



USER MANUAL



<u>Z-PASS2</u>

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



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

This document is property of SENECA srl. Duplication and reprodution are forbidden, if not authorized. Contents of the present documentation refers to products and technologies described in it. All technical data contained in the document may be modified without prior notice Content of this documentation is subject to periodical revision.

To use the product safely and effectively, read carefully the following instructions before use. The product must be used only for the use for which it was designed and built. Any other use must be considered with full responsibility of the user. The installation, programmation and set-up is allowed only for authorized operators; these ones must be people physically and intellectually suitable. Set up must be performed only after a correct installation and the user must perform every operation described in the installation manual carefully. Seneca is not considered liable of failure, breakdown, accident caused for ignorance or failure to apply the indicated requirements. Seneca is not considered liable of any unauthorized changes. Seneca reserves the right to modify the device, for any commercial or construction requirements, without the obligation to promptly update the reference manuals.

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

Table of Contents

Table	of Contents 2
1 P	reliminary information / Informazioni preliminari
2 F	irmware Licensing Terms
2.1	Firmware with Open Source GPL
3 ι	Ipgrading the firmware by USB pen
4 C	Discovering the Z-PASS IP address
5 E	thernet Mode
6 N	Aodbus Ethernet to Serial Gateway
7 T	ransparent Gateway
7.1	Virtual COM (with RFC 2217)14
7	7.1.1 Seneca Serial to Ethernet Connect
7.2	Serial Tunnel Point-to-Point on TCP
7.3	Serial Tunnel Point-to-Point on UDP25
7.4	Serial Tunnel Point-to-Multipoint
8 N	Aodbus Shared Memory Gateway
9 C	Data Logger
9.1	HTTP POST protocol
10	Alarms and Logic Rules
11	VPN
11.	1 "Single LAN" VPN
11.	2 "Point-to-Point" VPN
12	Router
13	Network Redundancy
14	Remote Connection Disable
15	Auto-APN
16	HTTP POST Communication protocol 40
17	OPC Unified Architecture (OPC-UA) server protocol 40
18	MQTT client protocol

19	S	VIS Commands	41
19	.1	PPP ON	42
19	.2	PPP OFF	42
19	.3	PPP IP	43
19	.4	PPP CNF	43
19	.5	VPN ON	44
19	.6	VPN OFF	45
19	.7	VPN CNF	45
19	.8	FWL ON	45
19	.9	FWL OFF	46
19	.10	GET DIN	46
19	.11	GET DOUT	46
19	.12	SET DOUT	47
19	.13	SET PULSE	48
19	.14	SET USER.PHONE	48
19	.15	RESET PHONE	49
19	.16	SET USER.EMAIL	50
19	.17	RESET EMAIL	50
19	.18	STATUS	51
19	.19	GET GPS	52
19	.20	RESET	52
19	.21	GET TAG	52
19	.22	SET TAG	53
19	.23	OVPN ON	54
19	.24	OVPN OFF	54
19	.25	CLEAN LOGS	54
19	.26	Initial Configuration	54
20	V	eb Configuration Pages	55
20	.1	Basic Configuration	56
	20.1	.1 Summary	56
	20.1	.2 Network and Services	57
	20.1	.3 Serial Ports	67

	0.1.4	Digital I/O Configuration	69
20).1.5	Real Time Clock Setup	77
20	0.1.6	Gateway Configuration	80
20).1.7	VPN Configuration	95
20).1.8	Router Configuration	. 116
20).1.9	NAT 1:1 RULES	. 127
20	0.1.10	STATIC ROUTES	. 127
20).1.11	OPC-UA Server Configuration	. 128
20).1.12	Users Configuration	. 136
20.2	Mot	pile Configuration	. 138
20).2.1	Mobile Network	. 138
20).2.2	DDNS Configuration	. 154
20.3	Shar	red Memory Tag Configuration	. 159
20).3.1	TCP Servers	. 159
20).3.2	Tag Setup	. 165
20).3.3	Tag View	. 182
20.4	Alar	ms	. 189
20) 4 1	Alarm Configuration	. 189
		-	
20).4.2	Alarm Summary	. 196
20 20).4.2).4.3	Alarm Summary	. 196 . 199
20 20 20.5).4.2).4.3 Clier	Alarm Summary Alarm History nt Protocols	. 196 . 199 . 201
20 20 20.5 20).4.2).4.3 Clier).5.1	Alarm Summary Alarm History nt Protocols SD Transfer Configuration	. 196 . 199 . 201 . 201
20 20 20.5 20 20).4.2).4.3 Clier).5.1).5.2	Alarm Summary Alarm History nt Protocols SD Transfer Configuration FTP Transfer Configuration	. 196 . 199 . 201 . 201 . 201
20 20.5 20 20 20 20 20 20).4.2).4.3 Clier).5.1).5.2).5.3	Alarm Summary Alarm History nt Protocols SD Transfer Configuration FTP Transfer Configuration Email Configuration	. 196 . 199 . 201 . 201 . 203 . 203
20 20.5 20 20 20 20 20 20 20 20 20).4.2).4.3 Clier).5.1).5.2).5.3).5.4	Alarm Summary Alarm History nt Protocols SD Transfer Configuration FTP Transfer Configuration Email Configuration HTTP Configuration	. 196 . 199 . 201 . 201 . 203 . 203 . 205 . 208
20 20.5 20 20 20 20 20 20 20 20 20).4.2).4.3 Clier).5.1).5.2).5.3).5.4).5.5	Alarm Summary Alarm History Int Protocols SD Transfer Configuration FTP Transfer Configuration Email Configuration HTTP Configuration	. 196 . 199 . 201 . 201 . 203 . 203 . 205 . 208 . 210
20 20.5 20 20 20 20 20 20 20 20 20 20).4.2).4.3 Clier).5.1).5.2).5.3).5.4).5.5).5.6	Alarm Summary Alarm History Int Protocols SD Transfer Configuration FTP Transfer Configuration Email Configuration HTTP Configuration MQTT Configuration Write a TAG(s) from MQTT	. 196 . 199 . 201 . 201 . 203 . 203 . 205 . 208 . 210 . 220
20 20.5 20 20 20 20 20 20 20 20 20 20 20 20 20).4.2).4.3 Clier).5.1).5.2).5.3).5.4).5.5).5.6).5.7	Alarm Summary Alarm History Int Protocols. SD Transfer Configuration FTP Transfer Configuration Email Configuration HTTP Configuration. MQTT Configuration Write a TAG(s) from MQTT.	. 196 . 199 . 201 . 201 . 203 . 203 . 205 . 208 . 210 . 220 . 220
20 20.5 20 20 20 20 20 20 20 20 20 20 20 20 20).4.2).4.3 Clier).5.1).5.2).5.3).5.4).5.5).5.6).5.6).5.7).5.8	Alarm Summary Alarm History Alarm History The Protocols SD Transfer Configuration FTP Transfer Configuration Email Configuration HTTP Configuration MQTT Configuration Write a TAG(s) from MQTT Send a command from MQTT	. 196 . 199 . 201 . 201 . 203 . 203 . 203 . 205 . 208 . 210 . 220 . 220 . 220
200 200 200 200 200 200 200 200 200 200).4.2).4.3 Clier).5.1).5.2).5.3).5.4).5.5).5.6).5.7).5.8 Logi	Alarm Summary Alarm History Int Protocols. SD Transfer Configuration FTP Transfer Configuration Email Configuration HTTP Configuration MQTT Configuration Write a TAG(s) from MQTT. Write multiple TAGs from MQTT Send a command from MQTT	. 196 . 199 . 201 . 201 . 203 . 203 . 203 . 205 . 208 . 210 . 220 . 220 . 220 . 221
20 20.5 20 20 20 20 20 20 20 20.6 20).4.2).4.3 Clier).5.1).5.2).5.3).5.4).5.5).5.6).5.7).5.8 Logi).6.1	Alarm Summary Alarm History nt Protocols SD Transfer Configuration FTP Transfer Configuration Email Configuration HTTP Configuration MQTT Configuration Write a TAG(s) from MQTT Write multiple TAGs from MQTT Send a command from MQTT Phonebook	. 196 . 199 . 201 . 201 . 203 . 203 . 203 . 203 . 205 . 208 . 210 . 220 . 220 . 220 . 221 . 221

20.6.3	Message Configuration	. 230
20.6.4	Timer Configuration	. 235
20.6.5	Rule Management	. 236
20.7 Dat	a Logger	. 264
20.7.1	General Settings	. 264
20.7.2	Group Configuration	. 267
20.7.3	SD File Manager	. 276
20.8 Ma	intenance	. 280
20.8.1	Ethernet Interfaces	. 280
20.8.2	Modbus Serial Trace	. 284
20.8.3	FW Versions	. 284
20.8.4	FW Upgrade	. 286
20.8.5	Configuration Management	. 295
20.9 Gue	est pages	. 299
20.10 L	Jser Pages	. 302
21 FTP/S	FTP access	. 302
22 Glossa	ary	. 304

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	-Added chapter "Timer Configuration"	
	(FW rel. SW003900_250)	-Added paragraphs under "Rule Management" for new logic features	
20/03/2019	23	- Paragraph "Rule Management": added "Bitmask" condition and "Set	
	(FW rel. SW003900_251)	Bits" action	
		- Paragraphs "Alarm Configuration", "Message Configuration": added	
		info about export/import to/from csv file	
		- Paragraph "Configuration Management": added type of configuration	
00/04/2010	21	Added chapter "OPC UA protocol"	
09/04/2019	(FW rel. SW003900 260)	-Added paragraph "OPC-UA protocol	
		-Audeu paragraphi Ore-OA server coomiguration	
23/07/2019	25	-Added chapter "MQTT client protocol"	
	(FW rel. SW003900_270)	-Changed Chapters order for new webserver menu	
26/07/2019	26	-Added OPC-UA server Security Policy	
	(FW rel. SW003900_280)	-Added MQTT client protocol chapter info	
27/08/2019	27	-Added the new option "Retain" in Tag Creation/Modification	
	(FW rel. SW003900_290)		
05/11/2019	28	-Max Modbus TCP-IP servers from 10 to 25	
	(FW rel. SW003900_292)		
		-Added NAT 1:1 feature	
		-Added Static Route feature	
19/12/2019	29 (EW rel SW003900 293)	Added new 64 bits Tags in chapter "Tag Creation/Modification"	
	(10010130003300_233)		
19/12/2019	30	Added info about OPC-UA Server namespace-id	
30/03/2020	31	Added "User" account	
	(FW rel. SW003900_295)		
23/09/2020	22	Added "Datalogger on Trigger" new feature	
23/03/2020	(FW rel SW003900 299)		
		Added "Serial Trace" new feature	
		Added "SMS command "OVPN ON" and "OVPN OFF"	
		Added now perspector MOTT "Sleep Timoout"	
		Added new parameter MQTT Sleep Timeout	
25/01/2021	33	Added new command "CLEAN LOGS" (From FW rel 313)	
		Added info on how to send commands from MQTT to the device	
		Added info on how to write a command from MQTT to the device	
		Removed all references to old Z-PASS models	
1			

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 <u>support@seneca.it</u> 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 simultaneously¹
- 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:

8	Seneca	Device Discovery	- rev. 2.1.3.0						_		×
<u>F</u> il	e										
[Devices f	ound									
	#	IP	Mode	MAC	Ping	Name	Hostname	Firmware	CRC	Comma	ands
	⊕	192.168.90.225	STATIC	C8:FA:81:16:00:03	Different Subnet	Z-TWS4	192.168.90.225	2940.310	OK	Assig	jn
	\oplus	192.168.85.83	STATIC	C8:F9:81:0C:01:9E	1 ms	Z-KEY	192.168.85.83	113.1	OK	Assig	ın
	⊕	192.168.85.8	STATIC	C8:F9:81:0C:01:9D	2 ms	Z-KEY	192.168.85.8	110.0	OK	Assig	jn
	⊕	192.168.85.200	STATIC	C8:F9:81:02:01:BD	2 ms	Z-TWS4	ZTWS4	2940.220	ОК		
	⊕	192.168.84.192	STATIC	C8:F9:81:02:03:5F	1 ms	Z-TWS4	ZTWS4	2940.210	ОК		
	⊕	192.168.85.7	STATIC	C8:F9:81:02:02:85	1 ms	Z-PASS	192.168.85.7	3900.122	ОК		
	⊕	192.168.85.6	STATIC	C8:F9:81:11:00:02	2 ms	Z-PASS2-S	192.168.85.6	2940.221	ОК		
	⊕	192.168.84.155	STATIC	00:22:4D:B6:D4:06	1 ms	Cloud BOX	cloud-dev.seneca	7800.106	ОК		
	⊕	192.168.85.102	STATIC	C8:F9:81:02:01:5B	1 ms	Z-TWS4	ZTWS4	2940.222	ОК		
	()	192.168.85.103	STATIC	C8:FA:81:16:00:02	8 ms	Z-PASS	192.168.85.103	3900.205	ОК	Assig	jn
	⊕	192.168.85.69	STATIC	08:00:27:5B:CB:12	2 ms	Cloud BOX	192.168.85.69	7800.106	ОК		
	<										>
	Found 1	1 devices									
	round 1	T devices							5	Search	
Ľ											

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:

	IP	
Static IP	192.168.95.101	
Netmask	Gateway	
255.255.255.0	192.168.95.1	

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.





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:

😡 Null-modem	emulator (com0cor	m)Setup 🗕 🗆 🗙					
Choose Components Choose which features of Null-modem emulator (com0com) you want to install.							
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.							
Select components to install:	Com0com Start Menu Shortcuts CNCA0 <-> CNCB0 COM# <-> COM#	Description Position your mouse over a component to see its description.					
Space required: 344.0KB							
Nullsoft Install System v2.46	< <u>B</u> ack	Next > Cancel					

Now Click on "Launch Setup":

🕞 Null-mo	dem emulator (com0com) Setup 🛛 – 🗖 🛛 🗙
	Completing the Null-modem emulator (com0com) Setup Wizard
	Null-modem emulator (com0com) has been installed on your computer.
	Click Finish to close this wizard.
	✓ Launch Setup
R	Show Readme
	Visit com0com homepage
	< Back Einish Cancel

Press Finish, the com0com setup will open:

₽	Setup for com0com – 🗆 🗙
Image: Second system Image: Second system Image: Secon	CNCA0 CNCB0 use Ports class use Ports class emulate baud rate enable buffer overnun enable buffer overnun enable buffer overnun enable plug-in mode enable plug-in mode enable exclusive mode enable exclusive mode enable hidden mode enable hidden mode RX • RX TX • TX DTR • DTR DSR • DSR DCD • DCD RTS • CTS RI • RI OUT1 • OUT1 OUT2 • OUT2 OPEN • OPEN ON
Add Pair Remove	Reset Apply

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:

10 10 10	Seneca Ethernet to Serial Connection 🛛 – 🗖 🗙
	Seneca Ethemet to Serial Connection rev. 1.04
	SENECA®
	Select PC Virtual Com Port COM5
	Select Z-PASS / Z-KEY IP address 192 . 168 . 90 . 101
	Select Z-PASS / Z-KEY PORT 8000
	CONNECT PORT DISCONNECT ALL PORTS
	Local port connected to remote ip 192.168.90.101
	DEVICE MANAGER

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

	Connetti a	?	×
Test			
lmmettere i dettagli p	er il numero telefonico da o	comporre:	
<u>P</u> aese:	Italia (39)		~
<u>I</u> ndicativo località:			
<u>N</u> umero di telefono:			
C <u>o</u> nnetti:	COM5		~
	ОК	Annulla	3

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

7.1.1.3 Configuring Seneca Serial to Ethernet Connect

 Seneca Ethernet to Serial Connection 🛛 – 🗖 🗙			
Seneca Ethemet to Serial Connection rev. 1.01			
SENECA [®]			
Select PC Virtual Com Port			
Select Z-PASS / Z-KEY IP address 192 . 168 . 90 . 101			
Select Z-PASS / Z-KEY PORT 8000			
CONNECT PORT DISCONNECT ALL PORTS Open Debug Window			

- 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:

<u> 697.</u>	C:\WINDOWS\system32\cmd.exe -	×
Connect(98) TCP(1)	ERROR 10060 - (null)	~
$S_{0} = S_{0} = S_{0$	r 0K = c4	
TCP(1): Connect(c4.	192.168.90.101:8000)	
Connect(c4) TCP(1)	ERROR 10060 - (null)	
TCP(1): Close(c4) -	- OK	
Socket(0.0.0.0:0) =	= 17c	
ICP(1): Connect(17c	t, 192.168.90.101:8000)	
$TCP(1) \cdot Class(17c)$	- OK	
Socket(0.0.0.0:0) =	= 17c	
TCP(1): Connect(17c	. 192.168.90.101:8000>	
Connect(17c) TCP(1)	ERROR 10060 - (null)	
TCP(1): Close(17c)	– OK	
Socket(0.0.0.0:0) =		
Coppost(o4) TCP(1)	, 192.168.90.101-8000/ EDDAD 10040 - (sull)	
TCP(1): Close(c4) -	- 0K	
Socket(0.0.0.0:0) =	= c4	
TCP(1): Connect(c4,	192.168.90.101:8000)	
Connect(c4) TCP(1)	ERROR 10060 - (null)	
ICP(1): Close(c4) -	- OK	
Socket(0.0.0.0:0) = TCP(1): Coppost(99)	578 192 160 90 101-9000	
IGP(1)- Connect(98,	. 172.100.70.101.0000/	

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:

<u>.</u> *	Seneca Ethernet to Serial Connection 🛛 – 🗖 🗙		
	Seneca Ethemet to Serial Connection rev. 1.04		
	S SENECA [®]		
	Select PC Virtual Com Port COM4 V		
	Select Z-PASS / Z-KEY IP address 192 . 168 . 90 . 101		
	Select Z-PASS / Z-KEY PORT 8000		
	CONNECT PORT DISCONNECT ALL PORTS		
	DEVICE MANAGER		

The com0com setup window will open:

₽	Setup for com0com – 🗆 🗙
⊡-Vitual Port Pair 0 ⊕-COM5 ⊕-COM4	COME COM4 use Ports class use Ports class emulate baud rate emulate baud rate enable buffer overnun enable buffer overnun enable plug-in mode enable plug-in mode enable kxclusive mode enable kxclusive mode enable hidden mode enable hidden mode RX RX TX DTR DSR DTR DCD RTS CTS CTS RI TI OUT1 OUT1 OUT2 OUT2 OPEN ON
Add Pair Remove	Reset Apply

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

₽	Setup for com0com 🛛 – 🗖 🗙
⊡ Virtual Port Pair 0 ⊕ COM5 ⊕ COM4	COM3 COM2 use Ports class ● use Ports class emulate baud rate ● emulate baud rate enable buffer overnun ● enable buffer overnun enable plug-in mode ● enable buffer overnun enable hidden mode ● enable hidden mode RX ● TX ● DTR ● DTR DSR DCD ● DCD ● RTS ● CTS ● RTS ● ● OUT1 ● OUT1 ● ● ● ● OPEN ● ● ● ●
Add Pair Remove	Reset Apply

Sometimes the COM can be marked as "in use":

Setup for com0com (CHANGE)
The port name COM3 is already logged as "in use" in the COM port database.
Annulla <u>R</u> iprova <u>C</u> ontinua

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":

	4		Gestione dispositivi
	File Azione	Visualizza ?	
1	♦ ♦	Dispositivi per tipo	
	A 🚔 PC-Mos	Dispositivi per connessione	
	🕞 🦃 Batte	Risorse per tipo	
	Blue	Risorse per connessione	
	⊳ 🖶 Cod		
	⊳ 🐺 com	Mostra dispositivi nascosti	
	⊳ 🖳 Com	Personalizza	
	Cont		
	▷ 1 com ▷ 1 Com ▷ 1 Com ▷ 1 Cont	Mostra dispositivi nascosti Personalizza	

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":

👘 Seneca Virtual Com Port (COM19)			
🐨 Seneca Virtual Com Port (COM3)		1	
👘 USB Serial Port (COM10)		Aggiornamer	nto software driver
🚏 USB Serial Port (COM14)		Disinstalla	
Processori			
👰 Schede di rete		Rileva modifiche hardware	
Network Schede video		Proprietà	
🔊 Schermi		riopricta	

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" outputs³, 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:

- <u>1000 log files</u>
- (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;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;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;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;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;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;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;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;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;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;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;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;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;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 product⁴, 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)

ELSE ACTION(s)

The "Then Action" is executed if the "If Condition" is true.

THEN ACTION(s)

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





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
- Iower 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 VPN⁵ 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: <u>the Z-PASS LANs and the PC</u> <u>LAN shall have different and not colliding subnets</u>; 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 data⁶ 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 DB⁷, 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 <u>support@seneca.it</u>).

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, highlatency 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"; <u>the password is made by the last four digits of the Z-PASS modem IMEI</u>; 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 <u>this command that does not enable the mobile data connection in a persistent way, so if</u> <u>the Z-PASS is restarted, the mobile data (PPP) connection is not re-established</u>.

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

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; <u>the changes are persistent</u>.

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

Examples:

- → VPN ON ← VPN ON EXECUTING
- → VPN ON PPP
- ← VPN ON PPP EXECUTING
- → VPN ON NOFWL
- ← VPN ON NOFWL EXECUTING
- \rightarrow 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 <u>this command that does not de-activate the VPN Box functionality in a persistent way, so if</u> <u>the Z-PASS is restarted, the functionality is re-activated</u>.

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; <u>the changes are persistent</u>.

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:

```
\rightarrow 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:

 \rightarrow FWL ON

 \leftarrow 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></n>	with <n>=14</n>	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
- $\rightarrow \qquad \text{GET DIN2} \\ \leftarrow \qquad \text{GET DIN2 EXECUTING (0)}$

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>=14</n></n>	get the status of a single digital output
----------------------------------	---

GET DOUT

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;

get the status of all the digital outputs

- 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
- \leftarrow GET DOUT1 EXECUTING (0)
- → GET DOUT2
- \leftarrow 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</n>	with <n>=14</n>	set the digital output to the HIGH state
SET	DOUT <n>.OPEN</n>	with <n>=14</n>	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 input¹¹, 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 input¹², 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:

 \rightarrow 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 <u>the telephone number shall always be given in the "international format"</u>, so the initial '+' <u>character shall always be present</u>.

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:

- \rightarrow 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 <u>the telephone number shall always be given in the "international format"</u>, so the initial '+' <u>character shall always be present</u>.

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, <u>if the Phonebook user with the specified telephone number also has an email address</u>, <u>this will be deleted by the command too</u>.

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, <u>if the Phonebook user with the specified email address also has a telephone number, this</u> 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>,<D01>,<D02>,<DID01>,<DID02>
```

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" LED¹³ ("OFF" | "ON" | "FAIL") <vpn status> reports the status of the "VPN" LED ("OFF" | "ON" | "FAIL") <DI1>,<DI2>,<DO1>,<DID01>,<DID02> 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[™]: <u>https://www.google.com/maps/?q=<latitude>,<longitude</u>>

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:

```
\rightarrow 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:

```
\rightarrow RESET

\leftarrow 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 <u>the "tag name" is case-sensitive</u>; also note that this command assumes that <u>each tag has a</u> <u>distinct name</u>; 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 <u>the "tag name" is case-sensitive</u>; also note that this command assumes that <u>each tag has a</u> <u>distinct name</u>; 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:

- \rightarrow 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 <u>this command that does not activate the OPEN VPN functionality in a persistent way, so if</u> <u>the Z-PASS is restarted, the functionality is not re-activated</u>.

Examples:

 \rightarrow 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 <u>this command that does not de-activate the OPEN VPN functionality in a persistent way, so</u> <u>if the Z-PASS is restarted, the functionality is re-activated</u>.

Example:

 \rightarrow 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.

Z-PASS2	×			(!) Giovanni	-		×
← → C ③ 192.	168.85.104:8080/setup.php				Q	☆ ≯	:
SENECCA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration	Z-PASS2 Network and Services [user: admin] [logout] Firmware Version: SW003900_224 [Modem: 1 MAC Address: C8F9811B0000 [IMEI: 8610756 Internet Access: Mobile Modbus Shared Memory Gateway: running Router: running	UC20GQBR03A 026500975] [IMS	14E1G] SI: 222101600237890]				
Users Configuration		CURRENT	UPDATED				
FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Digite I/O Digital I/O Digital I/O Digital I/O Configuration Diagnostics FW Versions Ethernet Interfaces	NETWORK Ethernet Mode (*) DHCP on WAN LAN IP Address LAN Network Mask WAN IP Address WAN Network Mask Default Gateway DNS Mode DNS Server IP Configuration from Discovery WEB SERVER Protocol (*) HTTP Conf Port (*) HTTP Conf Port (*) HTTP Vaser Port (*) FILE TRANSFER Protocol FTP Port SETP Port SETP Port SETP Port SETP Port Enable Ping Address WATCHDOG Enable (*) Timeout (s) DEBUG LOGS Enable	LAN/WAN OFF 192.168.90.101 255.255.255.0 192.168.85.104 255.255.252.0 192.168.85.1 8tatic 192.168.84.113 ON HTTP/HTTP8 8080 80 443 FTP/SFTP 21 22 OFF 8.8.4.4 ON 60 ON R8485	LAN/WAN ▼ OFF ▼ 192.168.90.101 255.255.255.0 192.168.85.104 255.255.252.0 192.168.85.1 Static ▼ 192.168.84.113 ON ▼ HTTP/HTTPS ▼ 8080 80 443 FTP/SFTP ▼ 21 22 OFF ▼ 8.8.4.4 ON ▼ 60 ON ▼ RS485 ▼				
			APPLY				

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.

Th Z-PASS2	×			🤃 Giovanni	_		×
← → C ① 192.	168.85.104:8080/setup.php				Q	☆ 🏃	:
SENECA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	Z-PASS2 Network and Services [user: admin] [logout] Firmware Version: SW003900_224 [Modem: U MAC Address: C8F9811B0000 [IMEI: 86107502 Internet Access: Ethernet Modbus Shared Memory Gateway: running Router: running	IC20GQBR03A 26500975] [IM4	14E1G] SI: 222101600237890]				
Router Configuration							
Users Configuration		CURRENT	UPDATED				
FW Upgrade	NETWORK						- 8
Conf. Management Shared Memory Tag Conf.	Ethernet Mode (*) 8	witch	Switch •				
Tag Setup	DHCP O)FF	OFF V				- 1
Tao View	IP Address 1	92.168.95.101	192.168.95.101				- 1
Mobile Configuration	Network Mask 2	55.255.255.0	255.255.255.0				- 1
Mobile Network	IP Address 2 Enable O	N	ON 🔻				- 1
DDNS Configuration	IP Address 2 1	92.168.85.104	192.168.85.104				- 1
Digital I/O	Network Mask 2 2	55.255.252.0	255.255.252.0				- 1
Digital I/O Configuration	Default Gateway 1	92.168.85.1	192.168.85.1				- 1
FW Versions	DNS Mode S	static	Static v				- 1
Ethernet Interfaces	DNS Server 1	92.168.84.113	192.168.84.113				- 1
	IP Configuration from Discovery O	N	ON 🔻				- 1
	WEB SERVER						- 1
	Protocol (*) H	TTP/HTTP8	HTTP/HTTPS V				- 1
	HTTP Conf Port (*) 8	080	8080				- 1
	HTTP liser Port (*) 8	0	80				- 1
	HTTPS Port (*) 4	43	443				- 1
			443				- 1
	FILE TRANSFER						- 1
	Protocol F	TP/SFTP	FTP/SFTP V				- 1
	FTP Port 2	1	21				- 1
	SFTP Port 2	2	22				- 1
	NETWORK REDUNDANCY						- 1
	Enable O)FF	OFF V				- 1
	Ping Address 8	.8.4.4	8.8.4.4				- 1
	WATCHDOG						- 1
	Enable (*) 0)N	ON V				- 1
	Timeout (s) 6	0	60				- 1
		-					
	DEBUG LOGS						
	Enable O	N	ON V				
	COM1						
	Mode R	8485	RS485 V				
	NOTE: changing fields marked with * will cause a system restart.						
			APPLY				-

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.

Z-PASS2	×		🤨 Giovanni	-		×
← → C ③ 192	.168.85.105:8080/setup.php			Q	☆ ♪	:
SENECA® General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration	Z-PASS2 Network and Services [user: admin] [logout] Firmware Version: SW003900_224 [Modem: 1231B02SIM MAC Address: C8FA81160002 [IMEI: 862264020406715] Internet Access: Ethernet Modbus Ethernet to Serial Gateway: running Router: disabled	5350E] [IMSI: 222101600237889]				
Users Configuration	CURREN	r updated				
FW Upgrade Conf. Management Mobile Configuration DDNS Configuration Diagnostics FW Versions Ethernet Interfaces	NETWORK Ethernet Mode (*) LAN/WAN DHCP on WAN OFF LAN IP Address 192.168.90.10 LAN Network Mass 255.255.250.0 WAN IP Address 192.168.85.10 WAN Network Mass 255.255.252.0 Default Gateway 192.168.85.11 WAN Network Mass 255.255.252.0 Default Gateway 192.168.85.11 DNS Mode 8tatic DNS Server 192.168.85.11 DNS Mode 8tatic DNS Mode 8tatic DNS Mode 8tatic DNS Server 192.168.100.1 IP Configuration from Discovery ON WEB SERVER 192.168.100.1 WEB SERVER 192.168.100.1 IP Configuration from Discovery ON WEB SERVER 192.168.100.1 WEB SERVER 192.168.100.1 HTTP/HTTPS 443 IP Configuration from Discovery 143 IP Configuration from Discovery 11 IP Configuration from Discovery 12	LAN/WAN ▼ OFF ▼ 192.168.90.101 255.255.255.0 192.168.85.105 255.255.252.0 192.168.85.1 Static ▼ 192.168.100.1 ON ▼ HTTP/HTTPS ▼ 8080 80 443 FTP/SFTP ▼ 21 22 OFF ▼ 8.8.4.4 ON ▼ 60 OFF ▼ APPLY				

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.

🖸 Z-PASS2	×	(!) Glovenni	_		×
	2.168.85.105:8080/setup.php		Q	☆ ♪	:
SENECA® General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration	Z-PASS2 Network and Services [user: admin] [logout] Firmware Version: SW003900_224 [Modem: 1231B02SIM5350E] MAC Address: C8FA81160002 [IMEI: 862264020406715] [IMSI: 22210160023784 Internet Access: Ethernet Modbus Ethernet to Serial Gateway: running Router: disabled	89]			
Users Configuration	CURRENT UPDATED				
FW Upgrade Conf. Management Mobile Configuration DDNS Configuration Diagnostics FW Versions Ethernet Interfaces	NETWORK Ethernet Mode (*) Switch Switch DHCP OFF OFF ▼ IP Address 192.168.97.101 192.168.97.101 Network Mask 255.255.25.0 255.255.255.0 IP Address 2 Enable ON ON ▼ IP Address 2 Enable ON ON ▼ IP Address 2 Enable ON I92.168.85.105 IP Address 2 Enable ON I92.168.85.105 Default Gateway 192.168.85.1 192.168.85.1 DNS Mode Static Static ▼ DNS Morey 192.168.100.1 192.168.100.1 IP Configuration from Discovery ON ON ▼ WEB SERVER Protocol (*) HTTP/HTTPS ▼ HTTP Conf Port (*) 8080 B080 8080 HTTP Dert (*) 8080 B101 HTTP/SFTP ▼ FTP Port 21 21 SFTP Port 22 22 NETWORK REDUNDANCY Enable OFF OFF ▼ Ping Address 8.8.4.4 8.8.4.4 WATCHDOG Enable (*) ON ON ▼ <t< td=""><td></td><td></td><td></td><td></td></t<>				

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.

☐ Z-PASS2	×	(!) Giovanni	_		×
← → C ① 192.	.168.85.105:8080/setup.php		Q	☆ J.	:
C 2-PASS2 ← → C 1 192. SENECA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration Event Configuration W Upgrade Conf. Management Mobile Configuration Mobile Configuration DDNS Configuration DDNS Configuration Diagnostics FW Versions Ethernet Interfaces	X 158.85.105:8080/setup.php Z-PASS2 Network and Services [user: admin] [logout] Firmware Version: SW003900_224 [Modem: 1231B02SIM5350E_20141015] MAC Address: C8F9810201D7 [IMEI: 862264020120878] Internet Access: Ethernet Modbus Ethernet to Serial Gateway: running Router: disabled Internet Access: 2010 IP Address 192.168.85.105 192.168.85.105				
	Enable OFF OFF NOTE: changing fields marked with * will cause a system restart.				
	APPLY				

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 <u>configured</u> values, whereas the latter are <u>actual</u> 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	LAN/WAN
	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.	
Ethernet Mode = "Switch"		
NETWORK/DHCP	Flag to enable/disable the DHCP	OFF
	functionality on the Ethernet	
	interface.	
NETWORK/IP Address	IP address of the Ethernet interface	192.168.90.101
	(disabled when "DHCP" is set to	
	"ON")	
NETWORK/Network Mask	Network mask of the Ethernet	255.255.255.0
	interface (disabled when "DHCP" is	
	set to "ON")	
NETWORK/IP Address 2 Enable	Flag to enable/disable the second	OFF
	IP address on the Ethernet	
	interface.	
	Note that the second IP address	
	can be enabled also when the	
	DHCP functionality is active.	
NETWORK/IP Address 2	Second IP address of the Ethernet	192.168.100.101
	interface	
NETWORK/Network Mask 2	Second network mask of the	255.255.255.0
	Ethernet interface	
Ethernet Mode = "LAN/WAN"		
NETWORK/DHCP on WAN	Flag to enable/disable the DHCP	ON
	functionality on the WAN Ethernet	
	interface	
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	255.255.255.0
	interface	
NETWORK/WAN IP Address	IP address of the WAN Ethernet	192.168.100.101
	interface (disabled when "DHCP on	
	WAN" is set to "ON")	
NETWORK/WAN Network Mask	Network mask of the WAN	255.255.255.0
	Ethernet interface (disabled when	
	"DHCP on WAN" is set to "ON")	
	·	
NETWORK/Default Gateway	Default Gateway IP address	192.168.100.1 , for Z-PASS1-
	(disabled when DHCP functionality	R0x and Z-PASS2-R0x (x=1,2)
	is enabled).	192.168.90.1, for all other
	When "Ethernet Mode" is set to	products
	"LAN/WAN", the Default Gateway	
	shall be in the WAN subnet.	
NETWORK/DNS Mode	Tells if the DNS Server shall be set	DHCP, for Z-PASS1-R0x and Z-
	statically (value: "Static") or	PASS2-R0x (x=1,2)
	dinamically assigned by the DHCP	Static, for Z-PASS1 and Z-PASS2
	Server (value: "DHCP")	
NETWORK/DNS Server	DNS server IP address (disabled	192.168.100.1 , for Z-PASS1-
	when DHCP functionality is enabled	R0x and Z-PASS2-R0x (x=1,2)
	and DNS Mode = DHCP)	192.168.90.1, for all other
		products
NETWORK/IP Configuration from	Flag to enable/disable the	ON
Discovery	possibility of changing some of the	
	network configuration parameters	
	by means of the SDD application	
	(see chapter 4)	
WEB SERVER/Protocol	Protocol used to access the web	HTTP/HTTPS
	pages:	
	HTTP/HTTPS, HTTPS, HTTP	
WEB SERVER/HTTP Conf Port	TCP port to access the	8080
	configuration pages, using HTTP	Default URL for conf pages:
	protocol.	Errore. Riterimento a
	Please note that if this parameter is	conegamento ipertestuale non valido
	set to 80 (standard HTTP port), the	
	web user site won't be available	
	anymore.	20
WEB SERVER/HITP User Port	ILP port to access the user pages,	ou Default LIPL for user pages
	using HTTP protocol.	Frrore Riferimento

-

		collegamento ipertestuale non
		valido.>
WEB SERVER/HTTPS Port	TCP port to access the	443
	configuration and user pages, using	Default URL for conf pages:
	HTTPS protocol.	Errore. Riferimento a
		collegamento ipertestuale non
		valido.
		Default URL for user pages:
		Errore. Riferimento a
		collegamento ipertestuale non
		valido.
FILE TRANSFER/Protocol	Protocol used for File Transfer:	FTP/SFTP
	FTP/SFTP, SFTP, FTP	
FTP Port	TCP Port for FTP protocol	21
SFTP Port	TCP Port for SFTP protocol	22
NETWORK REDUNDANCY/Enable	Flag to enable/disable the	OFF
	"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	
NETWORK REDUNDANCY/Ping	IP Address used as ping destination	8.8.4.4
Address	to check if access to the Internet	
	through the primary interface	
	(Ethernet) is available.	
	This address shall be different from	
	the one set for "DNS Server"	
	parameter, otherwise an error is	
	shown (see figure below).	
WATCHDOG/Enable	Flag to enable/disable the	ON
	watchdog functionality	
WATCHDOG/Timeout (s)	Watchdog timeout, in seconds;	60
	when watchdog is enabled, if it's	
	not refreshed for this amount of	
	seconds, the system will be	
	rebooted.	
	Possible values are in the range	
	[303600].	

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

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:

P1 Z-PASS2	×		🤃 Govan	đ —		×		
← → C ① 192.16	8.85.104:8080/serial_ports.php				☆ 🏸	:		
						•		
🥥 JEINEUA	Z-PASS2							
General Configuration	Serial Ports [user: admin] [logout]							
Main View	Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]							
Network and Services	MAC Address: C8F9811B0000 [IMEI: 86107502	MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]						
Serial Ports	Internet Access: Mobile							
Gateway Configuration								
Real Time Clock Setup	Modbus Shared Memory Gateway: running							
VPN Configuration	Router: running							
Router Configuration								
Users Configuration		CURRENT	UPDATED					
FW Upgrade	COM1 (RS232/RS485)							
Conf. Management	Baud Rate	115200	115200 ▼					
Tag Setup	Data Bits	8	8 🔻					
Tag View	Darity	None	None V					
Mobile Configuration	Pten Dite	4	1 •					
Mobile Network	Stop bits							
DDNS Configuration	COM2 (RS485)							
Digital I/O	Baud Rate	38400	38400 🔻					
Digital I/O Configuration	Data Bits	8	8 🔻					
FW Versions	Parity	None	None •					
Ethernet Interfaces	Stop Bits	1	1 •					
	COM4 (R8485)							
	Baud Bate	38400	38400 ▼					
	Data Bits	8	8 🔻					
	Darity	None	None V					
	Stop Bits	1	1 •					
			APPLY					

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

• COM1 RS232 or RS485¹⁴

 $^{^{\}rm 14}$ 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	38400
	are:	
	200	
	300	
	600	
	1200	
	2400	
	4800	
	9600	
	19200	
	38400	
	57600	
	115200	
Data Bits	Data bits; possible values are: 5/6/7/8	8
Parity	Parity; possible values are:	None
	None/Even/Odd	
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

☐ Z-PASS2	×						😲 Giovanni	-		×
← → C () 192.168	8.85.104:8080/digic	_conf.php							☆ 🎝	:
Seneral Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	Z-PASS2 Digital I/O 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									
Router Configuration				CURRENT	UPDATED)				
FW Upgrade		Digital I/O	Configuration							l
Conf. Management Shared Memory Tag Conf. Tag Setup		Digitar vo	Input 1 Mode	Remote connection disable	Remote connection	disable T				
Tag View		C)utput 1 Mode	Remote	Remote connection	active *				
Mobile Configuration Mobile Network			Input 2 Mode	General input	General input V					
DDNS Configuration		C	utput 2 Mode	General output	General output V					
Digital I/O		Input/C	utput 1 Mode	General input	General input 🔻					
Digital I/O Configuration	Input/Output 2 Mode General output General output									
FW Versions			Security Level							
Ethernet Interfaces		0.	miss Disskla	VDN Compation	VDN Connection	•				
	APPLY	30	ervice Disable	VPN Connection	VPN Connection	•				
			Digital I/O	Status						
	DI 1	DO 1	DI 2	DO 2	DIDO 1	DIDO 2				
	LOW	LOW	LOW	LOW	LOW	LOW				

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	Remote connection disable
	operating mode of the Digital Input	
	1 (DI 1).	
	Since this is the digital input used for	
	"Remote Connection Disable"	

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

 $^{\rm 15}$ "Remote toggle" function is still to be defined.

