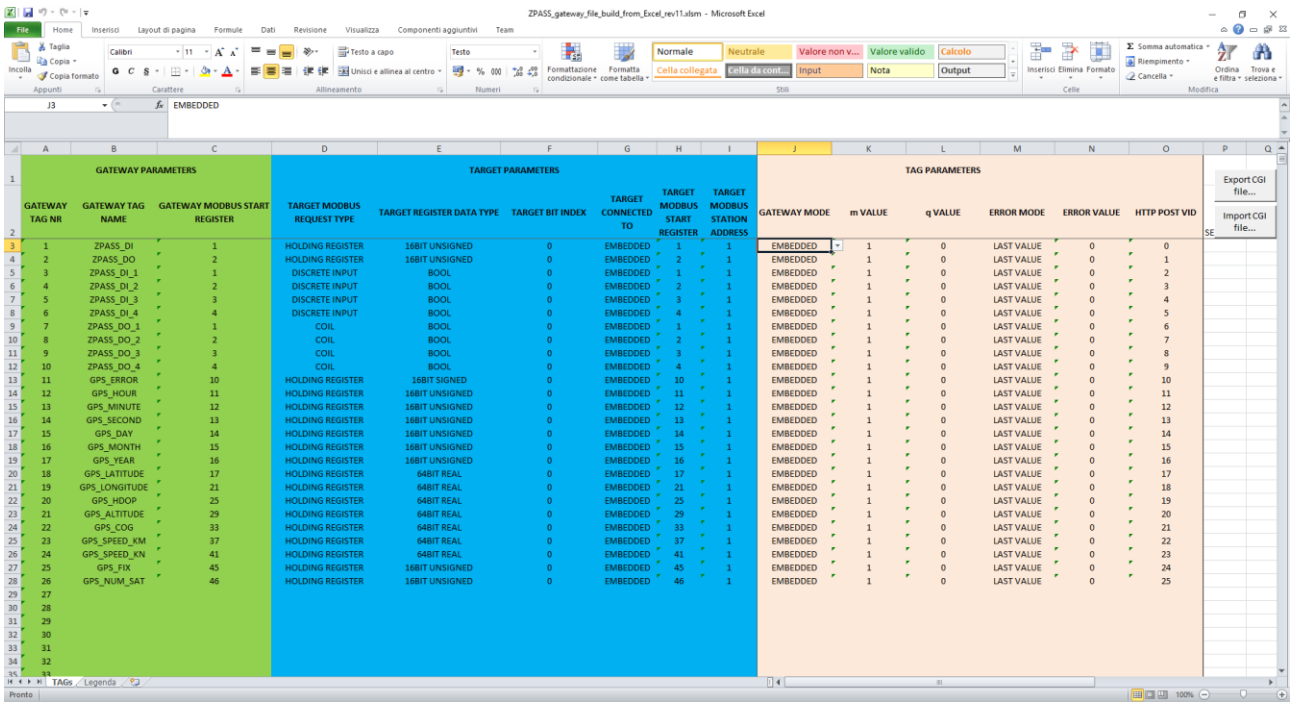
- GATEWAY TAG MODE EMBEDDED

The default configuration for Z-PASS2 already contain tags for GPS information, as shown in the following figure.




### *20.3.2.4 Microsoft Excel™ Template for Tag Setup*

Another way to create the tag configuration is by means of the “Microsoft Excel™ Template” provided by Seneca, shown in the following figure.



| GATEWAY PARAMETERS | | | TARGET PARAMETERS | | | | | | TAG PARAMETERS | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| GATEWAY TAG NR | GATEWAY TAG NAME | GATEWAY MODBUS START REGISTER | TARGET MODBUS REQUEST TYPE | TARGET REGISTER DATA TYPE | TARGET BIT INDEX | TARGET CONNECTED TO | TARGET MODBUS START REGISTER | TARGET MODBUS STATION ADDRESS | GATEWAY MODE | m VALUE | q VALUE | ERROR MODE | ERROR VALUE | HTTP POST VID | |
| 1 | ZPASS_DI | 1 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 1 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 0 | |
| 2 | ZPASS_DO | 1 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 2 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 1 | |
| 3 | ZPASS_DI_1 | 1 | DISCRETE INPUT | BOOL | 0 | EMBEDDED | 1 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 2 | |
| 4 | ZPASS_DI_2 | 2 | DISCRETE INPUT | BOOL | 0 | EMBEDDED | 2 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 3 | |
| 5 | ZPASS_DI_3 | 3 | DISCRETE INPUT | BOOL | 0 | EMBEDDED | 3 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 4 | |
| 6 | ZPASS_DI_4 | 4 | DISCRETE INPUT | BOOL | 0 | EMBEDDED | 4 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 5 | |
| 7 | ZPASS_DO_1 | 1 | COIL | BOOL | 0 | EMBEDDED | 1 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 6 | |
| 8 | ZPASS_DO_2 | 2 | COIL | BOOL | 0 | EMBEDDED | 2 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 7 | |
| 9 | ZPASS_DO_3 | 3 | COIL | BOOL | 0 | EMBEDDED | 3 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 8 | |
| 10 | ZPASS_DO_4 | 4 | COIL | BOOL | 0 | EMBEDDED | 4 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 9 | |
| 11 | GPS_ERROR | 10 | HOLDING REGISTER | 16BIT SIGNED | 0 | EMBEDDED | 10 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 10 | |
| 12 | GPS_HOUR | 11 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 11 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 11 | |
| 13 | GPS_MINUTE | 12 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 12 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 12 | |
| 14 | GPS_SECOND | 13 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 13 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 13 | |
| 15 | GPS_DAY | 14 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 14 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 14 | |
| 16 | GPS_MONTH | 15 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 15 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 15 | |
| 17 | GPS_YEAR | 16 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 16 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 16 | |
| 18 | GPS_LATITUDE | 17 | HOLDING REGISTER | 64BIT REAL | 0 | EMBEDDED | 17 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 17 | |
| 19 | GPS_LONGITUDE | 21 | HOLDING REGISTER | 64BIT REAL | 0 | EMBEDDED | 21 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 18 | |
| 20 | GPS_HDOP | 25 | HOLDING REGISTER | 64BIT REAL | 0 | EMBEDDED | 25 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 19 | |
| 21 | GPS_ALTITUDE | 29 | HOLDING REGISTER | 64BIT REAL | 0 | EMBEDDED | 29 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 20 | |
| 22 | GPS_COG | 33 | HOLDING REGISTER | 64BIT REAL | 0 | EMBEDDED | 33 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 21 | |
| 23 | GPS_SPEED_KM | 37 | HOLDING REGISTER | 64BIT REAL | 0 | EMBEDDED | 37 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 22 | |
| 24 | GPS_SPEED_KN | 41 | HOLDING REGISTER | 64BIT REAL | 0 | EMBEDDED | 41 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 23 | |
| 25 | GPS_FIX | 45 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 45 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 24 | |
| 26 | GPS_NUM_SAT | 46 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | EMBEDDED | 46 | 1 | EMBEDDED | 1 | 0 | LAST VALUE | 0 | 25 | |

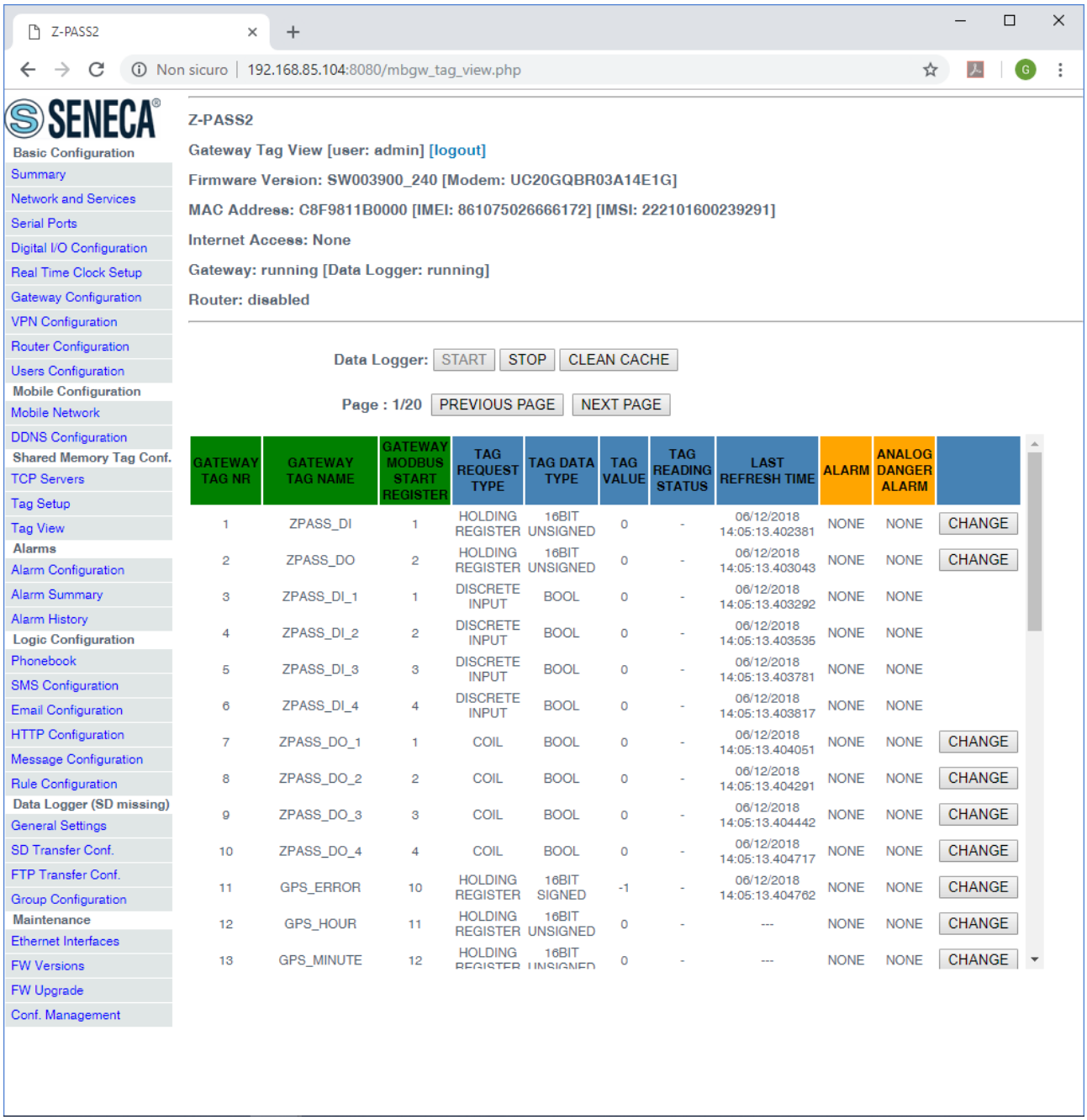
The tag configuration in the Excel sheet can be exported by clicking on the “Export CGI file…” button; the exported binary file can be uploaded to the Z-PASS, by means of the “Import tag configuration” button in the “Tag Setup” page (see 20.3.1 paragraph).

Conversely, the tag configuration created by means of the web page can be imported into the Excel sheet by clicking on the “Import CGI file…” button.

The sheet columns correspond to the parameters in the “Tag Setup” page; please, see 20.3.2.1 paragraph for their meanings.

### *20.3.3 Tag View*

The “Gateway Tag View” page shows the tag values in real-time, as shown in the following figure.



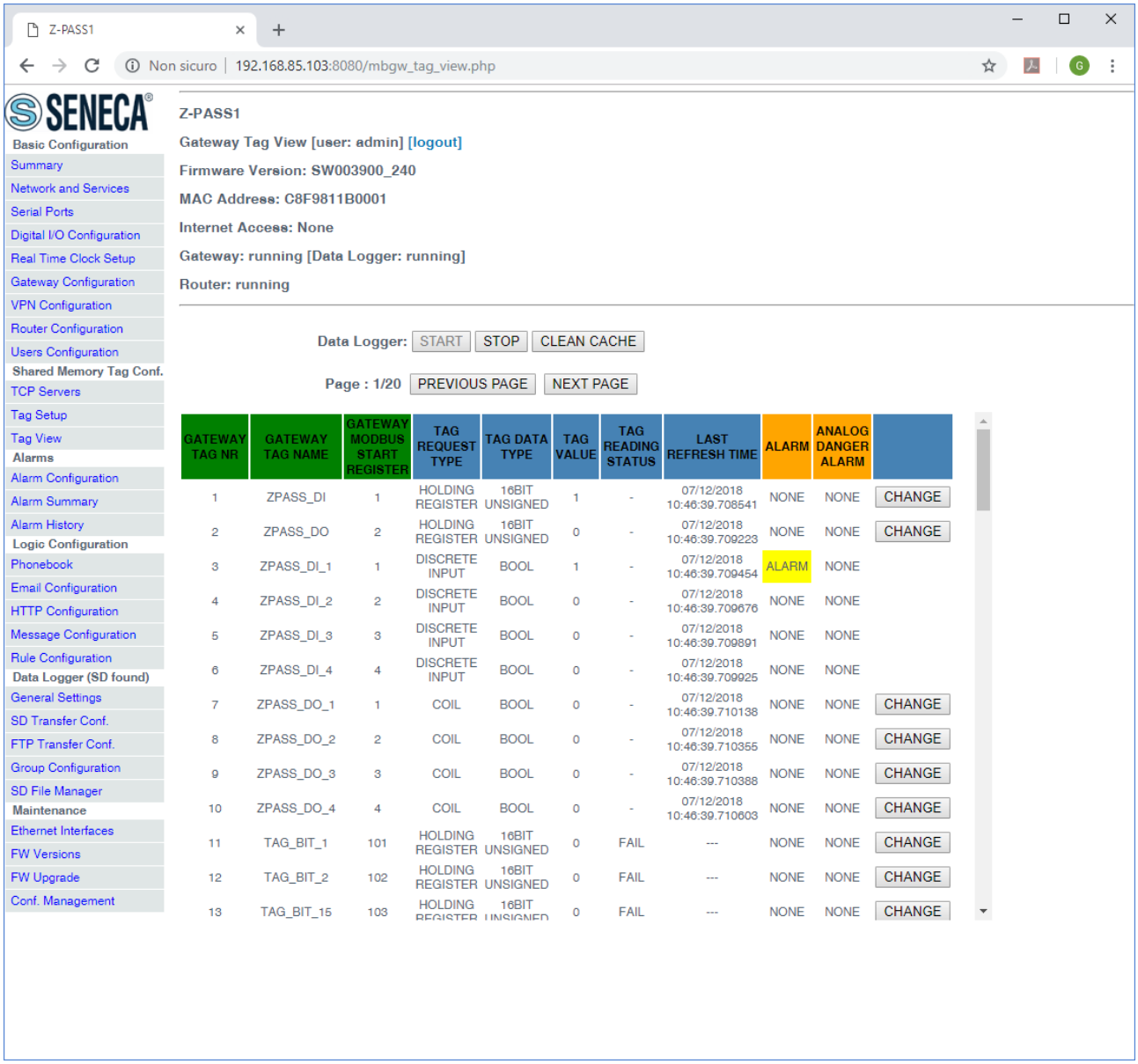

The “Data Logger” buttons can be used to:

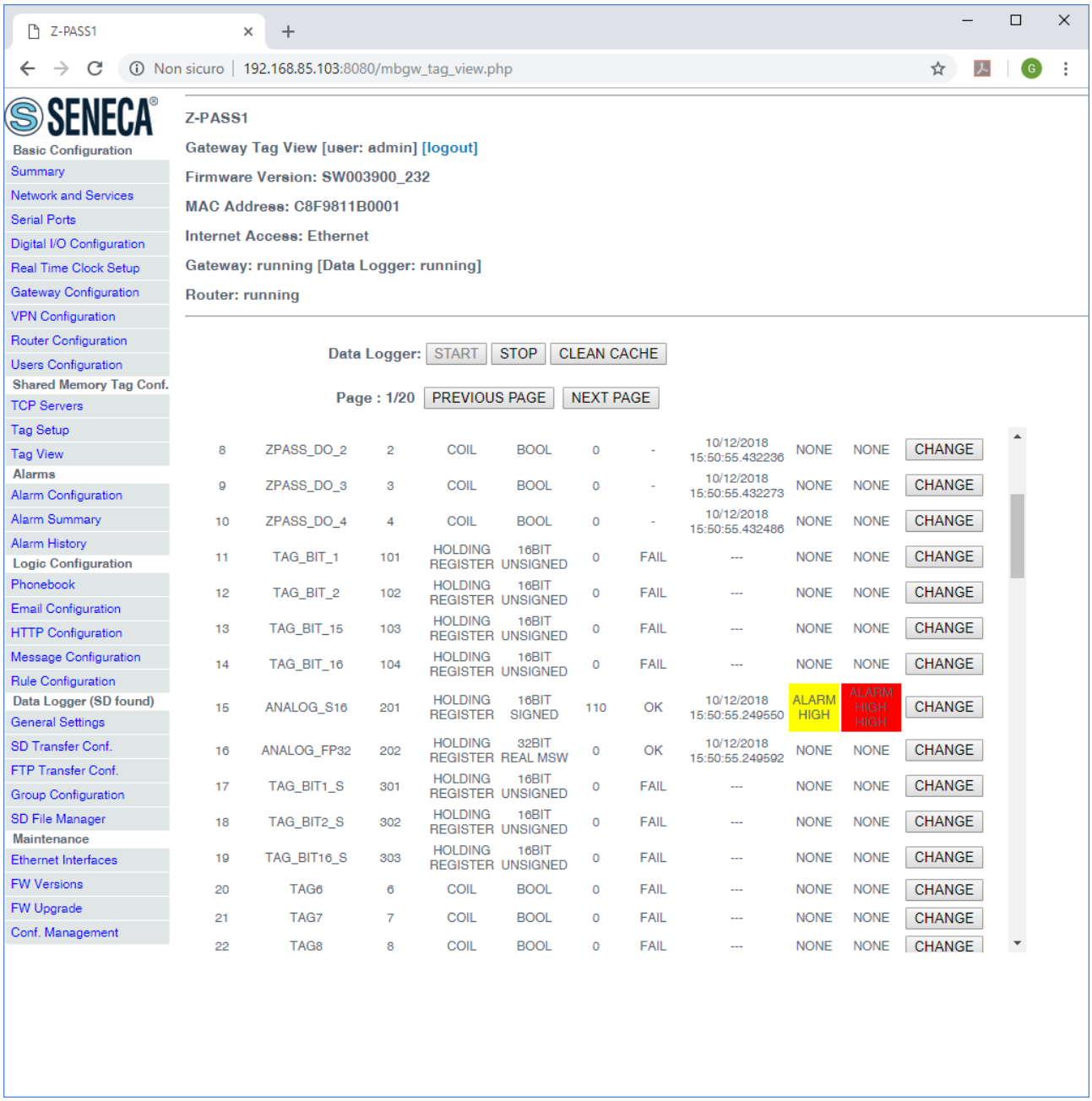
- start the Data Logger functionality, if it is stopped;
- stop the Data Logger functionality, if it is running;
- clean the internal Data Logger cache (this will also stop the Data Logger).

The view is automatically refreshed.

As shown in the following figures, the “ALARM” column reports the status of the alarm defined for the tag, if any; the “ANALOG DANGER ALARM” column has a similar behavior, but it is meaningful only for analog

tags when, in the alarm configuration, the “Alarm Low Low Value” and “Alarm High High Value” thresholds are defined (see paragraph “Alarm Configuration” 20.4.1).






Some notes are worthy about the “TAG READING STATUS” and “LAST REFRESH TIME” columns.

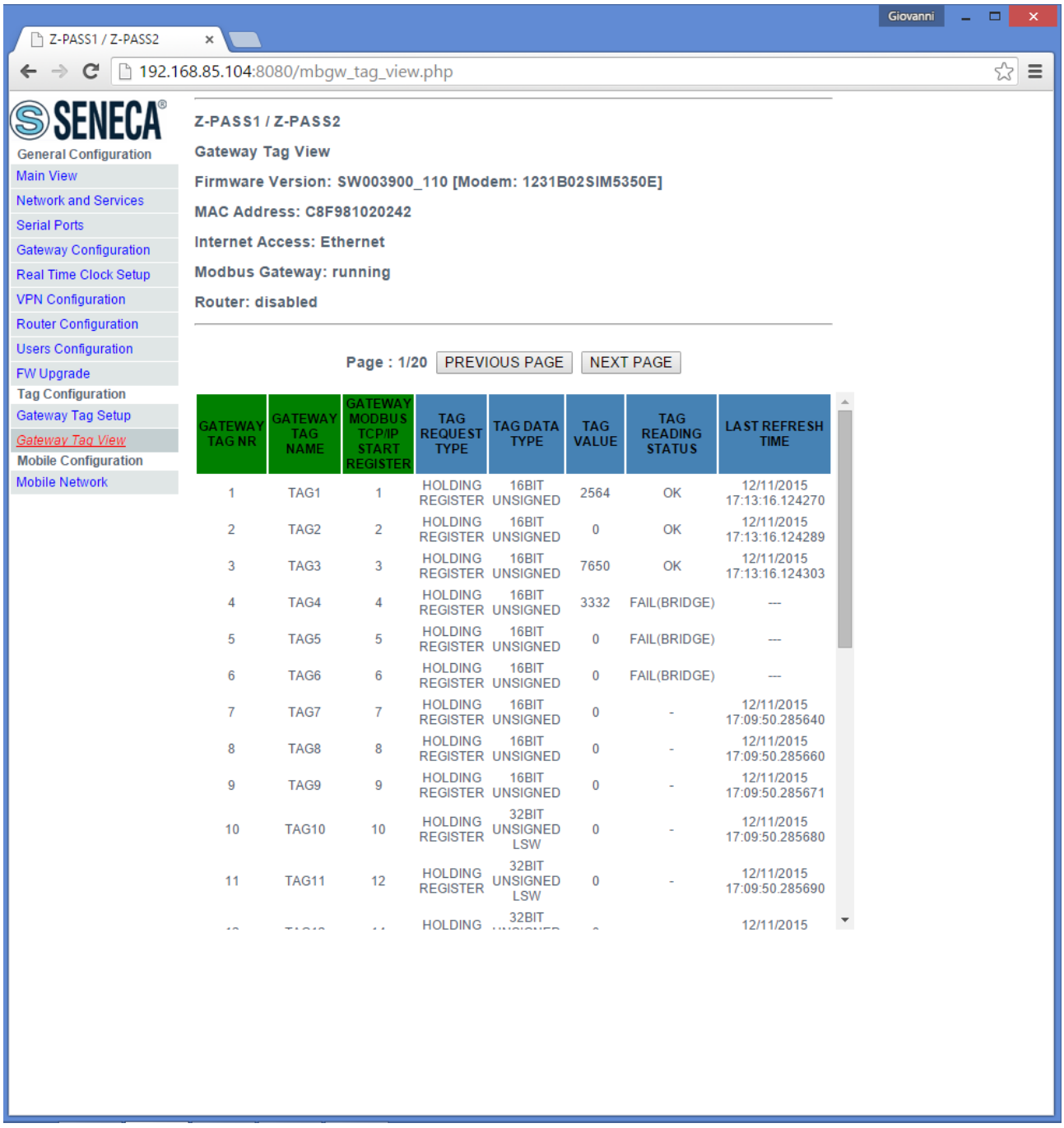
The possible “TAG READING STATUS” values depend on the “GATEWAY TAG MODE” value, in the following way:

| | |
|---|---|
| OK / FAIL | for tags with Mode=GATEWAY |
| OK (BRIDGE) / FAIL(BRIDGE) | for tags with Mode=BRIDGE |
| - | for tags with Mode=SHARED MEMORY or EMBEDDED |

The timestamp in the “LAST REFRESH TIME” column is updated:

- on a successful (Master) read/write operation, for tags with Mode=GATEWAY|BRIDGE|EMBEDDED

- on Modbus Shared Memory Gateway start and on a successful TCP or RTU (Slave) write operation, for tags with Mode=SHARED MEMORY




| GATEWAY TAG NR | GATEWAY TAG NAME | GATEWAY MODBUS TCP/IP START REGISTER | TAG REQUEST TYPE | TAG DATA TYPE | TAG VALUE | TAG READING STATUS | LAST REFRESH TIME |
|---|---|---|---|---|---|---|---|
| 1 | TAG1 | 1 | HOLDING REGISTER | 16BIT UNSIGNED | 2564 | OK | 12/11/2015 17:13:16.124270 |
| 2 | TAG2 | 2 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | OK | 12/11/2015 17:13:16.124289 |
| 3 | TAG3 | 3 | HOLDING REGISTER | 16BIT UNSIGNED | 7650 | OK | 12/11/2015 17:13:16.124303 |
| 4 | TAG4 | 4 | HOLDING REGISTER | 16BIT UNSIGNED | 3332 | FAIL(BRIDGE) | --- |
| 5 | TAG5 | 5 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | FAIL(BRIDGE) | --- |
| 6 | TAG6 | 6 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | FAIL(BRIDGE) | --- |
| 7 | TAG7 | 7 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | - | 12/11/2015 17:09:50.285640 |
| 8 | TAG8 | 8 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | - | 12/11/2015 17:09:50.285660 |
| 9 | TAG9 | 9 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | - | 12/11/2015 17:09:50.285671 |
| 10 | TAG10 | 10 | HOLDING REGISTER | 32BIT UNSIGNED LSW | 0 | - | 12/11/2015 17:09:50.285680 |
| 11 | TAG11 | 12 | HOLDING REGISTER | 32BIT UNSIGNED LSW | 0 | - | 12/11/2015 17:09:50.285690 |
| | | | HOLDING | 32BIT | | | 12/11/2015 |

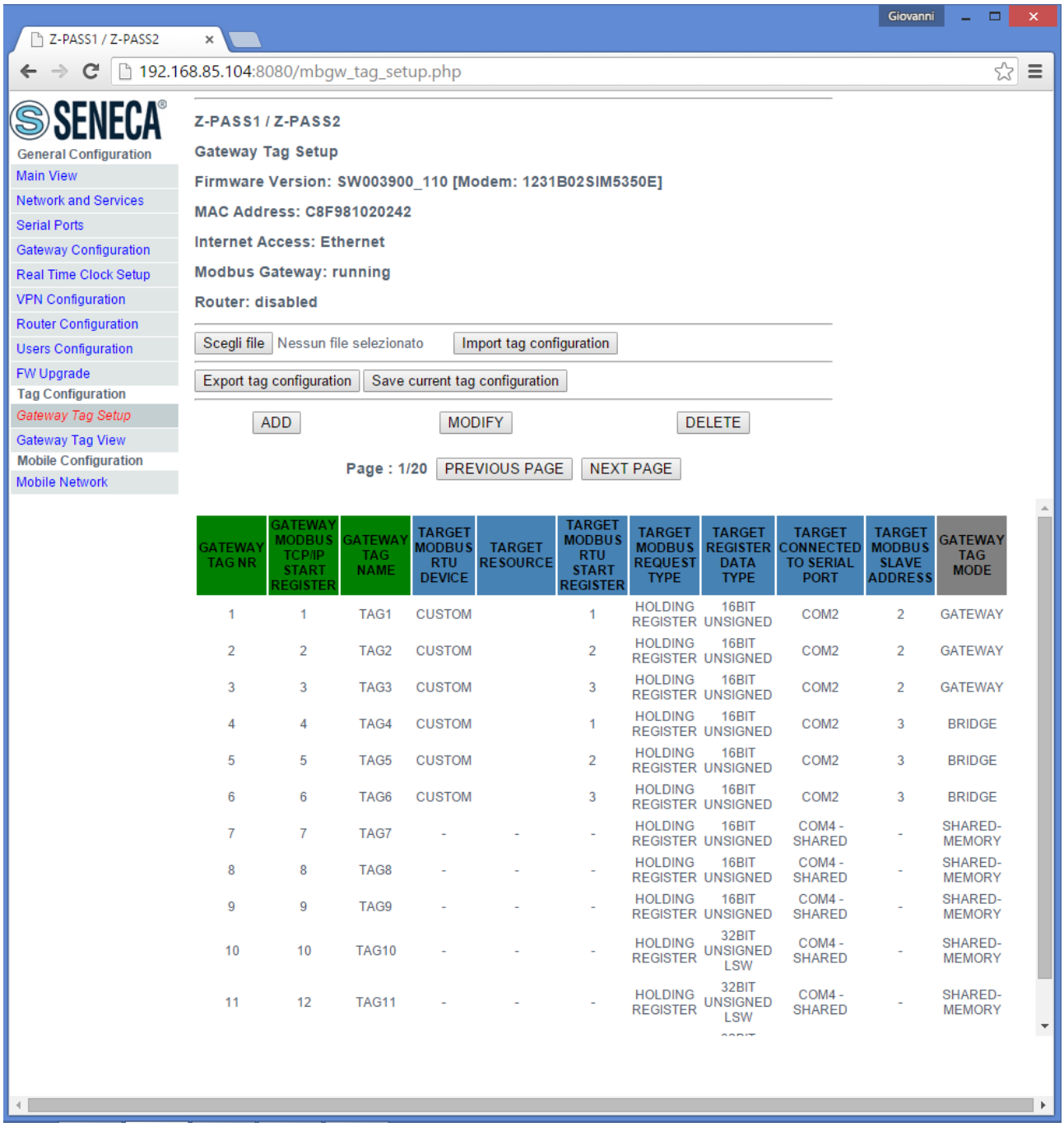
In the above figure[21], the first three tags (Mode=GATEWAY) have been successfully read, so the "TAG READING STATUS" column shows "OK" and the "LAST REFRESH TIME" column contains a valid timestamp.

The next three tags (Mode=BRIDGE) have not been read nor written yet, so the "TAG READING STATUS" column shows "FAIL(BRIDGE)" and the "LAST REFRESH TIME" column does not contain a timestamp.

Finally, for the last tags (Mode=SHARED MEMORY), the "TAG READING STATUS" column shows "-" and the "LAST REFRESH TIME" column contains a valid timestamp that, in this example, corresponds to the Modbus Shared Memory Gateway start time.

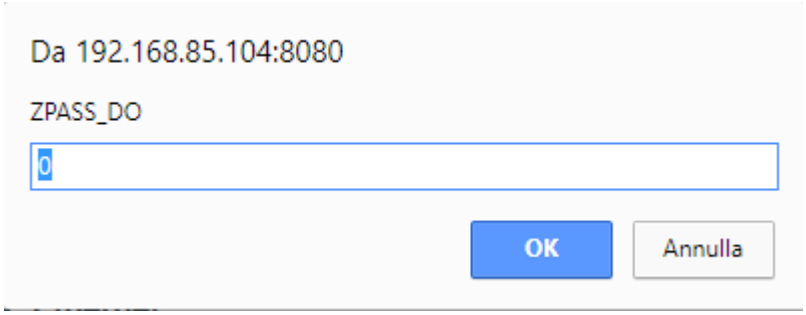
Just as an example, the tag configuration corresponding to the above figure is show below.

[21] This and the following figures refer to an old FW release.

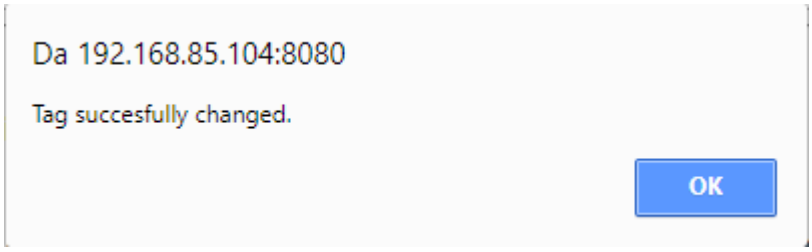



| GATEWAY TAG NR | GATEWAY MODBUS TCP/IP START REGISTER | GATEWAY TAG NAME | TARGET MODBUS RTU DEVICE | TARGET RESOURCE | TARGET MODBUS RTU START REGISTER | TARGET MODBUS REQUEST TYPE | TARGET REGISTER DATA TYPE | TARGET CONNECTED TO SERIAL PORT | TARGET MODBUS SLAVE ADDRESS | GATEWAY TAG MODE |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | TAG1 | CUSTOM | | 1 | HOLDING REGISTER | 16BIT UNSIGNED | COM2 | 2 | GATEWAY |
| 2 | 2 | TAG2 | CUSTOM | | 2 | HOLDING REGISTER | 16BIT UNSIGNED | COM2 | 2 | GATEWAY |
| 3 | 3 | TAG3 | CUSTOM | | 3 | HOLDING REGISTER | 16BIT UNSIGNED | COM2 | 2 | GATEWAY |
| 4 | 4 | TAG4 | CUSTOM | | 1 | HOLDING REGISTER | 16BIT UNSIGNED | COM2 | 3 | BRIDGE |
| 5 | 5 | TAG5 | CUSTOM | | 2 | HOLDING REGISTER | 16BIT UNSIGNED | COM2 | 3 | BRIDGE |
| 6 | 6 | TAG6 | CUSTOM | | 3 | HOLDING REGISTER | 16BIT UNSIGNED | COM2 | 3 | BRIDGE |
| 7 | 7 | TAG7 | - | - | - | HOLDING REGISTER | 16BIT UNSIGNED | COM4 - SHARED | - | SHARED-MEMORY |
| 8 | 8 | TAG8 | - | - | - | HOLDING REGISTER | 16BIT UNSIGNED | COM4 - SHARED | - | SHARED-MEMORY |
| 9 | 9 | TAG9 | - | - | - | HOLDING REGISTER | 16BIT UNSIGNED | COM4 - SHARED | - | SHARED-MEMORY |
| 10 | 10 | TAG10 | - | - | - | HOLDING REGISTER | 32BIT UNSIGNED LSW | COM4 - SHARED | - | SHARED-MEMORY |
| 11 | 12 | TAG11 | - | - | - | HOLDING REGISTER | 32BIT UNSIGNED LSW | COM4 - SHARED | - | SHARED-MEMORY |

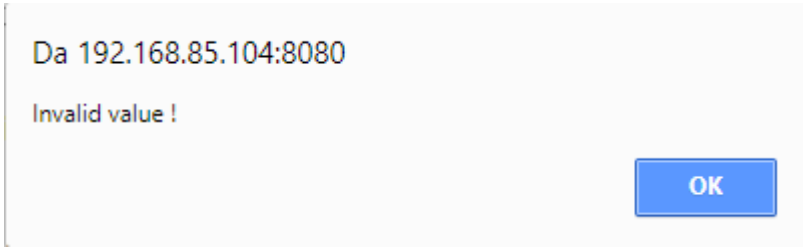
In the “Tag View” page, for each “HOLDING REGISTER” or “COIL” tag, a “CHANGE” button is present that lets you change the tag value; when clicking on this button, the following pop-up is shown:



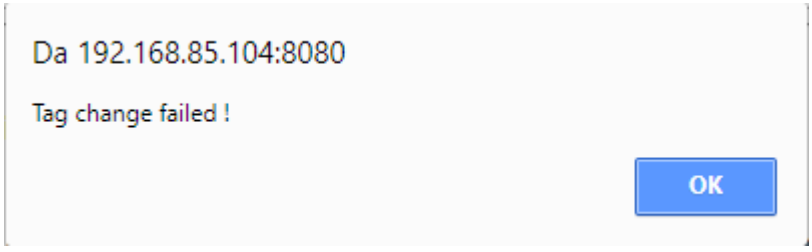

After changing the value in the text-box and clicking on the “OK” button, the following message is shown, if the tag value has been successfully changed.




If the given value does not fit the tag “Data Type”, the following message is shown:



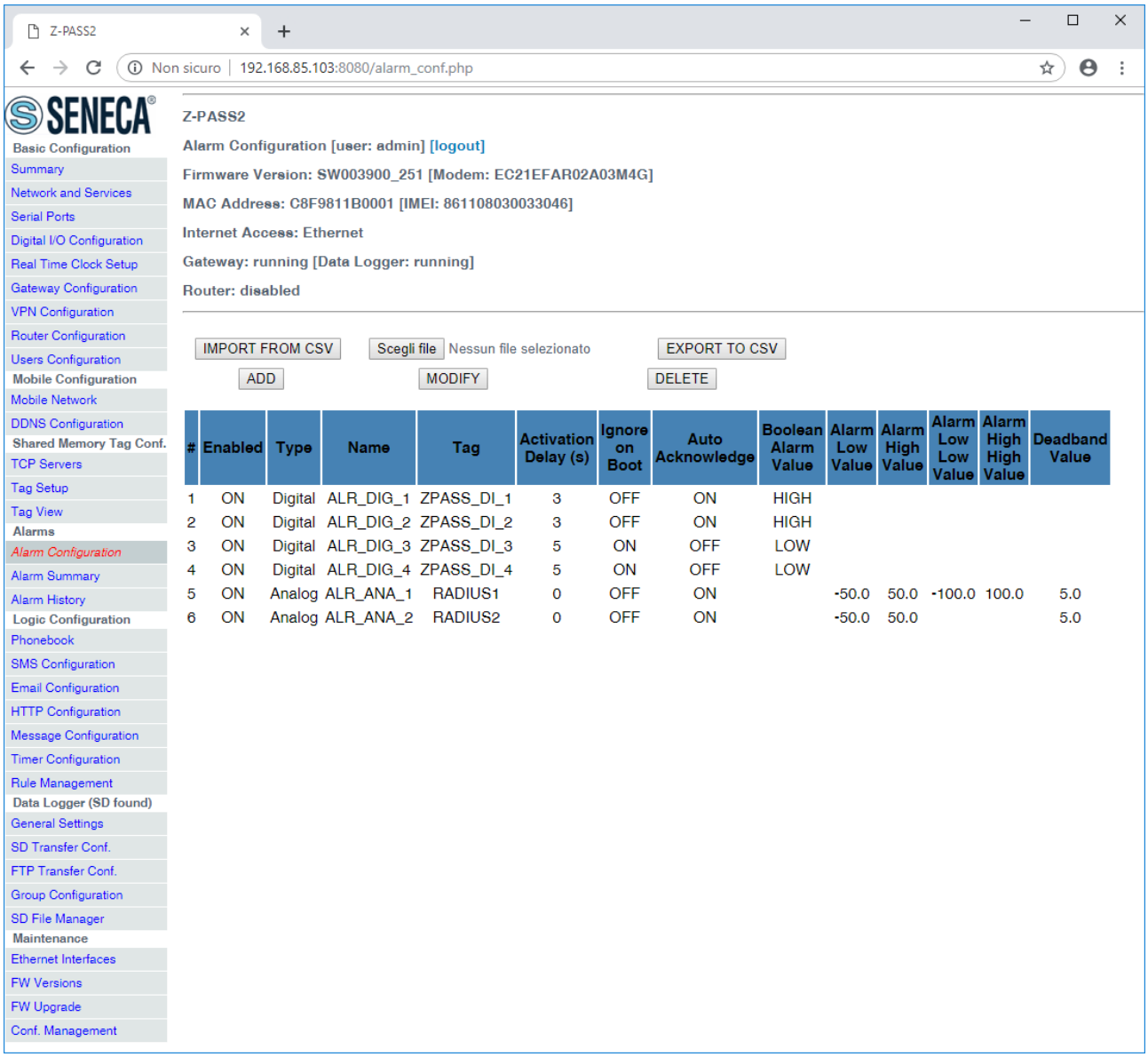

Finally, if the tag value could not be changed, the following message is shown:




## 20.4 Alarms

### 20.4.1 Alarm Configuration

By clicking on the “Alarm Configuration” link, in the “Alarms” section, you come to the following page:




In this page, the list of the configured alarms is shown.

By clicking on the “ADD” button, a new alarm can be configured, as in the following figure.


The following table explains the meaning of all the parameters available for an alarm.

