Alleantia
ALL <THINGS> JOINED

IOT SCADA SERVER
INSTALLATION AND USER MANUAL


Alleantia
ALL <THINGS> JOINED

Index

1 Introduction.....11

2 IOT SCADA SERVER hardware.....12
2.1 General characteristics.....12
2.2 Models.....12
2.3 Scheme and pinout.....13
2.3.1 LED Functionality.....14
2.3.2 Reset.....15
2.3.3 Backup batteries.....15
2.3.4 Dip Switch.....16

3 IOT SCADA SERVER Installation.....17
3.1 Wiring.....17
3.1.1 Power supply.....17
3.1.1.1 UPS Standard Version.....18
3.1.1.2 UPS Multi Version.....18
3.1.2 Analog inputs.....19
3.1.2.1 Analog voltage inputs.....19
3.1.2.2 Analog current inputs.....20
3.1.3 Digital inputs.....20
3.1.4 Current inputs.....21
3.1.5 Temperature inputs.....21
3.1.6 Relay outputs.....22
3.1.7 PNP outputs.....22
3.1.8 RS485 port.....23
3.2 Connection examples.....24
3.2.1 Environmental sensors connection.....24
3.2.2 Meters connection.....24
3.2.3 Meters connection with reed pulsed output.....25
3.3 Hardware extensions.....25
3.3.1 Wiring of RS485 network.....25
3.3.2 Use of USB-serial converters.....26
3.3.3 Use of Wi-Fi – serial converters.....26
3.3.4 Use of MODBUS Ethernet-serial converters.....26

4 ISS switching on and access.....27
4.1 Switching on/off.....27
4.1.1 Switching on.....27

Index

4.1.2 Switching off and restart....27
4.2 Local access....27
4.3 Wi-Fi access....28
4.4 Ethernet LAN access....28
4.4.1 Direct connection to a PC....28
4.4.1.1 Configuration for Windows XP....29
4.4.1.2 Configuration for Windows 7 system....32
4.4.2 Connection to an existing LAN network....35

5 Configuration....36
5.1 Communication....36
5.1.1 TCP/IP Configuration....36
5.1.2 Connection to an existing Wi-Fi network....37
5.1.3 Internet communication test....37
5.1.4 4.3 Port and communication parameters configuration....38
5.1.5 Modbus Gateway....39
5.1.5.1 Rules of automatic mapping....39
5.2 Installation....40
5.2.1 Configuration and use of IOT SCADA SERVER's I/O....40
5.2.1.1 Configuration of inputs and outputs....41
5.2.1.2 Use of IOT SCADA SERVER....42
5.2.2 System devices configuration....43
5.2.2.1 Adding new devices....43
5.2.2.2 Removing a device....45
5.2.2.3 Installation support manuals....46
5.2.3 Devices measures setup....46
5.2.3.1 Measures offset....47
5.2.3.2 Measures scaling....48
5.2.4 General settings....48
5.2.5 Password change....49
5.3 Customization....50
5.3.1 Logos and title....50
5.3.2 Custom measures....51
5.3.3 Custom alarms....52
5.3.4 Synoptics configuration....56
5.4 Interface and Cloud services....60
5.4.1 E-mail and SMS notifications....60
5.4.2 Dropbox connection....61
5.4.3 OneDrive account....65

Index

5.4.4 FTP Backup....66
5.4.4.1 Details of the transferred files....67
5.4.5 Connection to SQL Server....68
5.4.6 Connection to Azure IoT Hub....69
5.5 Information....71
5.5.1 Device catalogue....71
5.5.2 Licence management....72
5.5.3 Information....73
5.5.4 Logs....73

6 User interface....74
6.1 Synoptics....74
6.2 Devices....75
6.2.1 System measures display....75
6.2.1.1 Data and alarms display....76
6.2.2 Graphs....76
6.2.3 Measure write....78
6.2.4 Exporting data to Excel....79
6.3 Alarms....80
6.4 Alarms history....81
6.5 Energy reports generation....83
6.6 Documents....85
6.7 Favourites....86

7 Troubleshooting – FAQ....87
7.1 IOT SCADA SERVER does not switch on....87
7.2 Unable to complete the Internet communication test....87
7.3 Communication problems with serial devices....87
7.4 Unable to access IOT SCADA SERVER from the local network....87
7.5 Unable to access IOT SCADA SERVER from the Internet....87

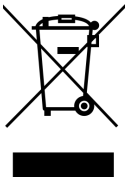
8 Contacts....88
Alleantia s.r.l....88
http://www.alleantia.com....88
info@alleantia.com....88

CE

ALLEANTIA hereby confirms that its products listed below are compliant to the following EUROPEAN EEA DIRECTIVES:

- EMC 2004/108/CE
- EN 300
- EN 301
- EN 50385 / 62311
- EN 55022
- EN 60950
- 2002/95/EC, 2011/65/EU (RoHS, RoHS2).

Waste Electronic Equipment



Electrical and electronic equipment with this symbol cannot be disposed in public landfills. In accordance with Directive 2002/96/EC, European users of electrical and electronic equipment have the possibility to return used equipment to Distributor or Manufacturer when purchasing a new one.

IoT SCADA Server and IoT Gateway Server Family

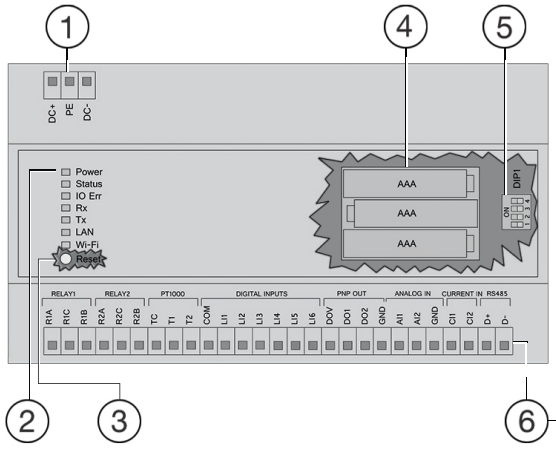
Safety Precautions

mm / in	6 / 0.24	
mm^2		4,0...0,14
AVG		12...28

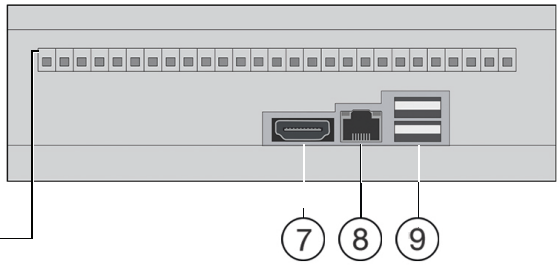
Ø 3 mm (0,14 in)		
c	N.m	0,40
	lb-in	3,5

Use only copper conductors

Top View



Front View



1 - Power supply screw terminal

2 - Controller and I/O status Leds

3 - Power Reset Button ∗

4 - Battery holder ∗

5 - Dip Switch ∗

6 - I/O screw terminal block

7 - USB 2.0 expansion ports

8 - Gb LAN port

9 - HDMI video output

∗ Accessible after removing the front cover

⚠⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION ORARC FLASH

- Power down all equipment before starting the installation, removal, wiring, maintenance or inspection of the product.
- Replace and secure all covers, accessories, hardware, cables, wires and confirm that a proper ground connection exists before applying power to the unit.
- Use only the specified voltage when operating this equipment and any associated products.
- Press the “Reset” button after supply disconnection until the “Power” LED off.

Failure to follow these instructions may result in death or serious injury.

Electrical equipment should be installed, operated, serviced and maintained only by qualified personnel.
No responsibility is assumed by Alleantia S.r.l. for any consequences arising from misuse of this material.

⚠ WARNING

POTENTIAL OF OVERHEATING AND FIRE

- Do not connect the modules directly to line voltage.
- Use only isolating PELV or SELV power supplies to supply power to the modules .

Failure to follow these instructions can result in death, serious injury or equipment damage.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- This product is not intended to be used for safety critical machine functions. Where personal and or equipment hazards exist, use approved hard-wired safety interlocks.
- Do not disassemble, repair or modify the modules.
- This product is designed for use within an enclosure.
- Install the modules in the operating conditions described in the user manual, section “INSTALLATION”.
- Use the sensor power supply only for supplying power to sensor connected to the module.
- For power line and output circuits, use a fuse designed to Type T standards per IEC60127. The fuse must meet the circuit voltage and current requirements.

Failure to follow these instructions can result in death, serious injury or equipment damage.

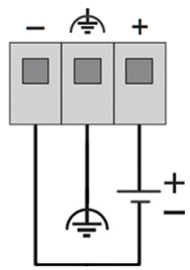
⚠ WARNING

RISK OF EXPLOSION IN HAZARDOUS LOCATIONS

- Install this equipment only in Class 1, Division 2, Groups A, B, C and D or non-hazardous locations only.
- Substitution of components may impair suitability for Class 1, Division 2 compliance.
- Do not disconnect equipment unless power has been switched off or the area is know to be non-hazardous .

Failure to follow these instructions can result in death, serious injury or equipment damage.

POWER SUPPLY



I•S_1•1_•••

⎓ 12 VDC
– 2%
+ 10%

I•S_1•3_•••

⎓/∼
12 - 24 VDC
15 - 26 VAC

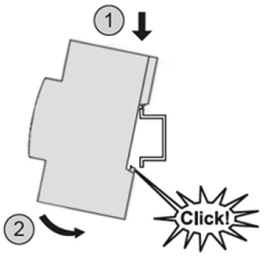
Power supply wiring should be as short as possible.

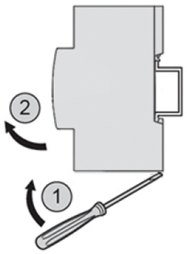
Connect ground as close as possible to plate.

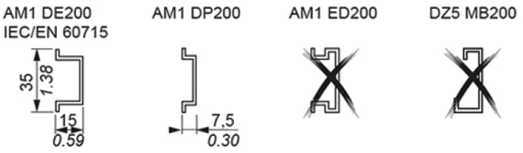
Respect the voltage level for the particular model.

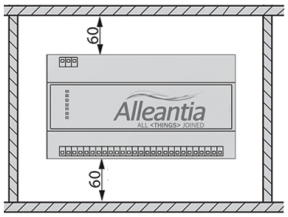
Getting started

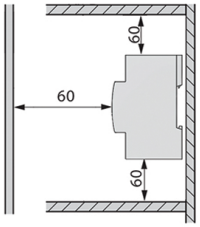
INSTALLATION









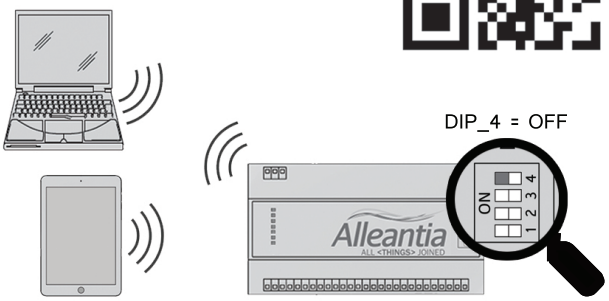


IOT SERVER ACCESS WITH WI-FI ACCESS POINT

Wi-Fi network name (SSID): IoT-SCADA

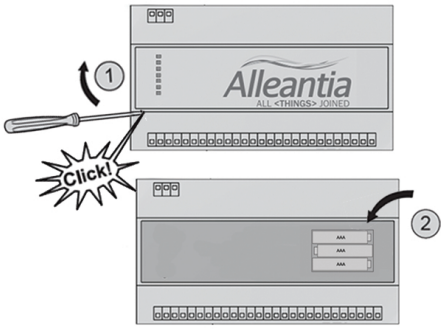
Password Wi-Fi: IoTSCADAwifi

Address IP: http://10.10.0.1



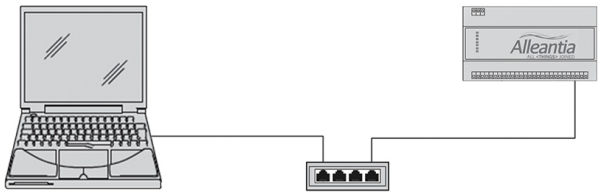
BATTERIES INSTALLATION

Open the cover after removing the power supply and waiting 10 seconds.



Use only rechargeable 3x batteries AAA NiMH ≥ 1000 mAh

IOT SERVER ACCESS WITH LAN CABLE



DEFAULT CONFIGURATION

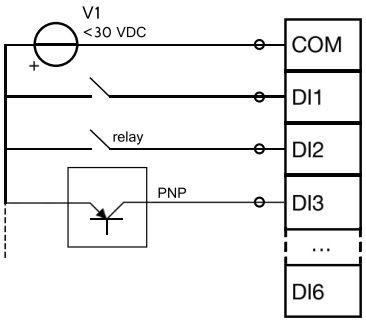
IP address: 192.168.1.29

Subnet mask: 255.255.255.0

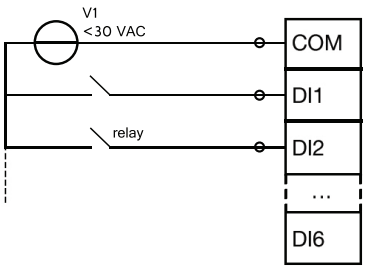
Gateway: 192.168.1.1

CONFIGURATION PROTECTED WITH AUTHENTICATION:
USER: admin
PASSWORD: webloggerSU
We suggest to change password immediately after installation.

Digital inputs (DC)

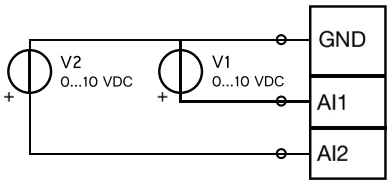


Digital inputs (AC)

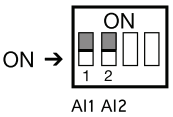


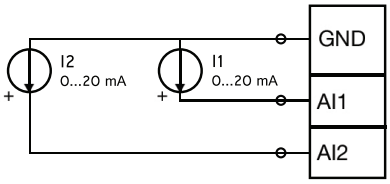
Analogue inputs (individually configurable)

Voltage

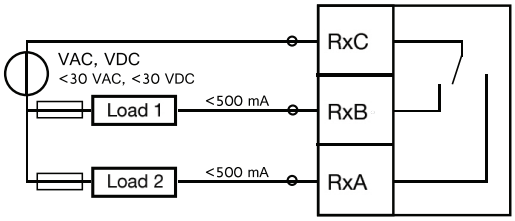


Current

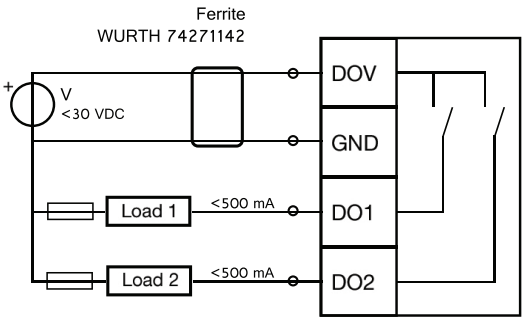




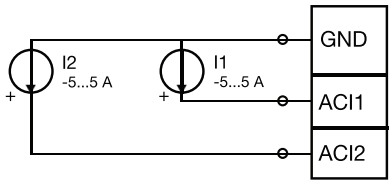
Digital Outputs (Relay)

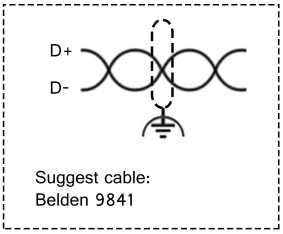


Digital Outputs (PNP)



Current inputs





RISK OF REVERSE-POLARITY DAMAGE ON PNP DIGITAL OUTPUTS

- Make sure to comply with the polarity markings on the transistor output terminals.
- Use of a reverse polarity can permanently damage or destroy the output circuits.

D-I•S-1015-IT

1 Introduction

This manual is intended for installation, configuration and use of software + integrated software systems Alleantia IOT GATEWAY SERVER (product codes IGS_XXX_YY) and IOT SERVER (product codes ISS_XXX_YY).

Configuration description and use of the systems will always refer to IOT SCADA SERVER, but the same operations can be carried out on IOT GATEWAY SERVER systems, which uses identical hardware (IOT SCADA SERVER).

2 IOT SCADA SERVER hardware

2.1 General characteristics

IOT SCADA SERVER is a miniaturized industrial minicomputer, designed to connect into one small object (9 DIN modules) devices of any type and most common interfaces, to build plug & play Industrial Internet of Things / Industry 4.0 solutions for monitoring and control of systems, industrial plants, machinery and communication with applications and other systems.

IOT SCADA SERVER features:

- 6 digital inputs, 2 analog inputs, 2 temperature inputs, 2 current input;
- 2 relay outputs, 2 PNP digital outputs;
- 1 RS485 port;
- 2 USB ports for peripheral and extensions connections;
- 1 HDMI port;
- 1 Ethernet port;
- Wi-Fi module;
- Power supply 12 VDC or 12-24VDC / 15-26 VAC (optional) with integrated UPS.

2.2 Models

IOT SCADA SERVER and IOT GATEWAY SERVER share the same hardware, while implementing different functions.

2 models are available according to the type of power supply. Depending on the model the power supply can accept a single voltage value (12 VDC) or multiple values (12-24 VDC, 15-26 VAC). The Integrated Mini UPS (using 3 AAA rechargeable batteries) provides few minutes of autonomy in case of power failure.

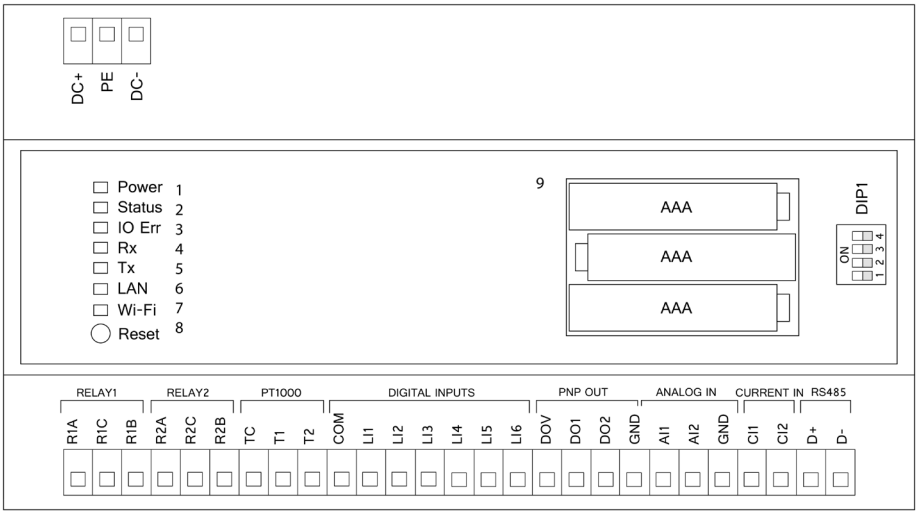
UPS: Power supply 12 VDC, Mini UPS functionality (codes ISS_1x1_ZZZ, IGS_1x1_ZZZ);
Multi+UPS: Power supply 12-24 VDC, 15-26 VAC, Mini UPS functionality (codes ISS_1x3_ZZZ, IGS_1x3_ZZZ).

For each model, 2 versions differ in the features available on the I/O:

- **Standard** (codes ISS_10x_ZZZ, IGS_10x_ZZZ);
- **Impulse counter** (codes ISS_11x_ZZZ, IGS_11x_ZZZ);

2 IOT SCADA SERVER hardware

2.3 Schema and pinout



DC+	Power supply (positive)	**LI3**	Digital input 3
PE	Earth	**LI4**	Digital input 4
DC-	Power supply (negative)	**LI5**	Digital input 5
R1A	Relay 1, normally open contact	**LI6**	Digital input 6
R1C	Relay 1, common contact	**DOV**	Digital outputs, common terminal (positive)
R1B	Relay 1, normally closed contact	**DO1**	Digital output 1 (PNP)
R2A	Relay 2, normally open contact	**DO2**	Digital output 2 (PNP)
R2C	Relay 2, common contact	**GND**	Common for digital outputs and analog inputs
R2B	Relay 2, normally closed contact	**AI1**	Analog input 1
TC	Common for the temperature inputs	**AI2**	Analog input 2
T1	Temperature input 1 (Pt 1000)	**GND**	Common for the current inputs
T2	Temperature input 2 (Pt 1000)	**CI1**	Current input 1
COM	Digital input, common terminal (negative)	**CI2**	Current input 2
LI1	Digital input 1	**D+**	RS485 A+
LI2	Digital input 2	**D-**	RS485 B-

DIP1: 1	Type of analog input 1	OFF = 0 .. 10 VDC	**1**	Power LED (Green/Red)	
		ON = 0 .. 20 mADC	**2**	Status LED (Green/Orange)	
DIP1: 2	Type of analog input 2	OFF = 0 .. 10 VDC	**3**	Communication error LED (Red)	
		ON = 0 .. 20 mADC	**4**	Data receiving LED RS485 (Yellow)	
DIP1: 3	Termination resistor RS485	OFF = Disconnected	**5**	Transmitting data LED RS485 (Yellow)	
		ON = Connected	**6**	LAN status LED (Green/Orange)	
DIP1: 4	Wi-Fi mode	OFF = Access Point	**7**	Wi-Fi status LED (Green/Orange)	
		ON = Client	**8**	Reset button	* accessible under battery holder lid
			9	Battery holder	* accessible under battery holder lid

2.3.1 LED Functionality

On the front panel 7 LED indicators are located. From top to bottom:

- LED **Power**: indicates the power supply status.

Colour	Description
Off	IOT SCADA SERVER is off
Green	External power connected and active
Red	External power not connected or not appropriate, internal UPS active

- LED **Status**: indicates the status of system activity

Colour	Description
Green blinking	IOT SCADA SERVER starting
Green steady	IOT SCADA SERVER turned on
Orange blinking	IOT SCADA SERVER shutting down

- LED **IO Error**

Colour	Description
Off	No problem found
Red	Communication problems with at least one device configured in the web interface

- LED **Rx**

Colour	Description
Yellow (blinking)	Received the serial communication packages RS485 of the IOT SCADA SERVER's terminal block

- LED **Tx**

Colour	Description
Yellow	Transmitted the serial communication packages RS485 of the IOT SCADA SERVER's terminal block

- LED **LAN**

Colour	Description
Green	LAN cable connected
Orange	LAN cable disconnected

- LED **Wi-Fi**

Colour	Description
Green	Wi-Fi active and correctly configured (Access Point or Client)
Orange	Wi-Fi inactive (off or not properly configured)

2.3.2 Reset

The reset button is accessible under the front panel. Press to shut down/restart the system as described in Section 4.1.

CAUTION: READ SECTION 4.1 BEFORE USE OF THE RESET BUTTON.

2.3.3 Backup batteries

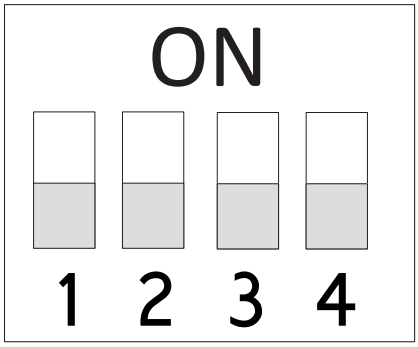
The backup batteries are accessed by removing the front panel of the IOT SCADA SERVER. We recommend the use of a sharp, non-metallic instrument to lift and remove the front panel. The battery holder accepts 3 **RECHARGEABLE** AAA size batteries**, preferably from 1000 mA each**, NiMH.