Service".
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.

'N Boy	x Manager - 3.2.0.8							- 🗆
BOX Lan. l	SingleLan (tlc.sened Utente Connesso SUPERVIS	ca.it) SOR						SENE
us Di	ispositivi SENECA Accessi	VPN						
Dispos	sitivo/i, 2 nuovi, 0 in aggiomar	mento, 5 configurati, 0 in alla	ime					(2) Aggioma
	TAG	MAC	IMEI	STATUS	ALARM	SIGNAL	UPTIME	
۲	zpass1_C8F981160066	C8:F9:81:16:00:66	MODEM NON INSTALLA	SERVICE OFF - VPN DO.	. 🔘	-	-	Reset
۲	ELTECO	C8:F9:81:1B:00:06	861075026509463	SERVICE OFF - VPN DO.		-	-	Reset
۲	GREEN_METHANE2	C8:F9:81:02:01:D6	862264020120993	SERVICE ON - VPN UP		6/7	Last 06/10/2017 11.43.5	Reset
•	Demo	C8:F9:81:16:00:9E	862264020393319	SERVICE OFF - VPN DO.		-	-	Reset
•	zpass2s_C8F981160017	C8:F9:81:16:00:17	862264020382288	SERVICE OFF - VPN DO.		-	-	Reset
•	ZEUS001	C8:F9:81:15:00:94	MODEM NON INSTALLA	SERVICE OFF - VPN DO.		-	-	Reset
•	TOPCO	C8:F9:81:11:00:6D	862264020400825	SERVICE OFF - VPN DO.		-	-	Reset
Config	urazione CONFIGURED, u	ltimo refresh 27/09/2017 14	1.17.08	- DI1 NA		OFF	DIDO1 CONNECTION DISAE	to Configura
Con	Network 192.168	.96.0/255.255.255.0 (VPN	10.9.1.133)	ON DO1 V	N STATUS	OFF	DIDO2 INPUT	
	Versione ver. SW002940_	331, hw Z-PASS1-R02, mod	le LAN/WAN	- DI2 NA				e Elimina
				OFF DO2 O	UTPUT			

20.1.4.2 Z-PASS1

P 7.04551	~					(!) Giovanni	- 🗆 X
← → C ① 192.16	8.85.177:8080/dig	io_conf.php					¥ .
SENECA®	Z-PASS1						
General Configuration	Digital I/O Con	figuration [use	er: admin] [I	ogout]			
Main View	Firmware Vers	ion: S W003900)_224				
Network and Services	MAC Address:	C8F9811B000	0				
Serial Ports	Internet Acces	a: Ethernet					
Gateway Configuration	Modbue Ethor	not to Sorial C	atoway: rup	ning			
Real Time Clock Setup			ateway. run	ining			
PIN Configuration	Router: disable	ed					
Users Configuration				CURRENT	UPDATED		
FW Upgrade		Disting					
Conf. Management		Digital I/O C	configuration				
Digital I/O		0	utput 1 Mode	Remote connection active	Remote connection active •		
Digital I/O Configuration		0	utput 2 Mode	General output	General output V		
FW Versions				Remote	·		
Ethernet Interfaces		Input/O	utput 1 Mode	connection disable	Remote connection disable •		
		Input/O	utput 2 Mode	General output	General output 🔻		
		s	ecurity Level				
			county Lover				
		Se	rvice Disable	VPN Connection	VPN Connection		
	APPLY						
			_	_			
			Digital I/O	Status			
	DO 1	DO 2	DIDO 1	DIDO 2			
	1.011	1.011/	1.000	1.011/			
	LOW	LOW	LOW	LOW			

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	General output
	operating mode of the Digital	
	Output 2 (DO 2).	
	Possible modes are: "General	
	output" "Remote toggle" ¹⁶ .	
Input/Output 1 Mode	This parameter represents the	Remote connection disable
	operating mode of the Digital	
	Input/Output 1 (first configurable	
	digital I/O) (DIDO 1).	
	Since this is used as an input for	
	"Remote Connection Disable"	
	feature, its value ("Remote	
	connection disable") cannot be	
	changed.	
Input/Output 2 Mode	This parameter represents the	General output
	operating mode of the Digital	
	Input/Output 2 (second configurable	
	digital I/O) (DIDO 2).	
	Possible modes are: "General input"	
	"General output" "Local alarm".	
Service Disable	This parameter determines which	VPN Connection
	access services are disabled when	
	"Remote Connection Disable" digital	
	input is HIGH.	
	Possible values are: "VPN	
	Connection" "VPN Service"	
	"Internet Connection" "SMS	
	Service".	
	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 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:

Z-PASS2	Ciovenni X	-		×
← → C ① 192.168	i8.85.104:8080/rtc.php		☆ 🛛	:
	7.04669			•
INLUA 🎯 JLINLUA				
General Configuration	Real Time Clock Setup [user: admin] [logout]			
Main View	Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]			
Network and Services	MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]			
Serial Ports	Internet Access: Mobile			
Gateway Configuration	Modhue Shared Memory Gateway: running			
NBN Castingueties	would blaied memory Gateway. Furning			
Priv Conliguration	Router: running			
Users Configuration	CURRENT UPDATED			
FW Upgrade	NTP			
Conf. Management				
Shared Memory Tag Conf.				
Tag Setup	Primary Server ntp1.inrim.it ntp1.inrim.it			
Mobile Configuration	Secondary Server ntp2.inrim.it ntp2.inrim.it			
Mobile Network	Time Zone Central Europe (CET/CEST) Central Europe (CET/CEST)			
DDNS Configuration	APPLY			
Digital I/O				
Digital I/O Configuration	RTC			
EW Versions	YEAR 2017 2017			
Ethernet Interfaces	MONTH December December			
	DAY 19 19			
	HOUR 12			
	SECOND 68 58			
	SET CLOCK			

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	ON
	synchronization by means of NTP	
	protocol	
NTP/Primary Server	IP address or FQDN ¹⁷ of the Primary	ntp1.inrim.it
	NTP Server	
NTP/Secondary Server	IP address or FQDN of the Secondary	ntp2.inrim.it
	NTP Server	
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".

Z-PASS2	×			(!) Giovanni	_		×
← → C ① 192.16	8.85.104:8080/rtc.php					☆ X	
Seneral 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 Tap Conf	Z-PASS2 Real Time Clock Setup [user: ad Firmware Version: SW003900_22 MAC Address: C8F9811B0000 [II Internet Access: Mobile Modbus Shared Memory Gatewa Router: running NTP Enable	min] [logout] 24 [Modem: UC MEI: 861075026 y: running CURRENT	20GQBR03A14E1G] 500975] [IMSI: 2221016002 UPDATED	37890]			
Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network DDNS Configuration Digital I/O Digital I/O Digital VO Configuration Diagnostics FW Versions Ethernet Interfaces	Primary Server Secondary Server Time Zone	ntp1.inrim.it ntp2.inrim.it (CET/CEST)	ntp1.inrim.it ntp2.inrim.it Central Europe (CET/CEST) UTC-10:00 Aleutian UTC-09:00 Alaska UTC-09:00 Alaska UTC-08:00 Pacific Coast UTC-07:00 Arizona UTC-07:00 Chihuahua UTC-06:00 Central Zone UTC-06:00 Mexico City UTC-05:00 Bogota UTC-05:00 Eastern Zone UTC-05:00 Havana UTC-05:00 Havana UTC-04:00 Caracas UTC-04:00 Caracas UTC-04:00 Caracas UTC-04:00 Catacas UTC-04:00 Catacas UTC-04:00 Catacas UTC-04:00 Catacas UTC-04:00 Catacas UTC-04:00 Catacas UTC-04:00 Santiago UTC-03:00 Araguaina	▼ ▲ CK			

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:

Network and Services Serial Ports	MAC Address: C8F9811B0001
Digital I/O Configuration	Internet Access: Ethernet
Real Time Clock Setup	Gateway: running [Data Logger: running]
Gateway Configuration	Router: disabled
VPN Configuration	
Router Configuration	CURRENT UPDATED
Users Configuration Mobile Configuration	COM1 (RS232/RS485) Gateway Mode Modbus Shared Memory Modbus Shared Memory
Mobile Network	COM2 (RS485) Gateway Mode Modbus Shared Memory Modbus Shared Memory
DDNS Configuration Shared Memory Tag Conf.	COM4 (RS485) Gateway Mode to Serial Modbus Ethernet to Serial

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	ON
	Ethernet to Serial Gateway	
	functionality on the port	
Port	TCP port to access the Modbus	COM1: 501
	Ethernet to Serial Gateway	COM2: 502
	If three distinct values are set, three	COM4: 503
	Modbus Ethernet to Serial Gateway	
	instances are run, each handling a	

	single serial port.	
	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	1000
	Modbus RTU responses	
	The value is in milliseconds; possible	
	values are in the range [10 - 10000].	

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

Th Z-PASS2	×	(!) Ciovanni	_		×
← → C ③ 192	168.85.104:8080/gateway_conf.php		Q	☆ 🎩	:
Senation Services General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Bouter Configuration Users Configuration FW Upgrade Conf. Management Mobile Configuration Mobile Network DDNS Configuration Digital I/O Configuration	Z-PASS2 Gateway Configuration [user: admin] [logout] Firmware Version: \$W003900_228 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222101600237891] Internet Access: Mobile Gateway: running Router: running COM1 Gateway Mode COM2 Gateway Mode COM4 Gateway Mode Modbus Ethernet to Serial Modbus Ethernet to Serial • Modbus Ethernet to Serial • Modbus Ethernet to Serial •				
Digital I/O Configuration Logic Configuration SMS Configuration Phonebook Diagnostics FW Versions Ethernet Interfaces	Slave ID for Embedded I/O 254 254 Modbus Shared Memory Enable NOTE: this parameter shall be set to ON OFF OFF if Modbus Shared Memory functionality is needed				
	TCP Port 502 TCP Connections Max Number [1-50] 32 Response Mode when Resource in Fail Exception COM1 Exception Port 502				
	Response Wait Time (ms) [10-10000] 1000 1000 COM2 Enable ON ON ▼ Port 502 502 Response Wait Time (ms) [10-10000] 1000 1000 COM4				
	Enable ONONPort 502502Response Wait Time (ms) [10-10000]1000APPLY000				

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).

□ Z-PASS2	×	(1) Giovanni	– 🗆 X
← → C ③ 192	.168.85.104:8080/gateway_conf.php		९☆ 🗵 :
S SENECA® General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration	Z-PASS2 Gateway Configuration [user: admin] [logout] Firmware Version: \$W003900_228 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222101600237891] Internet Access: Mobile Gateway: running Router: running		
Users Configuration FW Upgrade Conf. Management Mobile Configuration Mobile Network	CURRENT UPDATED COM1 Gateway Mode Modbus Ethernet to Serial Modbus Ethernet to Serial Modbus Ethernet to Serial ▼ COM2 Gateway Mode Modbus Ethernet to Serial Modbus Ethernet to Serial ▼ COM4 Gateway Mode Modbus Ethernet to Serial Modbus Ethernet to Serial ▼		
DDNS Configuration Digital I/O Configuration Digital I/O Configuration Logic Configuration SMS Configuration Phonebook	Modbus Ethernet to Serial Slave ID for Embedded I/O 254 254		
Diagnostics FW Versions Ethernet Interfaces	Include shared memory Enable NOTE: this parameter shall be set to ON OFF if Modbus Shared Memory functionality is needed TCP Port 502 502		
	TCP Connections Max Number [1-50] 32 32 Response Mode when Resource in Fail Exception COM1 COM1		
	Enable ON ON ▼ Port 501 501 Response Wait Time (ms) [10-10000] 1000 1000		
	Enable ON ON ▼ Port 502 502 Response Wait Time (ms) [10-10000] 1000		
	COM4 Enable ON ON ▼ Port 502 502 Response Wait Time (ms) [10-10000] 1000		
	AFFLI		

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.

□ Z-PASS2	×	(!) Giovanni	-		×
← → C ① 192	.168.85.104:8080/gateway_conf.php		Q	☆ 🔎	:
Sentecta General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration Users Configuration EW Upgrade Conf. Management Mobile Configuration Mobile Network DDNS Configuration	Z-PASS2 Gateway Configuration [user: admin] [logout] Firmware Version: SW003900_228 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222101600237891] Internet Access: Mobile Gateway: running Router: running Router: running COM1 Gateway Mode COM2 Gateway Mode COM4 Gateway Mode COM4 Gateway Mode				
Digital I/O Configuration Digital I/O Configuration Logic Configuration SMS Configuration Phonebook Diagnostics FW Versions Ethernet Interfaces	Modbus Ethernet to Serial Slave ID for Embedded I/O Modbus Shared Memory Enable NOTE: this parameter shall be set to ON OFF OFF ▼ if Modbus Shared Memory functionality is needed TCP Port 502 502				
	TCP Connections Max Number [1-50] 32 32 Response Mode when Resource in Fail Exception Exception COMT Enable ON ON Port 501 501 Response Wait Time (ms) [10-10000] 1000 COM2				
	Enable ON ON ▼ Port 502 502 Response Wait Time (ms) [10-10000] 1000 COM4 ON ▼ Port 503 503 Response Wait Time (ms) [10-10000] 1000				
	APPLY				

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.

רץ Z-PASS2	×	(!) Ciovanni	-		×
← → C ① 192	.168.85.104:8080/gateway_conf_save.php?do=1		Q	☆ 🏃	:
← → C (i) 192 (i) 192 (i) SENECA (i) General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration Very Configuration Router Configuration Very Configuration Very Configuration Very Configuration Digital VO Configuration Digital VO Configuration Digital VO Configuration Phonebook Diagnostics FW Versions Ethernet Interfaces 	168.85.104:8080/gateway_conf_save.php?do=1 Z-PASS2 Gateway Configuration [user: admin] [logoul] Firmware Version: SW003900_228 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861076026666172] [IMSI: 222101600237891] Internet Access: Mobile Gateway: running Router: running Router: running Response Wait Time' values must be equal for COMs having the same 'Port' va Configuration not changed.	alues !	Q		

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	254
	Registers corresponding to the	

"embedded" digital I/Os (for "IO" HW	
revision).	
In Z-PASS2, this id can also be used to	
access Modbus Registers containing	
GPS information.	
Possible values: [1255].	

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)	0 (40001)
	Bit 1: DI2	
	Bit 2: DI3	
	Bit 3: DI4	
Holding Registers	Bit 0: DO1 (LSB)	0 (40002)
	Bit 1: DO2	
	Bit 2: DO3	
	Bit 3: DO4	
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
		(0: OK,
		-1: Not fixed
		-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:

P 7-PASS2	×	🤔 Ciavanni	-		Х
$\leftarrow \rightarrow C$ (1) 192	.168.85.104:8080/gateway.conf.php		Q	☆ /	:
SENECA® General Configuration Main View Network and Services Serial Ports	Z-PASS2 Gateway Configuration [user: admin] [logout] Firmware Version: SW003900_228 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222101600237891]				
Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration	Internet Access: Mobile Gateway: running Router: running				
Users Configuration FW Upgrade Conf. Management Mobile Configuration Mobile Network	CURRENT UPDATED COM1 Gateway Mode Transparent Transparent COM2 Gateway Mode Modbus Ethernet to Serial Modbus Ethernet to Serial ▼ COM4 Gateway Mode Serial Modbus Ethernet to Serial ▼				
DDNS Configuration Digital I/O Configuration Digital I/O Configuration Logic Configuration SMS Configuration	Modbus Ethernet to Serial Slave ID for Embedded VO 254 254				
Phonebook Diagnostics FW Versions Ethernet Interfaces	Inducts shaled methody Enable NOTE: this parameter shall be set to ON OFF if Modbus Shared Memory functionality is needed TCP Port 502 502 TCP Connections Max Number [1-50] 32 32				
	COM1 Virtual COM Virtual COM Operating Mode Virtual COM				
	Destination Address 192.168.90.102 Destination Port 8000 Multicast Group 224.1.0.1 224.1.0.1 224.1.0.1 Multicast Interface Ethernet Ethernet Master Master Master Data Packing Interval (ms) [0-1000] 20				
	COM2 Enable ON ON ▼ Port 502 502 Response Wait Time (ms) [10-10000] 1000 COM4 COM4 Enable ON ON ▼				
	Port 503 503 Response Wait Time (ms) [10-10000] 1000 1000 APPLY 1000 1000 1000				

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	COM1: 8000
	gateway	COM2: 8001
		COM4: 8002
Data Packing Interval	Time interval used as a criterion to	20
	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.	
	The value is in milliseconds; possible	
	values are in the range [0 - 1000].	

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	COM1: 8000
	transparen	t gatew	ay			COM2: 8001
						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	COM1: 192.168.90.102
	gateway will connect to	COM2: 192.168.90.103
		COM4: 192.168.90.104
Destination Port	The TCP/UDP port which the	COM1: 8000
	transparent gateway will connect to	COM2: 8001
		COM4: 8002

Serial Tunnel Point-to-Multipoint (Master)

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

Serial Tunnel Point-to-Multipoint (Slave)

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

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 <u>TCP protocol</u>.

Field	Meaning	Default value
Enable	This parameter enables/disables the	OFF
	Modbus Shared Memory Gateway	
	service.	
	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.	
TCP Port	Listening port for the Modbus TCP	502
	server	
TCP Connections Max Number [1-	Maximum number of TCP	32
50]	connections that can be accepted by	
	the Modbus TCP server	
Response Mode when Resource in	This parameter defines how the	Exception
Fail	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	
	value, the value in the Moubus	
	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").	
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):	
	Bit value to 0 -> means Tag Reading	
	Frror (or tag not configured)	
	Bit value to 1 -> means Tag Peading	
	So if you need to check the fail status	
	of the first 10 tags using the default	
	Area (9001 Holding Pogistors) you	
	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.	
For example if the regsiter value is:	
0x3DB = 987 = 0000 0011 1101 1011	
Tag 1 = OK	
Tag 2 = OK	
Tag 3 = FAIL	
Tag 4 = OK	
Tag 5 = OK	
Tag 6 = FAIL	
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	None
	Modbus Shared Memory Gateway	
	task is running on the serial port;	
	possibile values are: None, Master,	
	Slave	
Slave Address	Modbus Address for the RTU Slave;	1
	this is the only parameter available	
	when Task=Slave	
Timeout (ms) [10 – 10000]	Response timeout for Modbus RTU	100
	requests, in milliseconds (available	
	only when Task=Master)	
Delay between Polls (ms) [10 –	Interval between Modbus RTU	100
1000]	requests, in milliseconds (available	
	only when Task=Master)	
Read/Write Retries [0 – 10]	Maximum number of retries for	0
	Modbus RTU 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)	
Multiple Read Max Number [1 –	Maximum number of Modbus	16
32]	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	
Multiple Write Max Number [1 –	Maximum number of Modbus	16
32]	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	

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:

C ① 192.168.85.104:3080/gateway_conf_save.php?do=1 Q ★ III IIII C ① 192.168.85.104:3080/gateway_conf_save.php?do=1 Q ★ IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
SENSE General Configuration Main View Network and Services Serial Ports Gadeway Configuration Real Time Clock Selup VPN Configuration Real Time Clock Selup VPN Configuration Bodier Configuration Router: configuration VPN Configuration Router: Configuration VPN Configuration Digits I/O Configuration Digits I/O Configuration Digits I/O Configuration Ponetocok Digits I/O Configuration Pronetock Pronetock

20.1.7 VPN Configuration

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

Th Z-PASS2	×	🗘 Giovanni — 🗆 🗙
← → C ① 192.16	3.85.104:8080/vpn_files.php	☆ 🖪 :
S SENECA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	Z-PASS2 VPN Configuration [user: admin] [logout] Firmware Version: SW003900_224 [Modem: UC20GQBR03A1 MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI Internet Access: Mobile Modbus Shared Memory Gateway: running Router: running	4E1G] : 222101600237890]
Router Configuration Users Configuration FW Upgrade	CURRENT	UPDATED
Conf. Management Shared Memory Tag Conf.	VPN Mode VPN Box	VPN Box •
Tag Setup Tag View Mobile Configuration Mobile Network DDNS Configuration Digital I/O Digital I/O Configuration Diagnostics FW Versions Ethernet Interfaces	VPN Box Enable ON OFF • Server 192.168.85.176 192.168.85.176 Password seneca seneca Tag Name zpass zpass APPLY SHOW VPN STATUS SHOW VPN STATUS	<u>\$</u>

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".

Pi Z-PASS2	×		(!) Giovan	ni —		×
$\leftarrow \rightarrow C 0 192.16$	8.85.104:8080/vpn files.php				☆ ル	:
						•
SENEUA	Z-PASS2					
General Configuration	VPN Configuration [user: admin] [logout]					
Main View	Firmware Version: SW003900_224 [Modem: U	C20GQBR03A14	E1G]			
Network and Services	MAC Address: C8F9811B0000 [IMEI: 8610750	265009751 [IMSI:	2221016002378901			
Serial Ports	Internet Access: Mobile		,			
Gateway Configuration	Internet Access. Mobile					
Real Time Clock Setup	Modbus Shared Memory Gateway: running					
VPN Configuration	Router: running					
Router Configuration						
Users Configuration		CURRENT	UPDATED			
FW Upgrade						
Conf. Management	VPN Mode	VPN Box	OpenVPN •			
Tag Setup						
Tag View	VPN Files					
Mobile Configuration	Configuration File					
Mobile Network	NOTE 1: the file will be renamed as 'ovpn.conf	Sceali file Ness	un file selezionato			
DDNS Configuration	NOTE 2: in options requiring a file ("ca", "cert", "key"					
Digital I/O	etc.), only filename must be specified (without path)					
Digital I/O Configuration	CA certificate	Scegli file Ness	un file selezionato			
FW Versions	Client certificate	Seeali file Need	un filo colozionato			
Ethernet Interfaces	(.crt)	Scegii nie Ness	un me selezionato			
	Client key (.key)	Scegli file Ness	un file selezionato			
	Additional File	Scegli file Ness	un file selezionato			
	UPLOAD RESET					
		1				
	VPN Configuration					
	Enable	OFF	OFF V			
	APPLY SHOW VPN STATUS					

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 are¹⁸:

- 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 <u>no path</u>, 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.

۲۹ Z-PASS2	× Giovani	-			×
← → C (i) 192.168	3.85.104:8080/vpn_upload_files_cust.php		☆	J.	:
SENECA®	Z-PASS2				
General Configuration	VPN Configuration [user: admin] [logout]				
Main View	Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]				
Network and Services	MAC Address: C8E9811B0000 [IME]: 8610750265009751 [IMS]: 222101600237890]				
Serial Ports					
Gateway Configuration	Internet Access: Mobile				
Real Time Clock Setup	Modbus Shared Memory Gateway: running				
VPN Configuration	Router: running				
Router Configuration					
Users Configuration	Upload: CLIENT1a.conf				
FW Upgrade	Size: 193 bytes				
Conf. Management	Stored in: /home/config/vpn/ovpn.conf				
Shared Memory Tag Conf.	Upload: ca.crt				
Tag View	Size: 1120 butee				
Mobile Configuration	Size. 1135 Dytes				
Mobile Network	Stored in: /home/config/vpn/ca.crt				
DDNS Configuration	Upload: CLIENT1.crt				
Digital I/O	Size: 3600 bytes				
Digital I/O Configuration	Stored in: /home/config/vpn/CLIENT1.crt				
EW Versions					
Ethernet Interfaces	opioad. Other Trikey				
	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"):

Z-PASS2	×	(!) Ciovanni	-			×
← → C () 192	.168.85.104:8080/vpn_files.php?showinfo=1		Q	ጵ	۶	:
SERVECA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Paular Configuration	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					
Users Configuration	CURRENT UPDATED					
FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network DDNS Configuration Digital I/O Digital I/O Digital I/O Configuration Diagnostics FW Versions Ethernet Interfaces	VPN Mode OpenVPN OpenVPN VPN Files Configuration File (ovpn or .conf) Scegli file Nessun file selezionato NOTE 1: the file will be renamed as 'ovpn.conf' Scegli file Nessun file selezionato NOTE 2: in options requiring a file ("cat", "cet", "key" Scegli file Nessun file selezionato CA certificate (.crt) Scegli file Nessun file selezionato Client certificate (.crt) Scegli file Nessun file selezionato Client key (.key) Scegli file Nessun file selezionato UPLOAD RESET Scegli file Nessun file selezionato UPLOAD RESET VPN Configuration Enable OFF OFF ▼ APPLY HIDE VPN STATUS Disconnected 0.0.0 Stopped 0.0.0 0.0 penVPN 8tatus Stopped 0.0 VPN Files (size in bytes) 0.0 0 VPN Files (size in bytes) 0.0 0 VPN Files (size in bytes) 0.0 0 NOTE: these files can be downloaded via FIP trom 'home/config/tpn' directory. CLIENT1.crt (3600) CLIENT1.crt (3600) CLIENT1.ety (9					

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.

F											_	
OpenVPN_Client - user@192.168.85.117 - W	inSCP									-		×
Locale Seleziona File Comandi Sessione C	pzioni Remo	oto Aiuto										
🚳 🎲 Coda 👻 🕂 🔁 🔁 Sincronizza	🗩 🦸 💽		Impostazioni trasferim	ento Prede	finito	- 🛃 -						
📮 user@192.168.85.117 🚅 Nuova sessione												
💶 Desktop 🔹 🥌 😨 🛛 🖛 🔹	» - i 🗈 🖻	a 🏫 🥭 🐁				- vpn - 🚰 😨 🛛 🖛>	- 🗈 🔽	🏫 <i> </i> 🔁 🔝 Trova file	R_			
📳 Upload 👻 📝 Modifica 👻 🚮 🕞 P	roprietà 📑					📲 Download 👻 📝 Modifica 👻 🛃 🕞 P	roprietà 📔 🖆					
C:\Users\Spagiari\Desktop\OpenVPN_Client						/home/config/vpn						
Nome	Dimensi	Тіро	Modificato	Attr		Nome	Dimensi	Modificato	Diritti	Proprietario		
▲		Cartella superi	16/09/2016 15.56.06			±		20/09/2016 09.26.52	rwxr-xr-x	root		
🛱 ca.crt	2 KB	Certificato di s	04/05/2015 09.30.28	a		🔄 ca.crt	2 KB	20/09/2016 10.42.53	rw-rr	root		
CLIENT1.conf	1 KB	File CONF	06/09/2016 14.19.40	a		CLIENT1.crt	4 KB	20/09/2016 10.42.53	rw-rr	root		
CLIENT1.crt	4 KB	Certificato di s	04/05/2015 09.30.42	a		CLIENT1.key	1 KB	20/09/2016 10.42.53	rw	root		
CLIENT1.key	1 KB	File KEY	04/05/2015 09.30.40	a		📓 ovpn.conf	1 KB	20/09/2016 10.42.53	rw-rr	root		
CLIENT1a.conf	1 KB	File CONF	07/09/2016 08.26.05	а								
CLIENT1a.ovpn	1 KB	File OVPN	07/09/2016 08.26.05	а								
CLIENT2.crt	4 KB	Certificato di s	04/05/2015 09.30.44	а								
CLIENT2.key	1 KB	File KEY	04/05/2015 09.30.44	а								
CLIEN I 53.crt	4 KB	Certificato di s	04/05/2015 09.33.54	a								
CLIENT53.key	1 KB	File KEY	04/05/2015 09.33.52	a								
CLIEN 154.0vpn	I KB	File OVPIN	06/05/2015 15.23.11	а								
						٢						>
0 B di 15.504 B in 0 di 11						0 B di 5.844 B in 0 di 4						
									G SE	TP-3 💷	0.0	0.52

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

	192.168.85.117:8080 dice:			×
¢	This will delete VPN files. Are you sure ?			
٤.				
0		ОК	Annulla	

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

	192.168.85.117:8080 dice:	×
	VPN is enabled: files can't be deleted.	
¢	ОК	
٤		

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	OFF
	connectivity; when enabled, Z-PASS	
	will run the Open VPN process with	
	the loaded configuration	

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:

P1 Z-PASS2	x Gavenni –	. 🗆	×
← → C (i) 192.16	8.85.104:8080/vpn_save.php?do=1	☆ 🗵	:
SENEC A®	Z-PASS2		
	VDN Configuration (upon admin) [[arout]		
General Configuration			
Network and Services	Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]		
Serial Ports	MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]		
Gateway Configuration	Internet Access: Mobile		
Beal Time Clock Setun	Modbus Shared Memory Gateway: running		
VPN Configuration			
Bouter Configuration	Notier. fulling		
Users Configuration			
FW Uporade	VPN files are not loaded yet ! Configuration not changed.		
Conf. Management			
Shared Memory Tag Conf.			
Tag Setup			
Tag View			
Mobile Configuration			
Mobile Network			
DDNS Configuration			
Digital I/O Configuration			
Diagnostics			
FW Versions			
Ethernet Interfaces			

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:

Z-PASS2	×	😲 Giovanni	-
← → C ① 192.	168.85.104:8080/vpn_files.php?showinfo=1		ର 🕁 🔼
SENERCA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	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	1]	
Users Configuration	CURRENT UPDATED		
FW Upgrade			
Tag Setup Tag View Mobile Configuration Mobile Network DDNS Configuration Digital I/O Digital I/O Digital I/O Diagnostics FW Versions Ethernet Interfaces	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 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) Scegli file Nessun file selezionato Client certificate (.crt) Scegli file Nessun file selezionato Client key (key) Scegli file Nessun file selezionato VPLOAD RESET Scegli file Nessun file selezionato UPLOAD RESET VPN Configuration Scegli file Nessun file selezionato UPLOAD RESET VPN Configuration Scegli file Nessun file selezionato UPLOAD RESET VPN Status Disconnected 0.0.0.0 OpenVPN Status Stopped 0.0.0.0 Stopped 0.0.0 Note VPN Files (size in bytes) 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 NOTE: these files can be downloaded via FTP VPN Files (size in bytes) <td< td=""><td></td><td></td></td<>		
	CLIENT1.key (912) ca.crt (1139) ovpn.conf (218) REFRESH		

B 7-04551 / 7-0455	2 *	🔑 Giovanti	- 🗆 X
$\epsilon \rightarrow \mathbf{C}$ (19)	2.168.85.103:8080/vpn_files.php?showinfo=1		९☆ 🗵 :
← → C ① 19 ← → C ① 19 Serial Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration Router Configuration FW Upgrade Mobile Network Diagnostics Ethernet Interfaces Ethernet Interfaces	2.168.85.103:8080/vpn_files.php?showinfo=1 Z-PASS1 / Z-PASS2 VPN Configuration [user: admin] [logout] Firmware Version: SW003900_205 [Modem: 1231B02SIM5350E] MAC Address: C8FA81160002 Internet Access: Mobile Modbus Bridge: running Router: disabled VPN Mode OpenVPN		
	CLIENTI.crt (3600) CLIENTI.key (912) ca.crt (1139) ovpn.conf (193) REFRESH		

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

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	/PN connection is working properly			
	Dlinking	VDN connection is not working properly			
	Blinking	VPN connection is not working property			
	OFF	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.

 □ Z-PASS2	(1) Giovenni — — — — — — — — — — — — — — — — — —	×
← → C ① 192.16	8.85.104:8080/vpn_files.php	:
Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	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	
Router Configuration Users Configuration FW Upgrade Conf. Management	CURRENT UPDATED	
Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network DDNS Configuration Digital I/O Digital I/O Digital I/O Configuration Diagnostics FW Versions Ethernet Interfaces	VPN Mode VPN Box VPN Box Enable OFF Server 192.168.85.176 Password seneca Tag Name zpass Zpats Zpats	

The "VPN Box" section contains the following parameters:

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

	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"	192.168.90.1
	server	
VPN BOX/Password	Password to access the "VPN Box"	seneca
	server	
VPN BOX/Tag Name	Mnemonic name used to uniquely	zpass
	identify the Z-PASS; if the default	
	("zpass") value is left, the Device will	
	register as "zpass_ <macaddress>"</macaddress>	
	on the VPN Box	

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:

│ [ʰ Z-PASS2	(1) Giovanni —		×
← → C ① 192.16	68.85.104:8080/vpn_files.php?showinfo=1	☆ 😕	:
SERNECA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	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		
Router Configuration Users Configuration			
FW Upgrade	CONNENT OPDATED		
Conf. Management Shared Memory Tag Conf. Tag Setup	VPN Mode VPN Box VPN Box VPN Box VPN Box		
Tag View	VPN Box		
Mobile Configuration	Enable OFF OFF •		
Mobile Network	Server 192.168.85.176 192.168.85.176		
DDNS Configuration	Password seneca seneca		
Digital I/O	Tag Name zpass ZDass		
Digital I/O Configuration	APPLY HIDE VPN STATUS		
FW Versions			
Ethernet Interfaces	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		

− Z-PASS2	بن ش x	lovenni —			×
$\leftarrow \rightarrow C \bigcirc 19216$	8 85 104:8080/vpp files php?showinfo=1		*	2	:
V / U 152.10			м		•
Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration Users Configuration	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 UPDATED				
FW Upgrade	of brief				
Conf. Management Shared Memory Tag Conf. Tag Setup	VPN Mode VPN Box VPN Box VPN Box				
Tag View	Enable ON ON V				
Mobile Configuration	Server 192 168 85 176 192 168 85 176				
DDNS Configuration					
Digital I/O	Password seneca Seneca				
Digital I/O Configuration	Tag Name zpass zpass				
Diagnostics	APPLY HIDE VPN STATUS				
FW Versions	VPN Status				
FW Versions Ethernet Interfaces	VPN StatusConnection StatusConnectedIP Address10.9.0.1OpenVPN StatusRunningRX Packets / Bytes0 / 0TX Packets / Bytes0 / 0VPN Box TypePoint-to-PointVPN Box StatusOK (Configured)REFRESH				

P1 Z-PASS2	×	🥵 Giovanni — 🗆 🗙
← → C ① 192.16	8.85.104:8080/vpn_files.php?showinfo=1	☆ 🗵 :
SERVECA® General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	Z-PASS2 VPN Configuration [user: admin] [logout] Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 2221016002 Internet Access: Mobile Modbus Shared Memory Gateway: running Router: running	:37890]
Router Configuration Users Configuration EW Unoracle	CURRENT UPDA	\TED
Conf. Management Shared Memory Tag Conf. Tag Setun	VPN Mode VPN Box	T
Tag View Mobile Configuration Mobile Network	VPN Box Enable ON ON Server 192.168.85.176 192.168.85.176	
DDNS Configuration Digital I/O Digital I/O Configuration Diagnostics	Password seneca Tag Name zpass APPLY HIDE VPN STATUS	
FW Versions Ethernet Interfaces	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 (Configure	:d)
	REFRESH gspagiari	

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		No response has been received from the VPN Box	
Box)		(response timeout)	
Error (Invalid response from		A response has been received whose content is	
VPN Box)		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	
ОК		The Z-PASS has just been registered on the VPN	
		Box	
ОК	New	The Z-PASS is registered on the VPN Box, but it is	
		not configured yet ("Single LAN" only)	
ОК	Configuration updated	The Z-PASS configuration has just been updated	
ОК	Configured	The Z-PASS is properly configured and available	
		for VPN connection	
ОК	Ban	The Z-PASS has been banned	
ОК	Not found	The Z-PASS is unknown for the VPN Box; this	
		happens when Z-PASS registration is deleted on	
		the VPN Box	
ОК	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)	
ОК	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:

Image: Control 0 12.168.55.1000/mobile_router.php Image: Control Image: Control<	□ [¹] Z-PASS2	×				Govenni	-			×
SPECION 2-PASS Secure Conjugation Period Conjugation Native Secure Conjugation Disc Lead Advises Native Site Site Site Site Site Site Site Sit	← → C 0 1	92.168.85.104:8080/mobile_router.php					Q	☆	ん	:
Namoka stavisa Van Pore MAC Address: CSF 91:110000 [ME: 80107:0205000172] [MSH: 22010100237903] MAC Address: CSF 91:110000 [ME: 80107:0205000172] [MSH: 22010100237903] MAC Address: CSF 91:110000 [ME: 80107:0205000172] [MSH: 22010100237903] MAC Address: CSF 91:110000 [ME: 80107:0205000172] [MSH: 22010100237903] Mater disabled Mater disabled	SENECA General Configuration Main View	Z-PASS2 Router Configuration [user: admin] [logout] Firmware Version: \$W003900, 232 [Modem:]	IC20GOBB03A	4E1G1						•
General Configuration Minter Accoses: Enthemed Weit Configuration General continuing (Data Logger: running (no group enabled)) Weit Configuration Restance Configuration Name Configuration Restance Restance Origit Name Second Namounde Restance Restance Origit Name Second <td>Network and Services Serial Ports</td> <td>MAC Address: C8F9811B0000 [IMEI: 8610750</td> <td>026666172] [IMS</td> <td>l: 222101600237893]</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Network and Services Serial Ports	MAC Address: C8F9811B0000 [IMEI: 8610750	026666172] [IMS	l: 222101600237893]						
Rever Configuration DURBENT UPDATED RVU Upper A Boade Enable OFF OFF T Cord Management Italiands Italia	Gateway Configuration Real Time Clock Setup VPN Configuration	Gateway: running [Data Logger: running (no Router: disabled	group enabled)]						1
PM Longenering Control Magneting Control Magneting Ethernet Bandwickting, Lindingson, Understand, Unders	Router Configuration		CURRENT							-1
Cord Magnetoria Ellivernel Bandradith Unitations Unitational Unitational Tag Steve 0000 0000 0000 Tag Steve 00000 00000 00000 TCP Steve 000000 000000 000000 000000 TCP Steve 000000000 0000000000 000000000000000000000000000000000000	FW Upgrade	Router Enable	OFF	OFF V						
Shared Memory Tag Veni DMS 50400 Tag Veni DMS Enable OF Tog Veni DMS Enable OF CPS Baree DMS Configuration Mobile Configuration DMS Print Address 102:108:0021 DDNE Configuration DMS Print Address 102:108:0021 DQNE Configuration DMS Configuration Dglie LO Configuration DMS Enable Monoch	Conf. Management	Ethernet Bandwidth Limitation	Unlimited	Unlimited V						
Ind yele// DNS Endle ON ON ON TCP Seven DHOP Seven Endles OF OF OF Mobie Configuration DHOP Find Addres 192 168 39.210 192 168 39.210 DNS Ecologuration DHOP Lasse Time (mini 15 15 Digle IO Configuration Use Load Addresses Through (17) 15 Digle IO Configuration Use Load Addresses Through (17) 15 Digle IO Configuration Use Load Addresses Through (17) 15 Digle IO Configuration Description 0FF Opportune Endle ON 0FF 0FF Digle IO Configuration Description 0FF 0FF Opportune Endle ON 0FF 0FF Opportune Endle ON 0FF 0FF Opportune	Shared Memory Tag Conf.	DNS-DHCP								
Industrial DBHD Parve Enable OFF Image: Configuration Mobile Configuration DBHD Planst Addees 192 105 80 201 192 105 80 201 DDHD Configuration DBHD Planst Addees 192 105 80 201 192 105 80 201 DDHD Configuration DBHD Planst Addees 192 105 80 201 192 105 80 201 DDHD Configuration DBHD Planst Addees 192 105 80 201 192 105 80 201 Digital ID Configuration DBHD Planst Addees 192 105 80 201 192 105 80 201 Digital ID Configuration DBHD Planst Addees 192 105 80 201 192 105 80 201 Digital ID Configuration DBHD Planst Addees IPE 100 100 IPE 100 100 Digital ID Configuration DBHD Planst Addees IPE 100 100 IPE 100 100 Digital ID Configuration DBHD Planst Addees IPE 100 100 IPE 100 100 General Enrice DHD Planst Addees IPE 100 100 IPE 100 100 General Enrice Port Magping / Vinus Server 2 IPE 100 100 IPE 100 100 General Enrice Port Magping / Vinus Server 2 IPE 100 100 IPE 100 100 General Enrice <td>Tag Setup</td> <td>DNS Enable</td> <td>ON</td> <td>ON V</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Tag Setup	DNS Enable	ON	ON V						
Ideals Configuration DBOP Field Address 192:168.90.201 DDBC Configuration DBOP Lass Trices 0.100 192:168.90.210 DDBC Configuration DBOP Lass Trices 0.100 15 DDBA Configuration DBOP Lass Trices 0.100 0 DBAR Configuration DBAR Local Addresses through VPT Image: 0 Lagi-Configuration DBAR Local Addresses through VPT Image: 0 Data Local Addresses through VPT Image: 0 Image: 0 Data Local Addresses through VPT Image: 0 Image: 0 Data Local Addresses through VPT Image: 0 Image: 0 Data Local Addresses through VPT Image: 0 Image: 0 Data Local Addresses through VPT Image: 0 Image: 0 Data Local Addresses through VPT Image: 0 Image: 0 Data Local Addresses through VPT Image: 0 Image: 0 Data Local Addresses through VPT Image: 0 Image: 0 Data Local Addresses through VPT Image: 0 Image: 0 Data Local Addresses through VPT Image: 0 Image: 0 Data Local Addreses Image: 0 Image:	TCP Servers	DHCP Server Enable	OFF	OFF V						
Mobile Metanovis DHOP Last Address 192 168 90 210 DOYS Configuration DHOP Last Address Time (m) 15 Dight IO Configuration Like Local Addresses Strong VPI Logic Configuration Strong Configuration OFF Configuration StR Configuration Mobile Metricox Firewal OFF Configuration Prostocic Mobile Metricox Firewal OFF Configuration Disgonation Port Magning / Virtual Server 1 TOPUDP	Mobile Configuration	DHCP First Address	192.168.90.201	192.168.90.201						
DDNB Configuration Digital I/O Configuration Capital I/O Configuration Use Local Addresses through VPH Eacen Configuration SMS Configuration Enable ON Enable ON SMS Configuration I/Addresses through VPH Eacen Configuration ON Darge I/O Configuration I/Addresses through VPH Eacen Configuration ON Despondation Protection Protection Phone Eacen I/Addresses through VPH and Beaver Eacen Configuration ON ON Carsent Searoge Eacen I/O Protection OPAUDP Concip Configuration Searose I/Addresses I I/OPAUDP Concip Configuration Searose I/Addresse I I/OPAUDP Concip Configuration Concip Configuration I/OPAUDP I/OPAUDP Port Mapping / Virtual Seares I I/OPAUDP I/OPAUDP Fearer Mapping / Virtual Seares I I/OPAUDP I/OPAUDP Fearer Mapping / Virtual Seares I I/OPAUDP I/OPAUDP F	Mobile Network	DHCP Last Address	192.168.90.210	192.168.90.210						
Light ID Configuration Use Local Addressee through VPH Logic Configuration Enable OFF • Silk Configuration Indentwork Firewart Phonebook Indentwork Firewart Dagnontics Configuration Expense Indentation Port Mapping / Virtual Server 1 Provision Provision Server IP Address CPUUP • General Server IP Address CPUUP • Port Mapping / Virtual Server 2 CPUUP • Port Mapping / Virtual Server 3 CPUUP • External Port CPUUP • External Port <td>DDNS Configuration</td> <td>DHCP Lease Time (min)</td> <td>15</td> <td>15</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	DDNS Configuration	DHCP Lease Time (min)	15	15						
Light Configuration BMB Config	Digital I/O Configuration	Use Local Addresses through VPN			,					
BMS Configuration Indebite Network Firewal Imagination Indebite Network Firewal Imagination Port Mapping / Virtual Saver 1 Imagination Port Mapping / Virtual Saver 1 Port Mapping / Virtual Saver 2 Port Mapping /	Logic Configuration	Enable	OFF	OFF V						
Productord Desprocitors Prov Mapping / Virtual Server 1 Protector Internationa Detat Logger (50 found) Care wat Settings Coup Octiguation SO File Manager SD File Manager Protector Internationa SD File Manager Coup Octiguation So File Manager Port Mapping / Virtual Server 2 Port Mapping / Virtual Server 4 Coup Octiguation Coup Octiguation Coup Octiguation So File Manager Coup Octiguation Coup Octiguation Coup Octiguation Cou	SMS Configuration	Mobile Network Firewall								
PW Variaors Port Magping / Virtual Server 1 Ethernist Interfaces Protocosi General Settings CEVENDP ▼ General Settings Sarver 1P Address BD File Manager Internal Port BD File Manager Internal Port Port Magping / Virtual Server 2 Port Magping / Virtual Server 3 Ethernial Port Internal Port Sarver 1P Address Internal Port Internal Port Port Magping / Virtual Server 3 Port Magping / Virtual Server 4 Port Magping / Virtual Server 4 Port Magping / Virtual Server 4 Port Magping / Virtual Server 4 Port Magping / Virtual Server 4 Protocol Port Magping / Virtual Server 4 Protocol Port Magping / Virtual Server 4 Protocol External Port Port Magping / Virtual Server 4 Port Magping / Virtual Server 4 Protocol External Port Port Magping / Virtual Server 4 Port Magping / Virtual Server 5 Port Magping / Virtual Server 4 Port Magping / Virtual Server 5 Port Magping / Virtual Server 5 Port Magping / Virtual Server 6 Port Magping / Virtual Server 6 Port Magping / Port Portoco <t< td=""><td>Phonebook Diagnostica</td><td>Enable</td><td>ON</td><td>ON T</td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	Phonebook Diagnostica	Enable	ON	ON T						
IPMIRAD Protocol TOP/UDP ▼ Data Logger (S0 found) External Pot	FW Versions	Part Manning (Virtual Convert								
Data Logor (SD found) EPidodo ICP/UDP ▼ General Setting Carried Carr	Ethernet Interfaces	Fort mapping / virtual server i	TODUDD	TODUDD -						
Unit if if obtaining of internal Port BD Fie Manager Internal Port Protocol TOP/UDP CP/UDP Protocol TOP/UDP Internal Port Server IP Address Internal Port Protocol TOP/UDP Internal Port Protocol TOP/UDP Internal Port Protocol TOP/UDP CP/UDP External Port Protocol TOP/UDP CP/UDP External Port Protocol TOP/UDP CP/UDP External Port Server IP Address Internal Port C Protocol TOP/UDP External Port Server IP Address Internal Port </td <td>Data Logger (SD found)</td> <td>Protocol Esternal Rest</td> <td>TCP/UDP</td> <td>TCP/UDP V</td> <td>1</td> <td></td> <td></td> <td></td> <td></td> <td></td>	Data Logger (SD found)	Protocol Esternal Rest	TCP/UDP	TCP/UDP V	1					
CUCP Origination Server IP Address Port Mapping / Virtual Server 2 Port Mapping / Virtual Server 3 Port Mapping / Virtual Server 4 Port Mapping / Virtual Server 5	Group Configuration	Carrier ID Address								
Port Mapping / Virtual Server 2 Protocol TOP/UDP External Port Server IP Address Internal Port Port Mapping / Virtual Server 3 Port Mapping / Virtual Server 4 External Port Server IP Address Internal Port Server IP Address Internal Port Server IP Address Internal Port Port Mapping / Virtual Server 4 Server IP Address Internal Port Server IP Address Server IP Address Internal Port Server IP Address Internal Port Server IP Address Internal Port	SD File Manager	Server IP Address								
Port Mapping / Virtual Server 2 Protocol TCP/UDP ▼ External Port Port Mapping / Virtual Server 3 Port Mapping / Virtual Server 4 Port Mapping / Virtual Server 4 Port Mapping / Virtual Server 5 Port Mapping / Virtual Server 4 Port Mapping / Virtual Server 5 Port Mapping / Virtual Server 5 Protocol TCP/UDP ▼ Port Mapping / Virtual Server 5 Protocol TCP/UDP ▼ Port Mapping / Virtual Server 5 Protocol TCP/UDP ▼ Port Mapping / Virtual Server 5 Port Mapping / Virtual Server 5 Port Mapping / Virtual Server 6 Protocol TCP/UDP ▼ Port Mapping / Virtual Server 7 Protocol TCP/UDP ▼ Port Mapping / Virtual Server 7		Internal Port								
Protocol TCP/UDP ▼ External Port Server IP Address Internal Port Protocol TCP/UDP ▼ Protocol TCP/UDP ▼ External Port Server IP Address Internal Port Server IP Address Protocol TCP/UDP ▼ External Port Server IP Address Protocol TCP/UDP ▼ External Port Server IP Address Internal Port Server IP Address Internal Port Protocol TCP/UDP ▼ Protocol TCP/UDP ▼ External Port Server IP Address Internal Port		Port Mapping / Virtual Server 2								
Server IP Address Internal Port Port Mapping / Virtual Server 3 Protocol TCP/UDP TCP/UDP Contract 1 Server IP Address Internal Port Server IP Address Protocol TCP/UDP Port Mapping / Virtual Server 3 Protocol TCP/UDP Port Mapping / Virtual Server 4 Protocol TCP/UDP Contract 1 Contract 1 Protocol TCP/UDP Contract 1 Contract 1 </td <td></td> <td>Protocol</td> <td>TCP/UDP</td> <td>TCP/UDP V</td> <td>1</td> <td></td> <td></td> <td></td> <td></td> <td></td>		Protocol	TCP/UDP	TCP/UDP V	1					
Server IP Address Internal Port Port Mapping / Virtual Server 3 Port Mapping / Virtual Server 3 Server IP Address Internal Port Port Mapping / Virtual Server 4 Port Mapping / Virtual Server 5 Port Mapping / Virtual Server 5 Port Mapping / Virtual Server 5 Internal Port Server IP Address Internal Port Server IP Address Internal Port ICP/UDP ▼		External Port								
Internal Port Port Mapping / Virtual Server 3 Protocol TCP/UDP ▼ Contract 100 Cont		Server IP Address								
Port Mapping / Virtual Sarver 3 Protocol TCP/UDP ▼ External Port		Internal Port								
Protocol TCP/UDP ▼ External Port		Port Mapping / Virtual Server 3								
External Port Server IP Addrese Internal Port Port Mapping / Virtual Server 4 Protocol TCP/UDP ▼ External Port Server IP Addrese Internal Port Server IP Addrese Internal Port Port Mapping / Virtual Server 5 Port Mapping / Virtual Server 5 Server IP Addrese Internal Port		Protocol	TCP/UDP	TCP/UDP V	1					
Server IP Addrese Internal Port Port Mapping / Virtual Server 4 Protocol TCP/UDP ▼ External Port Server IP Addrese Internal Port Port Mapping / Virtual Server 5 Port Mapping / Virtual Server 5 Protocol TCP/UDP ▼ External Port Server IP Addrese Internal Port Inte		External Port								
Internal Port Port Mapping / Virtual Sarver 4 Protocol TCP/UDP		Server IP Address								
Port Mapping / Virtual Sarver 4 Protocol TCP/UDP ▼ External Port		Internal Port								
Protocol TCP/UDP ▼ External Port Server IP Addresa Internal Port Port Mapping / Virtual Server 5 Protocol TCP/UDP ▼ External Port Server IP Addresa Internal Port Server IP Addresa Internal Port		Port Mapping / Virtual Server 4								
External Port Server IP Addresa Internal Port Port Mapping / Virtual Server 5 Protocol TCP/UDP ▼ External Port Server IP Addresa Internal Port Internal Port		Protocol	TCP/UDP	TCP/UDP V	1					
Server IP Address Internal Port Port Mapping / Virtual Server 5 Protocol TCP/UDP ▼ External Port Server IP Address Internal Port Internal Por		External Port								
Internal Port Port Mapping / Virtual Server 5 Protocol TCP/UDP ▼ External Port Server IP Addresa Internal Port		Server IP Address								
Port Mepping / Virtual Server 5 Protocol TCP/UDP ▼ External Port Server IP Address Internal Port		Internal Port								
Protocol TCP/UDP TCP/U		Port Mapping / Virtual Server 5								
External Port Server IP Address Internal Port		Protocol	TCP/UDP	TCP/UDP V						
Server IP Address Internal Port		External Port								
Internal Port		Server IP Address								
		Internal Port								-

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	OFF
	functionality	
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	
	\leftrightarrow WAN).	
	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).	
	Possible values are:	
	Unlimited	
	20 Mbit/s	
	10 Mbit/s	
	1 Mbit/s	
DNS Enable	Flag to enable/disable the DNS	ON
	forwarding service	
DHCP Server Enable	Flag to enable/disable the DHCP	OFF
	service (DHCP server)	
	NOTE: this parameter can be set to	
	<u>"ON" only if the "DHCP" parameter</u>	
	of the "Network and Services" page	
	<u>is set to "OFF"</u> .	
DHCP First Address	These parameters define the range	192.168.90.201
DHCP Last Address	of IP addresses assigned by the	192.168.90.210
	DHCP server to requesting clients	
DHCP Lease Time (min)	Validity time interval for the IP	15
	address assignment, in minutes.	
	Possible values are in the range	
	[160].	

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

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

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	OFF
	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.	
	To open a port in the firewall, a	
	"Port Mapping / Virtual Server" rule	
	shall be defined.	

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.

P 7-PASS2	(1) Giovenni —			Х
	385104:8080/vpn save php2do=2			:
		M _	E.	•
SENECA [®]	Z-PASS2			
General Configuration	VPN Configuration [user: admin] [logout]			
Main View	Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]			
Network and Services	MAC Address: C8E9811B0000 [IME]: 8610750265009751 [IME]: 2221016002278901			
Serial Ports				
Bateway Configuration	Internet Access: Ethernet			
Real Time Clock Setup	Modbus Shared Memory Gateway: running			
VPN Configuration	Router: running			
Router Configuration	-			
Jsers Configuration				
FW Upgrade	VPN Box configuration changed.			
Conf. Management	Mobile Network Firewall has been enabled.			
Shared Memory Tag Conf.				
Tag Setup				
Fag View				
Mobile Configuration				
Mobile Network				
ODNS Configuration				
Digital I/O				
Digital I/O Configuration				
Diagnostics				
thernet Interfaces				

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	TCP/UDP
	protocol (or kind of port) which is	
	affected by the rule: TCP, UDP or	
	both	
External Port	TCP or UDP port which a packet was	Empty
	originally sent to	
Server IP Address	IP address which the received packet	Empty
	is forwarded to	
Internal Port	TCP or UDP port which the received	Empty
	packet is forwarded to	

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:

	30/mobile_router_save.php?do=1 ☆ onfiguration [user: admin] [logout] e Version: \$W003900_224 [Modem: UC20GQBR03A14E1G] dress: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Access: Ethernet Shared Memory Gateway: running disabled configuration changed (router not active).	Z	
 ← → C (i) 192.168.85.104:8080 SEENECAS General Configuration Main View Network and Services Berial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration Users Configuration Wodbus S Router Configuration Wodbus S Router Configuration Wodbus S Router Configuration Wupgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration 	30/mobile_router_save.php?do=1	<u>ک</u>	
SERNECA General Configuration Main View Network and Services Berial Ports Bateway Configuration Real Time Clock Setup /PN Configuration Jsers Configuration Jsers Configuration Sutter Configuration State Memory Tag Conf. Tag Setup Tag View Mobile Configuration Abile Network	onfiguration [user: admin] [logout] e Version: SW003900_224 [Modem: UC20GQBR03A14E1G] dress: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Access: Ethernet Shared Memory Gateway: running disabled configuration changed (router not active).		
General Configuration Router Co Main View Firmware Network and Services MAC Addr Serial Ports Internet A Gateway Configuration Modbus S Real Time Clock Setup Modbus S VPN Configuration Router: di Router Configuration Router: di FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network Mobile Network	onfiguration [user: admin] [logout] e Version: SW003900_224 [Modem: UC20GQBR03A14E1G] dress: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Access: Ethernet Shared Memory Gateway: running disabled configuration changed (router not active).		
General Configuration Hotter Co Main View Firmware Main View Firmware Network and Services MAC Addr Serial Ports Internet Addr Gateway Configuration Modbus S Real Time Clock Setup Modbus S VPN Configuration Router: di Router Configuration Router: di Verse Configuration Router Co EW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network Router configuration	onfiguration [user: admin] [logout] e Version: SW003900_224 [Modem: UC20GQBR03A14E1G] dress: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Access: Ethernet Shared Memory Gateway: running lisabled		
Main View Firmware Network and Services MAC Addr Serial Ports Internet A Gateway Configuration Modbus S Real Time Clock Setup Modbus S VPN Configuration Router: di Router Configuration Bouter: di VPN Configuration Router: di VPN Configuration Router Configuration Users Configuration Router Configuration FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network Setup	e Version: SW003900_224 [Modem: UC20GQBR03A14E1G] dress: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Access: Ethernet Shared Memory Gateway: running disabled configuration changed (router not active).		
Network and Services MAC Addr Serial Ports Internet A Gateway Configuration Modbus S Real Time Clock Setup Modbus S VPN Configuration Router: di Router Configuration Router: di WUpgrade Router Configuration FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network Router Configuration	dress: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Access: Ethernet Shared Memory Gateway: running disabled		
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	Access: Ethernet Shared Memory Gateway: running lisabled configuration changed (router not active).		
Gateway Configuration Modbus S Real Time Clock Setup Modbus S VPN Configuration Router: di Router Configuration Bouter: di Users Configuration Router Configuration FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network Configuration	Shared Memory Gateway: running lisabled configuration changed (router not active).		
Heal Time Clock Setup Motibula S VPN Configuration Router: di Router Configuration Router Configuration Users Configuration Router Configuration FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network Configuration	lisabled		
VPN Configuration Router: di Router Configuration Router: di Users Configuration Router Co FW Upgrade Router Co Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network	lisabled configuration changed (router not active).		
Router Configuration Users Configuration FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network	configuration changed (router not active).		
Users Configuration FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network	configuration changed (router not active).		
FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network			
Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network			
Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network			
Tag Setup Tag View Mobile Configuration Mobile Network			
Tag View Mobile Configuration Mobile Network			
Mobile Network			
DDNS Configuration			
Digital I/O			
Digital I/O Configuration			
Diagnostics			
FW Versions			
Ethernet Interfaces			

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:

Th Z-PASS2	×				Giovanni	-		×
← → C 0 1	92.168.85.104:8080/mobile_router.php					Q	☆ 🛛	. :
SENECA General Configuration Main View	Z-PASS2 Router Configuration [user: admin] [logout]		45161					Î
Network and Services Serial Ports	MAC Address: C8F9811B0000 [IMEI: 8610750	26666172] [IMSI	: 222101600237893]					
Gateway Configuration Real Time Clock Setup VPN Configuration	Gateway: running [Data Logger: running (no	group enabled)]						
Router Configuration	Kouter: running	CURRENT	UPDATED					
FW Upgrade Conf. Management Shared Memory Tag Conf.	Router Enable Ethernet Bandwidth Limitation DNS-DHCP	ON Unlimited	ON ▼ Unlimited ▼					
Tag View TCP Servers	DNS Enable DHCP Server Enable	ON OFF	ON V OFF V					
Mobile Configuration Mobile Network DDNS Configuration	DHCP First Address DHCP Last Address DHCP Last Address DHCP Lesse Time (min)	192.168.90.201 192.168.90.210 15	192.168.90.201 192.168.90.210 15					
Digital I/O Configuration Digital I/O Configuration Logic Configuration	Use Local Addresses through VPN Enable	ON	ON V					
Phonebook Diagnostics	Mobile Network Firewall Enable	ON	ON V					
Ethernet Interfaces Data Logger (SD found)	Port Mapping / Virtual Server 1 Protocol	TCP	TCP V					
Group Configuration SD File Manager	Server IP Address Internal Port	8080	8080					
	Port Mapping / Virtual Server 2 Protocol	TCP/UDP	TCP/UDP V					
	External Port Server IP Address	502 192.168.85.103	502 192.168.85.103					
	Internal Port Port Mapping / Virtual Server 3 Port Mapping / Virtual Server 3 Port	502	502					
	External Port Server IP Address	TCP/ODP						
	Internal Port Port Mapping / Virtual Server 4							
	Protocol External Port	TCP/UDP	TCP/UDP V					
	Server IP Address Internal Port							
	Fort Mapping / Virtual Server 5 Protocol External Port	TCP/UDP	TCP/UDP V					
	Server IP Address Internal Port							

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 <u>which ports are</u> <u>open in the "Mobile Network Firewall"</u>; 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.

Z-PASS2	×				Ciovanti	-			×
← → C ① 1	92.168.85.104:8080/mobile_router.php					Q	☆	J.	:
	Z-PASS2 Router Configuration [user: admin] [logout]								-
Main View	Firmware Version: SW003900_232 [Modem:]	UC20GQBR03A	14E1G]						
Network and Services	MAC Address: C8F9811B0000 [IMEI: 8610750	26666172] [IMS	6l: 222101600237893]						- 8
Serial Ports	Internet Access: Ethernet		-						
Gateway Configuration	Cotoursu munning [Date Logger munning (no	group apphad	N						- 8
VPN Configuration	Caleway, running [Data Logger, running (no	group enabled)	11						- 8
Router Configuration	Router: running								_
Users Configuration		CURRENT	UPDATED						
FW Upgrade	Router Enable	ON	ON V						- 8
Conf. Management	Ethernet Bandwidth Limitation	Unlimited	Unlimited V						
Shared Memory Tag Conf.	DNS-DHCF								
Tao View	DNS Enable	ON	ON V						
TCP Servers	DHCP Server Enable	OFF	OFF V						- 8
Mobile Configuration	DHCP First Address	192.168.90.201	192.168.90.201						- 8
Mobile Network	DHCP Last Address	192.168.90.210	192.168.90.210						- 8
DDNS Configuration	DHCP Lease Time (min)	15	15						- 8
Digital I/O Configuration	Use Local Addresses through VPN								- 8
Logic Configuration	Enable	ON	ON V						- 8
SMS Configuration	Mobile Network Firewall								- 8
Phonebook	Enoble	ON	ON T						- 8
FW Versions	Cont Manalas (Matural Oscilla)	UN	UN V						- 8
Ethernet Interfaces	Port Mapping / Virtual Server 1								- 8
Data Logger (SD found)	Protocol	TCP	TCP V	1					- 8
General Settings	External Port	8080	8080]					
SD File Manager	Server IP Address			1					
ob i no managor	Internal Port	8080	8080						- 8
	Port Mapping / Virtual Server 2								
	Protocol	TCP	TCP V						
	External Port	22	22						
	Server IP Address								
	Internal Port	22	22						
	Port Mapping / Virtual Server 3								
	Protocol	TCP/UDP	TCP/UDP V						
	External Port								- 8
	Server IP Address								- 8
	Internal Port								
	Port Mapping / Virtual Server 4								
	Protocol	TCP/UDP	TCP/UDP T						
	External Port]					
	Server IP Address								
	Internal Port								
	Port Mapping / Virtual Server 5								
	Protocol	TCP/UDP	TCP/UDP V						
	External Port								
	Server IP Address								
	Internal Port								
									-

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:

	CURRENT	UPDATED
NAT 1:1 Configuration		
Interface		WAN ~
Device IP Address		192.168.0.12
Mapped IP Address		10.0.26
Description		WAN to LAN ACCESS1
APPLY		

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:

	CURRENT	UPDATED
Static Route Configuration		
Destination Address		192.168.85.23
Subnet Mask		255.255.255.255
Gateway		192.168.80.1
Interface		LAN ~
Description		Go to 85

And then:

	CURRENT	UPDATED
Static Route Configuration		
Destination Address		192.168.82.56
Subnet Mask		255.255.255.255
Gateway		192.168.80.100
Interface		LAN V
Description		Go to 82
APPLY		

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:

Z-PASS2

OPC-UA Server Conf. [user: admin] [logout] Firmware Version: SW003900_280 [Modem: EC21EFAR02A03M4G] MAC Address: C8F9811B0001 [IMEI: 861108030033046] [IMSI: 240422600279769]

Internet Access: Ethernet

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

Router: disabled

		CU	RRENT	UPDATED
NOTE: this if Modbus	OPC-UA Server Conf. Enable parameter can be ON, only Shared Memory Gateway is			
NC av	TE: if ON, the server will be ailable at the following URL opc.tcp://IP_Address:Port/	ON		ON V
	Port	4840		4840
	Username	seneo	a	seneca
	Password	seneo	a	seneca
	Certificate Enable	OFF		OFF •
APPLY				
.сп,.	OPC-UA Servi cer,.key,.pem files must be ii .der files must be in DER (b	er Cert n PEM inary)	t <mark>ificates</mark> (ASCII) format. format.	
	Ser	ver ce	rtificate	Scegli file Nessun file selezionato
	Serv	er priv	ate key	Scegli file Nessun file selezionato
	Truste	d certi	ficate 1	Scegli file Nessun file selezionato
	Truste	d certi	ficate 2	Scegli file Nessun file selezionato
	Truste	d certi	ficate 3	Scegli file Nessun file selezionato
	Truste	d certi	ficate 4	Scegli file Nessun file selezionato
	Truste	d certi	ficate 5	Scegli file Nessun file selezionato
UPLOAD	SHOW CERTIFICATE FIL	ES	RESET	CERTIFICATE FILES

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	OFF
	server functionality	
Port	OPC-UA server TCP port	4840
Username	Username that an OPC-UA Client	empty
	shall use to connect to the server	
Password	Password that an OPC-UA Client	empty
	shall use to connect to the server	
Security Policy	Select between "None"	"None"
	Or "None, Basic128Rsa15,	
	Basic256Sha256"	

-

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:

figuration Name				
iscovery Advanced				
ndpoint Filter: No Filter				
🔍 Local				
Y 😼 Local Network				
> 💆 Microsoft Wi	ndows Network			
> 💇 Microsoft Ter	minal Services			
Veb Client N	etwork			
 Keverse Discover Reverse Discover 	/ k to Add Poverse F			
Custom Discover	k to Add Reverse L	iscovery		1
Custom Discover	r k to Add Server >			/
Recently Used				
Seneca OPCI	IA Application			_
	Enter URL		2 3	×
En	ter the URL of a con	nputer with discov	ervice runnii	ng:
	pc.tcp://192.168.8	5.103:4840		~
		ОК	Cancel	
Authentication Settings				
Anonymous				
Username				Store
Password				
O				
Private Key				

Then press OK.

Now the server capability are shown:

Add Server	? ×
Configuration Name	
Discovery Advanced	
Endpoint Filter: No Filter	•
 Q. Local ✓ Solution ✓ Microsoft Windows Network ✓ Microsoft Terminal Services ✓ Web Client Network ✓ Solution ✓ Reverse Discovery ✓ < Double click to Add Reverse Discovery > 	/
 Charle Click to Add Server> Couble Click to Add Server> Copc.tcp://192.168.85.103:4840 Seneca OPC UA Application (opc.tcp) None - None (uatcp-uasc-uabinary) Basic128Rsa15 - Sign (uatcp-uasc-uabinary) Basic128Rsa15 - Sign & Encrypt (uatcp-uasc-uabinary) Basic256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary) Basic256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary) Seneca OPC UA Application 	
Anonymous Username Password] Store
Certificate Private Key	
Connect Automatically	Cancel

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

Add Server		?	×
onfiguration Name Seneca	OPC UA Application		_
Discovery Advanced			
Advanced			
Endpoint Filter: No Filter			•
🔍 Local			
V 🐼 Local Network			
> 💆 Microsoft V	(indows Network		
> 💆 Microsoft T	erminal Services		
> 💇 Web Client	Network		
✓ 10 Reverse Discove	ny		
V Curbus Dia	ick to Add Reverse Discovery >		
 Custom Discovi Custom Discovi 	ery isk to Add Server		
V onc top://10	12 168 85 103-4840	¬/	
× Ø Senecal	OPC LIA Application (one ten)	1/	
a Non	e - None (uatop-uasc-uabinary)	V	
🖉 Basi	c128Rsa15 - Sign (uatcp-uasc-uabinary)	Λ	
Basi	c128Rsa15 - Sign & Encrypt (uatcp-uasc-uabinary)	/	
🖉 Basi	c256Sha256 - Sign (uatcp-uasc-uabinary)		
🔒 Basi	c256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary)		
🗸 🕑 Recently Used			/
Seneca OPC	UA Application		
A			/
Authentication Settings			
 Anonymous 		- ×	
Username	senera	Store	1
Bacquerd]	
Passworu]	
Certificate			
O Private Key		1	
Private Key			
Connect Automatically			
	OK	Cano	ei

Then press OK:

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

🔡 Ur	nified Automation UaExpert - The O	PC Unified A	rchitecture Cli	ent - NewProje	ect*	
File	View Server Document Set	tings Help				
	🥖 🕞 🕑 🗣 🖣	= 🌣 🕺	(🔌 🚨	PX	D	
Project	:	🗗 🗙 🗖 Dat	a Access View			
× U × Addres	 Project Servers Seneca OPC UA Applicati Documents Data Access View 	on A		Server	Node ld	Displ

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.

Validating the certific	ate of server 'Seneca OPC UA /	Application' returned an error:	
BadCertificateC	hainIncomplete		
rtificate Chain			
lame		Trust Status	
621253a64ba620	064857470f51763bbbeaf13a961	Trusted	
rrors			
Error	SubjectAltName is missing	- this extension is mandatory according	g to th
Error	unable to get local issuer c	ertificate [BadCertificateChainIncomple	te]
Error	unable to get certificate CF	L [BadCertificateRevocationUnknown]	
Error	unable to verify the first ce	rtificate [BadCertificateChainIncomplet	el
ubject			
Common Name	621253a64ba62064857470f	i1763bbbeaf13a961	
Organization	SENECA		
OrganizationUnit	SENECA		
Locality	Padova		
State	Padova		
Country	IT		
DomainComponen	1		
suer	-		
Common Name	621253a64ba62064857470f	i1763bbbeaf13a961	
Organization	SENECA		
OrganizationUnit			
Locality	PD		
State	PD		
Country	Т		
DomainComponen	t		
alidity			
Valid From	ven 18. gen 16:08:20 2019		
Valid To	gio 13. gen 16:08:20 2039		
r			

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:

Unified Automation UaExpert - The	OPC Un	ied Architecture Client - NewProject*	
File view Server Document S	ettings		
roject	Β×	Data Access View	
 Project Servers Seneca OPC UA Applica Documents Data Access View 	ation	# Server Nod	e ld Display
ddress Space	₽×		
🨏 No Highlight	-		
Root	^		
Objects			
> GPS_ALTITUDE			
> 🔲 GPS_COG			
> 🔲 GPS_DAY			
> 🔲 GPS_ERROR			
> 🔲 GPS_FIX			
> 🔲 GPS_HDOP			
> 🔲 GPS_HOUR			
> GPS_LATITUDE			
> GPS_LONGITUDE			
> GPS_MINUTE			
> GPS_MONTH			
> GPS_NUM_SAT			
> GPS SECOND			
> GPS_SPEED_KM			
> 🔲 GPS SPEED KN			
> GPS_YEAR			
> 💑 Server			
> 🔲 V100			
> 💷 V1000			
> 🔲 V1001			
> 🛄 V1002			
> • V1002			

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

Unified Automation UaExpert - The OPC Uni	Inified Architecture Client - NewProject*
File View Server Document Settings	5 Help
D 💋 🕞 🖉 🧿 🜩 📼 🛇	a 🗙 🔩 🤰 🖻 🕱 🖵
Project & X	× Data Access View
♥ Project ♥ Project ♥ Servers Seneca OPC UA Application ♥ Documents Data Access View	# Server Node Id Digglay Name Value Datatype iourca Timestarry Server Timestarry Statuscode 1 Server CU A Application NSIShmrql/1025 VID5 0 Ulint16 1522823307 1522823307 Good 2 Servers OPC UA Application NSIShmrql/1025 VID25 0 Ulint16 1522823510 1522825356 Good 3 Senecs OPC UA Application NSIShtringl/1026 VID25 0 Ulint16 1522825356 Good
Address Space 🗗 🗙	×
😏 No Highlight 👻	•
> 💷 V1012 🔷	
> 🚭 V1013	
> 🔄 V1014	
> 🚽 V1015	
> 9 1010	
> 🚽 V1018	
> 💷 V1019	
> 💷 V102	
> 💷 V1020	
> 💷 V1021	
> 💷 V1022	
> 💷 V1023	
> 🕥 V1024	
> 🔄 V1025	
> V1026	
> 1027	
V1020	
> V102	
> 💷 V1030	
> 🚭 V1031	
> 💷 V1032	
> 💷 V1033	
> 💶 V1034	
	The second se

20.1.12 Users Configuration

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

P1 Z-PASS2	×			😲 Giovanni	0 —		×
← → C ① 192.168	3.85.104:8080/users.php					☆ 🔎	:
SERNECA® General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	Z-PASS2 Users Configuration [user: admin Firmware Version: SW003900_224 MAC Address: C8F9811B0000 [IM Internet Access: Mobile Modbus Shared Memory Gateway Router: running] [logout] 4 [Modem: UC El: 861075026 7: running	20GQBR03A14E1G] 500975] [IMSI: 2221016	00237890]			
Router Configuration		CURRENT	UPDATED				
FW Upgrade	WEB ADMINISTRATOR						
Conf. Management		- desta	a duain				
Shared Memory Tag Conf.	Username	admin	admin				
Tag View	Password	admin	admin				
Mobile Configuration	WEB GUEST						
Mobile Network	Username	guest	guest				
DDNS Configuration	Password	guest	guest				
Digital I/O	ETP LISER						
Digital I/O Contiguration	111 0021						
FW Versions	Username	user	user				
Ethernet Interfaces	Password	123456	123456				
			APPLY				

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	admin
	configuration site (full access)					