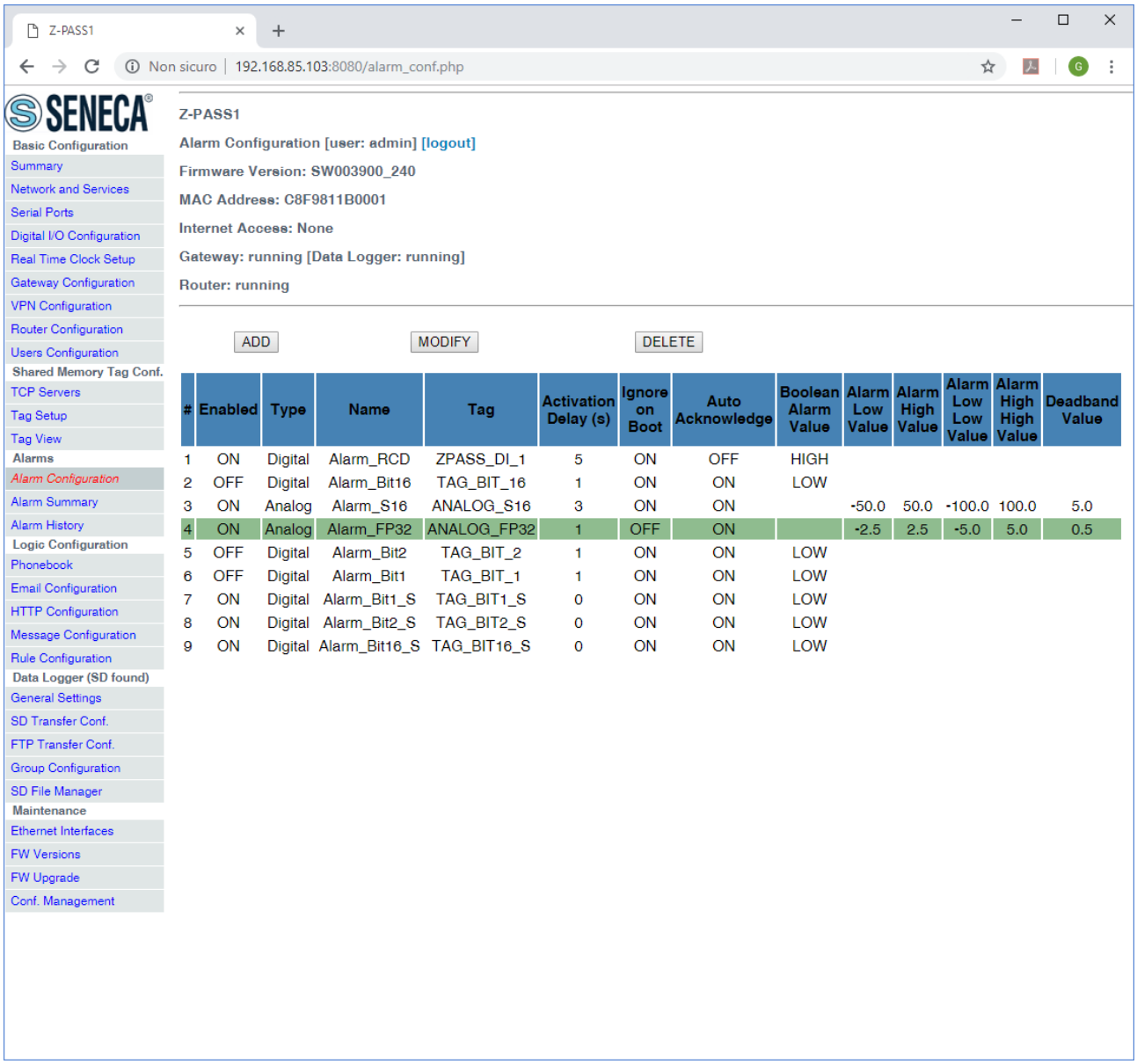
| Field | Meaning | Default value |
|---|---|---|
| Enabled | Flag to enable/disable the alarm | OFF |
| Type | This parameter tells if this is a Digital or Analog alarm; when changing the | Digital |

| | | |
|---|---|---|
| | type, some parameters become enabled or disabled | |
| Name | The alarm name; since this parameter is used as a key to identify the alarm, two alarms cannot be configured with the same name | *Empty* |
| Tag | The tag which the alarm is related to.<br>The tag list changes depending on the alarm type (Digital or Analog).<br>Only one alarm can be associated to a tag | *First tag in the list* |
| Activation Delays (s) | This parameter defines the time interval, in seconds, during which the alarm condition shall be kept true to generate the alarm | 0 |
| Ignore on Boot | This is a flag used to avoid generating the alarm, if the alarm condition is temporarily detected during the system boot | OFF |
| Auto Acknowledge | This is a flag used to avoid the need of an acknowledgment by the user to let the alarm be cancelled, after the alarm condition has ceased | ON |
| Boolean Alarm Value | For a Digital alarm, this parameter tells which is the tag value (LOW or HIGH) which corresponds to the alarm condition | HIGH |
| Alarm Low Value | For an Analog alarm, this parameter defines the low alarm threshold that is, when the tag value goes under this value, the alarm condition is entered | *Empty* |
| Alarm High Value | For an Analog alarm, this parameter defines the high alarm threshold that is, when the tag value goes over this value, the alarm condition is entered | *Empty* |
| Alarm Low Low Value | For an Analog alarm, this parameter defines the low danger alarm threshold that is, when the tag value | *Empty* |

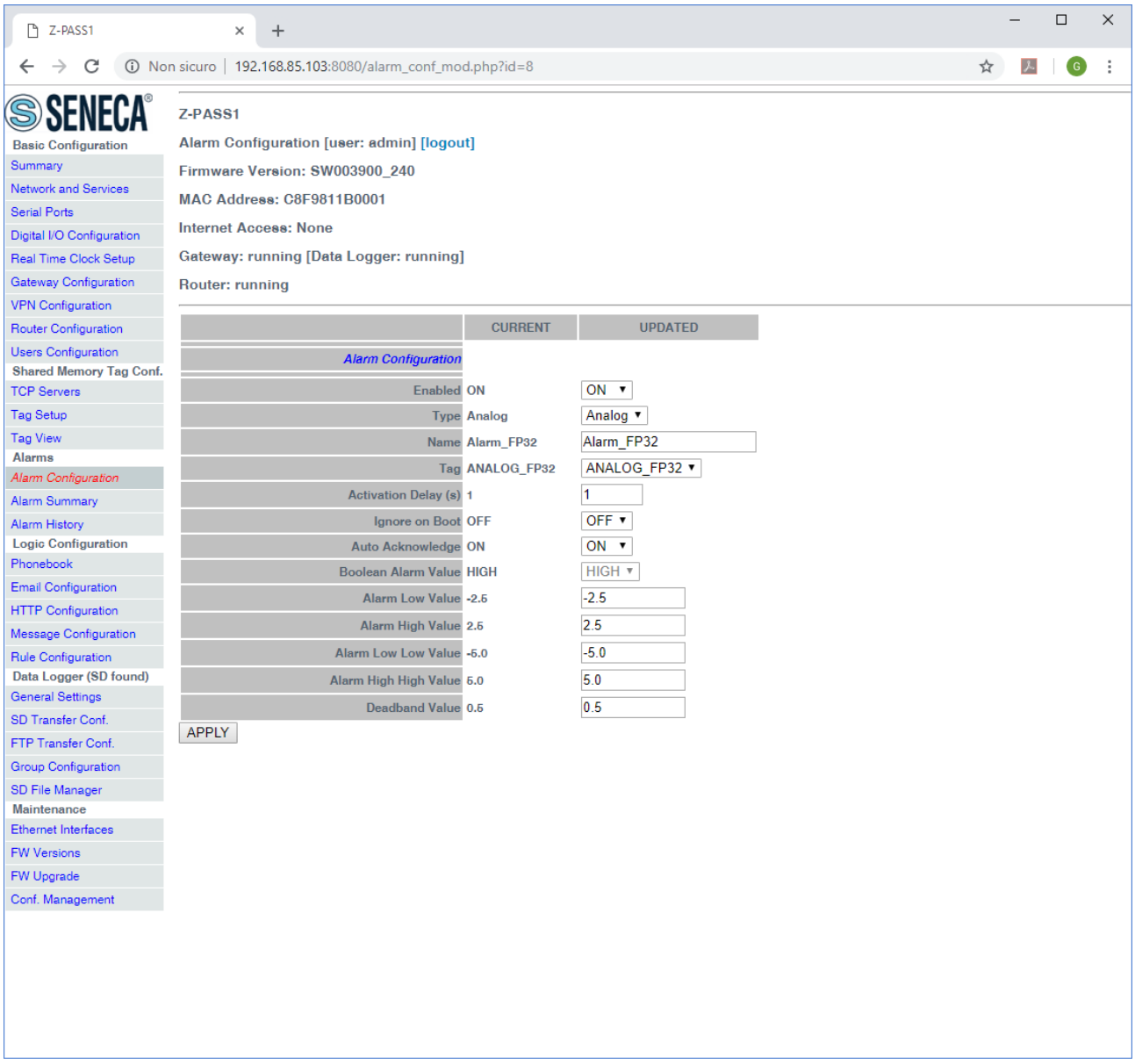
| | | |
|---|---|---|
| | goes under this value, the danger alarm condition is entered | |
| Alarm High High Value | For an Analog alarm, this parameter defines the high danger alarm threshold that is, when the tag value goes over this value, the danger alarm condition is entered | *Empty* |
| Deadband Value | This parameter defines a non negative value to be summed to the low threshold/subtracted from the high threshold, such that the tag value shall go over/under the resultant value to let the alarm condition be exited | 0 |

For an Analog alarm, at least one of the four threshold parameters (Alarm Low Value, Alarm High Value, Alarm Low Low Value, Alarm High High Value) shall be defined.

Selecting an alarm in the list and clicking on the “MODIFY” button, you can modify the alarm parameters, as in the following figures.




| # | Enabled | Type | Name | Tag | Activation Delay (s) | Ignore on Boot | Auto Acknowledge | Boolean Alarm Value | Alarm Low Value | Alarm High Value | Alarm Low Low Value | Alarm High High Value | Deadband Value |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ON | Digital | Alarm_RCD | ZPASS_DI_1 | 5 | ON | OFF | HIGH | | | | | |
| 2 | OFF | Digital | Alarm_Bit16 | TAG_BIT_16 | 1 | ON | ON | LOW | | | | | |
| 3 | ON | Analog | Alarm_S16 | ANALOG_S16 | 3 | ON | ON | | -50.0 | 50.0 | -100.0 | 100.0 | 5.0 |
| 4 | ON | Analog | Alarm_FP32 | ANALOG_FP32 | 1 | OFF | ON | | -2.5 | 2.5 | -5.0 | 5.0 | 0.5 |
| 5 | OFF | Digital | Alarm_Bit2 | TAG_BIT_2 | 1 | ON | ON | LOW | | | | | |
| 6 | OFF | Digital | Alarm_Bit1 | TAG_BIT_1 | 1 | ON | ON | LOW | | | | | |
| 7 | ON | Digital | Alarm_Bit1_S | TAG_BIT1_S | 0 | ON | ON | LOW | | | | | |
| 8 | ON | Digital | Alarm_Bit2_S | TAG_BIT2_S | 0 | ON | ON | LOW | | | | | |
| 9 | ON | Digital | Alarm_Bit16_S | TAG_BIT16_S | 0 | ON | ON | LOW | | | | | |




Selecting an alarm in the list and clicking on the “DELETE” button, you can delete an alarm.

The possible states of an alarm are explained in the following table.

| State | Level | Meaning |
|---|---|---|
| None | - | The tag has never entered the alarm condition |
| Alarm | Alarm | The digital tag has got the value defined by “Boolean Alarm Level” parameter |
| Alarm Low | Alarm | The analog tag has got a value that is under the one defined by “Alarm Low Value” parameter |
| Alarm High | Alarm | The analog tag has got a value that is over the one defined by “Alarm High Value” parameter |
| Alarm Low Low | Analog Danger Alarm | The analog tag has got a value that is under the one defined by “Alarm Low Low Value” parameter |

| | | |
|---|---|---|
| Alarm High High | Analog Danger Alarm | The analog tag has got a value that is over the one defined by “Alarm High High Value” parameter |
| Acknowledge | - | The alarm has been aknowledged (see page “Alarm Summary”) |
| Return | - | The tag has exited the alarm condition, but the alarm has not been acknowledged and the alarm has the parameter “Auto Acknowledge” set to OFF |
| End | - | The tag has exited the alarm condition and the alarm has been aknowledged or the alarm has the parameter “Auto Acknowledge” set to ON |

As already mentioned in the previous table, when exiting the alarm condition the alarm states can follow two different paths, depending on the value of the “Auto Acknowledge” parameter :

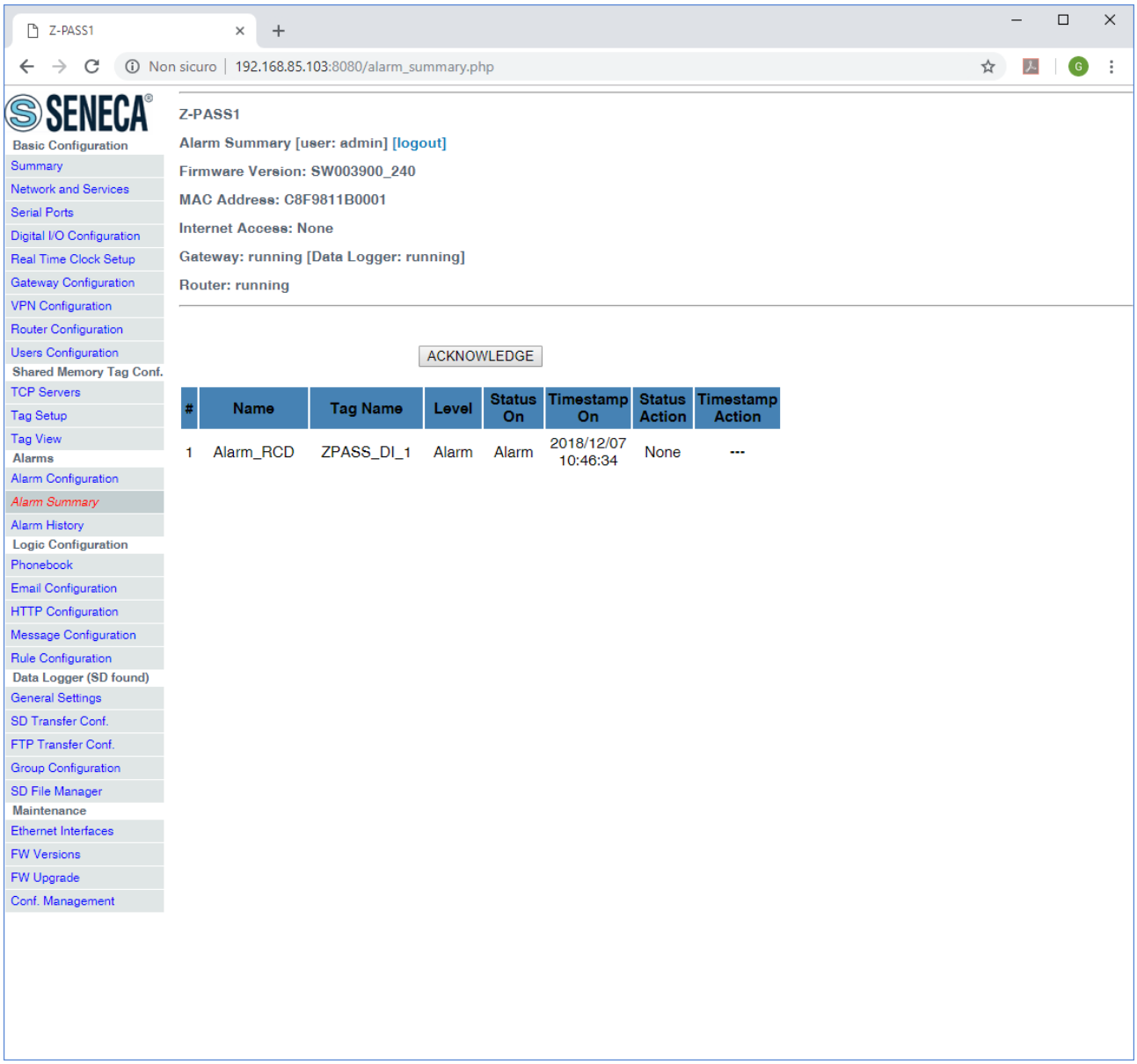
- Alarm* → Return → <acknowledgement> → End  if “Auto Acknowledge”=OFF
- Alarm* → End  if “Auto Acknowledge”=ON

The “EXPORT TO CSV” and “IMPORT FROM CSV” buttons let you export/import the alarm configuration to/from a “.csv” file (the separator character is “;”).

Please note that, when importing the alarm configuration from a .csv file, the previously existing alarms are deleted; so, a fast way to “clean” the alarm configuration, if it contains many entries, is to import an empty .csv file.

### *20.4.2 Alarm Summary*

By clicking on the “Alarm Summary” link, in the “Alarms” section, you come to the following page:




This page shows the alarms currently active in the system.

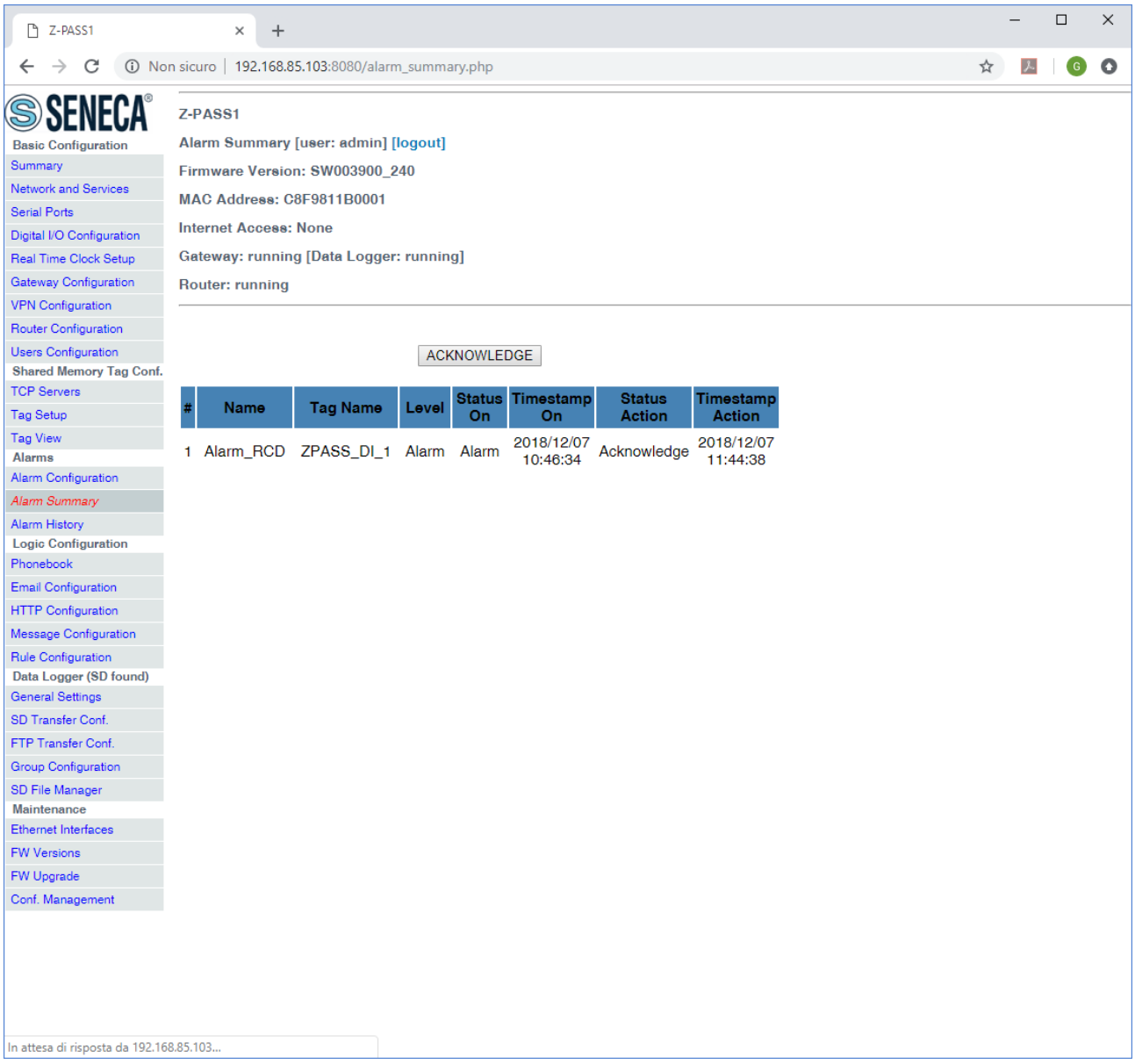
The following table explains the meaning of all the information given for an alarm.

| Field | Meaning |
|---|---|
| Name | The alarm name |
| Tag Name | The name of the tag which the alarm is related to |
| Level | Always “Alarm” for digital alarms<br>“Alarm” or “Analog Danger Alarm” for analog alarms |
| Status On | The alarm status when the alarm has been generated:<br>always “Alarm” for digital alarms<br>“Alarm Low” or “Alarm High” for analog alarms with Level = “Alarm”<br>“Alarm Low Low” or “Alarm High High” for analog alarms with Level = |

| | |
|---|---|
| | “Analog Danger Alarm” |
| Timestamp On | The timestamp corresponding to the alarm generation |
| Status Action | “None” when the alarm is generated<br>It may evolve in:<br>“Acknowledged”, if the alarm has been acknowledged when in the alarm state<br>“Return”, if the alarm state has been exited for an alarm with “Auto Acknowledge” = OFF |
| Timestamp Action | The timestamp corresponding to the acknowledgement action or alarm state evolution |

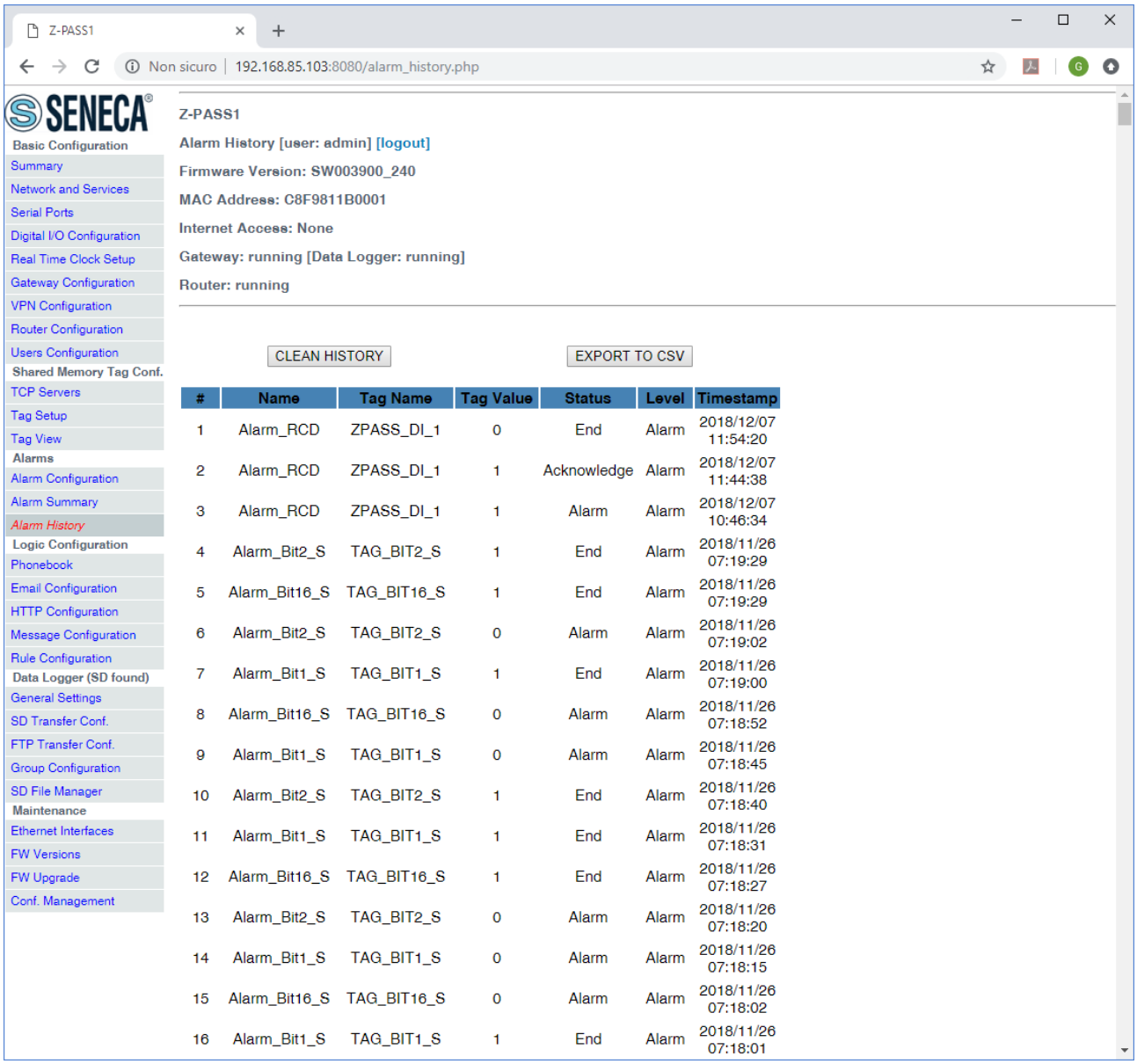
You can acknowledge an alarm by selecting it and clicking on the “ACKNOWLEDGE” button.

The row corresponding to the alarm changes as in the following figure.




### *20.4.3 Alarm History*

By clicking on the “Alarm History” link, in the “Alarms” section, you come to the following page:




| # | Name | Tag Name | Tag Value | Status | Level | Timestamp |
|---|---|---|---|---|---|---|
| 1 | Alarm_RCD | ZPASS_DI_1 | 0 | End | Alarm | 2018/12/07 11:54:20 |
| 2 | Alarm_RCD | ZPASS_DI_1 | 1 | Acknowledge | Alarm | 2018/12/07 11:44:38 |
| 3 | Alarm_RCD | ZPASS_DI_1 | 1 | Alarm | Alarm | 2018/12/07 10:46:34 |
| 4 | Alarm_Bit2_S | TAG_BIT2_S | 1 | End | Alarm | 2018/11/26 07:19:29 |
| 5 | Alarm_Bit16_S | TAG_BIT16_S | 1 | End | Alarm | 2018/11/26 07:19:29 |
| 6 | Alarm_Bit2_S | TAG_BIT2_S | 0 | Alarm | Alarm | 2018/11/26 07:19:02 |
| 7 | Alarm_Bit1_S | TAG_BIT1_S | 1 | End | Alarm | 2018/11/26 07:19:00 |
| 8 | Alarm_Bit16_S | TAG_BIT16_S | 0 | Alarm | Alarm | 2018/11/26 07:18:52 |
| 9 | Alarm_Bit1_S | TAG_BIT1_S | 0 | Alarm | Alarm | 2018/11/26 07:18:45 |
| 10 | Alarm_Bit2_S | TAG_BIT2_S | 1 | End | Alarm | 2018/11/26 07:18:40 |
| 11 | Alarm_Bit1_S | TAG_BIT1_S | 1 | End | Alarm | 2018/11/26 07:18:31 |
| 12 | Alarm_Bit16_S | TAG_BIT16_S | 1 | End | Alarm | 2018/11/26 07:18:27 |
| 13 | Alarm_Bit2_S | TAG_BIT2_S | 0 | Alarm | Alarm | 2018/11/26 07:18:20 |
| 14 | Alarm_Bit1_S | TAG_BIT1_S | 0 | Alarm | Alarm | 2018/11/26 07:18:15 |
| 15 | Alarm_Bit16_S | TAG_BIT16_S | 0 | Alarm | Alarm | 2018/11/26 07:18:02 |
| 16 | Alarm_Bit1_S | TAG_BIT1_S | 1 | End | Alarm | 2018/11/26 07:18:01 |

This page shows all alarm state transitions occurred in the system, up to a maximum of 1000; the alarm state transitions are given in reverse time order.

For example, the first three rows in the list show the state transitions for the alarm named “Alarm_RCD”, which is related to the tag named “ZPASS_DI_1”; this is a digital alarm, so its level can be only “Alarm”; the alarm has passed through the following states:

- “Alarm” when the alarm condition has been entered
- “Acknowledge” when the alarm has been acknowledged, in the “Alarm Summary” page
- “End” when the alarm condition has been exited

The “Tag Value” column gives the value of the tag corresponding to the alarm state transition.

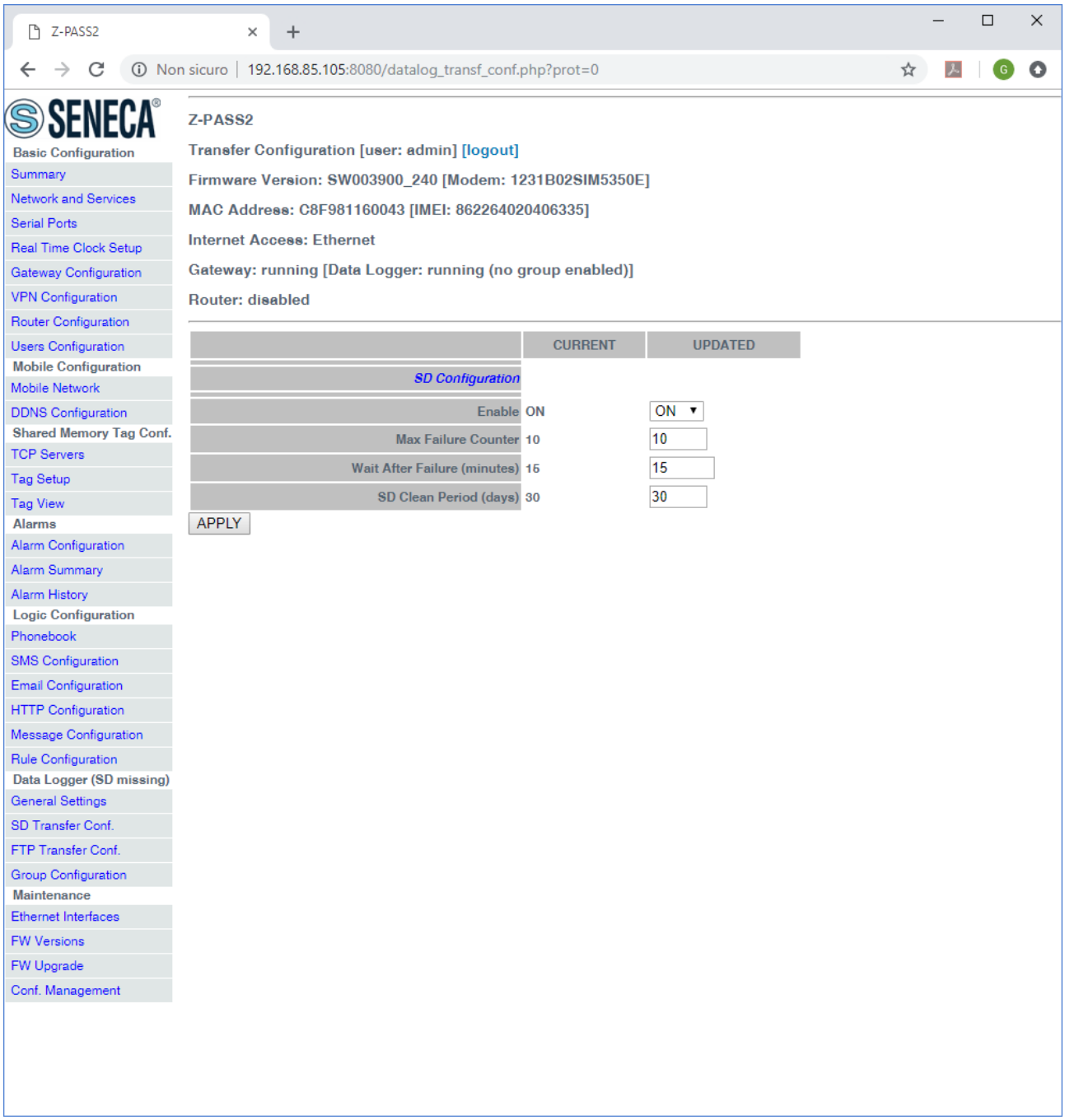
By clicking on the “CLEAN HISTORY” button, it’s possible to clean the whole alarm history.

By clicking on the “EXPORT TO CSV” button, it’s possible to export the alarm history to a “.csv” file (the separator character is “;”).

## 20.5 Client Protocols

### 20.5.1 SD Transfer Configuration

By clicking on the “SD Transfer Configuration” link, in the “Client Protocols” section, you come to the following page:




This page contains the parameters telling if log files are copied to the SD Card and how long they are kept, as explained in the following table.

| Field | Meaning | Default value |
|---|---|---|
| Enable | Flag telling if log files are copied to the SD Card or not | OFF |
| Max Failure Counter | This parameter defines the maximum number of failed copy attempts before entering the “Wait after failure” status | 10 |

| | | |
|---|---|---|
| | (see next field) | |
| Wait After Failure (minutes) | This parameter defines the duration, in minutes, of the "Wait after failure" status.<br>In this status, no further attempt to copy a log file to the SD Card is performed | 15 |
| SD Clean Period (days) | This parameter defines for how many days the log files shall be kept on the SD Card; that is, after the specified number of days, the log files are deleted | 30 |

On the SD card, log files are saved in directories with names having the following format:

*yyyymmdd* (yyyy=year, mm=month, dd=day)

e.g.:

*20180612*

Each of these directories contains one more subdirectories:

*logX* X=[1..4], group number

which in turn contain the log files of the corresponding group.

Log file names have the following format:

*Lmmmmmmm.csv*

where *mmmmmmm* is the number of minutes starting from the date/hour [1/1/2000 00:00], corresponding to the first line (sample) in the log file

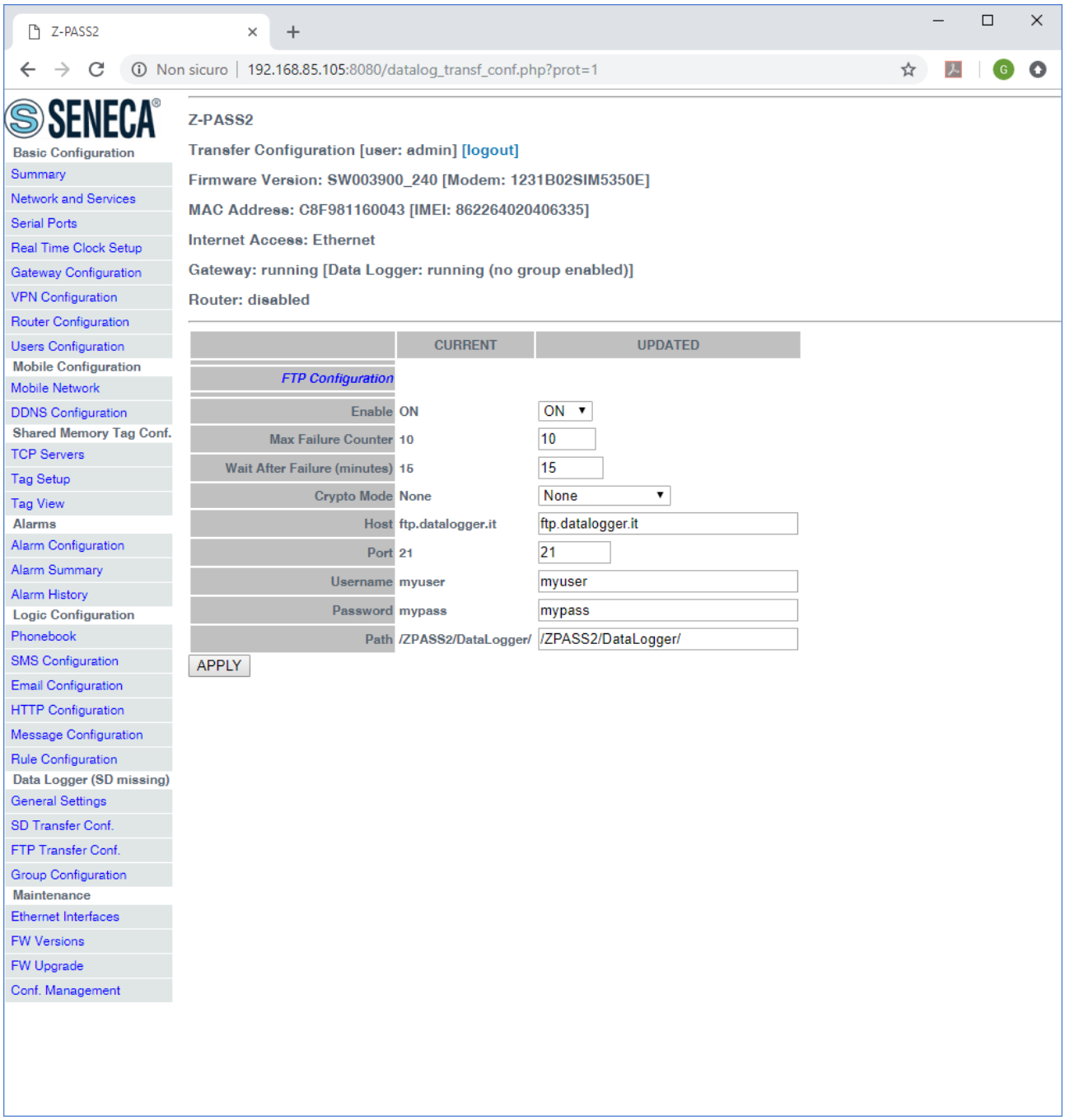
e.g.:

*L9701690.csv*

See also the "SD File Manager" [20.7.3] paragraph.

### *20.5.2 FTP Transfer Configuration*

By clicking on the "FTP Transfer Configuration" link, in the "Client Protocols" section, you come to the following page:




This page contains the parameters related to the transfer of log files via FTP, as explained in the following table.

| Field | Meaning | Default value |
|---|---|---|
| Enable | Flag telling if log files are transferred via FTP or not | OFF |
| Max Failure Counter | This parameter defines the maximum number of failed transfer attempts before entering the “Wait after failure” | 10 |

| | | |
|---|---|---|
| | status (see next field) | |
| Wait After Failure (minutes) | This parameter defines the duration, in minutes, of the "Wait after failure" status.<br>In this status, no further attempt to transfer a log file via FTP is performed | 15 |
| Crypto Mode | This parameter defines the encryption mode of the FTP connection.<br>Possible modes are:<br>- None<br>- TLS/SSL Implicit<br>- TLS/SSL Explicit | None |
| Host | Hostname (FQDN) or IP address of the FTP server | empty |
| Port | FTP server (TCP) port | 21 |
| Username | Username to access the FTP server | empty |
| Password | Password to access the FTP server | empty |
| Path | Path of the directory, on the FTP server, where the log files shall be saved | empty |

Log files transferred via FTP have names with the following format:

*<RTU_Name>_X_log<date_time>.csv*

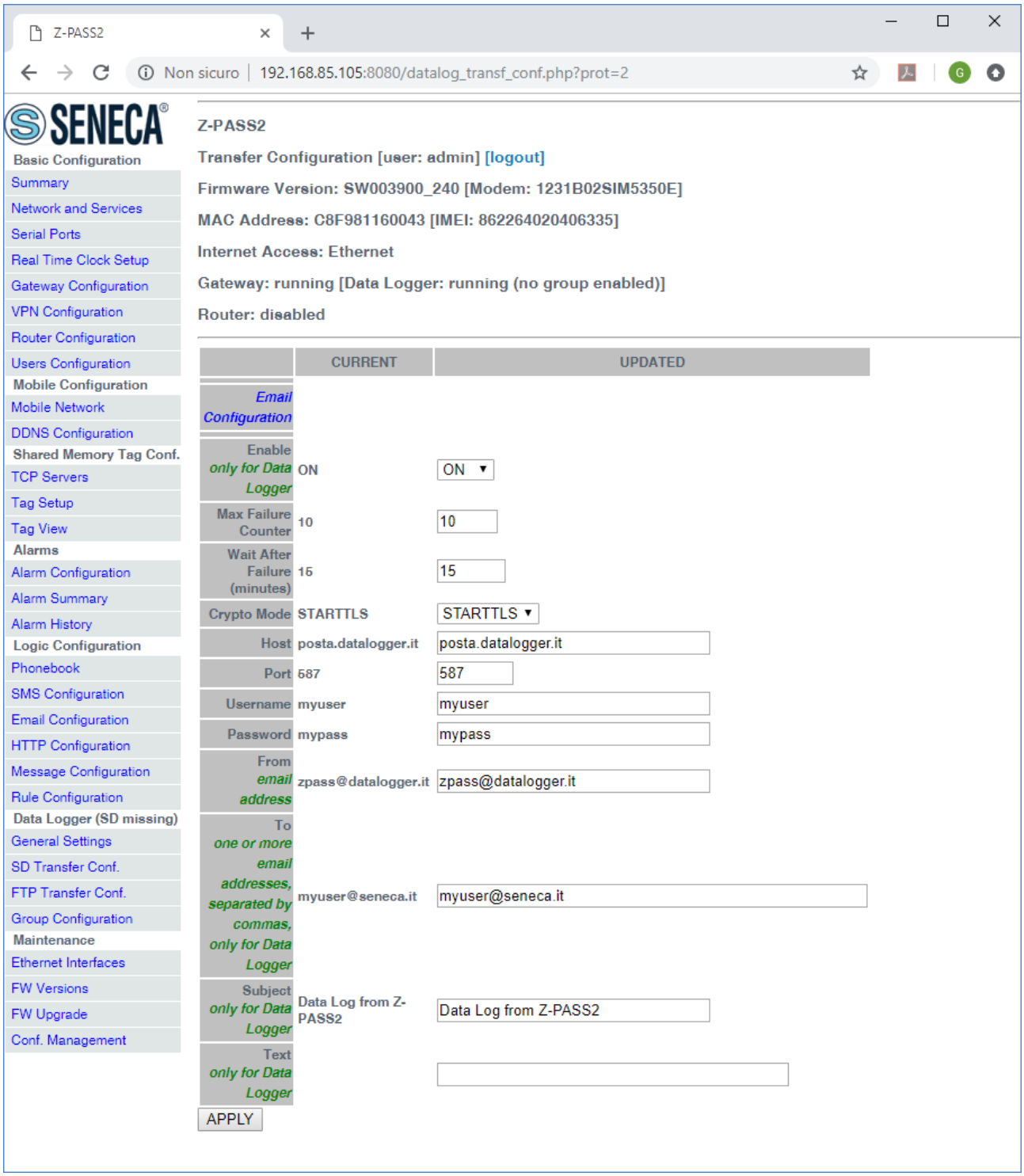
where:
- *<RTU_Name>* is the value of "RTU Name" parameter in "General Settings" page
- *X=[1..4]* is the group number
- *<date_time>* has the format *yyyymmdd* (yyyy=year, mm=month, dd=day); this is the timestamp of the first sample (line) in the log file

e.g.:

`Z-PASS_1_log20180507101507.csv`

### *20.5.3 Email Configuration*

By clicking on the "Email Configuration" link, in the "Client Protocols" section, you come to the following page:




In Z-PASS, emails can be used to transfer data log files or to send alarms; some parameters in this page are used only when transferring data log files, not when sending alarms; these parameters are marked with the “only for Data Logger” caption.

All parameters are explained in the following table.

| Field | Meaning | Default value |
|---|---|---|
| Enable | Flag telling if log files are transferred via EMAIL or not<br>Conversely, alarms can be sent via EMAIL even if this parameter is set to OFF, provided that the other parameters are correctly set | OFF |
| Max Failure Counter | This parameter defines the maximum number of failed attempts before entering the "Wait after failure" status (see next field) | 10 |
| Wait After Failure (minutes) | This parameter defines the duration, in minutes, of the "Wait after failure" status.<br>In this status, no further attempt to send a log file or an alarm via EMAIL is performed | 15 |
| Crypto Mode | This parameter defines the encryption mode of the EMAIL connection.<br>Possible modes are:<br>- None<br>- TLS/SSL<br>- STARTTLS | None |
| Host | Hostname (FQDN) or IP address of the EMAIL server | empty |
| Port | EMAIL server (TCP) port | 25 |
| Username | Username to access the EMAIL server | empty |
| Password | Password to access the EMAIL server | empty |
| From | Email sender address | empty |
| To | List of one or more email recipient addresses, separated by commas<br>This parameter is used only for log files transfer | empty |
| Subject | Email subject<br>This parameter is used only for log files transfer | empty |
| Text | Email text; if left empty, the text "This is a mail from Z-PASS2 [or Z-PASS1]" is sent<br>This parameter is used only for log | empty |

| | | |
|---|---|---|
| | files transfer | |

Log files sent as EMAIL attachments have names with the following format:

*<RTU_Name>_X_log<date_time>.csv*

where:
- *<RTU_Name>* is the value of “RTU Name” parameter in “General Settings” page
- *X=[1..4]* is the group number
- *<date_time>* has the format *yyyymmdd* (yyyy=year, mm=month, dd=day); this is the timestamp of the first sample (line) in the log file

e.g.:

*Z-PASS_1_log20180507101507.csv*

Emails carrying alarms have the following text format:

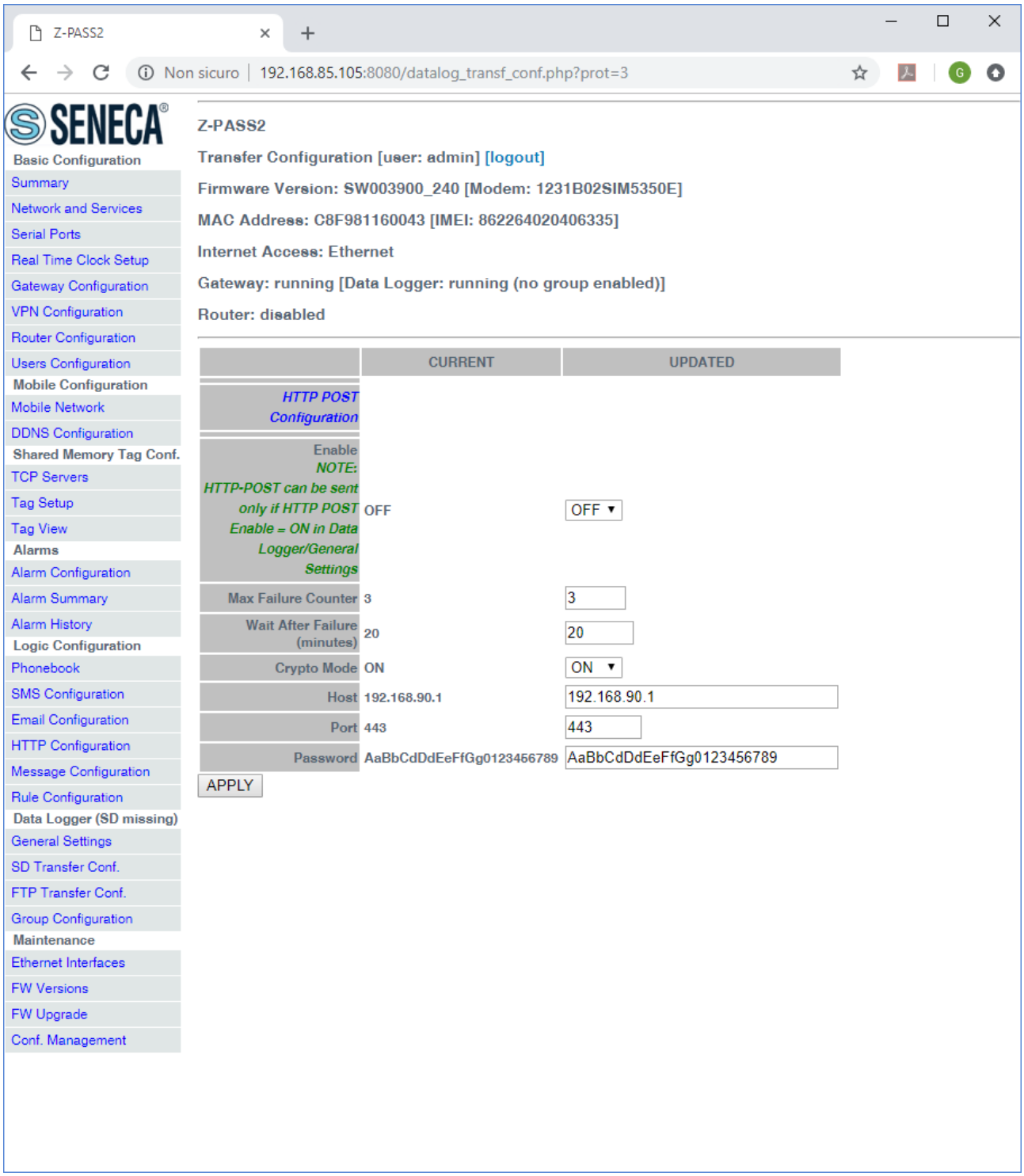
```
MESSAGE:<timestamp>
<rtu name> <message text>
```

with the following subject:

```
<rtu name>:ALARM
```

### *20.5.4 HTTP Configuration*

By clicking on the “HTTP Configuration” link, in the “Client Protocols” section, you come to the following page:




In Z-PASS, HTTP POSTs can be used to send log samples or alarms (events).