CAUTION: use ONLY rechargeable batteries. The use of non-rechargeable batteries can cause SERIOUS DAMAGE to people and equipment.
CAUTION: observe the polarity marked on the battery compartment. Failure to do so may result in SERIOUS DAMAGE to people and equipment.

The batteries are necessary to keep the system's time (RTC) also when power is disconnected. Therefore, if removed or replaced without an external power supply, date and time of the system should be reset as described in section 5.2.4. Batteries are also used to keep the system turned on for a few minutes without an external power supply pending its return and/or to launch the alert to warn user about a power failure. If not present or exhausted (end of life) then the UPS functionality is not exploitable. It is not necessary to recharge the battery outside the system, the IOT SCADA SERVER will do it automatically when powered. It is recommended to periodically check and replace batteries if used in UPS function, considering the number of charge cycles (operating frequency as UPS), power quality to the system and the operating temperature.

2.3.4 Dip Switch

The IOT SCADA SERVER incorporates a Dip Switch next to the battery holder, which can be accessed by removing the front panel.



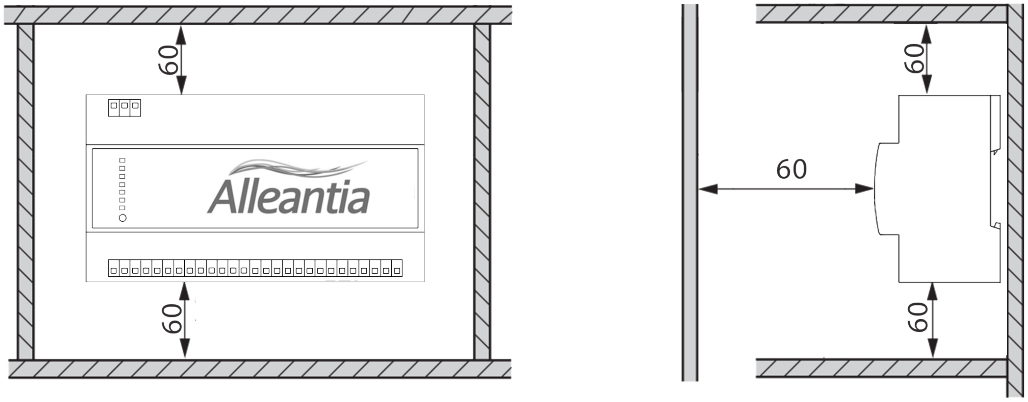
The switches 1 and 2 select two analog inputs: voltage input and current input respectively - see Section 3.1.2. The third switch connects and disconnects the termination resistor of serial RS485 on terminal block - see Section 3.3.1.
The fourth switch changes Wi-Fi mode from Access Point mode (toggle OFF) to Client mode (toggle ON). To access the Access Point please refer to Section 4.3. For setting the parameters of Wi-Fi Client network please refer to Section 5.1.1.

CAUTION:
Changing position of first two Dip Switch's toggles must be done BEFORE wiring analog inputs and must be IOT SCADA SERVER TURNED OFF; DO NOT change their position if the inputs are already connected and active. Failure to do so may cause SERIOUS DAMAGE to the IOT SCADA SERVER.

3 IOT SCADA SERVER Installation

The IOT SCADA SERVER must be installed on DIN rail in a panel with the bottom plate, occupying a 9 modules length. The plate must be in vertical position.

Proper ventilation requires 6 cm distance from other devices above and below the IOT SCADA SERVER.



CAUTION:
Failure to do so may cause overheating and consequently SERIOUS DAMAGE to the IOT SCADA SERVER.

3.1 Wiring

CAUTION:
ALL the wirings MUST ALWAYS BE set up with IOT SCADA SERVER TURNED OFF.

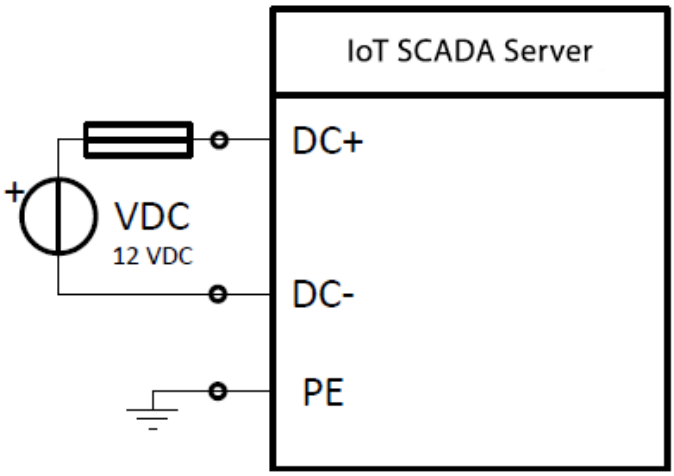
The devices and power suppliers which connect to the IOT SCADA SERVER MUST be turned off.

Any batteries of UPS system of the IOT SCADA SERVER MUST be disconnected.

3.1.1 Power supply

Power supply depends on the IOT SCADA SERVER model. Using a power supply which is able to release at least 15W power e 1.2A current is recommended.

3.1.1.1 UPS Standard Version

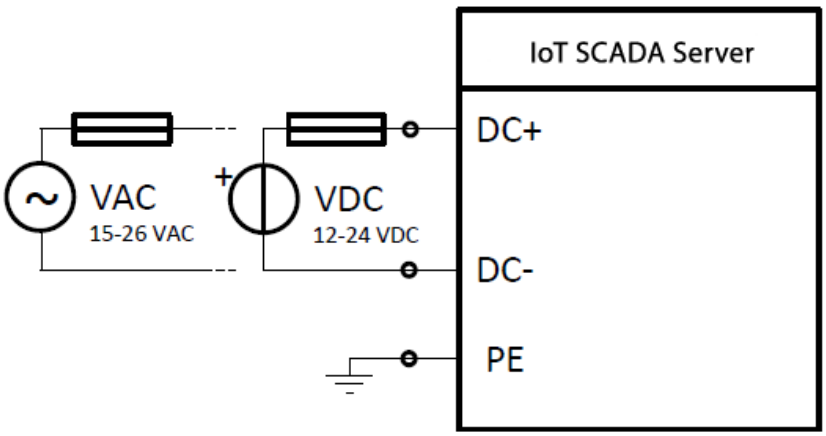


The power supply is 12 VDC and should to be connected to the DC+ and DC- terminals with correct polarity.

CAUTION:
failure to follow the polarity and value of the supply voltage may cause SERIOUS DAMAGE to people and equipment.

Using a fuse (1.5A) in series as short-circuit protection.

3.1.1.2 UPS Multi Version



The power can be supplied in direct current 12 or 24 VDC or in alternate current between 15 and 26 VAC. In both cases, use DC+ and DC-. Polarity connection is not influential for these models. A fuse (1.5 A) in series as short-circuit protection should be used.

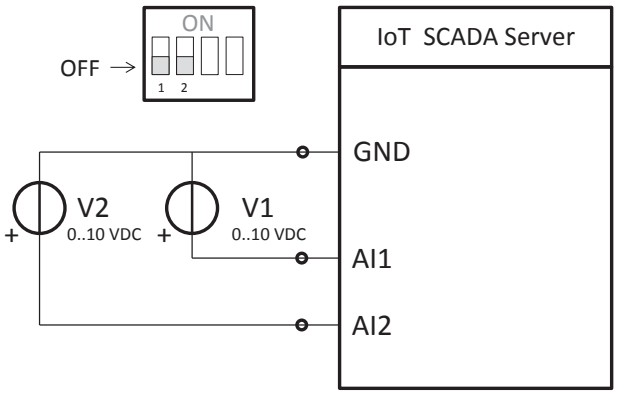
CAUTION:
failure to follow value of the supply voltage may cause SERIOUS DAMAGE to people and equipment.

3.1.2 Analog inputs

Two analog inputs are used for the acquisition of voltage signals (0-10 V) or current (up to 20 mA). For each, the input voltage or current mode is set via the DIP switch toggle located next to the batteries holder of the IOT SCADA SERVER: first toggle controls the first analog input, second toggle controls the second analog input; OFF value (see section 2.3.4) corresponds to a voltage input, ON value corresponds to a current input.

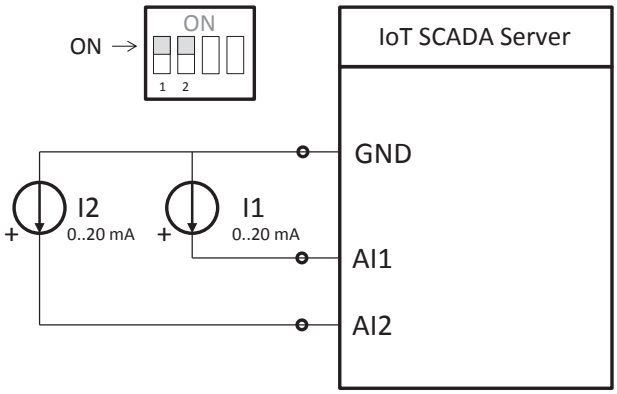
CAUTION:
mode selection using Dip Switch must be done BEFORE wiring the inputs and IOT SCADA SERVER MUST BE TURNED OFF; DO NOT change mode using Dip Switch if the inputs are already connected and active, which may cause damage to the IOT SCADA SERVER.

3.1.2.1 Analog voltage inputs



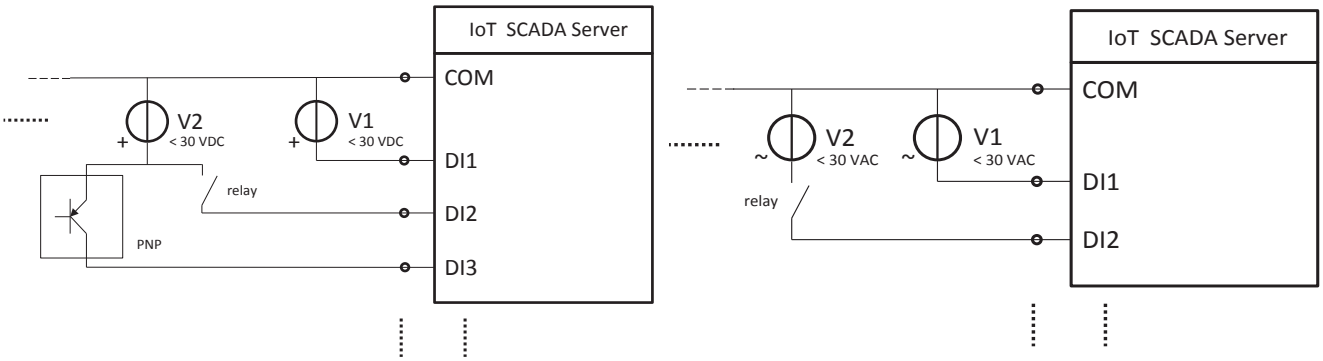
In the voltage mode, each input is able to read values in 0-10 VDC range and withstand over-voltages up to 30 VDC. Furthermore inputs are protected from inverse polarity up to -30 VDC maximum. The connection shall be set up between terminals AI1 (positive) and GND (negative) for the first input and between AI2 (positive) and GND (negative) for the second input.
To avoid malfunctions or inaccurate readings it is necessary to take account the input impedance which in voltage mode is about 200 kΩ. It is recommended to connect only signal sources with output impedance much lower of this value (refer to the datasheet of the connected device).

3.1.2.2 Analog current inputs



In the current mode, each input is able to read values in 0-20 mA range and withstand over-currents up to 35 mA. The input impedance is about 500Ω. Make sure that the device supports such load, otherwise it will cause an invalid current value reading.

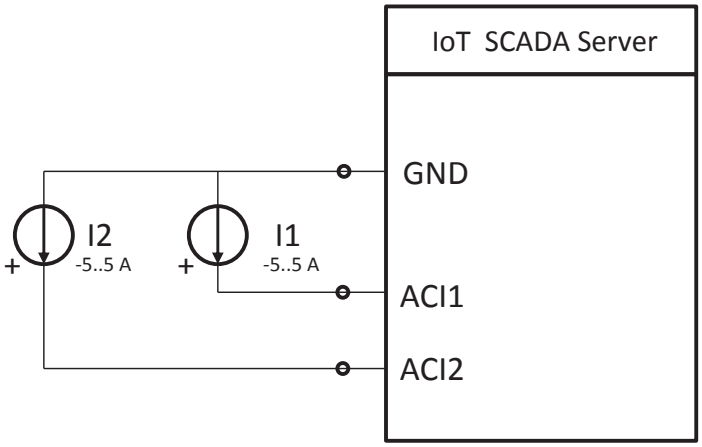
3.1.3 Digital inputs



The six digital inputs have the COM terminal in common. To activate the first input it is necessary to apply at least 9 VDC voltage between LI1 terminal (positive) and COM terminal (negative). Activation of the second input is carried out in a similar way between LI2 and COM terminals and so on for the remaining inputs.

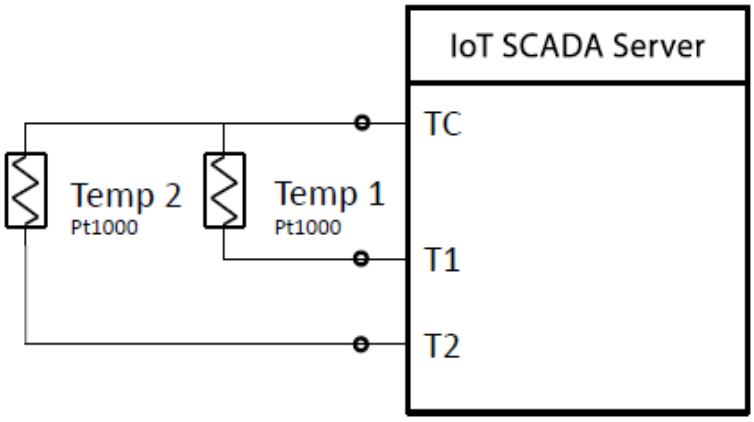
In **standard** version of the IOT SCADA SERVER (codes ISS_10x and IGS_10x) this alternating voltage is interpreted as a valid signal which activates the input.
In **counter** version (ISS_11x, IGS_11x) it is interpreted as a pulse train instead and how these are counted or ignored depending on the selected filter level in the IOT SERVER SCADA software.
The input impedance is higher than 14 kΩ and therefore it is necessary that the connected device is able to supply at least 0.65 mA at 9 VDC or at least 1.75 mA at 24 VDC.

3.1.4 Current inputs



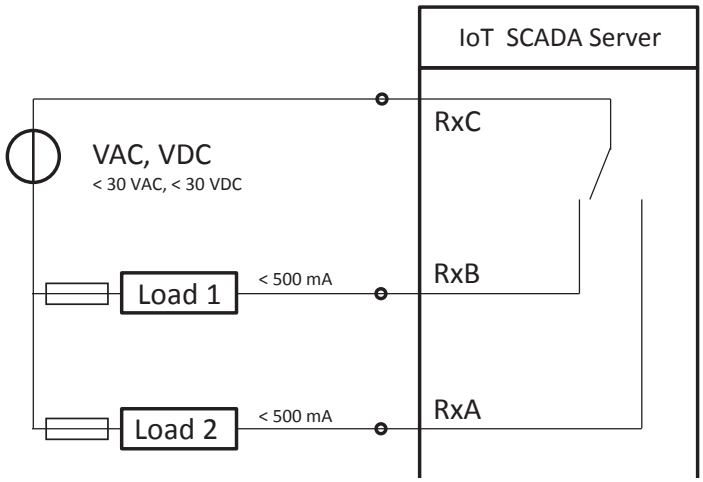
Two current inputs are used to connect current transformers xx/5. The first input connects to CI1 and GND terminals and the second connects between CI2 and GND terminals. The polarity is irrelevant because they are used to measure the rms value of the current.

3.1.5 Temperature inputs



Two temperature inputs connect Pt1000 type temperature probes. The first probe connects to the TC and T1 terminals, the second connects to the TC and T2 terminals.

3.1.6 Relay outputs



Two relay outputs have changeover contacts.

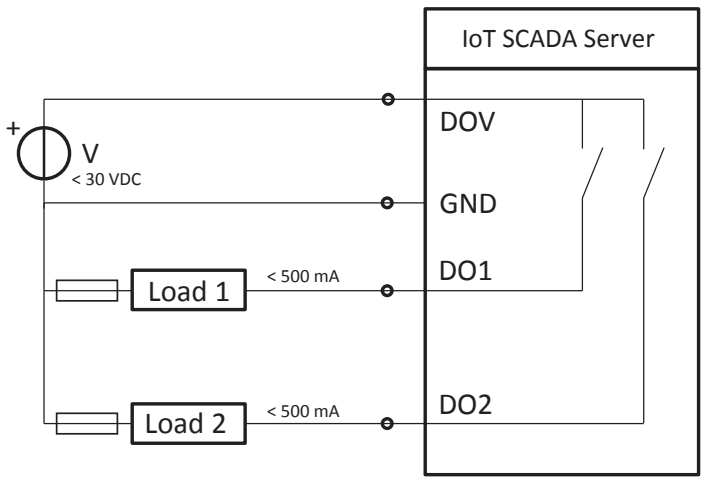
- For relay 1, in idle conditions, R1B and R1C terminals are closed (in short circuit between them) and the R1A terminal is open (floating, electrically disconnected). With active output R1A and R1C terminals are closed (in short circuit between them) and R1B terminal is open (floating, electrically disconnected).
- For relay 2, wiring and functionality are the same, and it is individually controllable.

The load range is 0.5 A at 30 VDC or 0.5 A at 30 VAC. The relay status is defined by software and editable by user.

Fuses from 0.5 A should be used in series to each load as protection from short circuits. In case of inductive loads, it is necessary to provide an appropriate external protection system. For example, in case of inductive load power supply with direct current voltage, it is necessary to insert a snubber diode antiparallel to the load itself, ensuring to place the diode cathode on the higher voltage so that it is blocked during normal operation.

CAUTION:
the use of a snubber diode connected in a wrong way may cause SERIOUS DAMAGE to people and equipment.

3.1.7 PNP outputs



Two PNP outputs are used to supply loads with variable voltage up to 30 VDC, 0.5 A maximum per channel. The connection is made by supplying external DC supply between DOV (positive) and GND (negative) terminals and connecting the first load between DO1 (positive) and GND (negative) and the second between DO2 (positive) and GND (negative).

The state of the outputs is defined by software and editable by user. The active output supplies the load with the current drained from DOV. The inactive output is in a passive state when it acts an internal pull-down resistor to GND.

Fuses from 0.5 A should be used in series to each load as protection from short circuits. In case of inductive loads, it is necessary to provide an appropriate external protection system, as described in Section 3.1.6.

Finally, to limit electromagnetic emissions within the normal limits a ferrite should be used on the pair of DOV - GND power cables. This ferrite should be placed on the cables close to the ISS terminals. Use of the following or similar product is recommended:

Manufacturer	Model
WURTH ELECTRONICS	74271142

3.1.8 RS485 port

The RS485 serial port has two terminals D + and D- and works in half-duplex. The line is NOT optically isolated and is internally polarized with a resistor network (failsafe).

The third toggle of Dip Switch located next to the battery holder (see Section 2.3.4) inserts (if ON) an integrated terminating resistor for the line. This resistance is coupled in frequency and is not a continuous load for the line.

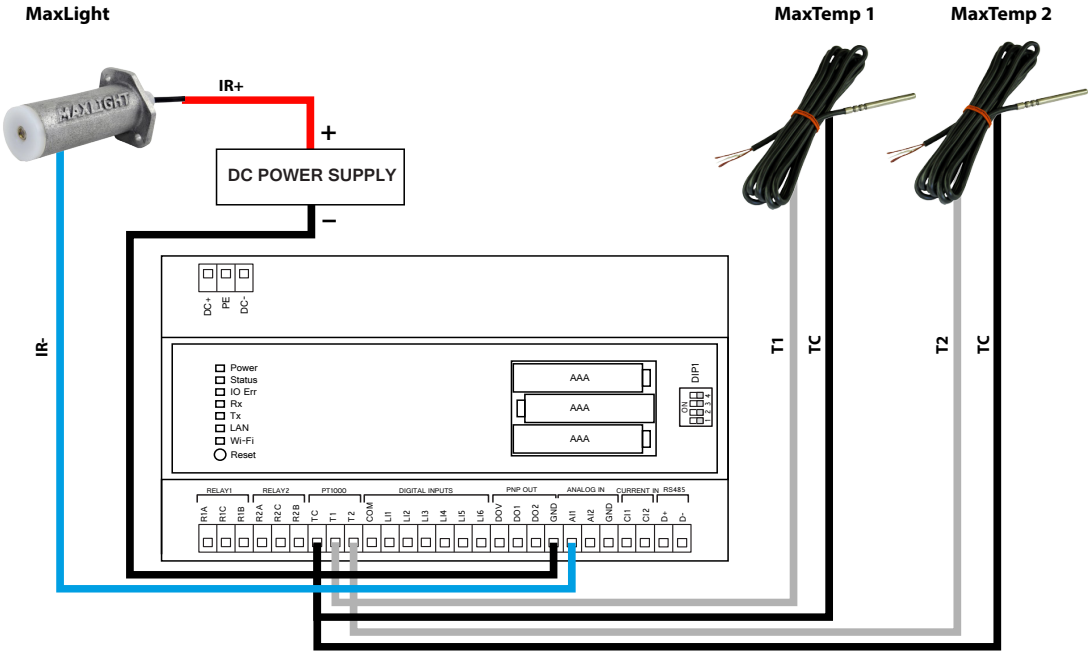
For wiring of the serial line please refer to Section 3.3.1.

3 IOT SCADA SERVER Installation

3.2 Connection examples

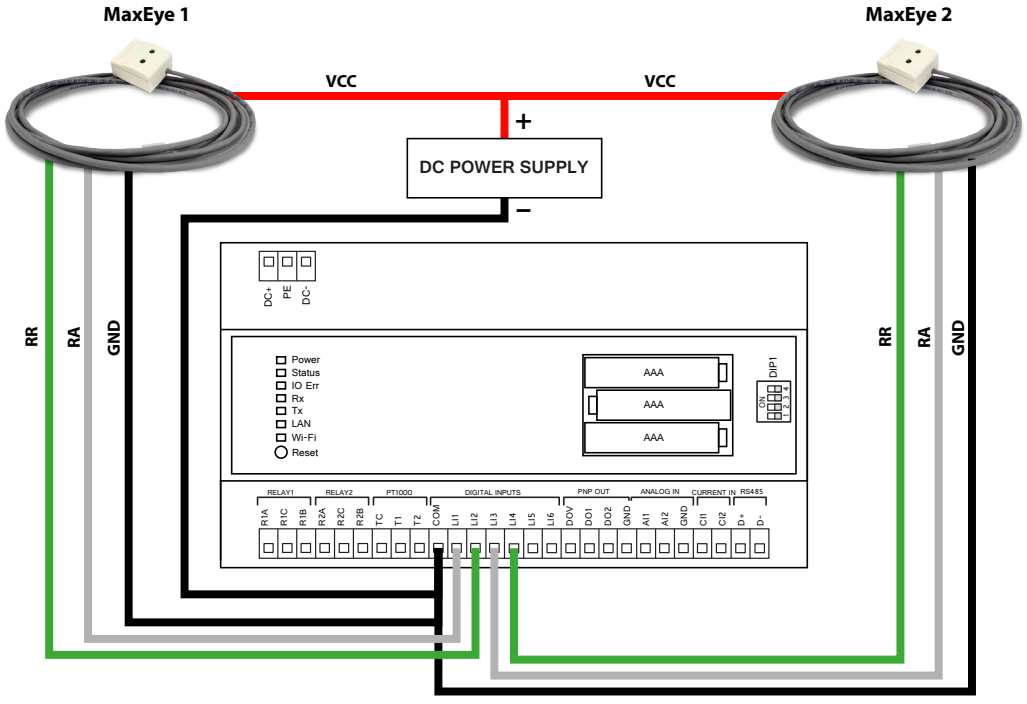
3.2.1 Environmental sensors connection

Examples of MaxLight environmental sensors connection (radiation, current sensor 4-20 mA) and MaxTemp (temperature, Pt1000).