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

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

```
a-zA-ZO-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:

(P) 7-PASS2	×	(!) Giovanni —		×
← → C (1) 192.16	8.85.104:8080/mobile_network.php	ث		:
Seneral Configuration Main View Network and Services Serial Ports Gateway Configuration	Z-PASS2 Mobile Network [user: admin] [logout] Firmware Version: SW003900_224 [Mo MAC Address: C8F9811B0000 [IMEI: 8 Internet Access: Ethernet	ut] Modem: UC20GQBR03A14E1G] : 861075026500975] [IMSI: 222101600237890]		
Real Time Clock Setup	Modbus Shared Memory Gateway: run	running		
VPN Configuration	Router: running			
Users Configuration	CUF	CURRENT UPDATED		
FW Upgrade	SIM			
Conf. Management	3111			
Shared Memory Tag Conf.	PIN (if required by SIM) 8342	8342		
Tag Setup	Operator Selection			
Tag View Mobile Configuration	Mode Automa	matic Automatic T		
Mobile Network	Operator [22201]	1] I TIM		
DDNS Configuration	(UMTS)	S)		
Digital I/O	Data Connection			
Digital I/O Configuration	Enable OFF	OFF T		
EW Versions	APN Mode Automa	matic Automatic T		
Ethernet Interfaces	APN ibox.tim	tim.it ibox.tim.it		
	Authentication Type None	None T	1	
	Username user	user		
	Deservord pass	nace	1	
	Ding Connection Testing ID	pass		
	Address www.go (if empty, testing is disabled)	.google.com www.google.com]	
	APPLY SHOW MOBILE STATUS GET	SET OPERATOR LIST		

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

P1 Z-PASS2	×	(!) Giovanni —		×
← → C ① 192	168.85.105:8080/mobile_network.php		쇼	:
				•
SENECA®	Z-PASS2			
General Configuration	Mobile Network [user: admin] [logout]			
Main View	Firmware Version: SW003900_224 [Modem:	1231B02SIM5350E]		
Network and Services	MAC Address: C8FA81160002 [IMEI: 862264	1020406715] [IMSI: 222101600237889]	I	
Serial Ports	Internet Access: Ethernet			
Real Time Clock Setun	Modbus Ethernet to Serial Gateway: running	q		
VPN Configuration	Pouter disabled	3		
Router Configuration				
Users Configuration	CURRENT	UPDATED		
FW Upgrade	em			
Conf. Management	3111			
Mobile Configuration	PIN (if required by SIM) 8342	8342		
Mobile Network	Data Connection			
DDNS Configuration	Enable OFF	OFE		
FW Versions	ADN Mode Automatic			
Ethernet Interfaces	ADN iber time	ibov tim it		
	APN IDOX.tim.it	ibox.um.it		
	Authentication Type None	None 🔻		
	Username user	user		
	Password pass	pass		
	Ping Connection Testing IP	om www.google.com		
	(if empty, testing is disabled)	www.google.com		
	APPLY SHOW MOBILE STATUS			

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	1234
	on it ¹⁹	
Operator Selection/Mode (only on Z-PASS2)	This parameter tells if the modem shall select the Mobile Network	Automatic
	Operator:	
	- automatically	
	(Mode=Automatic)	
	(Mode=Manual)	
	- reverting to "automatic" mode,	
	if "manual" selection fails (Mode	
	= Manual/ Automatic)	
Operator Selection/Operator	This parameter contains the list of	"[22201] I TIM (UMTS)"
(only on Z-PASS2)	the Mobile Network Operators	
	currently available, that is detected	
	by the modem.	
	The list items are strings with the	
	the MCC+MNC ²⁰ code in square.	
	brackets (e.g.: "[22201]")	
	- the string identifying the	
	operator (e.g.: "I TIM")	
	- the access technology, that is	
	"GSM" or "UMTS", in brackets	
	This list is initially empty: it shall be	
	filled by clicking on the "GET	
	OPERATOR LIST" button.	
Data Connection/Enable	Flag to enable/disable the Mobile	OFF
Data Canadian (ADNI Mada	Network connectivity	Automatia
	related parameters are	Automatic
	automatically retrieved (based on	
	SIM IMSI) (Mode=Automatic) or the	
	values given in this page are used	

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).	
When APN Mode = Automatic, APN,	
Authentication Type, Username and	
Password parameters are disabled.	
Access Point Name, as given by the	ibox.tim.it
Mobile Network Operator	
Type of authentication required;	None
possible values are: "None",	
"CHAP/PAP", "CHAP only", "PAP	
only"	
Username needed for UMTS/GPRS	user
connectivity, as given by the Mobile	
Network Operator; it may be empty,	
if "Authentication Type" parameter	
is "None"	
Password needed for UMTS/GPRS	pass
connectivity, as given by the Mobile	
Network Operator; it may be empty,	
if "Authentication Type" parameter	
is "None"	
FQDN or IP address used to	www.google.com
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.	
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.	
	 (Mode=Manual). When APN Mode = Automatic, APN, Authentication Type, Username and Password parameters are disabled. Access Point Name, as given by the Mobile Network Operator Type of authentication required; possible values are: "None", "CHAP/PAP", "CHAP only", "PAP only" Username needed for UMTS/GPRS connectivity, as given by the Mobile Network Operator; it may be empty, if "Authentication Type" parameter is "None" Password needed for UMTS/GPRS connectivity, as given by the Mobile Network Operator; it may be empty, if "Authentication Type" parameter is "None" 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. 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 dron it

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	_		×
	168.85.104:8080/mobile_network.php?showinfo=1		Q	☆ ▶	:
SENECA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	Z-PASS2 Mobile Network [user: admin] [logout] Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 22210160 Internet Access: Ethernet Modbus Shared Memory Gateway: running Router: running	0237890]			
Router Configuration					
FW Upgrade	811				
Conf. Management Shared Memory Tag Conf.	PIN (if required by SIM) 8342 8342]			
Tag Setup	Operator Selection				
Tag View Mobile Configuration	Mode Automatic Automatic	• •			
Mobile Network	(UMTS)				
DDNS Configuration	Data Connection				
Digital I/O	Enable OFF OFF				
Digital I/O Conliguration	APN Mode Automatic Automatic				
FW Versions	APN ibox.tim.it ibox.tim.it				
Ethernet Interfaces	Authentication Type None Vone Vone				
2	Username user user				
	Password pass pass				
	Ping Connection Testing IP Address (if empty, testing is disabled) www.google.com				
	APPLY HIDE MOBILE STATUS GET OPERATOR LIST				
	Mobile Status				
	SIM/PIN Status PIN required				
	PIN Remaining Attempts 3 Signal Level [07] 5				
	Selected Operator "vodafone IT	" (UMTS)			
	Registration Status Registered (h	nome network)			
	IP Address 0.0.0.0	a			
	RX Packets / Bytes 0 / 0				
	TX Packets / Bytes 0 / 0	04560 [] (==1			
	GPS Location 45.3/421,11.5	24202 [IVI30]			
🗋 Z-PASS2	×	🤃 Giovanni	_		×
--	---	---------------------------	---	-----	---
← → C ③ 192.	168.85.104:8080/mobile_network.php?showinfo=1		Q	☆ ≯	:
SERVECA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	Z-PASS2 Mobile Network [user: admin] [logout] Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600 Internet Access: Mobile Modbus Shared Memory Gateway: running Router: running	0237890]			
Router Configuration Users Configuration	CURRENT UPDATED				
FW Upgrade Conf. Management Shared Memory Tag Conf.	SIM PIN (if required by SIM) 8342 8342]			
Tag Setup Tag View Mobile Configuration Mobile Network	Mode Automatic Automatic Operator [22201] I TIM (UMT8) Operator list not available	e V			
DDNS Configuration Digital I/O Digital I/O Configuration	Data Connection Enable ON ▼ APN Mode Automatic Automatic ▼				
FW Versions Ethernet Interfaces	APN ibox.tim.it ibox.tim.it Authentication Type None Username user User				
	Password pass pass Ping Connection Testing IP Address (if empty, testing is disabled) www.google.com APPLY HIDE MOBILE STATUS GET OPERATOR LIST				
	Mobile Status SIM/PIN Status PIN required PIN Remaining Attempts 3 Signal Level [07] 5 Selected Operator "vodafone IT" Registration Status Registered (h Connection Status Connected	" (UMT8) nome network)			
	IP Address 10.211.101.16 RX Packets / Bytes 6 / 65 TX Packets / Bytes 6 / 98 GP8 Location 45.37421,11.9 REFRESH 8	17 34562 [Map]			

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 <u>Map</u> 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.

🗋 Z-PASS2	Cityanai	-		×
$\boldsymbol{\leftarrow}$ \rightarrow \mathbf{C} (i) 192.	168.85.104:8080/mobile_network.php?showinfo=1	Q	☆ 🗡	:
SENECA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	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			
Houter Configuration Users Configuration FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration <i>Mobile Network</i> DDNS Configuration Digital I/O Digital I/O Digital I/O Digital I/O Ethernet Interfaces	CURRENT UPDATED SIM PIN (if required by SIM) 1234 Operator Selection 1234 Operator Selection Mode Automatic Automatic Operator Selection Deta Connection Operator list not available Data Connection Enable OFF OFF APN Mode Automatic Automatic APN ibox.tim.it ibox.tim.it Mone Username user Username user Password pass pass			
	Ping Connection Testing IP Address (if empty, testing is disabled) www.google.com APPLY HIDE MOBILE STATUS GET OPERATOR LIST Mobile Status SIM/PIN Status PIN error PIN Remaining Attempts 2 Signal Level [07] 4 Selected Operator No operator Registration Status Disconnected IP Address 0.0.0.0 RX Packets / Bytes 0 / 0 TX Packets / Bytes 0 / 0 GP8 Location Not fixed			

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.

🗋 Z-PASS2	× 🗌 — — ×
$\boldsymbol{\leftarrow}$ \rightarrow \mathbf{C} (i) 192.	168.85.104:8080/mobile_network_scan.php
SENECA® General Configuration	Z-PASS2 Mobile Network [user: admin] [logout]
Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade Conf. Management	Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Internet Access: Ethernet Modbus Shared Memory Gateway: running Router: running Start retrieving operator list, please wait (this will take some minutes)
Shared Memory Tag Cor Tag Setup Tag View Mobile Configuration <i>Mobile Network</i> DDNS Configuration Digital I/O Digital I/O Digital I/O Digital I/O	
FW Versions Ethernet Interfaces	

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

	🗘 Giovanni — 🗆 🗙
Z-PA332	
$\leftarrow \rightarrow \mathbf{C}$ (i) 192.16	58.85.104:8080/mobile_network_scan.php 📩 💹 🗄
SENECA °	Z-PASS2
General Configuration	Mobile Network [user: admin] [logout]
Main View	Firmware Version: SW003900_224 [Modem: UC20GQBB03A14F1G]
Network and Services	
Serial Ports	MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Gateway Configuration	Internet Access: Ethernet
Real Time Clock Setup	Modbus Shared Memory Gateway: running
VPN Configuration	Router: running
Router Configuration	
Users Configuration	
FW Upgrade	Operator list retrieval in progress, please wait
Conf. Management	(15 seconds elapsed)
Shared Memory Tag Conf.	
Tag Setup	
Tag View	
Mobile Configuration	
Mobile Network	
DDNS Configuration	
Digital I/O	
Digital I/O Configuration	
EW Versions	
Ethernet Interfaces	
2	
L	

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

Th Z-PASS2	× Giovanni — — ×	
C - C 0 192.100		
SENECA [®]	Z-PASS2	
General Configuration	Mobile Network [user: admin] [logout]	
Main View	Firmware Version: SW003900_224 [Modem: UC20GQBB03A14F1G]	
Network and Services		
Serial Ports	MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IM5I: 222101600237890]	
Gateway Configuration	Internet Access: Ethernet	
Real Time Clock Setup	Modbus Shared Memory Gateway: running	
VPN Configuration	Router: running	
Router Configuration		
Users Configuration		
FW Upgrade	Operator list successfully retrieved !	
Conf. Management		_
Shared Memory Tag Conf.		
Tag Setup		
Tag View		
Mobile Configuration		
Mobile Network		
DDNS Configuration		
Digital I/O Configuration		
Diagnostics		
FW Versions		
Ethernet Interfaces		

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

Z-PASS2	×	😲 Giovanni —		×
← → C (i) 192.160	8.85.104:8080/mobile_network.php		☆ 🔎	:
SERVECA® General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	Z-PASS2 Mobile Network [user: admin] [logout] Firmware Version: SW003900_224 [Modem: UC20GQBR03 MAC Address: C8F9811B0000 [IMEI: 861075026500975] [I Internet Access: Ethernet Modbus Shared Memory Gateway: running Router: running	3A14E1G] MSI: 222101600237890]		
Router Configuration	CURRENT	UPDATED		
FW Upgrade	oun	UTDATED		
Conf. Management Shared Memory Tag Conf. Tag Setup	SIM PIN (if required by SIM) 8342 8342 Operator Selection			
Tag View	Mode Automatic Automatic	▼		
Mobile Configuration				
DDNS Configuration Digital I/O Digital I/O Configuration Diagnostics	Operator [22210] vol Data Connection [22210] vol Enable OFF [22250] ur APN Mode Automatic [22288] I	odafone IT (GSM) odafone IT (GSM) odafone IT (UMTS) TIM (GSM) nknown (UMTS) WIND (UMTS)		
Ethernet Interfaces	APN ibox.tim.it [22299] 3	VIND (GSM) ITA (UMTS)		
	Authentication Type None	TIM (UMTS)		
	Username user User			
	Password pass pass			
	Ping Connection Testing IP Address www.google.com (if empty, testing is disabled)	le.com		
	APPLY SHOW MOBILE STATUS GET OPERATOR LIST			

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:

	~		(!) (Ciovanni —		×
Z-PASS2	×			1	
← → C ① 192.168	3.85.104:8080/ddns_conf.php		<u>አ</u>	1	:
SENECA®	Z-PASS2				
General Configuration	DDNS Configuration [user: admin]	[logout]			
Main View	Firmware Version: SW003900_224	[Modem: UC	20GQBR03A14E1G]		
Network and Services	MAC Address: C8F9811B0000 [IM	EI: 861075026	6500975] [IMSI: 222101600237890]		
Serial Ports	Internet Assess Ethernet				
Gateway Configuration	Internet Access: Ethernet				
Real Time Clock Setup	Modbus Shared Memory Gateway	: running			
VPN Configuration	Router: running				
Router Configuration					
Users Configuration		CURRENT	UPDATED		
FW Upgrade	DDNS Configuration				
Conf. Management					
Shared Memory Tag Conf.	Туре	None	None •	1	
Tag Setup	Hostname				
Tag View	Username				
Mobile Network	Password				
DDNS Configuration	APPLY				
Digital I/O					
Digital I/O Configuration		_			
Diagnostics	DDNS Update S	tatus			
FW Versions	S	tatus			
Ethernet Interfaces	IP Add	Iress			

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

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

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

Z-PASS2	×	Covanti	-		×
	curo 192.168.85.104:8080/ddns_conf.php			☆ 🛛	
 Pass2 C ON Non si C ON Non si SENECA[®] General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration Bouter Configuration Users Configuration FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View TCP Servers Mobile Configuration Mobile Network DDNS Configuration 	x x 192.168.85.104:8080/ddns_conf.php Z-PASS2 DDNS Configuration [user: admin] [logout] Firmware Version: SW003900_232 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222101600237893] Internet Access: Ethernet Gateway: running [Data Logger: running (no group enabled)] Router: running CURRENT UPDATED DDNS Configuration Type None dyndns.it Hostname zpass_ddns.net Username zpass_usr Password zpass_psw				
DDNS 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	DDNS Update Status IP Address				

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.

P1 7-PASS2	×		😲 Giavanni —		×
	9 SE 104/2020/ddm			~	
← → C 0 192.160	8.85.104:8080/ddns_conf.php			¥	:
SENECA [®]	Z-PASS2				
General Configuration	DDNS Configuration [user: adm	nin] [logout]			
Main View	Firmware Version: SW003900 2	224 [Modem: UC	20GQBR03A14E1G1		
Network and Services		IMEL 961075090	5000751 [IM6], 2221016002278001		
Serial Ports	MAC Address. Corso TE0000 [IMEL 001075020	5500975J [IM31: 222101000237030]		
Gateway Configuration	Internet Access: Mobile				
Real Time Clock Setup	Modbus Shared Memory Gatew	ay: running			
VPN Configuration	Router: running				
Router Configuration					
Users Configuration		CURRENT	UPDATED		
FW Upgrade	DDNS Configuration				
Conf. Management	25No comgutation				
Shared Memory Tag Conf.	Туре	dyndns.it	dyndns.it 🔻		
Tag Setup	Hostname	zpasstest1.ns0.it	zpasstest1.ns0.it		
Tag View	Username				
Mobile Configuration	Password			_	
Nobile Network	APPLY				
Duris Configuration	74121				
Digital I/O Configuration					
Diagnostics	DDNS Update	e Status			
FW Versions		Statue	good		
Ethernet Interfaces	ID A	ddrees	91.80.5.100		
	IP A	adress	91.00.8.100		

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.

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

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:

Z-PASS2	×							😲 Ciovanni	- 0	×
← → C ① 192.168.8	5.104 :80)80/mb_servers.php							⊕ ☆ 🗵	:
Senation Services General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration	Z-PA Modt Firmv MAC Intern Gates Route	SS2 bus TCP Servers [u ware Version: SW0 Address: C8F9811 net Access: Mobile way: running er: running	ser: admin] [logout] 03900_228 [Modem: B0000 [IMEI: 8610756	UC20GQBR 026666172]	03A14E1G] [IMSI: 2221	01600237	891]			
FW Upgrade		ADD		MODIFY				DELETE		
Conf. Management Shared Memory Tag Conf. Tag Setup	#	Name	IP Address	TCP Port	Timeout	Poll Delay	Read/Write Retries	Mult.Read Max Num.	Mult.Write Max Num.	•
Tag View TCP Servers Mobile Configuration Mobile Network DDNS Configuration Digital I/O Configuration SMS Configuration Phonebook Diagnostics FW Versions Ethernet Interfaces	1 2 3 4	ZPASS2_105 ZPASS2_106 ZKEY_83 ZPASS2S_103	192.168.105.101 192.168.106.101 192.168.85.83 192.168.107.101	502 1100 502 502	5000 5000 5000	100 100 100	0 0 0	16 16 16	16 16 16	

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	empty
	This name is used to identify the TCP	
	Server in the "Tag Setup" and "Tag	
	View" pages.	
IP Address	IP Address of the TCP Server	empty
TCP Port	Modbus TCP Server port	502
Timeout (ms) [10-10000]	Connection/Response timeout for	5000
	Modbus TCP requests, in milliseconds	
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	0
	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)	
Multiple Read Max Number [1-32]	Maximum number of Modbus registers	16
	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	
Multiple Write Max Number [1-32]	Maximum number of Modbus registers	16
	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	

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

← C ① 192.168.85.104:8080/mb_servers_save.php?act=save&lid=0 Q ★ ☑ I SERVECA General Configuration Modbus TCP Servers [user: admin] [logout] Modbus TCP Servers [user: admin] [logout] Main View Firmware Version: SW003900_228 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 8610750266666172] [IMSI: 222101600237891] Network and Services MAC Address: C8F9811B0000 [IMEI: 8610750266666172] [IMSI: 222101600237891] Internet Access: Ethernet Gateway Configuration Real Time Clock Setup Gateway: running VPN Configuration Router: disabled
SENECA Z-PASS2 General Configuration Modbus TCP Servers [user: admin] [logout] Main View Firmware Version: SW003900_228 [Modem: UC20GQBR03A14E1G] Network and Services MAC Address: C8F9811B0000 [IMEI: 8610750266666172] [IMSI: 222101600237891] Serial Ports Internet Access: Ethernet Gateway Configuration Gateway: running VPN Configuration Router: disabled
Users Configuration FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View TCP Servers Mobile Configuration Mobile Configuration Digital I/O Configuration Digital I/O Configuration SMS Configuration Boilagnostics FW Versions Ethernet Interfaces

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.

Z-PASS2	×							(!) Ciovanni	- 0	×
← → C ③ 192.168.8	5.104:80	80/mb_servers.php							⊕ ☆ 🔼	:
SENECCA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration	Z-PA Modit Firmv MAC Intern Gates Rout	SS2 ous TCP Servers [u: ware Version: SW00 Address: C8F9811 net Access: Mobile way: running er: running	ser: admin] <mark>[logout]</mark> 03900_228 [Modem: I B0000 [IMEI: 8610750	JC20GQBR 926666172]	03A14E1G] [IMSI: 2221] 01600237	891]			
Users Configuration FW Upgrade		ADD		MODIFY				DELETE		
Conf. Management Shared Memory Tag Conf.	#	Name	IP Address	TCP Port	Timeout	Poll Delay	Read/Write Retries	Mult.Read Max Num.	Mult.Write Max Num.	
Tag Setup Tag View TCP Servers Mobile Configuration Mobile Network DDNS Configuration Digital VO Configuration Digital VO Configuration SMS Configuration Phonebook Diagnostics FW Versions Ethernet Interfaces	1 2 3 4	ZPASS2_105 ZPASS2_106 ZKEY_83 ZPASS2S_103	192.168.105.101 192.168.106.101 192.168.85.83 192.168.107.101	502 1100 502 502	5000 5000 5000 5000	100 100 100	0 0 0	16 16 16 16	16 16 16	

Z-PASS2	×			(!) Ciovanni	-		×
$\epsilon \rightarrow c$ (i) Non sicure	0 192.168.85.104:8080/mb_servers_mod.p	hp?id=12			Ð, 1	*	:
Seneral Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	Z-PASS2 Modbus TCP Servers [user: admin Firmware Version: SW003900_228 MAC Address: C8F9811B0000 [IME Internet Access: Mobile Gateway: running Router: running] [logout] [Modem: UC20 El: 86107502666	GQBR03A14E1G] 96172] [IMSI: 222101600237891]				
Users Configuration		CURRENT	UPDATED				
FW Upgrade	Modbus TCP Server						
Conf. Management		ZKEV 00	ZKEV 83				
Shared Memory Tag Conf.	Name	ZKET_03					
Tag Setup	IP Address	192.168.85.83	192.168.85.83				
TCP Servers	TCP Port	502	502				
Mobile Configuration	Timeout (ms) [10-10000]	500	400				
Mobile Network	Delay between Polls (ms) [10-1000]	100	100				
DDNS Configuration	Read/Write Retries [0-10]	0	0				
Digital I/O Configuration	Multiple Read Max Number [1-32]	16	16				
Logic Configuration	Multiple Write Max Number [1-32]	16	16				
SMS Configuration	APPLY						
Phonebook							
Diagnostics							
Ethernet Interfaces							
Enemerimenaces							

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.

	192.168.85.10 2 7 Tag Setup e Version: £ dress: C8F5 Access: No <i>:</i> : running [[disabled Tile Nessun f ADD ADD GATEWAY MODBUS START REGISTER 1	24:8080/mbgw_ti [user: admin] [WW003900_240 8811B0000 [IME ne Jata Logger: ru ile selezionato ile selezionato	ag_setup.phy [logout] [Modem: U [I: 86107502 inning] [Import MODIFY Page : 1/2 TARGET BEVICE CUSTOM	C20GQBR03A14E1 266666172] [IMSI: 22 t tag configuration 1 t tag configuration 0 PREVIOUS PAGE TARGET TARGET TARGET RESOURCE TARGET 1	G] 2101600233 Export tag co [DELETE] E] NEXT P TARGET MODBUS REQUEST TYPE HOLDING BEGISTE	AGE ARGET TARGET REGISTR DATA TYPE DATA TYPE DATA	TARGET BIT INDEX	TARGET CONNECTED TO	TARGET MODBUS STATION	GATEWAY TAG MODE	GAIN	OFFSET	ERROR	☆ ERROR VALUE	HTTP POST POST VID	G
SENERCA Basic Configuration Summary Network and Services Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration Reuter Configuration Mobile Configuration Mobile Configuration Mobile Configuration Mobile Configuration Shared Memory Tag Conf. TCP Serves Tag Setup Tag Setup Tag Setup Tag Setup Tag View Alarms Alarm Summary Alarm Summary Alarm Summary Alarm Summary Alarm Summary Alarm Signation Phonebook SMS Configuration Phonebook SMS Configuration Phonebook	2 7 Tag Setup e Version: 5 dress: CoRFS Access: No 7: running [[disabled ADD ADD GATEWAY MODEUS START REGISTER 1	[user: admin] [WW003900_240 8811B0000 [IME ne Data Logger: ru ile selezionato data Logger: ru ile selezionato Cateway TAG NAME ZPASS_DI	[logout] [Modem: U [Modem: U Import MoDIFY] Page : 1/2 TARGET DEVICE CUSTOM	C20GQBR03A14E1 26666172] [IMSI: 22 t tag configuration] t tag configuration] 0 PREVIOUS PAGE TARGET TARGET RESOURCE TARGET REGISTER 1	G] 2101600238 Export tag co DELETE NEXT P TARGET MODBUS REQUEST TYPE HOLDING DECISITO	AGE TARGET REGISTER DATA TYPE 16BIT	TARGET BIT INDEX	TARGET CONNECTED TO	TARGET MODBUS STATION	GATEWAY TAG MODE	GAIN	OFFSET	ERROR	ERROR	HTTP POST VID	ALARI
DDNS Configuration TCP Servers Tag Setup Tag Setup Tag View Alarms Alarm Summary Alarm History Logic Configuration Phonebook SMS Configuration Phonebook SMS Configuration Phonebook SMS Configuration Phonebook SMS Configuration 6 SMS Configuration 5 SMS Configuration 6 SMS Configuration 5 SMS Configuration 6 SMS Configuration 6 SMS Configuration 6 SMS Configuration 7 SMS Configuration 8 SMS Configuration 7 SMS Configuration	GATEWAY MODBUS START REGISTER	GATEWAY TAG NAME ZPASS_DI	TARGET MODBUS DEVICE	TARGET RESOURCE 1	TARGET MODBUS REQUEST TYPE HOLDING BEGISTEP	TARGET REGISTER DATA TYPE 16BIT	TARGET BIT INDEX	TARGET CONNECTED TO	TARGET MODBUS STATION	GATEWAY TAG MODE	GAIN	OFFSET	ERROR MODE	ERROR VALUE		ALARI NABLI
Alarms Alarms Alarms Alarms Alarms Alarms Alarms Alarms Alarm History 2 Alarm History 2 Logic Configuration 3 SMS Configuration 4 Email Configuration 5 Message Configuration 0	REGISTER	ZPASS_DI	CUSTOM	RESOURCE START REGISTER	HOLDING BEGISTEP	TYPE 16BIT	INDEX	то	STATION	TAG MODE			MODE	VALUE	VID	INABLI
Alarm Summary 2 Alarm History 2 Logic Configuration 3 Phonebook 5 SMS Configuration 4 Email Configuration 5 HTTP Configuration 6	1	ZPASS_DI	CUSTOM	1	REGISTER				ADDRESS				LAST			
Alarm History 2 Logic Configuration 3 SMS Configuration 4 Email Configuration 5 HTTP Configuration 6					HOLDING	UNSIGNED 16BIT	0	EMBEDDED	1	EMBEDDED	1	0	VALUE	0	Vo	OFF
Phonebook 3 Phonebook 4 Email Configuration 5 HTTP Configuration 6	2	ZPASS_DO	CUSTOM	2	REGISTER	UNSIGNED	0	EMBEDDED	1	EMBEDDED	1	0	VALUE	0	V1	OFF
MS Configuration 4 Email Configuration 5 HTTP Configuration 6	1	ZPASS_DI_1	CUSTOM	1	INPUT	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	VALUE	0	V2	OFF
Internation 5 ITTP Configuration 6 Message Configuration 6	2	ZPASS_DI_2	CUSTOM	2	DISCRETE INPUT	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	VALUE	0	V3	OFF
fessage Configuration 6	3	ZPASS_DI_3	CUSTOM	3	DISCRETE INPUT	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	LAST VALUE	0	V4	OFF
	4	ZPASS_DI_4	CUSTOM	4	DISCRETE	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	LAST	0	V5	OFF
Rule Configuration 7	1	ZPASS_DO_1	CUSTOM	1	COIL	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	LAST	0	V6	OFF
ieneral Settings 8	2	ZPASS_DO_2	CUSTOM	2	COIL	BOOL	0	EMBEDDED	1	EMBEDDED	1	0		0	V7	OFF
D Transfer Conf.	3	ZPASS DO 3	CUSTOM	3	COIL	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	LAST	0	V8	OFF
TP Transfer Conf.		70400 00 :	010701		001	BOOL		EMOCODED				č	VALUE LAST	č	10	055
laintenance	4	ZPASS_DO_4	CUSTOM	4		16RIT	0	EWREDDED	1	EMBEDDED	1	U	VALUE	0	48	OFF
thernet Interfaces 11	10	GPS_ERROR	CUSTOM	10	REGISTER	SIGNED	0	EMBEDDED	1	EMBEDDED	1	0	VALUE	0	V10	OFF
W Versions 12	11	GPS_HOUR	CUSTOM	11	HOLDING REGISTER	16BIT UNSIGNED	0	EMBEDDED	1	EMBEDDED	1	0	LAST VALUE	0	V11	OFF ,
onf. Management																

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.

 	<complex-block> </complex-block>	C Z-PASS2	×	+															-	
Specification Specification Name of conjunction Finance and Bricking Specification Finance and Bricking Specification Conjunction Specification Conjunction Specification Conjunction Specification Conjunction Specification Conjunction Specification Conjunction Real The Cock deep Specification Conjunction Readeway: conjunction Import tag configuration VMC Conjunction MoDiFY DELETE Specification Import tag configuration Export tag configuration VMC Conjunction Specification Import tag configuration Specification Import tag configuration Export tag configuration Atom Conjunction Import tag configuration Export tag configuration Tog School Tog School Tog School Tog School Tog School Tag School 1 1 PARSB_DL Custom Tog School Tag School 1 1 PARSB_DL Custom Tog	Selection Selection Base Contraction Contraction Selection Contraction	← → C (i) No	in sicuro 19	2.168.85.10	04:8080/mbgw_ta	ag_setup.ph	р											☆	入	G
VPN Configuration Segif Rie Nessun file selezionato Import tag configuration Export tag configuration Mobile Network ADD MODIFY DELETE Page : 1/20 PREVIOUS PAGE NEXT PAGE Shared Menory Tag Configuration MODIFY DELETE Tog Setup ATEWAY TARGET TARGET </td <td>VPNC Cedeguation Seeglifile Nessun Rie selezionalo Import tage configuration Export tage configuration Albeite Configuration ADD MODIFY DELETE Abeite Configuration ADD MODIFY DELETE To Status MODIEV DELETE To Status MODIEV DELETE Tage Status MODIEV DELETE Tage Status MODIEV TARGET TARGET TARGET MODIEV Tage Status MODIEV TARGET TARGET TARGET TARGET MODIEV CONNECCEDE Status MODIEV ALART Name Status MODIEV TARGET TARGET TARGET TARGET TARGET TARGET MODIEV CONNECCEDE Status MODIEV ALART ALART<td>S SENECA® Basic Configuration Summary Network and Services Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration</td><td>Z-PASS2 Gateway 1 Firmware MAC Addu Internet A Gateway: Router: di</td><td>Fag Setup Version: S ress: C8F9 ccess: Nor running [D sabled</td><td>[user: admin] [l sw003900_240 811B0000 [IME ne Data Logger: ru</td><td>logout] (Modem: L I: 8610750 nning]</td><td>JC20GQBF 26666172]</td><td>03A14E10 [IMSI: 222</td><td>3] 2101600239</td><td>291]</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td>	VPNC Cedeguation Seeglifile Nessun Rie selezionalo Import tage configuration Export tage configuration Albeite Configuration ADD MODIFY DELETE Abeite Configuration ADD MODIFY DELETE To Status MODIEV DELETE To Status MODIEV DELETE Tage Status MODIEV DELETE Tage Status MODIEV TARGET TARGET TARGET MODIEV Tage Status MODIEV TARGET TARGET TARGET TARGET MODIEV CONNECCEDE Status MODIEV ALART Name Status MODIEV TARGET TARGET TARGET TARGET TARGET TARGET MODIEV CONNECCEDE Status MODIEV ALART ALART <td>S SENECA® Basic Configuration Summary Network and Services Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration</td> <td>Z-PASS2 Gateway 1 Firmware MAC Addu Internet A Gateway: Router: di</td> <td>Fag Setup Version: S ress: C8F9 ccess: Nor running [D sabled</td> <td>[user: admin] [l sw003900_240 811B0000 [IME ne Data Logger: ru</td> <td>logout] (Modem: L I: 8610750 nning]</td> <td>JC20GQBF 26666172]</td> <td>03A14E10 [IMSI: 222</td> <td>3] 2101600239</td> <td>291]</td> <td></td>	S SENECA® Basic Configuration Summary Network and Services Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration	Z-PASS2 Gateway 1 Firmware MAC Addu Internet A Gateway: Router: di	Fag Setup Version: S ress: C8F9 ccess: Nor running [D sabled	[user: admin] [l sw003900_240 811B0000 [IME ne Data Logger: ru	logout] (Modem: L I: 8610750 nning]	JC20GQBF 26666172]	03A14E10 [IM SI: 222	3] 2101600239	291]										
Uses Configuration Mobile Configuration Mobile Configuration Mobile Configuration Mobile Network TCP Servers Tag Setup Tag Setup Ta	Uses Configuration Mobile Network Shared Memory Digent To genue To genue To genue Amm Susce Mamory Amm Susce Managenetic Strate Network To genue To genue Amm Susce Shared Memory Digent To genue Amm Susce Shared Memory Digent To genue To genue Shared Memory Digent To genue Shared Memory Digent To genue Amm Susce Shared Memory Digent To genue Shared Memory Digent To genue	VPN Configuration Router Configuration	Scegli file	Nessun fi	ile selezionato	Impor	rt tag configu	iration E	Export tag co	nfiguration]									
Shared Memory Tog Conf. CATEWAY Tag Setup CATEWAY MODELS CATEWAY TAG NUMP CATEWAY TAG NUMP CATEWAY TAG NUMP TARGET TAG NUMP TARGET MODELS TARGET NUMP TARGET NUMP TARGET NUMP TARGET NUM	Shared Memory Tag Cent TCP Servers Tag Setup Aamma CATEWAY NATURE Tag Setup Aamma CATEWAY TAD NAME CATEWAY TAD NAME CATEWAY TAD NAME CATEWAY TAD NAME TARGET NODEWIC TARGET DATA TARGET	Users Configuration Mobile Configuration Mobile Network DDNS Configuration	A	NDD	1	MODIFY Page : 1/2	20 PREVI	OUS PAGE	DELETE NEXT P	AGE	1									
And Sector And Edited And Edi	Alternal	Shared Memory Tag Conf. TCP Servers																		
Alarm Configuration 1 1 ZPASS_DI CUSTOM 1 HOLDING 16BIT REGISTER UNSIGNED 0 EMBEDDED 1 0 LAST VALUE 0 V0 OFF Alarm Summary 2 2 ZPASS_DO CUSTOM 2 HOLDING 16BIT REGISTER UNSIGNED 0 EMBEDDED 1 EMBEDDED 1 0 LAST VALUE 0 V1 OFF Jam Hatry 2 2 ZPASS_DI_1 CUSTOM 1 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 LAST VALUE 0 V2 OFF SMS Configuration 4 2 ZPASS_DL_2 CUSTOM 2 DISCRETE INPUT BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V3 OFF Email Configuration 6 4 ZPASS_DL_3 CUSTOM 1 COIL BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V4 OFF Email Configuration 6 4 ZPASS_DL_4 CUSTOM 1 COIL BOOL	Alam Confguration 1 1 2 PASS_DI C USTOM 1 HOLDING HEBIT HEGISTER UNSIGNED 0 EMBEDDED 1 0 LAST LAST VALUE 0 V0 OFF Alam Matry Lagic Confguration Phonebook 3 1 ZPASS_DI_1 CUSTOM 2 HOLDING HEBIT FINITHE 0 EMBEDDED 1 EMBEDDED 1 0 LAST VALUE 0 V1 OFF Carlo Confguration Phonebook 3 1 ZPASS_DI_2 CUSTOM 2 DISCRET PMOTE 00 EMBEDDED 1 EMBEDDED 1 0 LAST VALUE 0 V2 OFF SMS Confguration 4 2 ZPASS_DL3 CUSTOM 2 DISCRET PMOTE 00 EMBEDDED 1 EMBEDDED 1 0 LAST VALUE 0 V3 OFF Email Confguration 5 3 ZPASS_DL4 CUSTOM 1 Colu 60 EMBEDDED 1 EMBEDDED 1 ULAST VALUE 0 V4 OFF	Tag Setup Tag View Alarms	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	ALARI
Alam Summary 2 2 2PASS_DO CUSTOM 2 HOLDING 16BTT REGISTER UNSIGNED 0 EMBEDDED 1 EMBEDDED 1 EMBEDDED 1 CAST 0 VALUE 0 VALU	Alam Summary Alam History 2 2 2PASS_D0 CUSTOM 2 HOLDING HEGISTER 1BIT UNSIGNED 0 EMBEDDED 1 EMBEDDED 1 0 LAST VALUE 0 V1 OFF Alam History 3 1 ZPASS_D1_1 CUSTOM 1 DisConfiguration 1 EMBEDDED 1 EMBEDDED 1 0 LAST VALUE 0 V2 OFF BMS Configuration 4 2 ZPASS_D1_2 CUSTOM 2 DisCentification BOOL 0 EMBEDDED 1 EMBEDDED 1 0 LAST VALUE 0 V3 OFF Email Configuration 6 4 2 ZPASS_D1_4 CUSTOM 2 DISCNETTE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 LAST VALUE 0 V4 0 V5 OFF Email Configuration 6 4 ZPASS_D0_2 CUSTOM 1 COIL BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V5 0FF	Alarm Configuration	1	1	ZPASS_DI	CUSTOM		1	HOLDING REGISTER	16BIT UNSIGNED	0	EMBEDDED	1	EMBEDDED	1	0	LAST VALUE	0	Vo	OFF
Logic Configuration Phonebook 3 1 ZPASS_DL_1 CUSTOM 1 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V2 OFF SMS Configuration 4 2 ZPASS_DL_2 CUSTOM 2 DISCRETE INPUT BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V4	Lojo Configuration PhonebookS1ZPASS_DL_1CUSTOM1DISCRETE INPUTBOOL0EMBEDDED1EMBEDDED10VALUE VALUE0V2OFFSMS Configuration42ZPASS_DL_2CUSTOM2DISCRETE INPUTBOOL0EMBEDDED1EMBEDDED10LAST VALUE0V4OFFEmail Configuration53ZPASS_DL_4CUSTOM3DISCRETE INPUTBOOL0EMBEDDED1EMBEDDED10LAST VALUE0V4OFFEmail Configuration64ZPASS_DL_4CUSTOM4DISCRETE INPUTBOOL0EMBEDDED1EMBEDDED10LAST VALUE0V4OFFBuilt Configuration64ZPASS_DD_1CUSTOM4DISCRETE INPUTBOOL0EMBEDDED1EMBEDDED10LAST VALUE0V4OFFBuilt Configuration71ZPASS_DD_2CUSTOM1COILBOOL0EMBEDDED1EMBEDDED10LAST VALUE0V7OFFBota Logger (Smissing)82ZPASS_DD_2CUSTOM3COILBOOL0EMBEDDED1EMBEDDED10LAST VALUE0V7OFFBrander Conf.93ZPASS_DD_4CUSTOM10HOLDING HEGISTERBOOL0EMBEDDE	Alarm Summary Alarm History	2	2	ZPASS_DO	CUSTOM		2	HOLDING	16BIT UNSIGNED	0	EMBEDDED	1	EMBEDDED	1	0	LAST VALUE	0	V 1	OFF