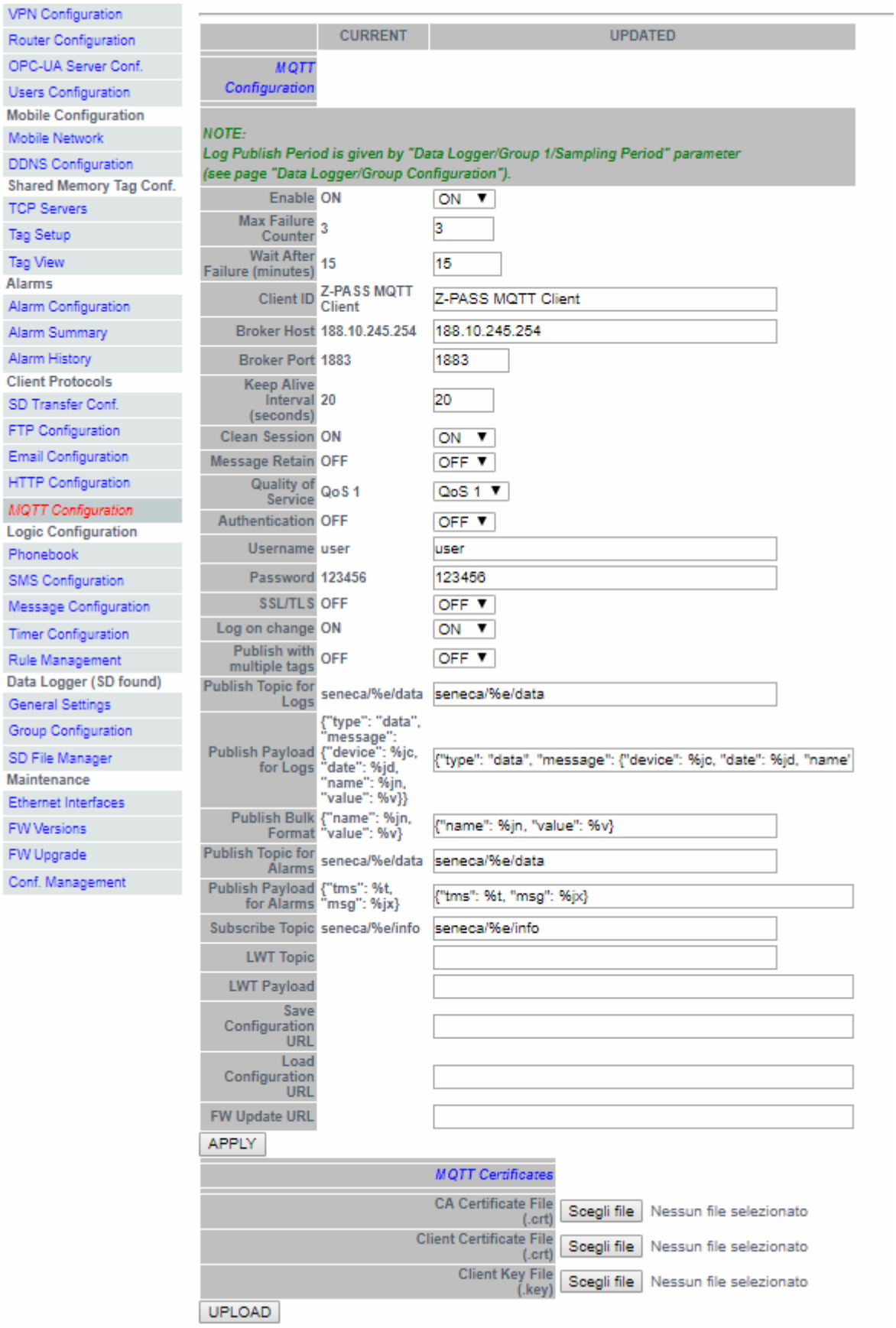
All parameters are explained in the following table.

| Field | Meaning | Default value |
|---|---|---|
| Enable | Flag telling if log samples/events are | OFF |

| | | |
|---|---|---|
| | sent via HTTP POST requests or not | |
| Max Failure Counter | This parameter defines the maximum number of failed attempts before entering the "Wait after failure" status (see next field) | 10 |
| Wait After Failure (minutes) | This parameter defines the duration, in minutes, of the "Wait after failure" status.<br>In this status, no further attempt to send a log sample via HTTP POST request is performed | 15 |
| Crypto Mode | This parameter defines the encryption mode of the HTTP connection.<br>Possible modes are:<br>- OFF (HTTP)<br>- ON (HTTPS) | ON |
| Host | Hostname (FQDN) or IP address of the HTTP server | 192.168.90.1 |
| Port | HTTP server (TCP) port | 443 |
| Password | Password to access the HTTP server | AaBbCdDdEeFfGg0123456789 |

### *20.5.5 MQTT Configuration*

By clicking on the "MQTT Configuration" link, in the "Client Protocols" section, you come to the following page:


VPN Configuration
Router Configuration
OPC-UA Server Conf.
Users Configuration
Mobile Configuration
Mobile Network
DDNS Configuration
Shared Memory Tag Conf.
TCP Servers
Tag Setup
Tag View
Alarms
Alarm Configuration
Alarm Summary
Alarm History
Client Protocols
SD Transfer Conf.
FTP Configuration
Email Configuration
HTTP Configuration
MQTT Configuration
Logic Configuration
Phonebook
SMS Configuration
Message Configuration
Timer Configuration
Rule Management
Data Logger (SD found)
General Settings
Group Configuration
SD File Manager
Maintenance
Ethernet Interfaces
FW Versions
FW Upgrade
Conf. Management
CURRENT
UPDATED
MQTT Configuration
NOTE:
Log Publish Period is given by "Data Logger/Group 1/Sampling Period" parameter
(see page "Data Logger/Group Configuration").
Enable ON ON
Max Failure Counter 3 3
Wait After Failure (minutes) 15 15
Client ID Z-PASS MQTT Client Z-PASS MQTT Client
Broker Host 188.10.245.254 188.10.245.254
Broker Port 1883 1883
Keep Alive Interval (seconds) 20 20
Clean Session ON ON
Message Retain OFF OFF
Quality of Service QoS 1 QoS 1
Authentication OFF OFF
Username user user
Password 123456 123456
SSL/TLS OFF OFF
Log on change ON ON
Publish with multiple tags OFF OFF
Publish Topic for Logs seneca/%e/data seneca/%e/data
Publish Payload for Logs {"type": "data", "message": {"device": %jc, "date": %jd, "name": %jn, "value": %v}} {"type": "data", "message": {"device": %jc, "date": %jd, "name"
Publish Bulk Format {"name": %jn, "value": %v} {"name": %jn, "value": %v}
Publish Topic for Alarms seneca/%e/data seneca/%e/data
Publish Payload for Alarms {"tms": %t, "msg": %jx} {"tms": %t, "msg": %jx}
Subscribe Topic seneca/%e/info seneca/%e/info
LWT Topic
LWT Payload
Save Configuration URL
Load Configuration URL
FW Update URL
APPLY
MQTT Certificates
CA Certificate File (.crt) Scegli file Nessun file selezionato
Client Certificate File (.crt) Scegli file Nessun file selezionato
Client Key File (.key) Scegli file Nessun file selezionato
UPLOAD

In Z-PASS, MQTT protocol can be used to send (and receive) data or events to a cloud (called broker).

All parameters are explained in the following table.

| Field | Meaning | Default value |
|---|---|---|
| Enable | Flag telling if data/events are sent/receive via MQTT protocol or not | OFF |
| Max Failure Counter | This parameter defines the maximum number of failed attempts before entering the "Wait after failure" status (see next field) | 3 |
| Wait After Failure (minutes) | This parameter defines the duration, in minutes, of the "Wait after failure" status.<br>In this status, no further attempt to send or receive MQTT data is performed | 15 |
| Client ID | This parameter defines the Client ID used in the MQTT protocol | Z-PASS MQTT Client |
| Broker Host | This parameter defines the Broker Host name or address | 192.168.90.1 |
| Broker Port | This parameter defines the Broker Port | 1883 |
| Keep Alive Interval (seconds) | This parameter defines the Keep alive: ensures that the connection between the broker and client is still open and that the broker and the client are aware of being connected. When the client establishes a connection to the broker, the client communicates a time interval in seconds to the broker. This interval defines the maximum length of time that the broker and client may not communicate with each other | 20 |
| Clean Session | This parameter defines the clean session.<br>When the clean session flag is set to true, the client does not want a persistent session. If the client disconnects for any reason, all | ON |

| | | |
|---|---|---|
| | information and messages that are queued from a previous persistent session are lost. | |
| Message Retain | This parameter defines the message retain. Normally if a publisher publishes a message to a topic, and no one is subscribed to that topic the message is simply discarded by the broker. However the publisher can tell the broker to keep the last message on that topic by setting theretained message flag. | OFF |
| Quality of service | This parameter defines the quality of service for the MQTT protocol.<br>Can be selected from<br>QOS 0 (only once, without ack)<br>QOS 1 (At Least Once, with ack)<br>QOS 2 (Only Once, with ack and resend) | QOS 1 |
| Authentication | This parameter defines if must be used the authentication with user/password for access to the broker | OFF |
| Username | Username for atuthentication (only if authentication is ON) | - |
| Password | Password for atuthentication (only if authentication is ON) | |
| SSL/TLS | This parameter defines if the communication is encrypted with SSL/TLS | OFF |
| Log on Change | This parameter defines if topics must be sent only on change (according to minimum datalog time) or not. | ON |
| Publish with multiple tags | This parameter defines if the publish contains multiple tags or if the device must send a publish for each tag. | ON |
| Publish Topic for Logs | Select the topic name for logs data using the following legenda:<br>%c Z-PASS Client ID<br>%m Z-PASS MAC Address<br>%e Z-PASS IMEI | seneca/%c/data |

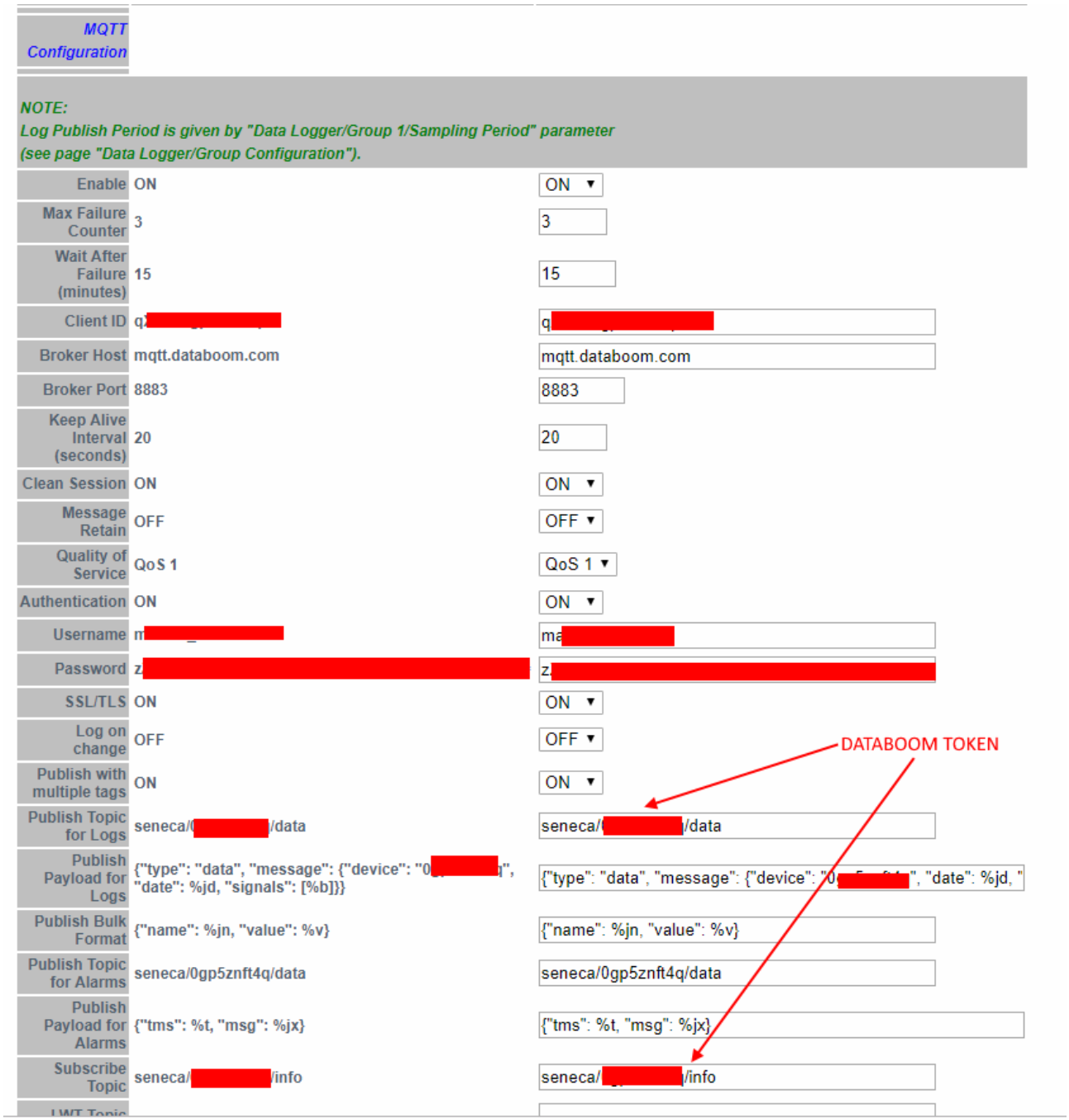
| | | |
|---|---|---|
| | %d: date-time<br>%t: timestamp (number of seconds since the "epoch")<br>%x: text (only in "Publish Payload for Alarms")<br>%b: bulk (format specified in "Publish Bulk Format" parameter)<br>%n: tag name (only in "Publish Bulk Format")<br>%v: tag value (only in "Publish Bulk Format")<br>%i: tag validity flag (only in "Publish Bulk Format")<br>%j[field]: print [field] as a JSON string<br>%$tag_name$: value of tag "tag_name"<br>%#tag_name#: validity flag of tag "tag_name" | |
| Publish Payload for Logs | Select the format that must be used for the publish payload in Json format using the following legenda:<br>%c: Z-PASS Client ID<br>%m: Z-PASS MAC Address<br>%e: Z-PASS IMEI<br>%d: date-time<br>%t: timestamp (number of seconds since the "epoch")<br>%x: text (only in "Publish Payload for Alarms")<br>%b: bulk (format specified in "Publish Bulk Format" parameter)<br>%n: tag name (only in "Publish Bulk Format")<br>%v: tag value (only in "Publish Bulk Format")<br>%i: tag validity flag (only in "Publish Bulk Format")<br>%j[field]: print [field] as a JSON string<br>%$tag_name$: value of tag "tag_name"<br>%#tag_name#: validity flag of tag | {"type": "data", "message": {"device": %jc, "date": %jd, "name": %jn, "value": %v}} |

<table>
<tr><td></td><td><table><tr><td></td><td>"tag_name"</td></tr></table></td><td></td></tr>
<tr><td>Publish Bulk Format</td><td>Select the format for the bulk mode using the following legenda:<table><tr><td>%c</td><td>Z-PASS Client ID</td></tr><tr><td>%m</td><td>Z-PASS MAC Address</td></tr><tr><td>%e</td><td>Z-PASS IMEI</td></tr><tr><td>%d</td><td>date-time</td></tr><tr><td>%t</td><td>timestamp (number of seconds since the "epoch")</td></tr><tr><td>%x</td><td>text (only in "Publish Payload for Alarms")</td></tr><tr><td>%b</td><td>bulk (format specified in "Publish Bulk Format" parameter)</td></tr><tr><td>%n</td><td>tag name (only in "Publish Bulk Format")</td></tr><tr><td>%v</td><td>tag value (only in "Publish Bulk Format")</td></tr><tr><td>%i</td><td>tag validity flag (only in "Publish Bulk Format")</td></tr><tr><td>%j[field]</td><td>print [field] as a JSON string</td></tr><tr><td>%$tag_name$</td><td>value of tag "tag_name"</td></tr><tr><td>%#tag_name#</td><td>validity flag of tag "tag_name"</td></tr></table></td><td>{"name": %jn, "value": %v}</td></tr>
<tr><td>Publish Topic for Alarms</td><td>Select the topic name for Alarms using the following legenda:<table><tr><td>%c</td><td>Z-PASS Client ID</td></tr><tr><td>%m</td><td>Z-PASS MAC Address</td></tr><tr><td>%e</td><td>Z-PASS IMEI</td></tr><tr><td>%d</td><td>date-time</td></tr><tr><td>%t</td><td>timestamp (number of seconds since the "epoch")</td></tr><tr><td>%x</td><td>text (only in "Publish Payload for Alarms")</td></tr><tr><td>%b</td><td>bulk (format specified in "Publish Bulk Format" parameter)</td></tr><tr><td>%n</td><td>tag name (only in "Publish Bulk Format")</td></tr><tr><td>%v</td><td>tag value (only in "Publish Bulk Format")</td></tr><tr><td>%i</td><td>tag validity flag (only in</td></tr></table></td><td>seneca/%c/data</td></tr>
</table>

<table>
<tr><td></td><td><table>
<tr><td></td><td>"Publish Bulk Format")</td></tr>
<tr><td>%j[field]</td><td>print [field] as a JSON string</td></tr>
<tr><td>%$tag_name$</td><td>value of tag "tag_name"</td></tr>
<tr><td>%#tag_name#</td><td>validity flag of tag "tag_name"</td></tr>
</table></td><td></td></tr>
<tr><td>Subscribe Topic</td><td>Select the subscribe topic using the following legenda:<table>
<tr><td>%c</td><td>Z-PASS Client ID</td></tr>
<tr><td>%m</td><td>Z-PASS MAC Address</td></tr>
<tr><td>%e</td><td>Z-PASS IMEI</td></tr>
<tr><td>%d</td><td>date-time</td></tr>
<tr><td>%t</td><td>timestamp (number of seconds since the "epoch")</td></tr>
<tr><td>%x</td><td>text (only in "Publish Payload for Alarms")</td></tr>
<tr><td>%b</td><td>bulk (format specified in "Publish Bulk Format" parameter)</td></tr>
<tr><td>%n</td><td>tag name (only in "Publish Bulk Format")</td></tr>
<tr><td>%v</td><td>tag value (only in "Publish Bulk Format")</td></tr>
<tr><td>%i</td><td>tag validity flag (only in "Publish Bulk Format")</td></tr>
<tr><td>%j[field]</td><td>print [field] as a JSON string</td></tr>
<tr><td>%$tag_name$</td><td>value of tag "tag_name"</td></tr>
<tr><td>%#tag_name#</td><td>validity flag of tag "tag_name"</td></tr>
</table></td><td>seneca/%c/info</td></tr>
<tr><td>LWT Topic</td><td>Select the Last Weel and Testament topic using the following legenda:<table>
<tr><td>%c</td><td>Z-PASS Client ID</td></tr>
<tr><td>%m</td><td>Z-PASS MAC Address</td></tr>
<tr><td>%e</td><td>Z-PASS IMEI</td></tr>
<tr><td>%d</td><td>date-time</td></tr>
<tr><td>%t</td><td>timestamp (number of seconds since the "epoch")</td></tr>
<tr><td>%x</td><td>text (only in "Publish Payload for Alarms")</td></tr>
</table></td><td>-</td></tr>
</table>

| | | |
|---|---|---|
| | <table><tr><td>%b</td><td>bulk (format specified in "Publish Bulk Format" parameter)</td></tr><tr><td>%n</td><td>tag name (only in "Publish Bulk Format")</td></tr><tr><td>%v</td><td>tag value (only in "Publish Bulk Format")</td></tr><tr><td>%i</td><td>tag validity flag (only in "Publish Bulk Format")</td></tr><tr><td>%j[field]</td><td>print [field] as a JSON string</td></tr><tr><td>%$tag_name$</td><td>value of tag "tag_name"</td></tr><tr><td>%#tag_name#</td><td>validity flag of tag "tag_name"</td></tr></table> | |
| LWT Payload | Select the Last Weel and Testament payload. | - |
| Save Configuration URL | The URL for the “Save Configuration” command received from MQTT | |
| Load Configuration URL | The URL for the “Load Configuration” command received from MQTT | |
| FW Update URL | The URL for the “FW Update” command received from MQTT | |
| Sleep Timeout | Wake-up time of the MQTT task, the shorter it is, the more reactive MQTT is (at the expense of a higher cpu load) | |
| MQTT Certificates | Used for load the certificates that can be used with the SSL/TLS encryption. | |

#### *20.5.5.1 MQTT Example configuration for Databoom.com*




Then you must add the Databoom certificates.

### *20.5.5.2 MQTT Example configuration for Amazon AWS*

Internet Access: Ethernet

Gateway: running [Data Logger: running (no group enabled)]

Router: running

| | CURRENT | UPDATED |
|---|---|---|
| *MQTT Configuration* | | |
| *NOTE: Log Publish Period is given by "Data Logger/Group 1/Sampling Period" parameter (see page "Data Logger/Group Configuration").* | | |
| Enable | ON | ON |
| Max Failure Counter | 3 | 3 |
| Wait After Failure (minutes) | 15 | 15 |
| Client ID | Any | Any |
| Broker Host | [redacted]nazonaws.com | a[redacted]azonaws. |
| Broker Port | 8883 | 8883 |
| Keep Alive Interval (seconds) | 20 | 20 |
| Clean Session | ON | ON |
| Message Retain | OFF | OFF |
| Quality of Service | QoS 1 | QoS 1 |
| Authentication | ON | ON |
| Username | [redacted] | [redacted] |
| Password | [redacted] | [redacted] |
| SSL/TLS | ON | ON |
| Log on change | OFF | OFF |
| Publish with multiple tags | ON | ON |
| Publish Topic for Logs | $aws/things/ZUMTS/shadow/update | $aws/things/ZUMTS/shadow/update |
| Publish Payload for Logs | {"state": {"reported": {"ZPASS_DI": %$ZPASS_DI$, "ZPASS_DO": %$ZPASS_DO$}}, "clientToken": "a[redacted]"} | {"state": {"reported": {"ZPASS_DI": %$ZPASS_DI$, "ZPAS |
| Publish Bulk Format | $aws/things/ZUMTS/shadow/update/accepted | $aws/things/ZUMTS/shadow/update/accepted |
| Publish Topic for Alarms | seneca/%c/events | seneca/%c/events |
| Publish Payload for Alarms | {"tms": %t, "msg": %jx} | {"tms": %t, "msg": %jx} |
| Subscribe Topic | $aws/things/ZUMTS/shadow/update/accepted | $aws/things/ZUMTS/shadow/update/accepted |
| LWT Topic | seneca/%c/lastwill | seneca/%c/lastwill |
| LWT Payload | Z-PASS has gone with the wind ! | Z-PASS has gone with the wind ! |
| Save Configuration URL | | |

Then you must add the AWS certificates.

### 20.5.6 Write a TAG(s) from MQTT

For write a single tag (for example ZPASS_DO_4 to value “1”) from MQTT use:

```
seneca/Z-PASS MQTT Client/info/ZPASS_DO_4
{"val": 1}
```

### 20.5.7 Write multiple TAGs from MQTT

For write multiple tags from MQTT use:

```
seneca/Z-PASS MQTT Client/info
{"tags": [{"ZPASS_DO_4": 1}]}
{"tags": [{"ZPASS_DO_2": 1}, {"ZPASS_DO_4": 0}]}
{"tags": [{"SHM_S16": -113}, {"SHM_FP": 0.7564}]}
{"tags": [{"SHM_U16": 69}, {"SHM_FP": -1.3291}]}
```

### 20.5.8 Send a command from MQTT

For send a command from MQTT use:

```
seneca/Z-PASS MQTT Client/info/act
{"act": 1}
This command will do a “RESET”

Other commands are:
RESET          = 1
CONF_SET       = 2
CONF_GET       = 3
FW_UPDATE      = 4
VPN_PPP_ON     = 5
VPN_ON         = 6
```

```
VPN_OFF         = 7

VPN_CUSTOM_ON   = 8

VPN_CUSTOM_OFF = 9

DL_CLEAN_LOGS   = 10
```

## 20.6 Logic Configuration

The logic configuration can be used to create programs that run in the gateway.

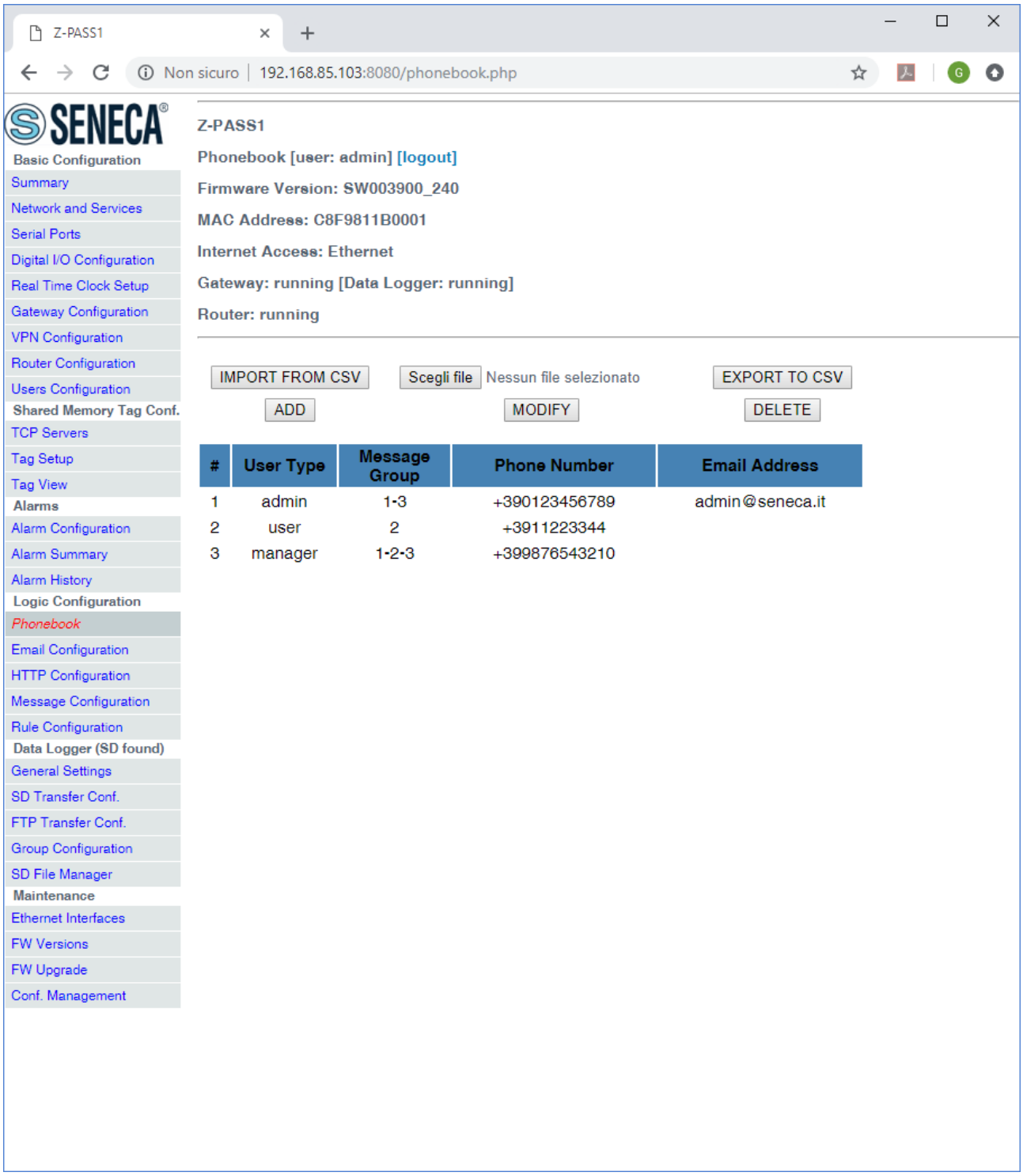
If you need to send text messages by SMS, EMAIL or HTTP, you have first to setup the corresponding configuration. After that the Rule configuration is used to write the program.

Up to 2000 rules can be written.

The rules are executed from top to down and from left to right.

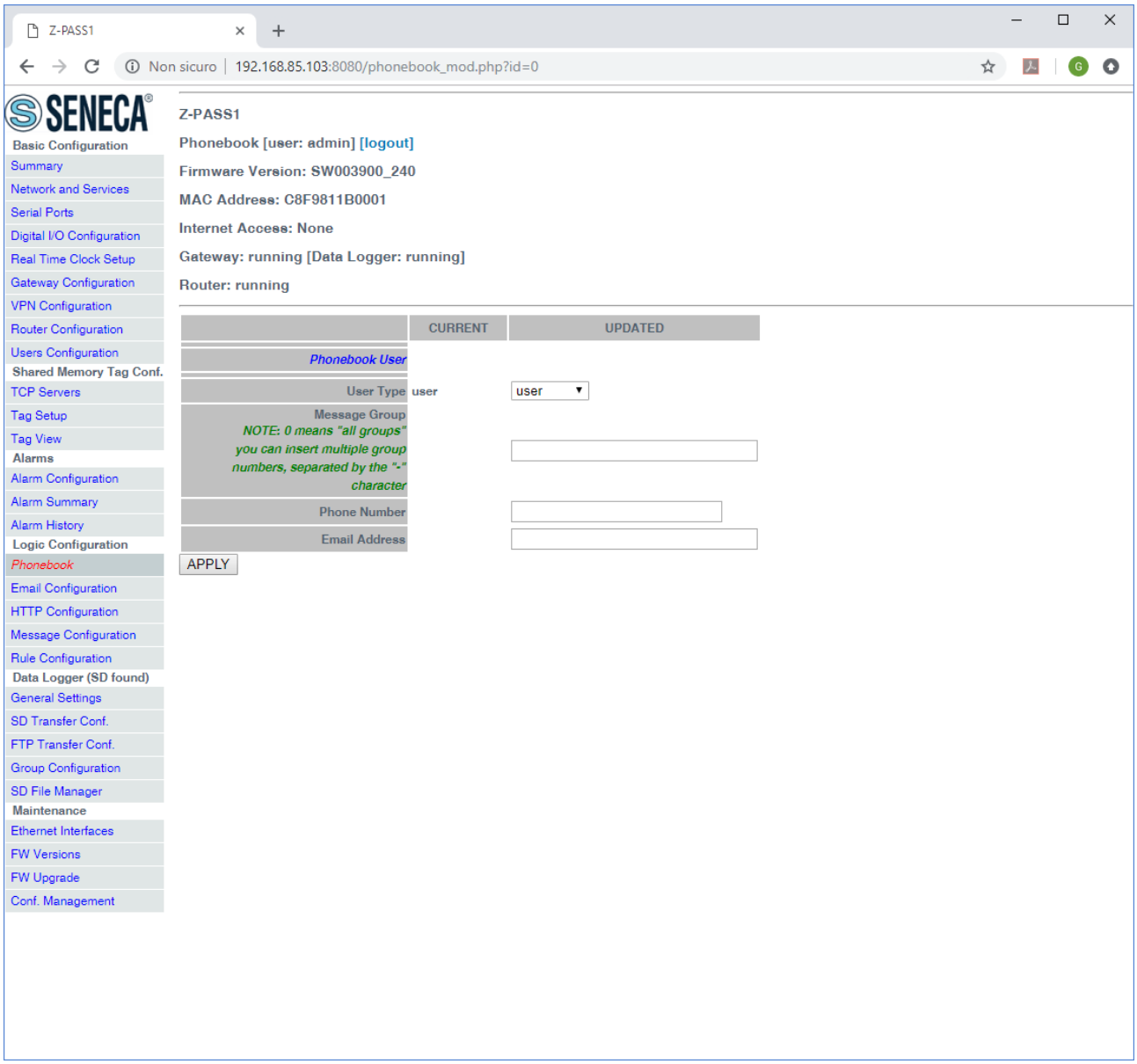
### 20.6.1 Phonebook

By clicking on the “Phonebook” link, in the “Logic Configuration” section, you come to the following page:




In this page, the list of the Phonebook “users” is shown.

By clicking on the “ADD” button, a new user can be inserted into the Phonebook, as in the following figure.

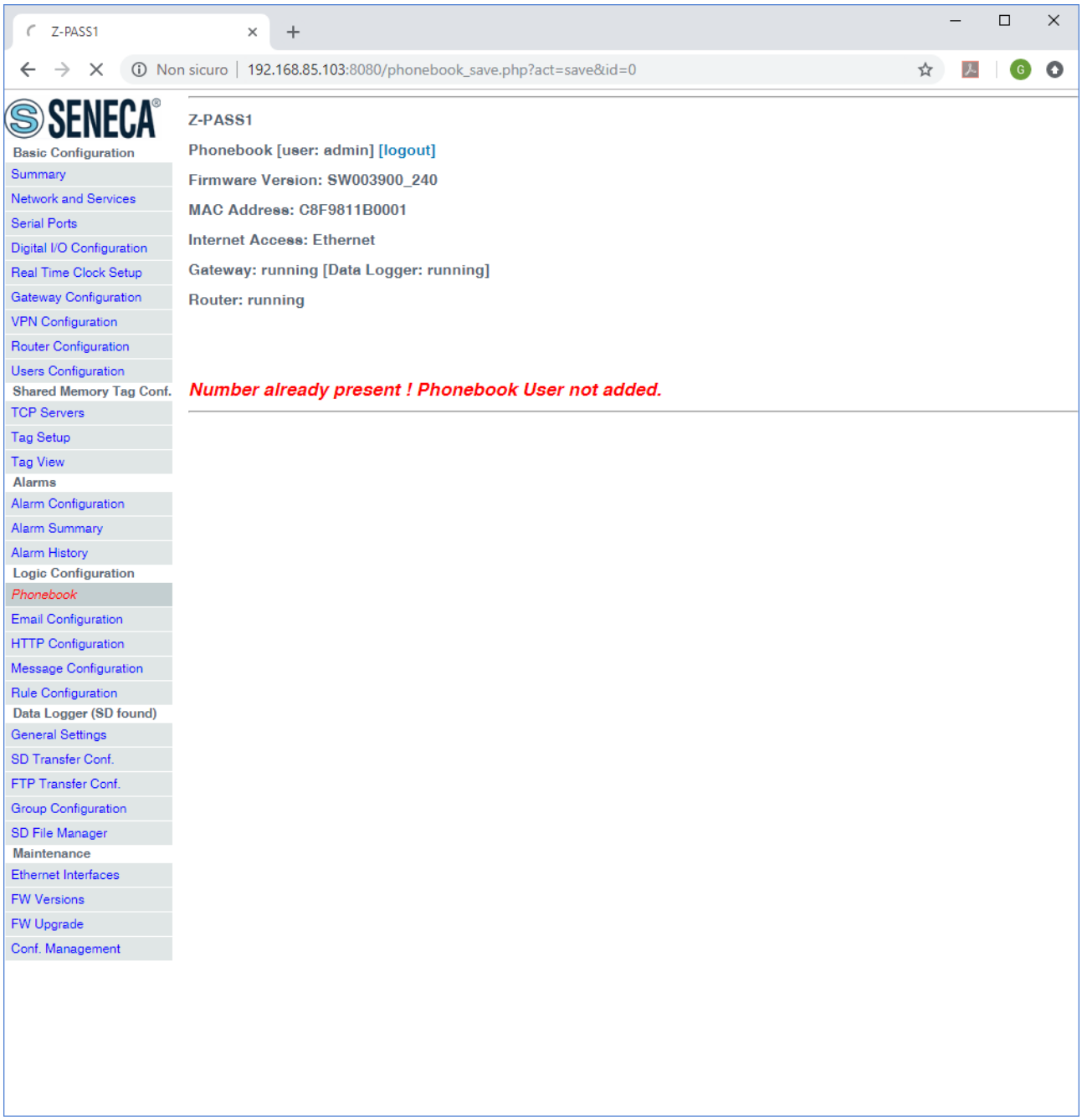



The following table explains the meaning of the parameters related to a Phonebook user.

| Field | Meaning | Default value |
|---|---|---|
| User Type | Possible user types:<br>- "admin": this is the user which receives all the rejected or unrecognized SMS commands, if the "SMS Relay to Admin" parameter is set to ON and the "Startup SMS" messages, if the "Startup SMS" parameter is set to ON; this user can send SMS | user |

| | | |
|---|---|---|
| | commands to the device; it also receives all SMS/EMAIL alarms<br>- "manager": this user can send SMS commands to the device; it receives SMS/EMAIL alarms sent to one of the message groups it belongs to<br>- "user": this user receives SMS/EMAIL alarms sent to one of the message groups it belongs to | |
| Message Group | This parameter contains a list of one or more numbers, separated by the '-' character, which identify the Message Groups which the user belongs to; Message Groups are used as recipients for SMS or EMAIL alarms.<br>The value 0 corresponds to "All Message Groups" | Empty |
| Phone Number | Phone Number in "international format"; the initial '+' character shall be present | Empty |
| Email Address | Email Address, used as a recipient for alarms sent via Email | Empty |

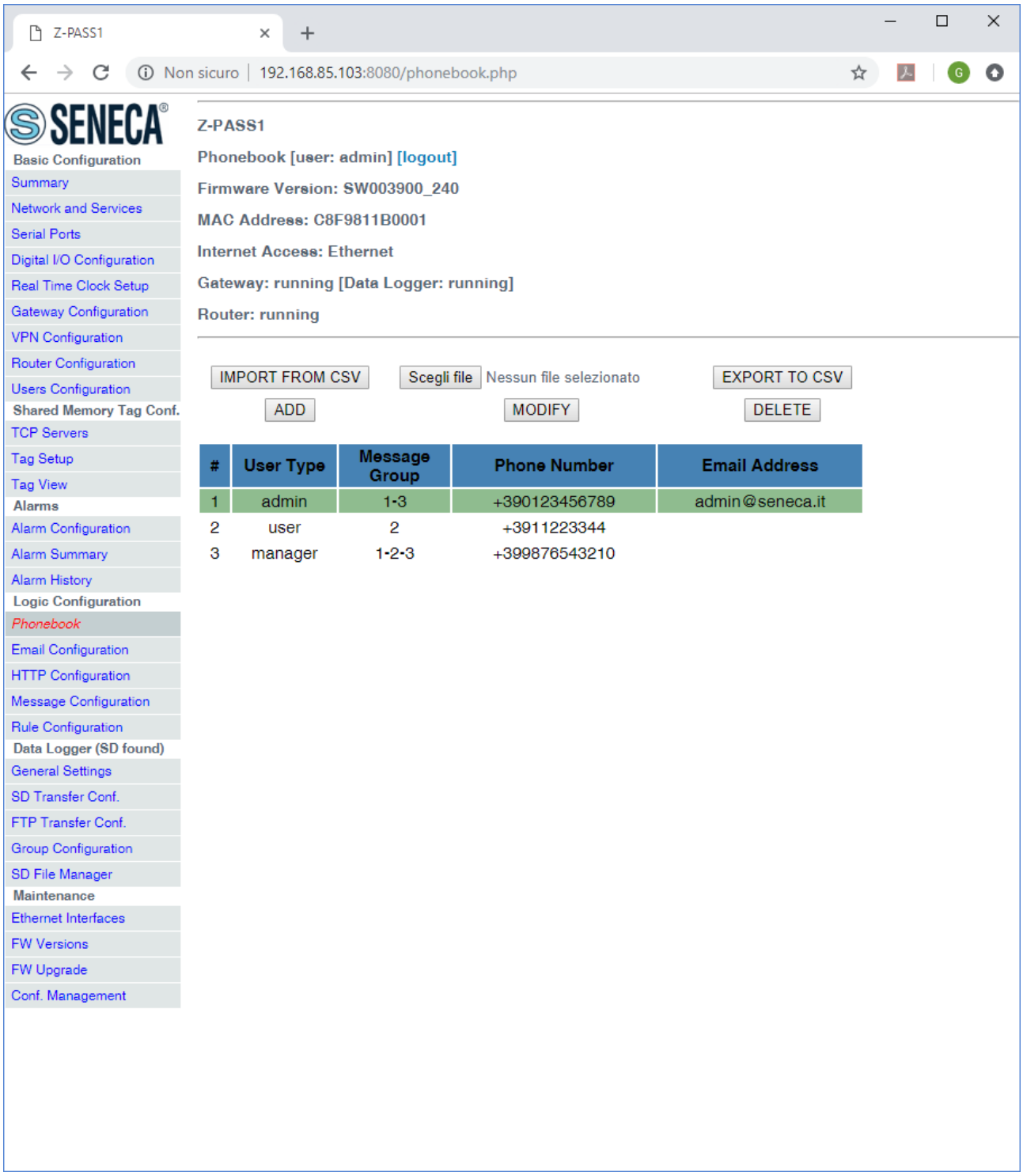
Two users with the same phone number cannot be present in the Phonebook; so, when trying to add a new user with an already existing phone number, the following error is given.