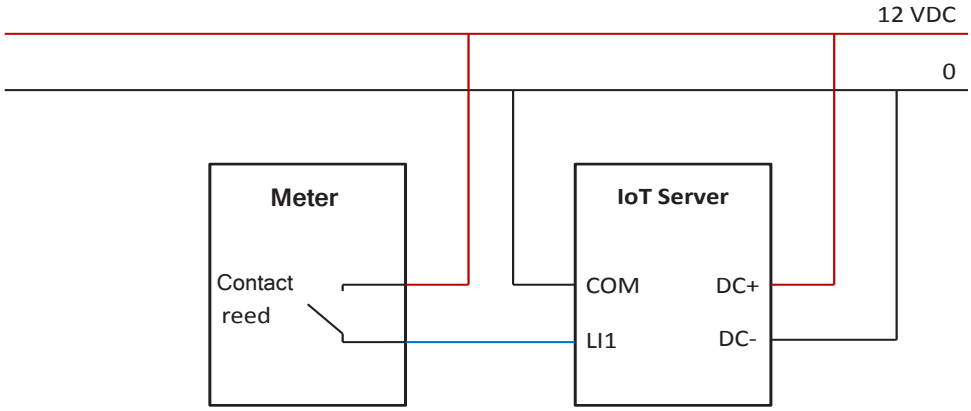
3.2.2 Meters connection

Connection examples of two MaxEye for reading the monodirectional meters



3.2.3 Meters connection with reed pulsed output

Example of connection to a meter with reed output to ISS digital input.



3.3 Hardware extensions

3.3.1 Wiring of RS485 network

There are a few simple rules that make RS485 serial connection reliable.

- The cable used must be shielded, with the shield grounded **at one end only**.
- Star configurations are not allowed. Only linear ones are, as shown in Figure 1. The line should be terminated at the end (the master, or the IOT SCADA SERVER, is not necessarily at an end of the line) with a suitable resistance which can often be inserted by means of a selector switch on the devices themselves. If the non-optically isolated RS485 serial port on the IOT SCADA SERVER is used, the internal termination (with the third toggle of internal Dip Switch) could be used to make the ISS the last element of the line.

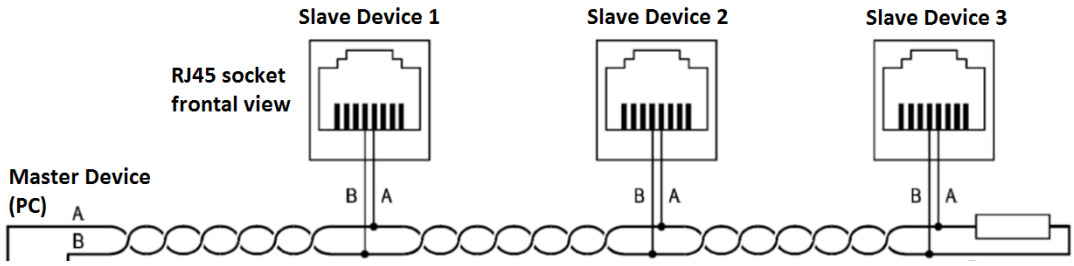


Figure 1 - RS485 wiring diagram

- A separate communication line must be set up for each communication protocol used in the system. For example, if you have network analysers that use Modbus RTU and inverters that use a proprietary protocol (e.g. ABB – PowerOne), you will need two separate cables and an equal number of RS-485 ports.

Additional information can be found in the troubleshooting guide in the section “Installation” -> “Devices configuration” that can be downloaded by pressing the button:

3.3.2 Use of USB-serial converters

Should you need to use multiple serial communication lines, or should you prefer to have an external opto-isolator (e.g. to connect long serial lines externally), a converter with TRP-C08 interface must be used.

These converters are optically isolated (up to 3 kV) and provide extra protection against overloads and EMC interference comparing to integrated RS485. They are absolutely necessary when the RS485 serial cable is deployed outside, and is therefore exposed to lightning.

To use these converters simply connect them to IOT SERVER with a special USB cable and carry out the serial ports detection procedure described in section 5.1.4.

3.3.3 Use of Wi-Fi – serial converters

It is possible to use the wireless network created by the Access Point of the IOT SCADA SERVER to connect serial Wi-Fi converters. These converters are used as a wireless bridge between the IOT SCADA SERVER and serial devices and might be useful in case of problems with laying of serial cables. For correct configuration of the converter and connection to wireless network of the IOT SCADA SERVER (Section 4.3) please refer to converter's user guide. Once a static address is assigned to the converter (e.g. 10.10.0.100), you can access the web interface and proceed with the configuration of serial devices (Section 5.2.2). These devices will be connected to the "Ethernet" port with the static address of the converter (e.g. 10.10.0.100). If you are using the Modbus protocol it is required to enable encapsulation of the Modbus RTU protocol on TCP ticking the checkbox at the bottom line of the created device (Section 5.2.2, Figure 9).

3.3.4 Use of MODBUS Ethernet-serial converters

The Ethernet Serial converters for the Modbus protocol are devices that not only change the physical transmission medium, but also perform the additional functions of converting the protocol from Modbus TCP / IP to Modbus RTU. So the IOT SERVER will have access to the devices downstream of these converters configuring them as directly connected to the Ethernet interface.

CAUTION:
Ethernet Serial converters cannot be used for protocols other than Modbus.

4 ISS switching on and access

4.1 Switching on/off

4.1.1 Switching on

The IOT SCADA SERVER turns on automatically as soon as it is connected to the power supply. With the external power supply the Power LED turns on with green light. After that, the Status LED blinks with green to signal that the IOT SCADA SERVER is starting. When this LED stops blinking and becomes steady green then the system is ready for use. If the system has already been configured, from that moment on you can begin to interrogate the devices.
If the batteries have been changed or inserted, it might be necessary to set system date and time as described in section 5.2.4. Specifically, if “inactive licence” pop up appears, check date and time in the lower left corner: if values are very different from the actual ones (e.g. 1970 year) they should be reset (section 5.2.4) with system restart (see following sections).

4.1.2 Switching off and restart

After disconnection of the external power supply the UPS will take over, keeping the system on for few minutes, drawing energy from the batteries. If the external power supply is not restored within few minutes, the system will shutdown automatically and only Power LED will be lit red. Pressing the reset button for 3 seconds will turn off the system completely.
To shutdown the system fast you should disconnect the external power supply (the Power LED will turn red), quickly press the reset button (the Status LED blinks orange), wait a few minutes until the Status LED turns off and then press the reset button for 3 seconds (all LEDs will turn off).

To force shutdown you need to disconnect power supply and then press the reset button for 3 seconds (all the LEDs ill turn off).

To restart the system (with active external power supply) you need to quickly press the reset button and wait a few minutes until the Status LED becomes steady green.

4.2 Local access

By connecting a monitor with HDMI interface and a USB mouse and keyboard to USB ports of the IOT SCADA SERVER, it is possible to proceed with the configuration described in the following sections without using another terminal.

4.3 Wi-Fi access

If the Dip Switch toggle n°4 of the IOT SCADA SERVER is OFF (Section 2.3.4), then Wi-Fi is in Access Point mode and a wireless network will be created with the following parameters:

Wi-Fi (SSID) network name: IoT-SCADA
Password: IoTSCADAwifi

Once connected, access the web interface of the IOT SCADA SERVER using the preferred internet browser and typing the URL in the address bar:

http://10.10.0.1

CAUTION:
The Wi-Fi network connects exclusively to the IOT SCADA SERVER to display its configuration interface. For security reasons, it is not possible to access any other devices connected to the IOT SCADA SERVER via the wired LAN network.

4.4 Ethernet LAN access

IOT SCADA SERVER default Ethernet LAN configuration is as follows:

IP address: 192.168.1.29
Subnet mask: 255.255.255.0
Gateway: 192.168.1.1
DNS 1: 208.67.222.222
DNS 2: 208.67.220.220

The DNS are necessary for the remote support connectivity.

It is also possible to use USB-Ethernet adaptor to connect the device to Ethernet LAN. Plug&Play connection; the settings can be found in *"Configuration TCP/IP"* tab.

4.4.1 Direct connection to a PC

This procedure requires a direct link (point to point) to a PC via an Ethernet cable, **not necessarily twisted**. The network configuration of the PC connecting to the ISS must be:

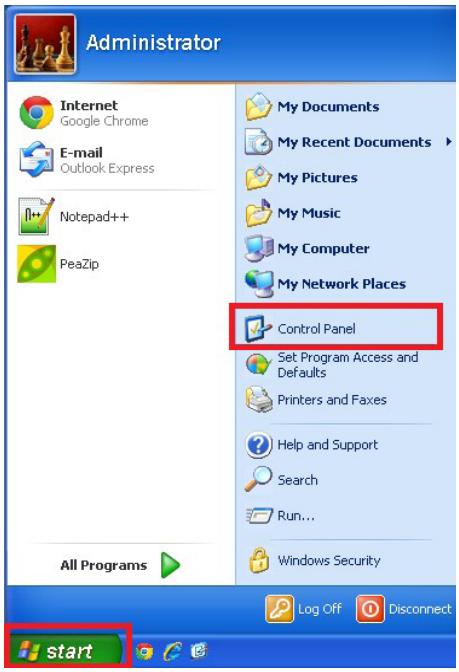
- **192.168.1.nnn** Static IP (with n between 2 and 254, with the exception of 29, which is already used by IOT SCADA SERVER)
- subnet mask **255.255.255.0**

Then, it will be possible to access the web interface of the IOT SCADA SERVER using the preferred internet browser and entering the following URL in the address bar:

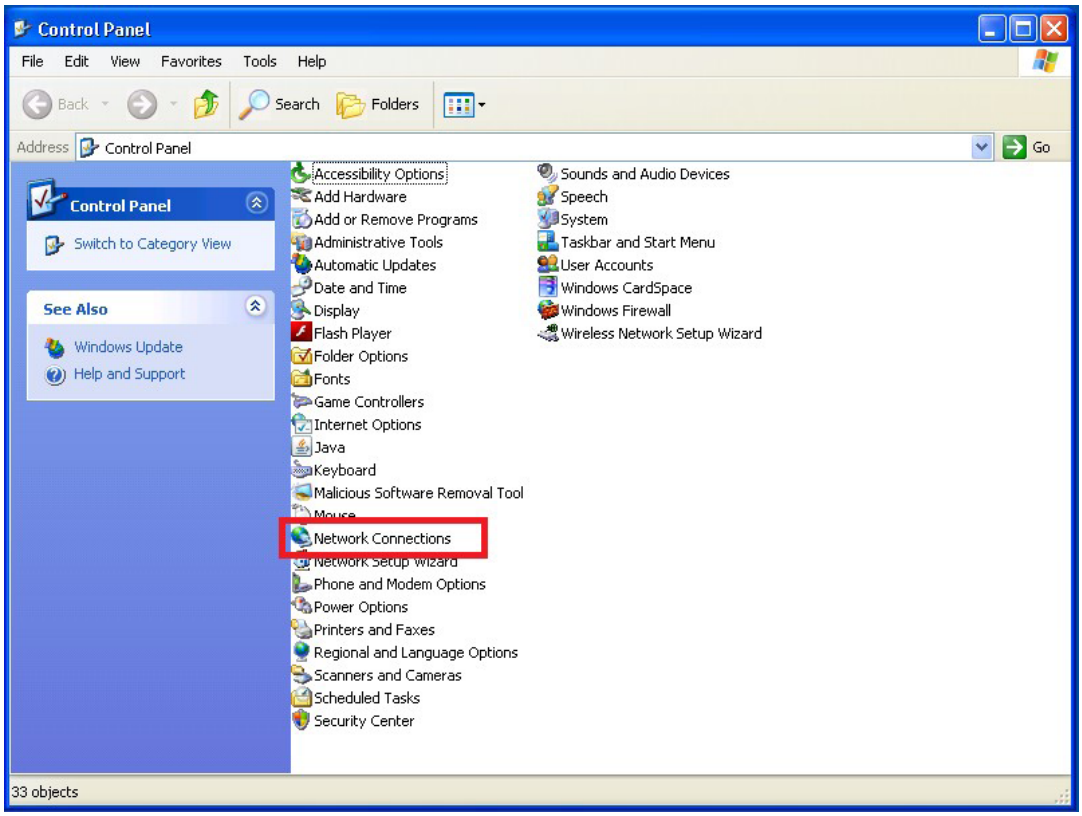
http://192.168.1.29

4.4.1.1 Configuration for Windows XP

Access the *"Start"* menu and then click on *"Control panel"*

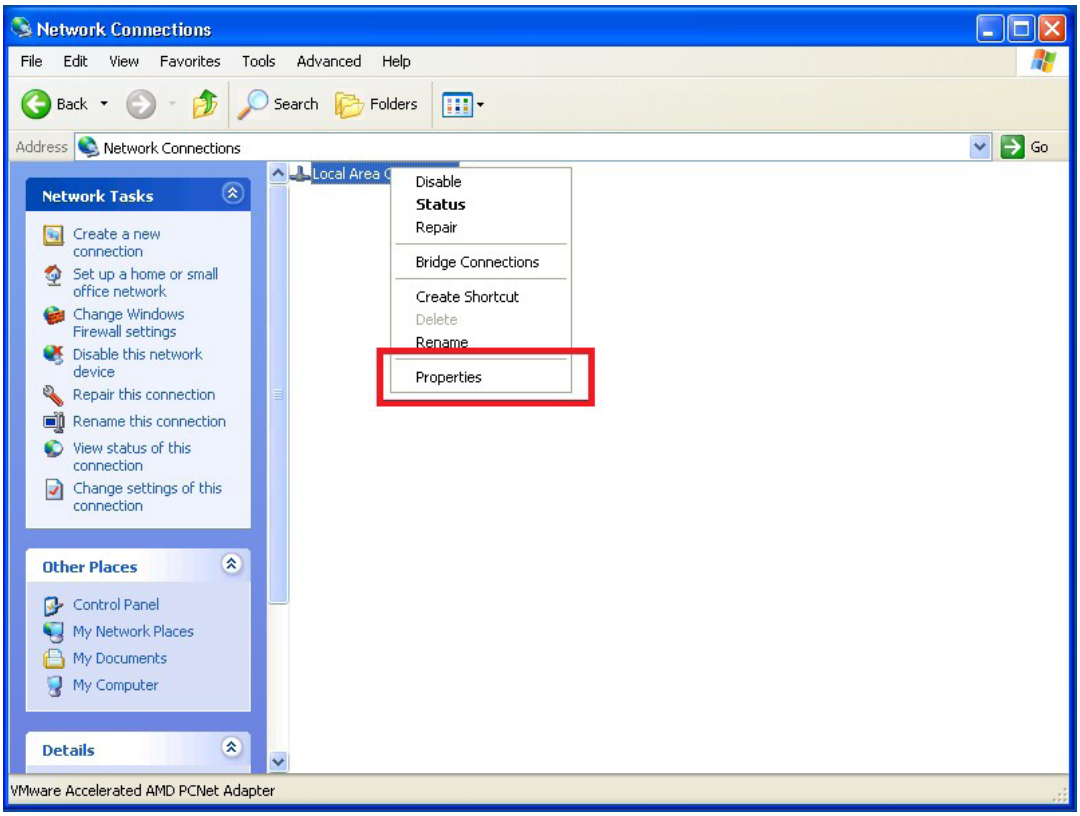


Click on *"Network connections"*

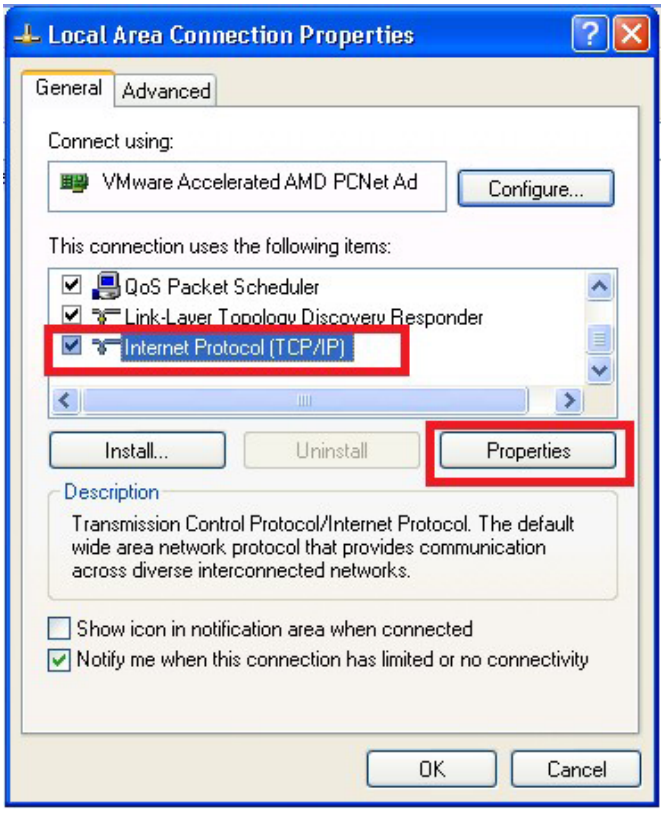


4 ISS switching on and access

Select the connection to be modified (usually *"Local area connection (LAN)"*). Click mouse right button and select *"Properties"*



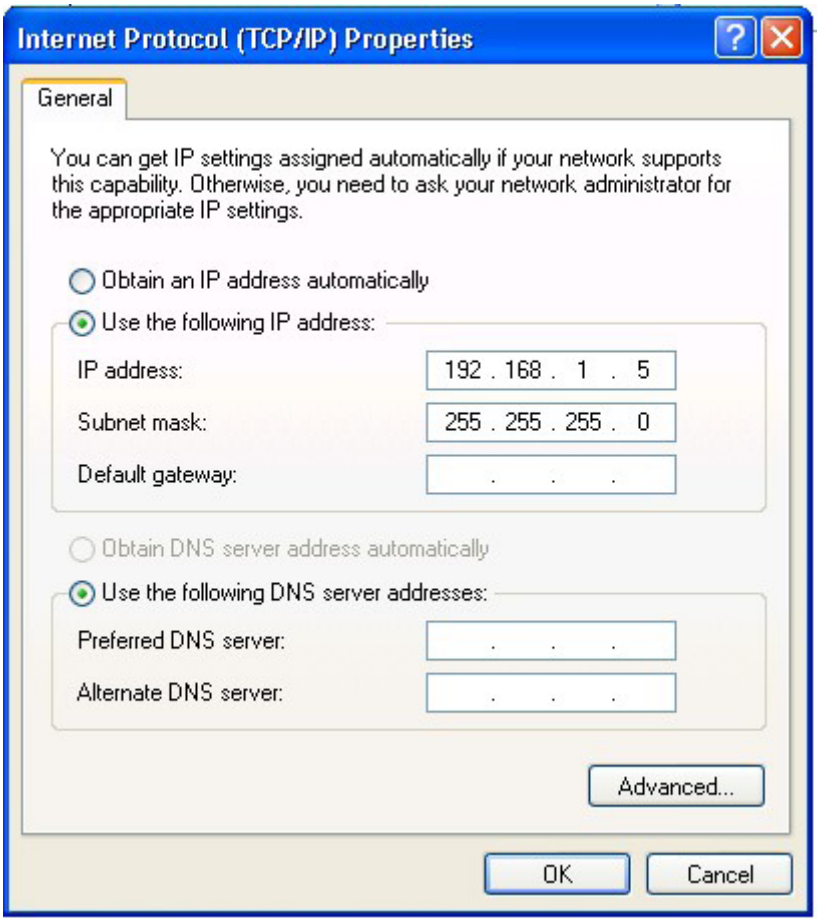
Select *"Internet Protocol (TCP/IP)"* and click on *"Properties"*



4 ISS switching on and access

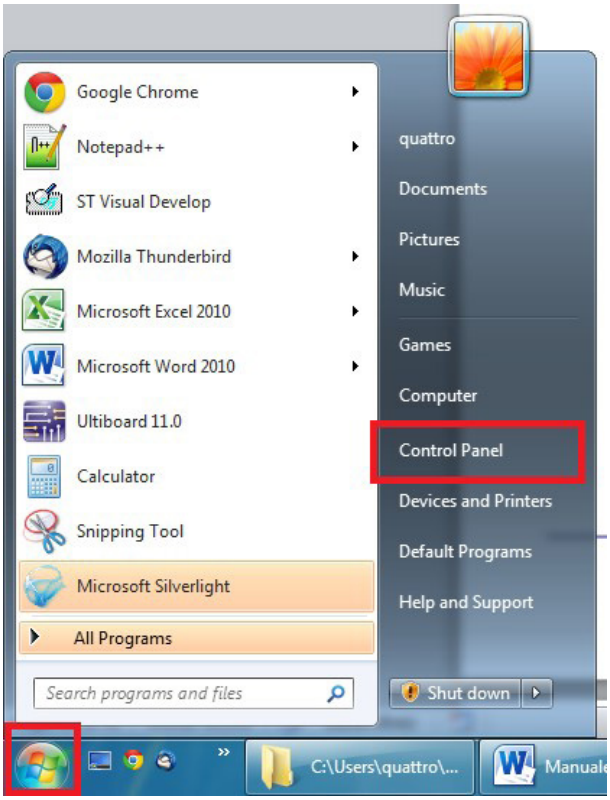
Set the network parameters as in the picture, namely:

IP address: 192.168.1.29
Subnet mask: 255.255.255.0

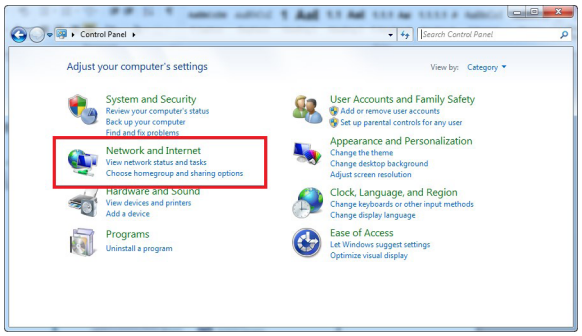


4.4.1.2 Configuration for Windows 7 system

Access the *"Start"* menu and then click on *"Control panel"*

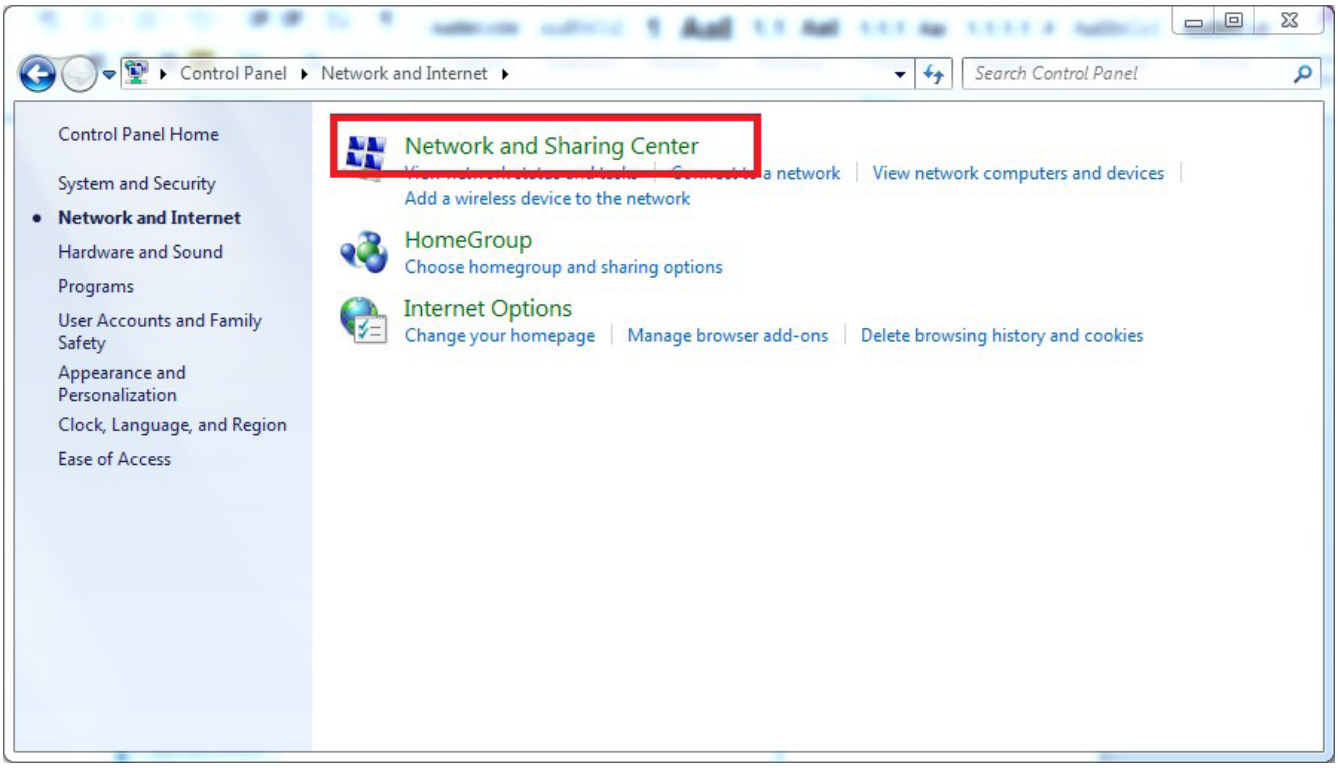


Click on *"Network and Internet"*

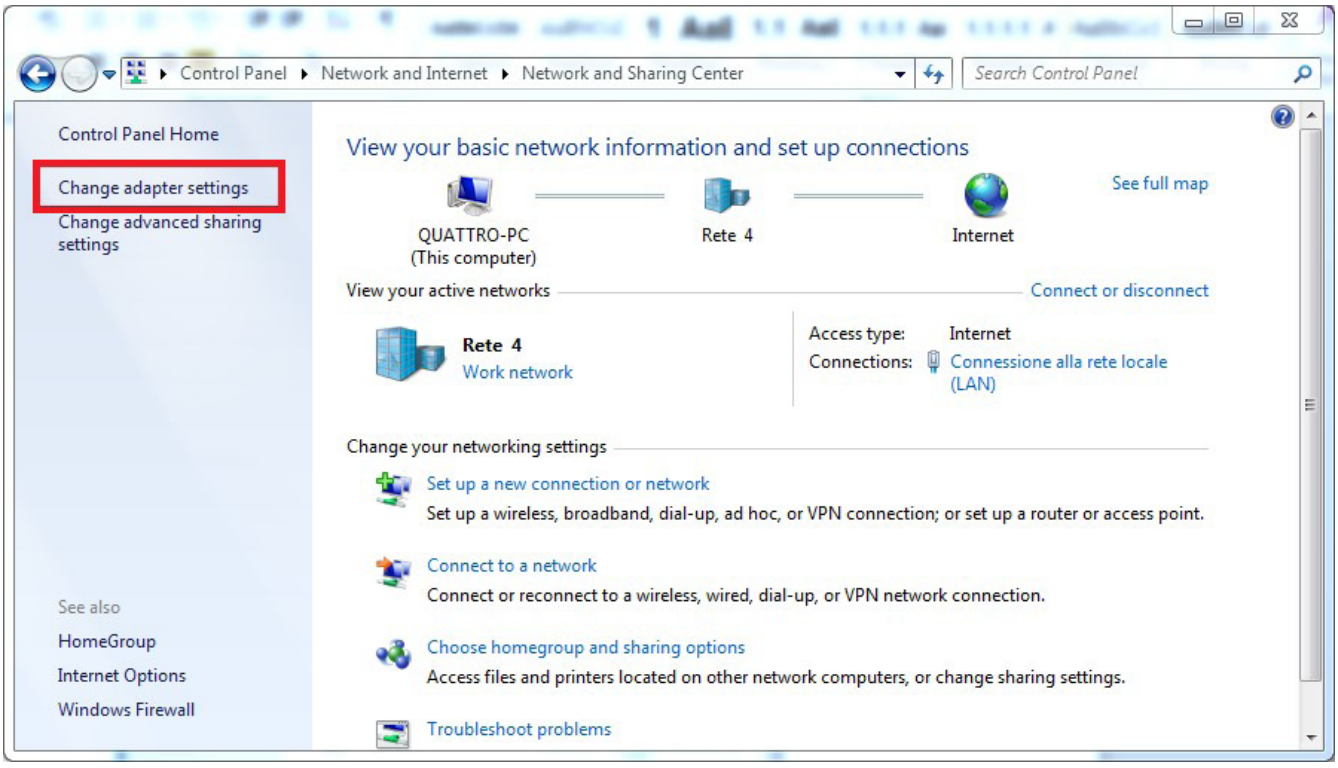


4 ISS switching on and access

Click on *"Network and sharing center"*

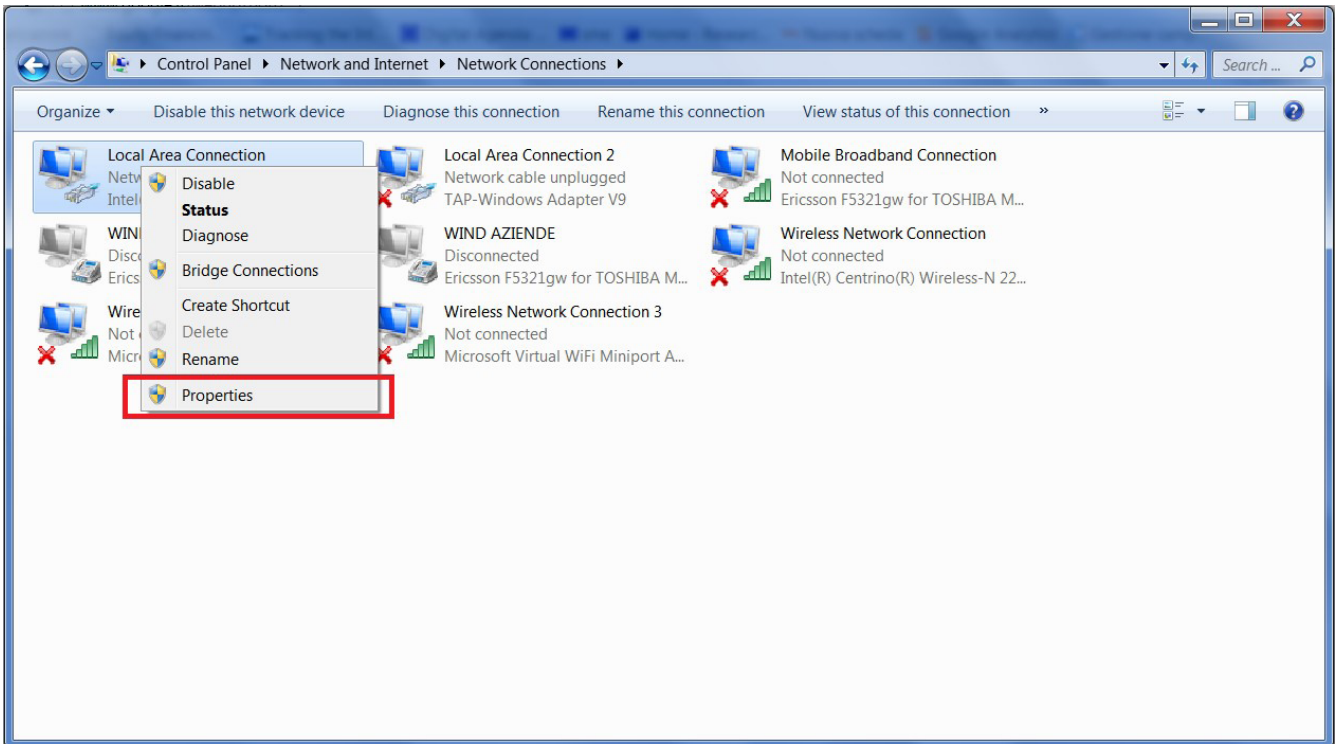


Click on *"Change adapter settings"*

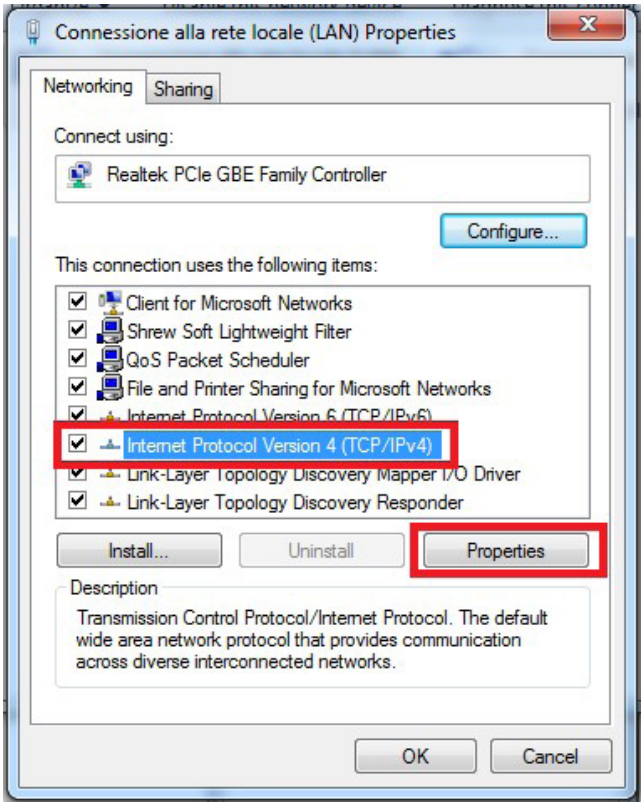


4 ISS switching on and access

Select the connection to be amended, usually *"Local area connection (LAN)"*. Click mouse right button and select *"Properties"*.

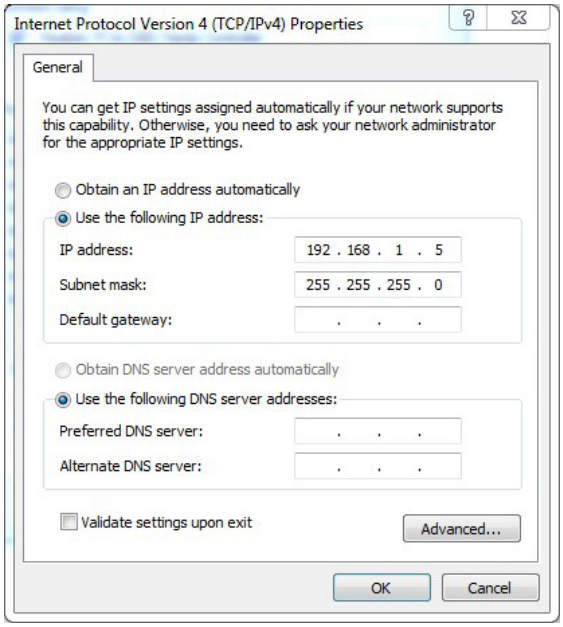


Select *"Internet protocol version 4 (TCP/IPv4)"* and click on *"Properties"*



Set the network parameters as in the figure, namely:

IP address: 192.168.1.29
Subnet mask: 255.255.255.0



4.4.2 Connection to an existing LAN network

In this case it is necessary that the ISS IP address is compatible with the existing network. Follow the procedure described in Section 5.1.

The configuration of the network to assign to IOT SCADA SERVER cannot be determined beforehand. Please, contact your system administrator to obtain the necessary parameters.

Once you have obtained the network configuration for the IOT SCADA SERVER, configure the ISS IP address via one of the methods described in sections 4.2, 4.3 or 4.4.1, and then connect the IOT SCADA SERVER to the existing LAN.

If the LAN is equipped with a firewall to filter access to Internet, the following TCP and UDP ports used by IOT SCADA SERVER should be opened to outbound traffic, to ensure proper operation (NATting included):

- 123 TCP (NTP) to synchronise the date and time
- 53 UDP (DNS) for domain names resolution, which is essential for the connection to the remote support VPN
- 443 TCP and 1194 UDP for the connection to the VPN of Alleantia remote support
- 21 TCP (FTP) for remote backup on FTP if enabled on a server not within the LAN network
- 25 TCP (SMTP) to send email notifications if enabled by a server not within the LAN network. Some SMTP servers may use a different TCP port. In this case open the specific port to traffic

If you want to remotely view the Web interface, enable the port to inbound traffic:

- 80 TCP (HTTP)

5 Configuration

The configuration includes the setup of ISS communication, connection to devices through different available interfaces and GUI customization.

Access the *"Configuration"* section from the main navigation bar and enter the following credentials:

User name: admin
Password: webloggerSU

A screen will appear as in Figure 2:

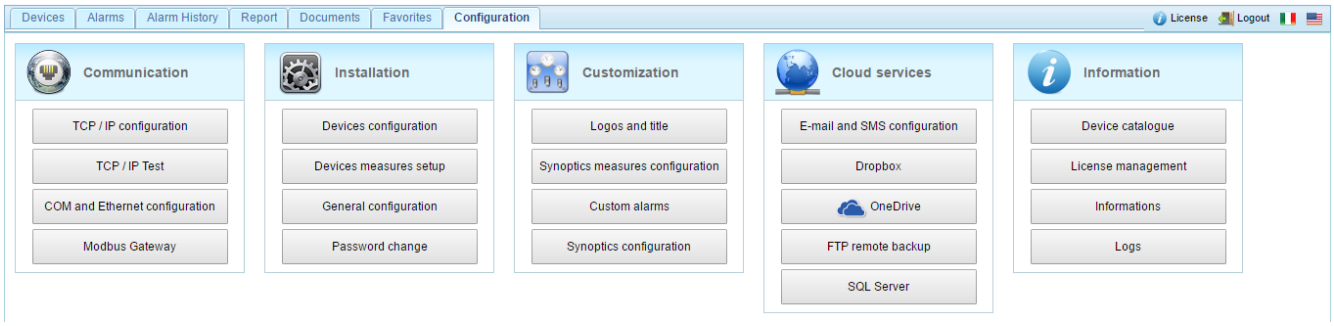


Figure 2 – System configuration

5.1 Communication

5.1.1 TCP/IP Configuration

If the IOT SCADA SERVER is connected to a LAN network, the settings must be changed in the *"Communication" -> "TCP / IP Configuration"* section. A screen as shown in Figure 3 will be displayed:

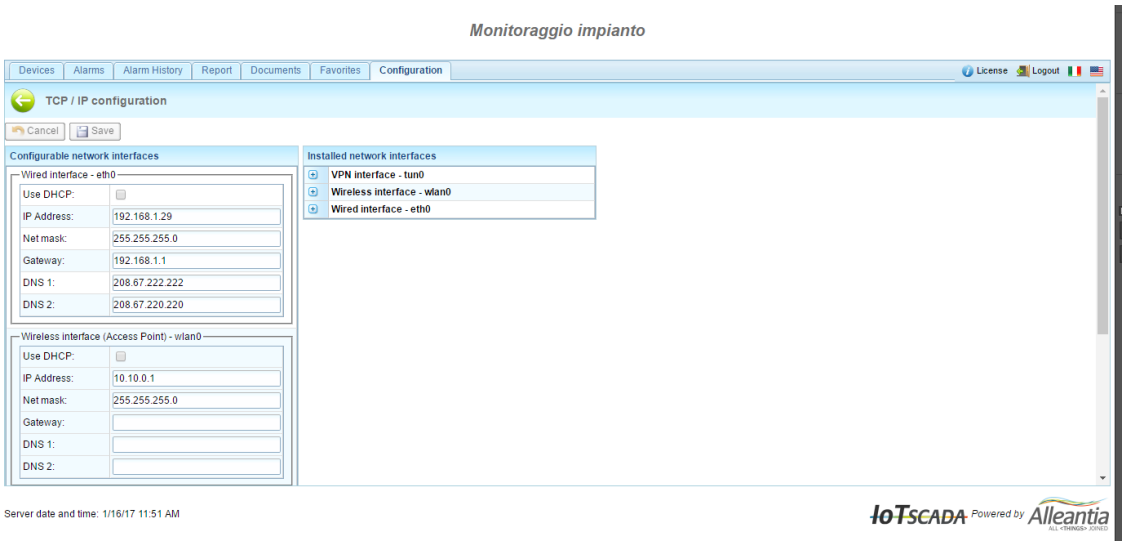


Figure 3 - Network configuration

If there is a DHCP server in the LAN network to which the IOT SCADA SERVER is connected, you can check the *"Use DHCP"* box and press the *"Save"* button. The IOT SCADA SERVER will lease the IP configuration directly from the DHCP server.
If the DHCP server is not available or you prefer to manually set the IP address, remove the check mark in the *"Use DHCP"* box and enter all the *"IP Parameters"* including the IP addresses of the DNS servers that may coincide with that of the gateway in simple network configuration.

CAUTION:
Changes to the network configuration become effective ONLY AFTER the rebooting of the IOT SCADA SERVER hardware

Please refer to your network administrator for further instructions on IP addresses setup in the LAN.

The right area "Network Interface" displays the current network configuration for both the wired interface (LAN) as well as the Alleantia VPN (Virtual Private Network) through which the IOT SCADA SERVER communicates with any centralised server (optional service) and the remote support, where available.

If the network to which you are connected has internet access, refer to Section 5.1.3 to verify the correctness of the LAN configuration set.

If the Client Wi-Fi mode is set (Dip Switch toggle n°4 of the IOT SCADA SERVER is ON), then a configuration section of the Wi-Fi network, you wish to connect to, will be displayed. If you use the Client Wi-Fi you need to be sure to remove the gateway from the wired interface configuration. If the connection as client to the network is successful then Wi-Fi LED becomes green.

5.1.2 Connection to an existing Wi-Fi network

If the IOT SCADA SERVER is connected to a Wi-Fi network as client, it is necessary to remove the gateway in the network configuration of the LAN card (see Section 5.1.1), otherwise it will not be possible to use the Wi-Fi gateway to access external servers, for example, to send email alerts or connect to the VPN of remote support.

5.1.3 Internet communication test

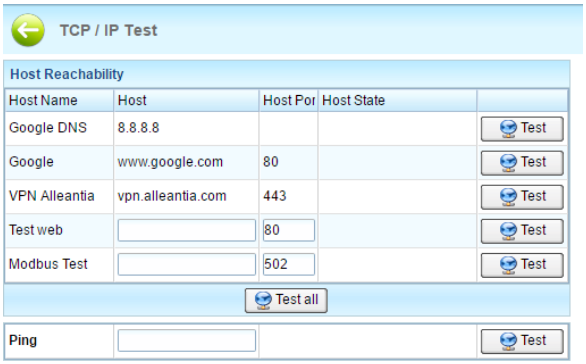


Figure 5 - Internet communication test

In the *"Communication" - > "TCP / IP test"* section you can test the reachability of some default hosts and others of your choice.
By pressing the "Test" button next to each host, or, alternatively, the "Test all" one, the reachability of these hosts can be verified and the result of the test will be shown in the "Host state" column. In the event that the host cannot be reached, check the configuration of the network, the network wiring or contact your network administrator.

5.1.4 Port and communication parameters configuration

The default configuration of the ports is carried out in the section *"Communication" -> "COM and Ethernet configuration"* and is illustrated in Figure 4.

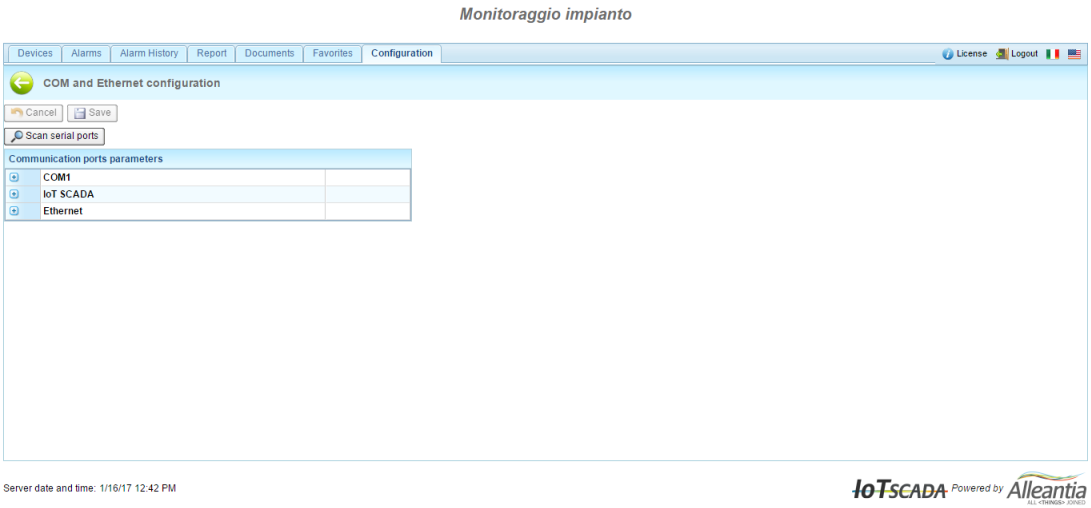


Figure 4 - Communication ports configuration

The configuration of every port (for example, baud rate, parity, stop bit, data bit) must be modified according to the characteristics of the connected devices, referring to their installation manuals. The Ethernet port is that associated to the RJ45 connector of the IOT SCADA SERVER.

COM1 port is associated to the RS485 serial port, located on the IOT SCADA SERVER terminal block. Other COM ports could be created in case of using serial USB converters, added to ISS USB ports, by pressing button *"Scan serial ports"* (Note: the converters should be physically connected to the IOT SCADA SERVER).
When scanning is complete, new found ports are displayed on green background. Remember to save new configuration before leaving the page.
The system provides for the polling of all devices on each communication line, inserting a pause between one cycle and the next equal to the *"Poll pause (ms)"* value *(can be set in web interface).*
In the event that the polling of a device is not successful within the *"Timeout (ms)"*, the system performs a number of attempts equal to *"Retries"* before highlighting a communication error and moving on to the next device.
In the event of communication problems, increase this value by up to a few seconds in order to avoid under-performing electronic systems being overloaded by repeated polling.
The non-functioning device will be called up in each scan cycle. Press *"Save"* to apply changes when the configuration is complete.

5.1.5 Modbus Gateway

The Modbus gateway feature makes the system data accessible to external software via the Modbus protocol enabling, for example, the integration with SCADA systems, regardless of the protocol used by devices to which the IOT SCADA SERVER is connected upstream.