Anomatocic 4 2 ZPASS_DL_2 CUSTOM 2 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V3 OFF SMS Chriguration 5 3 ZPASS_DL_3 CUSTOM 3 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V4 0FF Message Configuration 6 4 ZPASS_DL_4 CUSTOM 4 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V4 0FF Discreter INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V4 0FF Discreter 0 VA DISCRETE BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V5 OFF Discreter 7 1 ZPASS_DO_2 CUSTOM 1 COIL BOOL 0 EMBEDDED 1 0 LAST	Management 4 2 ZPASS_DL_2 CUSTOM 2 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 VA OFF Email Configuration 5 3 ZPASS_DL_3 CUSTOM 3 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V4 OFF Message Configuration 6 4 ZPASS_DL_4 CUSTOM 4 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V5 OFF Dista Logger (Smissing) 6 4 ZPASS_DO_2 CUSTOM 1 Coll BOOL 0 EMBEDDED 1 0 VALUE 0 V6 OFF Dista Logger (Smissing) 8 2 ZPASS_DO_2 CUSTOM 2 COIL BOOL 0 EMBEDDED 1 0 LAST 0 V7 OFF Group Configuration 8 2 ZPASS_DO_3 CUSTOM 3 COIL	Logic Configuration	3	1	ZPASS_DI_1	CUSTOM		1	DISCRETE	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	LAST VALUE	0	V2	OFF
Email Configuration 5 3 ZPASS_DL_3 CUSTOM 3 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 VA OFF Message Configuration 6 4 ZPASS_DL_4 CUSTOM 4 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V4 OFF Build Configuration 6 4 ZPASS_DO_1 CUSTOM 4 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V5 OFF Build Configuration 7 1 ZPASS_DO_1 CUSTOM 1 Coll BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V6 OFF State Configuration 8 2 ZPASS_DO_2 CUSTOM 3 COIL BOOL 0 EMBEDDED 1 0 VALUE 0	Email Configuration 5 8 2PASS_DL_3 CUSTOM 3 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 CMST VALUE 0 VA OFF Message Configuration 6 4 ZPASS_DL_4 CUSTOM 4 DISCRETE INPUT BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V5 OFF Bala Logger (SD missing) 6 4 ZPASS_DO_1 CUSTOM 1 COIL BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V6 OFF Bala Logger (SD missing) 8 2 ZPASS_DO_2 CUSTOM 1 COIL BOOL 0 EMBEDDED 1 0 VALUE 0 V6 OFF Group Configuration 3 ZPASS_DO_3 CUSTOM 3 COIL BOOL 0 EMBEDDED 1 0 LAST 0 V6 OFF <t< td=""><td>SMS Configuration</td><td>4</td><td>2</td><td>ZPASS_DI_2</td><td>CUSTOM</td><td></td><td>2</td><td>DISCRETE</td><td>BOOL</td><td>0</td><td>EMBEDDED</td><td>1</td><td>EMBEDDED</td><td>1</td><td>0</td><td>LAST</td><td>0</td><td>V3</td><td>OFF</td></t<>	SMS Configuration	4	2	ZPASS_DI_2	CUSTOM		2	DISCRETE	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	LAST	0	V3	OFF
If IP Configuration 0 4 ZPASS_DL_4 CUSTOM 4 DISCRETE INPUT BOOL 0 EMBEDDED 1 CMBEDDED 1 CMBEDDED </td <td>HTP Configuration 0 4 ZPASS_DL_4 CUSTOM 4 DISCRETE INPUT BOOL 0 EMBEDDED 1 0 VALUE 0 V5 OFF Message Configuration 7 1 ZPASS_DO_1 CUSTOM 1 COIL BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V6 OFF General Settings 8 2 ZPASS_DO_2 CUSTOM 2 COIL BOOL 0 EMBEDDED 1 0 VALUE 0 V6 OFF SD Transfer Conf. 9 3 ZPASS_DO_3 CUSTOM 3 COIL BOOL 0 EMBEDDED 1 0 LAST 0 V8 OFF Group Configuration 10 4 ZPASS_DO_4 CUSTOM 4 COIL BOOL 0 EMBEDDED 1 0 LAST 0 V8 OFF Maintenance 11 10 GPS_ERROR CUSTOM 10 HOLDING 16BIT 0 EMBEDDED 1 EMBEDDED 1</td> <td>Email Configuration</td> <td>5</td> <td>3</td> <td>ZPASS_DI_3</td> <td>CUSTOM</td> <td></td> <td>3</td> <td>DISCRETE</td> <td>BOOL</td> <td>0</td> <td>EMBEDDED</td> <td>1</td> <td>EMBEDDED</td> <td>1</td> <td>0</td> <td>LAST</td> <td>0</td> <td>V4</td> <td>OFF</td>	HTP Configuration 0 4 ZPASS_DL_4 CUSTOM 4 DISCRETE INPUT BOOL 0 EMBEDDED 1 0 VALUE 0 V5 OFF Message Configuration 7 1 ZPASS_DO_1 CUSTOM 1 COIL BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V6 OFF General Settings 8 2 ZPASS_DO_2 CUSTOM 2 COIL BOOL 0 EMBEDDED 1 0 VALUE 0 V6 OFF SD Transfer Conf. 9 3 ZPASS_DO_3 CUSTOM 3 COIL BOOL 0 EMBEDDED 1 0 LAST 0 V8 OFF Group Configuration 10 4 ZPASS_DO_4 CUSTOM 4 COIL BOOL 0 EMBEDDED 1 0 LAST 0 V8 OFF Maintenance 11 10 GPS_ERROR CUSTOM 10 HOLDING 16BIT 0 EMBEDDED 1 EMBEDDED 1	Email Configuration	5	3	ZPASS_DI_3	CUSTOM		3	DISCRETE	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	LAST	0	V4	OFF
Rule Configuration 7 1 ZPASS_DO_1 CUSTOM 1 COIL BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V6 OFF General Settings 8 2 ZPASS_DO_2 CUSTOM 2 COIL BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V7 OFF SD Transfer Cont. 9 3 ZPASS_DO_3 CUSTOM 2 COIL BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V7 OFF SD Transfer Cont. 9 3 ZPASS_DO_3 CUSTOM 3 COIL BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V8 OFF Group Configuration Maintenance 10 4 ZPASS_DO_4 CUSTOM 4 COIL BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V8 OFF Bitheren Interfaces 11 10 GPS_ERROR CUSTOM	Rule Configuration 7 1 ZPASS_DO_1 CUSTOM 1 COIL BOOL 0 EMBEDDED 1 CM LAST 0 V6 OFF General Settings 8 2 ZPASS_DO_2 CUSTOM 2 COIL BOOL 0 EMBEDDED 1 EMBEDDED 1 0 LAST 0 V6 OFF General Settings 8 2 ZPASS_DO_2 CUSTOM 2 COIL BOOL 0 EMBEDDED 1 0 LAST 0 V7 OFF SD Transfer Conf. 9 3 ZPASS_DO_3 CUSTOM 3 COIL BOOL 0 EMBEDDED 1 0 LAST 0 V8 OFF Group Configuration 10 4 ZPASS_DO_4 CUSTOM 4 COIL BOOL 0 EMBEDDED 1 0 LAST 0 V8 OFF Maintenance 11 10 GPS_ERROR CUSTOM 10 HOLDING 16BIT 0 EMBEDDED 1 EMBEDDED 1	HTTP Configuration Message Configuration	6	4	ZPASS_DI_4	CUSTOM		4	DISCRETE	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	LAST	0	V5	OFF
Under Sourger Gorman Search Sourger Gorman Search Sourger Gorman LAST 0 VALUE 0 VA 0 FFF Group Configuration 4 COL BOOL 0 EMBEDDED 1 EMBEDDED 1 0 VALUE 0 V0 OFF	Under Sourger Gommander Bancal Satting 8 2 ZPASS_DO_2 CUSTOM 2 COIL BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V7 OFF SD Transfer Conf. 9 3 ZPASS_DO_3 CUSTOM 3 COIL BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V8 OFF Group Configuration Maintenance 10 4 ZPASS_DO_4 CUSTOM 4 COIL BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V8 OFF Beneral Interfaces 11 10 GPS_ERROR CUSTOM 4 COIL BOOL 0 EMBEDDED 1 0 LAST VALUE 0 V9 OFF FW Versions 11 10 GPS_HOUR CUSTOM 10 HOLING REGISTER UNSIGNED 0 EMBEDDED 1 EMBEDDED 1 0 LAST VALUE 0 V10 OFF FW Upgrade 12 11 GPS_HOUR CUSTOM 11 HOLING TIBIT REGISTER UNSIGNED 0 EMBEDDED <	Rule Configuration	7	1	ZPASS_DO_1	CUSTOM		1	COIL	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	LAST	0	V6	OFF
SD Transfer Conf. 9 3 ZPASS_DO_3 CUSTOM 3 COIL BOOL 0 EMBEDDED 1 0 LASE 0 V6 OFF Group Configuration 10 4 ZPASS_DO_4 CUSTOM 3 COIL BOOL 0 EMBEDDED 1 0 LASE 0 V6 OFF Group Configuration 10 4 ZPASS_DO_4 CUSTOM 4 COIL BOOL 0 EMBEDDED 1 0 LASE 0 V0 OFF Maintenance 11 10 GPS_ERROR CUSTOM 10 HOLDING 16BIT 0 EMBEDDED 1 0 LAST 0 V10 OFF W Versions 12 11 GPS_HOUR CUSTOM 11 HOLDING 16BIT 0 EMBEDDED 1 EMBEDDED 1 LAST V11 OFF Conf. Management Conf. Management Custom 11 HOLDING 16BIT	SD Transfer Conf. 9 3 ZPASS_DO_3 CUSTOM 3 COIL BOOL 0 EMBEDDED 1 EMBEDDED 1 0 LAST 0 V6 OFF Group Configuration 10 4 ZPASS_DO_4 CUSTOM 4 COIL BOOL 0 EMBEDDED 1 0 LAST 0 V6 OFF Maintenance 11 10 GPS_ERROR CUSTOM 4 COIL BOOL 0 EMBEDDED 1 EMBEDDED 1 0 UAST 0 V6 OFF Weinsidenance 11 10 GPS_ERROR CUSTOM 10 HOLDING 16BT 0 EMBEDDED 1 EMBEDDED 1 0 UAST 0 V10 OFF FW Versions 12 11 GPS_HOUR CUSTOM 11 HOLDING 16BIT 0 EMBEDDED 1 EMBEDDED 1 LAST 0 V10 OFF FW Versions 12 11 GPS_HOUR CUSTOM 11 HOLDING 16BIT <	General Settings	8	2	ZPASS_DO_2	CUSTOM		2	COIL	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	LAST	0	V7	OFF
Instruction	Incomposition Image: Construction Image: Construction <td>SD Transfer Conf. ETP Transfer Conf</td> <td>9</td> <td>3</td> <td>ZPASS_DO_3</td> <td>CUSTOM</td> <td></td> <td>3</td> <td>COIL</td> <td>BOOL</td> <td>0</td> <td>EMBEDDED</td> <td>1</td> <td>EMBEDDED</td> <td>1</td> <td>0</td> <td>LAST</td> <td>0</td> <td>V8</td> <td>OFF</td>	SD Transfer Conf. ETP Transfer Conf	9	3	ZPASS_DO_3	CUSTOM		3	COIL	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	LAST	0	V8	OFF
Maintenance Image: Control of the state	Maintenance Image: Cont. Management Image:	Group Configuration	10	4	ZPASS_DO_4	CUSTOM		4	COIL	BOOL	0	EMBEDDED	1	EMBEDDED	1	0	LAST	0	V9	OFF
EW Versions 12 11 GUILING 10BIT EMBEDDED 1 LASS V11 OFF FW Upgrade 1 Conf. Management 1 HEGUEING 10BIT EMBEDDED 1 EMBEDDED 1 EMBEDDED 1 VALUE 0 V11 OFF VALUE V11 OFF V11 V1	FW Versions 12 11 GPS_HOUR CUSTOM 11 HOLDING 10BIT 0 LST 0 V11 OFF FW Upgrade Cont. Management </td <td>Maintenance Ethernet Interfaces</td> <td>11</td> <td>10</td> <td>GPS_ERROR</td> <td>CUSTOM</td> <td></td> <td>10</td> <td>HOLDING</td> <td>16BIT SIGNED</td> <td>0</td> <td>EMBEDDED</td> <td>1</td> <td>EMBEDDED</td> <td>1</td> <td>0</td> <td>LAST</td> <td>0</td> <td>V10</td> <td>OFF</td>	Maintenance Ethernet Interfaces	11	10	GPS_ERROR	CUSTOM		10	HOLDING	16BIT SIGNED	0	EMBEDDED	1	EMBEDDED	1	0	LAST	0	V10	OFF
Conf. Management	Conf. Management	FW Versions	12	11	GPS_HOUR	CUSTOM		11	HOLDING	16BIT UNSIGNED	0	EMBEDDED	1	EMBEDDED	1	0	LAST	0	V11	OFF
		Conf. Management	4																	÷.

DELETE

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.

Z-PASS2

Gateway Tag Setup [user: admin] [logout]

Firmware Version: SW003900_290 [Modem: EC21EFAR02A03M4G]

MAC Address: C8F9811B0001 [IMEI: 861108030033046]

Internet Access: Ethernet

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

Router: disabled

TAG 27

	CURRENT	UPDATED	
GATEWAY TAG NAME	SHM_S16	SHM_S16	
GATEWAY MODBUS START REGISTER ADDRESS	101	101	Equivalent to the address in the Seneca documentation : 40101
TARGET CONNECTED TO	INTERNAL	INTERNAL V	
TARGET MODBUS REQUEST TYPE	HOLDING REGISTER	HOLDING REGISTER V	
TARGET REGISTER DATA TYPE	16BIT SIGNED	16BIT SIGNED T	
GATEWAY TAG MODE	SHARED MEMORY	SHARED MEMORY V	
INITIAL VALUE	0	0	
HTTP POST VID	26	26	Corresponding to HTTP POST variable : V26
READ ONLY	OFF	OFF V	If READ ONLY = ON, tag value cannot be changed by means of Modbus protocol
RETAIN	ON	ON 🔻	
CALCULATED FUNCTION	NONE	NONE •	
ALARM ENABLED	OFF	OFF •	This parameter can be changed in "Alarm Configuration" page
		APPLY	

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	Start Register Address of the tag	1
Address		
Target Modbus Device	Type of Modbus device: "CUSTOM"	CUSTOM
	or one of the following Seneca	
	devices:	
	"Z-D-IN"	
	"Z-10-D-IN"	
	"Z-D-OUT"	
	"Z-10-D-OUT"	
	"Z-D-IO"	

	"ZC-24-DI"	
	"ZC-24-DO"	
	"ZC-16DI-8DO"	
	"Z-4-AI-1"	
	"Z-8-AI-1"	
	"Z-3-AO"	
	"Z-4-TC"	
	"Z-8-TC"	
	"Z-203"	
	"Z-4RTD-2"	
	"Z-SG"	
	"Z-DAQ-PID"	
	"S-203T"	
	"S-203TA"	
	"ZE-4DI-2AI-2DO"	
	"ZE-2AI"	
	"Z-4DI-2AI-2DO"	
	"S203TA-D"	
	"S203RC-D"	
	"Z-PASS-IO"	
	"Z-PASS-GPS"	
Target Resource	This field identifies a particular	Empty
	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	
Target Connected To	This field identifies the serial port	The first available serial port,
	the target device is connected to;	that is the first port with
	possible values are: COM1, COM2,	"Task" other than "None"
	COM4 (only if the ports are	
	configured as master), INTERNAL or	
	the Modbus TCP-IP Server name.	
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:	HOLDING REGISTER
	COIL	
	DISCRETE INPUT	
	HOLDING REGISTER	
	INPUT REGISTER	
Target Register Data Type	Possible data types:	16 BIT SIGNED
	16BIT SIGNED	
	16BIT UNSIGNED	
	32BIT SIGNED MSW	
	32BIT UNSIGNED MSW	
	32BIT SIGNED LSW	
	32BIT UNSIGNED LSW	
	32BIT REAL MSW	
	32BIT REAL LSW	
	64BIT UNSIGNED MSW	
	64BIT UNSIGNED LSW	
	64BIT SIGNED MSW	
	64BIT SIGNED LSW	
	64BIT REAL LSW	
	BOOL	
	For more information about the	
	above data types, see table below	
Target Bit Index	This parameter defines the position,	0
	in the [016] interval, of the bit to	
	be extracted from the tag value.	
	0 means no bit shall be extracted	
	and the tag value shall be taken as a	
	whole.	
	This parameter is meaningful only	
	when the tag "Target Register Data	
	Type" is set to "16 BIT UNSIGNED"	
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.	
	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.	
	EMBEDDED	
	for embedded Digital I/Os and GPS	
	Info tags (see next paragraphs)	
Gain	This field corresponds to the <i>m</i>	1
	coefficient value in the	
	m*val+α	
	formula applied to the <i>val</i> value read	
	from the device	
Offset	This field corresponds to the <i>a</i> factor	0
	value in the	0
	m^* val + q	
	formula applied to the <i>val</i> value read	
	from the device	
Initial Value	This filed is available only if "Gateway	0
	Tag mode" is configured in "Shared	0
	Memory" and define the TAG staring	
	value.	
Error Mode	This field defines which value is	LAST VALUE
	given in the response to a Modbus	
	(read) request, when the value from	
	the target device is not available.	
	Possible modes are:	
	LAST VALUE: the last available value	
	is given	
	ERROR VALUE: the value specified in	
	the "ERROR VALUE" field is given	
Error Value	This field defines which value is	Empty
	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"	
HTTP POST VID	This field is used to build the	"V" + tag index, e.g. "V0" for
	"Variable ID" (VID) which identifies	the first tag, "V1" for the
	the tag in HTTP POST requests	second and so on

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

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".

	CURRENT	UPDATED	
GATEWAY TAG NAME		TAG	
GATEWAY MODBUS START REGISTER ADDRESS		1	Equivalent t Seneca doc
TARGET MODBUS DEVICE		CUSTOM V	
TARGET RESOURCE		•	
TARGET CONNECTED TO		INTERNAL V	
TARGET MODBUS STATION ADDRESS		1	
TARGET MODBUS START REGISTER ADDRESS		1	Equivalent t Seneca doc
TARGET MODBUS REQUEST TYPE		HOLDING REGISTER V	
TARGET REGISTER DATA TYPE		16BIT SIGNED 🔹	
GATEWAY TAG MODE		EMBEDDED 🔻	
ERROR MODE		GATEWAY	
ERROR VALUE		SHARED MEMORY]
HTTP POST VID		EMBEDDED	Correspond

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:

TAG 127



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	TARGET MODBUS	TARGET REGISTER DATA
	START REGISTER ADDRESS	REQUEST TYPE	ТҮРЕ
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.

Image: Configuration Configuration Image: Configuration Configuration Image: Configuration Configuration Real Time Cook Setup Configuration Reserves Configuration Reserves Configuration Reserves Configuration Reserves Configuration Reserves Configuration Configuration Reserves Configuration Configuration Configuration Robie Network Configuration Configuration Configuration Configuration Digital VC Configuration Configuration Configuration Configuration Configuration Configuration CW Versions Configuration Configuration Configuration Configuration Configuration Configuration Digital VC Configuration Configuration Configuration Configuration Configuration Configuration Configuration Single Configuration Configuration Configuration	P₁ Z-PASS2	×	7						Cio	vanni —		×		
SENERCIA General Configuration Nam View Main View Main View Serial Ports Serial Ports Gateway Configuration Real Time Clock Setup VPA Configuration Real Time Clock Setup Control Quartion Reverse Configuration Division Configuration Sing Configuration Sing Configuration Sing Configuration Configuration Configuration </td <td>← → C ① 192.16</td> <td>58.85.104:80</td> <td> 180/mbgw_tag</td> <td>_setup.php</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>☆ 🛛</td> <td>:</td>	← → C ① 192.16	58.85.104:80	 180/mbgw_tag	_setup.php							☆ 🛛	:		
General Configuration Gateway Tag Setup [user: admin] [logout] Hain View Firmware Version: SW003900_230 [Modem: UC20GQBR03A14E1G] Mac Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222013200438015] Gateway Configuration Internet Access: Ethernet Read Time Clock Setup Gateway: running [Data Logger: running (no group enabled)] PRO Configuration Router: running Router: Configuration Router: running Very Configuration Scegil file Nessun file selezionato Import tag configuration PW Uograde Configuration Router: running Tag Setup Delle CT MODIFY DELETE Yew Configuration MODIFY DELETE Mobile Configuration ADD MODEN MODENT Mobile Network MODENT TARGET MODENT Digital UC configuration 3 1 ZPASS_DL ZPASS DigitAL INPUTS 1 HOLDING 10 Nightal UC configuration 3 1 ZPASS_DL ZPASS DigitAL INPUTS 1 HOLDING 10 Notice Configuration 3 1 ZPASS_DL ZPASS DigitAL INP	SENECA®	Z-PASS2												
Name View Firmware Version: SW003900_230 [Modem:: UC20GQBR03A14E1G] Network and Services Gateway: Configuration MAC Addrese:: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222013200438015] Gateway: Configuration Real Time Clock Setup Gateway: running [Date Logger: running (no group enabled)] VPN Configuration Router: running Model Configuration Export tag configuration RW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup DELETE Shared Memory Tag Conf. TAB MODIFY DELETE Noble Configuration MODIS MODIS MODIS MODIS Dive Configuration CATEWAY TARGET TARGET MODIS MODIS Dive Configuration 1 1 ZPASS_DI CPASS- DigITAL INPUTS 1 HOLDING Digital I/O Configuration 2 2 ZPASS_DL CPASS- DigITAL INPUTS 1 HOLDING 1 DISCRETE MODIS MODIS <t< td=""><td>General Configuration</td><td>Gateway</td><td>/ Tag Setup [</td><td>user: admin] [</td><td>logout]</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	General Configuration	Gateway	/ Tag Setup [user: admin] [logout]									
Network and Services MAC Addresse: C8F9811B0000 [IMEI: 8610750266666172] [IMSI: 222013200438015] Serial Ports Gateway: configuration Real Time Clock Setup Gateway: running [Data Logger: running (no group enabled)] VPN Configuration Router: running Router: Configuration Except Iffle Verse Configuration Scegli file Shared Memory Tag Configuration MODIFY Tag Setup Tag Setup Tag Setup Configuration Mobile Configuration MODENT Digital IO Configuration Cateway: Model Network Digital IO Configuration 2 Digital IO Configuration 2 Sine Configuration 2 Sing Configuration 2 Digital IO Configuration 2 Sing	Main View	Firmwar	e Version: S	W003900 230	[Modem: \	JC20GQBR03A1	4E1G]							
Serial Ports Internet Access: Ethernet Gateway: running [Data Logger: running (no group enabled)] Real Time Clock Setup VPN Configuration Router: running Router: running Moto: running (Data Logger: running (no group enabled)] Process Moto: running Router: running Segli file Nessun file selezionato Import tag configuration Figuration Configuration Export tag configuration TARGET TARGET <th col<="" td=""><td>Network and Services</td><td>MAGAd</td><td></td><td></td><td>1. 0010750</td><td>000001701 [IMO</td><td>. 0000100</td><td>004000451</td><td></td><td></td><td></td><td></td></th>	<td>Network and Services</td> <td>MAGAd</td> <td></td> <td></td> <td>1. 0010750</td> <td>000001701 [IMO</td> <td>. 0000100</td> <td>004000451</td> <td></td> <td></td> <td></td> <td></td>	Network and Services	MAGAd			1. 0010750	000001701 [IMO	. 0000100	004000451					
Gateway Configuration Internet Access: Ethernet Gateway: running [Data Logger: running (no group enabled)] Provide Configuration Router: running Configuration Router: running Mobile Configuration For Upgrade Configuration Configuration Mobile Configuration Mobile Configuration Mobile Configuration Configuration Configuration Mobile Configuration DINS Configuration DINS Configuration Digital I/O Configuration Digital I/O Configuration Configuration Phonebook Digital I/O Configuration Start model Phonebook Digital I/O Configuration Start model A model model A model model Configuration A mode	Serial Ports	MAG AU	uress: Corse		1: 0010730		: 2220132	00430015]						
Gateway: running [Data Logger: running (no group enabled)] Router Configuration Router Configuration Scegli file Nessun file selezionato Import tag configuration Router: running Scegli file Nessun file selezionato Import tag configuration Page : 1/20 PREVIOUS PAGE NEXT PAGE TARGET TARGET <th <="" colspan="2" td=""><td>Gateway Configuration</td><td>Internet</td><td>Access: Eth</td><td>ernet</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th>	<td>Gateway Configuration</td> <td>Internet</td> <td>Access: Eth</td> <td>ernet</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>		Gateway Configuration	Internet	Access: Eth	ernet								
VPN Configuration Router: running Router: Configuration Scegii file Nessun file selezionato Import tag configuration Export tag configuration FW Upgrade ADD MODIFY DELETE Conf. Management Stared Memory Tag Conf. TARGET	Real Time Clock Setup	Gateway	: running [D	ata Logger: ru	nning (no	group enabled)]	I							
Notice Configuration Users Configuration Export tag configuration Configuration Export tag configuration FW Upgrade Conf. Management Shared Memory Tag Conf. Tag View TCP Servers Mobile Configuration Mobile Configuration District IVO Configuration District IVO Configuration District IVO Configuration Configuration District IVO Configuration Configuration <th colspan<="" td=""><td>VPN Configuration</td><td>Bouter</td><td>rupping</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th>	<td>VPN Configuration</td> <td>Bouter</td> <td>rupping</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	VPN Configuration	Bouter	rupping										
Scegli file Nessun file selezionato Import tag configuration Export tag configuration FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup DELETE Tag View DELETE TARGET TARGET MODBUS REGISTER TARGET TARGET MODBUS REGISTER	Bouter Configuration	mouter.	unning											
Few Uograde Conf. Management ADD MODIFY DELETE Shared Memory Tag Conf. Tag Stup Page : 1/20 PREVIOUS PAGE NEXT PAGE Tag View TCP Servers Mobile Configuration MODBUS TARGET	Users Configuration	Sceali f	file Nessun fil	e selezionato	Impo	rt tag configuration	Export	tag configu	ration					
ADDMODIFYDELETEShared Manogrent Shared Memory Tag Corl. Tag SetupADDMODIFYDELETETag SetupTag SetupPage: 1/20PREVIOUS PAGENEXT PAGETCP Severs Mobile Configuration 	EW Llograde	Joogin												
Contension of the property tage contension of the property tage of the	Conf Management	[ADD		MODIFY		DFI	ETE						
Page : 1/20 PREVIOUS PAGE NEXT PAGE Tag Setur Tage Tage Tage Tage Tage Tage Tage Tage	Shared Memory Tag Conf	l												
ControlTag ViewTCP ServersMobile ConfigurationCATEWAY MODEUSCATEWAY MODEUSCATEWAY TAG NAMETARGET TAG NAMETARGET RESOURCETARGET MODEUS RESOURCETARGET MODEUS REGISTERTARGET MODEUS REGISTERTARGET MODEUS TARGET TYPETARGET TARGET TYPETARGET TARGET TYPETARGET MODEUS TARGET REGISTERTARGET MODEUS TARGET TYPETARGET MODEUS TARGET TYPETARGET MODEUS TARGET REGISTERTARGET MODEUS TARGET TYPETARGET TARGET TODEUS TYPETARGET TARGET TARGET TYPETARGET MODEUS TARGET TREGISTERTARGET MODEUS TARGET TYPETARGET TARGET TARGET TODEUS TYPETARGET TARGET TARGET TODEUS TYPETARGET TARGET TARGET TARGET TARGET TODEUS TODEUS TYPETARGET TARGET TARGET TARGET TARGET TODEUS TYPETARGET TARGET TARGET TARGET TODEUS TYPETARGET TARGET TARGET TARGET TARGET TYPETARGET TARGET<	Tag Setup				Page: 1/	20 PREVIOUS	PAGEN	EXT PAGE						
Tep Servers Mobile Configuration Mobile NetworkCATEWAY TAG NRCATEWAY MODBUS START HEGISTERCATEWAY TAG NAMETARGET MODBUS DEVICETARGET MODBUS RESOURCETARGET MODBUS RESOURCETARGET MODBUS REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARGET REGISTERTARG	Tag View				3									
Instruction Configuration Configuration <thconfiguration< th=""> <thconfiguration< th=""></thconfiguration<></thconfiguration<>	TCP Servers											_		
Mabile Network DDNS ConfigurationTAG NRSTATT HEGISTERTAG NAMEMODBUS TAG NAMERESOURCESTART RESOURCEREOUEST RESOURCEREOUEST REGISTERNDATA TYPEDigital VO Configuration Digital VO Configuration11ZPASS_DI2.PASS 0DIGITAL INPUTS1HOLDING HOLDING10BIT 10BIT 10BIT 10BIT 10BIT 222ZPASS_DI 102.PASS 0DIGITAL INPUTS1HOLDING 10BIT 10BIT 10BIT 10BIT 10BIT 10BIT 10BIT 10BIT 10BITAL INPUT1BOLDING 10BIT 10BIT 10BIT 10BIT 10BIT 10BIT 10BITAL INPUT1HOLDING 10BITAL 10BIT 10BIT 10BIT 10BIT 10BIT 10BITAL INPUT1HOLDING 10BITAL 10BIT 10BIT 10BIT 10BITAL INPUT1BOLDINSCRETE 10BITAL INPUTPhonebook Diagnostics42ZPASS_DI_2Z-PASS- 10DIGITAL INPUT 11DISCRETE 10BITAL INPUTBOOL 10PUT 10PUTINPUT 10PUTBOOL 10PUTFW Versions Ethernet Interfaces 0 064ZPASS_DI_3Z-PASS- 10DIGITAL INPUT 33DISCRETE 10PUTBOOL 10PUTGroup Configuration71ZPASS_D0_12.PASS- 10DIGITAL OUTPUT 11COIL 10CILBOOL93ZPASS_D0_3Z-PASS- 10DIGITAL OUTPUT 12COIL 10BOOL93ZPASS_D0_4Z-PASS- 10DIGITAL OUTPUT 33COIL 10BOOL104ZPASS_D0_4	Mobile Configuration	GATEWA	GATEWAY MODBUS	GATEWAY	TARGET	TARGET	TARGET	TARGET	TARGET	TARGET	TARGE	ET G		
DDNS Configuration Digital I/O ConfigurationREGISTERTYPETYPETYPETYPE111ZPASS_DIZ-PASS- IODIGITAL INPUTS1HOLDING REGISTER UNSIGNEI22ZPASS_DOZ-PASS- 	Mobile Network	TAG NR	START	TAG NAME	MODBUS	RESOURCE	START	REQUEST	DATA	CONNECTED	STATIC	DN T.		
Digital I/O Configuration11ZPASS_DIZ-PASS-DIDIGITAL INPUTS1HOLDING10BIT REGISTER UNSIGNETDigital I/O Configuration22ZPASS_DOZ-PASS- IODIGITAL OUTPUTS2HOLDING10BIT REGISTER UNSIGNETSMS Configuration31ZPASS_DL 2Z-PASS- IODIGITAL INPUT 11DISCRETE INPUTBOOLPhonebook42ZPASS_DL2Z-PASS- IODIGITAL INPUT 22DISCRETE INPUTBOOLPhonebook42ZPASS_DL2Z-PASS- IODIGITAL INPUT 22DISCRETE INPUTBOOLFW Versions53ZPASS_DL3Z-PASS- IODIGITAL INPUT 33DISCRETE INPUTBOOLEthernet Interfaces64ZPASS_DL4Z-PASS- IODIGITAL OUTPUT 33DISCRETE INPUTBOOLGroup Configuration71ZPASS_DD_2Z-PASS- IODIGITAL OUTPUT 11COILBOOL82ZPASS_DD_2Z-PASS- IODIGITAL OUTPUT 11COILBOOL93ZPASS_DD_3Z-PASS- IODIGITAL OUTPUT 33COILBOOL104ZPASS_DD_4Z-PASS- IODIGITAL OUTPUT 3COILBOOL104ZPASS_DD_4Z-PASS- IODIGITAL OUTPUT 3COILBOOL1110GPS_ERRORZ-PASS- GPSGPS_ERROR10HOLDING 10BIT REGISTER SIGNED12 </td <td>DDNS Configuration</td> <td></td> <td>REGISTER</td> <td></td> <td>DEVICE</td> <td></td> <td>REGISTER</td> <td>TYPE</td> <td>TYPE</td> <td>10</td> <td>ADDRE</td> <td>SS</td>	DDNS Configuration		REGISTER		DEVICE		REGISTER	TYPE	TYPE	10	ADDRE	SS		
Digital I/O Configuration22ZPASS_DOZ-PASS- IODIGITAL OUTPUTS2HOLDING REGISTER UNSIGNEISMS Configuration31ZPASS_DLZ-PASS- IODIGITAL INPUT1IDISCRETE INPUTBOOLPhonebook42ZPASS_DL2Z-PASS- IODIGITAL INPUT1IDISCRETE INPUTBOOLFW Versions53ZPASS_DL3Z-PASS- IODIGITAL INPUT2DISCRETE INPUTBOOLEthernet Interfaces64ZPASS_DL4Z-PASS- IODIGITAL INPUT3DISCRETE INPUTBOOLData Logger (SD missing)64ZPASS_DD_1Z-PASS- IODIGITAL INPUT4DISCRETE INPUTBOOLGroup Configuration71ZPASS_DD_1Z-PASS- IODIGITAL OUTPUT 11COILBOOL82ZPASS_DD_2Z-PASS- IODIGITAL OUTPUT IO1COILBOOL93ZPASS_DD_3Z-PASS- IODIGITAL OUTPUT 33COILBOOL93ZPASS_DD_3Z-PASS- IODIGITAL OUTPUT 44COILBOOL104ZPASS_DD_4Z-PASS- IODIGITAL OUTPUT 44COILBOOL1110GPS_ERRORZ-PASS- GPSGPS_ERROR10HOLDING HEGISTER SIGNED1211GPS_HOURZ-PASS- GPSGPS_UTC_HH11HOLDING HOLDING 108IT HEGISTER UNSIGNEE12<	Digital I/O Configuration	1	1	ZPASS_DI	Z-PASS-	DIGITAL INPUTS	1	HOLDING	16BIT UNSIGNED	EMBEDDED	1	EI		
Logic Configuration2222PASS_DOIOOUTPUTS2REGISTER UNSIGNEISMS Configuration31ZPASS_DL1Z-PASS_DI2DIGITAL INPUT1DISCRETE INPUTBOOLPhonebook42ZPASS_DL2Z-PASS- IODIGITAL INPUT 11DISCRETE INPUTBOOLFW Versions53ZPASS_DL3Z-PASS- 	Digital I/O Configuration		_		Z-PASS-	DIGITAL	_	HOLDING	16BIT					
SMS Configuration 3 1 ZPASS_DL_1 Z-PASS- IO DIGITAL INPUT 1 1 DISCRETE INPUT BOOL Phonebook 4 2 ZPASS_DL_2 Z-PASS- IO DIGITAL INPUT 2 2 DISCRETE INPUT BOOL FW Versions 5 3 ZPASS_DL_3 Z-PASS- IO DIGITAL INPUT 3 3 DISCRETE INPUT BOOL Data Logger (SD missing) 6 4 ZPASS_DL_4 Z-PASS- IO DIGITAL INPUT 4 4 DISCRETE INPUT BOOL General Settings 7 1 ZPASS_DO_1 Z-PASS- IO DIGITAL OUTPUT 1 1 COIL BOOL 8 2 ZPASS_DO_2 Z-PASS- IO DIGITAL OUTPUT 2 2 COIL BOOL 9 3 ZPASS_DO_3 Z-PASS- IO DIGITAL OUTPUT 2 2 COIL BOOL 9 3 ZPASS_DO_4 Z-PASS- IO DIGITAL OUTPUT 3 3 COIL BOOL 10 4 ZPASS_DO_4 Z-PASS- IO DIGITAL OUTPUT 4 4 COIL BOOL 11 10 GPS_ERROR Z-PASS- IO <td>Logic Configuration</td> <td>2</td> <td>2</td> <td>ZPASS_DO</td> <td>IO</td> <td>OUTPUTS</td> <td>2</td> <td>REGISTER</td> <td>UNSIGNED</td> <td>EWBEDDED</td> <td>1</td> <td>EI</td>	Logic Configuration	2	2	ZPASS_DO	IO	OUTPUTS	2	REGISTER	UNSIGNED	EWBEDDED	1	EI		
Phonebook Diagnostics42ZPASS_DI_2Z-PASS- IODIGITAL INPUT 22DISCRETE INPUTBOOLFW Versions53ZPASS_DI_3Z-PASS- IODIGITAL INPUT 33DISCRETE INPUTBOOLEthernet Interfaces Data Logger (SD missing) General Settings64ZPASS_DI_4Z-PASS- IODIGITAL INPUT 44DISCRETE INPUTBOOLGroup Configuration71ZPASS_DO_1Z-PASS- IODIGITAL OUTPUT 11COILBOOL82ZPASS_DO_2Z-PASS- IODIGITAL OUTPUT 22COILBOOL93ZPASS_DO_3Z-PASS- IODIGITAL OUTPUT 33COILBOOL93ZPASS_DO_4Z-PASS- IODIGITAL OUTPUT 33COILBOOL104ZPASS_DO_4Z-PASS- IODIGITAL OUTPUT 33COILBOOL1110GPS_ERRORZ-PASS- GPSGPS_ERROR10HOLDING HOLDING REGISTER SIGNED16BIT REGISTER IDBIT1211GPS_HOURZ-PASS- GPSGPS_UTC_HH11HOLDING HOLDING REGISTER UNSIGNED	SMS Configuration	3	1	ZPASS_DI_1	Z-PASS-	DIGITAL INPUT 1	1	DISCRETE	BOOL	EMBEDDED	1	EI		
Diagnostics 4 2 ZPASS_DI_2 2 FNOS DIGITAL INPUT 2 2 DISCRETE BOOL FW Versions 5 3 ZPASS_DI_3 Z-PASS- IO DIGITAL INPUT 3 3 DISCRETE BOOL Ethernet Interfaces 6 4 ZPASS_DI_4 Z-PASS- IO DIGITAL INPUT 3 3 DISCRETE INPUT BOOL General Settings 6 4 ZPASS_DO_1 Z-PASS- IO DIGITAL OUTPUT 4 4 DISCRETE INPUT BOOL Group Configuration 7 1 ZPASS_DO_2 Z-PASS- IO DIGITAL OUTPUT 1 1 COIL BOOL 8 2 ZPASS_DO_2 Z-PASS- IO DIGITAL OUTPUT 2 2 COIL BOOL 9 3 ZPASS_DO_3 Z-PASS- IO DIGITAL OUTPUT 2 2 COIL BOOL 9 3 ZPASS_DO_4 Z-PASS- IO DIGITAL OUTPUT 3 3 COIL BOOL 10 4 ZPASS_DO_4 Z-PASS- IO DIGITAL OUTPUT 4 COIL BOOL 11 10 GPS_ERROR Z-PASS- GPS_ERROR GPS_ERROR <td>Phonebook</td> <td></td> <td></td> <td></td> <td>7-PASS-</td> <td></td> <td></td> <td>DISCRETE</td> <td></td> <td></td> <td></td> <td></td>	Phonebook				7-PASS-			DISCRETE						
FW Versions 5 3 ZPASS_DL_3 Z-PASS- IO DIGITAL INPUT 3 3 DISCRETE INPUT BOOL Data Logger (SD missing) 6 4 ZPASS_DL_4 Z-PASS- IO DIGITAL INPUT 4 4 DISCRETE INPUT BOOL General Settings 7 1 ZPASS_DO_1 Z-PASS- IO DIGITAL OUTPUT 1 1 COIL BOOL 8 2 ZPASS_DO_2 Z-PASS- IO DIGITAL OUTPUT 2 2 COIL BOOL 9 3 ZPASS_DO_3 Z-PASS- IO DIGITAL OUTPUT 2 2 COIL BOOL 9 3 ZPASS_DO_3 Z-PASS- IO DIGITAL OUTPUT 2 3 COIL BOOL 10 4 ZPASS_DO_4 Z-PASS- IO DIGITAL OUTPUT 3 3 COIL BOOL 11 10 GPS_ERROR Z-PASS- GPS_ERROR IO HOLDING 4 HOLDING REGISTER HOBIT REGISTER IdBIT REGISTER IdBIT REGISTER IdBIT REGISTER IdBIT REGISTER IdBIT REGISTER IdBIT REGISTER IdBIT REGISTER	Diagnostics	4	2	ZPASS_DI_2	10	DIGITAL INPUT 2	2	INPUT	BOOL	EMBEDDED	1	EI		
Ethernet Interfaces 0 Ethernet Interfaces 10 Ethernet Interfaces 10 Ethernet Interfaces 0 Ethernet Interfaces Ethere Ethernet Interfaces Ethe	FW Versions	5	3	ZPASS DL 3	Z-PASS-	DIGITAL INPUT 3	3	DISCRETE	BOOL	EMBEDDED	1	FI		
Data Logger (SD missing) 6 4 ZPASS_DI_4 2PASS_DIGITAL INPUT 4 4 DISCHETE BOOL INPUT BOOL General Settings 7 1 ZPASS_DO_1 Z-PASS- IO DIGITAL INPUT 4 4 DISCHETE BOOL INPUT BOOL 8 2 ZPASS_DO_2 Z-PASS- IO DIGITAL OUTPUT 2 2 COIL BOOL 9 3 ZPASS_DO_3 Z-PASS- IO DIGITAL OUTPUT 2 2 COIL BOOL 9 3 ZPASS_DO_3 Z-PASS- IO DIGITAL OUTPUT 3 3 COIL BOOL 10 4 ZPASS_DO_4 Z-PASS- IO DIGITAL OUTPUT 4 COIL BOOL 11 10 GPS_ERROR Z-PASS- GPS_GPS_ERROR 10 HOLDING REGISTER SIGNED 12 11 GPS_HOUR Z-PASS- GPS GPS_UTC_HH 11 HOLDING REGISTER UNSIGNED	Ethernet Interfaces	-	-		10			INPUT						
General Settings 7 1 ZPASS_DO_1 Z-PASS- IO DIGITAL OUTPUT 1 1 COIL BOOL 8 2 ZPASS_DO_2 Z-PASS- IO DIGITAL OUTPUT 2 2 COIL BOOL 9 3 ZPASS_DO_3 Z-PASS- IO DIGITAL OUTPUT 2 3 COIL BOOL 10 4 ZPASS_DO_4 Z-PASS- IO DIGITAL OUTPUT 3 3 COIL BOOL 10 4 ZPASS_DO_4 Z-PASS- IO DIGITAL OUTPUT 4 4 COIL BOOL 11 10 GPS_ERROR Z-PASS- GPS_ERROR IO HOLDING 4 HOLDING REGISTER SIGNED 12 11 GPS_HOUR Z-PASS- GPS GPS_UTC_HH 11 HOLDING HEGISTER UNSIGNED	Data Logger (SD missing)	6	4	ZPASS_DI_4	Z-PASS- IO	DIGITAL INPUT 4	4	INPUT	BOOL	EMBEDDED	1	Eľ		
8 2 ZPASS_DO_2 Z-PASS- IO DIGITAL OUTPUT 2 2 COIL BOOL 9 3 ZPASS_DO_3 Z-PASS- IO DIGITAL OUTPUT 3 3 COIL BOOL 10 4 ZPASS_DO_4 Z-PASS- IO DIGITAL OUTPUT 4 4 COIL BOOL 11 10 GPS_ERROR Z-PASS- GPS_ERROR IO HOLDING 4 HOLDING REGISTER IfBIT REGISTER 12 11 GPS_HOUR Z-PASS- GPS GPS_UTC_HH 11 HOLDING REGISTER IfBIT REGISTER	General Settings Group Configuration	7	1	ZPASS_DO_1	Z-PASS- IO	DIGITAL OUTPUT 1	1	COIL	BOOL	EMBEDDED	1	EI		
9 3 ZPASS_DO_3 Z-PASS- DIGITAL OUTPUT 3 COIL BOOL 10 4 ZPASS_DO_4 Z-PASS- DIGITAL OUTPUT 4 COIL BOOL 11 10 GPS_ERROR Z-PASS- GPS_ERROR 10 HOLDING 16BIT 12 11 GPS_HOUR Z-PASS- GPS_UTC_HH 11 HOLDING 16BIT REGISTER UNSIGNED 4		8	2	ZPASS_DO_2	Z-PASS- IO	DIGITAL OUTPUT 2	2	COIL	BOOL	EMBEDDED	1	EI		
10 4 ZPASS_DO_4 Z-PASS- IO DIGITAL OUTPUT 4 4 COIL BOOL 11 10 GPS_ERROR Z-PASS- GPS GPS_ERROR 10 HOLDING REGISTER 16BIT SIGNED 12 11 GPS_HOUR Z-PASS- GPS GPS_UTC_HH 11 HOLDING HOLDING 16BIT REGISTER		9	3	ZPASS_DO_3	Z-PASS- IO	DIGITAL OUTPUT 3	3	COIL	BOOL	EMBEDDED	1	EI		
11 10 GPS_ERROR Z-PASS- GPS_ERROR 10 HOLDING 16BIT GPS GPS_GPS_GPS_UTC_HH 11 HOLDING 16BIT 12 11 GPS_HOUR GPS GPS_UTC_HH 11 HOLDING 16BIT REGISTER UNSIGNED		10	4	ZPASS_DO_4	Z-PASS- IO	DIGITAL OUTPUT 4	4	COIL	BOOL	EMBEDDED	1	EI		
12 11 GPS_HOUR Z-PASS- GPS_UTC_HH 11 HOLDING 16BIT GPS GPS_UTC_HH 11 REGISTER UNSIGNED		11	10	GPS_ERROR	Z-PASS- GPS	GPS_ERROR	10	HOLDING REGISTER	16BIT SIGNED	EMBEDDED	1	EI		
4 GF3 REGISTER UNSGINEL		12	11	GPS_HOUR	Z-PASS-	GPS_UTC_HH	11	HOLDING		EMBEDDED	1	EL		
4	4											•		

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	TARGET MODBUS	TARGET REGISTER DATA		
	START REGISTER ADDRESS	REQUEST TYPE	ТҮРЕ		
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 EMBEDDED

- TARGET CONNECTED TO

180
- GATEWAY TAG MODE

EMBEDDED

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

C Z-PASS2	×\							Co	and —		×
← → C 🛈 192.16	8.85.104:8	080/mbgw_t	ag_setup.php							☆ ♪	:
Seneral Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Bouter Configuration	Z-PASS Gatewa Firmwa MAC Ad Internet Gatewa Router:	Z-PASS2 Gateway Tag Setup [user: admin] [logout] Firmware Version: SW003900_230 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 8610750266666172] [IMSI: 222013200438015] Internet Access: Ethernet Gateway: running [Data Logger: running (no group enabled)] Router: running Scegli file Nessun file selezionato									
Users Configuration	Scegli	file Nessun	file selezionato	Impo	ort tag configuration	Expo	ort tag configura	ation			
FW Upgrade				ODIEV							
Conf. Management Shared Memory Tag Conf. Tag Setup		ADD	M	ODIFY Page : 1	20 PREVIOUS PA	GE	NEXT PAGE				
Tag View		10	0.00 50000	Z-PASS-		10	HOLDING	16BIT			- 4
Mobile Configuration		10	GP5_ERROR	GPS	GPS_ERROR	10	REGISTER	SIGNED	EMBEDDED		EI
Mobile Network	12	11	GPS_HOUR	GPS	GPS_UTC_HH	11	REGISTER	UNSIGNED	EMBEDDED	1	El
Digital I/O Configuration	13	12	GPS_MINUTE	Z-PASS- GPS	GPS_UTC_MM	12	HOLDING REGISTER	16BIT UNSIGNED	EMBEDDED	1	El