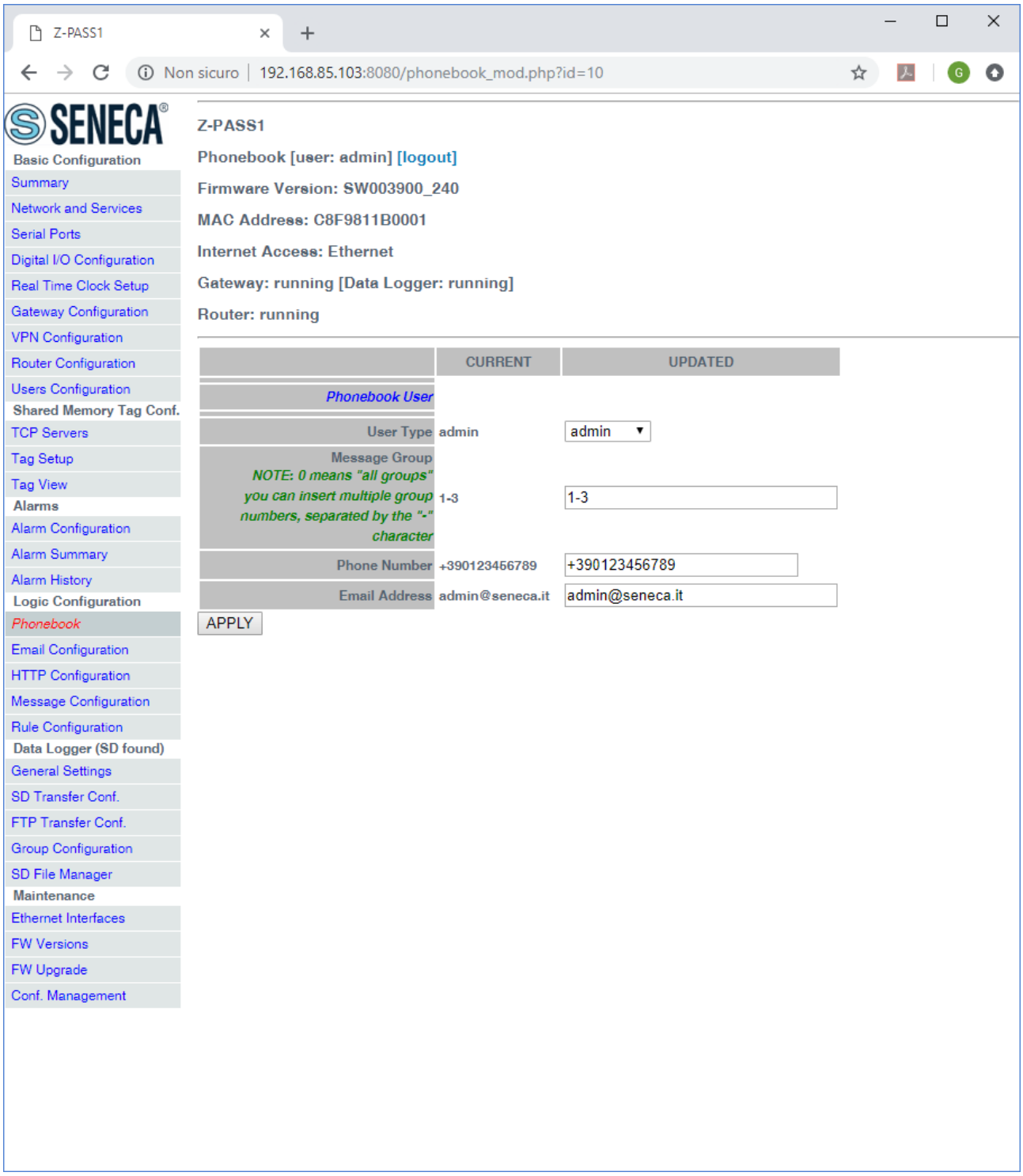



It is possible to insert more than one “admin” user into the Phonebook; just note that only the most recently inserted “admin” user will receive “relayed” SMS commands and “Startup SMS” messages.

Conversely, if no “admin” user is present in the Phonebook, rejected and unrecognized SMS commands won’t be relayed and “Startup SMS” messages won’t be sent, even if the corresponding enable parameters are set to ON.

Selecting a user in the list and clicking on the “MODIFY” button, you can modify the user’s parameters, as in the following figures.


Z-PASS1
Non sicuro | 192.168.85.103:8080/phonebook.php
SENECA
Basic Configuration
Summary
Network and Services
Serial Ports
Digital I/O Configuration
Real Time Clock Setup
Gateway Configuration
VPN Configuration
Router Configuration
Users Configuration
Shared Memory Tag Conf.
TCP Servers
Tag Setup
Tag View
Alarms
Alarm Configuration
Alarm Summary
Alarm History
Logic Configuration
Phonebook
Email Configuration
HTTP Configuration
Message Configuration
Rule Configuration
Data Logger (SD found)
General Settings
SD Transfer Conf.
FTP Transfer Conf.
Group Configuration
SD File Manager
Maintenance
Ethernet Interfaces
FW Versions
FW Upgrade
Conf. Management
Z-PASS1
Phonebook [user: admin] [logout]
Firmware Version: SW003900_240
MAC Address: C8F9811B0001
Internet Access: Ethernet
Gateway: running [Data Logger: running]
Router: running
IMPORT FROM CSV
Scegli file
Nessun file selezionato
EXPORT TO CSV
ADD
MODIFY
DELETE
# User Type Message Group Phone Number Email Address
1 admin 1-3 +390123456789 admin@seneca.it
2 user 2 +3911223344
3 manager 1-2-3 +399876543210



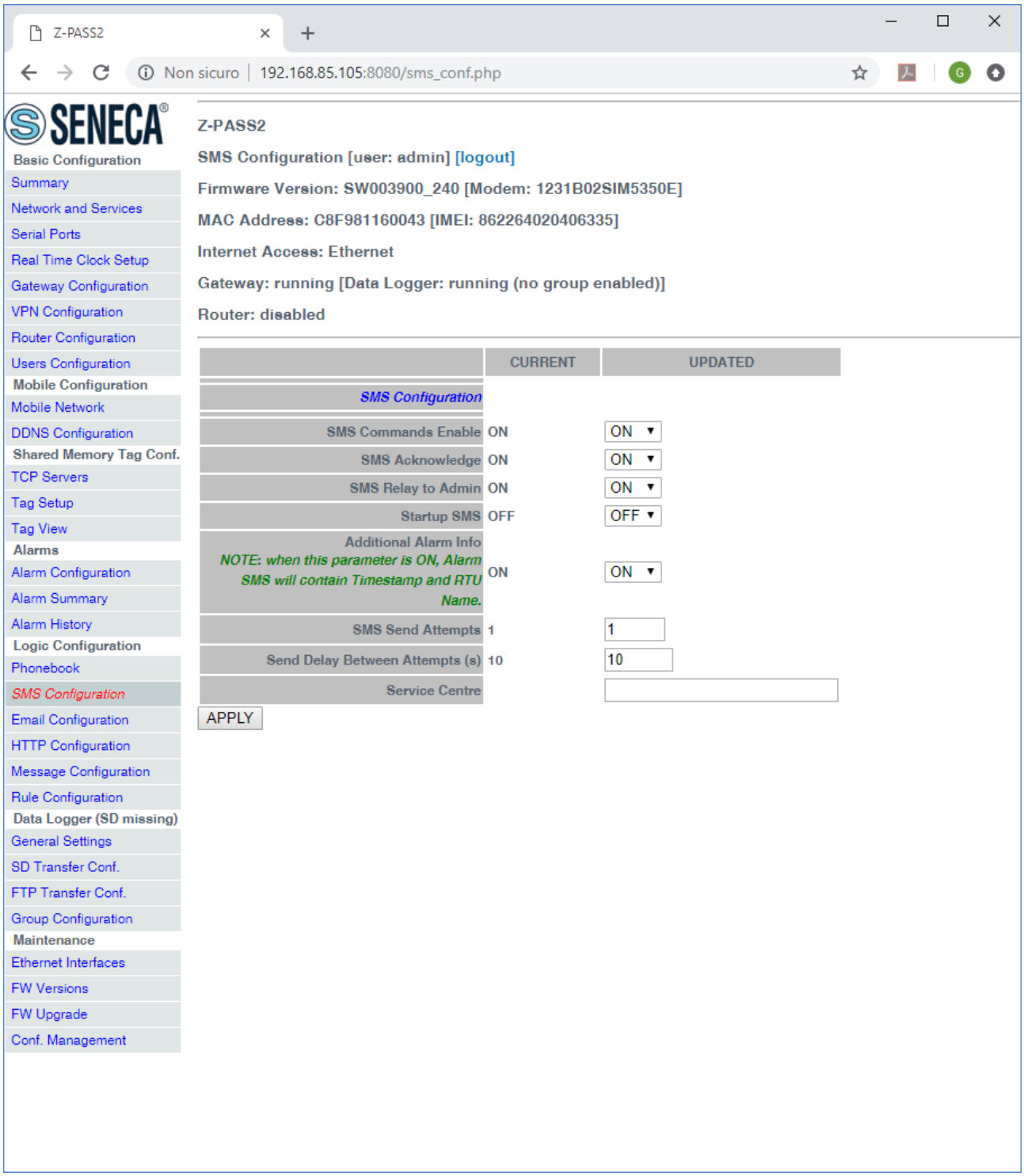

Selecting a user in the list and clicking on the “DELETE” button, you can remove a user from the Phonebook.

Finally, the “EXPORT TO CSV” and “IMPORT FROM CSV” buttons let you export/import the Phonebook to/from a “.csv” file (the separator character is “;”).

Please note that, when importing the Phonebook from a .csv file, the previous Phonebook contents are deleted; so, a fast way to "clean" the Phonebook, if it contains many users, is to import an empty .csv file.

### *20.6.2 SMS Configuration*

By clicking on the "SMS Configuration" link, in the "Logic Configuration" section, you come to the following page:




In this page, you can set the parameters related to the “SMS Commands” functionality (see chapter 17), as listed in the following table:

| Field | Meaning | Default value |
|---|---|---|
| SMS Commands Enable | Flag to enable/disable the SMS commands functionality | ON |

| | | |
|---|---|---|
| SMS Acknowledge | Flag to enable/disable the sending of a response ("acknowledge") to "set" commands (while "get" commands always have a response) (see chapter 17) | ON |
| SMS Relay To Admin | Flag to enable/disable the relaying of rejected or unrecognized commands to the "admin" user | ON |
| Startup SMS | Flag to enable/disable the sending of a "startup" message to the "admin" user | OFF |
| SMS Send Attempts | Number of attempts to send an SMS | 1 |
| Additional Alarm Info | Flag telling if "additional info", that is RTU Name and timestamp, shall be put before the message text in alarm SMS | ON |
| Send Delay Between Attempts (s) | Delay, in seconds, between attempts to send an SMS | 10 |
| Service Centre | SMS Service Centre (SMS-SC) number<br>Typically, this parameter can be left empty, since SMS-SC number is already configured on the SIM | empty |

The "Startup SMS", controlled by the corresponding parameter, has the following format:

```
Z-PASS2<hwrev> '<vpnbox tag name>' (IMEI:<modem IMEI>) STARTED
```

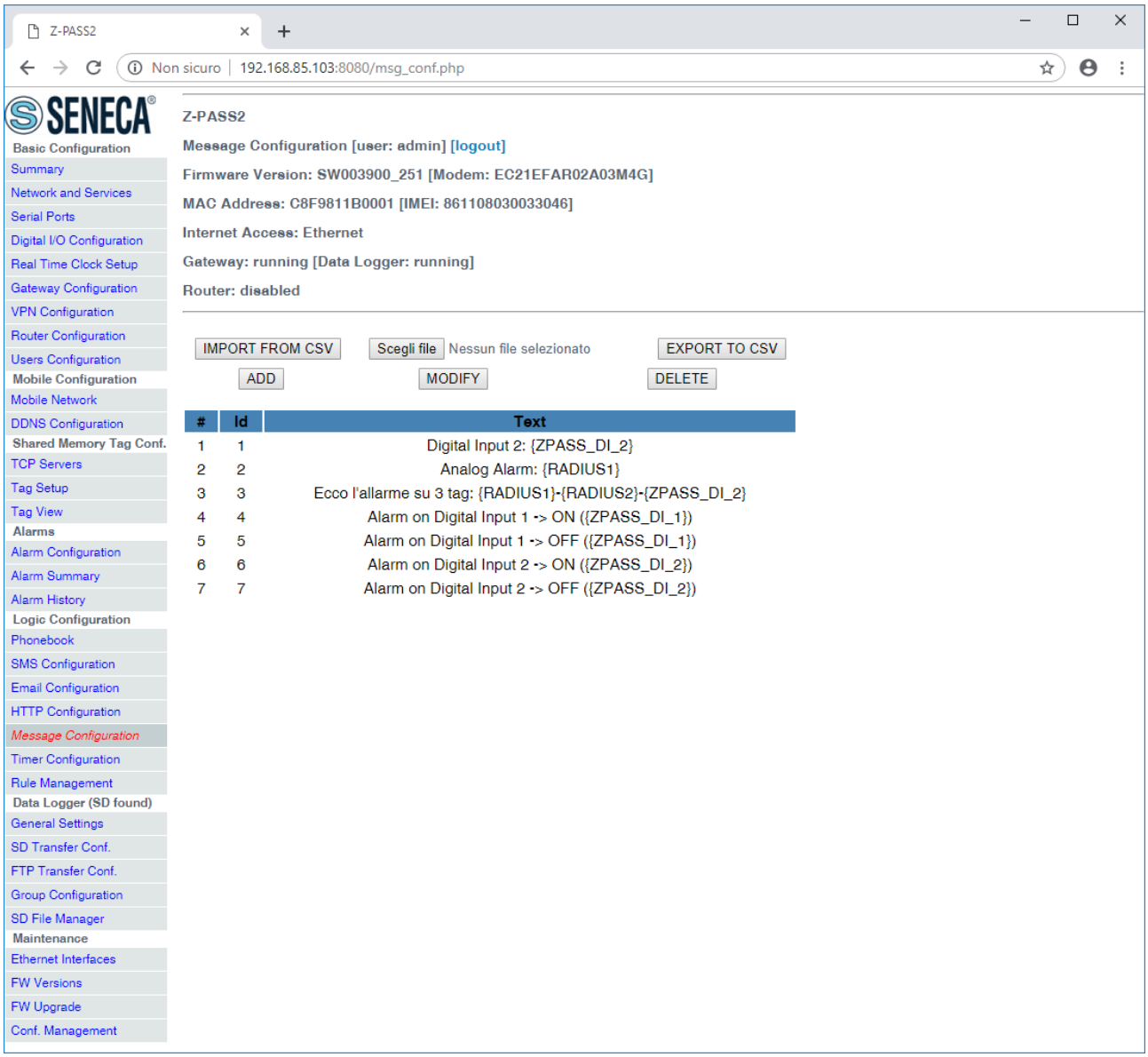
as in the following example:

```
Z-PASS2-IO 'zpass' (IMEI:861108030033046) STARTED
```

Obviously, this page is not available for Z-PASS1 products.

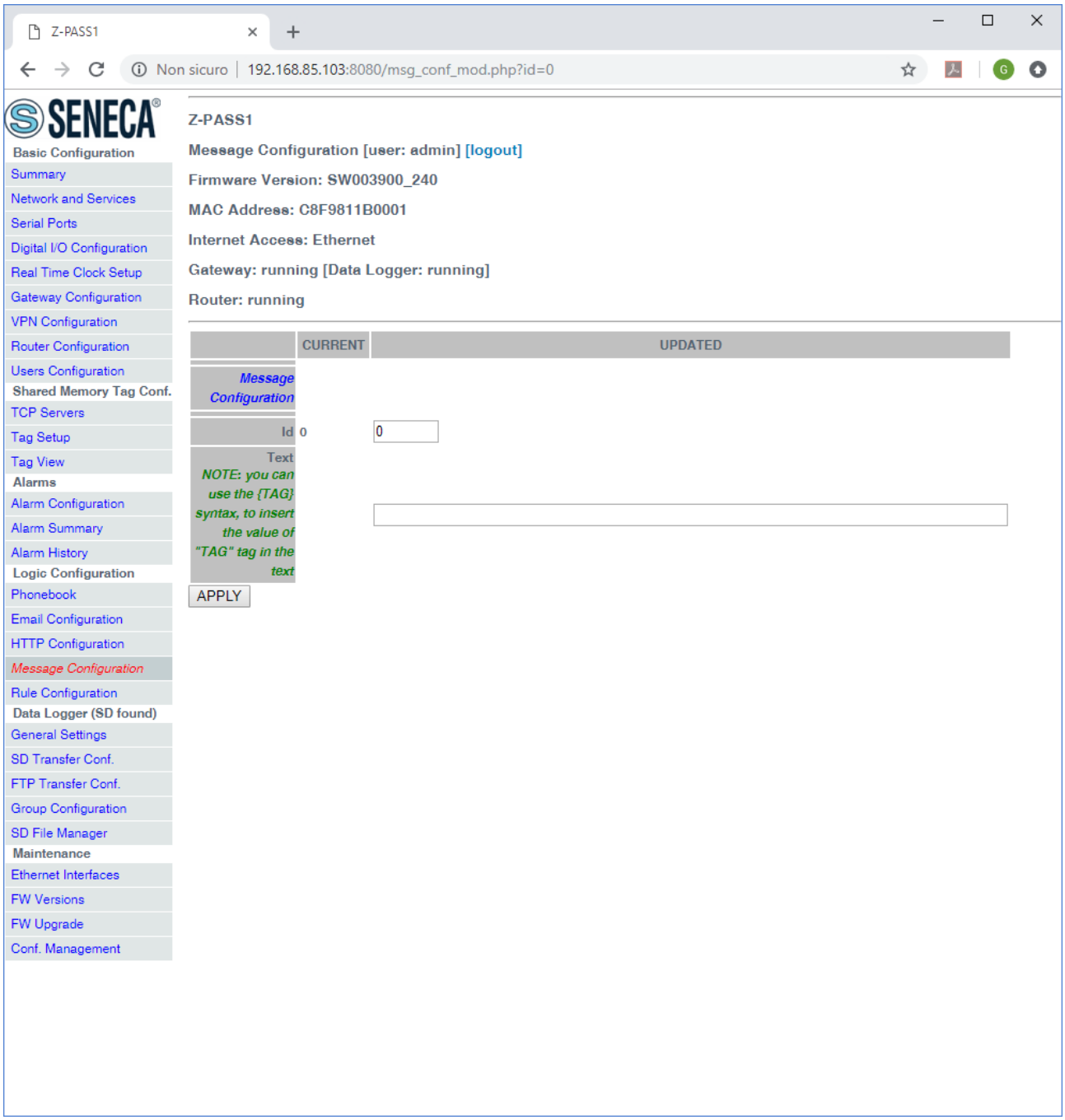
### *20.6.3 Message Configuration*

By clicking on the "Message Configuration" link, in the "Logic Configuration" section, you come to the following page:




This page lets you configure text messages used for alarms sent via SMS, EMAIL, HTTP POST.

By clicking on the “ADD” button, a new message can be configured, as in the following figure.

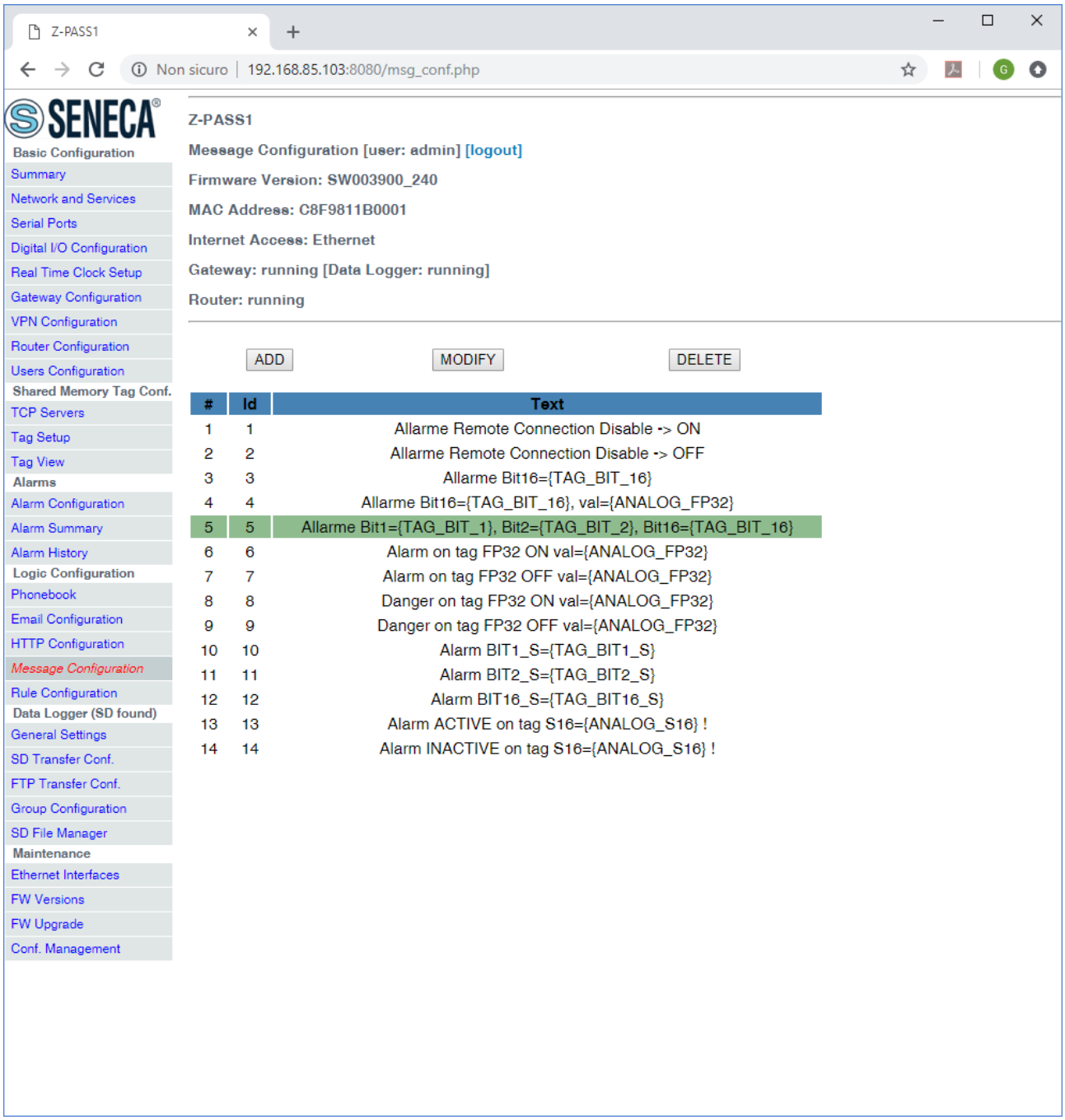


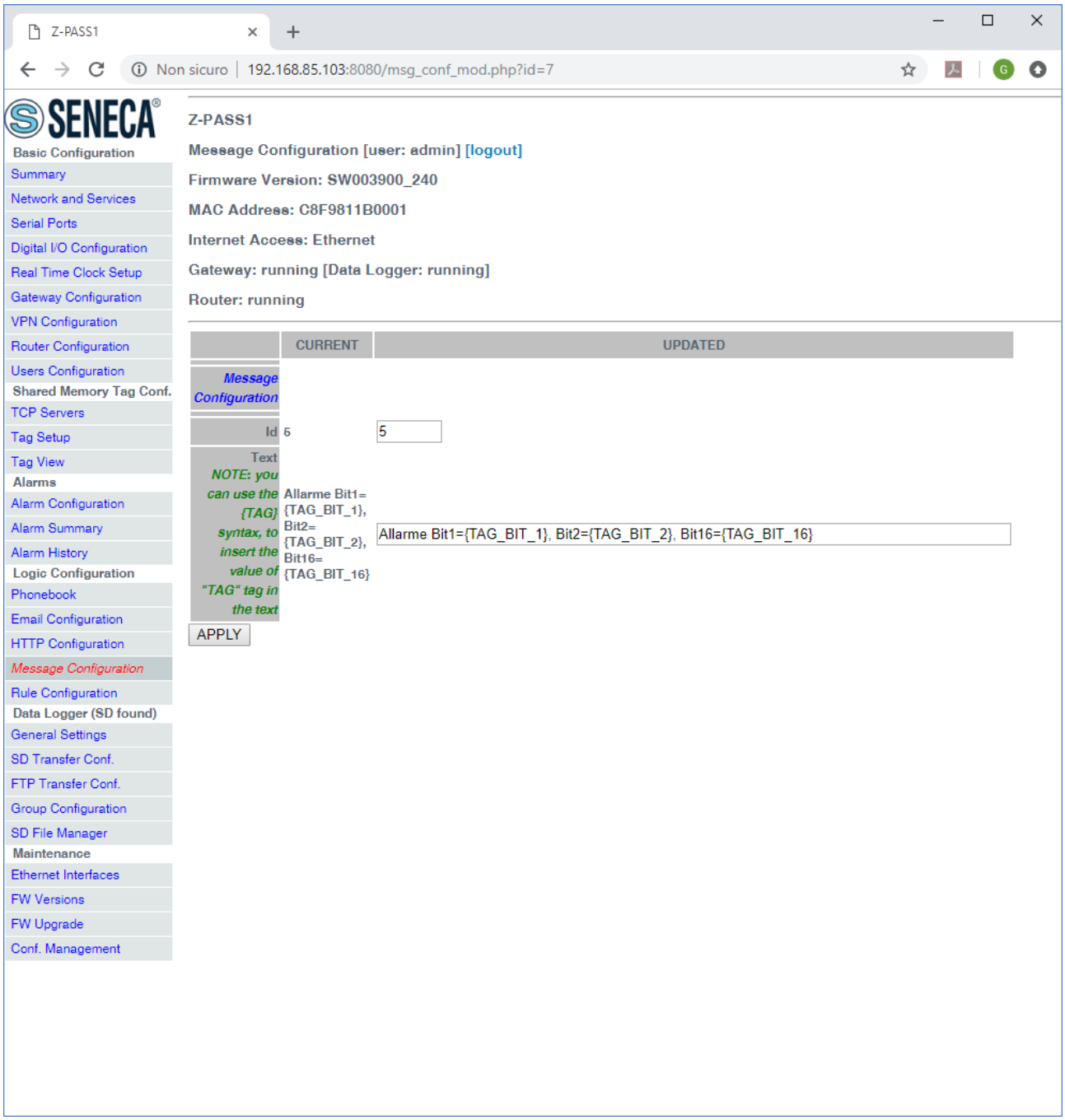

Messages are identified by a numeric identifier.

The message text can currently contain only ASCII characters.

As highlighted by the note in the page, the syntax *{TAG}* will be replaced, in the text, with the current value of the "TAG" tag. This syntax can be used more than once in a message text.

Selecting a message in the list and clicking on the "MODIFY" button, you can modify the message id and text, as in the following figures.


Z-PASS1
Non sicuro | 192.168.85.103:8080/msg_conf.php
SENECA
Basic Configuration
Summary
Network and Services
Serial Ports
Digital I/O Configuration
Real Time Clock Setup
Gateway Configuration
VPN Configuration
Router Configuration
Users Configuration
Shared Memory Tag Conf.
TCP Servers
Tag Setup
Tag View
Alarms
Alarm Configuration
Alarm Summary
Alarm History
Logic Configuration
Phonebook
Email Configuration
HTTP Configuration
Message Configuration
Rule Configuration
Data Logger (SD found)
General Settings
SD Transfer Conf.
FTP Transfer Conf.
Group Configuration
SD File Manager
Maintenance
Ethernet Interfaces
FW Versions
FW Upgrade
Conf. Management
Z-PASS1
Message Configuration [user: admin] [logout]
Firmware Version: SW003900_240
MAC Address: C8F9811B0001
Internet Access: Ethernet
Gateway: running [Data Logger: running]
Router: running
ADD
MODIFY
DELETE
# Id Text
1 1 Allarme Remote Connection Disable -> ON
2 2 Allarme Remote Connection Disable -> OFF
3 3 Allarme Bit16={TAG_BIT_16}
4 4 Allarme Bit16={TAG_BIT_16}, val={ANALOG_FP32}
5 5 Allarme Bit1={TAG_BIT_1}, Bit2={TAG_BIT_2}, Bit16={TAG_BIT_16}
6 6 Alarm on tag FP32 ON val={ANALOG_FP32}
7 7 Alarm on tag FP32 OFF val={ANALOG_FP32}
8 8 Danger on tag FP32 ON val={ANALOG_FP32}
9 9 Danger on tag FP32 OFF val={ANALOG_FP32}
10 10 Alarm BIT1_S={TAG_BIT1_S}
11 11 Alarm BIT2_S={TAG_BIT2_S}
12 12 Alarm BIT16_S={TAG_BIT16_S}
13 13 Alarm ACTIVE on tag S16={ANALOG_S16} !
14 14 Alarm INACTIVE on tag S16={ANALOG_S16} !




Selecting a message in the list and clicking on the “DELETE” button, you can delete a message.

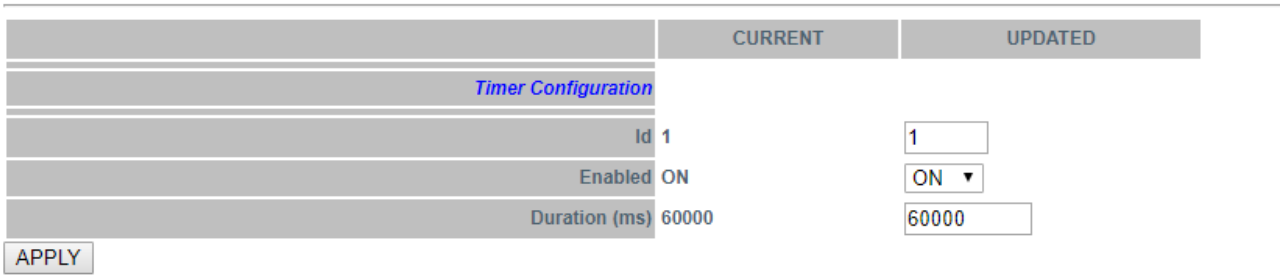
Finally, the “EXPORT TO CSV” and “IMPORT FROM CSV” buttons let you export/import the message configuration to/from a “.csv” file (the separator character is “;”).

Please note that, when importing the message configuration from a .csv file, the previously existing messages are deleted; so, a fast way to “clean” the message configuration, if it contains many entries, is to import an empty .csv file.

Also it is important to note that, to let the Z-PASS properly handle the messages, the imported text must contain only ASCII characters.

### *20.6.4 Timer Configuration*

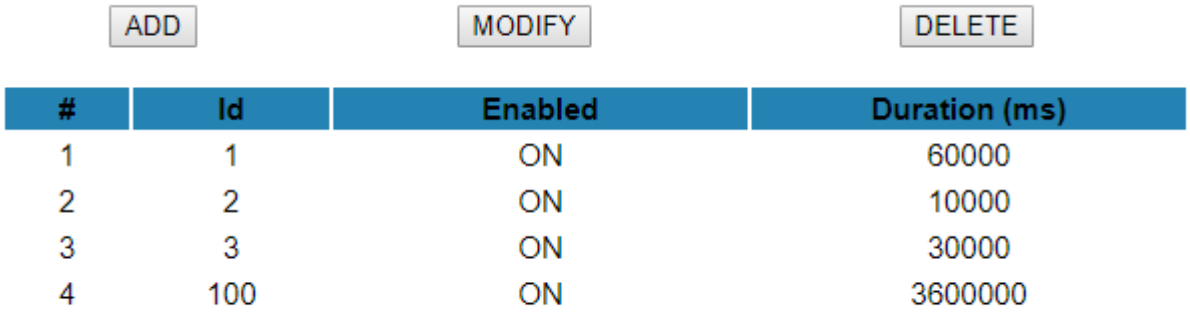
The "Timer Configuration" page lets you define up to 100 timers to be used in the logic rules.




The ID represents the timer mnemonic that must be used in the rules.

Enabled selects if the timer is active or not.

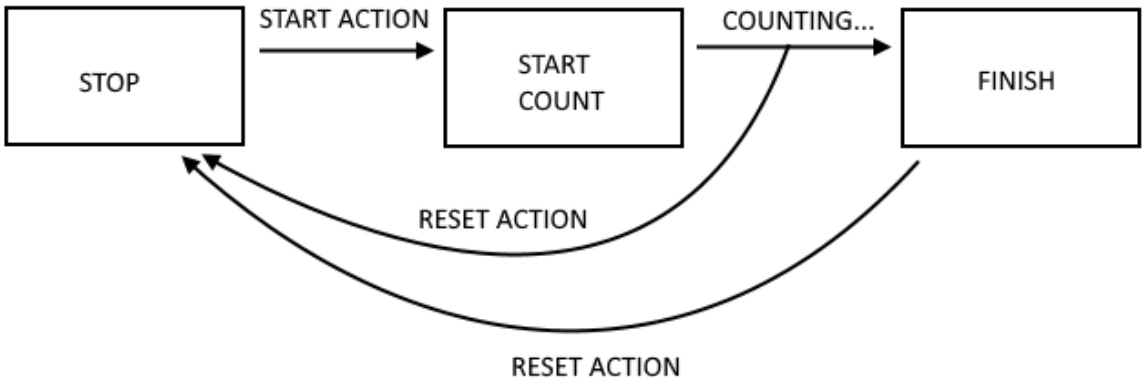
Duration is the trigger value in [ms].




| # | Id | Enabled | Duration (ms) |
|---|---|---|---|
| 1 | 1 | ON | 60000 |
| 2 | 2 | ON | 10000 |
| 3 | 3 | ON | 30000 |
| 4 | 100 | ON | 3600000 |

***Note***

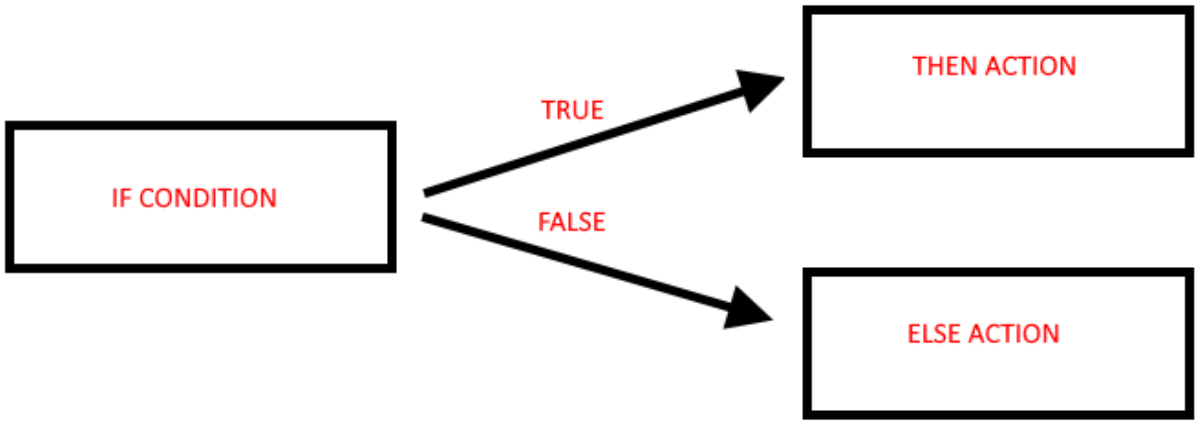
***The Timers by default are in stop mode, they need an action for start and an action for reset, see the following diagram:***




### *20.6.5 Rule Management*

#### *20.6.5.1 Basic Information*

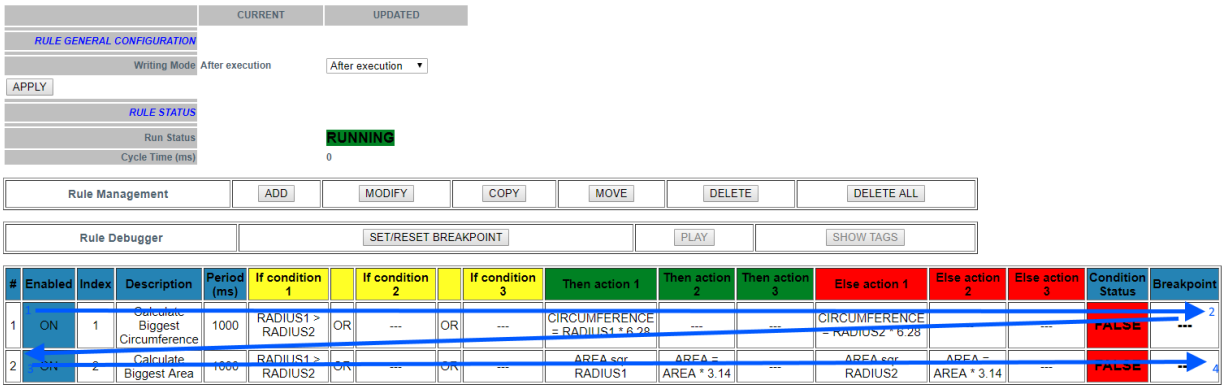
A Rule is composed by “If Condition(s)”, “Then Action(s)” and “Else Action(s)”.




If the “If condition” is true the “then action” is executed

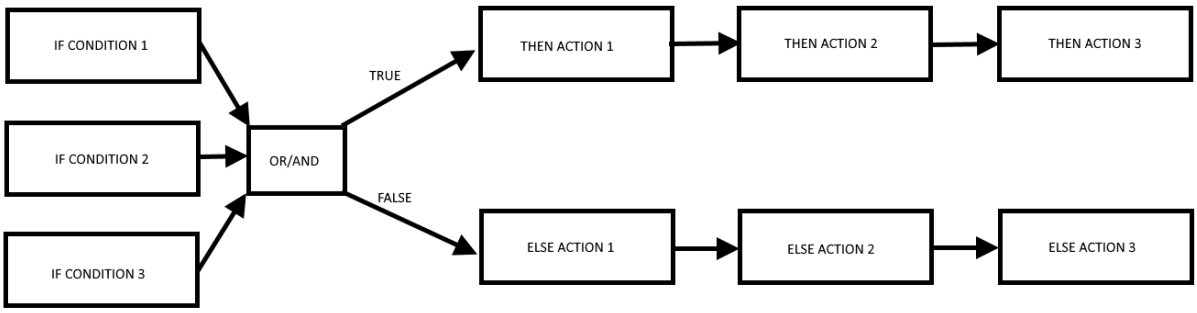
If the “if condition” is false the “else action” is executed

The Rules are executed from top to down and from left to right (in figure 1->2->3->4):




When the rules are terminated then the execution returns to the first.

More in details the correct diagram is:




The “If conditions” can be combined together in “OR” or “AND” logic to obtain a unique boolean state:

| *IF CONDITION 1* | *IF CONDITION 2* | *IF CONDITION 3* | *“OR” RESULT* | *“AND” RESULT* |
|---|---|---|---|---|
| FALSE | FALSE | FALSE | FALSE | FALSE |
| FALSE | FALSE | TRUE | TRUE | FALSE |
| FALSE | TRUE | FALSE | TRUE | FALSE |
| FALSE | TRUE | TRUE | TRUE | FALSE |
| TRUE | FALSE | FALSE | TRUE | FALSE |
| TRUE | FALSE | TRUE | TRUE | FALSE |
| TRUE | TRUE | FALSE | TRUE | FALSE |

| | | | | |
|---|---|---|---|---|
| TRUE | TRUE | TRUE | TRUE | TRUE |

Up to 3 different actions can be executed for each true/false result, the execution order is from 1 to 3.

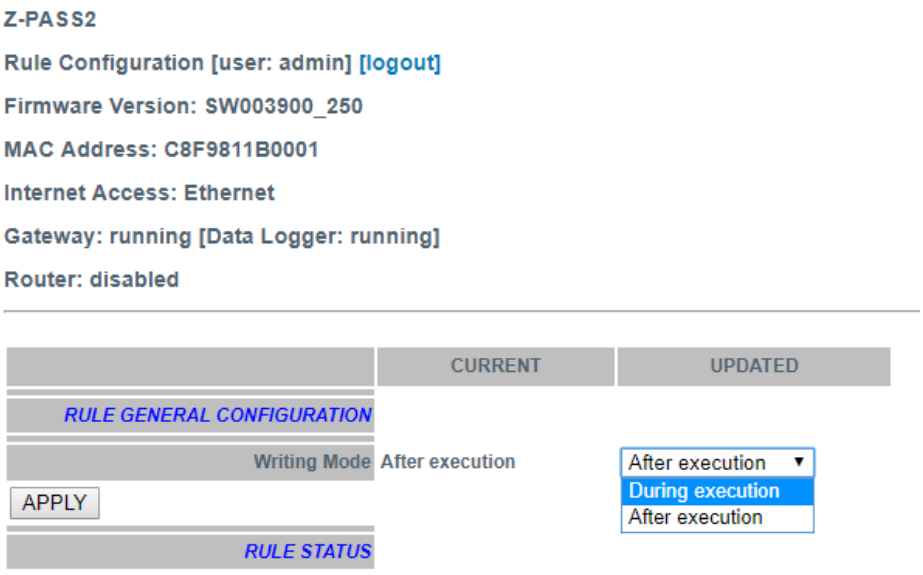
Combining more than one rules, you can create a program, up to 2000 rules can be created.

A rule can be configured to execute actions:

-Only when there is a change in the “OR/AND” result

-At every loop

In the “Rule General Configuration” we can choose when the Tags are written to the external (Modbus) memory image:

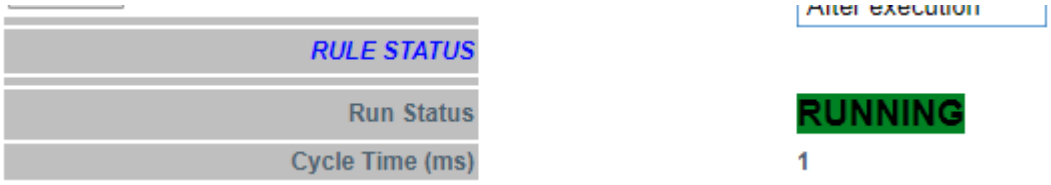



With “After Execution”, we obtain that the tag values are copied to the external image memory at the end of all rules.

With “During Execution”, we obtain that the tag values are copied to the external image memory at the end of each rule.

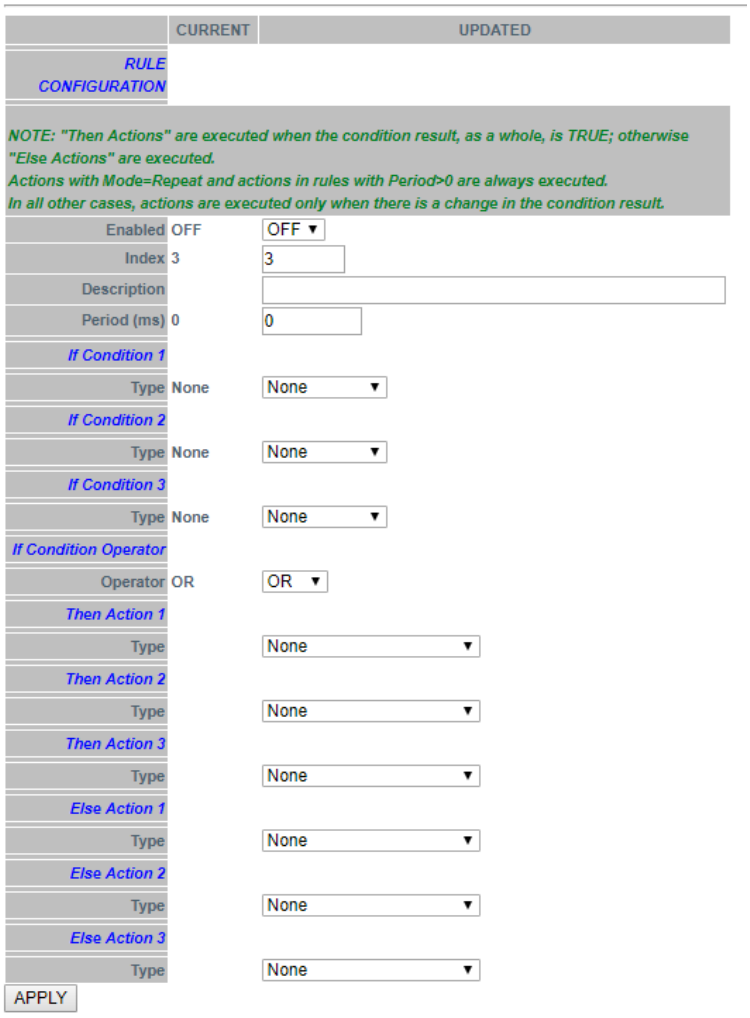
So, using the “After Execution” mode, the new tag values will be refreshed only at end of all rules (also tags that must be written to Mobus RTU/TCP-IP).