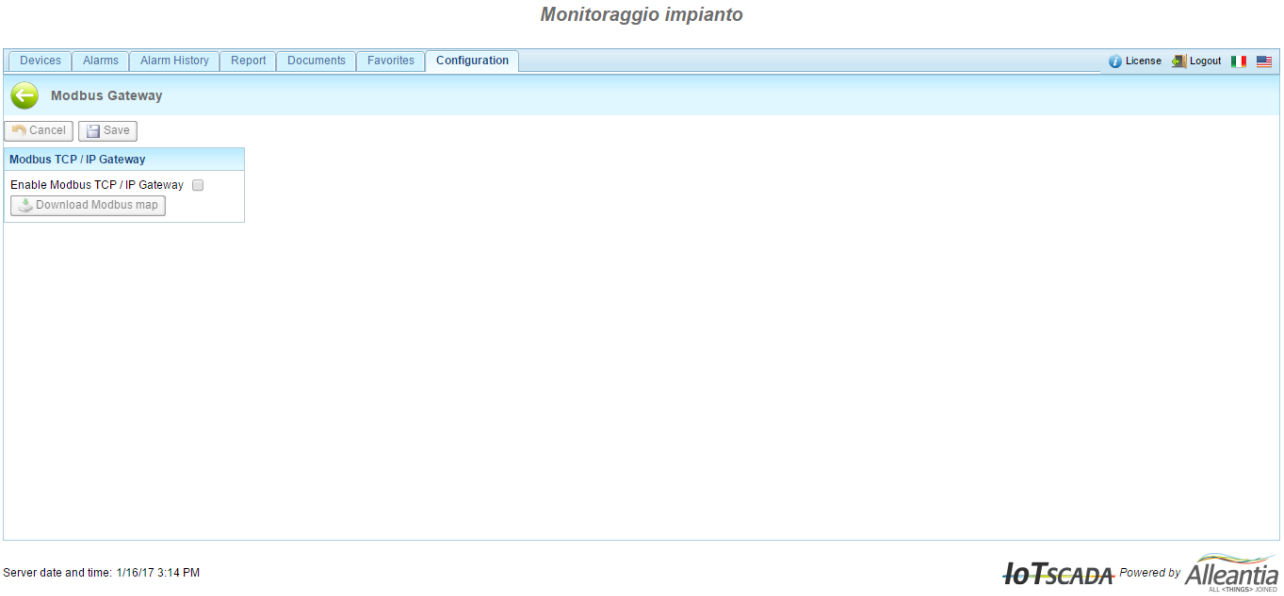


Figure 5 - Modbus gateway

The Modbus map with information is created automatically and can be downloaded in Excel format, including the configured information set, by pressing the button *"Download Modbus map (Excel. XLSX),"* which is enabled when the gateway is in turn enabled. The file can be used within the target application (e.g. Wonderware (c) SCADA system, SAP (c) MII) to set up the communication with the ISS.

5.1.5.1 Rules of automatic mapping

The mapping of the measures of the devices on the Modbus gateway follows the following rules:

- For each IO SCADA SERVER serial port where devices are connected and configured, a TCP Modbus slave is created on a different TCP port:
    - o COM1 -> TCP 502 port
    - o COM2 -> TCP 503 port
    - o COM3 -> TCP 504 port
    - o COM4 -> TCP 505 port
    - o COM5 -> TCP 506 port
    - o Ethernet -> TCP 565 port
- Within each Modbus slave the devices keep the address configured on the physical device. If, however, this address is greater than 247, the maximum permitted by the Modbus protocol, it will be arbitrarily reassigned.
- The Modbus devices maintain the same identical mapping of the original device, both in respect of the areas as well as the addresses, data types etc. Byte and word swaps will not be considered.
- Non-Modbus devices will show the Boolean types in the coil area and numeric types both in Holding as well as in Input. The number will be in 2-word float format. The register address will be calculated arbitrarily.

- The bits within a word of the gateway are in Big-Endian format (More Significant Byte First) and the word in data types in 32 or 64 bits are in Little Endian format (Less Significant Word First).
- If a physical device goes offline, it will not respond when contacted through the gateway and the request will time out.
- If the value of a register containing a measure not read by IOT SCADA SERVER (see Section 5.2.3), is requested, the gateway responds with a default value of 0 for numeric data types and false for Boolean
- If the value of a non-existent Modbus register is requested, the gateway responds with the exception code “2”, that is “Illegal Data Address”.
- The gateway does not support writing, so if these are carried out by an external Modbus master, the Modbus register values are immediately restored to the value prior to the writing.

5.2 Installation

5.2.1 Configuration and use of IOT SCADA SERVER’s I/O

The IOT SCADA SERVER is preconfigured with two devices called “IoT Server” and “IoT Server (Configuration)”.

These virtual devices are used to read the values of the inputs and control outputs of the IOT SCADA SERVER.

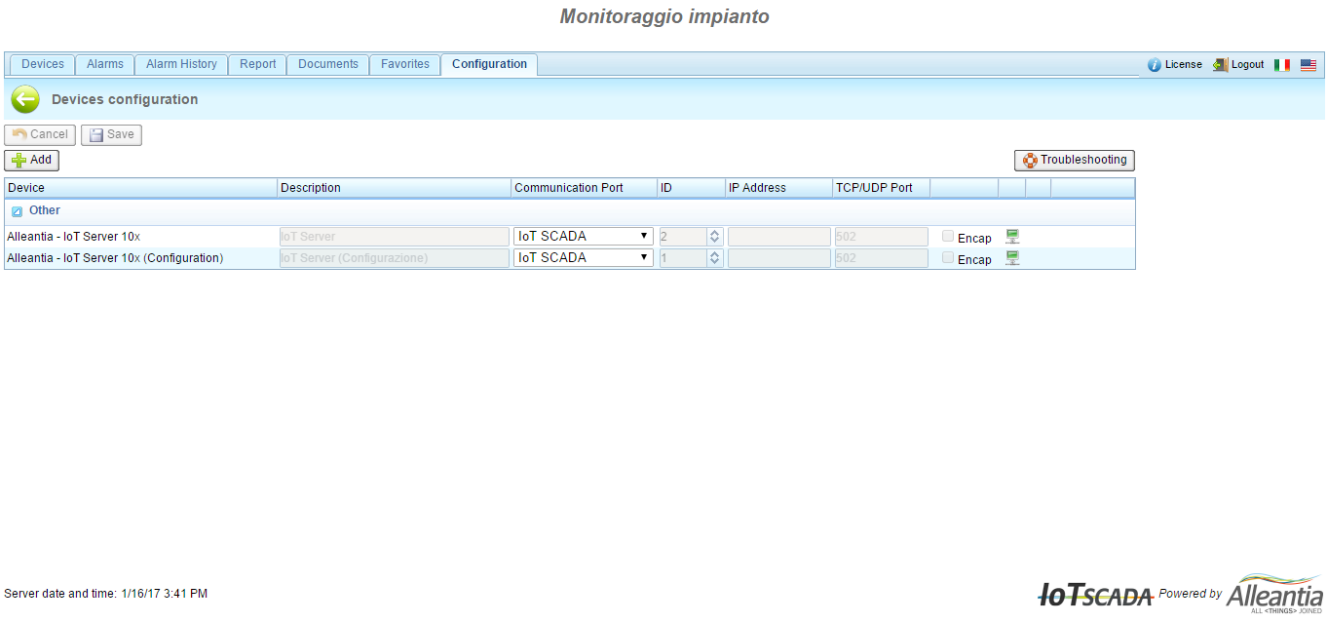


Figure 6 – IOT SCADA SERVER preconfigured devices

5.2.1.1 Configuration of inputs and outputs

To use inputs and outputs, first of all, you need to configure them to choose an IOT SCADA SERVER mode. In the ISS *"Device"* tab under *"IoT Server (Configuration)"* it will be possible to choose analog input type (voltage, current), digital output type (active with steady value or inactive), etc. (Figure 7). Click the pencil button on the row you wish to change, to open a configuration pop up.

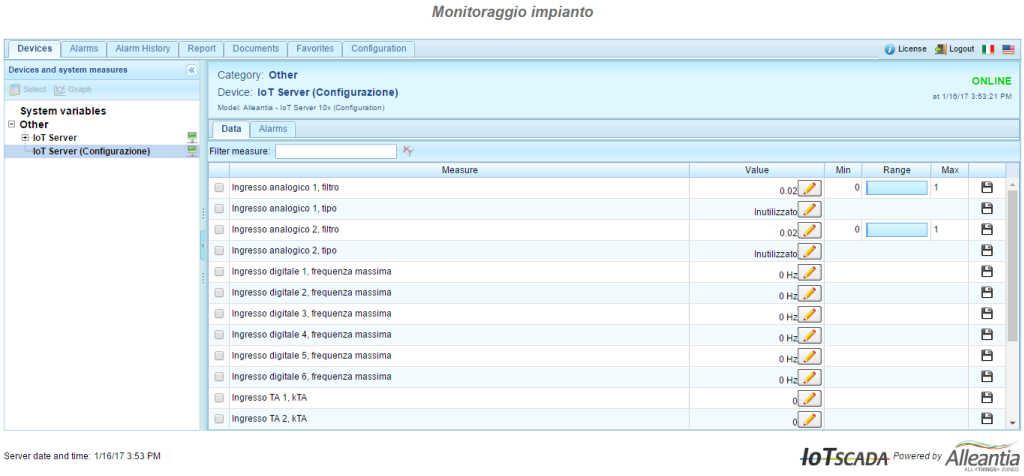


Figure 7 - Configuration variables IoT Server

The following are some examples of IoT Server inputs and outputs configuration:

• Configuration of a temperature probe Pt1000 type: If the probe is in the input 1 - T1, from *"IoT Server (Configuration)"* tree menu select *"Temperature input 1, sensor type"* and set *"Pt1000"*. Proceed in the same way if the probe is in the input 2 - T2, selecting *"Temperature input 2, sensor type"* .

• Configuration of a current transformer (TA): If the TA is in the input 1 - CI1, from *"IoT Server (Configuration)"* tree menu select *"Input TA 1, kTA"* and set the number corresponding to ratio of the TA currents (for example, for TA 150/5 set 30). Proceed in the same way if the TA is in the input 2 - CI2, selecting *"Input TA 2, kTA"*.

• Activation of digital outputs: To activate the digital output 1 - DO1, from *"IoT Server (Configuration)"* tree menu select *"Digital output 1, mode"* and then in the *"Iot Server"* tree menu set digital output to "False" or "True" (respectively for a low logic value corresponding to about DO2 or a logic value alto corresponding to about DO1). Proceed in the same way to activate the digital output 2 - DO2.

• Activation of analog inputs: After having set the IOT SCADA SERVER Dip Switch toggle n.1 in the position ON **when the machine is TURNED OFF and with disconnected analog input** (see Section 3.1.2), you can proceed with the configuration. To activate the analog input 1 - AI1, from *"IoT Server (Configuration)"* tree menu select *"Analog input 1, type"* and the equivalent entry (*"Voltage 0-10V"*, *"Current 0-20mA"*, *"Current 4-20mA"* and *"Digital"*), according to the type of use. In the even that a voltage input is selected (e.g. *"Voltage 0-10V"* or *"Digital"*) set the DIP1 switch at OFF or for a current input (e.g. *"Current 0-20mA"* or *"Current 4-20mA"*) set the DIP2 switch at ON. Proceed in the same way to activate the analog input 2 - AI2.

• Activation of relay outputs: To activate the relay output 1 - R1, under *"Iot Server"* of the tree interface set "True" or "False" to inactivate the output. Proceed in the same way for the relay output 2 - R2.

5.2.1.2 Use of IOT SCADA SERVER

From the tree interface structure, selecting he entry *"other"* and then *"IoT Server"*, in "Data" Tab the IOT SCADA SERVER variables are displayed (Figure 8).

The variables are divided in 3 sections:

- System: The variables of this section apply to the relevant information about the IoT Server hardware. This section contains information about firmware version, temperature, operating voltage, UPS state.
- Input: In this section there are the variables associated to the analog and digital inputs, and to the temperature probes; in the last column the symbol  is displayed according to the input for which an alarm has been defined.
- Output: Digital outputs state and relay state.

In the tab "Alarms" you can see any defined alarms, the association to the variable to be monitored (e.g. "UPS activation" or "input value out of range") and the actual condition of such warning.

Monitoraggio impianto

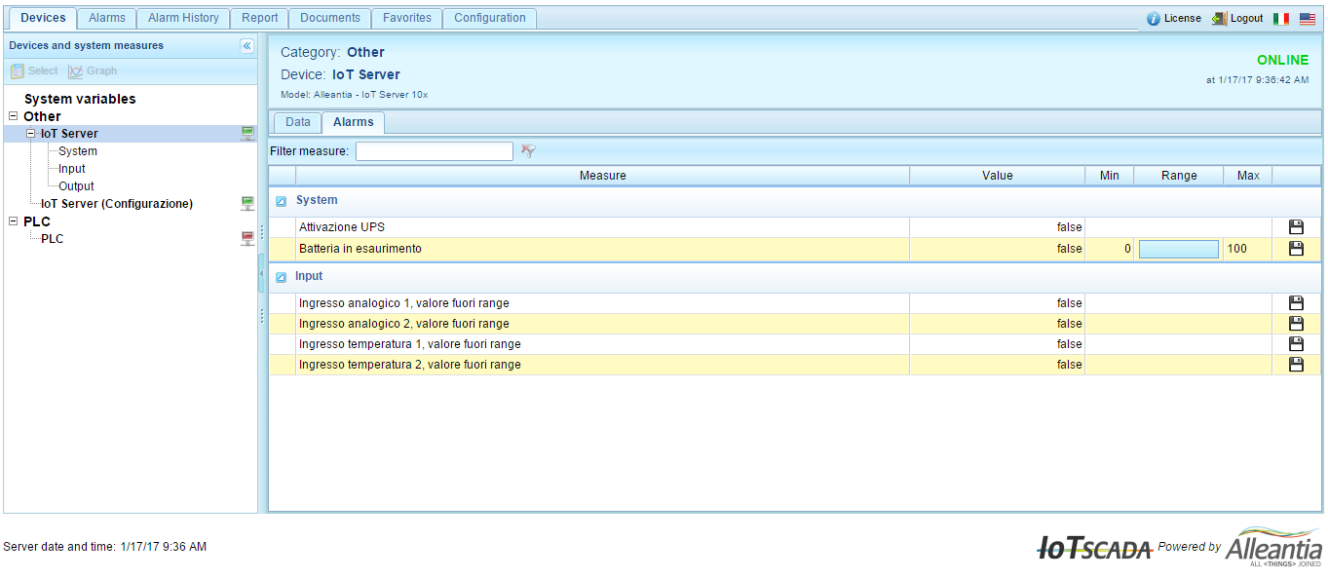


Figure 8 - IoT Server variables display

5.2.2 System devices configuration

This section describes how to add and remove new devices connected to the IOT SCADA SERVER via the RS485 serial interface or via Ethernet.

5.2.2.1 Adding new devices

Any device from which you want the IOT SCADA SERVER to collect measures must be inserted in the section “Installation” -> “Devices configuration”.

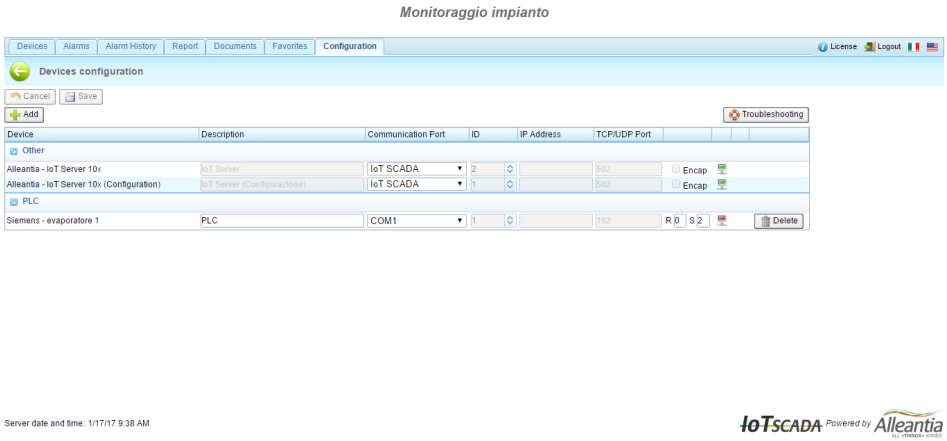


Figure 9 – System devices configuration

To add a device, press the *“Add”* button. A popup window appears as in Figure 10, showing device drivers loaded in the IOT SCADA SERVER catalogue. To add new devices please refer to Section 5.5.1

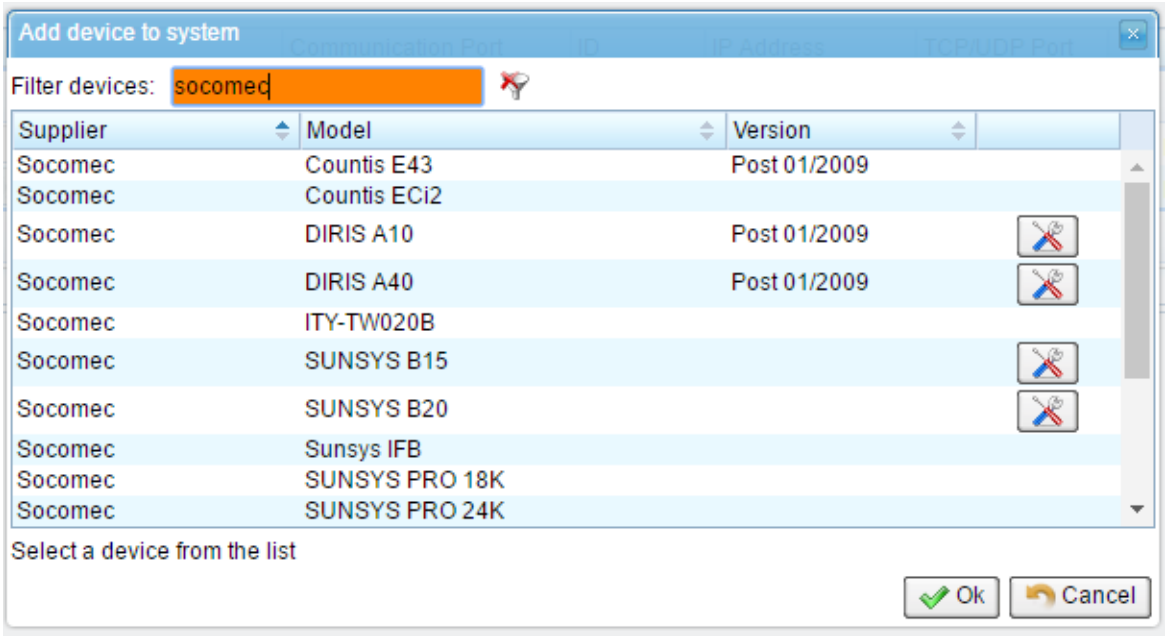


Figure 10 - List of supported devices

5 Configuration

The list contains all of the devices supported by IOT SCADA SERVER and can be sorted and filtered by manufacturer, model and version in order to facilitate the search.
To add a device to the system configuration, select it, set the number of identical devices present and press the *"Add"* button. The number of devices selected will be inserted in the main page and will appear with a green background to indicate that they have just been added:

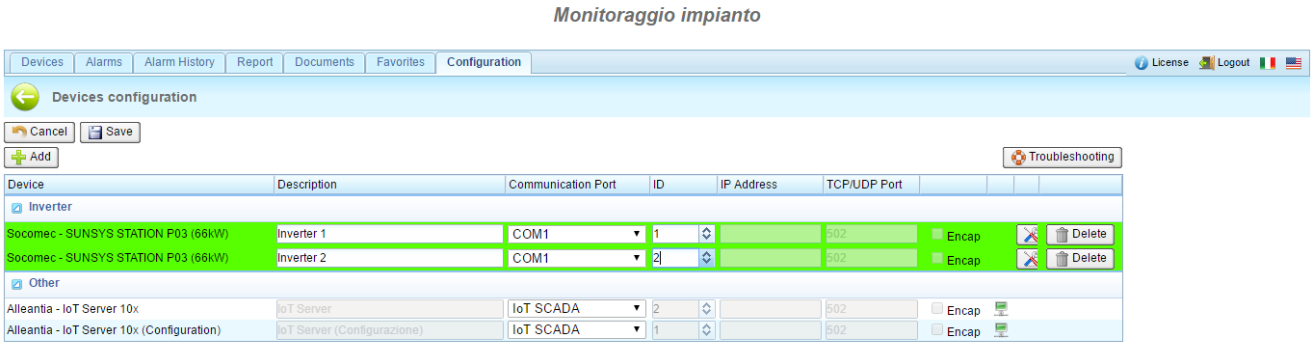


Figure 11 - New devices added

Each new device shall be assigned a unique name to be recognised in the user interface (e.g. West Inverter 1), a unique numeric identifier to allow addressing on the RS232/485 bus or Ethernet (the ID in the case of the Modbus protocol) and the communication port to poll. For the list of existing ports or to add new ones using converters, refer to Section 5.1.

The device parameters can be inserted directly on the line. The "IP Address" and "TCP / UDP Port" fields will also be completed for the devices with Ethernet interface which, in the case of Modbus TCP / IP, is generally "502".
Repeat the operation for all devices to add.

CAUTION:
The identifier must be assigned to the first device (e.g. Inverter) according to the procedure described in the device's manual, and then copied in the configuration section of the IOT SCADA SERVER.

The devices with "<disconnected>" communication port are not "polled" as they are not associated with any communication line (Ethernet or serial). If a device is out of service its communication port can be set to "<disconnected>" to avoid any communication errors and speed up the reading of data from the system without changing the configuration.

Once the system configuration is complete, press the *"Save"* button at the top to make the changes effective. After a few moments the IOT SCADA SERVER will begin to poll the devices and an icon will appear next to each representing the communication status with the device itself.

If the configuration and wiring are correct the icon will be green:  , while if the device is not reachable the icon will be red:  .

Figure 12 - System configured

The measures collected by the devices will appear in the "Devices" section in the main menu, see Section 6.2.1. Each device provides a number of measures that can be appropriately chosen by the user to facilitate the readability of the synoptics, as explained in Section 5.2.3.

5.2.2.2 Removing a device

If a device is no longer present in the system it can be removed from the configuration by pressing the *"Delete"* button at the end of device line. The device will disappear from the list and the change will become effective after pressing the *"Save"* button.

CAUTION: Deleting a device will cause the loss of all of its recorded data. If you no longer wish to poll the device but keep the collected data, set its communication port to "<disconnected>".

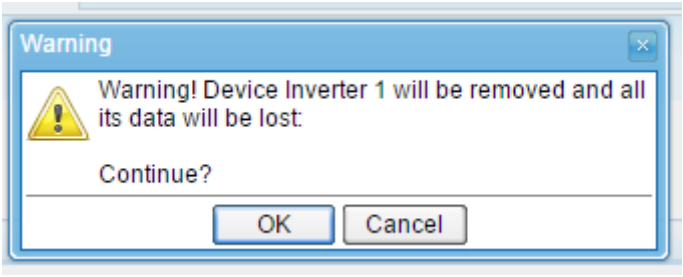


Figure 13 – Confirmation Popup window for the removal of a device

5.2.2.3 Installation support manuals

During both the device selection, as shown in Figure 9, as well as in the device list as shown in Figure 10, two icons can appear next to each device that allow to download and view the help documentation during installation:

User manual

Quick installation guide

The “User Manual” is the same as that provided by the device manufacturer configured in IOT SCADA SERVER, while the “Quick Start Guide” is a concise guide created by Alleantia to help you configure the device and IOT SCADA SERVER.