Digital I/O Configuration	14	13	GPS_SECOND	Z-PASS- GPS	GPS_UTC_SS	13	HOLDING REGISTER	16BIT UNSIGNED	EMBEDDED	1	EI
SMS Configuration	15	14	GPS_DAY	Z-PASS-	GPS_DATE_DD	14	HOLDING	16BIT	EMBEDDED	1	EI
Phonebook	16	15	GPS MONTH	Z-PASS-	GPS DATE MM	15	HOLDING	16BIT	EMBEDDED	1	EI
FW Versions	17	18		Z-PASS-		10	HOLDING	16BIT			-
Ethernet Interfaces	17	10	GP5_TEAR	GPS	GPS_DATE_TT	10	REGISTER	UNSIGNED	EMBEDDED		EI
Data Logger (SD missing)	18	17	GPS_LATITUDE	GPS	GPS_LATITUDE	17	REGISTER	REAL	EMBEDDED	1	EI
General Settings Group Configuration	19	21	GPS_LONGITUDE	Z-PASS- GPS	GPS_LONGITUDE	21	HOLDING REGISTER	64BIT REAL	EMBEDDED	1	EI
	20	25	GPS_HDOP	Z-PASS- GPS	GPS_HDOP	25	HOLDING REGISTER	64BIT REAL	EMBEDDED	1	EI
	21	29	GPS_ALTITUDE	Z-PASS- GPS	GPS_ALTITUDE	29	HOLDING REGISTER	64BIT REAL	EMBEDDED	1	EI
	22	33	GPS_COG	Z-PASS- GPS	GPS_COG	33	HOLDING	64BIT REAL	EMBEDDED	1	EI
	23	37	GPS_SPEED_KM	Z-PASS- GPS	GPS_SPKM	37	HOLDING	64BIT REAL	EMBEDDED	1	EI
	24	41	GPS_SPEED_KN	Z-PASS- GPS	GPS_SPKN	41	HOLDING	64BIT REAL	EMBEDDED	1	EI
	4										Þ
4											+

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.

8	- 17 - Ci	~ -				ZPASS_gateway_file	e_build_from_Ex	cel_rev11.xlsm	- Microsoft E	xcel						- 0	×
F	e Home	Inserisci Layo	out di pagina Formule Dat	i Revisione Visualia	za Componenti aggiuntivi Te	iam.										۵ 🕜	- 9° 23
ľ	👗 Taglia	Calibri	· 11 · A ∧ = =	🗧 😹 🖓 🕶 📑 Testo	a capo Testo	-		Normale	Neutr	ale Valore no	n v Valore va	lido Calcolo		*	Σ Somma automatica	· 27	an i
Inco	IIa		• m • & • A • = =		e allinea al centro - 📑 - % 000	+0 00 Formattazione	Formatta	Cella colleg	ata Cella o	da cont Input	Nota	Output	- Inserise	i Elimina Formato	Riempimento *	Ordina	Trova e
	Copia 1	formato =	Carallera	Alliansanta	The second	condizionale	r come tabella *			C100			·	Calle	Z Cancella *	e filtra * si	eleziona *
_	Appunti		Carattere 13	Allineamento	ia Numeri	9				200				Celle	Mod	fica	-
	13	• (5	Jx EMBEDDED														^
																	0
		0	C	D	r	r	0				V			N	0	0	
- 41	A	в	U	U	E	P	0	n		, , , , , , , , , , , , , , , , , , , ,	ĸ	L	IVI	IN	0	٢	<u>u</u> =
		GATEWAY PA	RAMETERS		TARGET	PARAMETERS					1	AG PARAMETERS	÷				
1								TARGET	TARGET							Export	tugi
	GATEWAY	GATEWAY TAG	GATEWAY MODBUS START	TARGET MODBUS			TARGET	MODBUS	MODBUS							ine.	····
	TAG NR	NAME	REGISTER	REQUEST TYPE	TARGET REGISTER DATA TYPE	TARGET BIT INDEX	CONNECTED	START	STATION	GATEWAY MODE	m VALUE	q VALUE	ERROR MODE	ERROR VALUE	HTTP POST VID	Import	rt CGI
2							то	REGISTER	ADDRESS							se file.	in
3	1	ZPASS DI	1	HOLDING REGISTER	16BIT UNSIGNED	0	EMBEDDED	1	1	EMBEDDED	1	0	LAST VALUE	0	0		
4	2	ZPASS_DO	· 2	HOLDING REGISTER	16BIT UNSIGNED	0	EMBEDDED	2 '	1	EMBEDDED	1 '	0	LAST VALUE	0	1		
5	3	ZPASS_DI_1	1	DISCRETE INPUT	BOOL	0	EMBEDDED	1 1 [']	1	EMBEDDED	1 '	0	LAST VALUE	· 0	2		
6	4	ZPASS_DI_2	2	DISCRETE INPUT	BOOL	0	EMBEDDED	2	1	EMBEDDED	1	0	LAST VALUE	0	3		
7	5	ZPASS_DI_3	3	DISCRETE INPUT	BOOL	0	EMBEDDED	3	1	EMBEDDED	1	0	LAST VALUE	0	4		
8	6	ZPASS_DI_4	4	DISCRETE INPUT	BOOL	0	EMBEDDED	4 [1	EMBEDDED	1	0	LAST VALUE	0	5		
9	7	ZPASS_DO_1	1	COIL	BOOL	0	EMBEDDED	1 1	1	EMBEDDED	1	0	LAST VALUE	0	6		
10	8	ZPASS_DO_2	2	COIL	BOOL	0	EMBEDDED	2	1	EMBEDDED	1	0	LAST VALUE	0	7		
11	9	ZPASS_DO_3	3	COIL	BOOL	0	EMBEDDED	3	1	EMBEDDED	1	0	LAST VALUE	0	8		
12	10	ZPASS_DO_4	4	COIL	BOOL	0	EMBEDDED	4 1	1	EMBEDDED	1	0	LAST VALUE	0	9		
13	11	GPS_ERROR	10	HOLDING REGISTER	16BIT SIGNED	0	EMBEDDED	10	1	EMBEDDED	1	0	LAST VALUE	0	10		
14	12	GPS_HOUR	11	HOLDING REGISTER	16BIT UNSIGNED	0	EMBEDDED	11	1	EMBEDDED	1	0	LAST VALUE	0	11		
15	13	GPS_MINUTE	, 12	HOLDING REGISTER	16BIT UNSIGNED	0	EMBEDDED	, 12 ,	1	EMBEDDED	1	0	LAST VALUE	0	. 12		
16	14	GPS_SECOND	, 13	HOLDING REGISTER	16BIT UNSIGNED	0	EMBEDDED	, 13 ,	1	EMBEDDED	1	0	LAST VALUE		, 13		
17	15	GPS_DAY	, 14	HOLDING REGISTER	16BIT UNSIGNED	0	EMBEDDED	, 14 ,	1	EMBEDDED	1	0	LAST VALUE		, 14		
18	10	GPS_MONTH	, 15	HOLDING REGISTER	16BIT UNSIGNED	0	EMBEDDED	, 15 ,	1	EMBEDDED	1	0	LAST VALUE		· 15		
19	10	GPS_TEAK	, 10	HOLDING REGISTER	10BIT UNSIGNED	0	EMBEDDED	, 10 ,	1	EMBEDDED	- t -	0	LAST VALUE		· 10		
20	10	GPS_DATITODE	* ¹⁷	HOLDING REGISTER	64BIT REAL	0	EMBEDDED	, 1/, ,	1	EMBEDDED			LAST VALUE	-	· 10		
22	20	GPS HDOP	/ 25	HOLDING REGISTER	64BIT REAL	0	EMBEDDED	· 25 ·	1	EMBEDDED	1 .	0	LAST VALUE		19		
23	21	GPS ALTITUDE	29	HOLDING REGISTER	64BIT REAL	0	EMBEDDED	29	1	EMBEDDED	1 .	ő	LAST VALUE	· .	* 20		
24	22	GPS COG	/ 33	HOLDING REGISTER	64BIT REAL	0	EMBEDDED	33 '	1	EMBEDDED	1 .	0	LAST VALUE	· 0	21		
25	23	GPS SPEED KM	37	HOLDING REGISTER	64BIT REAL	ő	EMBEDDED	37	1	EMBEDDED	1 .	0	LAST VALUE	. 0	- 22		
26	24	GPS SPEED KN	41	HOLDING REGISTER	64BIT REAL	0	EMBEDDED	41	1	EMBEDDED	1 .	0	LAST VALUE	. 0	23		
27	25	GPS FIX	45	HOLDING REGISTER	16BIT UNSIGNED	0	EMBEDDED	45	1	EMBEDDED	1 .	0	LAST VALUE		- 24		
28	26	GPS NUM SAT	46	HOLDING REGISTER	16BIT UNSIGNED	0	EMBEDDED	46	1	EMBEDDED	1	0	LAST VALUE	0	25		
29	27																
30	28																
31	29																
32	30																
33	31																
34	32																
35	B H TAGE																*
Pro	to	Constanting (Cal													III II 100% (-		()
																- V	

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.

🗅 Z-PASS2	×	+									-		>
\leftrightarrow \rightarrow C \odot No	n sicuro 192	2.168.85.104:808	0/mbgw_ta	ig_view.php						☆	· 2	G	
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 Mobile Configuration Mobile Network	Z-PASS2 Gateway Ti Firmware W MAC Addre Internet Ao Gateway: r Router: dis	ag View [user: /ersion: SW003 ess: C8F9811B cess: None unning [Data L uabled Data I	admin] [lc 9900_240 00000 [IME 00gger: ru	ogout] [Modem: U(I: 86107502 nning] START ST PREVIOUS F	C20GQBR(66666172] OP CLE/	03A14E IMSI: 2 AN CAC	:1G] 22101600 HE)239291]		ж 			
DDNS Configuration Shared Memory Tag Conf. TCP Servers	GATEWAY TAG NR	GATEWAY TAG NAME	GATEWAY MODBUS START REGISTER	TAG REQUEST TYPE	TAG DATA TYPE	TAG VALUE	TAG READING STATUS	LAST REFRESH TIME	ALARM	ANALOG DANGER ALARM		l	•
Tag Setup Tag View	1	ZPASS_DI	1	HOLDING REGISTER	16BIT UNSIGNED	0	-	06/12/2018 14:05:13.402381	NONE	NONE	CHANG	E	
Alarms	2	ZPASS_DO	2	HOLDING	16BIT UNSIGNED	0	-	06/12/2018	NONE	NONE	CHANG	E	
Alarm Summary	3	ZPASS_DI_1	1	DISCRETE	BOOL	0	-	06/12/2018	NONE	NONE			
Alarm History Logic Configuration	4	ZPASS_DI_2	2	DISCRETE	BOOL	0	-	06/12/2018	NONE	NONE			
Phonebook	5	ZPASS_DI_3	3	DISCRETE INPUT	BOOL	0	-	06/12/2018 14:05:13.403781	NONE	NONE			
SMS Configuration Email Configuration	6	ZPASS_DI_4	4	DISCRETE	BOOL	0	-	06/12/2018 14:05:13.403817	NONE	NONE			
HTTP Configuration	7	ZPASS_DO_1	1	COIL	BOOL	0	-	06/12/2018	NONE	NONE	CHANG	ε	
Message Configuration Rule Configuration	8	ZPASS_DO_2	2	COIL	BOOL	0	-	06/12/2018 14:05:13.404291	NONE	NONE	CHANG	θE	
Data Logger (SD missing) General Settings	9	ZPASS_DO_3	з	COIL	BOOL	0	-	06/12/2018 14:05:13.404442	NONE	NONE	CHANG	ε	
SD Transfer Conf.	10	ZPASS_DO_4	4	COIL	BOOL	0	-	06/12/2018 14:05:13 404717	NONE	NONE	CHANG	ε	
FTP Transfer Conf.	11	GPS_ERROR	10	HOLDING	16BIT SIGNED	-1	-	06/12/2018	NONE	NONE	CHANG	ε	
Aroup Configuration Maintenance	12	GPS_HOUR	11	HOLDING	16BIT UNSIGNED	0	-		NONE	NONE	CHANG	ε	
Ethernet Interfaces FW Versions FW Upprade	13	GPS_MINUTE	12	HOLDING		0	-		NONE	NONE	CHANG	E	Ŧ
Conf. Management													

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).

🗋 Z-PASS1	×	+											-		×
\leftrightarrow \rightarrow C (i) No	n sicuro 19	2.168.85.103:80	080/mbgw	_tag_view.pl	hp							☆	r	G	:
SENECA® Basic Configuration Summary Network and Services Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration VPN Configuration	Z-PASS1 Gateway 1 Firmware MAC Addr Internet A Gateway: Router: ru	Z-PASS1 Gateway Tag View [user: admin] [logout] Firmware Version: SW003900_240 MAC Address: C8F9811B0001 Internet Access: None Gateway: running [Data Logger: running] Router: running													
Router Configuration		Dat	a Logger:	START	STOP CI	LEAN C	ACHE								
Shared Memory Tag Conf. TCP Servers		Pa	ge : 1/20	PREVIOU	S PAGE	NEXT P	AGE								
Tag Setup			GATEWAY	TAG			TAG								
Tag View Alarms	GATEWAY TAG NR	GATEWAY TAG NAME	MODBUS START	REQUEST	TAG DATA TYPE	TAG VALUE	READING	LAST REFRESH TIME	ALARM	DANGER					
Alarm Configuration			REGISTER	HOLDING	16BIT		314103	07/12/2018		ALAIIM					
Alarm Summary	1	ZPASS_DI	1	REGISTER	UNSIGNED	1	-	10:46:39.708541	NONE	NONE	CHANGE				
Alarm History	2	ZPASS_DO	2	HOLDING REGISTER	16BIT UNSIGNED	0	-	07/12/2018 10:46:39.709223	NONE	NONE	CHANGE				
Phonebook	3	ZPASS_DI_1	1	DISCRETE	BOOL	1	-	07/12/2018	ALARM	NONE					
Email Configuration	4	78488 DL 0	0	DISCRETE	ROOL	0		07/12/2018	NONE	NONE					
HTTP Configuration	4	ZPASS_DI_2	2	INPUT	BOOL	U	-	10:46:39.709676	NONE	NONE					
Message Configuration	5	ZPASS_DI_3	3	INPUT	BOOL	0	-	07/12/2018 10:46:39.709891	NONE	NONE					
Rule Configuration Data Logger (SD found)	6	ZPASS_DI_4	4	DISCRETE INPUT	BOOL	0	-	07/12/2018 10:46:39.709925	NONE	NONE					
General Settings	7	ZPASS_DO_1	1	COIL	BOOL	0	-	07/12/2018 10:46:39 710138	NONE	NONE	CHANGE				
SD Transfer Conf.	8	ZPASS DO 2	2	COIL	BOOL	0		07/12/2018	NONE	NONE	CHANGE				
FTP Transfer Cont.		2.7.00_00_0	-	0012	2002			10:46:39.710355							
SD File Manager	9	ZPASS_DO_3	3	COIL	BOOL	0	-	10:46:39.710388	NONE	NONE	CHANGE				
Maintenance	10	ZPASS_DO_4	4	COIL	BOOL	0	-	07/12/2018 10:46:39.710603	NONE	NONE	CHANGE				
Ethernet Interfaces	11	TAG BIT 1	101	HOLDING	16BIT	0	FAIL		NONE	NONE	CHANGE				
FW Versions				HOLDING	16BIT				NONE	NONE					
FW Upgrade	12	TAG_BIT_2	102	REGISTER	UNSIGNED	0	FAIL		NONE	NONE	CHANGE				
Coni. Management	13	TAG_BIT_15	103	HOLDING	16BIT	0	FAIL		NONE	NONE	CHANGE	•			

C Z-PASS1)	× +									-		×
← → C ① No	on sicuro 1	192.168.85.103:80)80/mbgw	_tag_view.p	hp						☆ ル	G	E E
S SENECA Basic Configuration Summary Network and Services Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration VPN Configuration	Z-PASS1 Gateway Firmward MAC Add Internet Gateway Router: r	Tag View [user e Version: SW0 dress: C8F9811 Access: Ethern : running [Data running	r: admin] 03900_23 B0001 et Logger: 1	[logout] 2 running]									
Router Configuration		Det	a Logger:	START	STOP C		ACHE						
Users Configuration Shared Memory Tag Conf. TCP Servers		Pa	ge : 1/20	PREVIOU	S PAGE	NEXT F	PAGE						
Tag Setup								10/12/2018			0110105		
Tag View	8	ZPASS_DO_2	2	COIL	BOOL	0	-	15:50:55.432236	NONE	NONE	CHANGE		
Alarm Configuration	9	ZPASS_DO_3	3	COIL	BOOL	0	-	10/12/2018 15:50:55.432273	NONE	NONE	CHANGE	а.	
Alarm Summary	10	ZPASS_DO_4	4	COIL	BOOL	0	-	10/12/2018 15:50:55.432486	NONE	NONE	CHANGE		
Alarm History	11	TAG_BIT_1	101	HOLDING	16BIT	0	FAIL		NONE	NONE	CHANGE		
Phonebook	12	TAG BIT 2	102	HOLDING	16BIT	0	FAII		NONE	NONE	CHANGE		
Email Configuration	12		102	REGISTER HOLDING	UNSIGNED 16BIT	0	T/ME		NONE	NONE			
HTTP Configuration	13	TAG_BIT_15	103	REGISTER	UNSIGNED	0	FAIL		NONE	NONE	CHANGE		
Message Configuration	14	TAG_BIT_16	104	HOLDING	16BIT UNSIGNED	0	FAIL		NONE	NONE	CHANGE		
Data Logger (SD found) General Settings	15	ANALOG_S16	201	HOLDING REGISTER	16BIT SIGNED	110	ОК	10/12/2018 15:50:55.249550	ALARM HIGH	ALARM HIGH HIGH	CHANGE		
SD Transfer Conf.	16	ANALOG_FP32	202	HOLDING	32BIT REAL MSW	0	ОК	10/12/2018 15:50:55.249592	NONE	NONE	CHANGE		
FTP Transfer Conf.	17	TAG_BIT1_S	301	HOLDING	16BIT	0	FAIL		NONE	NONE	CHANGE		
Group Configuration	10		800	HOLDING	16BIT	0	EAU		NONE	NONE	CHANGE		
Maintenance	18	TAG_BIT2_S	302	REGISTER	UNSIGNED	U	FAIL		NONE	NONE	CHANGE		
Ethernet Interfaces	19	TAG_BIT16_S	303	REGISTER	UNSIGNED	0	FAIL		NONE	NONE	CHANGE		
FW Versions	20	TAG6	6	COIL	BOOL	0	FAIL		NONE	NONE	CHANGE		
FW Upgrade	21	TAG7	7	COIL	BOOL	0	FAIL		NONE	NONE	CHANGE		
Conr. Management	22	TAG8	8	COIL	BOOL	0	FAIL		NONE	NONE	CHANGE	-	

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



In the above figure²¹, 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.

	~									Giovanni		×
← → C	68.85.104:80)80/mbav	v tad set	up.php							<pre></pre>	<u>र</u> ु =
 ← → C □ 192.10 SENECA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade Tag Configuration 	A Content of the second	2-PASS2 ag Setup Version: 9 ess: C8F9 ccess: Eth ateway: rr sabled Nessun fil configuratio	v_tag_set SW00390 81020242 hernet unning e seleziona n Save	ato Im	dem: 1231 port tag conf configuration	B02SIM53	350E]				5	<u>کر</u>
Gateway Tag Setup	A	DD		MOD	IFY		DI	ELETE				
Gateway Tag View Mobile Configuration Mobile Network			Page : 1	/20 PRE	VIOUS PAG	E NEXT	PAGE					
	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	e - 1
	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:

Da 192.168.85.104:8080		
ZPASS_DO		
0		
	ОК	Annulla

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:

Da 192.168.85.104:8080	
Tag change failed !	
	ОК

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:

C Z-PASS2		×	+										_	X	
← → C () №	n sicu	uro 192.	168.85.1	03:8080/alarm_	_conf.php									☆ 0 :	
Sentecta Basic Configuration Summary Network and Services Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration	Z-P Ala Firi MA Inte Gat	Z-PASS2 Alarm Configuration [user: admin] [logout] Firmware Version: SW003900_251 [Modem: EC21EFAR02A03M4G] MAC Address: C8F9811B0001 [IMEI: 861108030033046] Internet Access: Ethernet Gateway: running [Data Logger: running] Router: disabled													
Router Configuration			DOM CS	2V Soorli	file Necoup file			EXPORT TO C	ev/						
Users Configuration				Stegn	MODIEY	SCIEZIOIId(O		DELETE							
Mobile Network		AU			MODIT			DELETE							
DDNS Configuration Shared Memory Tag Conf. TCP Servers	#	Enabled	Туре	Name	Тад	Activation Delay (s)	lgnore on Boot	Auto Acknowledge	Boolean Alarm Value	Alarm Low Value	Alarm High Value	Alarm Low Low Value	Alarm High High Value	Deadband Value	
Tag Setup	1	ON	Digital	ALR DIG 1	ZPASS DI 1	3	OFF	ON	HIGH			Value	Value		
Tag View	2	ON	Digital	ALR DIG 2	ZPASS DI 2	3	OFF	ON	HIGH						
Alarms	3	ON	Digital	ALB DIG 3	ZPASS DL 3	5	ON	OFF	LOW						
Alarm Contiguration	4	ON	Digital		ZPASS DL 4	5	ON	OFF	LOW						
Alarm Summary	5	ON	Analog		BADIUS1	0	OFF	ON	LOW	-50.0	50.0	-100.0	100.0	5.0	
Alarm History	6	ON	Analog		PADILISO	0	OFF	ON		-50.0	50.0	-100.0	100.0	5.0	
Logic Configuration	0	ON	Analog	ALN_ANA_2	RADIU82	U	OFF	ON		-50.0	50.0			5.0	
Phonebook CMC Configuration															
Swis Configuration															
Email Configuration															
HTTP Configuration															
Message Configuration															
Timer Configuration															
Rule Management															
General Settings															
SD Transfer Conf															
ETP Transfer Conf															
Group Configuration															
SD File Manager															
Maintenance															
Ethernet Interfaces															
FW Versions															
FW Upgrade															
Conf. Management															

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.

C Z-PASS1	× +		-	-		×
← → C ① No	n sicuro 192.168.85.103 :8080/alarm_conf_mod.php?id=0	Ţ	27	ょ	G	:
Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration VPN Configuration	Z-PASS1 Alarm Configuration [user: admin] [logout] Firmware Version: SW003900_240 MAC Address: C8F9811B0001 Internet Access: None Gateway: running [Data Logger: running] Router: running					
Router Configuration	CURRENT UPDATED					
Users Configuration Shared Memory Tag Conf.	Alarm Configuration					
TCP Servers	Enabled OFF OFF •					
Tag Setup	Type Digital Digital V					
Tag View	Name					
Alarm Configuration	Tag ZPASS_DI_1 •					
Alarm Summary	Activation Delay (s) 0 0					
Alarm History	Ignore on Boot OFF OFF ▼					
Logic Configuration	Auto Acknowledge ON ON V					
Phonebook	Boolean Alarm Value HIGH HIGH V					
Email Configuration	Alarm Low Value					
HTTP Configuration	Alarm High Value					
Message Configuration						
Rule Configuration	Alarm Low Low Value					
General Settings	Alarm High High Value					
SD Transfer Conf.	Deadband Value 0 0					
FTP Transfer Conf.	APPLY					
Group Configuration						
SD File Manager						
Maintenance						
Ethernet Interfaces						
FW Versions						
FW Upgrade						
Conf. Management						

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
Туре	This parameter tells if this is a Digital	Digital
	or Analog alarm; when changing the	

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

-

	goes under this value, the danger	
	alarm condition is entered	
Alarm High High Value	For an Analog alarm, this parameter	Empty
	defines the high danger alarm	
	threshold that is, when the tag value	
	goes over this value, the danger	
	alarm condition is entered	
Deadband Value	This parameter defines a non	0
	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	

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.

🗅 Z-PASS1		×	+										-		×
← → C ① Nor	n sic	uro 192	.168.85.1(03:8080/alarm_co	nf.php							\$	2	G	:
SENECA® Basic Configuration Summary Network and Services Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration VPN Configuration	Z-F Ale Fir MA Int Ga Ro	Z-PASS1 Alarm Configuration [user: admin] [logout] Firmware Version: SW003900_240 MAC Address: C8F9811B0001 Internet Access: None Gateway: running [Data Logger: running] Router: running													
Router Configuration		AD	D	Ν	MODIFY		DEL	ETE							
Users Configuration Shared Memory Tag Conf. TCP Servers Tag Setup Tag View	#	Enabled	Турө	Name	Тад	Activation Delay (s)	lgnore on Boot	Auto Acknowledge	Boolean Alarm Value	Alarm Low Value	Alarm High Value	Alarm Low Low Value	Alarm High High Value	Deadba Valu	and e
Alarms	1	ON	Digital	Alarm_RCD	ZPASS_DI_1	5	ON	OFF	HIGH						
Alarm Configuration	2	OFF	Digital	Alarm_Bit16	TAG_BIT_16	1	ON	ON	LOW						
Alarm Summary	3	ON	Analog	Alarm_S16	ANALOG_S16	3	ON	ON		-50.0	50.0	-100.0	100.0	5.0	
Alarm History	4	ON	Analog	Alarm_FP32	ANALOG_FP32	1	OFF	ON		-2.5	2.5	-5.0	5.0	0.5	
Logic Configuration	5	OFF	Digital	Alarm_Bit2	TAG_BIT_2	1	ON	ON	LOW						
Phonebook	6	OFF	Digital	Alarm_Bit1	TAG_BIT_1	1	ON	ON	LOW						
Email Configuration	7	ON	Digital	Alarm Bit1 S	TAG BIT1 S	0	ON	ON	LOW						
HTTP Configuration	8	ON	Digital	Alarm Bit2 S	TAG BIT2 S	0	ON	ON	LOW						
Message Configuration	g	ON	Digital	Alarm Bit16 S	TAG BIT16 S	0	ON	ON	LOW						
Rule Configuration	0		Digital	Alaim_bitro_o	IAd_birito_o	U U		011	2011						
Data Logger (SD found)															
General Settings															
SD Transfer Cont.															
FTP Transfer Conf.															
Group Configuration															
SD File Manager															
Maintenance															
EW Versions															
Fw versions															
Carl Management															

🗋 Z-PASS1	× +					-		×
← → C ① No	n sicuro 192.168.85.103:8080/alarm_conf_mo	d.php?id=8			☆	ん	G	:
SENECA Basic Configuration Summary Network and Services Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration	Z-PASS1 Alarm Configuration [user: admin] [logou Firmware Version: SW003900_240 MAC Address: C8F9811B0001 Internet Access: None Gateway: running [Data Logger: running] Router: running	t]						
VPN Configuration		CURRENT						
Router Configuration		CURRENT	UPDATED					
Osers Configuration	Alarm Configuration							
TCP Servers	Enabled	ON	ON V					
Tag Setup	Туре	Analog	Analog V					
Tag View	Name	Alarm FD32	Alarm EP32					
Alarms	T							
Alarm Configuration	lag	ANALOG_FP32	ANALOG_FP32 V					
Alarm Summary	Activation Delay (s)	1	1					
Alarm History	Ignore on Boot	OFF	OFF V					
Logic Configuration	Auto Acknowledge	ON	ON 🔻					
Phonebook	Boolean Alarm Value	HIGH	HIGH 🔻					
Email Configuration	Alarm Low Value	-2.5	-2.5					
HTTP Configuration	Alarm High Value	2.5	2.5					
Message Configuration	Alarm Low Value	5.0	5.0					
Rule Configuration	Alami Low Low Value	-0.0	-5.0					
General Settings	Alarm High High Value	5.0	5.0					
SD Transfer Conf.	Deadband Value	0.5	0.5					
FTP Transfer Conf.	APPLY							
Group Configuration								
SD File Manager								
Maintenance								
Ethernet Interfaces								
FW Versions								
FW Upgrade								
Conf. Management								

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	The analog tag has got a value that is under the one defined by "Alarm Low Low
	Alarm	Value" parameter

Alarm High High	Analog Danger	The analog tag has got a value that is over the one defined by "Alarm High High
	Alarm	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* \rightarrow Return \rightarrow <acknowledgement> \rightarrow End if "Auto Acknowledge"=OFF
 - 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, <u>when importing the alarm configuration from a .csv file, the previously existing alarms are</u> <u>deleted</u>; 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

Alarm* \rightarrow End

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

🗅 Z-PASS1	×	+								-		×
← → C () N	on sicuro 192.16	58.85.103:8080/alarm_	summary.p	hp					☆	r	G	1
Sentectal 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	Z-PASS1 Alarm Summa Firmware Ver MAC Address Internet Accea Gateway: runn Router: runnin	ary [user: admin] [lo sion: SW003900_24 o: C8F9811B0001 ss: None ning [Data Logger: n ng	gout] 0 running] ACKNO)	NLEDGE]							
TCP Servers	# Name	Tag Name	Level	Status	Timestamp	Status	Timestamp					
Tag View Alarms Alarm Configuration Alarm Configuration Alarm History Logic Configuration Phonebook Email Configuration HTTP Configuration Message Configuration Message Configuration Bata Logger (SD found) General Settings SD Transfer Conf. FTP Transfer Conf. FTP Transfer Conf. Group Configuration SD File Manager Maintenance Ethemet Interfaces FW Upgrade Conf. Management	1 Alarm_R	CD ZPASS_DI_1	Alarm	Alarm	2018/12/07 10:46:34	None						

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
	"Alarm" or "Analog Danger Alarm" for analog alarms
Status On	The alarm status when the alarm has been generated:
	always "Alarm" for digital alarms
	"Alarm Low" or "Alarm High" for analog alarms with Level = "Alarm"
	"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
	It may evolve in:
	"Acknowledged", if the alarm has been acknowledged when in the alarm
	state
	"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.

🗋 Z-PASS1	× +								-		×
← → C ① No	on sicuro 192.168.85.1	103:8080/alarm_s	ummary.php					☆	r	G	0
Serial Ports Basic Configuration Summary Network and Services Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration Router Configuration Network and Services Stared Memory Tag Conf. TCP Servers Tag Setup Tag View Alarms Alarm Configuration Alarm Summary Alarm History Logic Configuration Phonebook Email Configuration HTTP Configuration Rule Configuration Rule Configuration Rule Configuration Rule Configuration Bata Logger (SD found) General Settings SD Transfer Conf. FTP Transfer Conf. Group Configuration SD File Manager Maintenance Ethernet Interfaces FW Versions	Z-PASS1 Alarm Summary [u Firmware Version: MAC Address: C8F Internet Access: N Gateway: running Router: running # Name 1 Alarm_RCD Z	Tag Name L TAG Name L TAG Name L TAG Name L	gout] unning] ACKNOWLE .evel Status On Jarm Alarm	EDGE Timestamp 0n 2018/12/07 10:46:34	Status Action Acknowledge	Timestamp Action 2018/12/07 11:44:38		X			
In attesa di risposta da 192.16	8.85.103										

20.4.3 Alarm History

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

← → C ③ Non sicuro 192.168.85.103:8080/alarm_history.php	☆	ス	
SERVECA Z-PASS1 Alarm History [user: admin] [logout] Summary Firmware Version: SW003900_240 Network and Services MAC Address: C8F9811B0001 Serial Ports Internet Access: None Real Time Clock Setup Gateway: running [Data Logger: running] Gateway Configuration Router: running VPN Configuration Router: running			
Users Configuration CLEAN HISTORY EXPORT TO CSV			
Shared Memory Tag Cont. TCP Servers # Name Tag Name Tag Value Status Level Timestamp			
Tag Setup 1 Alarm PCD 7PASS DI 1 0 End Alarm 2018/12/07			
Tag View 1 Alami_RCD ZFA35_DI_T 0 End Alami 11:54:20			
Alarms 2 Alarm_RCD ZPASS_DI_1 1 Acknowledge Alarm 2018/12/07			
Alarm Summary 3 Alarm_RCD ZPASS_DI_1 1 Alarm Alarm 10.46:34			
Alarm History 10.4004 Logic Configuration 4 Alarm_Bit2_S TAG_BIT2_S 1 End Alarm 07.19:29			
Email Configuration 5 Alarm_Bit16_S TAG_BIT16_S 1 End Alarm 2018/11/26 07:10:20			
HTTP Configuration 6 Alarm Bit2 S TAG BIT2 S 0 Alarm Alarm 2018/11/26			
Rule Configuration 07:19:02			
Data Logger (\$D found) 7 Alarm_Bit1_S TAG_BIT1_S 1 End Alarm 2018/11/26 07:19:00			
General Settings 8 Alarm_Bit16_S TAG_BIT16_S 0 Alarm 2018/11/26 SD Transfer Conf. 8 Alarm_Bit16_S TAG_BIT16_S 0 Alarm Alarm 2018/11/26			
FTP Transfer Conf. 9 Alarm_Bit1_S TAG_BIT1_S 0 Alarm Alarm 2018/11/26			
Group Contiguration 07:16:49 SD File Manager 10 Alarm Bit2 S TAG BIT2 S 1 End Alarm 2018/11/26			
Maintenance 07:18:40			
FW Versions 11 Alarm_Bit1_S TAG_BIT1_S 1 End Alarm 07:18:31			
FW Upgrade 12 Alarm_Bit16_S TAG_BIT16_S 1 End Alarm 2018/11/26 07:18:27			
Conf. Management 13 Alarm_Bit2_S TAG_BIT2_S 0 Alarm Alarm 2018/11/26			
14 Alarm Bit1 S TAG BIT1 S 0 Alarm Alarm 2018/11/26			
15 Alarm Bitte S TAG BITte S 0 Alarm Alarm 2018/11/26			
16 Alarm Bitt S TAG BITt S 4 End Alarm 2018/11/26			

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:

C Z-PASS2	× +		-		×
← → C ③ N	on sicuro 192.168.85.105:8080/datalog_transf_conf.php?prot=0	☆	ょ	G	0
Passe ← → C ○ N Second paration Summary N Basic Configuration Summary N Network and Services Serial Ports Real Time Clock Setup Gateway Configuration Real Time Clock Setup Gateway Configuration N VPN Configuration N N Mobile Configuration Mobile Configuration N Shared Memory Tag Configuration Shared Memory Tag Configuration N Tag Setup Tag Configuration N N Alarms Alarm Summary Alarm Summary N Alarm Summary Logic Configuration N N Phonebook SMS Configuration N N SMS Configuration Email Configuration N N HTTP Configuration N N N N Rule Configuration N N N	x + n sicure 192.168.85.105:8080/datalog_transf_conf.php?prot=0 Z-PASS2 Transfer Configuration [user: admin] [logout] Firmware Version: SW003900_240 [Modem: 1231B02SIM5350E] MAC Address: C8F981160043 [IMEI: 862264020406335] Internet Access: Ethernet Gateway: running [Data Logger: running (no group enabled)] Router: disabled SD Configuration N Wat After Failure Counter 10 10 Wat After Failure (minutes) 16 SD Clean Period (days) 30 30 30	<u>★</u>)			× 0

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	OFF
	SD Card or not	
Max Failure Counter	This parameter defines the maximum	10
	number of failed copy attempts before	
	entering the "Wait after failure" status	

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

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:

🗋 Z-PASS2	× +			-		×
← → C ③ Nor	n sicuro 192.168.85.105:8080/d	latalog_transf_conf.ph	p?prot=1	\$ よ	G	0
SENECA®	Z-PASS2	r: admin] [logout]				
Basic Configuration	Transier Configuration [use	r. admini [logoul]				
Network and Services	Firmware Version: SW00390	0_240 [Modem: 123	1B02SIM5350E]			
Reviel Deste	MAC Address: C8F98116004	13 [IMEI: 862264020	406335]			
Beel Time Oleah Ostur	Internet Access: Ethernet					
Gateway Configuration	Gateway: running [Data Log	ger: running (no gr	oup enabled)]			
VPN Configuration	Poutor: disabled					
Router Configuration				 		
Users Configuration		CURRENT	UPDATED			
Mobile Configuration						
Mobile Network	FTP Configuration					
DDNS Configuration	Enable	ON	ON V			
Shared Memory Tag Conf.	Max Failure Counter	10	10			
TCP Servers	Wait After Failure (minutes)	15	15			
Tag Setup	Crypto Mode	None	None			
Tag View		fter detelerence it	ftn datalaggar it			
Alarm Configuration	nosi	np.uatalogger.n				
Alarm Summary	Port	21	21			
Alarm History	Username	myuser	myuser			
Logic Configuration	Password	mypass	mypass			
Phonebook	Path	/ZPASS2/DataLogger/	/ZPASS2/DataLogger/			
SMS Configuration	APPLY					
Email Configuration						
HTTP Configuration						
Message Configuration						
Rule Configuration						
Data Logger (SD missing)						
General Settings						
SD Transfer Conf.						
FTP Transfer Conf.						
Group Configuration						
Maintenance Ethernet Interfesse						
Ethemet Intenaces						
FW Llograde						
Conf. Management						

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	OFF
	FTP or not	
Max Failure Counter	This parameter defines the maximum	10
	number of failed transfer attempts	
	before entering the "Wait after failure"	

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

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:

C Z-PASS2	× +		-	
\leftrightarrow \rightarrow C \odot No	n sicuro 192.168.85.105:8080/da	talog_transf_conf.php?prot=2	☆ <u>}</u>	60
SFNFCA [®]	Z-PASS2			
Basic Configuration	Transfer Configuration [user:	admin] [logout]		
Summary	Eirmware Vareion, SW002000	940 [Modern: 1991D026]M5250E1		
Network and Services	Firmware version: Sw003900	_240 [modem: 1231B0281M0330E]		
Sarial Parta	MAC Address: C8F981160043	3 [IMEI: 862264020406335]		
Beal Time Cleak Setur	Internet Access: Ethernet			
Ostavan Osafiavastias	Geteway: rupping [Dete Logg	er: running (no group engbled)]		
Gateway Configuration	Clateway. Turning [Data Logg	er. running (no group enabled)]		
VPN Configuration	Router: disabled			
Router Configuration				
Users Configuration	CURRENT	UPDATED		
Mobile Configuration	Email			
DDNO Configuration	Configuration			
Shared Memory Tag Conf	Enable			
TCP Servers	only for Data ON	ON V		
Tag Setup	Logger			
Tag View	Max Failure	10		
Alarms	Wait After			
Alarm Configuration	Failure 15	15		
Alarm Summary	(minutes)			
Alarm History	Crypto Mode STARTTLS	STARTTLS V		
Logic Configuration	Host posta.datalogger.it	posta.datalogger.it		
Phonebook	Port 587	587		
SMS Configuration	Unamental museus	myunor		
Email Configuration	Username myuser	IIIyusei		
HTTP Configuration	Password mypass	mypass		
Message Configuration	From			
Rule Configuration	email zpass@datalogger.i	it zpass@datalogger.it		
Data Logger (SD missing)	To			
General Settings	one or more			
SD Transfer Conf.	email			
FTP Transfer Conf.	addresses, myuser@seneca.it	myuser@seneca.it		
Group Configuration	commas			
Maintenance	only for Data			
Ethernet Interfaces	Logger			
FW Versions	Subject Disk of T			
FW Upgrade	only for Data Log from 2- PASS2	Data Log from Z-PASS2		
Conf. Management	Logger			
	Text only for Data			
	Logger			
	APPLY			

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

-

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	10
	maximum number of failed	
	attempts before entering the "Wait	
	after failure" status (see next field)	
Wait After Failure (minutes)	This parameter defines the duration,	15
	in minutes, of the "Wait after	
	failure" status.	
	In this status, no further attempt to	
	send a log sample via HTTP POST	
	request is performed	
Crypto Mode	This parameter defines the	ON
	encryption mode of the HTTP	
	connection.	
	Possible modes are:	
	- OFF (HTTP)	
	- ON (HTTPS)	
Host	Hostname (FQDN) or IP address of	192.168.90.1
	the HTTP server	
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		CURRENT	UPDATED
OPC-UA Server Conf.	MQTT		
Users Configuration	Configuration		
Mobile Configuration			
Mobile Network	NOTE:		
DDNS Configuration	Log Publish Period	d is given by "Da	ata Logger/Group 1/Sampling Period" parameter
Shared Memory Tag Conf.	(see page "Data Lo	ogger/Group Co	nfiguration").
TCP Servers	Enable	ON	ON V
Tag Setup	Max Failure Counter	3	3
Tao View	Wait After	15	15
Alarms	Failure (minutes)	7 PASS MOTT	
Alarm Configuration	Client ID	Client	Z-PASS MQTT Client
Alarm Summary	Broker Host	188.10.245.254	188.10.245.254
Alarm History	Broker Port	1883	1883
Client Protocols	Keep Alive		
SD Transfer Conf.	Interval 2 (seconds)	20	20
FTP Configuration	Clean Session (ON	ON T
Email Configuration	Message Retain (OFF	OFF
HTTP Configuration	Quality of	0-84	
MQTT Configuration	Service	Q05 I	
Logic Configuration	Authentication (OFF	OFF Y
Phonebook	Username u	user	user
SMS Configuration	Password 1	123456	123456
Message Configuration	SSL/TLS	OFF	OFF T
Timer Configuration	Log on change (ON	ON T
Rule Management	Publish with	OFF	OFF T
Data Logger (SD found)	Publish Topic for		
General Settings	Logs	seneca/%e/data	seneca/%e/data
Group Configuration	{	{"type": "data", "message":	
SD File Manager	Publish Payload {	{"device": %jc,	{"type": "data". "message": {"device": %ic. "date": %id. "name"
Maintenance	for Logs	"date": %jd, "name": %jn,	
Ethernet Interfaces		"value": %v}}	
FW Versions	Publish Bulk { Format	{"name": %jn, "value": %v}	{"name": %jn, "value": %v}
FW Upgrade	Publish Topic for Alarms	seneca/%e/data	seneca/%e/data
Conf. Management	Publish Payload {	{"tms": %t, "msq": %ix}	{"tms": %t, "msg": %ijx}
	Subscribe Topic	seneca/%e/info	seneca/%e/info
	LWT Tania		
	LWT Pauload		
	Livi Fayload		
	Configuration		
	Load		
	Configuration URL		
	FW Update URL		
	APPLY		
			MOTT Certificates
			CA Certificate File
			(.crt) Scegli file Nessun file selezionato
		С	lient Certificate File Scegli file Nessun file selezionato
			Client Key File 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	OFF
	sent/receive via MQTT protocol or	
	not	
Max Failure Counter	This parameter defines the	3
	maximum number of failed attempts	
	before entering the "Wait after	
	failure" status (see next field)	
Wait After Failure (minutes)	This parameter defines the duration,	15
	in minutes, of the "Wait after	
	failure" status.	
	In this status, no further attempt to	
	send or receive MQTT data is	
	performed	
Client ID	This parameter defines the Client ID	Z-PASS MQTT Client
	used in the MQTT protocol	
Broker Host	This parameter defines the Broker	192.168.90.1
	Host name or address	
Broker Port	This parameter defines the Broker	1883
	Port	
Keep Alive Interval (seconds)	This parameter defines the Keep	20
	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	
Clean Session	This parameter defines the clean	ON
	session.	
	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	

	information -	nd massages that are			
	information a	nd messages that are			
	queued from	a previous persistent			
	session are los	t.			
Message Retain	This paramete	er defines the message	OFF		
	retain. Norm	ally if a publisher			
	publishes a m	essage to a topic, and			
	no one is sul	oscribed to that topic			
	the message	is simply discarded by			
	the broker. H	owever the publisher			
	can tell the b	roker to keep the last			
	message on	that topic by setting			
	theretained message flag				
Quality of service	This paramete	r defines the quality of	0051		
	convice for the	MOTT protocol	0031		
	Service for the	wight protocol.			