The Rule Status will show the Run status (if the rules are in run or pause mode) and the Cycle time that is the time spent to execute all the rules (note that if you need to write tags with modbus protocol the cycle time will include also the time spent for this operation):




### *20.6.5.2 Add a Rule*

By clicking on the “ADD” button, a new rule can be configured:




To configure a rule, the parameters explained in the following table are available.

| Field | Meaning | Default value |
|---|---|---|
| Enabled | Flag telling if the rule is enabled or disabled, that is if the rule will be processed or not | OFF |

| | | |
|---|---|---|
| Index | This parameter defines the rule execution order (1 = first rule to be executed) | - |
| Description | Rule text description | - |
| Period [ms] | If the value is = 0 then the Actions are executed only if there is a change in the "OR/AND" result.<br>If the value is different from 0 the Actions are executed every Period [ms].<br><br>***Don't use little Period values for sending EMAIL/SMS Actions!***<br>***Note that the Period is in milliseconds (seconds/1000).***<br>***NOTE:***<br>***If Period is >0 the Actions are always executed in "repeat" mode*** | 0 |
| If Condition X Type<br>X=[1..3] | This parameter defines the type of condition, for each of the three available "if conditions"<br>Possible types are:<br>- None<br>- Alarm State<br>- Alarm Active<br>- Always<br>- Digital Tag<br>- Analog Tag<br>- Timer<br>- Scheduler<br>- Rule Status<br>- Bitmask<br>See paragraph 20.6.5.2.1 | None |
| If Condition Operator | The possible types are: OR/AND<br>IF Conditions can be combined in OR or AND boolean operations.<br>Remember that using "OR" the result is true if at least one condition is true.<br>Using "AND" the result is true if all the conditions are true. | OR |
| Then/Else | This parameter defines the type of | None |

| | | |
|---|---|---|
| Action X with X=[1..3] | action, for each of the three available “then/else actions”<br>Possible types are:<br>- None<br>- Send Alarm SMS[22]<br>- Send Alarm EMAIL<br>- Send Alarm HTTP POST<br>- Digital Tag<br>- Analog Tag<br>- Timer<br>- Scheduler<br>- Datalogger<br>- Network<br>- Set Bits<br>See paragraph 20.6.5.2.2 | |

#### 20.6.5.2.1 If Condition

Alarm State parameters

| Field | Meaning | Default value |
|---|---|---|
| Alarm Name | The name of the alarm can be selected from the list of all configured alarms | *First alarm name in the list* |
| Alarm State | The state of the alarm; possible states are:<br>- None<br>- Alarm (digital only)<br>- Alarm Low Low (analog only)<br>- Alarm Low (analog only)<br>- Alarm High (analog only)<br>- Alarm High High (analog only)<br>- Acknowledge<br>- Return<br>- End<br>Depending on the type (digital or analog) of the selected alarm, some states are disabled | None |

[22] This option is not available in Z-PASS1 product.

| | | |
|---|---|---|
| Analog Danger Alarm | Flag telling if alarm level shall be "Analog Danger" or not, meaningful only for analog alarms | OFF |

Alarm Active parameters

| **Field** | **Meaning** | **Default value** |
|---|---|---|
| Alarm Name | The name of the alarm can be selected from the list of all configured alarms | *First alarm name in the list* |
| Alarm Active | Flag telling if alarm shall be "active" or not<br>Alarm is "active" if it is in one of the states:<br>- Alarm (digital only)<br>- Alarm Low Low (analog only)<br>- Alarm Low (analog only)<br>- Alarm High (analog only)<br>- Alarm High High (analog only)<br>- Acknowledge<br>Alarm is "not active" if it is in one of the states:<br>- None<br>- Return<br>- End | OFF |
| Analog Danger Alarm | Flag telling if alarm level shall be "Analog Danger" or not, meaningful only for analog alarms. | OFF |

Always

The If condition is always true.
***Note that the Rule is executed only one time if Period is = 0 ms or if the actions are in one time mode.***
***If you need to execute a rule at every cycle you must put the actions in "repeat mode".***
***If you need to execute a rule every xx ms you need to put Period > 0ms.***

Digital Tag

| **Field** | **Meaning** | **Default value** |
|---|---|---|
| Tag | Select the Tag that must be used for the condition | - |

| | | |
|---|---|---|
| Operator | Can be only "=" | = |
| Tag / Constant value | Select if the comparison is between a tag or a constant boolean value | - |

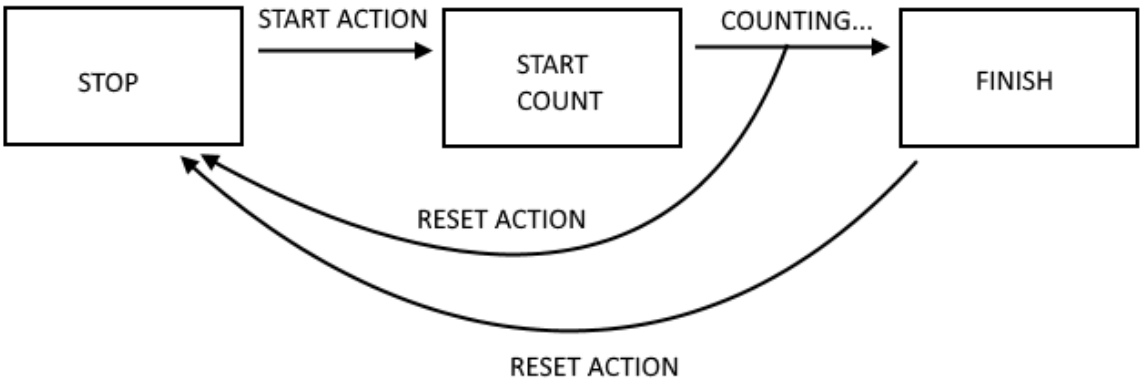
Analog Tag

| Field | Meaning | Default value |
|---|---|---|
| Tag | Select the Tag that must be used for the condition | - |
| Operator | Can be :<br>"="<br>">"<br>"<"<br>">="<br>"<=" | = |
| Tag / Constant value | Select if the comparison is between a tag or a constant value | - |

Timer

| Field | Meaning | Default value |
|---|---|---|
| ID | Select the Timer ID to be used | - |
| Expired | Can be:<br>"OFF" or "ON"<br>With "ON" the condition is true only when the timer is expired (finish state).<br>With "OFF" the condition is true until the timer is in STOP or COUNTING STATE. When the timer is in FINISH state the condition became false.<br>See chapter 20.6.4 | OFF |

The Timer functioning is represented in the following diagram:




Schedule

| Field | Meaning | Default value |
|---|---|---|
| Type | Can be Daily, Weekly Monthly<br>Daily: the condition is true every day at Hour:minute configured<br><br>Weekly: the condition is true the selected day of the week at hour:minute<br><br>Monthly: : the condition is true the selected day of the month at hour:minute | - |
| Day | If type is Weekly:<br>0 = Sunday<br>1 = Monday<br>2 = Tuesday<br>3 = Wednesday<br>4 = Thursday<br>5 = Friday<br>6 = Saturday<br><br>If type is Monthly:<br>Select the day of the month from 1 to 31 | - |
| Hour | Hours | - |
| Minute | Seconds | - |

Rule Status

| Field | Meaning | Default value |
|---|---|---|
| ID | Select which Rule ID | - |
| Enabled | Select between Enabled or Disabled.<br>If “Enabled” the condition is TRUE if the selected Rule is enabled.<br>If “Disabled” the condition is TRUE if the selected Rule is disabled. | - |

Bitmask

| Field | Meaning | Default value |
|---|---|---|
| Tag | Select which tag the bit mask shall be applied to from a list containing all the tags with data type “16Bit Unsigned” and bit index 0 | - |
| Mask | The bitmask represented as a string of 4 hexadecimal digits | 0000 |

The “Bitmask” condition is TRUE if the bitwise AND operation between the given Tag and Mask is different from 0; FALSE otherwise.

#### 20.6.5.2.2 Then/Else Actions

None

No Action must be executed

Send Alarm SMS, Send Alarm EMAIL parameters

| Field | Meaning | Default value |
|---|---|---|
| Message | The message text to be inserted in the SMS or EMAIL | *First message in the list* |
| Group | The group of users the alarm will be sent to | *First group in the list* |

Send Alarm HTTP POST parameters

| Field | Meaning | Default value |
|---|---|---|
| Message | The message text to be inserted in the HTTP POST | *First message in the list* |

Please note that the currently available conditions (“Alarm State”, “Alarm Active”) act as “event triggered”, that is the condition is true, and the action is executed, only when:

- the specified state is entered, for “Alarm State”
- one of the states of the “active” or “not active” sets is entered, for “Alarm Active”

Digital Tag

| Field | Meaning | Default value |
|---|---|---|
| Action Mode | Action mode, select from “One time” or “Repeat”.<br><br>With “One Time” the Actions are executed only if there is a change in the OR/AND Conditions Result.<br><br>With “Repeat” the Actions are executed at every loop (if the rule is enabled and if there is no period configured). | One time |
| Destination Tag | It’s the Tag where the calculated result is copied to | - |
| Operator | It’s the boolean operator to use, select between =, NOT, OR etc… | - |
| Source Tag 1 / Constant value 1 | Select the Tag to use in the boolen calculation.<br>You can also use a boolean constant | - |
| Source Tag 2 / Constant value 2 | Select the second Tag if the operator needs 2 inputs (For example “OR” operator). You can also use a boolean constant | - |

Analog Tag

| Field | Meaning | Default value |
|---|---|---|
| Action Mode | Action mode, select from “One time” or “Repeat”.<br><br>With “One Time” the Actions are executed only if there is a change in the OR/AND Conditions Result.<br><br>With “Repeat” the Actions are executed at every loop (if the rule is | One time |

| | | |
|---|---|---|
| | enabled and if there is no period configured). | |
| Destination Tag | It's the Tag where the calculated result is copied to | - |
| Operator | It's the mathematical operator to use, select between:<br>***"="***<br>copy the Source Tag 1/ Constant value 1 into the Destination Tag<br>Example:<br>Destination Tag = Source Tag 1<br>Or<br>Destination Tag = Constant value 1<br><br>***"+="***<br>Sum to the Destination Tag the value of Source Tag1 / Constant value 1 and copy the result to the Destination Tag.<br><br>Example:<br>Destination Tag = Destination Tag+Source Tag1<br><br>***"-="***<br>Subtract to the Destination Tag the value of Source Tag1 and copy the result to the Destination Tag.<br>Example:<br>Destination Tag = Destination Tag – Source Tag1<br><br>***"*="***<br>Multiply the Destination Tag with the value of Source Tag1 and copy the result to the Destination Tag.<br>Example:<br>Destination Tag = Destination Tag * Source Tag1<br><br>***"/="***<br>Divide the Destination Tag with the value of Source Tag1 and copy the result to the Destination Tag.<br>Example:<br>Destination Tag = Destination Tag / Source Tag1 | - |

| | | |
|---|---|---|
| | ***"%="***<br>Calculate the rest of the division From the Destination Tag and the value of Source Tag1 and copy the result to the Destination Tag.<br>(Note that 53%7 = 4)<br><br>Example:<br>Destination Tag = Destination Tag % Source Tag1<br><br>***"abs"***<br>Calculate the absolute value of Source Tag 1/ Constant value 1 and copy the result to the Destination Tag<br>(Note that abs(-4) = 4)<br><br>Example:<br>Destination Tag = abs(Source Tag 1)<br><br>***"sqrt"***<br>Calculate the square root value of Source Tag 1 / Constant value 1 and copy the result to the Destination Tag.<br>(Note that sqrt(9) = √9 = 3)<br>Example:<br>Destination Tag = sqrt(Source Tag 1)<br><br>***"sqr"***<br>Calculate the square value of Source Tag 1 / Constant value 1 and copy the result to the Destination Tag.<br>(Note that sqr(3) = $3^2$ = 9 )<br>Example:<br>Destination Tag = sqr(Source Tag 1)<br><br>***"log"***<br>Calculate the decimal logarithm of Source Tag 1 / Constant value 1 and copy the result to the Destination Tag.<br>(Note that log(3) = 0.4771212 )<br>Example:<br>Destination Tag = log (Source Tag 1)<br><br>***"ln"*** | |

| | | |
|---|---|---|
| | Calculate the natural logarithm of Source Tag 1 / Constant value 1 and copy the result to the Destination Tag.<br>(Note that ln(3) = 1.09861228867)<br>Example:<br>Destination Tag = ln (Source Tag 1)<br><br>***"exp"***<br>Calculate the Euler's number raised to Source Tag 1 / Constant value 1 and copy the result to the Destination Tag.<br>(Note that<br>$\exp(3) = e^3 = 20.0855369232$<br>ln(exp(3)) = 3<br>Example:<br>Destination Tag = exp(Source Tag 1)<br><br>***"+"***<br>Sum to Source Tag 1 / Constant value 1 With the value of Source Tag 2 / Constant value 2 and copy the result to the Destination Tag.<br>Example:<br>Destination Tag = Source Tag 1+ Source Tag 2<br><br>***"-"***<br>Subtract the Source Tag 1 / Constant value 1 With the value of Source Tag 2 / Constant value 2 and copy the result to the Destination Tag.<br>Example:<br>Destination Tag = Source Tag 1- Source Tag 2<br><br>***"*"***<br>Multiply the Source Tag 1 / Constant value 1 With the value of Source Tag 2 / Constant value 2 and copy the result to the Destination Tag.<br>Example:<br>Destination Tag = Source Tag 1* Source Tag 2<br><br>***"/"***<br>Divide the Source Tag 1 / Constant value 1 With the value of Source Tag 2 / Constant value 2 and copy the result to the Destination Tag. | |

| | | |
|---|---|---|
| | Example:<br>Destination Tag = Source Tag 1 / Source Tag 2<br><br>***"%"***<br>Calculate the rest of the division between the Source Tag 1 / Constant value 1 and the value of Source Tag 2 / Constant value 2 and copy the result to the Destination Tag.<br>(Note that 53%7 = 4)<br><br>Example:<br>Destination Tag = Source Tag 1 % Source Tag 2<br><br>***"pow"***<br>Calculate the Source Tag1 / Constant value 1 raised to the power of the Sorce Tag2 / Constant value 2 and copy the result to the Destination Tag.<br>Example:<br>$DestinationTag = Source\ Tag1^{Source\ Tag2}$ | |
| Source Tag 1 / Constant value 1 | Select the Tag to use as input 1 for the operator used. You can also use a constant value. | - |
| Source Tag 2 / Constant value 2 | Select the Tag to use as input 2 in the calculation if the operator needs 2 inputs.<br>You can also use a constant value. | - |

Timer

| **Field** | **Meaning** | **Default value** |
|---|---|---|
| ID | Select the Timer ID to use.<br>See chapter 20.6.4 | - |
| Action | Select the action to be done to the specified timer:<br>"Start" will start a timer to count<br>"Reset" will reset the timer to the stop state (See chapter 20.6.4) | - |

Rule Status

| Field | Meaning | Default value |
|---|---|---|
| ID | Select the Rule to Control | - |
| Enable | Select the action to be done to the specified rule:<br>"ON" will enable a disabled Rule<br>"OFF" will disable an enabled Rule | - |

Data Logger

| Field | Meaning | Default value |
|---|---|---|
| Group | Select the Logger group to start/stop<br>Select between ALL, 1, 2, 3, 4 | - |
| Enable | Select the action to be done to the specified rule:<br>"ON" will start to log the selected group(s)<br>"OFF" will stop to log the selected group(s) | - |

Network

| Field | Meaning | Default value |
|---|---|---|
| Feature | Select the action to be done to a network feature, select between:<br>PPP* (Start or Stop the connection to the data mobile connection)<br><br>VPN (Start or Stop the VPN /Let's connection)<br><br>Firewall (Start or Stop the Firewall)<br><br>* Only for Z-PASS2 model | - |
| Start | Select the action to be done to the specified Feature:<br>"ON" will enable the feature<br>"OFF" will disabled the feature | - |

Set Bits

| Field | Meaning | Default value |
|---|---|---|
| Action Mode | Action mode, select from "One time" or "Repeat". | One Time |

| | | |
|---|---|---|
| | With “One Time”, the Actions are executed only if there is a change in the OR/AND Conditions Result.<br>With “Repeat”, the Actions are executed at every loop (if the rule is enabled and if there is no period configured). | |
| Destination Tag | Select the destination tag from a list containing all the tags with data type “16Bit Unsigned” and bit index 0 | - |
| Source Tag | Select the source tag from a list containing all the tags with data type “16Bit Unsigned” and bit index 0 | - |
| Mask | The bitmask represented as a string of 4 hexadecimal digits | 0000 |
| Action | *Reset*: set the masked bits to 0<br>*Set*: set the masked bits to 1 | Reset |

#### *20.6.5.3 Example Program*

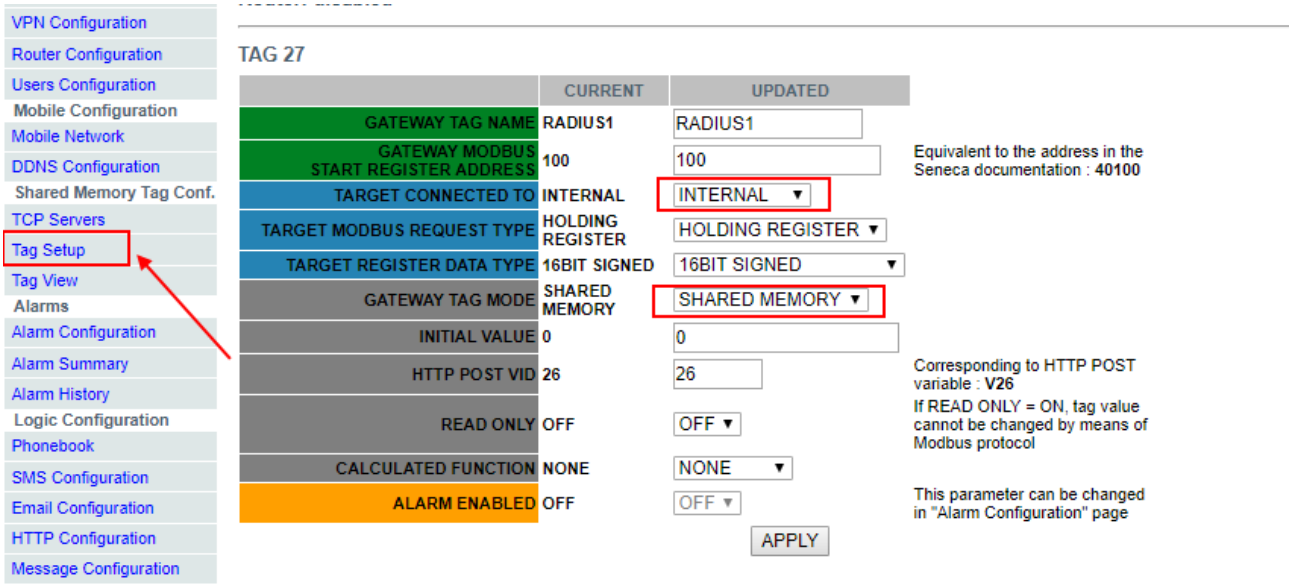
Now we want to create a program that calculate the maximum Circumference and the maximum Area from 2 radius.

##### 20.6.5.3.1 Add the Tags

First of all we add the Tags that we need for the program:

We define Radius1 and Radius2 tags in integer type

Circumference and Area in Real 32 bits (floating point single precision) type:




| | CURRENT | UPDATED | |
|---|---|---|---|
| GATEWAY TAG NAME | RADIUS2 | RADIUS2 | |
| GATEWAY MODBUS START REGISTER ADDRESS | 101 | 101 | Equivalent to the address in the Seneca documentation : **40101** |
| TARGET CONNECTED TO | INTERNAL | INTERNAL | |
| TARGET MODBUS REQUEST TYPE | HOLDING REGISTER | HOLDING REGISTER | |
| TARGET REGISTER DATA TYPE | 16BIT SIGNED | 16BIT SIGNED | |
| GATEWAY TAG MODE | SHARED MEMORY | SHARED MEMORY | |
| INITIAL VALUE | 0 | 0 | |
| HTTP POST VID | 27 | 27 | Corresponding to HTTP POST variable : **V27** |
| READ ONLY | OFF | OFF | If READ ONLY = ON, tag value cannot be changed by means of Modbus protocol |
| CALCULATED FUNCTION | NONE | NONE | |
| ALARM ENABLED | OFF | OFF | This parameter can be changed in "Alarm Configuration" page |

APPLY

TAG 29

| | CURRENT | UPDATED | |
|---|---|---|---|
| GATEWAY TAG NAME | CIRCUMFERENCE | CIRCUMFERENCE | |
| GATEWAY MODBUS START REGISTER ADDRESS | 103 | 103 | Equivalent to the address in the Seneca documentation : **40103** |
| TARGET CONNECTED TO | INTERNAL | INTERNAL | |
| TARGET MODBUS REQUEST TYPE | HOLDING REGISTER | HOLDING REGISTER | |
| TARGET REGISTER DATA TYPE | 32BIT REAL MSW | 32BIT REAL MSW | |
| GATEWAY TAG MODE | SHARED MEMORY | SHARED MEMORY | |
| INITIAL VALUE | 0 | 0 | |
| HTTP POST VID | 28 | 28 | Corresponding to HTTP POST variable : **V28** |
| READ ONLY | OFF | OFF | If READ ONLY = ON, tag value cannot be changed by means of Modbus protocol |
| CALCULATED FUNCTION | NONE | NONE | |
| ALARM ENABLED | OFF | OFF | This parameter can be changed in "Alarm Configuration" page |

APPLY

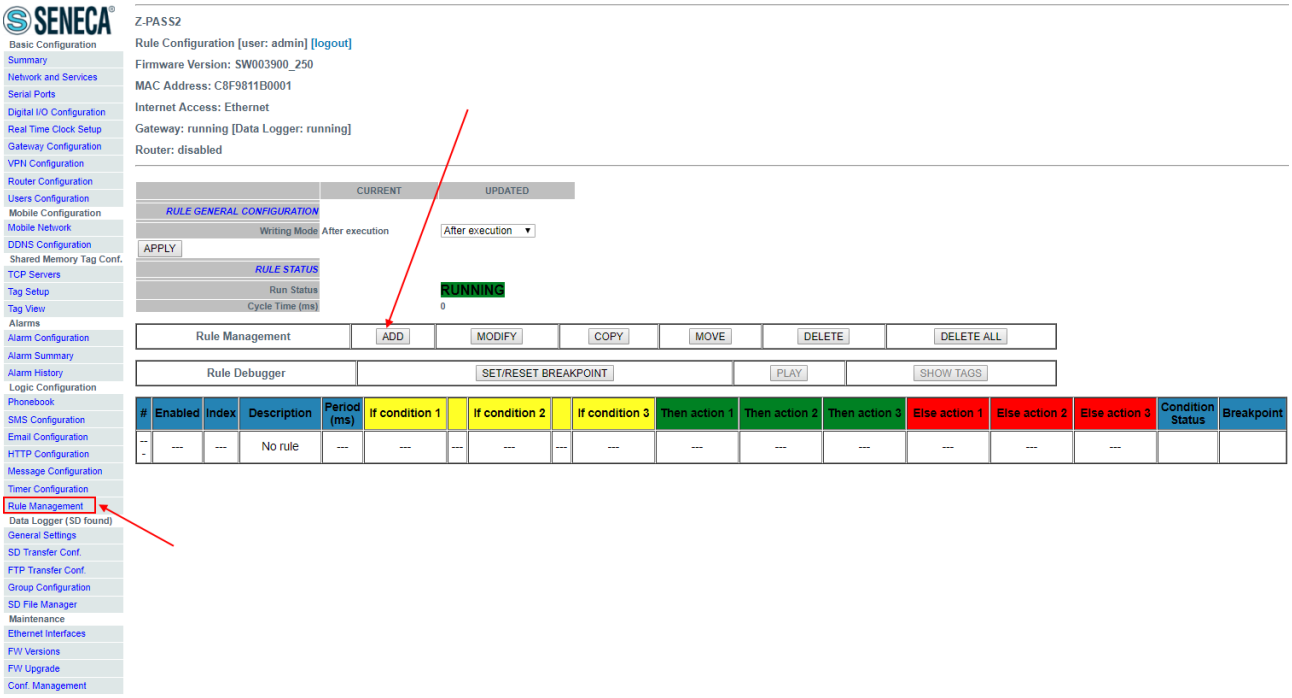
TAG 30

| | CURRENT | UPDATED | |
|---|---|---|---|
| GATEWAY TAG NAME | AREA | AREA | |
| GATEWAY MODBUS START REGISTER ADDRESS | 105 | 105 | Equivalent to the address in the Seneca documentation : **40105** |
| TARGET CONNECTED TO | INTERNAL | INTERNAL | |
| TARGET MODBUS REQUEST TYPE | HOLDING REGISTER | HOLDING REGISTER | |
| TARGET REGISTER DATA TYPE | 32BIT REAL MSW | 32BIT REAL MSW | |
| GATEWAY TAG MODE | SHARED MEMORY | SHARED MEMORY | |
| INITIAL VALUE | 0 | 0 | |
| HTTP POST VID | 29 | 29 | Corresponding to HTTP POST variable : **V29** |
| READ ONLY | OFF | OFF | If READ ONLY = ON, tag value cannot be changed by means of Modbus protocol |
| CALCULATED FUNCTION | NONE | NONE | |
| ALARM ENABLED | OFF | OFF | This parameter can be changed in "Alarm Configuration" page |

APPLY

### 20.6.5.3.2 Add the Rules

Now click on “Rule Mangement” and then ADD to add a new rule:




We Create now the first Rule for calculate the circumference using the biggest Radius between Radius1 and Radius2:

We need that the Rule will be executed every 1000 ms:

| | CURRENT | UPDATED |
|---|---|---|
| *RULE CONFIGURATION* | | |
| *NOTE: "Then Actions" are executed when the condition result, as a whole, is TRUE; otherwise "Else Actions" are executed.<br>Actions with Mode=Repeat and actions in rules with Period>0 are always executed.<br>In all other cases, actions are executed only when there is a change in the condition result.* | | |
| Enabled | ON | ON ▼ |
| Index | 1 | 1 |
| Description | Calculate Biggest Circumference | Calculate Biggest Circumference |
| Period (ms) | 1000 | 1000 |

Then the “if condition” with the biggest radius (we need only 1 if condition):

| | | | | |
|---|---|---|---|---|
| *If Condition 1* | | | | |
| Type | | | Analog Tag | Analog Tag ▼ |
| Tag | RADIUS1 | RADIUS1 ▼ | | |
| Operator | > | > ▼ | | |
| Tag | RADIUS2 | RADIUS2 ▼ | | |
| *If Condition 2* | | | | |
| Type | | | None | None ▼ |
| *If Condition 3* | | | | |
| Type | | | None | None ▼ |
| *If Condition Operator* | | | | |
| Operator | | | OR | OR ▼ |

So, if the condition is true the Radius1 > Radius2 so we must calculate the circumference with Radius1 (Circumference = Radius 1 * 6.28):

| | | | | |
|---|---|---|---|---|
| *Then Action 1* | | | | |
| Type | | | Analog Tag | Analog Tag ▼ |
| Action Mode | One time | One time ▼ | | |
| Destination Tag | CIRCUMFERENCE | CIRCUMFERENCE ▼ | | |
| Operator | * | * ▼ | | |
| Source Tag 1 | RADIUS1 | RADIUS1 ▼ | | |
| Source Tag 2 | constant value | constant value ▼ | | |
| Constant Value 2 | 6.28 | 6.28 | | |
| *Then Action 2* | | | | |
| Type | | | | None ▼ |
| *Then Action 3* | | | | |
| Type | | | | None ▼ |

Else the Radius 1< Radius 2 so we need to calculate the circumference with Radius2 (Circumference = Radius 2 * 6.28):

| | | | |
|---|---|---|---|
| | | *Else Action 1* | |
| | | Type Analog Tag | Analog Tag ▼ |
| Action Mode | One time | One time ▼ | |
| Destination Tag | CIRCUMFERENCE | CIRCUMFERENCE ▼ | |
| Operator | * | * ▼ | |
| Source Tag 1 | RADIUS2 | RADIUS2 ▼ | |
| Source Tag 2 | constant value | constant value ▼ | |
| Constant Value 2 | 6.28 | 6.28 | |
| | | *Else Action 2* | |
| | | Type | None ▼ |
| | | *Else Action 3* | |
| | | Type | None ▼ |

Now click on “APPLY” to save the first Rule:

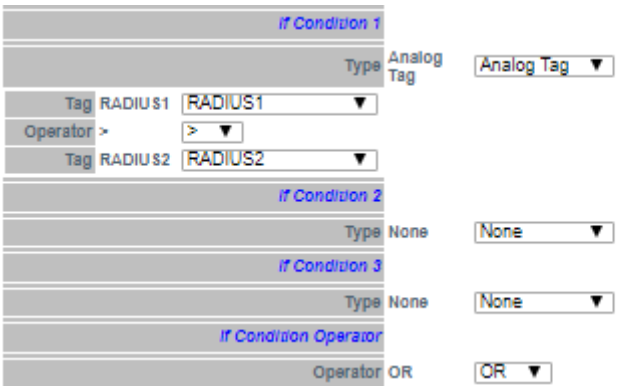
| # | Enabled | Index | Description | Period (ms) | If condition 1 | | If condition 2 | | If condition 3 | Then action 1 | Then action 2 | Then action 3 | Else action 1 | Else action 2 | Else action 3 | Condition Status | Breakpoint |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ON | 1 | Calculate Biggest Circumference | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | CIRCUMFERENCE = RADIUS1 * 6.28 | --- | --- | CIRCUMFERENCE = RADIUS2 * 6.28 | --- | --- | FALSE | --- |

In the same way we create the Second Rule for calculate the biggest Area:

Also this rule must be execute every 1000ms:

| | CURRENT | UPDATED |
|---|---|---|
| *RULE CONFIGURATION* | | |
| *NOTE: "Then Actions" are executed when the condition result, as a whole, is TRUE; otherwise "Else Actions" are executed.*<br>*Actions with Mode=Repeat and actions in rules with Period>0 are always executed.*<br>*In all other cases, actions are executed only when there is a change in the condition result.* | | |
| Enabled | ON | ON ▼ |
| Index | 2 | 2 |
| Description | Calculate Biggest Area | Calculate Biggest Area |
| Period (ms) | 1000 | 1000 |

The “if condition” is the same of the first rule:




Now we must calculate the AREA using the following calculation:

$$AREA = (RADIUS^2) * 3.14$$

We need to brench the realtion in two step:

In the first step we calculate:

$$AREA = RADIUS1^2$$

And in the second:

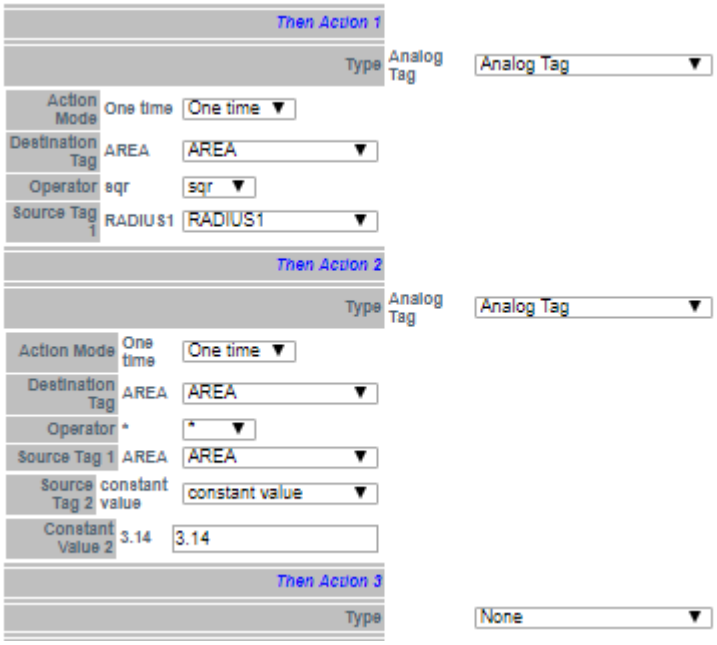
$$AREA = AREA * 3.14$$

So, in our rule if RADIUS1 > RADIUS2 we calculate AREA with RADIUS1 using the square function (sqr):

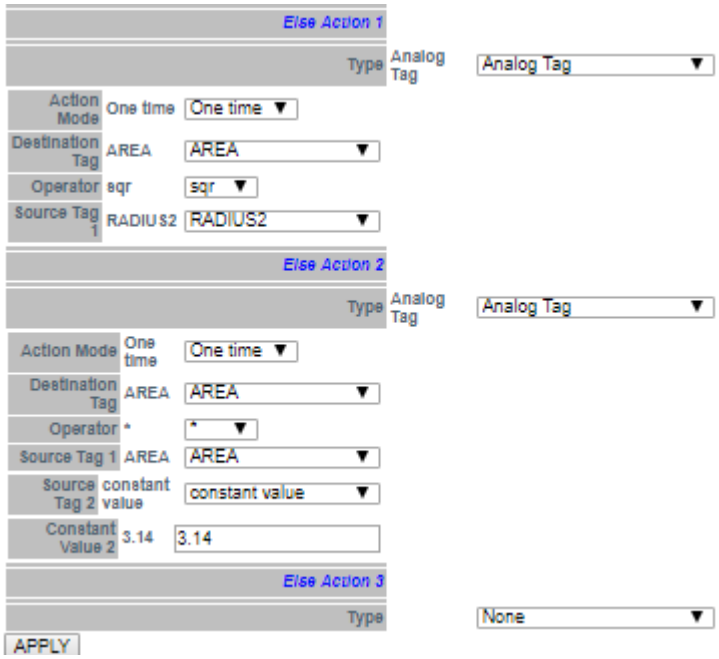
AREA = sqr(RADIUS1)

And then

AREA = AREA*3.14




Then if RADIUS1 < RADIUS2 we calculate AREA with RADIUS2:

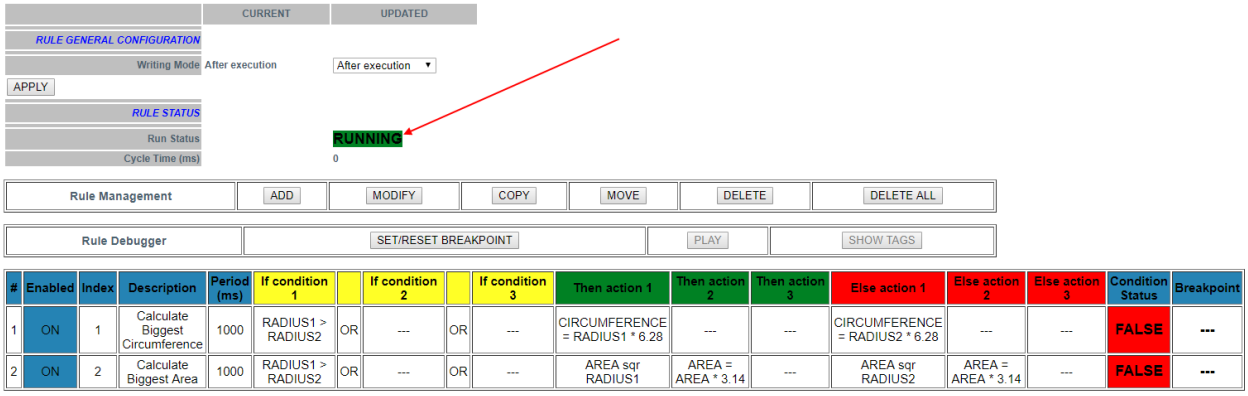



Now click on “APPLY” to save the second Rule too:

| # | Enabled | Index | Description | Period (ms) | If condition 1 | | If condition 2 | | If condition 3 | Then action 1 | Then action 2 | Then action 3 | Else action 1 | Else action 2 | Else action 3 | Condition Status | Breakpoint |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ON | 1 | Calculate Biggest Circumference | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | CIRCUMFERENCE = RADIUS1 * 6.28 | --- | --- | CIRCUMFERENCE = RADIUS2 * 6.28 | --- | --- | FALSE | --- |
| 2 | ON | 2 | Calculate Biggest Area | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | AREA sqr RADIUS1 | AREA = AREA * 3.14 | --- | AREA sqr RADIUS2 | AREA = AREA * 3.14 | --- | FALSE | --- |

### *20.6.5.4 Testing the Example Program*

When a rule is added the Rule start automatically (RUNNING):



| | CURRENT | UPDATED |
|---|---|---|
| RULE GENERAL CONFIGURATION | | |
| Writing Mode | After execution | After execution |
| APPLY | | |
| RULE STATUS | | |
| Run Status | | RUNNING |
| Cycle Time (ms) | | 0 |

| Rule Management | ADD | MODIFY | COPY | MOVE | DELETE | DELETE ALL |
|---|---|---|---|---|---|---|

| Rule Debugger | SET/RESET BREAKPOINT | PLAY | SHOW TAGS |
|---|---|---|---|

| # | Enabled | Index | Description | Period (ms) | If condition 1 | | If condition 2 | | If condition 3 | Then action 1 | Then action 2 | Then action 3 | Else action 1 | Else action 2 | Else action 3 | Condition Status | Breakpoint |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ON | 1 | Calculate Biggest Circumference | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | CIRCUMFERENCE = RADIUS1 * 6.28 | --- | --- | CIRCUMFERENCE = RADIUS2 * 6.28 | --- | --- | FALSE | --- |
| 2 | ON | 2 | Calculate Biggest Area | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | AREA sqr RADIUS1 | AREA = AREA * 3.14 | --- | AREA sqr RADIUS2 | AREA = AREA * 3.14 | --- | FALSE | --- |

For testing the program we can write the tags RADIUS1 and RADIUS2 from Modbus RTU/MODBUS TCP-IP (registers 40100-40101 in our example) or using the page “Tag View”:

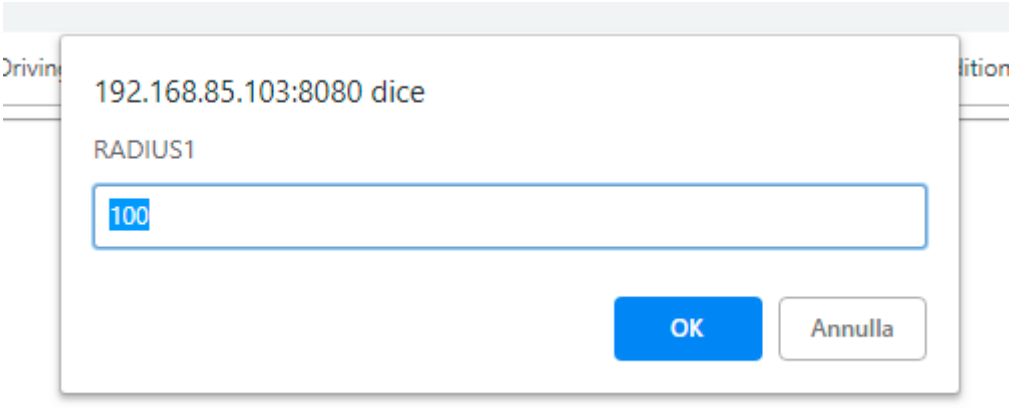
Router Configuration
Users Configuration
Mobile Configuration
Mobile Network
DDNS Configuration
Shared Memory Tag Conf.
TCP Servers
Tag Setup
Tag View
Alarms
Alarm Configuration
Alarm Summary
Alarm History
Logic Configuration
Phonebook
SMS Configuration
Email Configuration
HTTP Configuration
Message Configuration
Timer Configuration
Rule Management
Data Logger (SD found)
General Settings
SD Transfer Conf.
FTP Transfer Conf.
Group Configuration
SD File Manager
Maintenance
Ethernet Interfaces

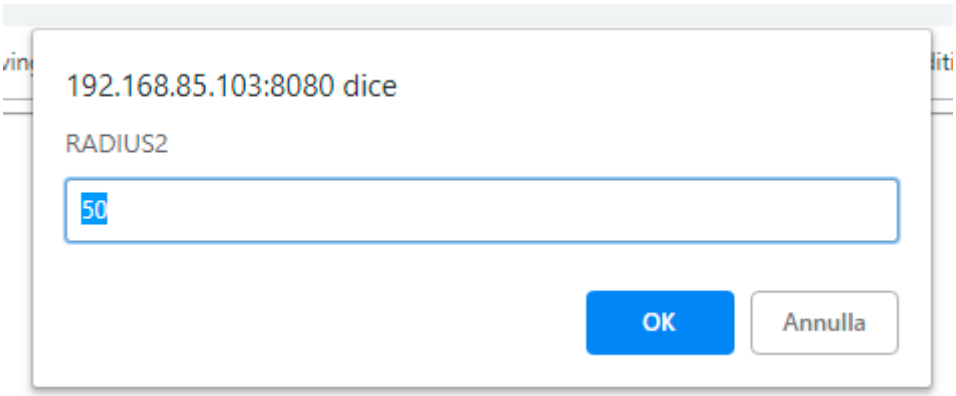
Data Logger: START STOP CLEAN CACHE

Page : 1/20 PREVIOUS PAGE NEXT PAGE

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 17 | GPS_YEAR | 16 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | - | --- | NONE | NONE | |
| 18 | GPS_LATITUDE | 17 | HOLDING REGISTER | 64BIT REAL | 0 | - | --- | NONE | NONE | |
| 19 | GPS_LONGITUDE | 21 | HOLDING REGISTER | 64BIT REAL | 0 | - | --- | NONE | NONE | |
| 20 | GPS_HDOP | 25 | HOLDING REGISTER | 64BIT REAL | 0 | - | --- | NONE | NONE | |
| 21 | GPS_ALTITUDE | 29 | HOLDING REGISTER | 64BIT REAL | 0 | - | --- | NONE | NONE | |
| 22 | GPS_COG | 33 | HOLDING REGISTER | 64BIT REAL | 0 | - | --- | NONE | NONE | |
| 23 | GPS_SPEED_KM | 37 | HOLDING REGISTER | 64BIT REAL | 0 | - | --- | NONE | NONE | |
| 24 | GPS_SPEED_KN | 41 | HOLDING REGISTER | 64BIT REAL | 0 | - | --- | NONE | NONE | |
| 25 | GPS_FIX | 45 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | - | --- | NONE | NONE | |
| 26 | GPS_NUM_SAT | 46 | HOLDING REGISTER | 16BIT UNSIGNED | 0 | - | --- | NONE | NONE | |
| 27 | RADIUS1 | 100 | HOLDING REGISTER | 16BIT SIGNED | 0 | - | 07/03/2019 10:07:25.651279 | NONE | NONE | CHANGE |
| 28 | RADIUS2 | 101 | HOLDING REGISTER | 16BIT SIGNED | 0 | - | 07/03/2019 10:07:25.651519 | NONE | NONE | CHANGE |
| 29 | CIRCUMFERENCE | 103 | HOLDING REGISTER | 32BIT REAL MSW | 0 | - | 07/03/2019 11:11:16.130379 | NONE | NONE | CHANGE |
| 30 | AREA | 105 | HOLDING REGISTER | 32BIT REAL MSW | 0 | - | 07/03/2019 11:11:16.130488 | NONE | NONE | CHANGE |