In the event of communication problems between the IOT SCADA SERVER devices, refer to the troubleshooting guide that can be downloaded by pressing the button:

5.2.3 Devices measures setup

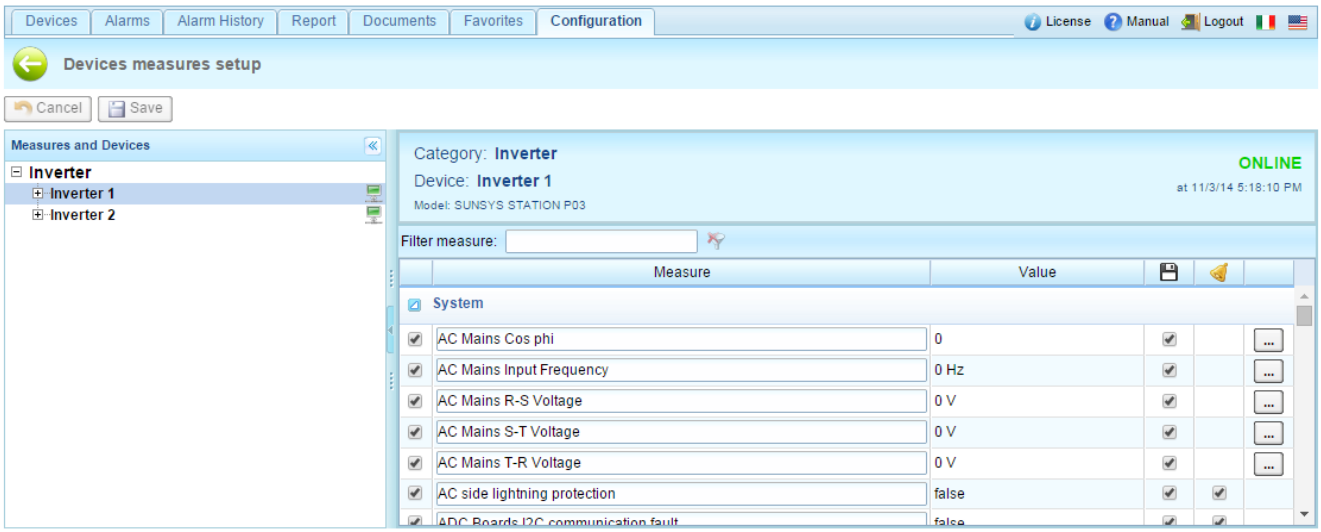


Figure 14 - Devices measures setup

Each device supported by IOT SCADA SERVER carries all information about any measure provided by the device. In order to avoid showing too many measures and slow down the scanning of the devices, only the measures actually considered useful for the monitoring are read when the device is added.

To change the default configuration, access the *“Installation” -> “Devices measures setup”* section; there is a tree menu on the left where all devices that the IOT SCADA SERVER is polling can be seen, organised by category. Once you have selected a device, all available measures will appear on the right.

Checking the boxes at the beginning of each line enables the reading of a single measure. Unchecking disable reading check boxes in the column with the symbol, it is possible to enable or disable measure logging in the IOT SCADA SERVER.

CAUTION:
Graphs can only be generated for the measures with enabled logging

If the measure is configured as an alarm there will also be a check box in the column with th symbol. If checked, IOT SCADA SERVER will display an alarm in case of abnormal value of the measure and, if the alarm notification is configured, an e-mail will be sent to the notification recipients.

The name of the measure can be directly changed in the text box. To change the other settings, if any, a dedicated popup window can be opened by clicking on the ... button.

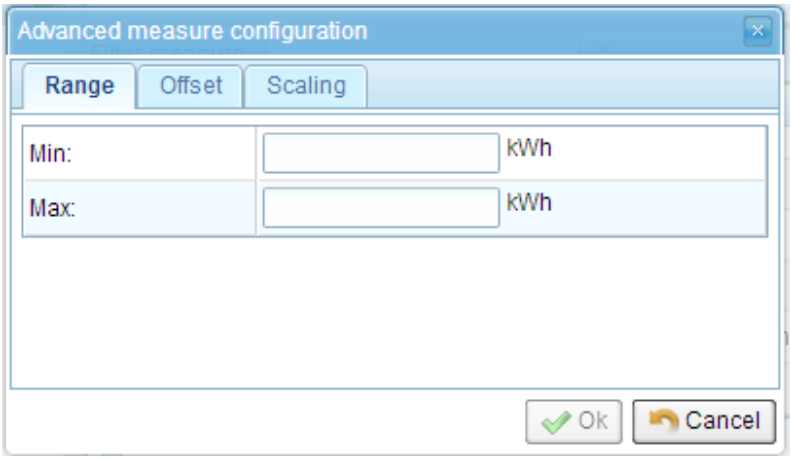


Figure 15 - Measure range configuration popup window

By specifying a minimum and maximum value in the popup window *"Range"* tab it will be possible to make the screen reading of the measure easier (see, for example, the horizontal bars of some measures in Figure 56).

5.2.3.1 Measures offset

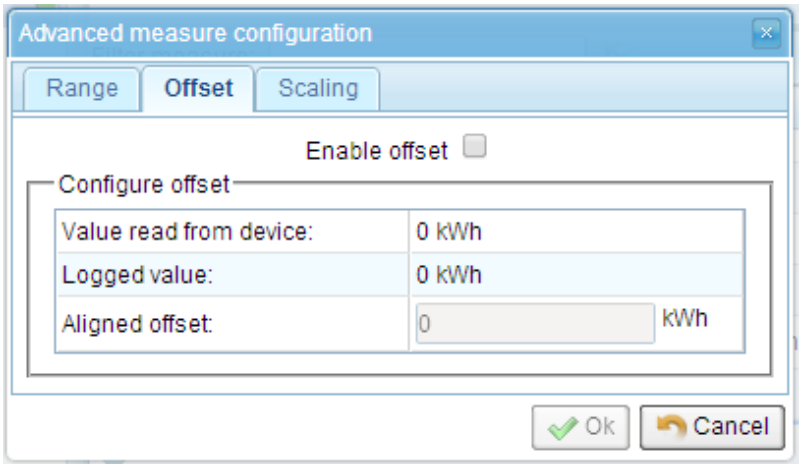


Figure 16 - Measure offset configuration popup window

The measure offset feature is very useful in the case of network analysers that measure the energy produced or consumed. These devices are in fact often installed in parallel to an exchange meter and begin counting from 0 kWh, while the meter has a higher value. To facilitate the reading it can be aligned with that of the existing meter "correcting" the value displayed and recorded.
In the advanced configuration popup window *"Offset"* tab (see Figure 16) a value can be set in the *"Aligned offset"* box. The IOT SCADA SERVER will calculate the difference between the actual value and that desired, and this will be applied to the measures read by the device from that moment on. The values of the measures so aligned will appear in italic as a reminder that these values are not the real ones read but those purposefully modified by the user.

5.2.3.2 Measures scaling

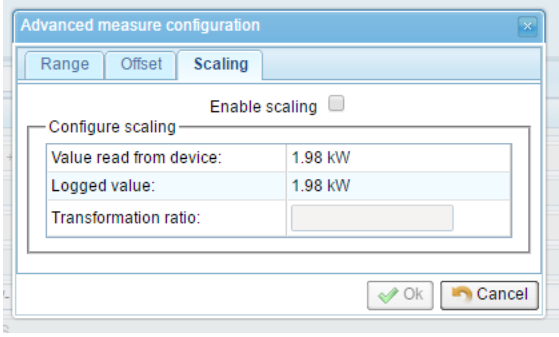


Figure 17 - Measures scaling configuration popup window

The measure scaling feature is very useful in the case of fiscal meters that measure energy through external current transformer. The measured value is a fraction of the real value, i.e. 1 / K, with K the transformation ratio of the current transformer.
In the advanced configuration popup window *"Scaling"* tab (see Figure 17) a value can be set in the *"Transformation ratio"*. The IOT SCADA SERVER will multiply the value aligned (see Section 5.2.3.1) for the transformation ratio set.
The values of the measures scaled in this manner will appear in italic as a reminder that these are not real values but those purposefully modified by the user.

5.2.4 General settings

Figure 18 – Data sampling configuration

Data sampling will affect the accuracy of the measure as it will increase or decrease the number of samples available to be analysed. A too high number of samples could excessively slow the processing.
On the same page you can set the system date and time: 'Date-Time Set', 'System Reset' e 'System Reboot'. It's even possible to reset IOT SCADA SERVER configuration by clicking on the *"Reset"* button, in this case:

CAUTION:
In case of reset all data and configurations of devices, alarms and notifications WILL BE LOST without possibility to recover

5.2.5 Password change

To change the access password to the configuration section, go to the *"Installation" -> "Password Change"* section and enter the old password (the initial installation default password is webloggerSU, as specified in Section 5). Select the new password and re-enter to confirm the selection. When finished, press the *"Save"* button.

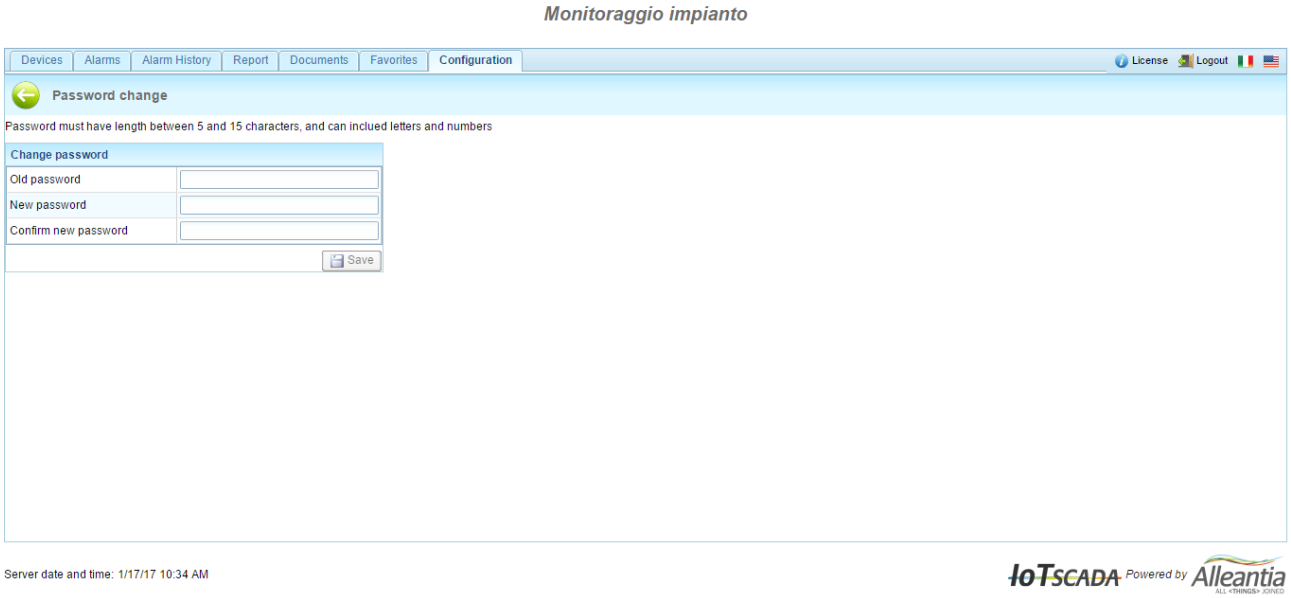


Figure 19– Password change

CAUTION:
For security reasons it is strongly recommended to change the IOT SCADA SERVER admin password immediately

5 Configuration

5.3 Customization

5.3.1 Logos and title

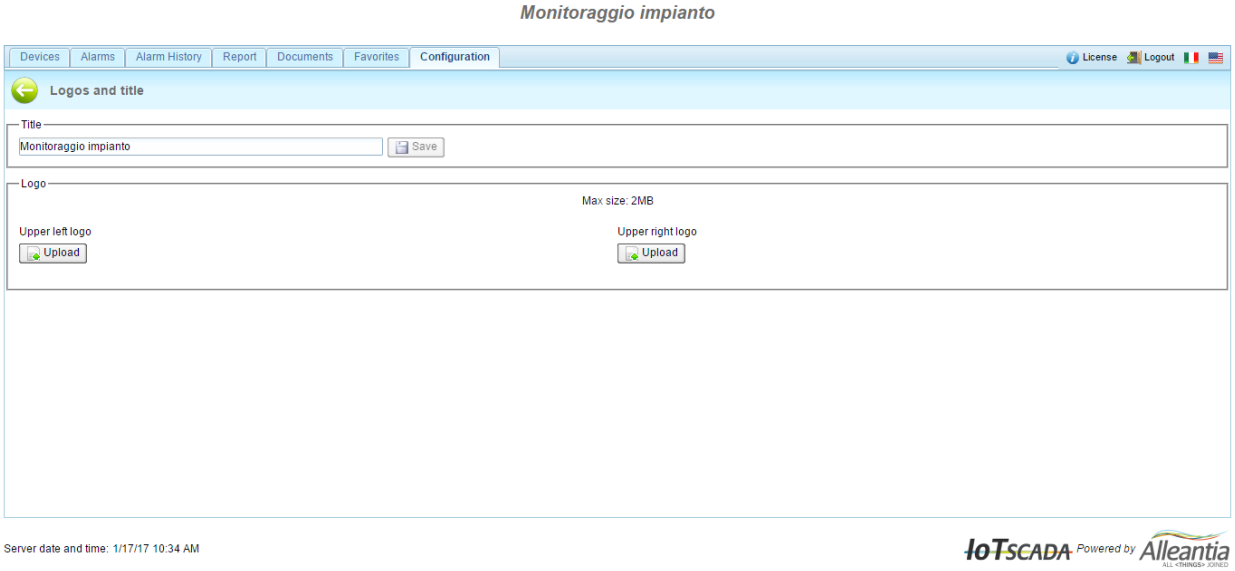


Figure 20 - System logos and title customization

In the *"Customization" -> "Logos and title"* section the IOT SCADA SERVER interface can be customized:

- in the *"Title"* section the upper title present in all the pages of the interface can be set
- in the *"Logo"* section 2 logos can be entered, one on the upper right and one on the upper left. These are also always present in all the pages GUI

5.3.2 Custom measures

In addition to the measures read by the devices, you can define custom measures (such as, for example, sums of other measures): clicking the *"Add"* button in the *"Configuration"* > *"Synoptic measures configuration"* -> *"Custom measures"* section (Figure 21) a popup menu will open that allows you to enter the name of the new measure and select the existing ones which, when summed, will contribute to its value (Figure 22).

Figure 21 - Custom measures

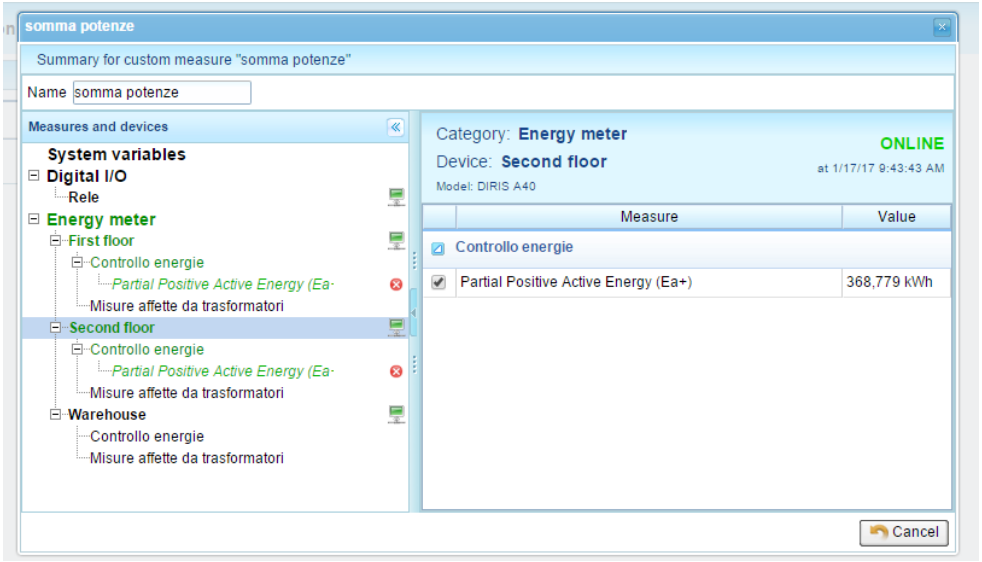


Figure 22 – Custom measures popup window

For example, if the system is divided into two levels, you can create the custom measures "East Power" and "West Power" and select the power of the inverters associated to each level for each one. Please note that it is only possible to choose measures with the same measure units. Therefore, after selecting the first one, an automatic filter will remove all those that have different units of measures from the list on the right.

5.3.3 Custom alarms

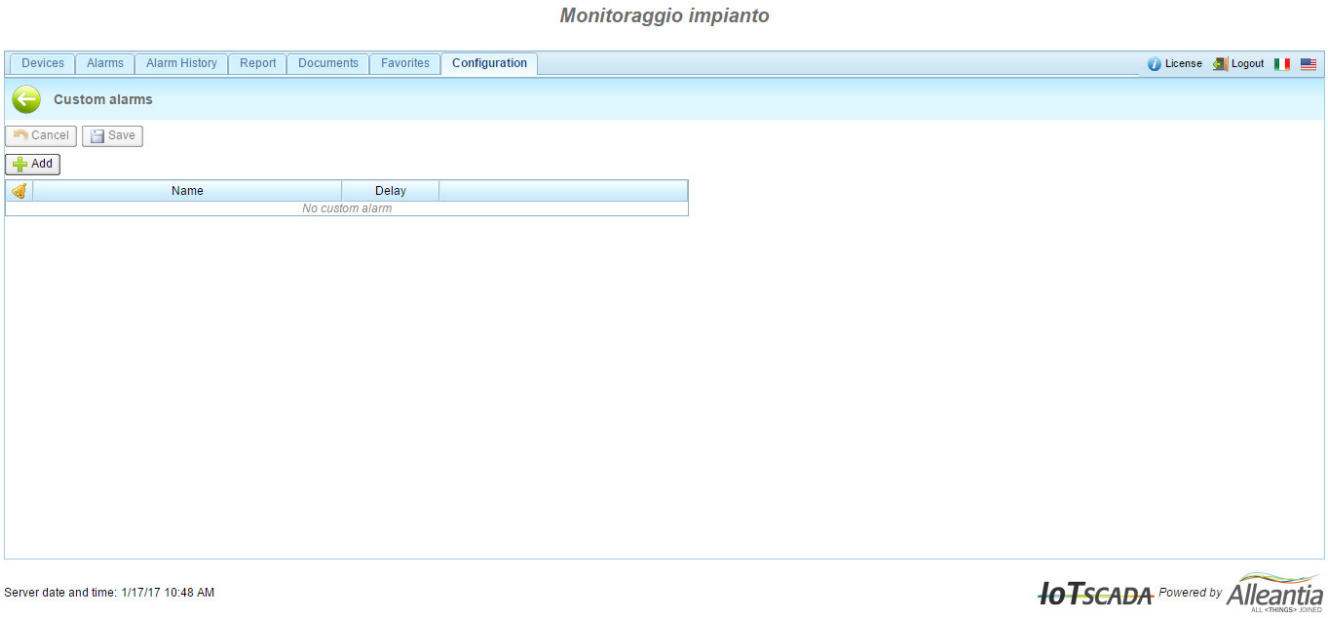


Figure 23 – Custom alarms start screen

By accessing the *"Customization" -> "Custom alarms"* section it is possible to define new and more complex alarm conditions, in addition to those that are already set in the device. For example, if you want to create a new alarm condition that notifies an anomalous situation of low production on a solar inverter. Pressing the *"Add"* button will open a popup menu that allows you to configure the new alarm in detail:

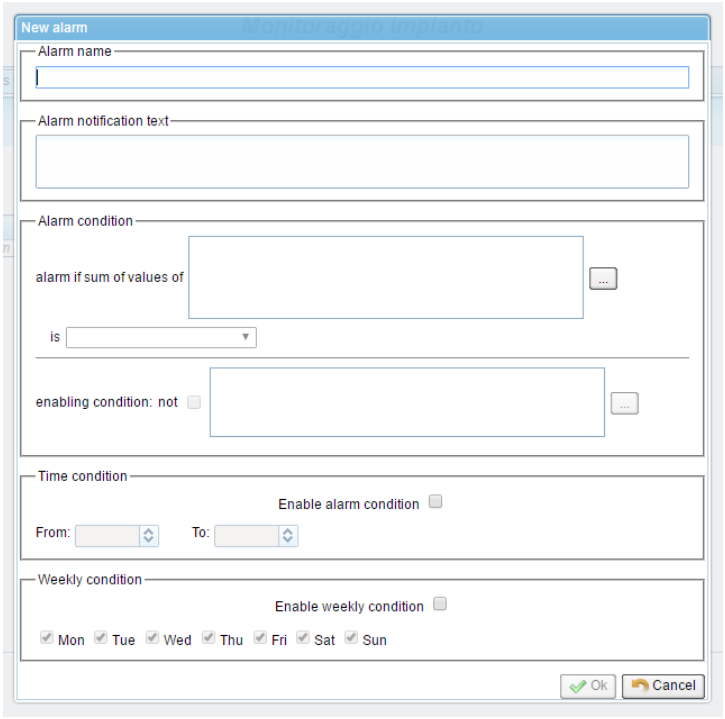


Figure 24 - New custom alarm configuration

In the popup window insert the name for the alarm and text description that will be used during the notification to the user. Below, in the *"Alarm Condition"* section proceed to the selection of all the measures that you intend to monitor by pressing the ... button. In this case we select only the power of inverter 1. Following the selection, the list of measures selected will appear next to the button. The check boxes enable the control types to be performed on the measure value. In this case the alarm will be triggered if the power of the inverter 1 falls below a certain threshold:

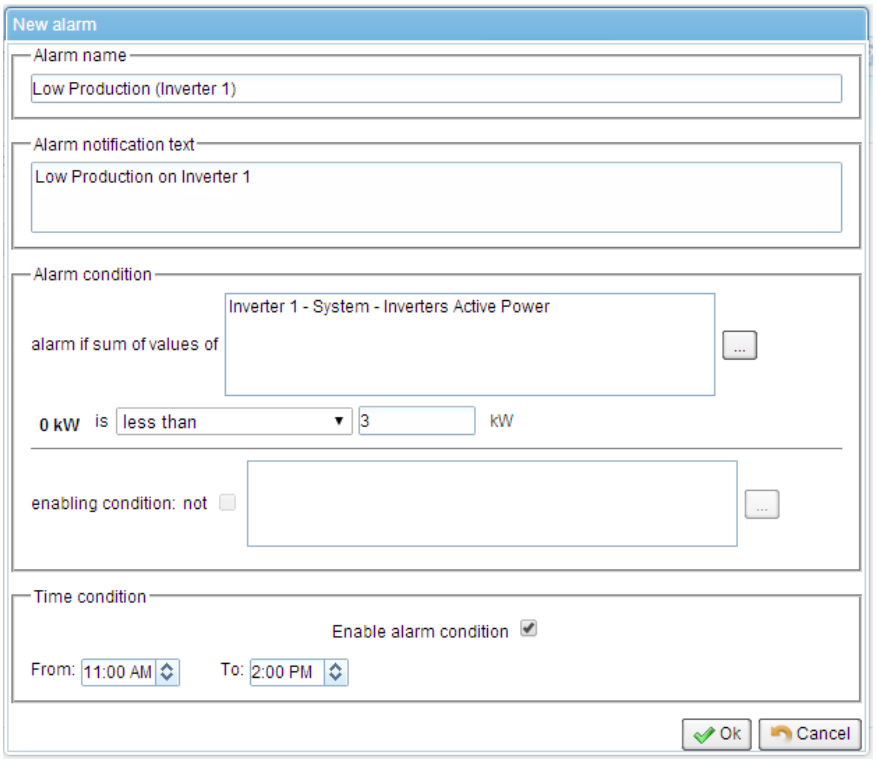


Figure 25 - Low production alarm

A time range for the control can be specified. In this case, to avoid the control perform during the night when the solar inverter is not active. To save and activate the alarm, press *"Ok"* and then click on *"Save"* in the *"Custom alarms"* screen.