	QUS 0 (only or	ice, without ack)			
	QUS 1 (At Leas	st Once, with ack)			
	QOS 2 (Only	Once, with ack and			
	resend)				
Authentication	This parameter defines if must be		OFF		
	used the	authentication with			
	user/password	for access to the			
	broker				
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		OFF		
	communicatio	n is encrypted with			
	SSL/TLS				
Log on Change	This parameter defines if topics must		ON		
	be sent only o	n change (according to			
	minimum datalog time) or not				
Publish with multiple tags	This paramete	r defines if the nublish	ON		
	contains multiple tags				
	dovico must s	and a publich for each			
	device must send a publish for each				
Publish Topic for Logs	Select the top	nc name for logs data	seneca/%c/data		
	using the following legenda:				
	%с	Z-PASS Client ID			
	%m	Z-PASS MAC Address			
	%e	Z-PASS IMEI			

	0/ d	date-time	
	700		
	%t	seconds since the "epoch")	
	%x	text (only in "Publish Payload for Alarms")	
	%b	bulk (format specified in "Publish Bulk Format" parameter)	
	%n	tag name (only in "Publish Bulk Format")	
	%v	tag value (only in "Publish Bulk Format")	
	%i	tag validity flag (only in "Publish Bulk Format")	
	%j[field]	print [field] as a JSON string	
	%\$tag_name\$	value of tag "tag_name"	
	%#tag_name#	validity flag of tag "tag_name"	
Publish Payload for Logs	Select the form	nat that must be used	{"type": "data", "message":
	for the publ	ish payload in Json	{"device": %jc, "date": %jd,
	format using th	ne following legenda:	"name": %jn, "value": %v}}
	%с	Z-PASS Client ID	
	%m	Z-PASS MAC Address	
	%е	Z-PASS IMEI	
	%d		
	, o a	date-time	
	%t	date-time timestamp (number of seconds since the "epoch")	
	%t %x	date-time timestamp (number of seconds since the "epoch") text (only in "Publish Payload for Alarms")	
	%t %x %b	date-time timestamp (number of seconds since the "epoch") text (only in "Publish Payload for Alarms") bulk (format specified in "Publish Bulk Format" parameter)	
	%t %x %b %n	date-time timestamp (number of seconds since the "epoch") text (only in "Publish Payload for Alarms") bulk (format specified in "Publish Bulk Format" parameter) tag name (only in "Publish Bulk Format")	
	%t %x %b %n %v	date-time timestamp (number of seconds since the "epoch") text (only in "Publish Payload for Alarms") bulk (format specified in "Publish Bulk Format" parameter) tag name (only in "Publish Bulk Format") tag value (only in "Publish Bulk Format")	
	%t %x %b %n %v %i	date-time timestamp (number of seconds since the "epoch") text (only in "Publish Payload for Alarms") bulk (format specified in "Publish Bulk Format" parameter) tag name (only in "Publish Bulk Format") tag value (only in "Publish Bulk Format") tag validity flag (only in "Publish Bulk Format")	
	%t %x %b %n %v %i %j[field]	date-time timestamp (number of seconds since the "epoch") text (only in "Publish Payload for Alarms") bulk (format specified in "Publish Bulk Format" parameter) tag name (only in "Publish Bulk Format") tag value (only in "Publish Bulk Format") tag validity flag (only in "Publish Bulk Format") print [field] as a JSON string	
	%t %x %b %n %v %i %j[field] %\$tag_name\$	date-time timestamp (number of seconds since the "epoch") text (only in "Publish Payload for Alarms") bulk (format specified in "Publish Bulk Format" parameter) tag name (only in "Publish Bulk Format") tag value (only in "Publish Bulk Format") tag validity flag (only in "Publish Bulk Format") print [field] as a JSON string value of tag "tag_name"	

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

		"Publish Bulk Format")	
	%j[field]	print [field] as a JSON string	
	%\$tag_name\$	value of tag "tag_name"	
	%#tag_name#	validity flag of tag "tag_name"	
Subscribe Topic	Select the sub	scribe topic using the	seneca/%c/info
	following legenda:		
	%с	Z-PASS Client ID	
	%m	Z-PASS MAC Address	
	%e	Z-PASS IMEI	
	%d	date-time	
	%t	timestamp (number of seconds since the "epoch")	
	%x	text (only in "Publish Payload for Alarms")	
	%b	bulk (format specified in "Publish Bulk Format" parameter)	
	%n	tag name (only in "Publish Bulk Format")	
	%v	tag value (only in "Publish Bulk Format")	
	%i	tag validity flag (only in "Publish Bulk Format")	
	%j[field]	print [field] as a JSON string	
	%\$tag_name\$	value of tag "tag_name"	
	%#tag_name#	validity flag of tag "tag_name"	
LWT Topic	Select the Last	t Weel and Testament	-
	topic using the following legenda:		
	%с	Z-PASS Client ID	
	%m	Z-PASS MAC Address	
	%e	Z-PASS IMEI	
	%d	date-time	
	%t	timestamp (number of seconds since the "epoch")	
	%x	text (only in "Publish Payload for Alarms")	
	%b	bulk (format specified in "Publish Bulk Format" parameter)	
------------------------	-------------------	--	---
	%n	tag name (only in "Publish Bulk Format")	
	%v	tag value (only in "Publish Bulk Format")	
	%i	tag validity flag (only in "Publish Bulk Format")	
	%j[field]	print [field] as a JSON string	
	%\$tag_name\$	value of tag "tag_name"	
	%#tag_name#	validity flag of tag "tag_name"	
LWT Payload	Select the Last	t 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	^r the "FW Update"	
	command rece	eived from MQTT	
Sleep Timeout	Wake-up time	of the MQTT task, the	
	shorter it is, th	e more reactive MQTT	
	is (at the exp	ense of a higher cpu	
	load)		
MQTT Certificates	Used for load	I the certificates that	
	can be used	d with the SSL/TLS	
	encryption.		

20.5.5.1 MQTT Example configuration for Databoom.com

MQTT Configuration		
NOTE: Log Publish Pe (see page "Dat	eriod is given by "Data Logger/Group 1/Sampling Period" Logger/Group Configuration").	' parameter
Enable	ON	ON V
Max Failure Counter	3	3
Wait After Failure (minutes)	15	15
Client ID	q)	q
Broker Host	mqtt.databoom.com	mqtt.databoom.com
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 V
Authentication	ON	ON V
Username	m	ma
Password	2	z.
SSL/TLS	ON	ON V
Log on change	OFF	OFF DATABOOM TOKEN
Publish with multiple tags	ON	ON V
Publish Topic for Logs	seneca/(<mark>data</mark> /data	seneca/
Publish Payload for Logs	{"type": "data", "message": {"device": "0, ", ", "date": %jd, "signals": [%b]}}	{"type": "data", "message": {"device": "0
Publish Bulk Format	{"name": %jn, "value": %v}	{"name": %jn, "value": %v}
Publish Topic for Alarms	seneca/0gp5znft4q/data	seneca/0gp5znft4q/data
Publish Payload for Alarms	{"tms": %t, "msg": %jx}	{"tms": %t, "msg": %jx}
Subscribe Topic	seneca/	seneca/
LW/T Topic		

Then you must add the Databoom certificates.

20.5.5.2 MQTT Example configuration for Amazon AWS

IIIICIIICI AUUCSS, LUICIIICI

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

Router: running

	CURRENT	UPDATED
MQTT Configuration		
NOTE:		
Log Publish Pe	riod is given by "Data Logger/Group 1/Samplin	g Period" parameter
(see page "Data	a Logger/Group Configuration*).	
Enable	ON	ON V
Max Failure Counter	3	3
Wait After Failure (minutes)	15	15
Client ID	Any	Any
Broker Host	nazonaws.com	a. azonaws.
Broker Port	8883	8883
Keep Alive Interval (seconds)	20	20
Clean Session	ON	ON V
Message Retain	OFF	OFF T
Quality of Service	QoS 1	QoS 1 V
Authentication	ON	ON V
Username		
Password	i	
SSL/TLS	ON	ON V
Log on change	OFF	OFF T
Publish with multiple tags	ON	ON T
Publish Topic for Logs	<pre>\$aws/things/ZUMTS/shadow/update</pre>	Saws/things/ZUMTS/shadow/update
Publish Payload for Logs	{"state": {"reported": {"ZPASS_DI": %\$ZPASS_DI\$, "ZPASS_DO": %\$ZPASS_DO\$}}, "clientToken": "a	{"state": {"reported": {"ZPASS_DI": %\$ZPASS_DI\$, "ZPAS
Publish Bulk Format	\$aws/things/ZUMTS/shadow/update/accepted	Saws/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	Saws/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		

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:	user
	- "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	

	commands to the device; it also	
	receives all SMS/EMAIL alarms	
	- "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	
	- "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	Empty
	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.	
	The value 0 corresponds to "All	
	Message Groups"	
Phone Number	Phone Number in "international	Empty
	format"; the initial '+' character shall	
	be present	
Email Address	Email Address, used as a recipient	Empty
	for alarms sent via Email	

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.

C Z-PASS1	× +		-		×
\leftrightarrow \rightarrow X (i) No	n sicuro 192.168.85.103:8080/phonebook_save.php?act=save&id=0	☆	۶	G	0
SENECA®	Z-PASS1				
Basic Configuration	Phonebook [user: admin] [logout]				
Summary	Firmware Version: SW003900, 240				
Network and Services	MAC Address: C8F9811B0001				
Serial Ports	Internet Access: Ethernet				
Digital I/O Configuration					
Real Time Clock Setup	Gateway: running [Data Logger: running]				
Gateway Configuration	Router: running				
VPN Configuration					
Router Configuration					
Users Configuration					
Shared Memory Tag Conf.	Number already present ! Phonebook User not added.				
TCP Servers					
Tag Setup					
Tag View					
Alarms					
Alarm Configuration					
Alarm Summary					
Alarm History					
Logic Configuration					
Email Configuration					
UTTD Configuration					
HTTP Configuration					
Message Configuration					
Rule Configuration					
General Settings					
SD Transfer Conf					
ETP Transfer Conf					
Group Configuration					
OD Ella Managari					
Maintenance					
Ethernet Interfaces					
FW Versions					
EW Llograde					
Conf Management					

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.



C Z-PASS1	× +		-		×
\leftrightarrow \rightarrow C \odot No	n sicuro 192.168.85.103:8080/phonebook_mod.php?id=10	☆	ょ	G	0
 ▲ 2-PASS1 ← → C () No ♦ SENECA® Basic Configuration Summary Network and Services Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration VPN Configuration VPN Configuration VPN Configuration Users 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 	× + n sicuro 192.168.85.103:8080/phonebook_mod.php?id=10 Z-PASS1 Phonebook [user: admin] [logout] Firmware Version: SW003900_240 MAC Address: C8F9811B0001 Internet Access: Ethernet Gateway: running [Data Logger: running] Router: running Message Group NOTE: 0 means "all groups" you can insert multiple group NOTE: 0 means "all groups" solaracter Phone Number +390123456789 admin@seneca.it APPLY				0
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					

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, <u>when importing the Phonebook from a .csv file, the previous Phonebook contents are</u> <u>deleted</u>; 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	ON
	commands functionality	

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

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:

🗅 z-PASS2 🗙 +		×
← → C (③ Non sicuro 192.168.85.103:8080/msg_conf.php	☆ 0	:
SENECA® Z-PASS2 Basic Configuration Kessage Configuration [user: admin] [logout] Summary Firmware Version: SW003900_251 [Modem: EC21EFAR02A03M4G] Network and Services MAC Address: C8F9811B0001 [IMEI: 861108030033046] Serial Ports Internet Access: Ethernet Digital I/O Configuration Gateway: running [Data Logger: running]		
Gateway Configuration Router: disabled		
VPN Configuration Router Configuration Users Configuration IMPORT FROM CSV Mobile Configuration ADD Mobile Network MODIFY		
DDNS Configuration # Id Text		
Shared Memory Tag Conf. 1 1 Digital Input 2: (ZPASS_DL_2) TCP Servers 2 2 Analog Alarm: (RADIUS1) Tag Selup 3 3 Ecoo l'allarme su 3 tag: (RADIUS1-(RADIUS2)-(ZPASS_DL_2)) Tag View 4 Alarm on Digital Input 1 -> OK ((ZPASS_DL_1)) Alarms 5 5 Alarm on Digital Input 1 -> OK ((ZPASS_DL_2)) Alarm Configuration 6 6 Alarm on Digital Input 2 -> ON ((ZPASS_DL_2)) Alarm Hetry 7 7 Alarm on Digital Input 2 -> OK ((ZPASS_DL_2)) Logic Configuration Final Configuration Final Configuration Phonebook SMS Configuration Final Configuration HTTP Configuration Final Configuration Final Configuration HTTP Configuration Final Configuration Final Configuration Rule Management Dota Logger (8D found) General Settinge SD Fine Manager SD Fine Manager Final F		
FW Upgrade Conf. Management		

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, <u>the syntax {TAG} will be replaced</u>, in the text, with the current value <u>of the "TAG" tag</u>. 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		×	+	-	I		×
← → C ③ No	n sicuro	192.1	68.85.103:8080/msg_conf.php	\$	k.,	G	0
SENECA®	Z-PAS	S1		 			
Basic Configuration	Мезза	nge Cor	figuration [user: admin] [logout]				
Summary	Firmw	are Ve	aion: SW003900_240				
Network and Services			- 005004400004				
Serial Ports	MAG	Addres	8: C9F9811B0001				
Digital I/O Configuration	Intern	et Acce	ss: Ethernet				
Real Time Clock Setup	Gatew	ay: run	ning [Data Logger: running]				
Gateway Configuration	Route	r: runni	ing				
VPN Configuration							
Router Configuration							
Users Configuration		ADD	MODIFY DELETE				
Shared Memory Tag Conf.			_				
TCP Servers	#	ld	Text				
Tag Setup	1	1	Allarme Remote Connection Disable -> ON				
Tag View	2	2	Allarme Remote Connection Disable -> OFF				
Alarms	3	3	Allarme Bit16={TAG_BIT_16}				
Alarm Configuration	4	4	Allarme Bit16={TAG_BIT_16}, val={ANALOG_FP32}				
Alarm Summary	5	5	Allarme Bit1={TAG_BIT_1}, Bit2={TAG_BIT_2}, Bit16={TAG_BIT_16}				
Alarm History	6	6	Alarm on tag FP32 ON val={ANALOG_FP32}				
Logic Configuration	7	7	Alarm on tag FP32 OFF val={ANALOG_FP32}				
Phonebook	8	8	Danger on tag FP32 ON val={ANALOG_FP32}				
Email Configuration	9	9	Danger on tag FP32 OFF val={ANALOG_FP32}				
HTTP Configuration	10	10	Alarm BIT1 S={TAG BIT1 S}				
Message Configuration	11	11	Alarm BIT2 S={TAG_BIT2_S}				
Rule Configuration	12	12	Alarm BIT16 S={TAG BIT16 S}				
Data Logger (SD found)	13	13	Alarm ACTIVE on tag S16=(ANALOG_S16)				
General Settings	14	14	Alarm INACTIVE on tag S16-(ANALOG, S16)				
SD Transfer Conf.	14	14					
FTP Transfer Conf.							
Group Configuration							
SD File Manager							
Maintenance							
Ethernet Interfaces							
FW Versions							
FW Upgrade							
Conf. Management							



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.

	CURRENT	UPDATED
Timer Configuration		
Id	1	1
Enabled	ON	ON 🔻
Duration (ms)	60000	60000
APPLY		

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].

	ADD	MODIFY	DELETE
#	ld	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):

				CI	URRENT		UPDATED										
R	ULE GE	NERAL	CONFIGURATION														
			Writing Mode	After exec	ution	After	execution •										
APPLY	1																
			RULE STATUS														
			Run Status		1	RUN	INING										
			Cycle Time (ms))											
-				1													
	R	ule Mai	nagement		ADD		MODIFY		COPY	MOVE	DELE	TE	DELETE ALL				
		Rule D	ebugger				SET/RESET	BREA	KPOINT		PLAY		SHOW TAGS				
						_		_									
# Ena	abled	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 =			Oulculate		RADIUS1 >					CIRCUMEERENCE			CIRCUMEERENCE				2
1	NC NC	1	Biggest	1000	RADIUS2	OR		OR		= RADIUS1 * 6.28			- KADIUS2 * 6.28			FALSE	
H			Calculate		RADIUS1 >					AREA sor	AREA =		AREA sor	AREA -			
2	211	2	Biggest Area	1000	RADIUS2	OR		OR		RADIUS1	AREA * 3.14		RADIUS2	AREA * 3.14		FALSE	- 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	TDUIE	TDUIE	TDUIS	TDUIS
TRUE	IRUE	IRUE	IRUE	IRUE

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:

Z-PASS2								
Rule Configuration [user: admin] [logout]								
Firmware Version: SW003900_250								
MAC Address: C8F9811B0001								
Internet Access: Ethernet								
Gateway: running [Data Logger: ru	nning]							
Router: disabled								
	CURRENT	UPDATED						
RULE GENERAL CONFIGURATION	RULE GENERAL CONFIGURATION							
Writing Mode	After execution	After execution •						
APPLY		During execution After execution						
RULE STATUS								

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):

	Aller execution
RULE STATUS	
Run Status	RUNNING
Cycle Time (ms)	1

20.6.5.2 Add a Rule

By clicking on the "ADD" button, a new rule can be configured:

	CURRENT	UPDATED
RULE		
CONFIGURATION		
OTE: "Then Actions'	" are execute	ed when the condition result, as a whole, is TRUE; otherwise
Else Actions" are exe	ecuted.	
ctions with Mode=Re all other cases, acti	epeat and actions are exec	tions in rules with Period>0 are always executed.
Enabled	OFF	OFF V
Index	3	3
Description		
Period (ms)	0	0
If Condition 1		
Туре	None	None
If Condition 2		
Туре	None	None 🔻
If Condition 3		
Туре	None	None V
f Condition Operator		
Operator	OR	OR V
Then Action 1		
Туре		None
Then Action 2		
Type		None
Then Action 3		
Type		None
Else Action 1		
Type		None v
Fise Action 2		
Tune		None
Type		
Elso Action 3		

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	OFF
	disabled, that is if the rule will be	
	processed or not	

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	0
	are executed only if there is a	
	change in the "OR/AND" result.	
	If the value is different from 0 the	
	Actions are executed every Period	
	íms].	
	Don't use little Period values for	
	sending EMAIL/SMS Actions!	
	Note that the Period is in	
	milliseconds (seconds/1000).	
	ΝΟΤΕ:	
	If Period is >0 the Actions are	
	always executed in "repeat" mode	
If Condition X Type	This parameter defines the type of	None
X=[13]	condition. for each of the three	
J	available "if conditions"	
	Possible types are:	
	- None	
	- Alarm State	
	- Alarm Active	
	- Always	
	- Digital Tag	
	- Analog Tag	
	- Timer	
	- Scheduler	
	- Bule Status	
	- Bitmask	
	See paragraph 20.6.5.2.1	
If Condition Operator	The possible types are: OR/AND	OB
	IF Conditions can be combined in OR	
	or AND boolean operations.	
	Remember that using "OR" the	
	result is true if at least one condition	
	is true.	
	Using "AND" the result is true if all	
	the conditions are true.	
Then/Else	This parameter defines the type of	None

-

Action X with X=[13]	action, for each of the three
	available "then/else actions"
	Possible types are:
	- None
	- Send Alarm SMS ²²
	- Send Alarm EMAIL
	- Send Alarm HTTP POST
	- Digital Tag
	- Analog Tag
	- Timer
	- Scheduler
	- Datalogger
	- Network
	- Set Bits
	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: - None - Alarm (digital only) - Alarm Low Low (analog only) - Alarm Low (analog only) - Alarm High (analog only) - Alarm High High (analog only) - Acknowledge - Return - End 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	OFF
	"Analog Danger" or not, meaningful	
	only for analog alarms	

Alarm Active parameters

Field	Meaning	Default value
Alarm Name	The name of the alarm can be	First alarm name in the list
	selected from the list of all	
	configured alarms	
Alarm Active	Flag telling if alarm shall be "active"	OFF
	or not	
	Alarm is "active" if it is in one of the	
	states:	
	 Alarm (digital only) 	
	 Alarm Low Low (analog only) 	
	 Alarm Low (analog only) 	
	- Alarm High (analog only)	
	- Alarm High High (analog	
	only)	
	- Acknowledge	
	Alarm is "not active" if it is in one of	
	the states:	
	- None	
	- Return	
	- End	
Analog Danger Alarm	Flag telling if alarm level shall be	OFF
	"Analog Danger" or not, meaningful	
	only for analog alarms.	

<u>Always</u>

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
Тад	Select the Tag that must be used for	-
	the condition	
Operator	Can be :	=
	"="	
	">"	
	"<"	
	">="	
	"<="	
Tag / Constant value	Select if the comparison is between a	-
	tag or a constant value	

<u>Timer</u>

Field	Meaning	Default value
ID	Select the Timer ID to be used	-
Expired	Can be:	OFF
	"OFF" or "ON"	
	With "ON" the condition is true only	
	when the timer is expired (finish	
	state).	
	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.	
	See chapter 20.6.4	

The Timer functioning is represented in the following diagram:



<u>Schedule</u>

Field	Meaning	Default value
Туре	Can be Daily, Weekly Monthly	-
	Daily: the condition is true every day	
	at Hour:minute configured	
	Weekly: the condition is true the	
	selected day of the week at	
	hour:minute	
	Monthly: • the condition is true the	
	solocted day of the month at	
	bourminute	
Day	If type is Weekly:	-
	0 = Sunday	
	1 = Monday	
	2 = Tuesday	
	3 = Wednesday	
	4 = Thursday	
	5 = Friday	
	6 = Saturday	
	If type is Monthly:	
	Select the day of the month from 1	
	to 31	
Hour	Hours	-
Minute	Seconds	-

<u>Rule Status</u>

Field	Meaning	Default value
ID	Select which Rule ID	-
Enabled	Select between Enabled or Disabled.	-
	If "Enabled" the condition is TRUE if	
	the selected Rule is enabled.	
	If "Disabled" the condition is TRUE if	
	the selected Rule is disabled.	

<u>Bitmask</u>

Field	Meaning	Default value
Тад	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	0000
	of 4 hexadecimal digits	

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	First message in the list
	the SMS or EMAIL	
Group	The group of users the alarm will be	First group in the list
	sent to	

Send Alarm HTTP POST parameters

Field	Meaning	Default value
Message	The message text to be inserted in	First message in the list
	the HTTP POST	

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	One time
	time" or "Repeat".	
	With "One Time" the Actions are	
	executed only if there is a change in	
	the OR/AND Conditions Result.	
	With "Repeat" the Actions are	
	executed at every loop (if the rule is	
	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 boolean operator to use,	-
	select between =, NOT, OR etc	
Source Tag 1 / Constant value 1	Select the Tag to use in the boolen	-
	calculation.	
	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".	One time
	With "One Time" the Actions are executed only if there is a change in the OR/AND Conditions Result.	
	With "Repeat" the Actions are executed at every loop (if the rule is	

	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: "="	-
	copy the Source Tag 1/ Constant value 1 into the Destination Tag	
	Example:	
	Destination Tag = Source Tag 1	
	Or	
	Destination Tag = Constant value 1	
	"+="	
	Sum to the Destination Tag the value of	
	Source Tag1 / Constant value 1 and copy	
	the result to the Destination Tag.	
	Example:	
	Destination Tag = Destination Tag+Source	
	Tag1	
	<i>""</i>	
	Subtract to the Destination Tag the	
	value of Source Tag1 and copy the result	
	to the Destination Tag.	
	Example:	
	Source Tag1	
	"*_"	
	Multiply the Destination Tag with the value of Source Tag1 and copy the result to the Destination Tag. Example:	
	Destination Tag = Destination Tag * Source Tag1	
	"/="	
	Divide the Destination Tag with the	
	value of Source Tag1 and copy the result	
	to the Destination Tag.	
	Example:	
	Source Tag1	

%="
70-

Calculate the rest of the division From the Destination Tag and the value of Source Tag1 and copy the result to the Destination Tag.

(Note that 53%7 = 4)

Example: Destination Tag = Destination Tag % Source Tag1

"abs"

Calculate the absolute value of Source Tag 1/ Constant value 1 and copy the result to the Destination Tag (Note that abs(-4) = 4)

Example: Destination Tag = abs(Source Tag 1)

"sqrt"

Calculate the square root value of Source Tag 1 / Constant value 1 and copy the result to the Destination Tag. (Note that sqrt(9) = v9 = 3) Example: Destination Tag = sqrt(Source Tag 1)

"sqr"

Calculate the square value of Source Tag 1 / Constant value 1 and copy the result to the Destination Tag. (Note that sqr(3) = 3² = 9) Example: Destination Tag = sqr(Source Tag 1)

"log"

Calculate the decimal logarithm of Source Tag 1 / Constant value 1 and copy the result to the Destination Tag. (Note that log(3) = 0.4771212) Example: Destination Tag = log (Source Tag 1)

[&]quot;In"

Calculate the natural logarithm of	
Source Tag 1 / Constant value 1 and	
copy the result to the Destination Tag.	
(Note that ln(3) = 1.09861228867)	
Example:	
Destination Tag = $\ln(Source Tag 1)$	
"ovp"	
Coloulate the Sularle number rejead to	
Calculate the Euler's number faised to	
Source Tag 1 / Constant value 1 and	
copy the result to the Destination Tag.	
(Note that	
$\exp(3) = e^3 = 20.0855369232$	
ln(exp(3)) = 3	
Example:	
Destination Tag = exp(Source Tag 1)	
"+"	
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	
Evample:	
Destination Tag = Source Tag 1+ Source Tag 2	
Destination rag = Source rag 11 Source rag 2	
<i>и п</i>	
-	
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.	
Example:	
Destination Tag = Source Tag 1- Source Tag 2	
<i>u</i> * <i>n</i>	
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.	
Example:	
Destination Tag = Source Tag 1* Source Tag 2	
יין וי	
Divide the Source Tag 1 / Constant value	
1 With the value of Source Tag $2/$	
Constant value 2 and conv the result to	
the Destination Tag	
the Destination Tag.	

	Example:	
	Destination Tag = Source Tag 1 / Source Tag	
	2	
	"%"	
	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.	
	(Note that $53\%7 = 4$)	
	Example:	
	Destination Tag - Source Tag 1 % Source Tag	
	-	
	"pow"	
	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.	
	Example:	
	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	Soloct the Tag to use as input 2 in the	
	select the lag to use as input 2 in the	-
	calculation if the operator needs 2	
	inputs.	
	You can also use a constant value.	

<u>Timer</u>

Field	Meaning	Default value
ID	Select the Timer ID to use.	-
	See chapter 20.6.4	
Action	Select the action to be done to the	-
	specified timer:	
	"Start" will start a timer to count	
	"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:	
	"ON" will enable a disabled Rule	
	"OFF" will disable an enabled Rule	

Data Logger

Field	Meaning	Default value
Group	Select the Logger group to start/stop	-
	Select between ALL, 1, 2, 3, 4	
Enable	Select the action to be done to the	-
	specified rule:	
	"ON" will start to log the selected	
	group(s)	
	"OFF" will stop to log the selected	
	group(s)	

<u>Network</u>

Field	Meaning	Default value
Feature	Select the action to be done to a	-
	network feature, select between:	
	PPP* (Start or Stop the connection	
	to the data mobile connection)	
	VPN (Start or Stop the VPN /Let's	
	connection)	
	Firewall (Start or Stop the Firewall)	
	* Only for Z-PASS2 model	
Start	Select the action to be done to the	-
	specified Feature:	
	"ON" will enable the feature	
	"OFF" will disabled the feature	

<u>Set Bits</u>

Field	Meaning	Default value
Action Mode	Action mode, select from "One	One Time
	time" or "Repeat".	

	With "One Time", the Actions are	
	executed only if there is a change in	
	the OR/AND Conditions Result.	
	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	0000
	of 4 hexadecimal digits	
Action	Reset: set the masked bits to 0	Reset
	Set: set the masked bits to 1	

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 V	
TARGET MODBUS REQUEST TYPE	HOLDING REGISTER	HOLDING REGISTER V	
TARGET REGISTER DATA TYPE	16BIT SIGNED	16BIT SIGNED V	
GATEWAY TAG MODE	SHARED MEMORY	SHARED MEMORY V	
INITIAL VALUE	0	0	
HTTP POST VID	27	27	Corresponding to HTTP POST variable : V27
READ ONLY	OFF	OFF V	If READ ONLY = ON, tag value cannot be changed by means of Modbus protocol
CALCULATED FUNCTION	NONE	NONE v	
ALARM ENABLED	OFF	OFF V	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 V	
TARGET REGISTER DATA TYPE	32BIT REAL MSW	32BIT REAL MSW V]
GATEWAY TAG MODE	SHARED MEMORY	SHARED MEMORY V	
INITIAL VALUE	0	0	
HTTP POST VID	28	28	Corresponding to HTTP POST variable : V28
READ ONLY	OFF	OFF V	If READ ONLY = ON, tag value cannot be changed by means of Modbus protocol
CALCULATED FUNCTION	NONE	NONE V	
ALARM ENABLED	OFF	OFF V	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:

SENECA SENECA	Z-PASS2																		
Basic Configuration	Rule Configu	uration [u	user: admin] [lo	ogout]															
Summary	Firmware Ve	rsion: S	W003900 250																
Network and Services	MACAUL	COFO	44.00004																
Serial Ports	MAC Addres	IS: C8F90	51180001																
Digital I/O Configuration	Internet Acce	ess: Eth	ernet				1												
Real Time Clock Setup	Gateway: rui	nning [D	ata Logger: rui	nning]		1	/												
Gateway Configuration	Router: disa	bled				1													
VPN Configuration						/													
Router Configuration	_					<u> </u>	100.4750												
Users Configuration					URRENT		UPDATED												
Mobile Configuration	RULE G	ENERAL	CONFIGURATION																
Mobile Network			Writing Mode	After exe	ecution	Afte	r execution 🔻												
DDNS Configuration	APPLY																		
Shared Memory Tag Conf.			RULE STATUS																
TCP Servers			Bup Status			DII	NINING												
Tag Setup			Cycle Time (me)																
Lag View			Cycle Time (ma)			·													
Alarm Configuration	F	Rule Man	agement		ADD		MODIFY	Т	COPY	MOVE		DEL	ETE		DELETE /	ALL			
Alarm Summary			0																
Alarm History		Rule D	ebuager				SET/RESET B	REA	KPOINT	1		PLAY			SHOW TAGS				
Logic Configuration		Trailo Di	00009901			SETTRESET BREAK ONT									011011 11100]			
Phonebook		(Period							I							Condition	
SMS Configuration	# Enabled	Index	Description	(ms)	If condition 1		If condition 2		If condition 3	Then action 1	The	in action 2	Then a	ction 3	Else action 1	Else action	2 Else action 3	Status	Breakpoint
Email Configuration			No rule			Γ													
HTTP Configuration			Notuic																
TITTE Configuration																			
Message Configuration				1	1						1			-					
Message Configuration Timer Configuration																			
Message Configuration Timer Configuration Rule Management				1	1														
Message Configuration Timer Configuration Rule Management Data Logger (SD found) General Satisfies				1	1														
Message Configuration Timer Configuration Rule Management Data Logger (SD found) General Settings SD Transfer Conf.	·			<u>д</u>	1										1	<u> </u>		<u>I</u>	
Message Configuration Timer Configuration Rule Management Data Logger (SD found) General Settings SD Transfer Conf.	·			<u>и</u>	<u>и</u>		1								<u> </u>	1		1	
Message Configuration Message Configuration Timer Configuration Rule Management Data Logger (SD found) General Settings SD Transfer Conf. FTP Transfer Conf. Group Configuration				<u>u</u>			<u> </u>		<u> </u>	<u> </u>					<u> </u>	1		<u>I</u>	
Mine Configuration Timer Configuration Timer Configuration Rule Management Data Logger (SD found) General Settings SD Transfer Conf. FTP Transfer Conf. Group Configuration SD File Manager	<u> </u>						1			<u> </u>					<u> </u>	1		<u>I</u>	
Mine 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	· · ·				1		1		<u> </u>	<u> </u>					<u> </u>	1		1	
HTTP Comparation Message Configuration Timer Configuration Rule Management Data Logger (50 found) General Settings SD Transfer Conf. FTP Transfer Conf. FTP Transfer Conf. Group Configuration SD File Manager Maintenance Ethermel Intefaces	<u> </u>	11			1					<u> </u>					<u> </u>	1		<u>I</u>	
HTTP Configuration Timer Configuration Rule Management Data Logger (SD Found) General Settings SD Transfer Conf. FTP Transfer Conf. FTP Transfer Conf. Group Configuration SD File Manager Maintenance Ethernel Interfaces FTV Versions	<u> </u>	11			1		1			<u> </u>					<u> </u>	1		<u>I</u>	
HTTP Configuration Time: Configuration Time: Configuration Date Logger (SD Found) General Settings SD Transfer Conf. FTP Transfer Conf. FTP Transfer Conf. SD File Manager Maintenance Ethernet Interfaces FtV Vesions FVV Vesions	<u> </u>	11						<u></u>							1	1		<u>I</u>	
In the Configuration Time Configuration Tube Configuration Tube Management Data Logger (SD found) General Settings 5D Transfer Conf. FTP Transfer Conf. Group Configuration SD File Manager Maintenance Ethermet Interfaces FVW Upgrade Conf. Management	<u> </u>				1			<u>n</u>		L					1	1		1	

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. Actions with Mode=Repeat and actions in rules with Period>0 are always executed. In all other cases, actions are executed only when there is a change in the condition result.												
Enabled	ON	ON V										
Index	1	1										
Description	Calculate Biggest Circumference	Calculate Biggest Circumference										
Period (ms)	1000	1000										
16 Countration of												

Then the "if condition" with the biggest radius (we need only 1 if condition):

			If Condition 1		
			Туре	Analog Tag	Analog Tag 🔻
Tag	RADIU \$1	RADIUS1	۲		
Operator	>	> 🔻			
Tag	RADIU \$2	RADIUS2	۲		
			Туре	None	None V
			If Condition 3		
			Туре	None	None V
			Operator	OR	OR V

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 V	
Operator *	* V	
Source Tag 1 RADIUS1	RADIUS1 V	
Source Tag 2 constant value	constant value	
Constant Value 2 6.28 6.2	28	
	Then Action 2	
	Туре	None 🔻
	Then Action 3	
	Туре	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 t	me 🔻
Destination Tag	JMFERENCE V
Operator *	T
Source Tag 1 RADIUS2 RADI	JS2 V
Source Tag 2 constant const	ant 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. Actions with Mode=Repeat and actions in rules with Period>0 are always executed. In all other cases, actions are executed only when there is a change in the condition result.											
Enabled	ON	ON V									
Index	2	2									
Description	Calculate Biggest Area	Calculate Biggest Area									
Period (ma)	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 Action 1	
Type Analog Tag	Analog Tag 🛛 🔻
Action Mode One time One time V	
Destination Tag	
Operator aqr Sqr 🔻	
Source Tag 1 RADIUS1	
Then Action 2	
Type Analog Tag	Analog Tag 🔹 🔻
Action Mode One time One time	
Destination AREA Tag	
Operator *	
Source Tag 1 AREA AREA V	
Source constant Tag 2 value constant value	
Constant Value 2 3.14 3.14	
Then Action 3	
Туре	None 🔻

Then if RADIUS1 < RADIUS2 we calculate AREA with RADIUS2:

Else Action 1	
Тура Analog Tag	Analog Tag 🔹 🔻
Action Mode One time One time ▼	
Destination Tag AREA AREA V	
Operator sqr 🛛 🔻	
Source Tag RADIUS2 RADIUS2	
Else Action 2	
Туре Analog Tag	Analog Tag 🛛 🔻
Action Mode One time ▼	
Tag AREA AREA V	
Operator *	
Source Tag 1 AREA AREA V	
Source constant Tag 2 value Constant value	
Constant Value 2 3.14 3.14	
Else Action 3	
Туре	None 🔻
APPLY	

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):

				CI	URRENT		UPDATED										
	RULE GI	ENERAL	CONFIGURATION Writing Mode	After exec	ution [After	execution •										
			RULE STATUS Run Status Cycle Time (ms)		I		INING	/									
	R	ule Ma	nagement		ADD		MODIFY		COPY	MOVE	DELE	TE	DELETE ALL				
		Rule D	ebugger				SET/RESET E	BREA	KPOINT		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	Breakpoin
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":