Now we change the RADIUS1=100 and RADIUS2=50 by clicking on “CHANGE” button:




Now we can pass to “Rule Management” page for view the result:

| | CURRENT | UPDATED |
|---|---|---|
| RULE GENERAL CONFIGURATION | | |
| Writing Mode | After execution | After execution |
| APPLY | | |
| RULE STATUS | | |
| Run Status | | RUNNING |
| Cycle Time (ms) | | 0 |

| Rule Management | ADD | MODIFY | COPY | MOVE | DELETE | DELETE ALL |
|---|---|---|---|---|---|---|

| Rule Debugger | SET/RESET BREAKPOINT | PLAY | SHOW TAGS |
|---|---|---|---|

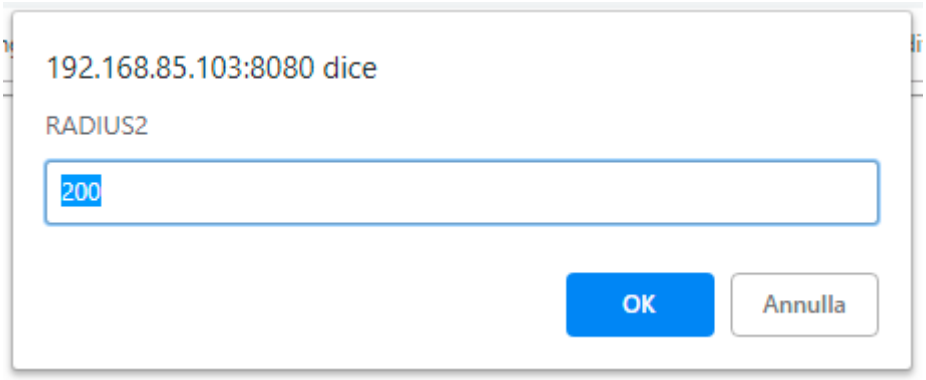
| # | Enabled | Index | Description | Period (ms) | If condition 1 | | If condition 2 | | If condition 3 | Then action 1 | Then action 2 | Then action 3 | Else action 1 | Else action 2 | Else action 3 | Condition Status | Breakpoint |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ON | 1 | Calculate Biggest Circumference | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | CIRCUMFERENCE = RADIUS1 * 6.28 | --- | --- | CIRCUMFERENCE = RADIUS2 * 6.28 | --- | --- | TRUE | --- |
| 2 | ON | 2 | Calculate Biggest Area | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | AREA sqr RADIUS1 | AREA = AREA * 3.14 | --- | AREA sqr RADIUS2 | AREA = AREA * 3.14 | --- | TRUE | --- |

Now the condition status of the 2 rules is true because the RADIUS1 > RADIUS2, so are executed the “Then Actions”

In Tag view the calculation of CIRCUMFERENCE and AREA are updated:

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 27 | RADIUS1 | 100 | HOLDING REGISTER | 16BIT SIGNED | 100 | - | 07/03/2019 11:15:56.934313 | NONE | NONE | CHANGE |
| 28 | RADIUS2 | 101 | HOLDING REGISTER | 16BIT SIGNED | 50 | - | 07/03/2019 11:34:12.465220 | NONE | NONE | CHANGE |
| 29 | CIRCUMFERENCE | 103 | HOLDING REGISTER | 32BIT REAL MSW | 628 | - | 07/03/2019 11:34:39.634836 | NONE | NONE | CHANGE |
| 30 | AREA | 105 | HOLDING REGISTER | 32BIT REAL MSW | 31400 | - | 07/03/2019 11:34:39.634973 | NONE | NONE | CHANGE |

Now we change to 200 the RADIUS2 value in the tag view pages:




And now:

| | CURRENT | UPDATED |
|---|---|---|
| RULE GENERAL CONFIGURATION | | |
| Writing Mode | After execution | After execution |
| APPLY | | |
| RULE STATUS | | |
| Run Status | | RUNNING |
| Cycle Time (ms) | | 0 |

| Rule Management | ADD | MODIFY | COPY | MOVE | DELETE | DELETE ALL |
|---|---|---|---|---|---|---|

| Rule Debugger | SET/RESET BREAKPOINT | PLAY | SHOW TAGS |
|---|---|---|---|

| # | Enabled | Index | Description | Period (ms) | If condition 1 | | If condition 2 | | If condition 3 | Then action 1 | Then action 2 | Then action 3 | Else action 1 | Else action 2 | Else action 3 | Condition Status | Breakpoint |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ON | 1 | Calculate Biggest Circumference | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | CIRCUMFERENCE = RADIUS1 * 6.28 | --- | --- | CIRCUMFERENCE = RADIUS2 * 6.28 | --- | --- | FALSE | --- |
| 2 | ON | 2 | Calculate Biggest Area | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | AREA sqr RADIUS1 | AREA = AREA * 3.14 | --- | AREA sqr RADIUS2 | AREA = AREA * 3.14 | --- | FALSE | --- |

Now the condition status of the 2 rules is false because the RADIUS1 < RADIUS2, so are executed the “Else Actions”

In Tag view the calculation of CIRCUMFERENCE and AREA are updated:

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 27 | RADIUS1 | 100 | HOLDING REGISTER | 16BIT SIGNED | 100 | - | 07/03/2019 11:15:56.934313 | NONE | NONE | CHANGE |
| 28 | RADIUS2 | 101 | HOLDING REGISTER | 16BIT SIGNED | 200 | - | 07/03/2019 11:35:39.122325 | NONE | NONE | CHANGE |
| 29 | CIRCUMFERENCE | 103 | HOLDING REGISTER | 32BIT REAL MSW | 1256 | - | 07/03/2019 11:35:43.55955 | NONE | NONE | CHANGE |
| 30 | AREA | 105 | HOLDING REGISTER | 32BIT REAL MSW | 125600 | - | 07/03/2019 11:35:43.56111 | NONE | NONE | CHANGE |

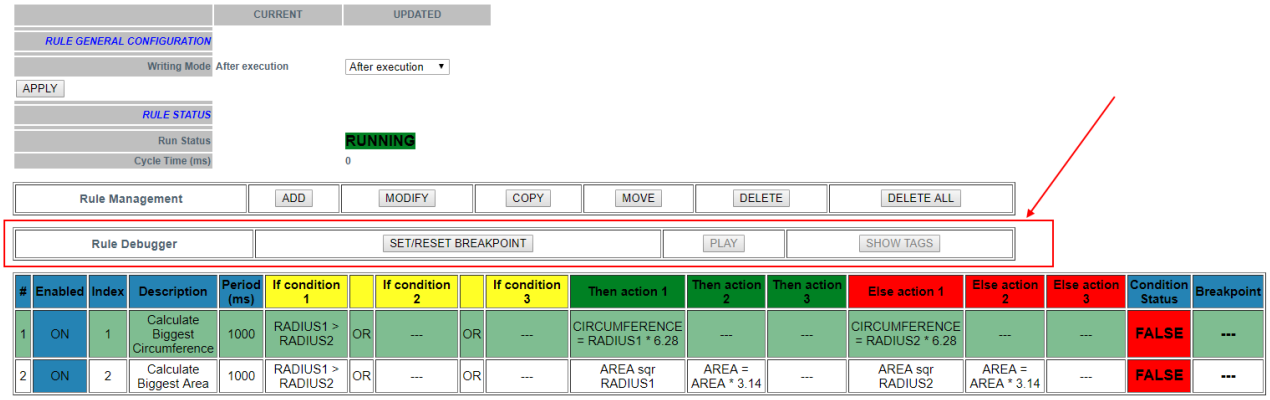
### *20.6.5.5 Debug the Example Program*

A program can be debugged by using the internal Rule debugger.

With the internal debugger you can:

-Insert a Breakpoint before the execution of a rule

-View the tag values before/after the execution of a rule



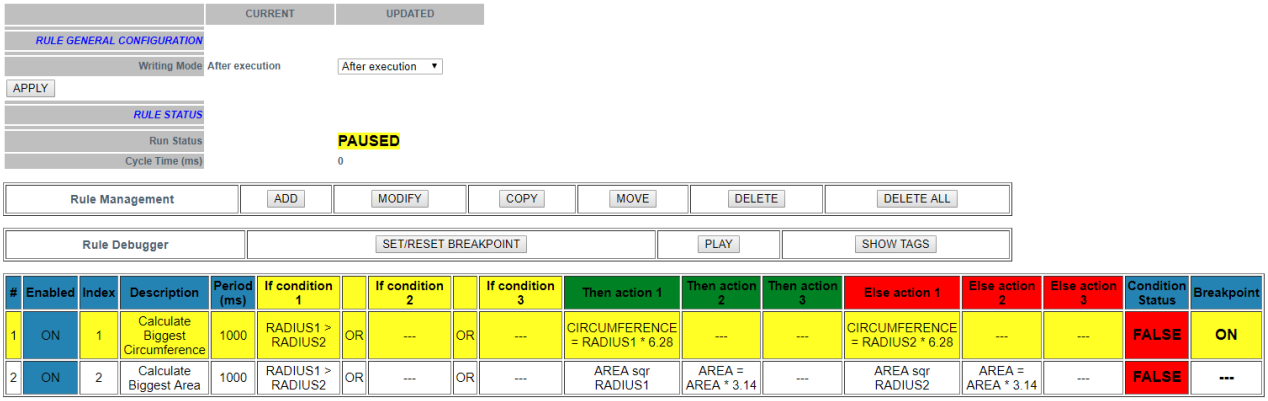
| | CURRENT | UPDATED |
|---|---|---|
| RULE GENERAL CONFIGURATION | | |
| Writing Mode | After execution | After execution |
| APPLY | | |
| RULE STATUS | | |
| Run Status | | RUNNING |
| Cycle Time (ms) | | 0 |

| Rule Management | ADD | MODIFY | COPY | MOVE | DELETE | DELETE ALL |
|---|---|---|---|---|---|---|

| Rule Debugger | SET/RESET BREAKPOINT | PLAY | SHOW TAGS |
|---|---|---|---|

| # | Enabled | Index | Description | Period (ms) | If condition 1 | | If condition 2 | | If condition 3 | Then action 1 | Then action 2 | Then action 3 | Else action 1 | Else action 2 | Else action 3 | Condition Status | Breakpoint |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ON | 1 | Calculate Biggest Circumference | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | CIRCUMFERENCE = RADIUS1 * 6.28 | --- | --- | CIRCUMFERENCE = RADIUS2 * 6.28 | --- | --- | FALSE | --- |
| 2 | ON | 2 | Calculate Biggest Area | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | AREA sqr RADIUS1 | AREA = AREA * 3.14 | --- | AREA sqr RADIUS2 | AREA = AREA * 3.14 | --- | FALSE | --- |

For adding a breakpoint select the a rule and then press the “SET/RESET BREAKPOINT”:



| | CURRENT | UPDATED |
|---|---|---|
| RULE GENERAL CONFIGURATION | | |
| Writing Mode | After execution | After execution |
| APPLY | | |
| RULE STATUS | | |
| Run Status | | PAUSED |
| Cycle Time (ms) | | 0 |

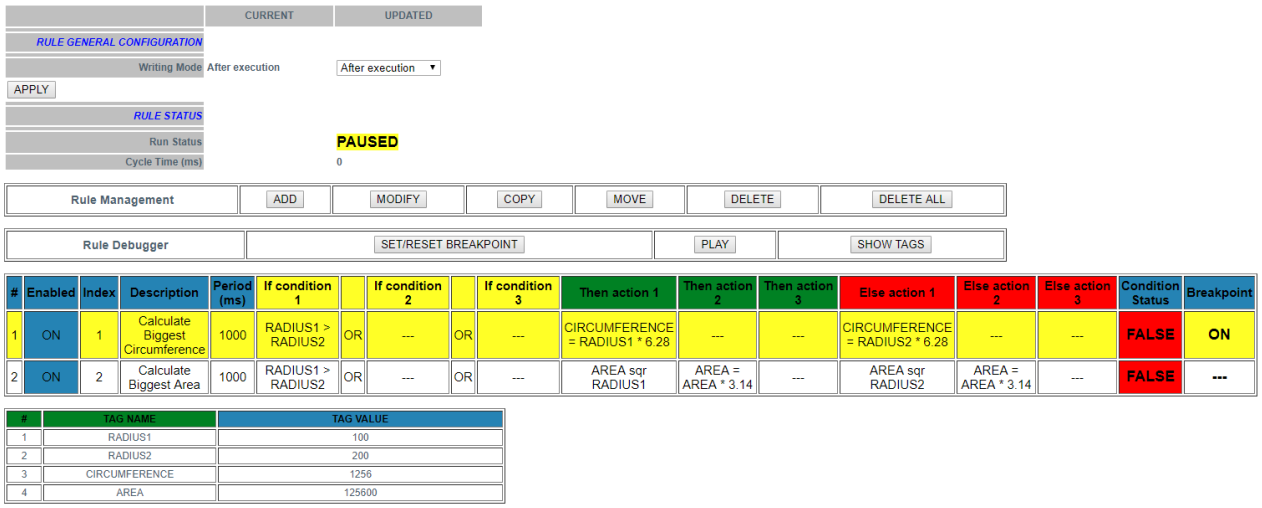
| Rule Management | ADD | MODIFY | COPY | MOVE | DELETE | DELETE ALL |
|---|---|---|---|---|---|---|

| Rule Debugger | SET/RESET BREAKPOINT | PLAY | SHOW TAGS |
|---|---|---|---|

| # | Enabled | Index | Description | Period (ms) | If condition 1 | | If condition 2 | | If condition 3 | Then action 1 | Then action 2 | Then action 3 | Else action 1 | Else action 2 | Else action 3 | Condition Status | Breakpoint |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ON | 1 | Calculate Biggest Circumference | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | CIRCUMFERENCE = RADIUS1 * 6.28 | --- | --- | CIRCUMFERENCE = RADIUS2 * 6.28 | --- | --- | FALSE | ON |
| 2 | ON | 2 | Calculate Biggest Area | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | AREA sqr RADIUS1 | AREA = AREA * 3.14 | --- | AREA sqr RADIUS2 | AREA = AREA * 3.14 | --- | FALSE | --- |

The rule became yellow and the rule status change in “paused”. Note that the breakpoint is ***before*** the execution of the rule.

By clicking on “Show tags” the actual tags values are displayed:



| | CURRENT | UPDATED |
|---|---|---|
| RULE GENERAL CONFIGURATION | | |
| Writing Mode | After execution | After execution |
| APPLY | | |
| RULE STATUS | | |
| Run Status | | PAUSED |
| Cycle Time (ms) | | 0 |

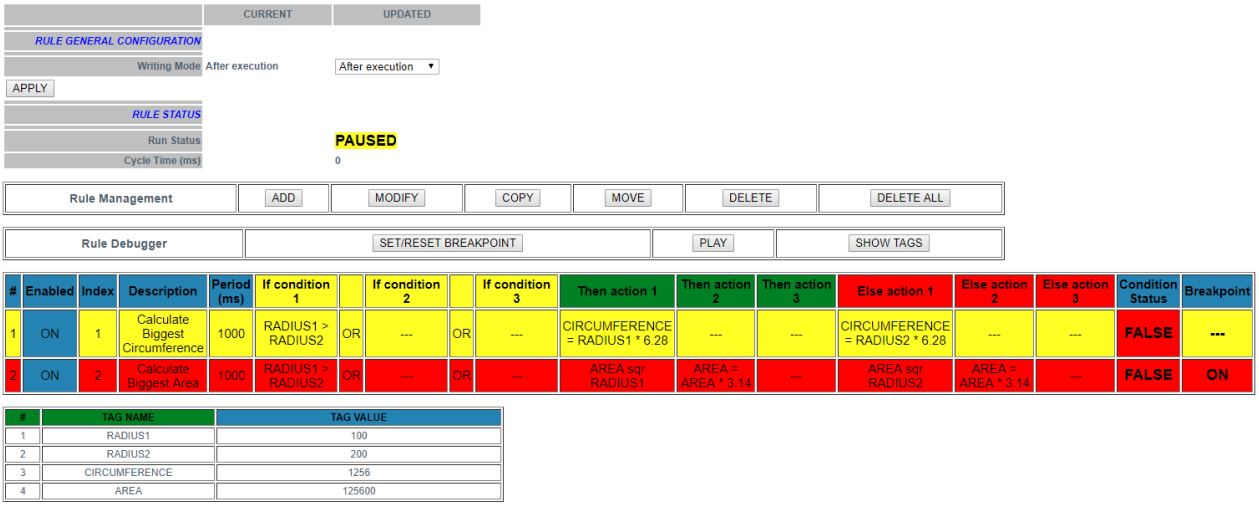
| Rule Management | ADD | MODIFY | COPY | MOVE | DELETE | DELETE ALL |
|---|---|---|---|---|---|---|

| Rule Debugger | SET/RESET BREAKPOINT | PLAY | SHOW TAGS |
|---|---|---|---|

| # | Enabled | Index | Description | Period (ms) | If condition 1 | | If condition 2 | | If condition 3 | Then action 1 | Then action 2 | Then action 3 | Else action 1 | Else action 2 | Else action 3 | Condition Status | Breakpoint |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ON | 1 | Calculate Biggest Circumference | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | CIRCUMFERENCE = RADIUS1 * 6.28 | --- | --- | CIRCUMFERENCE = RADIUS2 * 6.28 | --- | --- | FALSE | ON |
| 2 | ON | 2 | Calculate Biggest Area | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | AREA sqr RADIUS1 | AREA = AREA * 3.14 | --- | AREA sqr RADIUS2 | AREA = AREA * 3.14 | --- | FALSE | --- |

| # | TAG NAME | TAG VALUE |
|---|---|---|
| 1 | RADIUS1 | 100 |
| 2 | RADIUS2 | 200 |
| 3 | CIRCUMFERENCE | 1256 |
| 4 | AREA | 125600 |

Now you can move the breakpoint to the following rule, select the next rule and press the “SET/RESET BREAKPOINT” button:



| | CURRENT | UPDATED |
|---|---|---|
| RULE GENERAL CONFIGURATION | | |
| Writing Mode | After execution | After execution |
| APPLY | | |
| RULE STATUS | | |
| Run Status | | PAUSED |
| Cycle Time (ms) | | 0 |

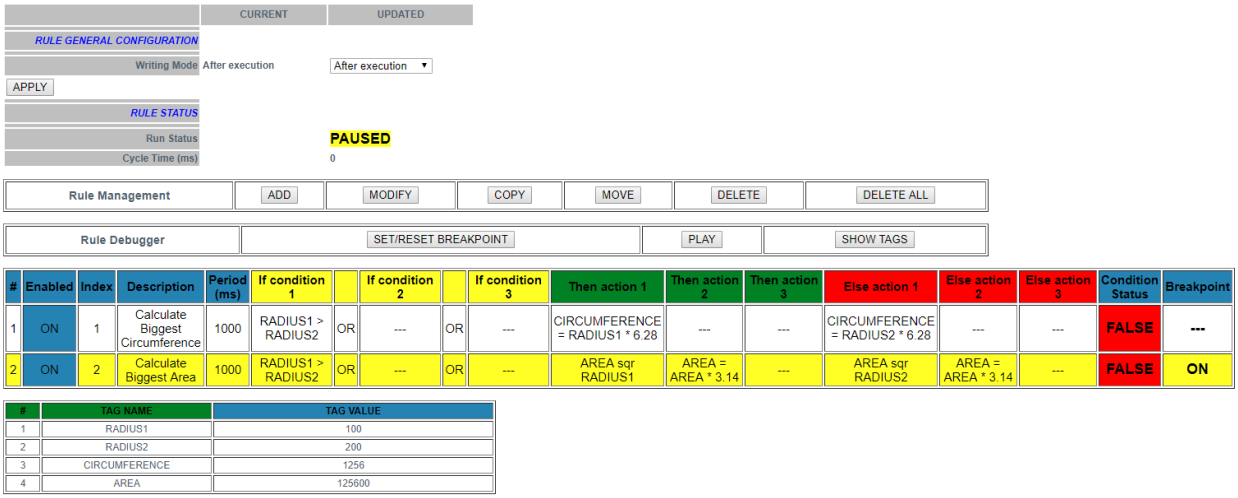
| Rule Management | ADD | MODIFY | COPY | MOVE | DELETE | DELETE ALL |
|---|---|---|---|---|---|---|

| Rule Debugger | SET/RESET BREAKPOINT | PLAY | SHOW TAGS |
|---|---|---|---|

| # | Enabled | Index | Description | Period (ms) | If condition 1 | | If condition 2 | | If condition 3 | Then action 1 | Then action 2 | Then action 3 | Else action 1 | Else action 2 | Else action 3 | Condition Status | Breakpoint |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ON | 1 | Calculate Biggest Circumference | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | CIRCUMFERENCE = RADIUS1 * 6.28 | --- | --- | CIRCUMFERENCE = RADIUS2 * 6.28 | --- | --- | FALSE | --- |
| 2 | ON | 2 | Calculate Biggest Area | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | AREA sqr RADIUS1 | AREA = AREA * 3.14 | --- | AREA sqr RADIUS2 | AREA = AREA * 3.14 | --- | FALSE | ON |

| # | TAG NAME | TAG VALUE |
|---|---|---|
| 1 | RADIUS1 | 100 |
| 2 | RADIUS2 | 200 |
| 3 | CIRCUMFERENCE | 1256 |
| 4 | AREA | 125600 |

Note that the execution is pause because you must press “PLAY” for advance to the next breakpoint, press “PLAY”:



| | CURRENT | UPDATED |
|---|---|---|
| RULE GENERAL CONFIGURATION | | |
| Writing Mode | After execution | After execution |
| APPLY | | |
| RULE STATUS | | |
| Run Status | | PAUSED |
| Cycle Time (ms) | | 0 |

| Rule Management | ADD | MODIFY | COPY | MOVE | DELETE | DELETE ALL |
|---|---|---|---|---|---|---|

| Rule Debugger | SET/RESET BREAKPOINT | PLAY | SHOW TAGS |
|---|---|---|---|

| # | Enabled | Index | Description | Period (ms) | If condition 1 | | If condition 2 | | If condition 3 | Then action 1 | Then action 2 | Then action 3 | Else action 1 | Else action 2 | Else action 3 | Condition Status | Breakpoint |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ON | 1 | Calculate Biggest Circumference | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | CIRCUMFERENCE = RADIUS1 * 6.28 | --- | --- | CIRCUMFERENCE = RADIUS2 * 6.28 | --- | --- | FALSE | --- |
| 2 | ON | 2 | Calculate Biggest Area | 1000 | RADIUS1 > RADIUS2 | OR | --- | OR | --- | AREA sqr RADIUS1 | AREA = AREA * 3.14 | --- | AREA sqr RADIUS2 | AREA = AREA * 3.14 | --- | FALSE | ON |

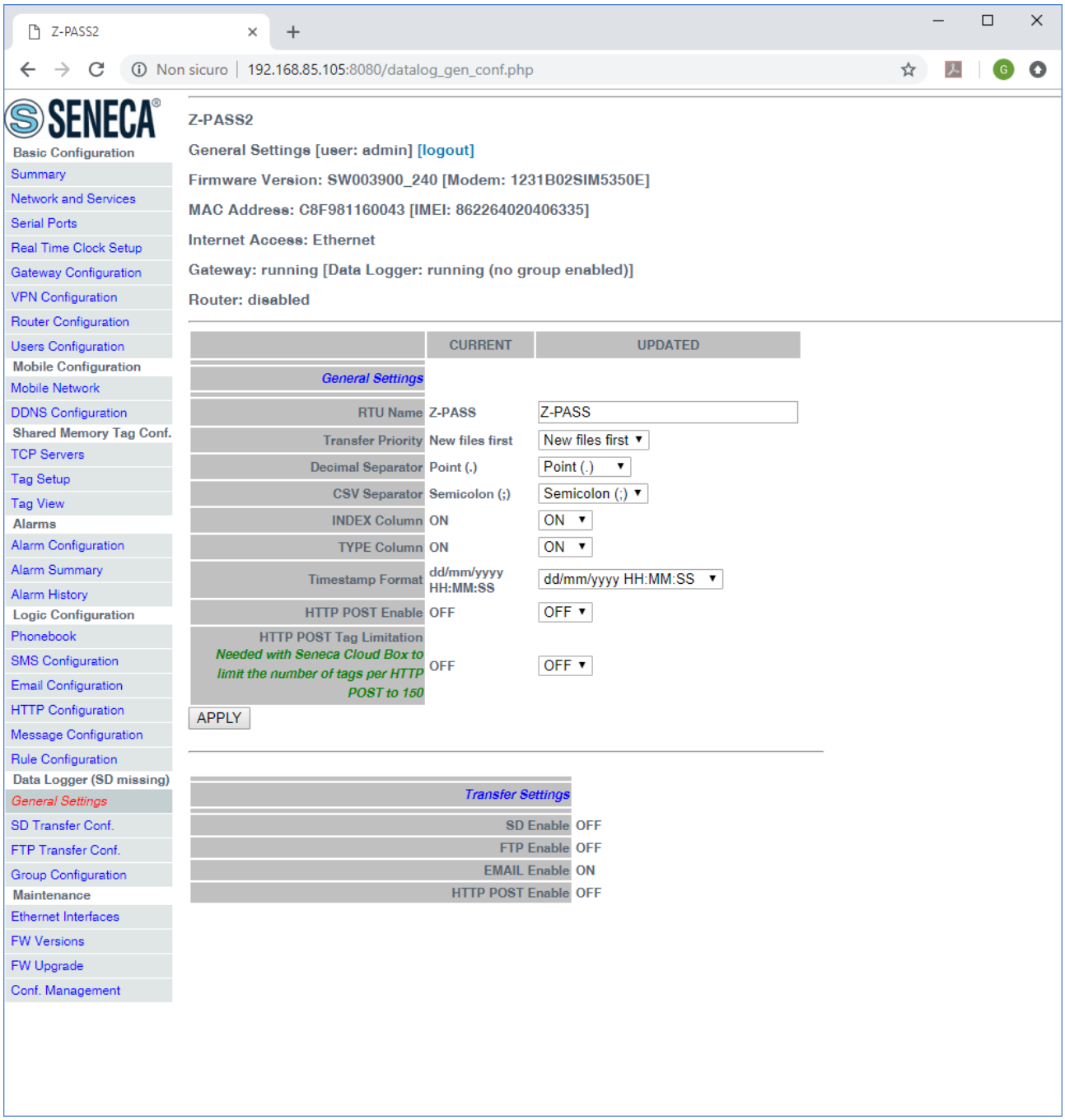
| # | TAG NAME | TAG VALUE |
|---|---|---|
| 1 | RADIUS1 | 100 |
| 2 | RADIUS2 | 200 |
| 3 | CIRCUMFERENCE | 1256 |
| 4 | AREA | 125600 |

The execution is stopped before the Rule nr 2.

## 20.7 Data Logger

### 20.7.1 General Settings

By clicking on the “General Settings” link, in the “Data Logger” section, you come to the following page:




In the “General Settings” section, this page contains the general parameters related to the Data Logger functionality, as listed in the following table.

| Field | Meaning | Default value |
|---|---|---|
| RTU Name | Name identifying the Z-PASS device.<br>It is used in log file names, transferred via FTP or sent as email attachments | Z-PASS |
| Transfer Priority | This field tells if newer or older log files shall be transferred first. | New files first |

| | | |
|---|---|---|
| | Possible values are:<br>- Old files first<br>- New files first | |
| Decimal separator | Character used as decimal separator for floating point values in log files.<br>Possible values are:<br>- Point (.)<br>- Comma (,) | Point (.) |
| CSV Separator | Character used as field separator in *csv* log files.<br>Possible values are:<br>- Semicolon (;)<br>- Point (.)<br>- Blank ( ) | Semicolon (;) |
| INDEX Column | Flag telling if the "INDEX" column, containing the line (sample) progressive index, shall be present in the log files or not | ON |
| TYPE Column | Flag telling if the "TYPE" column, containing the line (sample) type, shall be present in the log files or not.<br>NOTE: currently, this column always contains the "LOG" string | ON |
| Timestamp Format | Format of the timestamp value in the "TIMESTAMP" column.<br>Possible formats are:<br>dd/mm/yyyy HH:MM:SS<br>yyyy/mm/dd HH:MM:SS<br>dd/mm/yy HH:MM:SS<br>yy/mm/dd HH:MM:SS<br>seconds since the Epoch | dd/mm/yyyy HH:MM:SS |
| HTTP POST Enable | Flag to enable/disable the HTTP POST protocol (see paragraph 9.1) | OFF |
| HTTP POST Tag Limitation | When this parameter is set to ON, the HTTP POST requests contain a maximum of 150 tags, even if Group 1 contains a larger number of tags; conversely, when it is set to OFF, the HTTP POST requests contain all the Group 1 tags.<br>This limitation is needed when using the Z-PASS with the Seneca Cloud Box product. | OFF |

Please note that, when the "HTTP POST Enable" parameter is changed from OFF to ON, the following changes are also automatically applied:

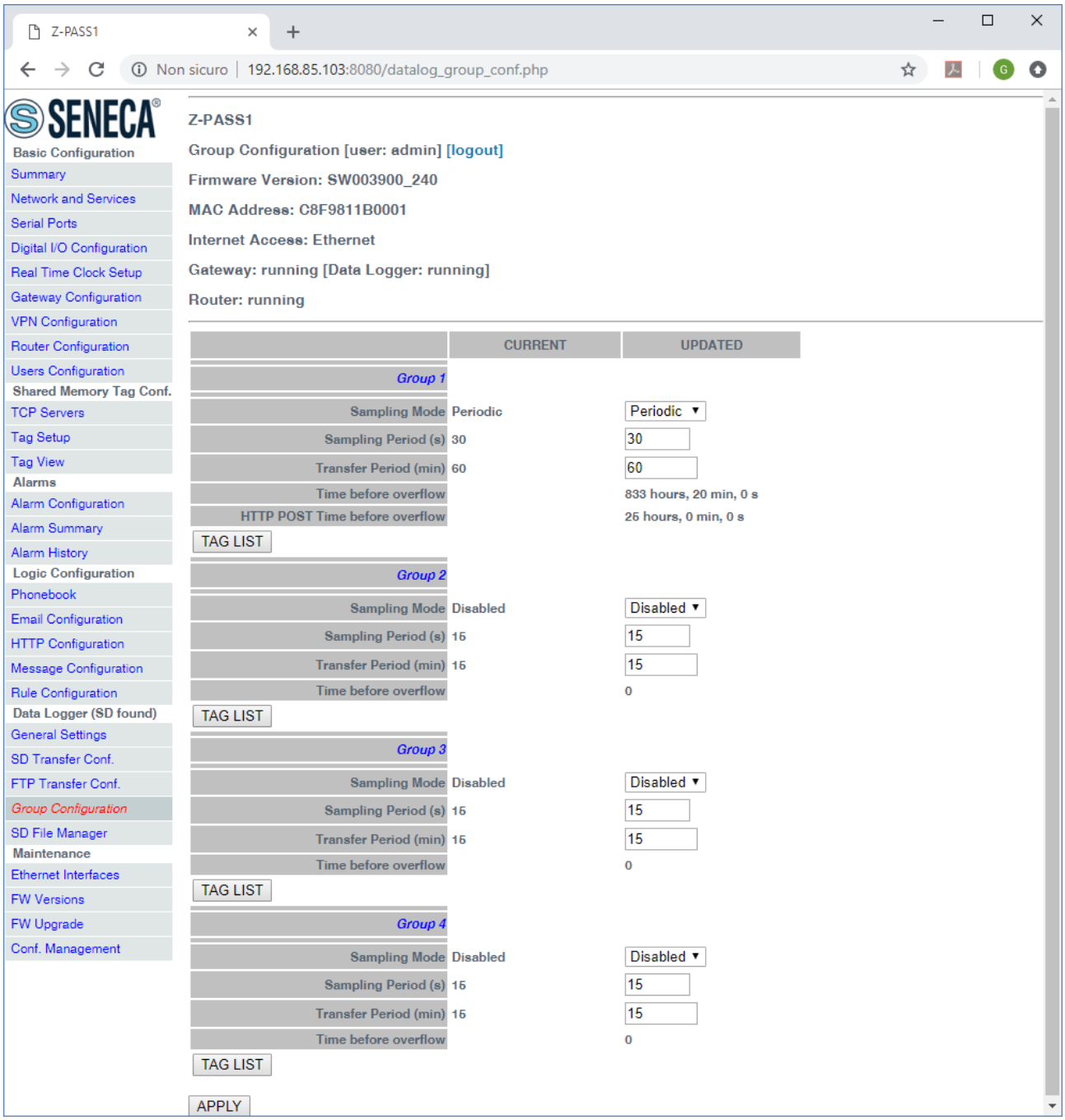
- the “Enable” parameter in the “HTTP POST Configuration” page is set to ON;
- the “Sampling Mode” parameter for all the groups in the “Group Configuration” page is set to Disabled; then, it can be changed only for Group 1;
- the “Sampling Period” parameter for Group 1 in the “Group Configuration” page shall be a multiple of 30 (seconds).

In the “Transfer Settings” section, the “enable” (OFF/ON) status for all the transfer methods is shown.

Note that from release FW SW00390_297 it’s also possible to use the Datalogger on trigger feature. In this mode the data acquisition it’s made only when a rule command it’s “TRIGGER LOG” (see Logic Configuration).

### *20.7.2 Group Configuration*

By clicking on the “Group Configuration” link, in the “Data Logger” section, you come to the following page:




The page contains four sections, one for each Data Logger group.

Each section contains the parameters described in the following table.

| Field | Meaning | Default value |
|---|---|---|
| Sampling Mode | Since, currently, the only supported sampling mode is “Periodic”, this parameter is actually a flag used to enable (“Periodic”) or disable (“Disabled”) the group. | Disabled |

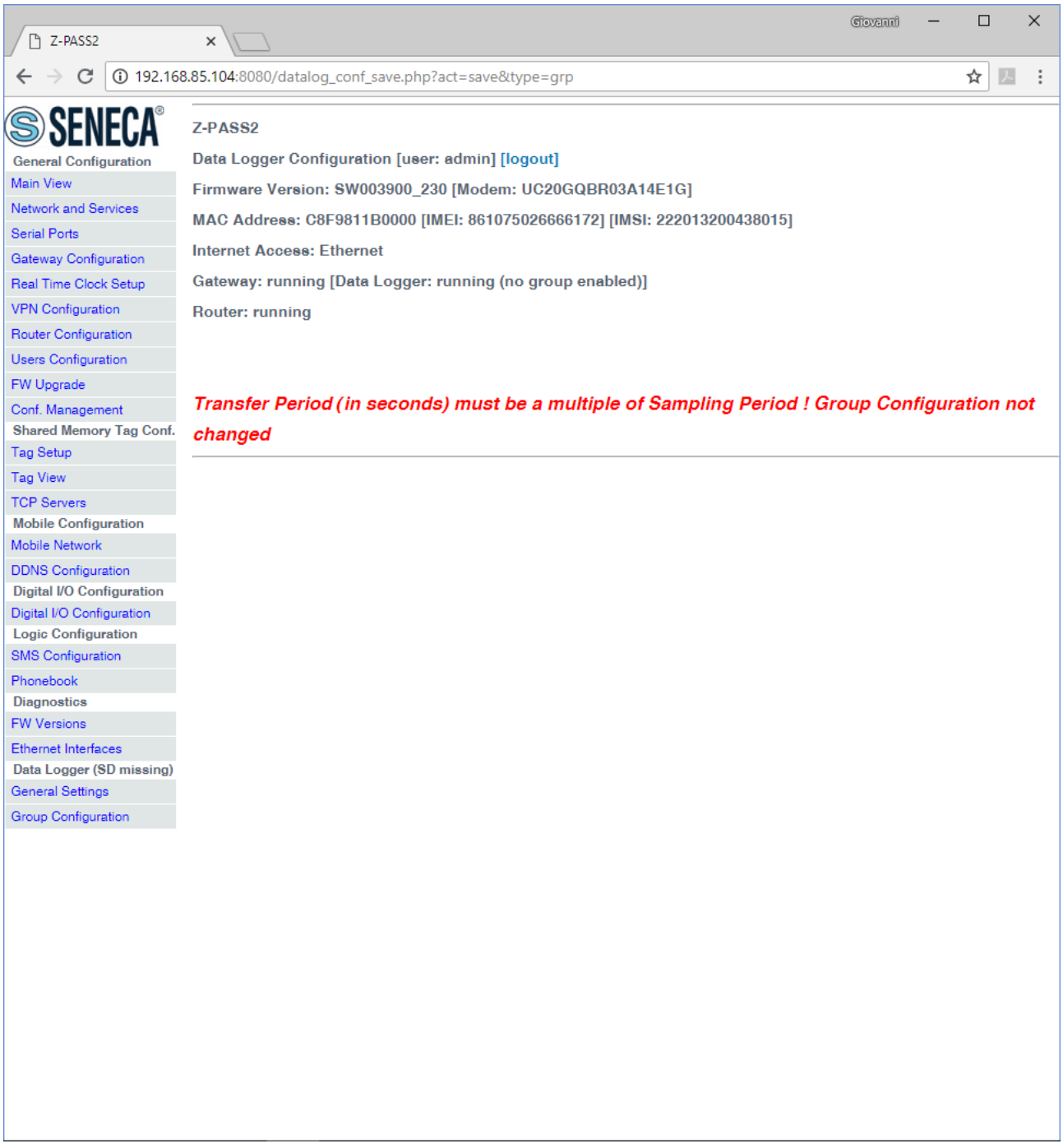
| | | |
|---|---|---|
| Sampling Period (s) | This parameter defines the sampling period, in seconds.<br>Minimum: 1, Maximum: 7200 | 15 |
| Transfer Period (min) | This parameter defines the transfer period, in minutes; that is every time interval defined by this parameter the log file is closed and transferred.<br>Minimum: 1, Maximum: 43200 | 15 |

For any group with “Sampling Mode” set to “Periodic”, the “Time before overflow” information is given; this is the time (given in hour, minutes, seconds) after which the oldest log files will be overwritten by the new files; in other words, this value represents the time interval during which Z-PASS can store data samples, before data loss occurs.

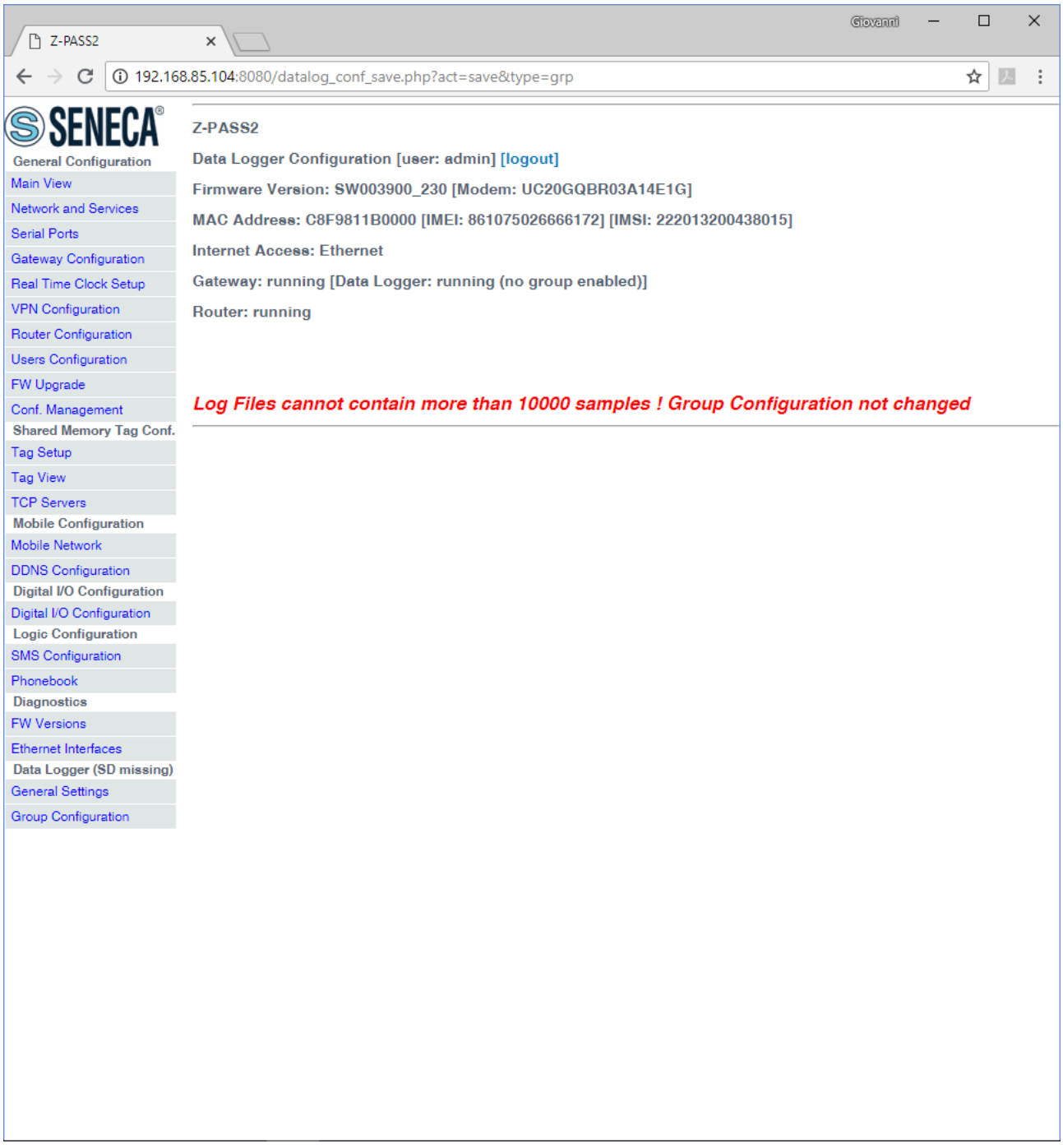
If “HTTP POST Enable” is set to ON, for Group 1 with “Sampling Mode” set to “Periodic”, also the “HTTP POST Time before overflow” is given, which is the same concept of “Time before overflow” applied to data samples sent via HTTP POST.

It should be noticed that the values of the “Sampling Period” and “Transfer Period” parameters determine the maximum number of lines (samples) in a log file.