Once this alarm is entered, it is displayed on the main screen where it can be enabled or disabled using the checkbox and it is possible to set the delay time before which the alarm is to be considered as true (for example, 5 minutes), thus limiting the effect of transients:

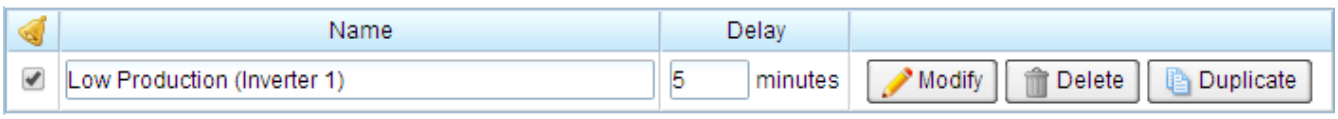


Figure 26 - New alarm

It is also possible to enable an alarm in relation to another: for example, using a pyranometer the alarm previously created can be reinforced by connecting the value of irradiation and then testing the low production only at times when it is expected to be high. To do this, simply create a new alarm to act as an “enabling condition”, an alarm that shall not be notified and, therefore, without the relevant box being checked:

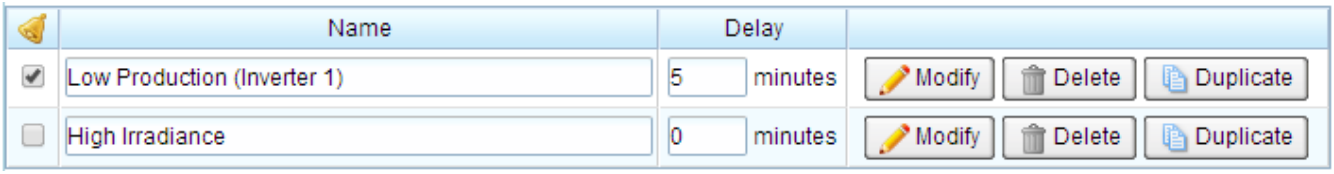


Figure 27 - Multiple custom alarms

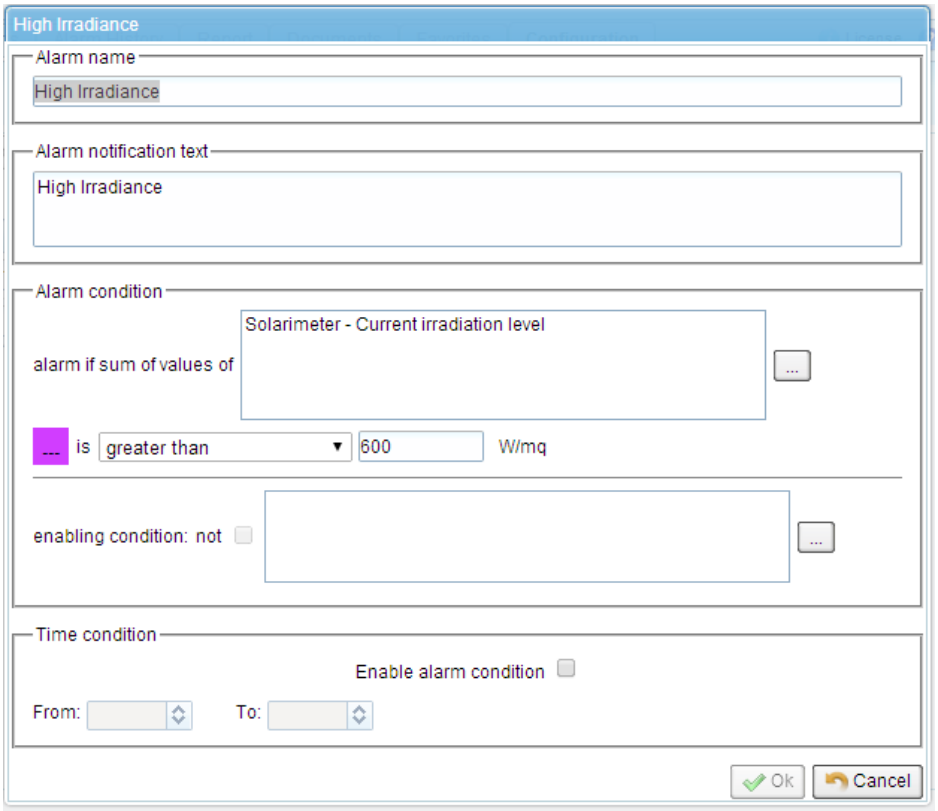


Figure 28 - High irradiance condition

The alarm condition is unusual in this case (and is, in fact, not notified), but allows the user to avoid the application of a time condition: a “low irradiance” condition without a time slot would be triggered every night. Once the alarm condition has been saved, change the low production alarm to link it to that of the irradiation thanks to the *“enabling condition”*:

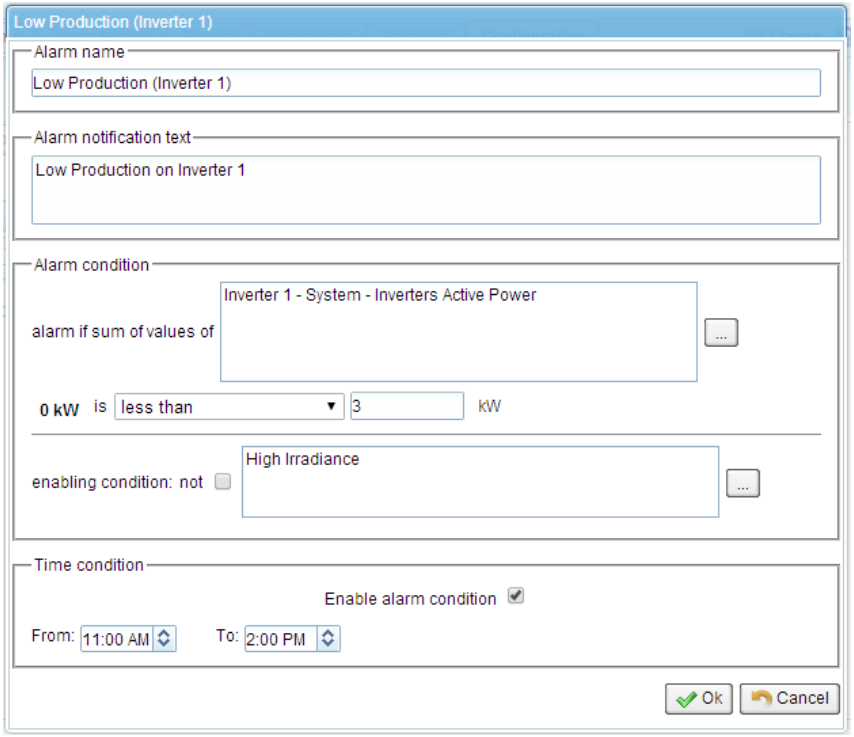


Figure 29 - Change low production alarm enabling condition

At this point the time condition can be removed from this alarm as well given that there will not be high irradiation during the night and the low production alarm will not be enabled.

It is useful to create an alarm that acts as an enabling condition for many others.
If there are 10 inverters it would then be possible to insert the "High irradiance" condition only once and use it in the 10 "Low production" alarms.

5.3.4 Synoptics configuration

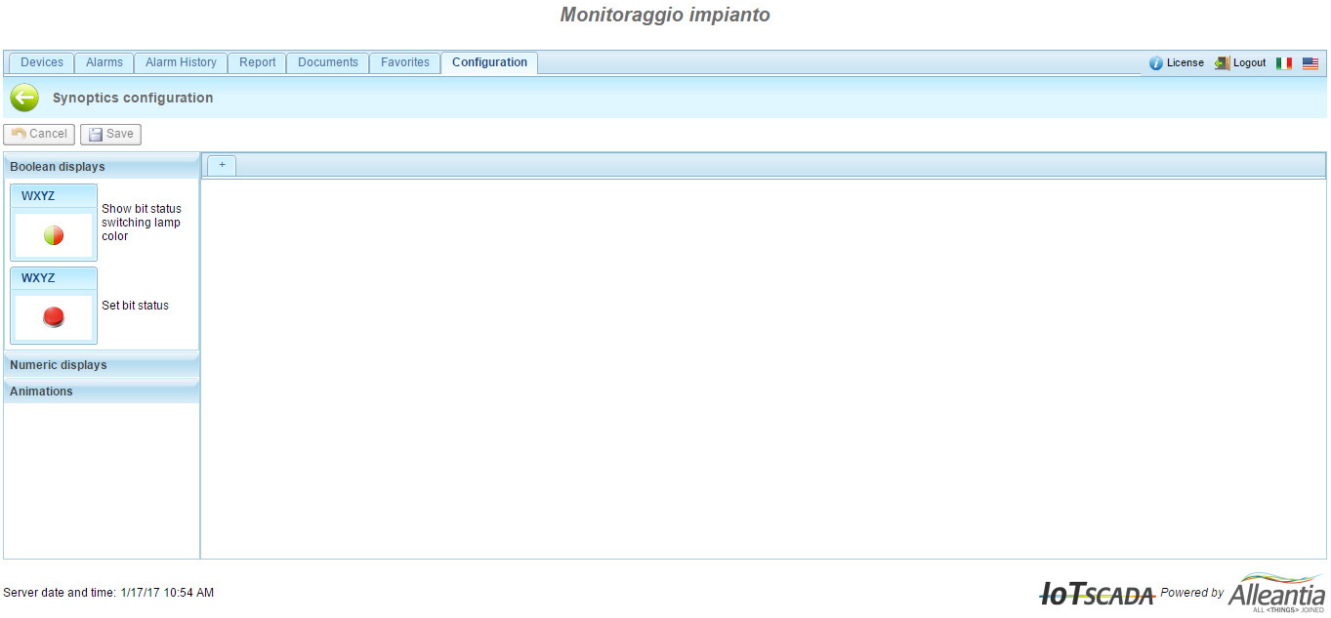


Figure 30 - Creation of system synoptics

In the *"Customization" -> "Synoptics configuration"* section you can create custom synoptics with a personalised background and measures.

To create a new synoptic, click on the + tab. A popup window will appear as in Figure 31, to choose the screen sizes most commonly used for tablets and monitors, the background and the title.

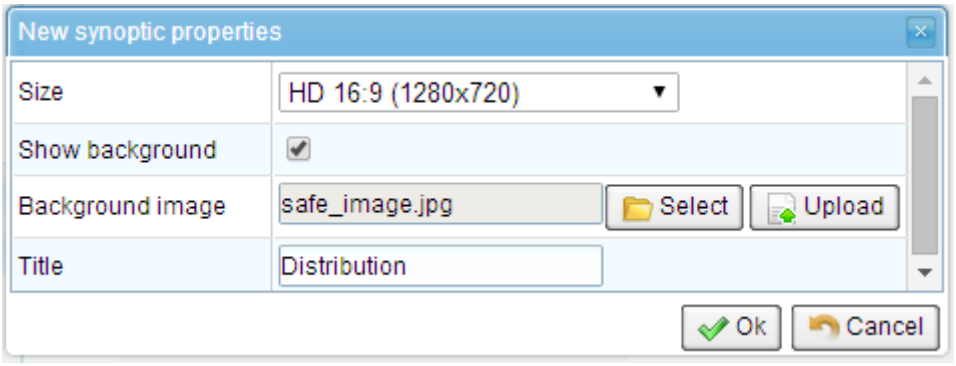


Figure 31 - Synoptics properties

5 Configuration

The IOT SCADA SERVER contains a catalogue of reusable images. In order to load an image in the catalogue, press the *"Upload"* button and choose the file from the hard drive of your PC/tablet. This will be loaded into the IOT SCADA SERVER and will be available for the creation of more synoptics. To reuse, press the *"Select"* button and choose from the catalogue images, as in Figure 32:

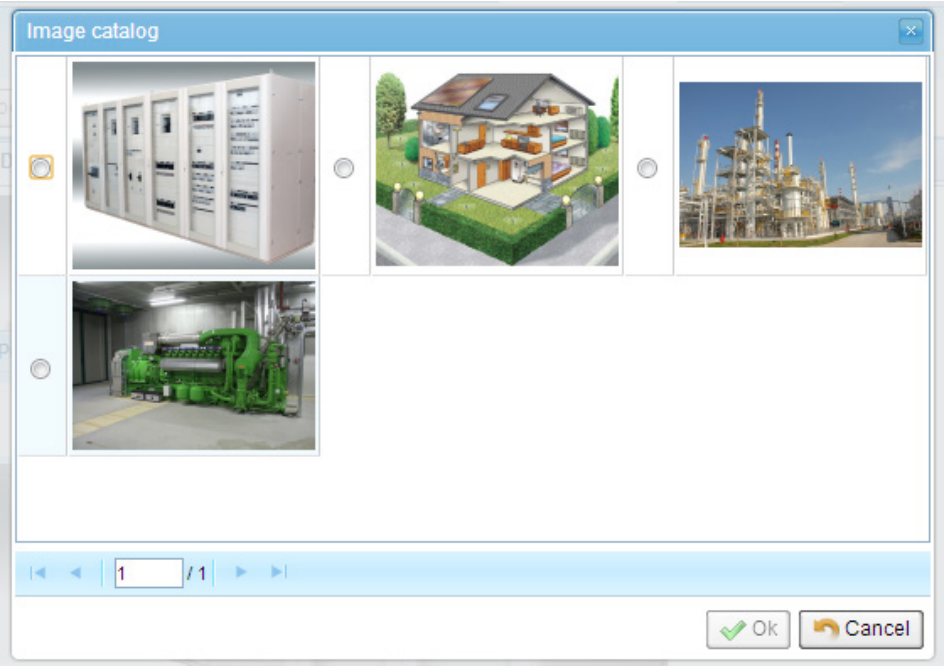


Figure 32 - Image catalogue

The image is uploaded in the original size and automatically resized depending on the size chosen for the synoptic.

At the end of the changes the empty synoptic will be displayed, as shown in Figure 33:

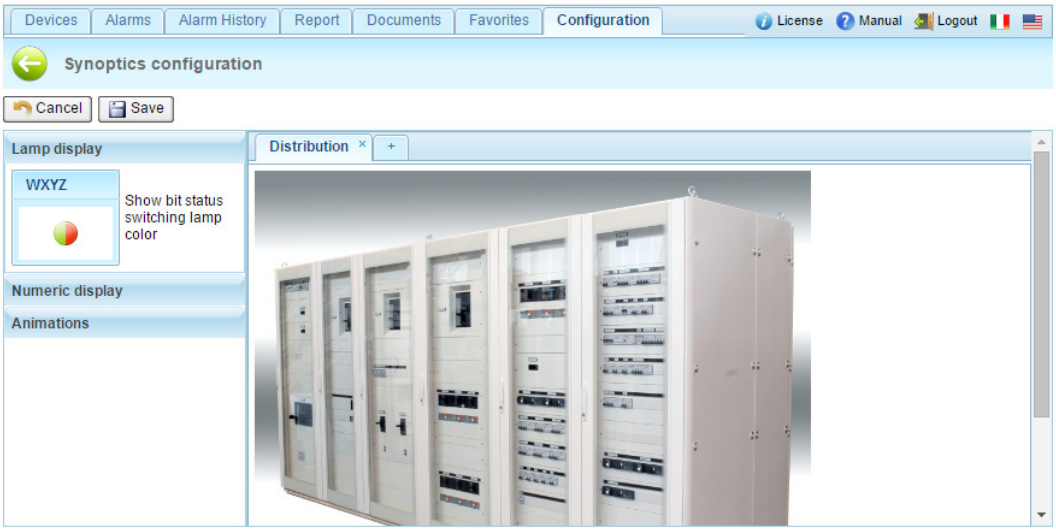


Figure 33 - Empty synoptic

To change the properties of the synoptic double click on the corresponding tab or on the background. The popup window in Figure 33 will appear again.

To delete the synoptic, click on the "X" in the upper right corner of the corresponding tab.

From now on it is possible to add the displays that will show the values of the measures in the system, which are of 2 types: numeric and visual (lamp) displays. The numeric display shows just numeric values, while the lamp display shows Boolean values.
These two displays are shown on the left side of the page. To add one, simply drag it on to the synoptic into the position where you want it to be shown. Once released, a popup window will appear as in Figure 34 and Figure 35 to change its properties.

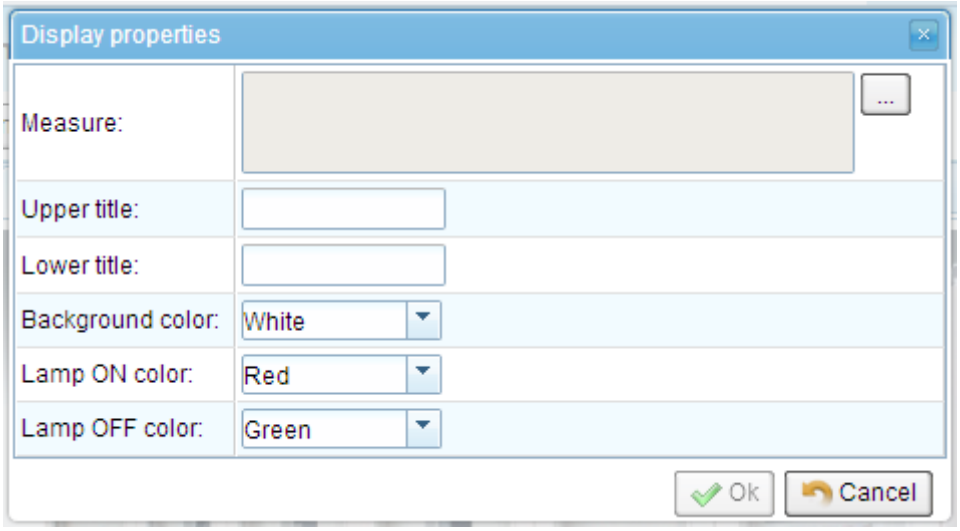


Figure 34 - Lamp type display properties

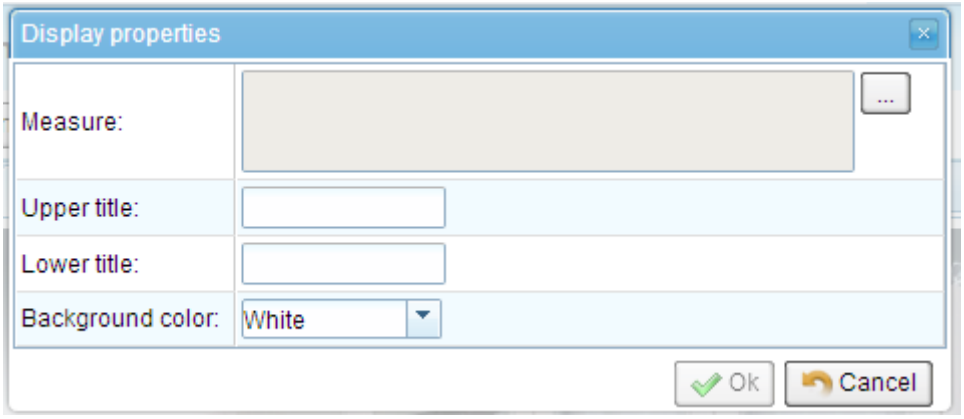


Figure 35 - Numeric type display properties

The measure to be shown, the upper (first line) and lower (second row) title, the colours of the background and of any lamp displays can be chosen.

Once the parameters have been entered, the synoptic will appear for example as shown in Figure 36:

Figure 36 - Synoptic with display

To subsequently change the properties of the display, double click on the displays themselves. The popup window in Figure 34 and Figure 35 will appear again, from which it is possible to delete the properties.

In the *"Animations"* section the synoptic in the home page can be automatically changed by selecting the check box *"Enable synoptic rotation"* and defining an interval in seconds.
Once defined the synoptic will appear in *"Synoptic"* window of the graphic interface (see Figure 35 at the top left).

5.4 Interface and Cloud services

5.4.1 E-mail and SMS notifications

The IOT SCADA SERVER can automatically send e-mail and SMS notifications in the following cases:

- an alarm condition occurs
- notification of the backup occurring (see Sections 5.4.2 and 5.4.3)

To take advantage of these features, *"Cloud Services" -> "E-mail and SMS configuration"* must be enabled.

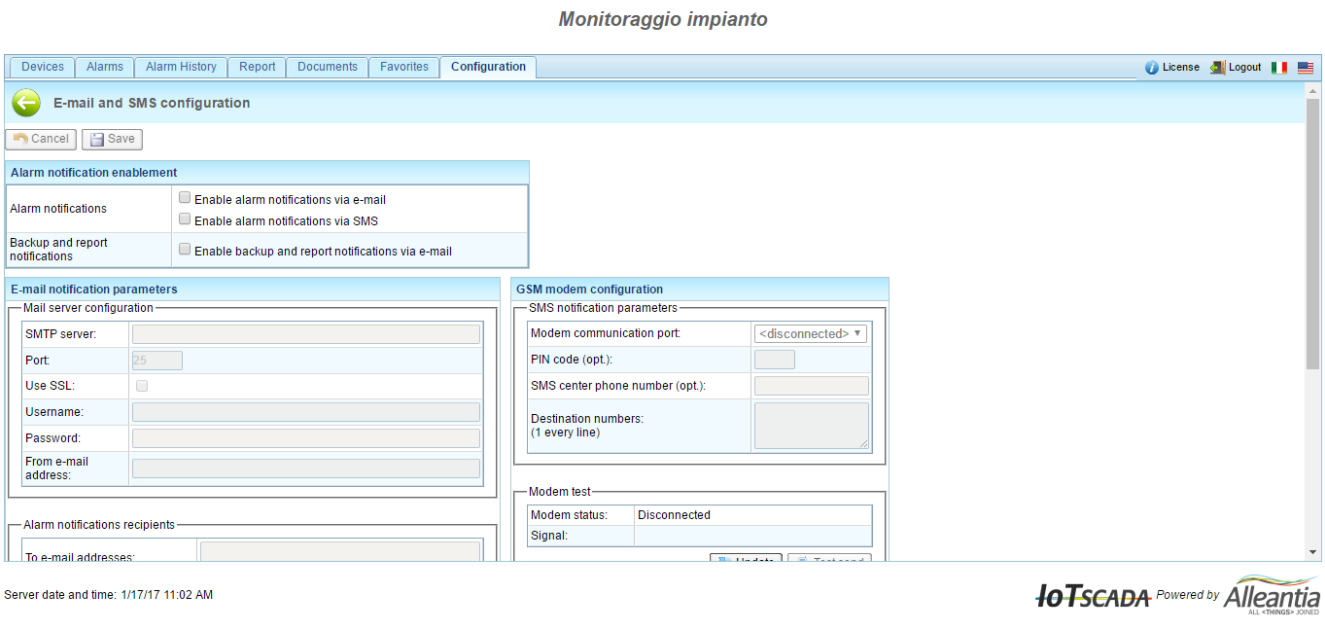


Figure 37 – Alarm and data logging configuration

After having ticked at least one checkbox to enable notifications, the email notification in the *"E-mail notification parameters"* and SMS notification in the *"GSM modem configuration"* can be configured.