VER Comparation											
Router Configuration											
Users Configuration		Data Lo	ogger:	START ST	OP CLEA	N CACHE	=				
Mobile Configuration		_					-				
Mobile Network		Page	: 1/20	PREVIOUS P	AGE NEX	KT PAGE					
DDNS Configuration		-		REGISTER	UNSIGNED						
Shared Memory Tag Conf.	17	GPS YEAR	16	HOLDING	16BIT	0			NONE	NONE	
TCP Servers		0.0_12.0.0		REGISTER	UNSIGNED					HOLL	
Tag Setup	18	GPS_LATITUDE	17	REGISTER	64BH REAL	0	-		NONE	NONE	
Tag View Alarms	19	GPS_LONGITUDE	21	HOLDING REGISTER	64BIT REAL	0	-		NONE	NONE	
Alarm Configuration	20	GPS_HDOP	25	HOLDING REGISTER	64BIT REAL	0	-		NONE	NONE	
Alarm Summary	21	GPS ALTITUDE	20	HOLDING	64BIT	0			NONE	NONE	
Alarm History	21	OI 3_ALITTODE	23	REGISTER	REAL	0	-		NONE	NONE	
Logic Configuration Phonebook	22	GPS_COG	33	HOLDING REGISTER	64BIT REAL	0	-		NONE	NONE	
SMS Configuration	23	GPS_SPEED_KM	37	HOLDING REGISTER	64BIT REAL	0	-		NONE	NONE	I
Email Configuration	24	GPS_SPEED_KN	41	HOLDING REGISTER	64BIT REAL	0	-		NONE	NONE	
Message Configuration	25	GPS_FIX	45	HOLDING	16BIT	0	-		NONE	NONE	
Timer Configuration	26	GPS_NUM_SAT	46	HOLDING		0	-		NONE	NONE	
Rule Management				HOLDING	16BIT			07/03/2019			
Data Logger (SD found)	27	RADIUS1	100	REGISTER	SIGNED	0	-	10:07:25.651279	NONE	NONE	CHANGE
Seneral Settings	28	RADIUS2	101	HOLDING REGISTER	16BIT SIGNED	0	-	07/03/2019 10:07:25.651519	NONE	NONE	CHANGE
FTP Transfer Conf.	29	CIRCUMFERENCE	103	HOLDING	32BIT	0	-	07/03/2019	NONE	NONE	CHANGE
Group Configuration				HOLDING	32BIT	-		07/03/2019			
SD File Manager	30	AREA	105	REGISTER	REAL MSW	0	-	11:11:16.130488	NONE	NONE	CHANGE
Maintenance											
The second behavior as a											

Now we change the RADIUS1=100 and RADIUS2=50 by clicking on "CHANGE" button:



/ing	192.168.85.103:8080 dice	liti
	RADIUS2	
	50	
	OK Annulla	

Now we can pass to "Rule Management" page for view the result:

				Cl	JRRENT		UPDATED										
	RULE GE	NERAL	CONFIGURATION														
			Writing Mode	After exec	ution [After	execution 🔻										
A	PPLY																
			RULE STATUS														
			Run Status			RUN	INING										
			Cycle Time (ms)		(D											
	R	ule Ma	nagement		ADD		MODIFY		COPY	MOVE	DELE	TE	DELETE ALL				
		Rule D	ebugger				SET/RESET E	BREA	KPOINT		PLAY		SHOW TAGS				
#	Rule Debugger # Enabled Index Description (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	1 ON 1 Calculate Biggest Circumference			1000	RADIUS1 > RADIUS2	OR		OR		CIRCUMFERENCE = RADIUS1 * 6.28			CIRCUMFERENCE = RADIUS2 * 6.28			TRUE	
2	# Enabled Index Description 1 ON 1 Calculate Biggest Circumferer 2 ON 2 Calculate Biggest Arr Biggest Arr			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	16BH 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 F	32BIT REAL MSW	628	-	07/03/2019 11:34:39.634836	NONE	NONE	CHANGE
30	AREA	105	HOLDING REGISTER F	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 ADI	MODIFY	COPY	MOVE	DELE	TE	DELETE ALL				
Rule Debugger	SET/RESET	BREAKPOINT		PLAY		SHOW TAGS				
# Eachlad Index Description Period If co	dition If condition	If condition	These sections 4	Then action	Then action		Else action	Else action	Condition	Duralmaint
# Enabled Index Description (ms)	2	3	Then action 1	2	3	Else action 1	2	3	Status	Бгеакроіпт
1 ON 1 Calculate Biggest Circumference	JS1 > US2 OR	OR	CIRCUMFERENCE = RADIUS1 * 6.28			CIRCUMFERENCE = RADIUS2 * 6.28			FALSE	
2 ON 2 Calculate 1000 RAD Biggest Area 1000 RAD	JS1 > US2 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	16BH 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 I	32BIT REAL MSW	1256	-	07/03/2019 11:35:43.55955	NONE	NONE	CHANGE
30	AREA	105	HOLDING REGISTER I	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

	C	URRENT		UPDATED										
RULE GENERAL CONFIGURATIO	N													
Writing Mo	e After exe	cution	After	execution •										
APPLY	_											,		
RULE STATU	s													
Run State	s		RUM	INING										
Cycle Time (m	5)		0											
Rule Management		ADD		MODIFY		COPY	MOVE	DELE	TE	DELETE ALL		_		
Rule Debugger				SET/RESET I	BREA	KPOINT		PLAY		SHOW TAGS				
# Enabled Index Description	n 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 Circumferen	1000	RADIUS1 > RADIUS2	OR		OR		CIRCUMFERENCE = RADIUS1 * 6.28			CIRCUMFERENCE = RADIUS2 * 6.28			FALSE	
2 ON 2 Calculate Biggest Are	a 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":

				CL	JRRENT		UPDATED										
	RULE G	ENERAL	CONFIGURATION														
			Writing Mode A	After exec	ution [After	execution •										
A	PPLY																
			RULE STATUS														
			Run Status		ļ	PAU	SED										
			Cycle Time (ms)		()											
	F	Rule Ma	nagement		ADD		MODIFY		COPY	MOVE	DELE	TE	DELETE ALL				
		Rule D	ebugger				SET/RESET E	BREA	KPOINT		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 exe	ecution	After	execution •										
APF	PLY																
			RULE STATUS														
			Run Status			PAL	ISED										
			Cycle Time (ms)			0											
		Rule Ma	nagement		ADD		MODIFY		COPY	MOVE	DELE	TE	DELETE ALL				
		Rule D	Debugger				SET/RESET	BREA	KPOINT		PLAY		SHOW TAGS				
								_			-	-			-	a	
# E	nable	d Index	Description	Period (ms)	If condition		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				RADIUS1 > RADIUS2	OR		OR		AREA sqr RADIUS1	AREA = AREA * 3.14		AREA sqr RADIUS2	AREA = AREA * 3.14		FALSE	
#		TA	G NAME			TAG V	ALUE										
1		R	ADIUS1			10	0										
2		R	ADIUS2			20	0										
4		CIRCU	AREA		125	6											

Now you can move the breakpoint to the following rule, select the next rule and press the "SET/RESET BREAKPOINT" button:

				C	URRENT		UPDATED										
	RULE G	ENERAL	CONFIGURATION														
			Writing Mode	After exec	cution	After	execution •										
F	PPLY																
			RULE STATUS														
			Run Status			PAL	JSED										
			Cycle Time (ms)			0											
	F	Rule Ma	nagement		ADD		MODIFY		COPY	MOVE	DELE	ETE	DELETE ALL				
]					
L		ebugger			SET/RESET	BREA	KPOINT		PLAY		SHOW TAGS						
				Deried	If condition		If condition		If condition		Then action	Then action		Elec action	Electronic .	Condition	
#	Enabled	Index	Description	(ms)	1		2		3	Then action 1	2	3	Else action 1	2	3	Status	Breakpoint
	ON	1	Calculate	1000	RADIUS1 >					CIRCUMFERENCE			CIRCUMFERENCE				
	ON		Circumference	1000	RADIUS2	UR		UR		= RADIUS1 * 6.28			= 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
┢	1	R	ADUUS1			10 10	0										
F	2	R	ADIUS2			20	0										
	3	CIRCU	MFERENCE			125	56		_								
Ē	3 CIRCUMFERENCE 4 AREA					1256	500										

Note that the execution is pause because you must press "PLAY" for advance to the next breakpoint, press "PLAY":

				С	URRENT		UPDATED										
	RULE	GENERAL	CONFIGURATION														
			Writing Mode	After exe	cution	After	execution •										
A	PPLY																
			RULE STATUS														
			Run Status			PAL	ISED										
			Cycle Time (ms)			0											
Γ		Rule Ma	nagement		ADD		MODIFY		COPY	MOVE	DELE	TE	DELETE ALL				
	Rule Debugger																
		Rule D	Debugger				SET/RESET	BREA	KPOINT		PLAY		SHOW TAGS				
				,													
#	Enabled Index Description				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 1 Diggest Circumference 1 ON 2 Calculate Biggest Area 10				RADIUS1 > RADIUS2	OR		OR		AREA sqr RADIUS1	AREA = AREA * 3.14		AREA sqr RADIUS2	AREA = AREA * 3.14		FALSE	ON
	#	ТА	G NAME														
	1	R	ADIUS1			10	0										
	2	R	ADIUS2			20	0										
F	3	CIRCU	MFERENCE			125	i6		_								

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:

🕒 Z-PASS2	× +		-		×
← → C ③ Nor	sicuro 192.168.85.105:8080/datalog_gen_conf.php	☆	ト	G	0
Serial Ports Basic Configuration Summary Network and Services Serial Ports Real Time Clock Setup Gateway Configuration VPN Configuration Wobile 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 Email Configuration HTTP Configuration HTTP Configuration Rule Configuration HTTP Configuration HTTP Configuration Rule Configuration Rule Configuration Rule Configuration Rule Configuration Rule Configuration Rule Configuration	Sicuro (192.168.85.105:8080/datalog_gen_cont.php) Z-PASS2 General Settings [user: admin] [logout] Firmware Version: SW003900_240 [Modern: 1231B02SIM5350E] MAC Address: C8F981160043 [IMEI: 862264020406335] Internet Access: Ethernet Gateway: running [Data Logger: running (no group enabled)] Router: disabled CURRENT UPDATED General Settings RTU Name Z-PASS Z-PASS RTU Name Z-PASS Z-PASS Transfer Priority New files first New files first O Decimal Separator Point () Point () V CSV Separator Semicolon (;) Semicolon (;) V INDEX Column ON ON V TYPE Column ON ON V HI:HMM:SS V HITP POST Enable OFF OFF V HTTP POST Enable OFF OFF V HTTP POST fag Limitation Needed with Seneca Cloud Box to OFF OFF V POST to 130 Transfer Settings				
General Settings SD Transfer Conf. FTP Transfer Conf.	SD Enable OFF FTP Enable OFF				
Group Configuration Maintenance	EMAIL Enable ON HTTP POST Enable OFF				
Ethernet Interfaces					
FW Versions					
Conf. Management					

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.	Z-PASS
	It is used in log file names, transferred	
	via FTP or sent as email attachments	
Transfer Priority	This field tells if newer or older log files	New files first
	shall be transferred first.	

	Possible values are:	
	- Old files first	
	- New files first	
Decimal separator	Character used as decimal separator for	Point (.)
	floating point values in log files.	
	Possible values are:	
	- Point (.)	
	- Comma (,)	
CSV Separator	Character used as field separator in csv	Semicolon (;)
	log files.	
	Possible values are:	
	- Semicolon (;)	
	- Point (.)	
	- Blank ()	
INDEX Column	Flag telling if the "INDEX" column	ON
	containing the line (sample) progressive	
	index shall be present in the log files or	
	not	
TYPE Column	Flag talling if the "TYPE" column	ON
	ridg terming in the TTPE columnity,	SN
	containing the line (sample) type, shall	
	be present in the log files of not.	
	NOTE: currently, this column always	
	contains the "LOG" string	
Timestamp Format	Format of the timestamp value in the	dd/mm/yyyy HH:MM:SS
	"TIMESTAMP" column.	
	Possible formats are:	
	dd/mm/yyyy HH:MM:SS	
	yyyy/mm/dd HH:MM:SS	
	dd/mm/yy HH:MM:SS	
	yy/mm/dd HH:MM:SS	
	seconds since the Epoch	
HTTP POST Enable	Flag to enable/disable the HTTP POST	OFF
	protocol (see paragraph 9.1)	
HTTP POST Tag Limitation	When this parameter is set to ON, the	OFF
	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.	
	This limitation is needed when using the	
	Z-PASS with the Seneca Cloud Box	
	product.	
1		1

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:

C Z-PASS1	× +				-		×
← → C ③ Nor	n sicuro 192.168.85.103:8080/datalog_	group_conf.php		1	2	G	0
SENECA® Basic Configuration Summary Network and Services	Z-PASS1 Group Configuration [user: admin] Firmware Version: SW003900_240 MAC Address: C8E9811B0001	[logout]					
Serial Ports Digital I/O Configuration Real Time Clock Setup Gateway Configuration VPN Configuration	Internet Access: Ethernet Gateway: running [Data Logger: run Router: running	nning]					
Router Configuration Users Configuration	Group 1	CURRENT	UPDATED				
Shared Memory Tag Conf. TCP Servers Tag Setup Tag View	Sampling Mode Sampling Period (s)	Periodic 30	Periodic V				
Alarms Alarm Configuration Alarm Summary	Transfer Period (min) Time before overflow HTTP POST Time before overflow	60	833 hours, 20 min, 0 s 25 hours, 0 min, 0 s				
Logic Configuration Phonebook Email Configuration	Group 2 Sampling Mode	Disabled	Disabled •				
HTTP Configuration Message Configuration Rule Configuration Data Logger (SD found)	Sampling Period (s) Transfer Period (min) Time before overflow	16	15 15 0				
General Settings SD Transfer Conf. FTP Transfer Conf.	Group 3 Sampling Mode	Disabled	Disabled •				
Group Configuration SD File Manager Maintenance Ethernet Interfaces	Sampling Period (s) Transfer Period (min) Time before overflow	16 15	15 15 0				
FW Versions FW Upgrade Conf. Management	TAG LIST Group 4	Product	Disabled				
	Sampling Mode Sampling Period (s) Transfer Period (min) Time before overflow	Disabled 15 15	15 0				
	TAG LIST APPLY						•

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	Disabled
	sampling mode is "Periodic", this	
	parameter is actually a flag used to	
	enable ("Periodic") or disable	
	("Disabled") the group.	

Sampling Period (s)	This parameter defines the sampling	15
	period, in seconds.	
	Minimum: 1, Maximum: 7200	
Transfer Period (min)	This parameter defines the transfer	15
	period, in minutes; that is every time	
	interval defined by this parameter the	
	log file is closed and transferred.	
	Minimum: 1, Maximum: 43200	

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 <u>the values of the "Sampling Period" and "Transfer Period" parameters determine</u> 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:

	Govanni —		×
Z-PASS2			
$\leftarrow \rightarrow \mathbf{C}$ (i) 192.16	8.85.104:8080/datalog_conf_save.php?act=save&type=grp	☆ 🗵	:
SENEC A®	Z-PASS2		
ULIILUA			
General Configuration	Data Logger Configuration [user: admin] [logout]		
Main View	Firmware Version: SW003900_230 [Modem: UC20GQBR03A14E1G]		
Network and Services	MAC Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222013200438015]		
Serial Ports	Internet Access: Ethernet		
Gateway Configuration			
Real Time Clock Setup	Gateway: running [Data Logger: running (no group enabled)]		
VPN Configuration	Router: running		
Router Configuration			
Users Configuration			
FW Upgrade			
Conf. Management	Transfer Period (in seconds) must be a multiple of Sampling Period ! Group Configura	tion n	ot
Shared Memory Tag Conf.	changed		
Tag Setup			
Tag View			
TCP Servers			
Mobile Configuration			
Mobile Network			
DDNS Configuration			
Digital I/O Configuration			
Logic Configuration			
SMS Configuration			
Phonebook			
Diagnostics			
FW Versions			
Ethernet Interfaces			
Data Logger (SD missing)			
General Settings			
Group Configuration			

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.

		Governi -	- 🗆	×
Z-PA	ISS2	×		
$\leftrightarrow \rightarrow$	C (i) 192.16	8.85.104:8080/datalog_conf_save.php?act=save&type=grp	☆	E.
© C		7.04889		
<u>)</u> 7	INEGA	2-F A352		
General Co	onfiguration	Data Logger Configuration [user: admin] [logout]		
Main View		Firmware Version: SW003900_232 [Modem: UC20GQBR03A14E1G]		
Network an	nd Services	MAC Address: C8F9811B0000 [IME]: 861075026666172] [IMS]: 222101600237893]		
Serial Ports	3	Internet Access: Ethernet		
Gateway Co	onfiguration			
Real Time (Clock Setup	Gateway: running [Data Logger: running (no group enabled)]		
VPN Config	guration	Router: disabled		
Router Con	figuration			
Jsers Confi	figuration			
FW Upgrad	le			
Conf. Mana	agement	For HTTP POST, Sampling Period must be a multiple of 30 seconds ! Group Config	uration	not
Shared Me	emory Tag Conf.	changed		
Tag Setup		•		
Tag View				
TCP Server	rs			
Mobile Cor	nfiguration			
Mobile Netv	work			
DDNS Conf	figuration			
Digital I/O	Configuration			
Digital I/O C	Configuration			
Logic Con	figuration			
SMS Config	guration			
Phonebook	¢			
Diagnostic	08			
-vv version	ns			
thernet Int	tertaces			
Seneral Set	et (SD Iouna)			
Brown Conf	figuration			
PD Eil- M	nguration			
5D File Mar	nager			

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:

Th Z-PASS2	×		Ciovanti — 🗆 🗙
← → C ① 192	.168.85.104:8080/datalog_tag_conf.	php?id=0	९☆ 🛛 :
SENECA® General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration	Z-PASS2 Tag Configuration [user: admin] [Firmware Version: SW003900_234 MAC Address: C8F9811B0000 [IM Internet Access: Ethernet Gateway: running [Data Logger: r Router: running	[logout] 0 [Modem: UC20GQBR03A14E1G] IEI: 8610750266666172] [IMSI: 222013200438015] running (no group enabled)]	
Users Configuration FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup	PREV GROUP IMPORT FROM CSV ADD	Group 1 Scegli file Nessun file selezionato	EXPORT TO CSV DELETE
Tag View TCP Servers Mobile Configuration Mobile Network DDNS Configuration Digital I/O Configuration Logic Configuration SMS Configuration Phonebook Diagnostics FW Versions Ethernet Interfaces Data Logger (8D missing) General Settings Group Configuration	# 1 2 3 4 5 6 7 8 9 10 11 12 13 13 14 15 16 17 18 19 20 21 22 23 24 25 26	NameZPASS_DIZPASS_DOZPASS_DI_1ZPASS_DI_2ZPASS_DI_3ZPASS_DO_1ZPASS_DO_2ZPASS_DO_2ZPASS_DO_3ZPASS_DO_4GPS_ERRORGPS_HOURGPS_MOURGPS_MOURGPS_MONTHGPS_VEARGPS_LATITUDEGPS_LONGITUDEGPS_HOOPGPS_ALTITUDEGPS_SPEED_KMGPS_SPEED_KMGPS_FIXGPS_NUM_SAT	

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.

Z-PASS2	×			Ciovanti	-		×	¢
← → C (i) 192.16	8.85.104:8080/datalog_tag_mod.php?id=0&grp=1					☆		:
S SENECA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration	Z-PASS2 Tag Configuration [user: admin] [logout] Firmware Version: SW003900_230 [Modem: U MAC Address: C8F9811B0000 [IMEI: 8610750 Internet Access: Ethernet Gateway: running [Data Logger: running (no Router: running	IC20GQBR03A14 266666172] [IMSI: group enabled)]	IE1G] 222013200438015]					
Users Configuration	Add Tag to Group 2							
FW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View TCP Servers Mobile Configuration Mobile Network DDNS Configuration Digital I/O Configuration Logic Configuration Configuration SMS Configuration Phonebook Diagnostics FW Versions Ethernet Interfaces Data Logger (SD missing) General Settings Group Configuration	Select tag to be added	Tag Name	ZPASS_DI ZPASS_DO ZPASS_D0_ ZPASS_D0_1 ZPASS_D1_2 ZPASS_D1_3 ZPASS_D0_4 ZPASS_D0_1 ZPASS_D0_2 ZPASS_D0_3 ZPASS_D0_4 GPS_ERROR GPS_HOUR GPS_HOUR GPS_MINUTE GPS_SECOND GPS_DAY GPS_MONTH GPS_YEAR GPS_LATITUDE GPS_LONGITUDE GPS_HDOP					

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:

Data Logger (SD missing) General Settings SD Transfer Conf. FTP Transfer Conf. Group Configuration

When the SD Card is inserted in the Z-PASS, the "Data Logger" section of the web pages menu becomes:

Data Logger (SD found) General Settings SD Transfer Conf. FTP Transfer Conf. Group Configuration SD File Manager

By clicking on the "SD File Manager" link, you come to the following page:

[[™]] Z-PASS2	×				Ciovanni	-		×
← → C ① 192.168	3.85.105:8080/filemgr.p	hp#datalog	js				☆ 🛛	
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	Z-PASS2 SD File Manager [us Firmware Version: 5 MAC Address: C8F5 Internet Access: Mo Gateway: running [I Router: disabled Create New Folder	eer: admir SW003900 9811B0030 obile Data Logg Cr Cr	n] [logout] 0_230 [Modem: UC2003 6 [IMEI: 861075026651 eer: stopped] eate Clean SD	QBR03A14E1G] 331] [IMSI: 222101600237891] selezionato				
Mobile Configuration	Home datalogs 	0	N. 100 1					
Mobile Network DDNS Configuration Digital I/O Configuration	Name 20180611	Size	Jun 12, 2018 7:28 AM	Actions				
Digital I/O Configuration	20180612		Jun 12, 2018 7:50 AM	💥 delete				
SMS Configuration	20180613		Jun 13, 2018 2:01 PM	💢 delete				
Phonebook Diagnostics FW Versions	20180614		Jun 14, 2018 6:00 AM	🛠 delete				
Ethernet Interfaces Data Logger (SD found) General Settings Group Configuration SD File Manager								

D Z-PASS2	×				Ciovanti	-			×
← → C ③ 192.16	8.85.105:8080/file	mgr.php#d	latalogs/20180611				☆	۶.	:
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	Z-PASS2 SD File Manag Firmware Vers MAC Address Internet Access Gateway: runn Router: disabl Create New Folder	er [user: a ion: SW00 : C8F98111 es: Mobile hing [Data ed s Here To Up	admin] [logout] 03900_230 [Modem: B0036 [IMEI: 861075 Logger: stopped] Create Clean SD	UC20GQBR03A14E1G] 026651331] [IMSI: 222101600237891] ssun file selezionato					
TCP Servers Mobile Configuration	Home < datale	ogs ⊩ 201	80611						
Mobile Network	Name	Size	Modified	Actions					
DDNS Configuration	log1		Jun 12, 2018 2:00 AM	💥 delete					
Digital I/O Configuration Logic Configuration	log2		Jun 12, 2018 7:29 AM	🗱 delete					
SMS Configuration	log3		Jun 12, 2018 7:28 AM	💥 delete					
Finanebook Diagnostics FW Versions Ethernet Interfaces Data Lagrage (SD (sp. 1))	log4		Jun 12, 2018 7:28 AM	💥 delete					
General Settings Group Configuration SD File Manager									

Z-PASS2	×				Ciovanni –	- 🗆 X
← → C ① 192.168	8.85.105:8080/filemgr.ph	p#datalogs/201	80611/log1			☆ 🗵 :
SENECA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration Users Configuration EW Upgrade Conf. Management Shared Memory Tag Conf. Tag Setup Tag View TCP Servers	Z-PASS2 SD File Manager [use Firmware Version: SI MAC Address: C8F98 Internet Access: Mot Gateway: running [D Router: disabled Create New Folder	er: admin] [log W003900_230 311B0036 [IME bile ata Logger: at Create	out] [Modem: UC20GQBR0 II: 861075026651331] [I opped] Clean SD	3A14E1G] MSI: 222101600237891] onato		
Mobile Configuration	Home 🕨 datalogs 🕨	20180611 × lo	og1			
Mobile Network	Name	Size	Modified	Actions		
DDNS Configuration Digital I/O Configuration	L9700781.csv	950.8 KB	Jun 11, 2018 6:00 PM	🕹 download 🛛 🞇 delete		
Digital I/O Configuration Logic Configuration	L9700860.csv	2.8 MB	Jun 11, 2018 10:00 PM	🚽 download 🛛 😫 delete		
SMS Configuration	L9701100.csv	2.8 MB	Jun 12, 2018 2:00 AM	🕂 download 🛛 💥 delete		
Phonebook Diagnostics FW Versions Ethernet Interfaces Data Logger (SD found) General Settings Group Configuration SD File Manager						

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:

Y varions Y varion Y varion	Confunction Configuration Kobic Configuration Mobic Configura
SENERCIA General Configuration Mair Vew Serial Ports Z-PASZ Serial Ports Ethernet Status [user: admin] [logout] Gateway Configuration Real Time Clock Setup Intermet Access: Mobile Modus Shared Memory Gateway: running VPN Configuration Real Time Clock Setup Router: running Vers Configuration Real Status Down Conf. Management Shared Memory Tag Conf. Tag Setup Shared Memory Tag Conf. Tag Setup Link Status Down On Data Data Data Data Data Data Data Dat	Serial Configuration Min Vew Network and Services Serial Porte Gateway Configuration Neal Time Coke Setup VPN Configuration Real Time Coke Setup VPN Configuration Base Configuration Base Configuration Users Configuration Base Configuration Darge Setup Tag View Mobile Network Mobile Configuration Darge Setup Tag View Mobile Configuration Digration Porticito

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:

🗅 Z-PASS2	× Giovanni —	
← → C ③ 192.16	8.85.104:8080/fwver_full.php	☆ 🗵 :
Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration	Z-PASS2 FW Versions [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	
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 Digital I/O Digital I/O Ethernet Interfaces	HW VersionIW Components VarsionsEV Components VarsionsLinux Kerrel2.6.28 #137 PREEMPT Tue Jun 20 10:46:10 CEST 2017Initial RAM DiskJun 11 3:56:29 2017Root File System227_20171201Default Disk File SystemSW003900_224Disk File System	

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:

192.168.85.104:8080 dice:	×
Do you want to stop gateway services during upload ?	
(Once services are stopped, you can restart them by clicking on the 'RESTART GATEWAY SERVICES' button.)	
OK Annulla	

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.

← → C ① 192.168.85.104:8080/fw_files_bin.php?stop=1 ☆ SENECA® Z-PASS2 General Configuration FW Upgrade [user: admin] [logout] Main View Firmware Version: \$W003900_224 [Modem: UC20GQBR03A14E1G]
 A C ① 192.168.85.104:8080/fw_files_bin.php?stop=1 A Z A SERVECA[®] General Configuration Main View Z-PASS2 FW Upgrade [user: admin] [logout] Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
SENECA Z-PASS2 General Configuration FW Upgrade [user: admin] [logout] Main View Firmware Version: \$W003900_224 [Modem: UC20GQBR03A14E1G]
Network and Services MAC Addrees: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Gateway Configuration Internet Access: Mobile Real Time Clock Setup Modbus Shared Memory Geteway: stopped VPN Configuration Router: running Boater Configuration FW Upgrade Conf. Management FW Upgrade Shared Memory Tag Conf. FW Upgrade Tag Stup FW Upgrade Dons Configuration FW Upgrade Tag View Mobile Configuration Mobile Configuration DDNS Configuration Digital I/O Configuration Digital I/O Configuration Digital I/O Configuration Ehernet Interfaces

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").

□ Z-PASS2	C ¹) Giovand -	-		×
< → C 0	192.168.85.104:8080/fw_upgrade_bin.php	5	۲ ا	:
SENEC	X [®] Z-PASS2			
General Configurati	ion FW Upgrade [user: admin] [logout]			
Main View	Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]			
Network and Service	MAC Address: C8F9811B0000 [IME]: 861075026500975] [IMS]: 222101600237890]			
Serial Ports	Internet Assess Mahila			
Gateway Configuration	on Internet Access: Mobile			
Real Time Clock Set	up Modbus Shared Memory Gateway: running			
VPN Configuration	Router: running			
Router Configuration	· · · · · · · · · · · · · · · · · · ·			
Users Configuration	lovalid file 'disk tar oz' !			
FW Upgrade				
Conf. Management Shared Memory Tag	g Conf. A 'SW003900_*.bin' file is needed.			
Tag View				
Mobile Configuration				
Mobile Network				
DDNS Configuration				
Digital I/O				
Digital I/O Configurat	tion			
Diagnostics				
FW Versions				
Ethernet Interfaces				

Once a file is selected, you can start the upload, by pressing the "UPLOAD" button.

	(!) Ciovanii -	- 🗆 X
← → C ① 192.16	3.85.104:8080/fw_files_bin.php?stop=1	☆ ▶ :
SENECA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration Router Configuration	Z-PASS2 FW Upgrade [user: admin] [logout] Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Internet Access: Mobile Modbus Shared Memory Gateway: stopped Router: running	
Users Configuration	FW Upprade	
FW Upgrade	i ii opgrade	
Conf. Management Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration Mobile Network DDNS Configuration Digital I/O Digital I/O Digital I/O Digital I/O Configuration Diagnostics FW Versions Ethernet Interfaces	FW file (\$W003900_*.bin) Scegli file SW003900_224.bin UPLOAD RESTART GATEWAY SERVICES	

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 simultaneously²⁴; the upgrade procedure is ended when only the LED "RUN" is blinking²⁵;

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.

Z-PASS2	(!) @iovenni X	— C	ב	×
← → C ③ 192.16	8.85.104:8080/fw_upgrade_start.php?do=0	☆	x	:
 ← → C ① 192.16 ◆ 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. 	8.85.104:8080/fw_upgrade_start.php?do=0 Z-PASS2 FW Upgrade [ueer: admin] [logout] Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Internet Access: Mobile Modbus Shared Memory Gateway: stopped Router: running Upgrade cancelled, rebooting			:
Shared Memory Tag Cont. Tag Setup Tag View Mobile Configuration Mobile Network DDNS Configuration Digital I/O Digital I/O Digital I/O Digital I/O Configuration Diagnostics FW Versions Ethernet Interfaces				
Ethemet Intenaces				

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
	- OpenVPN configuration (if present)
	- Modbus Shared Memory Gateway tags
	- Logic configuration
	- web user pages (if present)
Configuration	- configuration parameters
	- OpenVPN configuration (if present)

Logic	- Modbus Shared Memory Gateway tags
	- Logic configuration
	 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 <u>when you carry the configuration archive from a device to another one is that the two</u> <u>devices should be the same product model</u>; 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.

	×	<u>ç</u> ı	Govanni		_			×
	*							
$\epsilon \rightarrow G$	192.168.85.104:8080/index.php			Q	07	☆	J.,	:
SENECA®	Z-PASS2							
General Configuration	Main View [user: guest] [logout]							
Main View	Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]							
Network and Services	MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]							
Senal Ports	Internet Access: Mobile							
Real Time Clock Setup	Modbus Ethernet to Serial Gateway: running							
VPN Configuration	Router: running							
Router Configuration								
Users Configuration	NETWORK							
Mobile Configuration	Ethernet Mode LANWAN							
Mobile Network	DHCP on WAN OFF							
Digital VO	LAN IP Address 192.168.90.101							
Digital I/O Configuration	WAN IP Address 192.168.85.104							
Diagnostios	WAN Network Mask 255.255.252.0							
FW Versions	Default Gateway 10.64.64.64							
Ethernet Interfaces	DNS Mode Statio							
	IP Configuration from Discovery ON							
	WEB SERVER							
	Protocol HTTD/HTTPS							
	HTTP Conf Port 8080							
	HTTP User Port 80							
	HTTPS Port 443							
	FILE TRANSFER							
	Protocol FTP/SFTP							
	FTP Port 21							
	SFIP Pon 22							
	NIP							
	Enable ON Primary Server ato1 ingin it							
	Secondary Server ntp2.inrim.it							
	Time Zone Central Europe (CET/CEST)							
	VPN							
	Mode VPN Box							
	Enable ON							
	Server 192.168.85.176 Password senera							
	Tag Name zpass							
	MOBILE NETWORK							
	Enable ON							
	APN Mode Manual							
	APN m2mbic.vodafone.it							
	Authentioation Type None Username user							
	Password pass							
	PIN 8342							
	Ping Connection Testing IP Address www.google.com							
	NETWORK REDUNDANCY							
	Enable OFF							
	Ping Address 0.0.4.4							
	WAICHDOG							
	Enable ON Timeout (c) 60							
	DEBUGLOGS							
	Eastle ON							
	Enable ON							
	Mode RS485							
	MOTORT DEPAULT RESTART							

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.

Z-PASS2	×		🤔 Giovanni –	- 🗆 X
← → C (i) 192.	168.85.104:8080/mobile_network.php?showinfo=1			Q☆ 🗵 :
SENECCA General Configuration Main View Network and Services Serial Ports Gateway Configuration Real Time Clock Setup VPN Configuration	Z-PASS2 Mobile Network [user: guest] [logout] Firmware Version: SW003900_224 [Modem: UC20GQB MAC Address: C8F9811B0000 [IMEI: 861075026500975 Internet Access: Mobile Modbus Shared Memory Gateway: running Router: running	BR03A14E1G] 5] [IMSI: 222101600237890]		
Router Configuration Users Configuration	CURRENT	UPDATED		
Shared Memory Tag Conf. Tag Setup Tag View Mobile Configuration <i>Mobile Network</i>	SIM PIN (if required by SIM) 8342 8342 Operator Selection Mode Automatic Auto	e omatic •		
DDNS Configuration Digital I/O Digital I/O Configuration	Operator (22210) vodafone IT Oper (GSM)	rator list not available 🔻		
Diagnostics FW Versions Ethernet Interfaces	Enable ON ON APN Mode Manual Man	▼ ual ▼		
	Authentication Type None None Username user user Password pass pass Ping Connection Testing IP Address (if empty, testing is disabled) www.google.com www APPLY HIDE MOBILE STATUS GET OPERATOR LIST	e v v.google.com		
	Mobile Status SIM/PIN Status PIN Remaining Attempts Signal Level [07] Selected Operator Registration Status Connection Status IP Address IP Address RX Packets / Bytes TX Packets / Bytes GP8 Location REFRESH	PIN required 3 6 "vodafone IT" (UMTS) Registered (home network) Connected 91.80.15.232 738 / 57.9K 698 / 51.1K 45.37421,11.94561 [Map]		

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):

🌆 Login			_		\times
Nuovo sito MyFTP Sviluppo@194.184.235.245 Telecontrollo test@82.106.249.61 user@ZTWS4 vpnbox	Sessione Protocollo file SFTP V Nome server 192.168.85.103 Nome utente user Salva	Password	Nume	ro po <u>r</u> ta 22 ate	
S <u>t</u> rumenti ▼ Gestisci ▼	Accedi ▼	Chiudi		Aiuto	

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.

🌆 user - user@192.168.85.103 - WinSCP										-		×
Locale Seleziona File Comandi Sessione O												
a Coda - I III 🗮 🛱 Sincronizza 🔲 🖓			Impostazioni trasferim	ento Prede	finito	• 1 🚑 •						
urer@192.158.85.103												
Vuova sessione									•			
🗄 Documenti 🔹 🚰 🔽 🖛 🖛 🗏		i î 🖉 🍾				user 🔹 📴 🔽		👔 💞 🔯 Trova file	4 <u>0</u>			
🛛 🕼 Upload 👻 📝 Modifica 👻 🚮 🕞 Pr	oprietà 😁					📲 Download 👻 📝 Modifica 👻	🗙 🛃 🕞 Proprietà 🖆					
C:\Users\Spagiari\Documents						/disk/pages/user						
Nome	Dimensi	Tipo	Modificato	Attr	^	Nome	Dimensi	Modificato	Diritti	Proprietario		
t. ,		Cartella superi	23/12/2016 11.04.47	r		€		16/01/2017 09.43.41	DVXDVXT-X	root		
Adf lighting		Cartella di file	27/04/2016 09.05.43									
Azienda		Cartella di file	23/12/2016 11.04.14									
Bluetooth Folder		Cartella di file	15/11/2013 07.46.42									
Boards		Cartella di file	24/06/2016 13.54.46									
Bug 1474 – Etc GMT Timezones misplaced		Cartella di file	22/11/2013 18.19.50									
CaseHistory		Cartella di file	07/10/2016 13.12.38									
Codesys		Cartella di file	07/10/2014 11.07.56									
Copalp		Cartella di file	05/03/2014 12.14.09									
CPU_Linux		Cartella di file	23/12/2016 11.33.53									
Crickets		Cartella di file	15/04/2015 15.38.59									
Downloaded Installations		Cartella di file	29/03/2016 09.52.49									
File di Outlook		Cartella di file	18/01/2017 09.21.16									
Freescale		Cartella di file	29/10/2014 17.43.51									
Gara_Pubbliacque		Cartella di file	24/11/2016 07.33.24									
Huawei		Cartella di file	30/01/2015 10.21.17									
HW		Cartella di file	01/06/2016 13.20.27									
📧 Immagini		Cartella di file	25/07/2016 18.42.40	sh								
JMobile Suite		Cartella di file	12/09/2014 17.17.37									
- Manuali		Cartella di file	01/09/2016 10.49.25									
MQX		Cartella di file	13/01/2017 15.52.36									
🕽 Musica		Cartella di file	25/07/2016 18.42.40	sh								
NAT with Linux and iptables - Tutorial (Intr		Cartella di file	26/03/2014 13.41.54									
Oldies		Cartella di file	13/03/2015 14.07.57									
OPC_Server_IO		Cartella di file	26/08/2016 09.59.37									
OpenEmbedded		Cartella di file	10/09/2014 12.23.41									
OpenSIPS		Cartella di file	14/12/2015 13.57.38									
🔄 Origini dati utente		Cartella di file	04/11/2015 07.43.41	s								
Processo Sviluppo		Cartella di file	12/01/2015 10.26.13		~	<						>
0 B di 886 KB in 0 di 88						0 B di 0 B in 0 di 0						
									🔒 SF	ТР-З 🔍	0.0	0.16

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.

<u>Gateway</u>: a device that acts as a portal between two programs allowing them to share information by communicating between different protocols.

<u>Serial Device Server</u>: 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.

<u>Router</u>: a networking device that forwards data packets between computer networks, e.g. between a LAN and a WAN (the Internet).

<u>Switch</u>: 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.

<u>VPN</u>: 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.

<u>Tunnel</u>: 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.