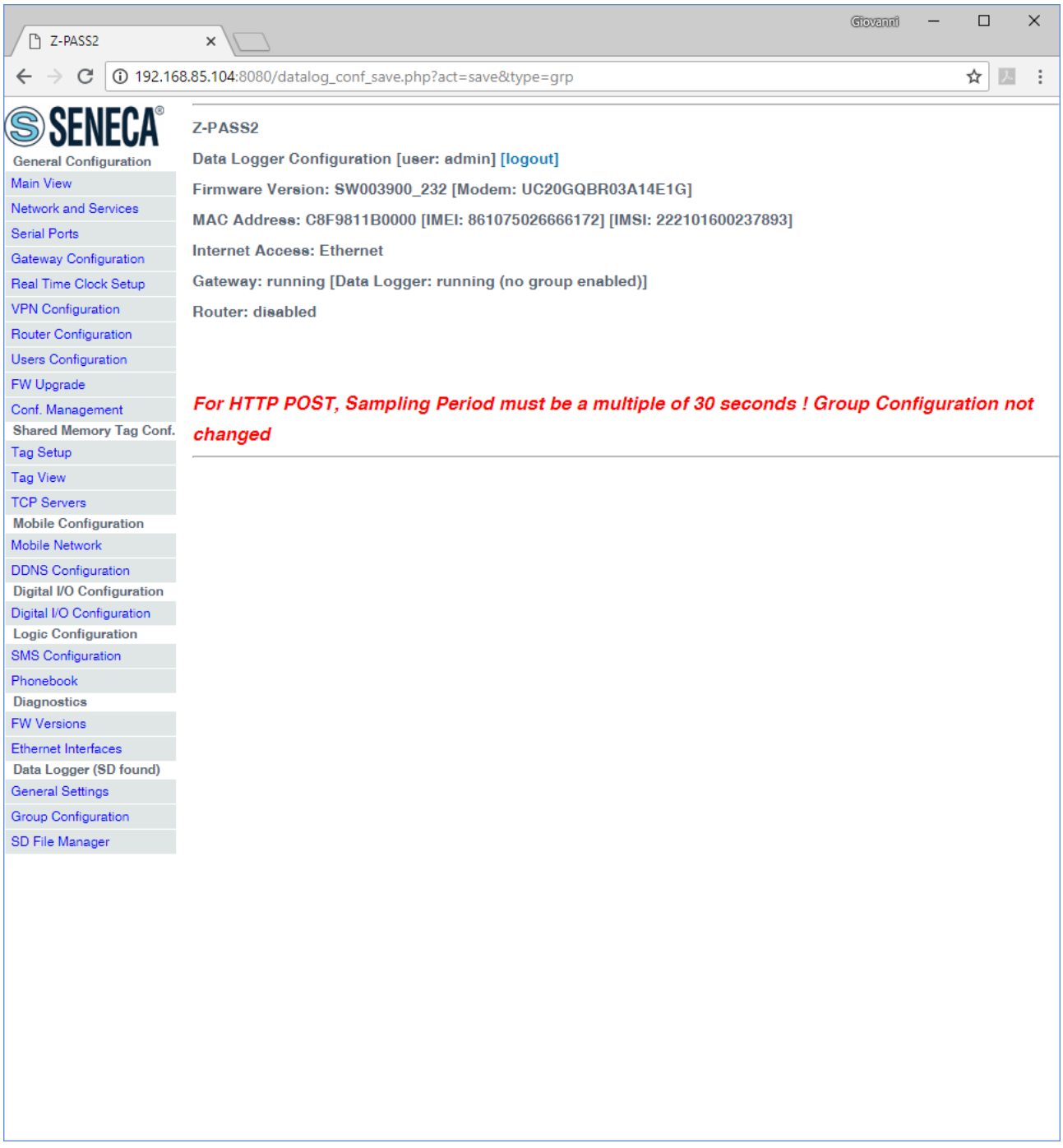
The “Transfer Period” (in seconds) shall be a multiple of the “Sampling Period”: if this condition is not satisfied the following error message is shown:




To prevent creating log files that are too large to store and transfer, a maximum number of 10000 lines (samples) per log file has been set; if the “Sampling Period” and “Transfer Period” values are such that this limit is overcome, the following error message is shown.




When HTTP POST protocol is enabled and the Group 1 Sampling Mode parameter is set to a value that is not a multiple of 30, the following error message is shown.




If the Data Logger is running but no group is enabled, the Data Logger status in the page headers is reported as:

*[Data Logger: running (no group enabled)]*

Instead, if the Data Logger is running and at least one group is enabled, the Data Logger status in the page headers is reported as:

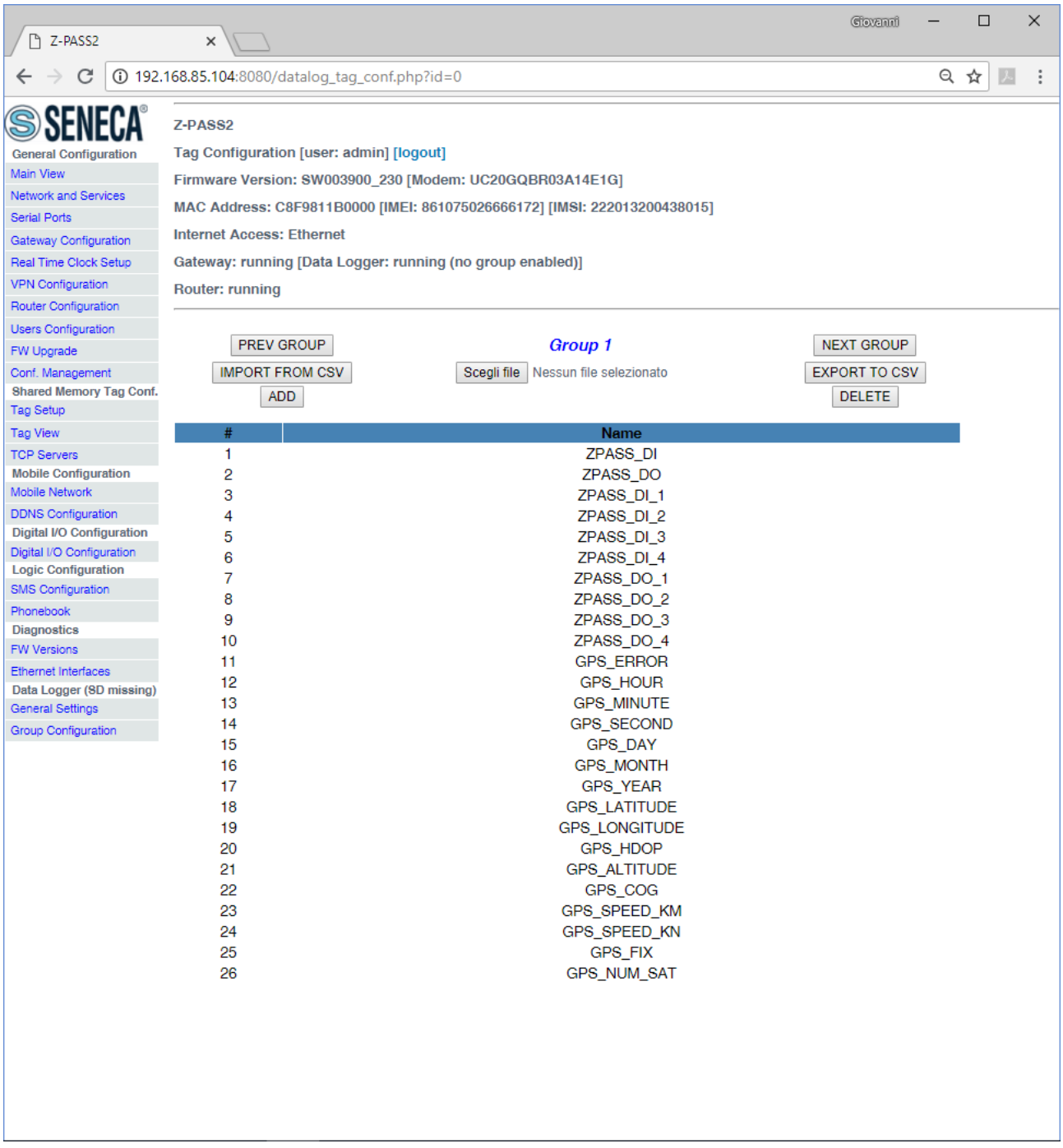
*[Data Logger: running]*

The Data Logger implementation is such that a log file is closed and transferred when the current date-time in seconds is a multiple of the “Transfer Period“ in seconds; so, for example, if the “Transfer Period“ is set to 60 (1 hour), the log files are closed and transferred at the beginning of each hour (00:00, 01:00, 02:00 etc.); obviously, if the Data Logger is started after the beginning of the current hour, the first log file will contain less lines that the expected number.

For enabled groups, the log files are closed and transferred, regardless of the transfer period, also in the following situations:

- if any change to Data Logger configuration parameters is applied;
- if Data Logger is stopped and restarted.

Each group section contains a button named “TAG LIST”; by clicking on this button, you come to a page like the following:




In this page, the list of the Modbus Shared Memory Gateway tags associated to the group (Group 1, in the above figure) is shown.

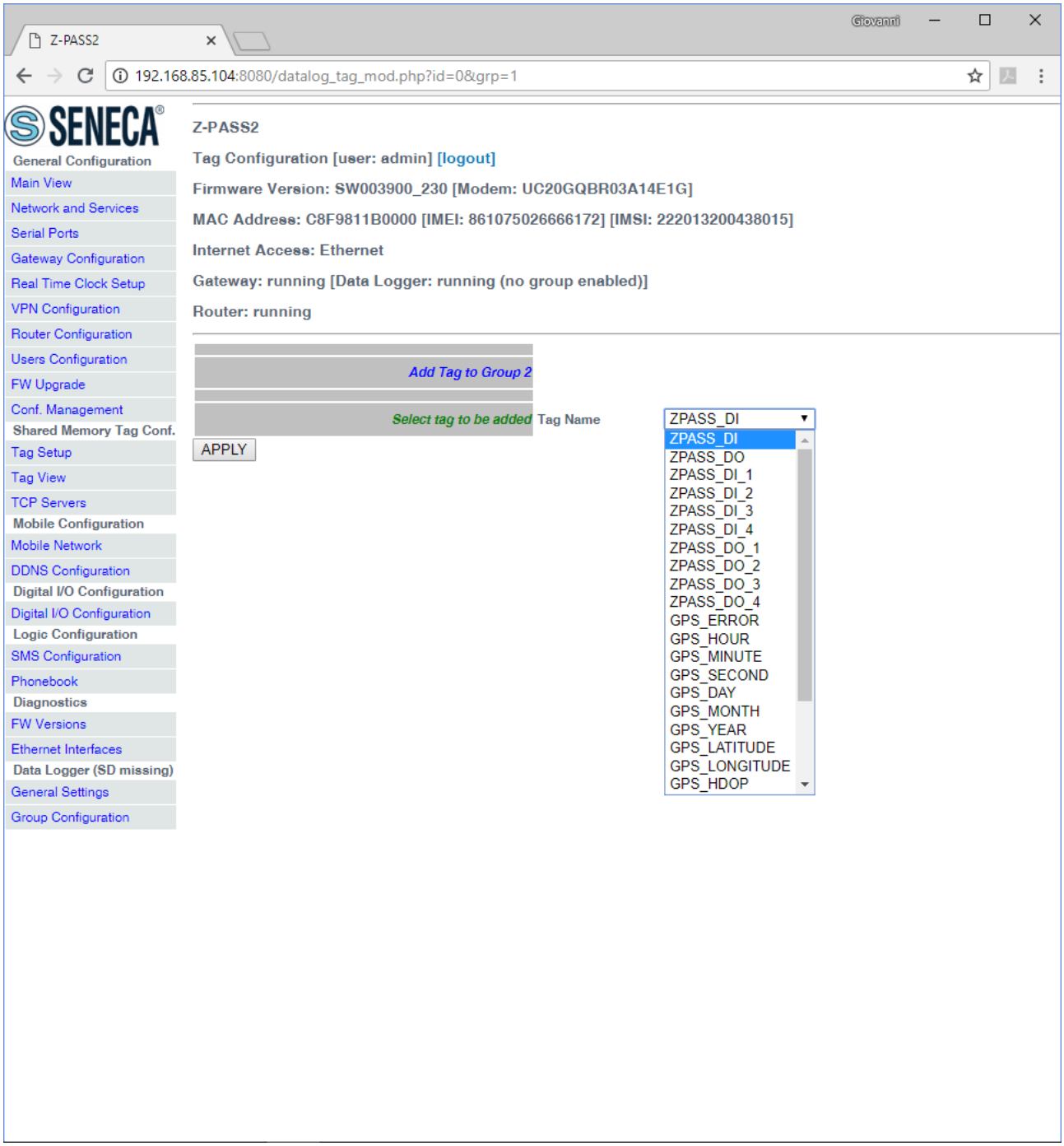
Please note that the order of the tags in the list corresponds to the order of the tag columns in the log files.

In this page, you can:

- select a tag and delete it (that is de-associate it from the group), by means of the “DELETE” button

- export the tag list to a csv file (actually, containing a single column, that is the tag names), by means of the "EXPORT TO CSV" button; by default, the name of the exported file is: *zpass_dl_tags_X.csv*, where X=[1..4] is the group number)
- importing the tag list from a csv file, by means of the "IMPORT FROM CSV" button
- go to the next/previous group, by means of the "NEXT GROUP"/"PREV GROUP" button

Finally, by clicking on the "ADD" button, you come to a page like the following.




In this page, the list of the tags not associated to the group is shown.

By selecting a tag and clicking on the “APPLY” button, the tag is added to the group.

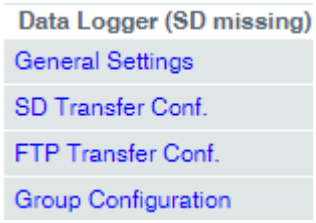
It is important to highlight some points about the association between tags and groups:

- a tag can be associated to more than one group;
- when a tag is added, in the “Tag Setup” page, it is automatically added to Group 1;
- when a tag is deleted, in the “Tag Setup” page, it is automatically deleted from all the groups;
- when a tag name is changed, in the “Tag Setup” page, it is automatically changed in all the groups which contain it;
- when the tag configuration is imported from a “cgi” file, in the “Tag Setup” page, the tag list is cleaned for all the groups and all imported tags are associated to Group 1.

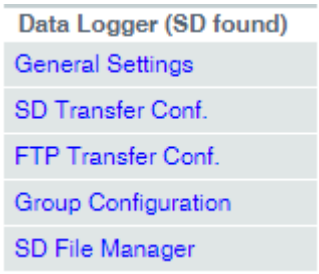
Finally, it is useful to note that a very fast and simple way to modify the tag list for the groups (e.g., to change the tag order) is to export the list, modify it and then import it.

### *20.7.3 SD File Manager*

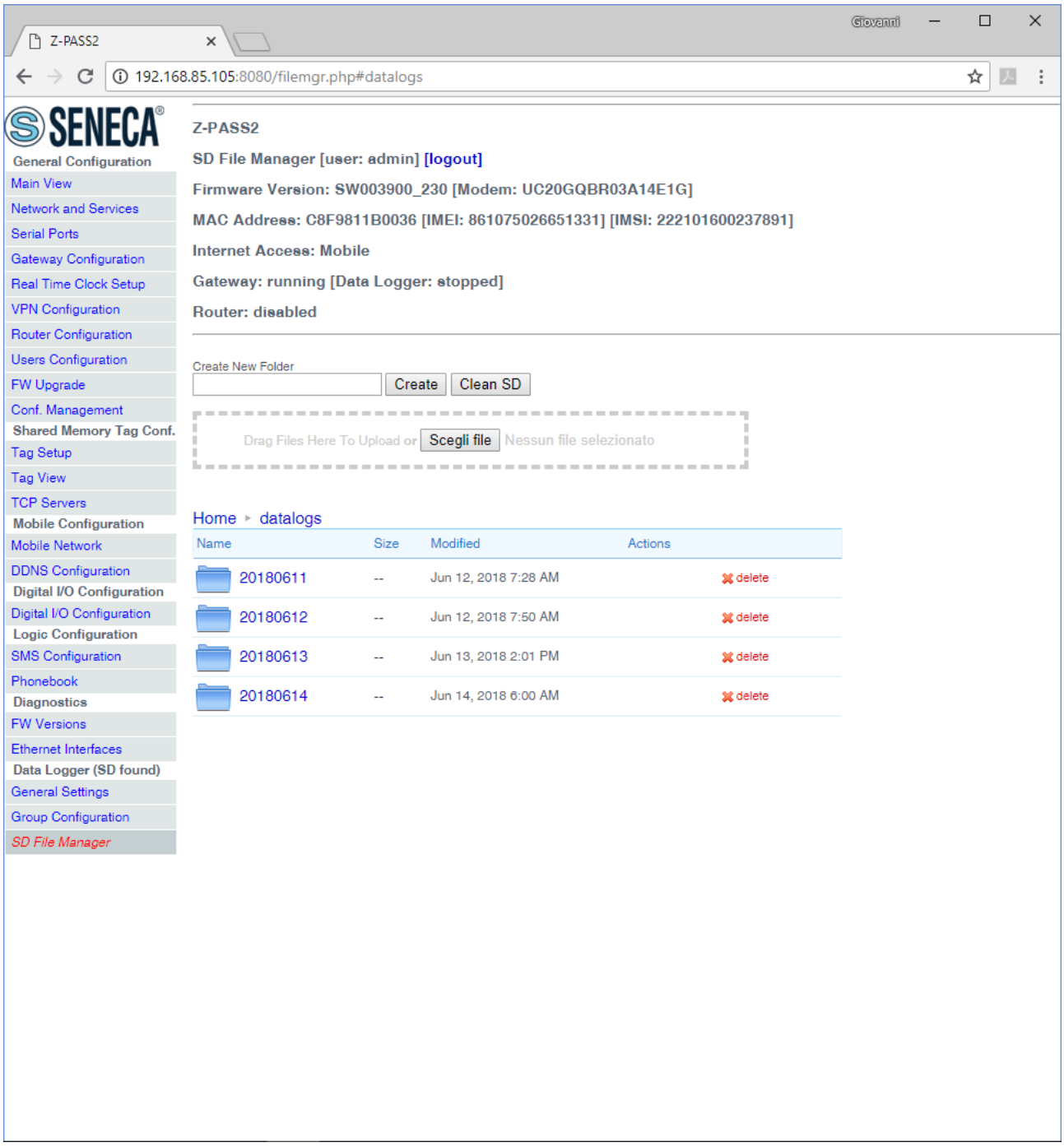
If the SD Card is not inserted in the Z-PASS, the “Data Logger” section of the web pages menu is like the following:

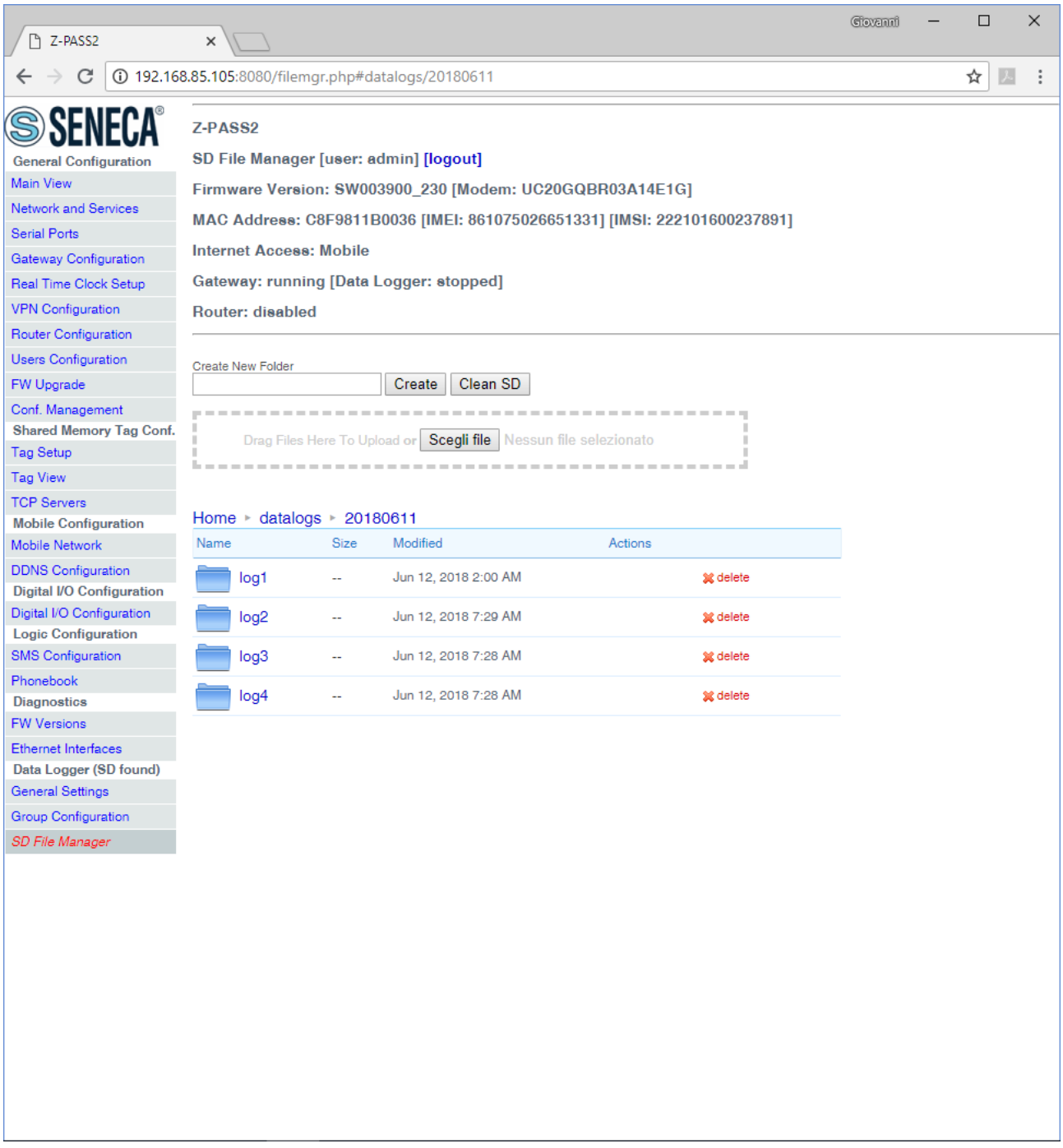



When the SD Card is inserted in the Z-PASS, the “Data Logger” section of the web pages menu becomes:




By clicking on the “SD File Manager” link, you come to the following page:


Giovanni
Z-PASS2
192.168.85.105:8080/filemgr.php#datalogs
SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
TCP Servers
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O Configuration
Digital I/O Configuration
Logic Configuration
SMS Configuration
Phonebook
Diagnostics
FW Versions
Ethernet Interfaces
Data Logger (SD found)
General Settings
Group Configuration
SD File Manager
Z-PASS2
SD File Manager [user: admin] [logout]
Firmware Version: SW003900_230 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0036 [IMEI: 861075026651331] [IMSI: 222101600237891]
Internet Access: Mobile
Gateway: running [Data Logger: stopped]
Router: disabled
Create New Folder
Create
Clean SD
Drag Files Here To Upload or
Scegli file
Nessun file selezionato
Home ▸ datalogs
Name
Size
Modified
Actions
20180611 -- Jun 12, 2018 7:28 AM delete
20180612 -- Jun 12, 2018 7:50 AM delete
20180613 -- Jun 13, 2018 2:01 PM delete
20180614 -- Jun 14, 2018 6:00 AM delete


Giovanni
Z-PASS2
192.168.85.105:8080/filemgr.php#datalogs/20180611
SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
TCP Servers
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O Configuration
Digital I/O Configuration
Logic Configuration
SMS Configuration
Phonebook
Diagnostics
FW Versions
Ethernet Interfaces
Data Logger (SD found)
General Settings
Group Configuration
SD File Manager
Z-PASS2
SD File Manager [user: admin] [logout]
Firmware Version: SW003900_230 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0036 [IMEI: 861075026651331] [IMSI: 222101600237891]
Internet Access: Mobile
Gateway: running [Data Logger: stopped]
Router: disabled
Create New Folder
Create
Clean SD
Drag Files Here To Upload or
Scegli file
Nessun file selezionato
Home ▸ datalogs ▸ 20180611
Name
Size
Modified
Actions
log1 -- Jun 12, 2018 2:00 AM delete
log2 -- Jun 12, 2018 7:29 AM delete
log3 -- Jun 12, 2018 7:28 AM delete
log4 -- Jun 12, 2018 7:28 AM delete


This page shows the contents of the SD card which, typically, is used to store the data log files.

The page lets you perform the following operations:

- browse the SD folder tree, clicking on the folder name links
- delete a folder, clicking on the “delete” link
- create a new folder, by means of the “Create New Folder” text-box and “Create” button; the new folder is created in the folder currently shown
- download a file, clicking on the filename link or on the “download” link

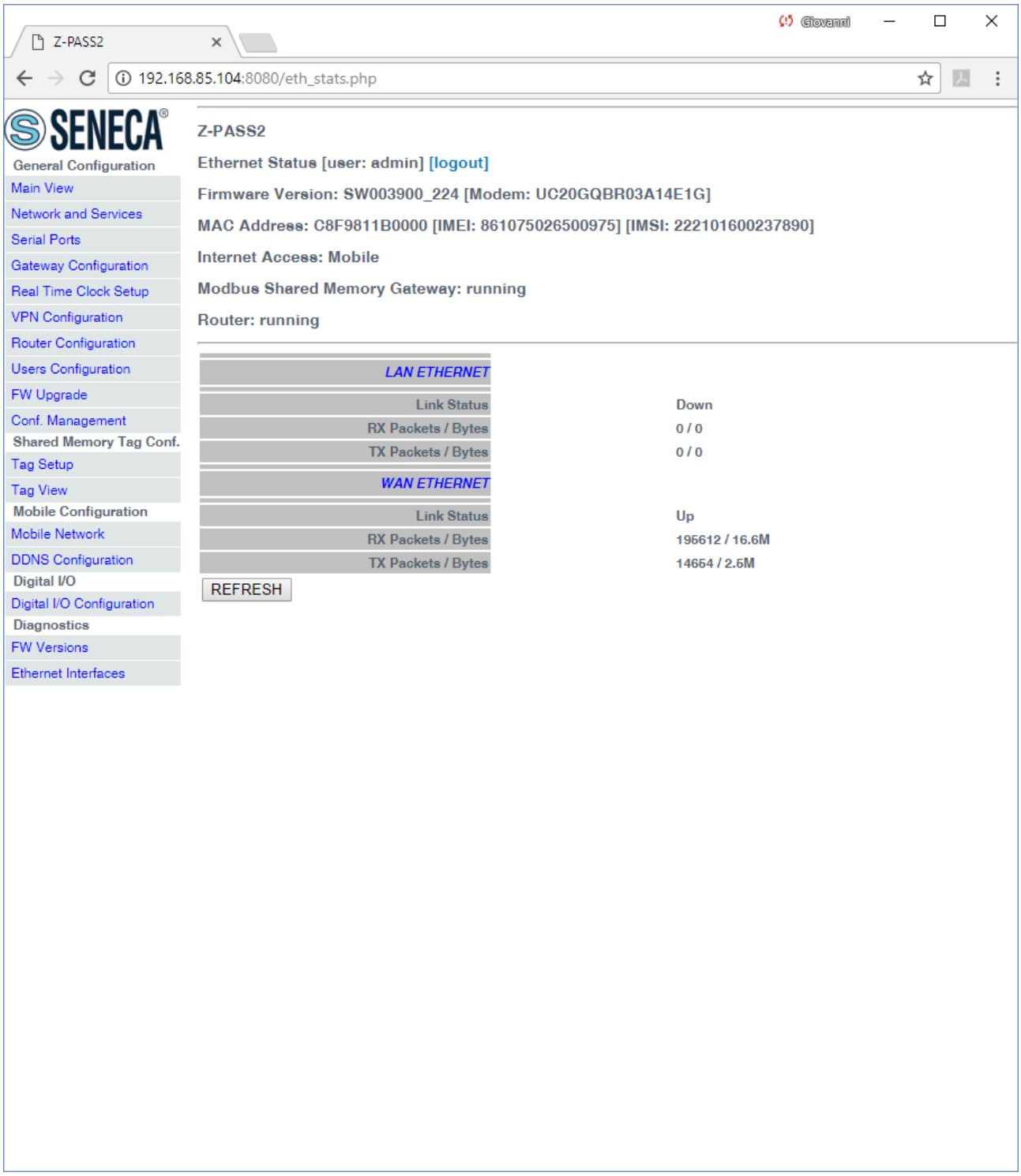
- delete a file, clicking on the “delete” link
- uploading a file, selecting it by means of the “Choose file” button or dragging it into the dashed area; the file is created in the folder currently shown
- clean the SD, by means of the “Clean SD” button; please note that this is done by formatting the SD, so all SD contents will be lost

Please note that the “guest” user (see 20.8.3 paragraph) cannot access the “SD File Manager” page.

## *20.8 Maintenance*

### *20.8.1 Ethernet Interfaces*

By clicking on the “Ethernet Interfaces” link, in the “Maintenance” section, you come to the following page:



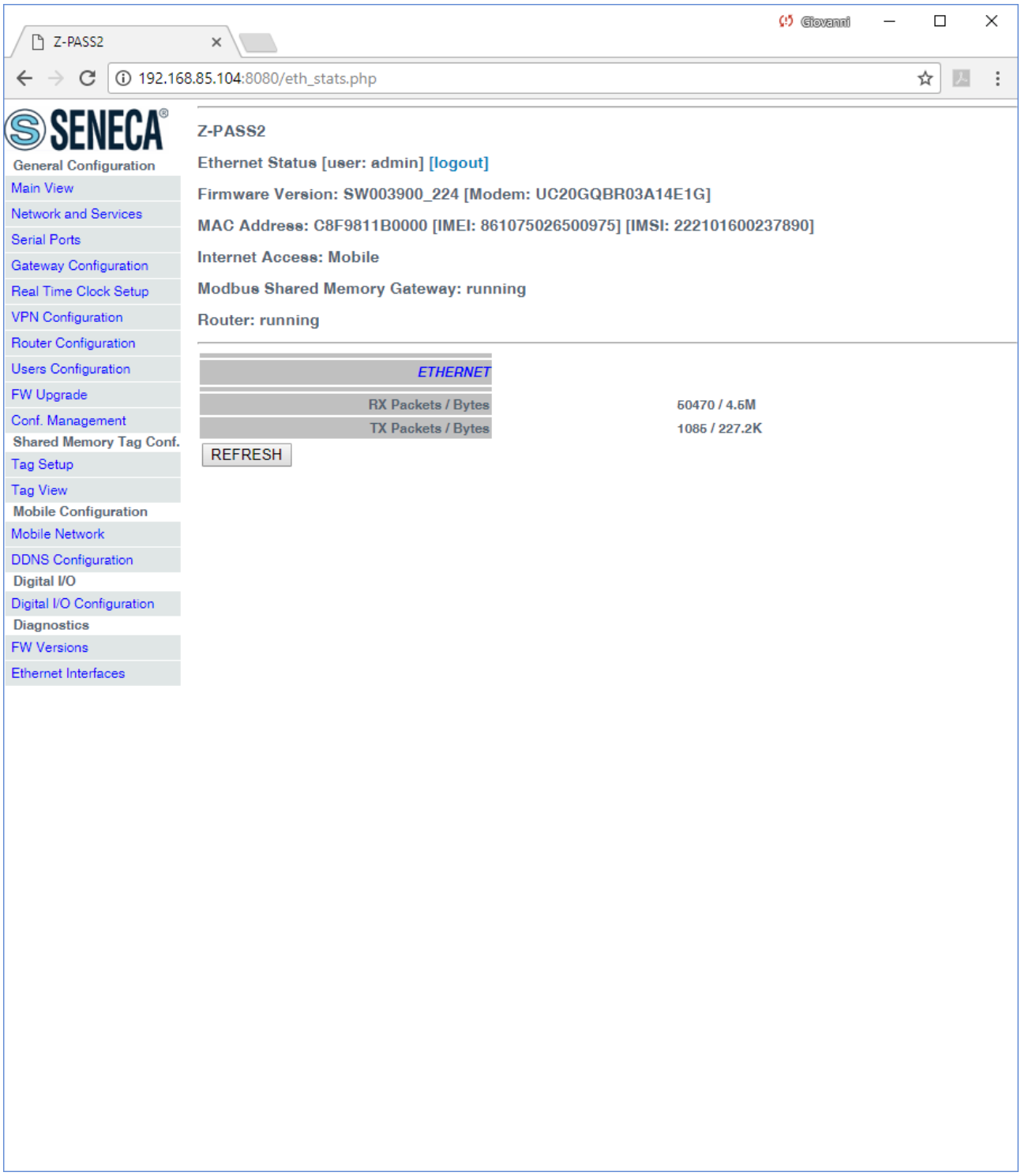

The above figure applies to a Z-PASS2, when the “Ethernet Mode” is “LAN/WAN.

In this page, for each of the two available Ethernet interfaces (LAN and WAN), the following information is shown:

- the Ethernet link status (i.e. “Down” or “Up”)

- the number of packets/bytes received from the Ethernet interface, when the link is up; “0/0” when the link is down
- the number of packets/bytes sent to the Ethernet interface, when the link is up; “0/0” when the link is down

For Z-PASS1, Z-PASS2 when the “Ethernet Mode” is “Switch”, the “Ethernet Interfaces” page is similar to the one shown in the following figure.




In this page, for the one available Ethernet interface, the following information is shown:

- the number of packets/bytes received from the Ethernet interface
- the number of packets/bytes sent to the Ethernet interface

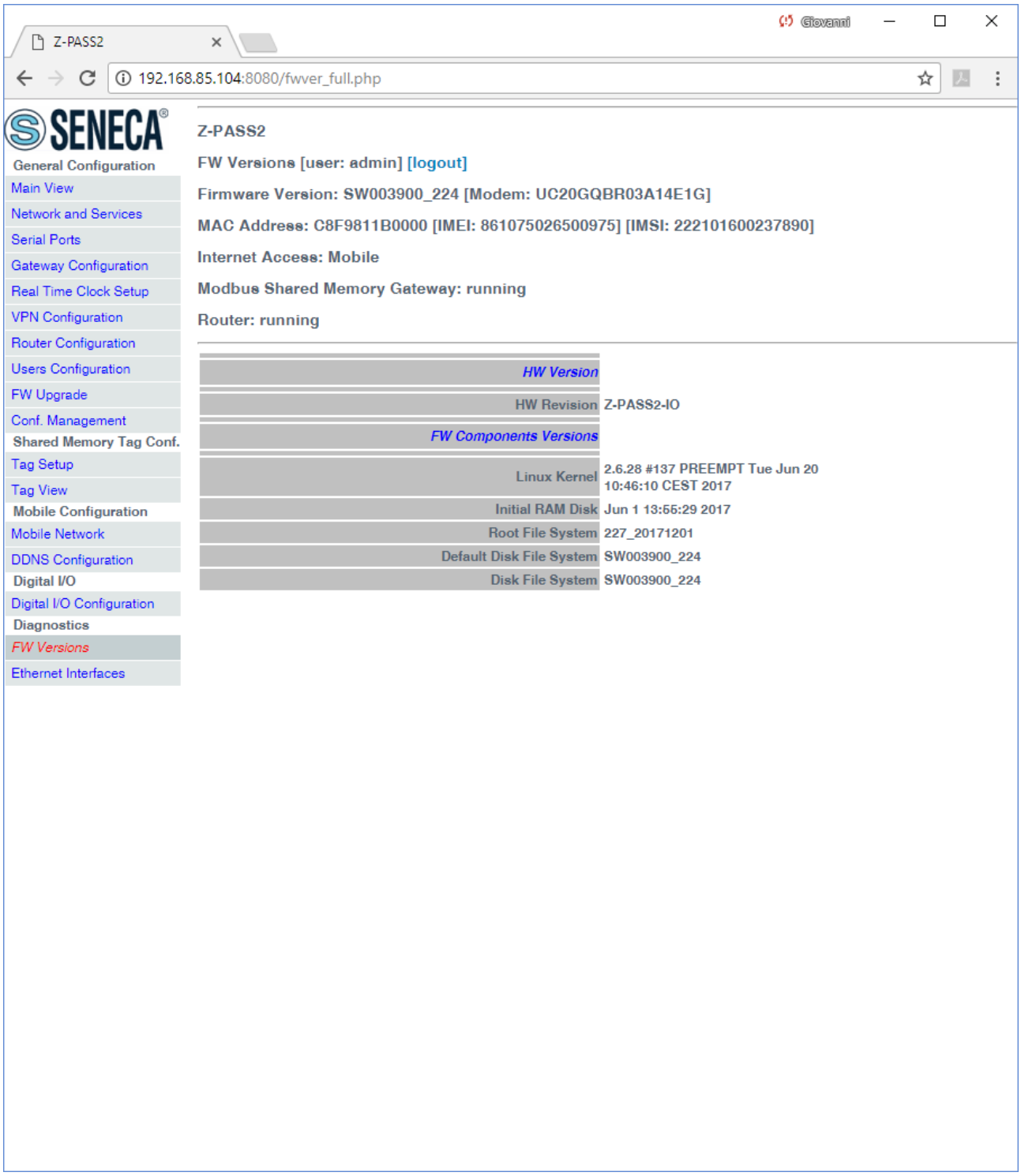
You can refresh the Ethernet status, by clicking on the “REFRESH” button.

### 20.8.2 Modbus Serial Trace

This is a serial sniffer useful for analyzing serial traffic. It is also possible to export the traffic to analyze it later.

### 20.8.3 FW Versions

By clicking on the “FW Versions” link, in the “Diagnostics” section, you come to the following page:



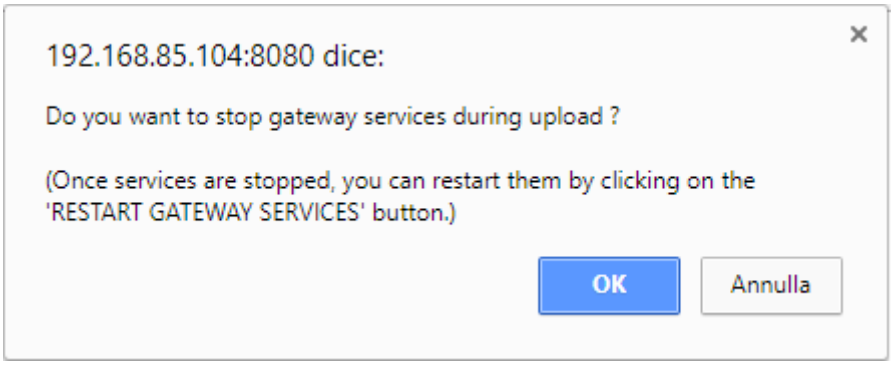

In this page, the following information are shown:

- the product name along with its HW revision (in the above figure: “Z-PASS2-R01”)
- the version strings of all the FW components, which are:
  - Linux Kernel (*kernel*)
  - Initial RAM Disk (*initrd*)

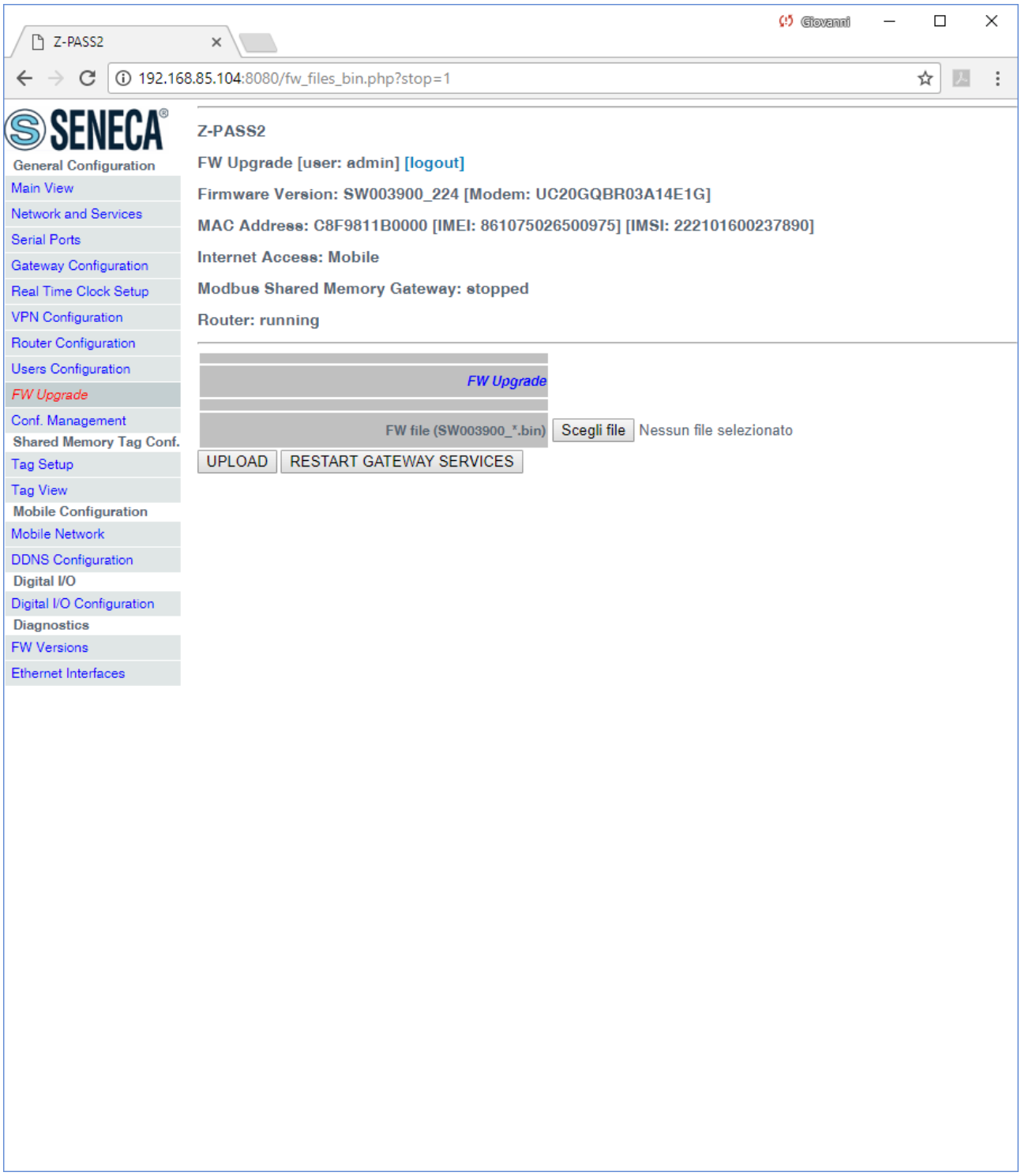
- Root File System (*rootfs*)
- Default Disk File System (*diskdfl*)
- Disk File System (*disk*)

### *20.8.4 FW Upgrade*

When clicking on the "FW Upgrade" link, in the "Maintenance" section, the following pop-up is shown:

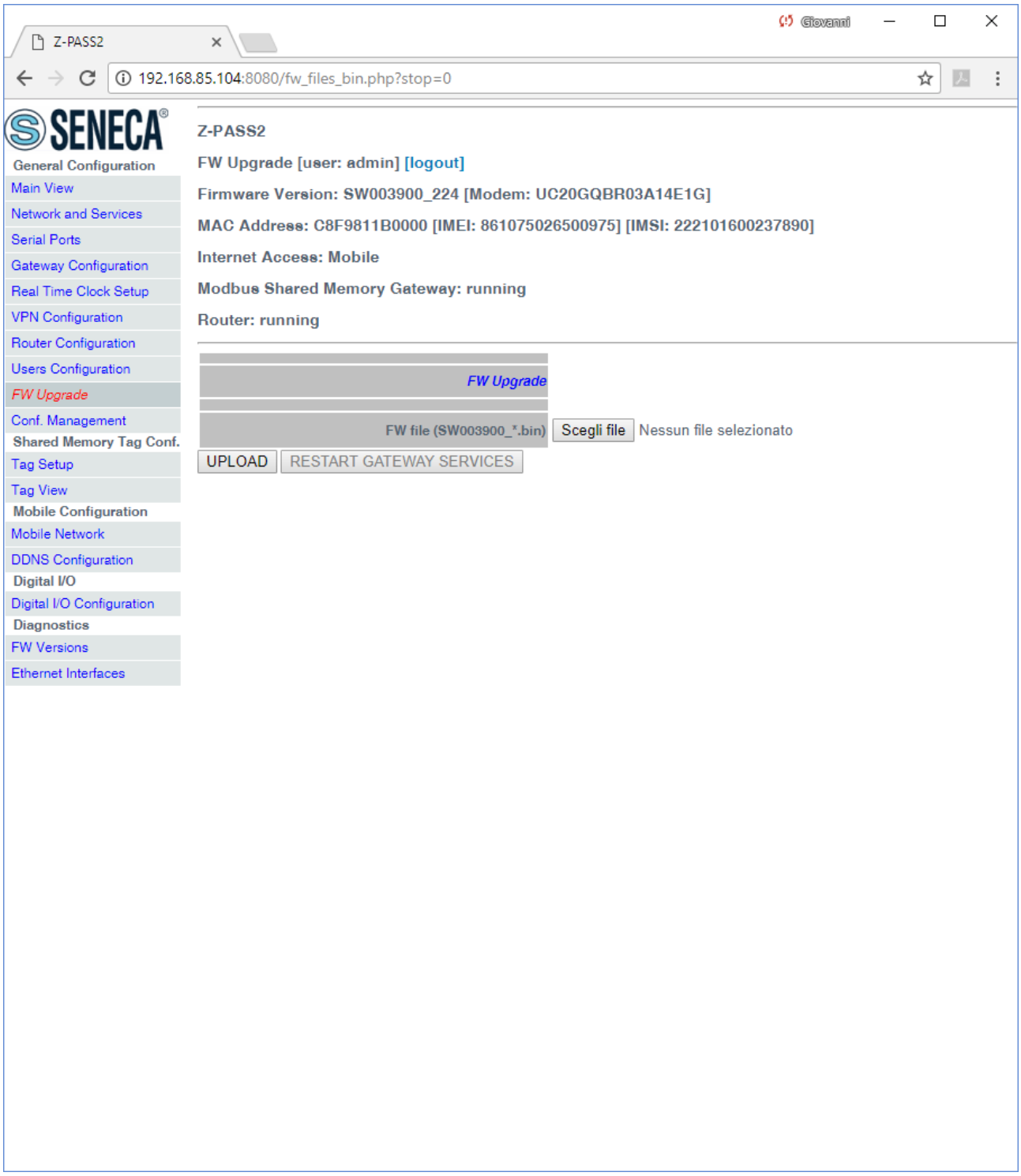



If you click on the "OK" button, Modbus Ethernet to Serial/Transparent/Modbus Shared Memory Gateway Services are stopped and you come to the "FW Upgrade" page, shown in the following figure.




Now, if you want to leave this page without performing the FW upgrade, the “RESTART GATEWAY SERVICES” button lets you restart the gateway services which, otherwise, would remain in the “stopped” state.

Otherwise, if you click on the “Cancel” button of the pop-up, Gateway Services are not stopped and you come to the same page where the “RESTART TWS SERVICES” button is disabled.




So, it is up to the user to choose if Gateway Services shall be stopped or not, during FW Upload; on one side, stopping them is more safe and let the upload be completed in a shorter time; on the other side, there are situations in which gateway services stop time shall be as short as possible.

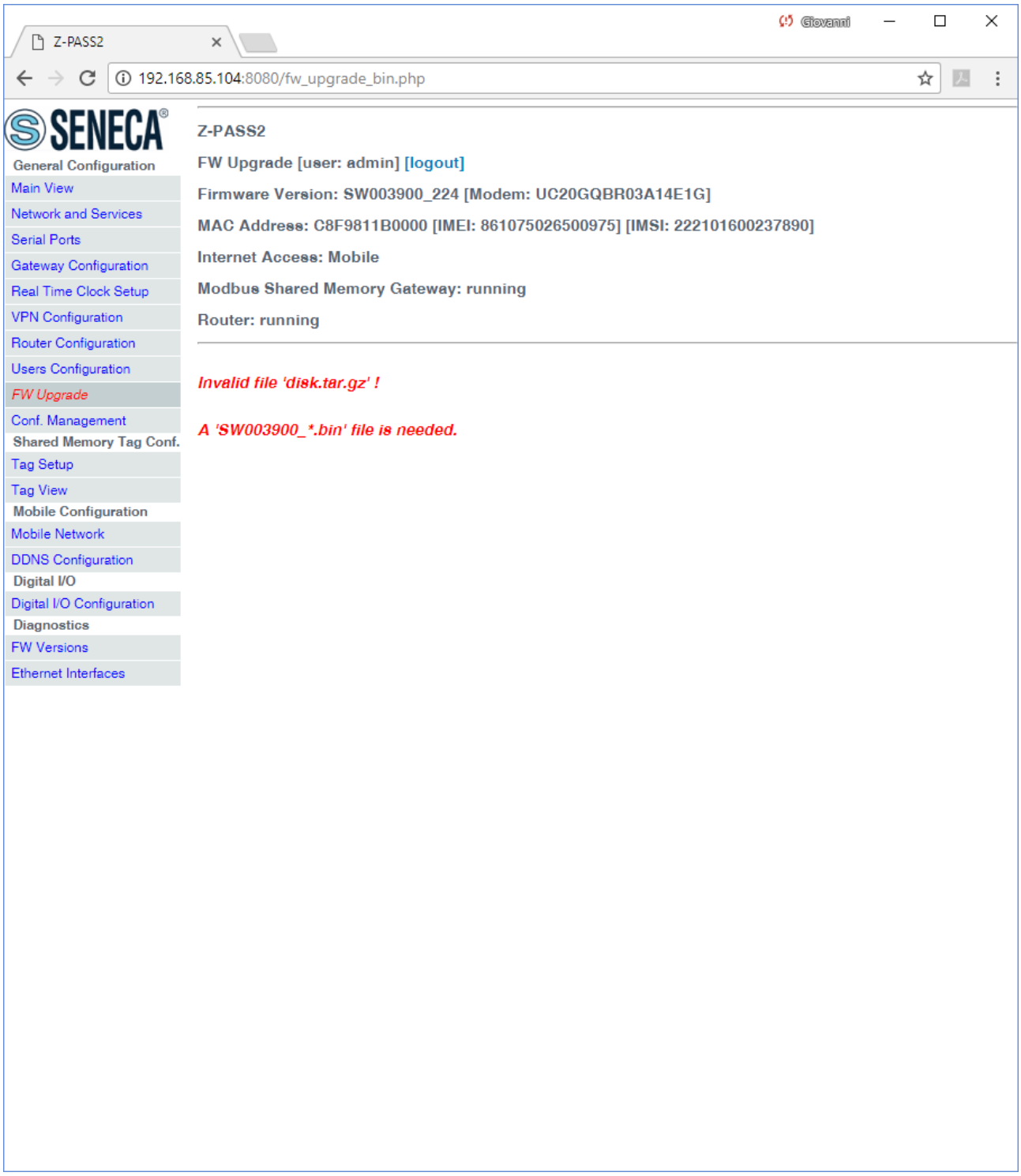
Since an erroneous use of the FW Upgrade functionality might compromise the proper Z-PASS operation, use this page only to apply upgrades provided by Seneca, with the support of Seneca personnel.

This page lets you browse your PC to select the file containing the FW, which shall have a name of the following type:

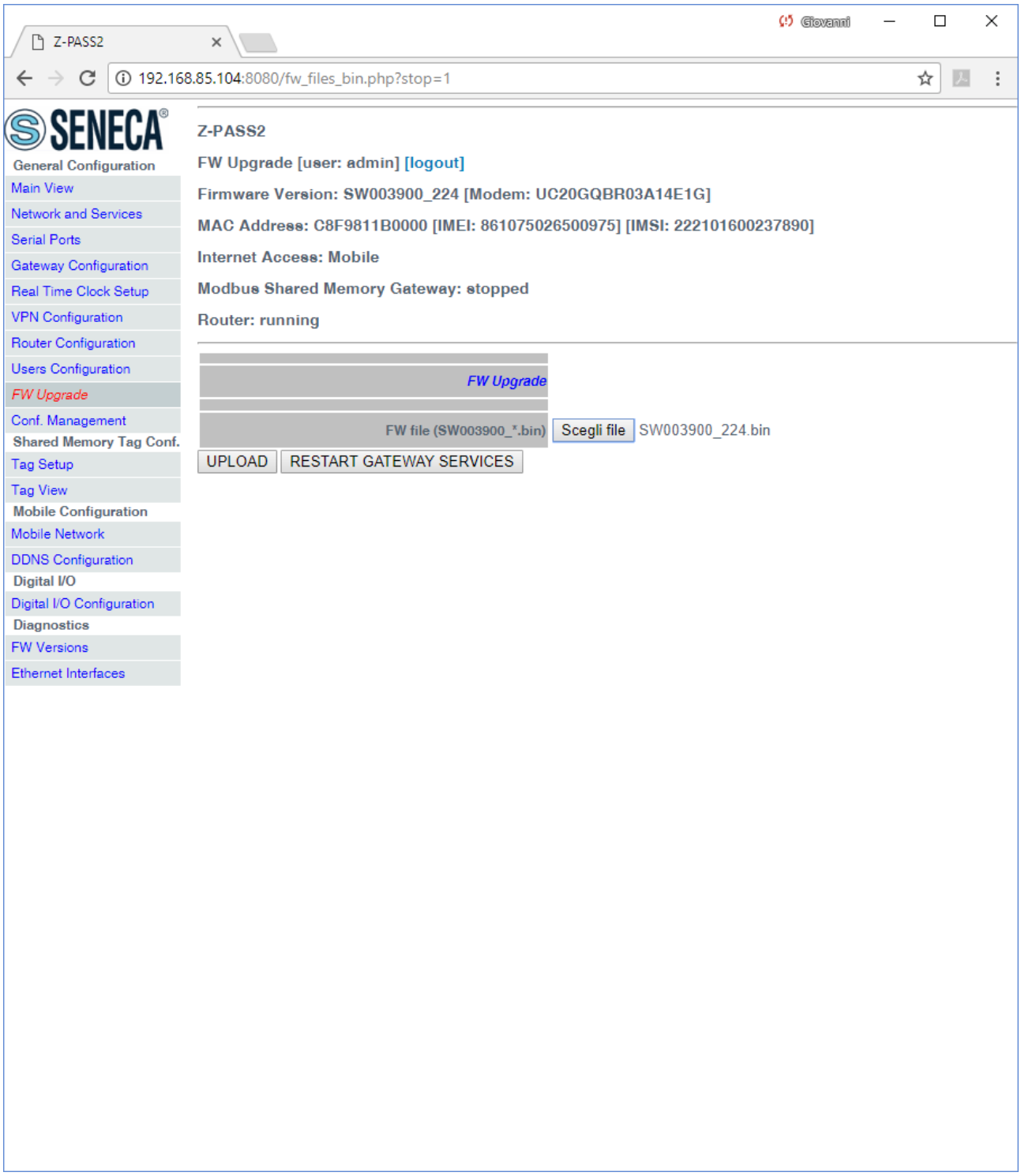
*SW003900_xxx.bin*[23]

If you select a file with a different name, an error will be shown at the end of the upload, as in the following figure.

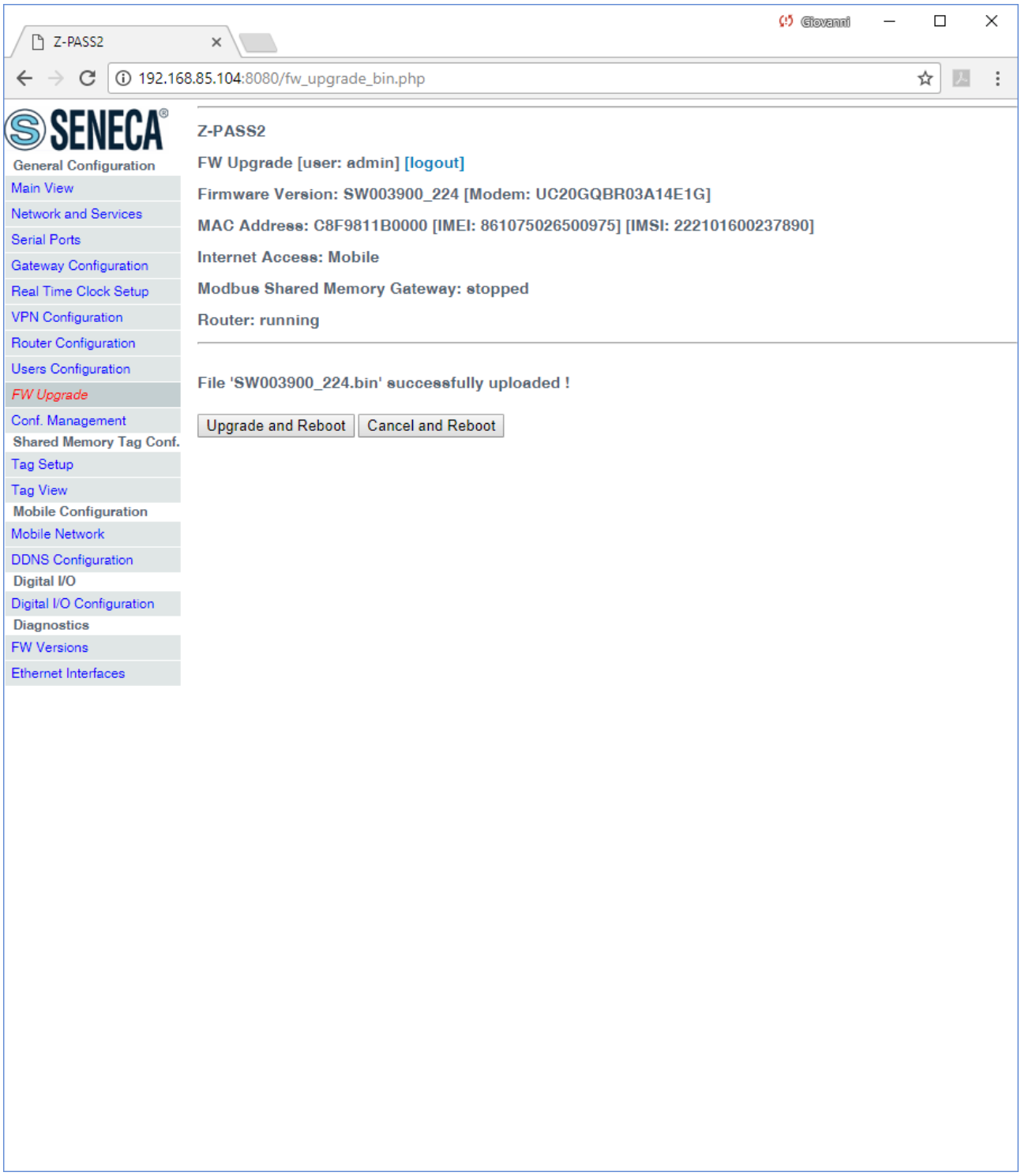
[23] The FW file can be downloaded from Seneca web site (see chapter “Upgrading the firmware by USB pen”).




Once a file is selected, you can start the upload, by pressing the “UPLOAD” button.



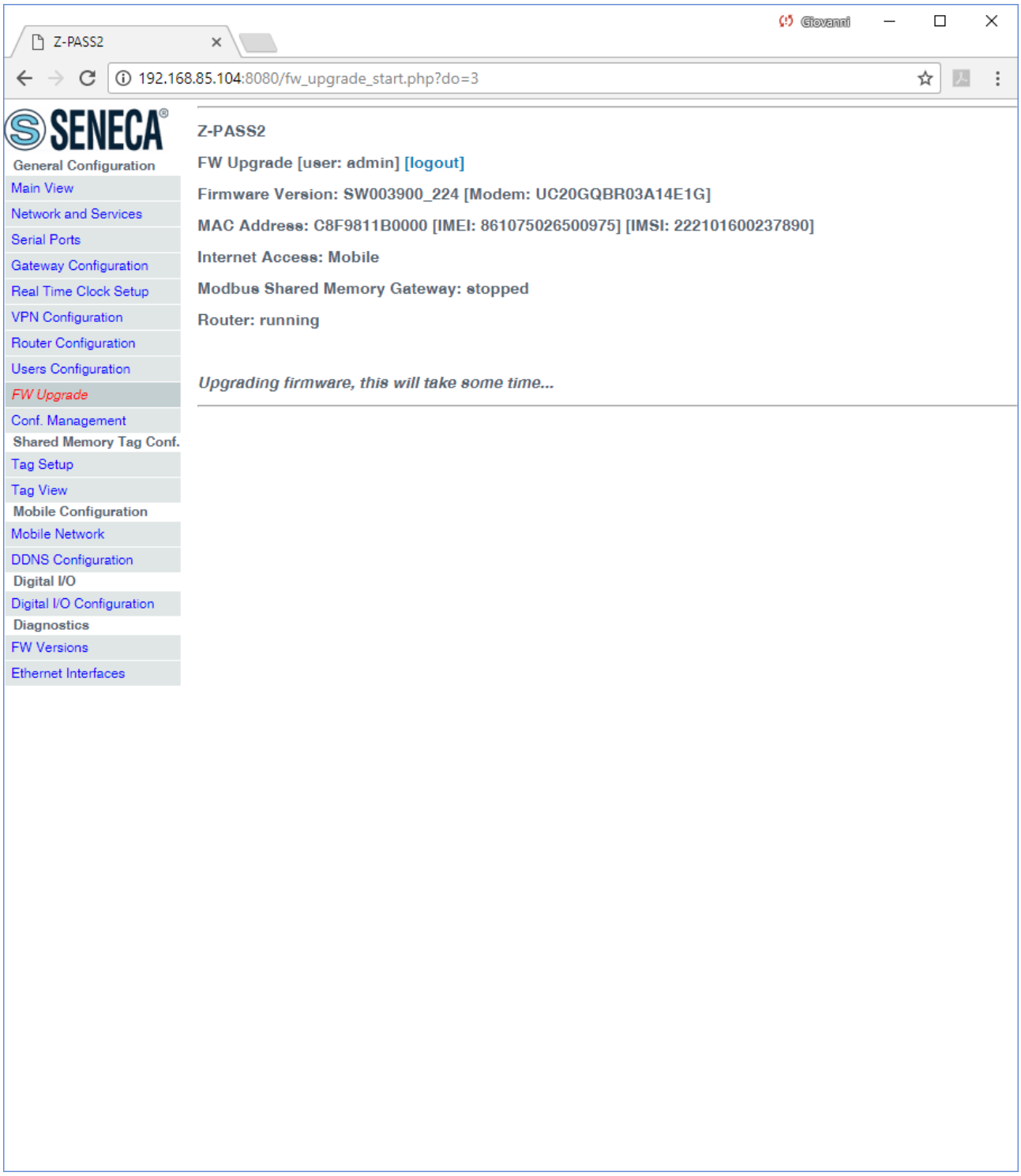

Once the upload is successfully completed, the following page is shown:



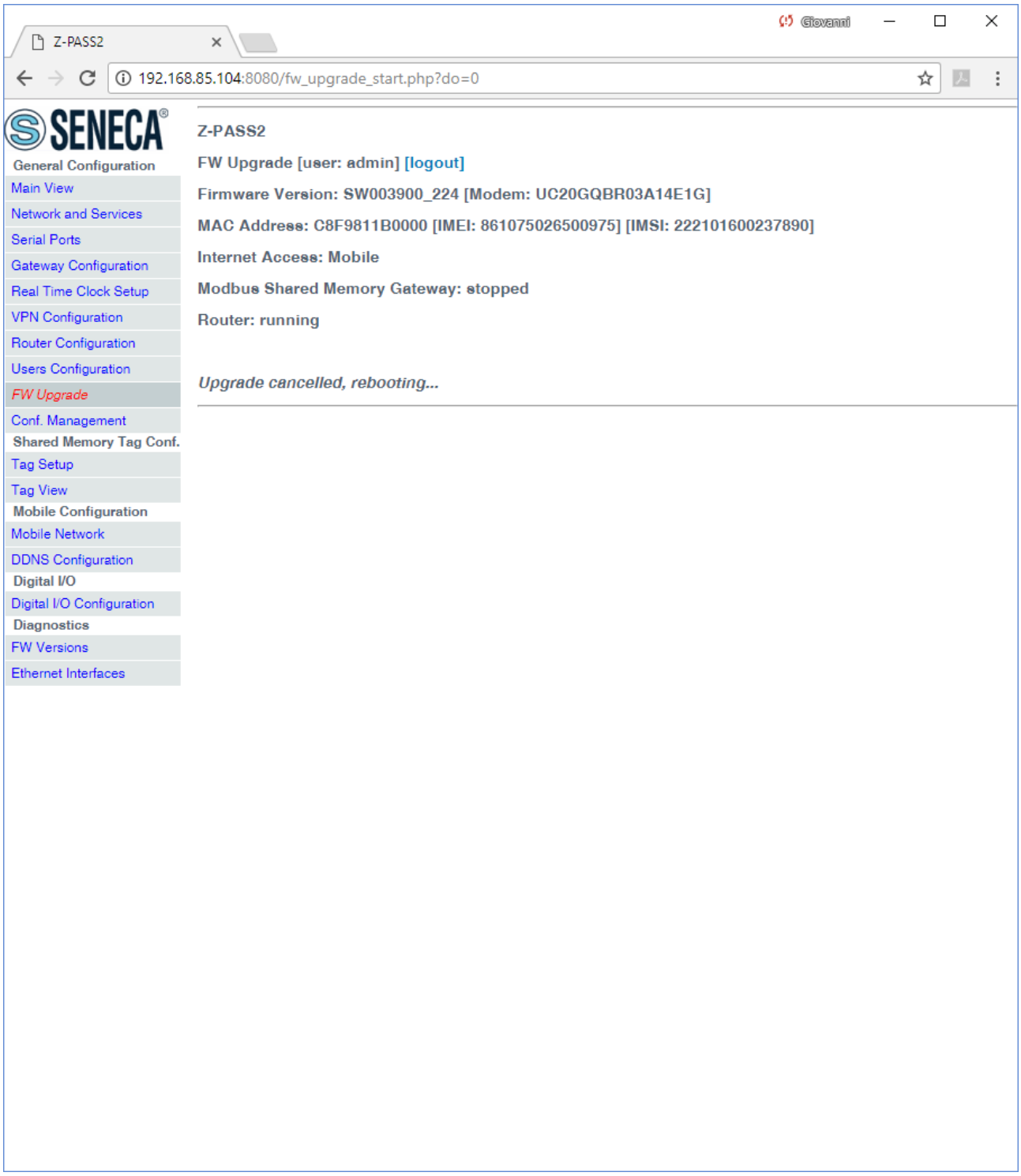

In this page, you can:

- press the “Upgrade and Reboot” button: this will start the upgrade procedure, which takes some minutes to be completed; during this time, the Z-PASS MUST NOT be switched off; during the procedure, the Z-PASS will be rebooted several times; also, during the procedure, several LEDS will blink simultaneously[24]; the upgrade procedure is ended when only the LED “RUN” is blinking[25];

[24] This applies only to products with HW revisions IO and R01; in details: for IO HW revision, all LEDs will blink simultaneously, except for Power, LAN/WAN, COM and modem LEDs; for R01 HW revision, RUN, VPN and SERV LEDs will blink.
[25] Also SERV and VPN LEDs might blink, depending on the Device configuration and status.



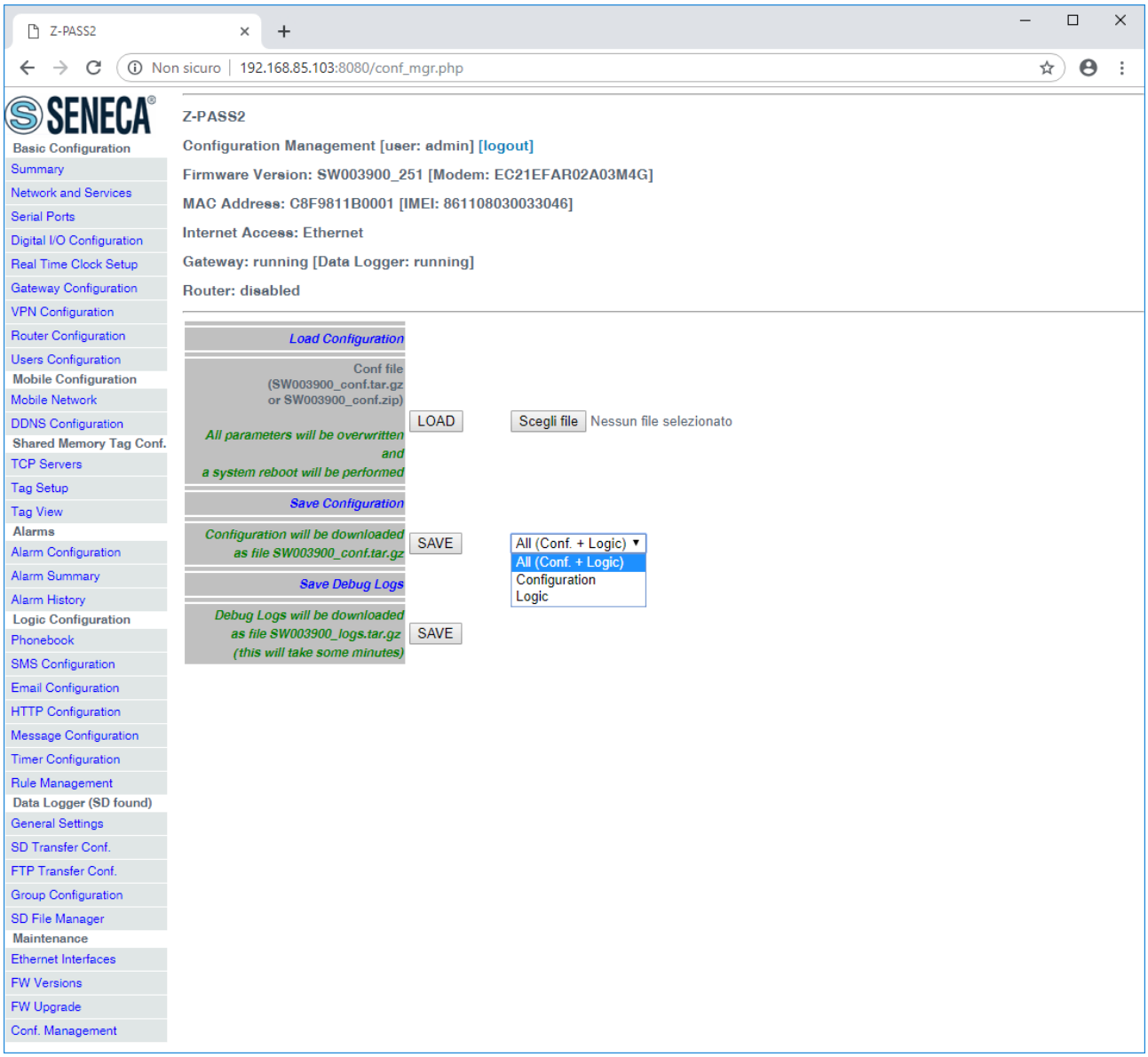

- press the “Cancel and Reboot” button: this will delete the uploaded file on the Z-PASS and perform the reboot.




Please note that the “guest” user (see 20.8.3 paragraph) cannot access the “FW Upgrade” page.

### *20.8.5 Configuration Management*

By clicking on the “Conf. Management” link, in the “Maintenance” section, you come to the following page:




This page lets you save and load the whole Z-PASS configuration; this is very useful, for example, when you have to apply the same configuration to many devices.

The configuration archive file is named *SW003900_conf.tar.gz*; its contents depend on the selected option, as shown in the following table:

| **Option** | **Files** |
|---|---|
| All (Conf. + Logic) | - configuration parameters<br>- OpenVPN configuration (if present)<br>- Modbus Shared Memory Gateway tags<br>- Logic configuration<br>- web user pages (if present) |
| Configuration | - configuration parameters<br>- OpenVPN configuration (if present) |

| | |
|---|---|
| Logic | - Modbus Shared Memory Gateway tags<br>- Logic configuration<br>- web user pages (if present) |

The configuration archive, once created and downloaded by means of the “SAVE” button can be uploaded to the same or another device, in two ways:

- by means of the “LOAD” button, in this page
- by means of a USB pen

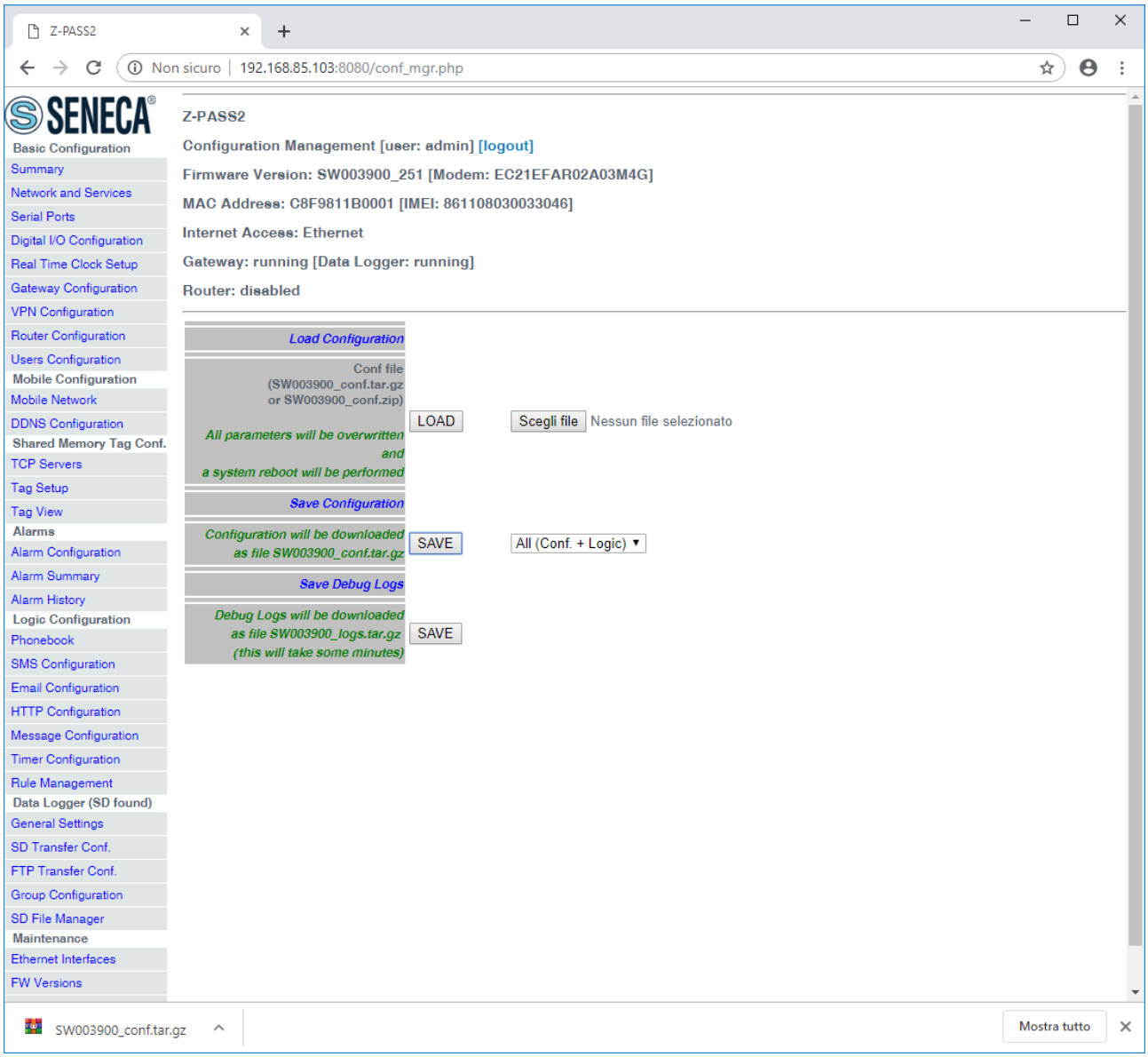
The procedure to load the configuration into the Z-PASS by means of a USB pen is the following:

- copy the *SW003900_conf.tar.gz* file into the root folder of the USB pen;
- switch off the Device;
- insert the USB pen into the USB#1 port of the Z-PASS;
- switch on the Z-PASS; the procedure will take some minutes to be completed; during this time, the Z-PASS MUST NOT be switched off; during the procedure, the Z-PASS will be rebooted;
- after the reboot, wait until you see the “RUN” LED blinking;
- remove the USB pen;
- the configuration has been applied to the Z-PASS.

The only care when you carry the configuration archive from a device to another one is that the two devices should be the same product model; for example, it’s not safe to load the configuration archive saved on a Z-PASS1 into a Z-PASS2.

This page lets you also load the configuration archive as a zip file (*SW003900_conf.zip*).

Another useful feature available in this page is the one provided by the “Save Debug Logs / SAVE” button: when you click on it, a file named *SW003900_logs.tar.gz* is downloaded, which contains the debug logs stored by the CPU during its operation.




Please note that, to get detailed debug logs, the “DEBUG LOGS / Enable” parameter, in “Network and Services” page, shall be set to ON.

Also note that the “guest” user (see 20.8.3 paragraph) cannot access the “Configuration Management” page.

### *20.8.5.1 Factory reset by USB pen*

A USB pen can be used also to reset the Z-PASS to its factory state; the procedure is the following:

- create an empty file named *SW003900_reset_cmd* into the root of the USB pen;
- switch off the Z-PASS;
- insert the USB pen into the USB#1 port of the Z-PASS;
- switch on the Z-PASS; the procedure will take some minutes to be completed; during this time, the Z-PASS MUST NOT be switched off; during the procedure, the Z-PASS will be rebooted;

- after the reboot, wait until you see the “RUN” LED blinking;
- remove the USB pen;
- the factory reset has been performed.

## *20.9 Guest pages*

It is also possible to access the Z-PASS configuration site as a “guest” user; this user is allowed to access all the pages except for “FW Upgrade”, “Configuration Management” and “SD File Manager” pages, viewing all configuration parameters and status information, without changing any parameter; so, in all the pages, the “APPLY” buttons (and any other button used to perform changes) are disabled.

To login as “guest” user, connect the browser to the Device IP address on port 8080, e.g.:

http://192.168.90.101:8080

and, when asked, provide the following credentials (default values):

Username: guest
Password: guest

You come to the “Summary” page, shown in the following figure.


Note that, as told above, the “FACTORY DEFAULT” and “RESTART” buttons are disabled.

Another example of a page accessed by the “guest” user is given in the following figure.


In the “Mobile Network” page, the “APPLY” and “GET OPERATOR LIST” buttons are disabled, whereas the “SHOW MOBILE STATUS”/”HIDE MOBILE STATUS” and “REFRESH” buttons are enabled, letting the “guest” user view the Mobile Status.

### 20.10 User Pages

It is also possible to access the Z-PASS configuration site as a “user” user; this user is allowed to access only to the “Summary” and the “tag view” pages.

To login as “user” user, connect the browser to the Device IP address on port 8080, e.g.:

http://192.168.90.101:8080

and, when asked, provide the following credentials (default values):

Username: user
Password: user

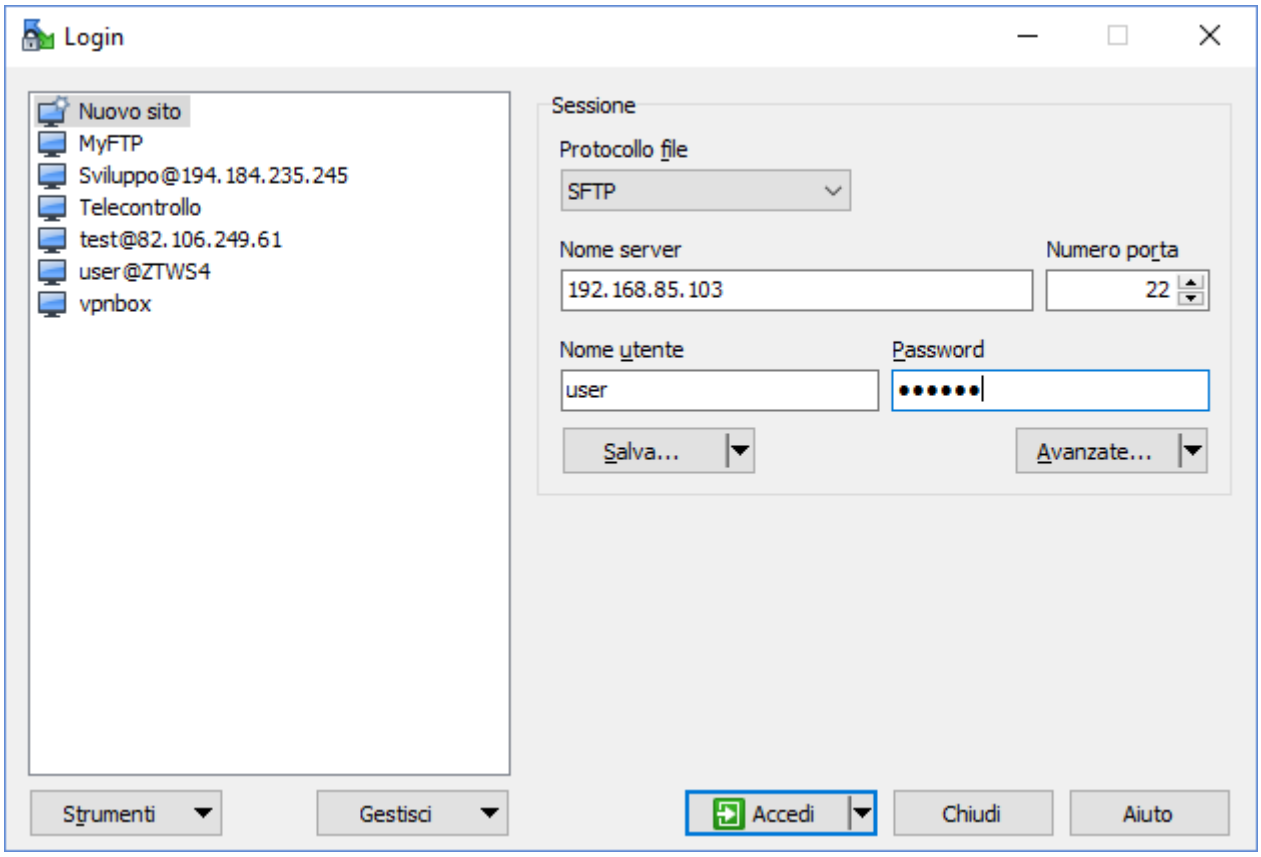
You come to the “Summary” page.

## 21 FTP/SFTP access

To easily access the Z-PASS by means of FTP/SFTP, you can use the WINSCP™ program; you can free download WINSCP™ from:

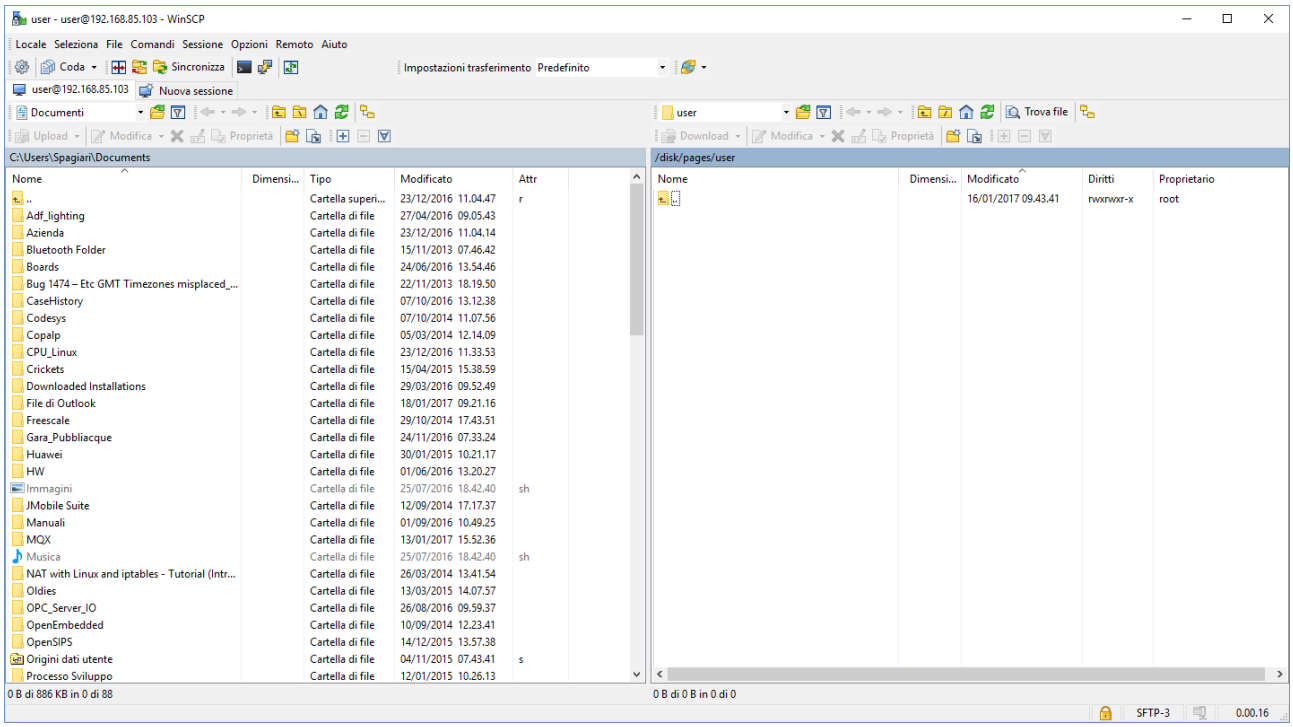
http://winscp.net/eng/download.php

You must set the connection as in the following figure (the screenshot shows a connection to the 192.168.85.103 IP address):




The credentials (username and password) are those (“user”, “123456”) set for the “FTP USER” (see “Users Configuration” web page in paragraph 20.1.9).

After clicking the “Access” button, you will get a new window, as in the following screenshot; on the right, you can copy and delete files directly to/from the Device.




The WinSCP program can be used both as an FTP or SFTP client to transfer files to/from the Z-PASS; just select “FTP” or “SFTP” protocol in the “WinSCP Login” window; normally, it’s better to use SFTP, since it provides a secure (i.e. encrypted) service.

# 22 Glossary

Bridge: a device that translates from one communications protocol into another.

Gateway: a device that acts as a portal between two programs allowing them to share information by communicating between different protocols.

Serial Device Server: a device that enables devices with an RS-232, RS-422 or RS-485 serial interface to connect to a local area network (LAN) or, more generally, an IP network.

Router: a networking device that forwards data packets between computer networks, e.g. between a LAN and a WAN (the Internet).

Switch: a networking device that connects devices together on a computer network, by using a form of packet switching to forward data to the destination device.

VPN: a Virtual Private Network extends a private network across a public network, such as the Internet. It enables a device to send and receive data across the public network as if it were directly connected to the private network. A VPN is created by establishing a virtual point-to-point connection through the use of tunnelling protocols, with traffic encryption.

Tunnel: an IP tunnel is an Internet Protocol (IP) network communications channel between two networks. It is used to transport another network protocol by encapsulation of its packets.

Tunnel Point-to-Point: an IP tunnel between a single Master device and a single Slave device.

Tunnel Point-to-Multipoint: an IP tunnel between a single Master device and multiple Slave devices.