For the e-mail notification the details of your SMTP server for sending email and that of the recipient must be included. At the end a test email can be sent to verify the correctness of the settings entered by pressing the corresponding *"Send test mail"* button.

For the SMS notification a GSM modem must first be connected to one of the IOT SCADA SERVER, serial ports, selecting from among those supported. The serial port must be properly configured according to the GSM modem manufacturer's instructions, see Section 5.1.1. The parameters of the recipients must subsequently be entered.

If the settings are correct, following the application of the changes, the IOT SCADA SERVER will connect to the modem and *"Modem Status: Connected"* will appear in the *"Modem Test"* box; then check the GSM signal strength in the appropriate *"Signal"* indicator and evaluate the displacement of the GSM antenna or the purchase of a magnified one if the signal is low, otherwise an SMS alarm notification may not be received.

You can send a test SMS to check the correctness of the settings entered by pressing the corresponding *"Send test mail"* button.

5.4.2 Dropbox connection

An existing Dropbox account can be indicated as an additional destination for the backup files. This account can also be used to upload the documents generated by IOT SCADA SERVER on the Dropbox by pressing the Send to Dropbox buttons in the application (for example, in energy reports). Before connecting a Dropbox account make sure internet connection is available on the device from which you are configuring.

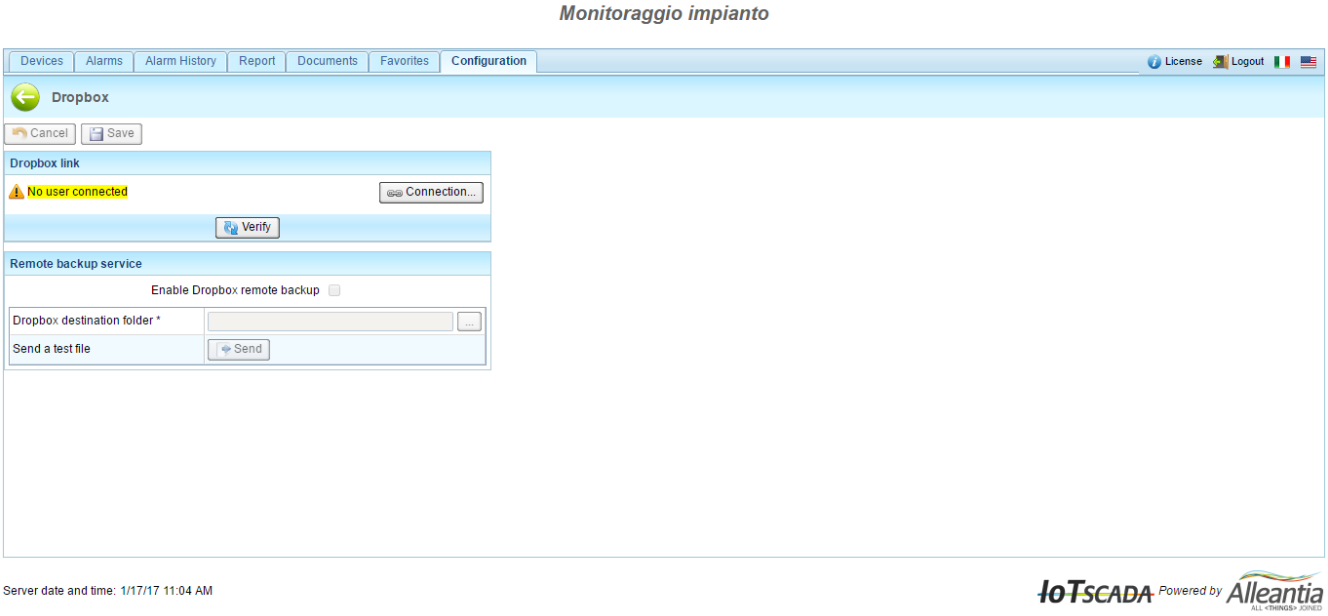


Figure 38 - Dropbox account configuration

Go to *"Configuration" -> "Cloud Services" -> "Dropbox"* and press the *"Connection..."* button to start the connection procedure of the IOT SCADA SERVER to a Dropbox account. The popup window of Figure 39 will open.

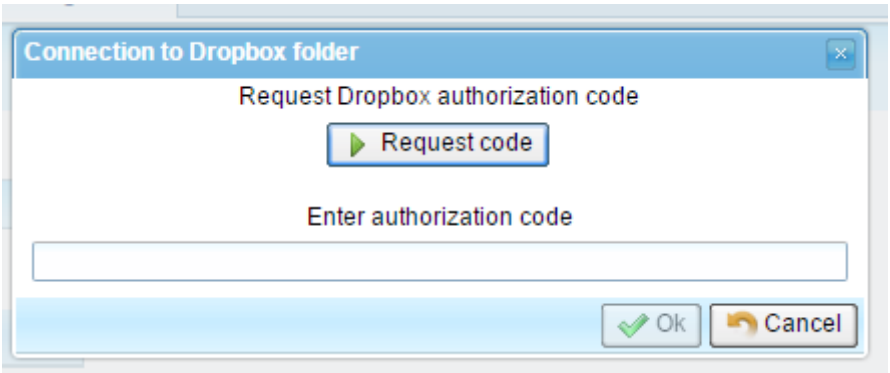


Figure 39 - Authorization code request

Press the *"Request code"* button to access your Dropbox account, if necessary by entering your email and password (Figure 40).

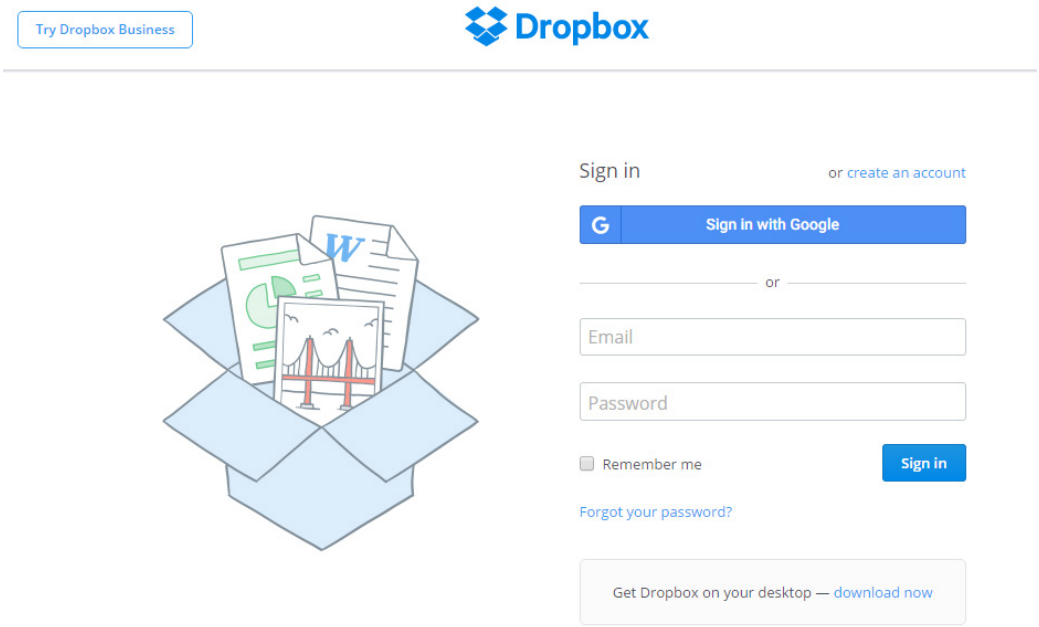


Figure 40 - Dropbox account access

On the subsequent screen, click *"Allow"* to allow the IOT SCADA SERVER access to your Dropbox folder (Figure 41).

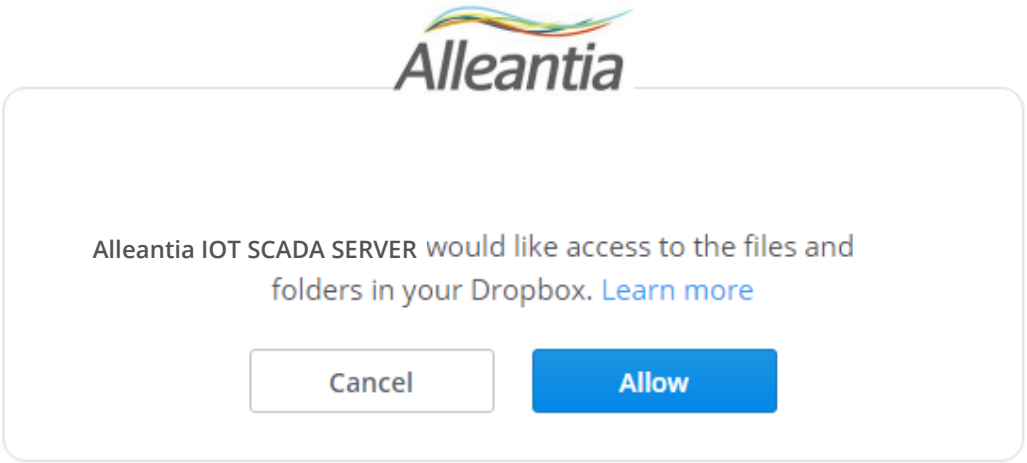


Figure 41 – Authorization

Enter the code shown in Figure 42 in the start popup window (Figure 39).

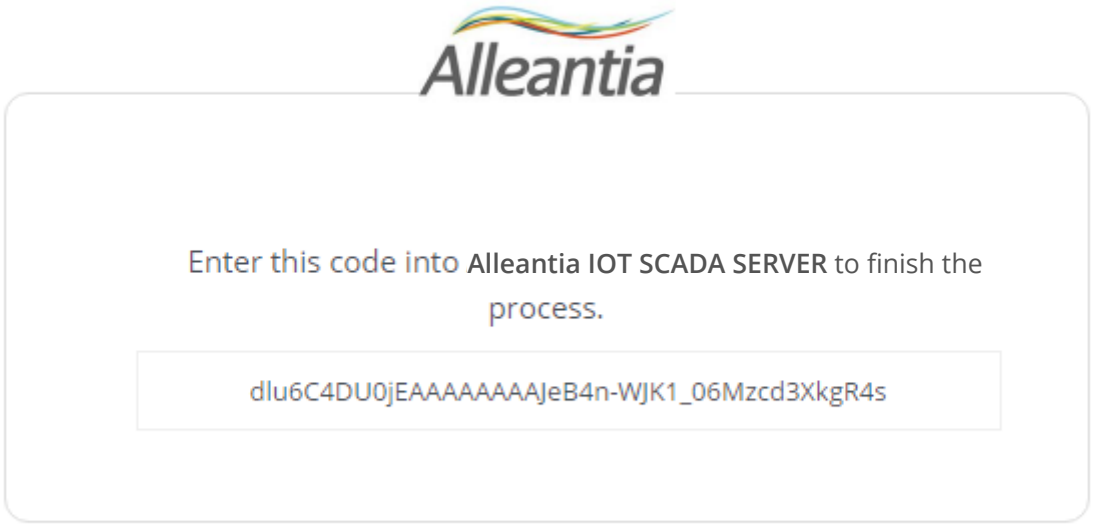


Figure 42 – Authorization code

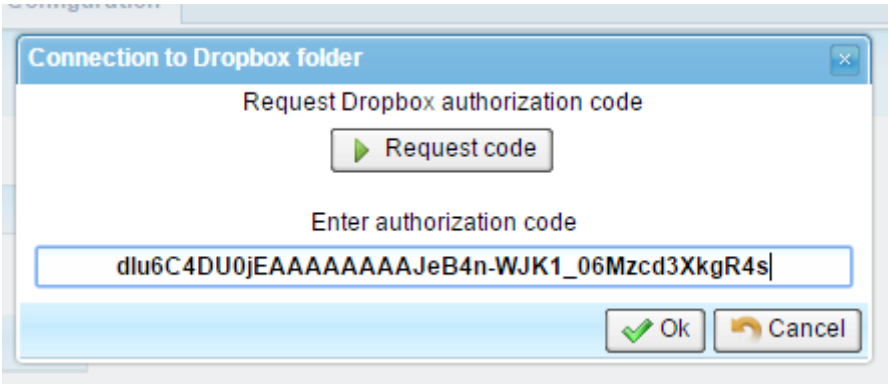


Figure 43 - Authorization code shown in IOT SCADA SERVER

Press *"Ok"* to end the procedure. If successful, the account appears correctly connected (Figure 44).

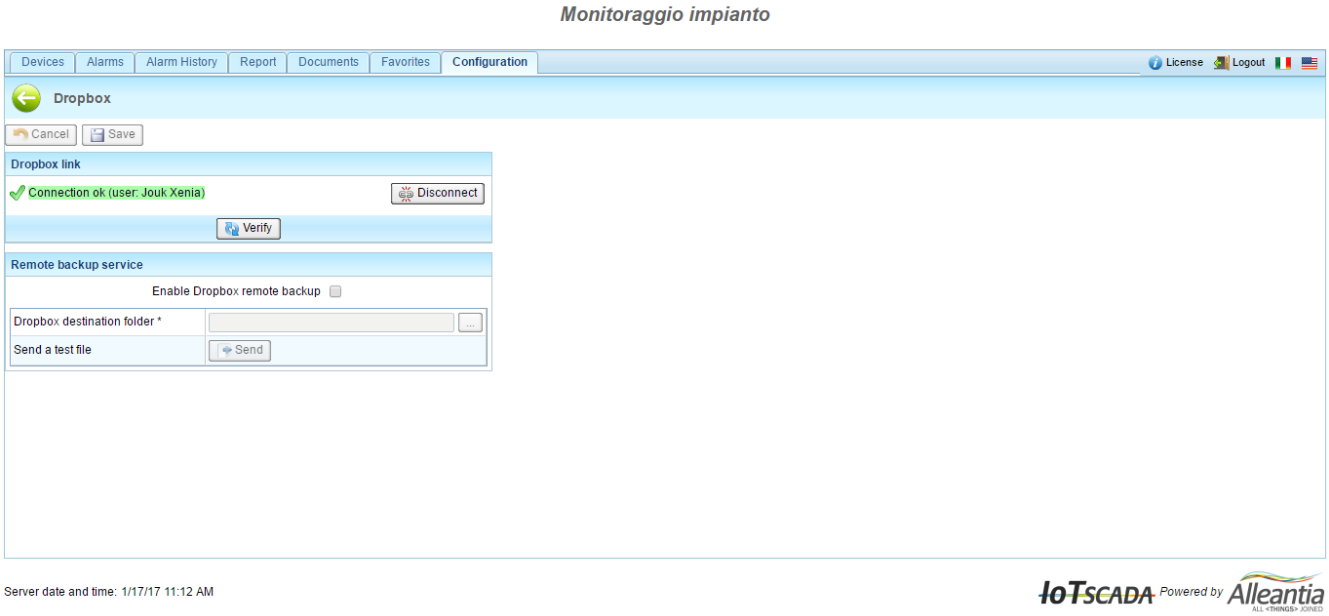


Figure 44 - Dropbox account connected

At this point the *"Send to Dropbox"* buttons of IOT SCADA SERVER can already be used to send documents on Dropbox. To disconnect the account in the future, simply press the *"Disconnect"* button.

If you want to enable the sending of backups to Dropbox press *"Enable Dropbox remote backup"* (Figure 45) and choose a destination folder for the files by clicking on the button "...". To test the backup feature, send a test file to the specified folder by pressing the *"Send"* button. When finished, press the *"Save"* button to save the configuration.

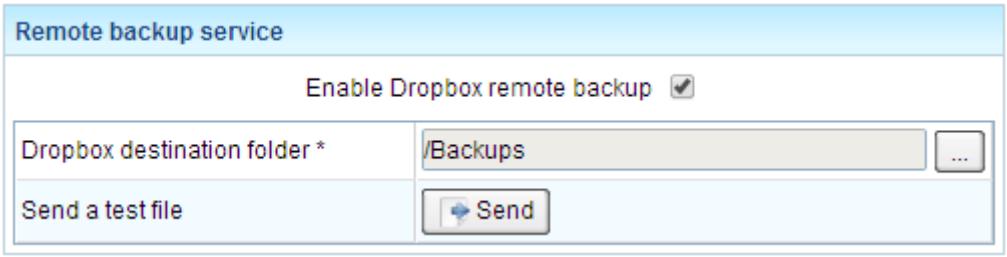


Figure 45 - Backup parameters

The backup files sent to Dropbox are not related to those of any FTP backup: in other words, complete backups of IOT SCADA SERVER will be present on both Dropbox as well as FTP.

5.4.3 OneDrive account

An existing OneDrive for Business account can be indicated as an additional destination for the backup files. This account can also be used to upload the documents generated by IOT SCADA SERVER on the Microsoft cloud. Before connecting OneDrive for Business account **make sure internet connection is available on the device from which you are configuring.**

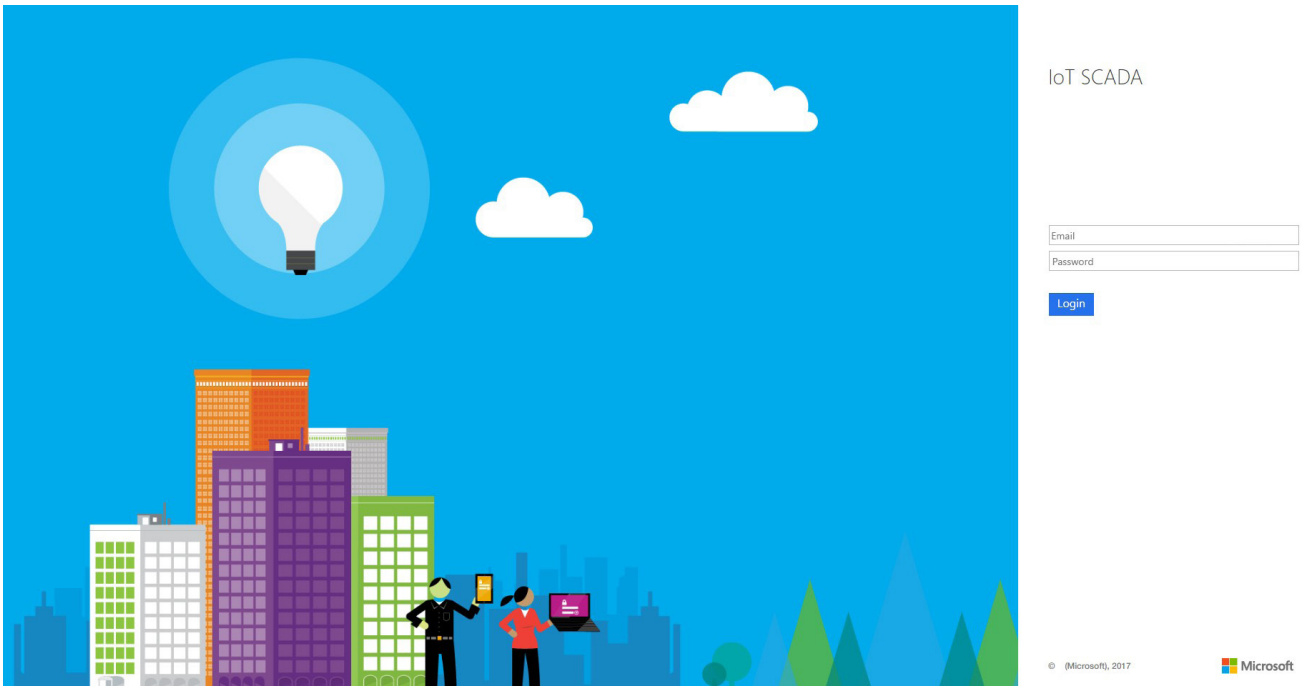


Figure 46 - OneDrive for Business account

CAUTION: IT IS POSSIBLE TO SYNCHRONIZE ONEDRIVE BUSINESS ACCOUNT ONLY

Press the *"Connect Account"* button. The popup window will open with a request to insert email and password of the account to be synchronized. If successful, the account appears correctly connected. The IOT SCADA SERVER will synchronize with the OneDrive for Business cloud for the backup saving.
At this point the *"Send"* button of IOT SCADA SERVER can already be used to send documents on OneDrive for Business. To disconnect the account in the future, simply press the *"Disconnect"* button.

If you want to enable the sending of backups to OneDrive for Business, press *"Enable OneDrive remote backup"* and choose a destination folder for the files by clicking on the button "...". To test the backup feature, send a test file to the specified folder by pressing the *"Send"* button. When finished, press the *"Save"* button to save the configuration.

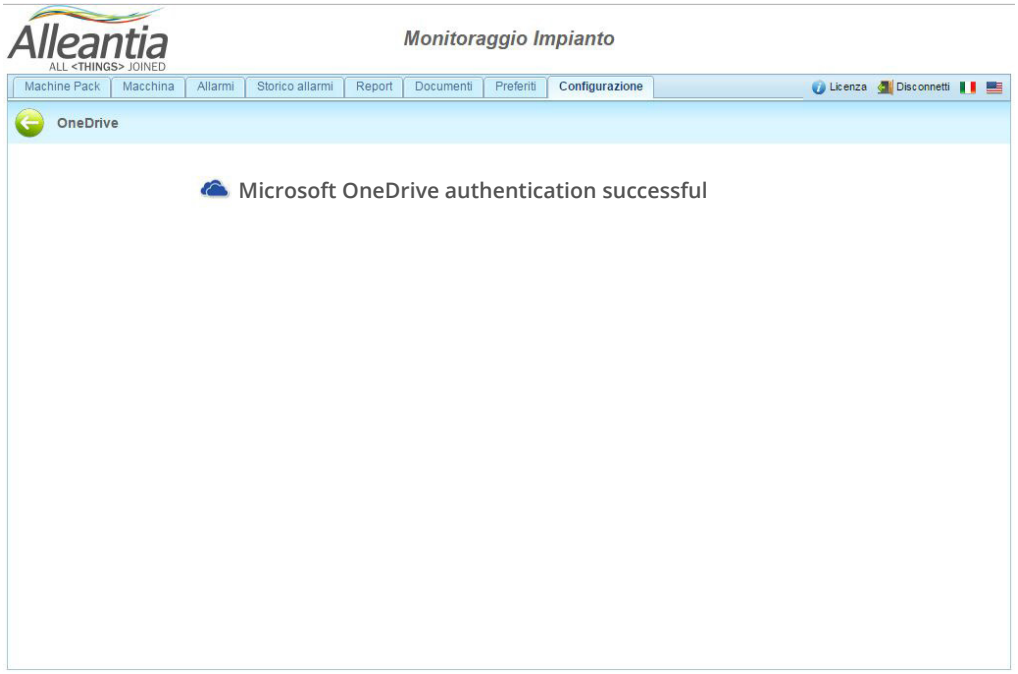


Figure 47 - OneDrive for Business authorization

5.4.4 FTP Backup

The remote backup function to FTP provides for the creation and sending of daily backups of IOT SCADA SERVER data and the configuration on an FTP server in order to ensure recovery in case of hardware failure of the internal hard disk.
To use this function an FTP server must be available on which to make the transfer, as well as all the parameters necessary for its access, which are to be entered in the *"Configuration" -> "Cloud Services" -> "FTP remote backup"* section:

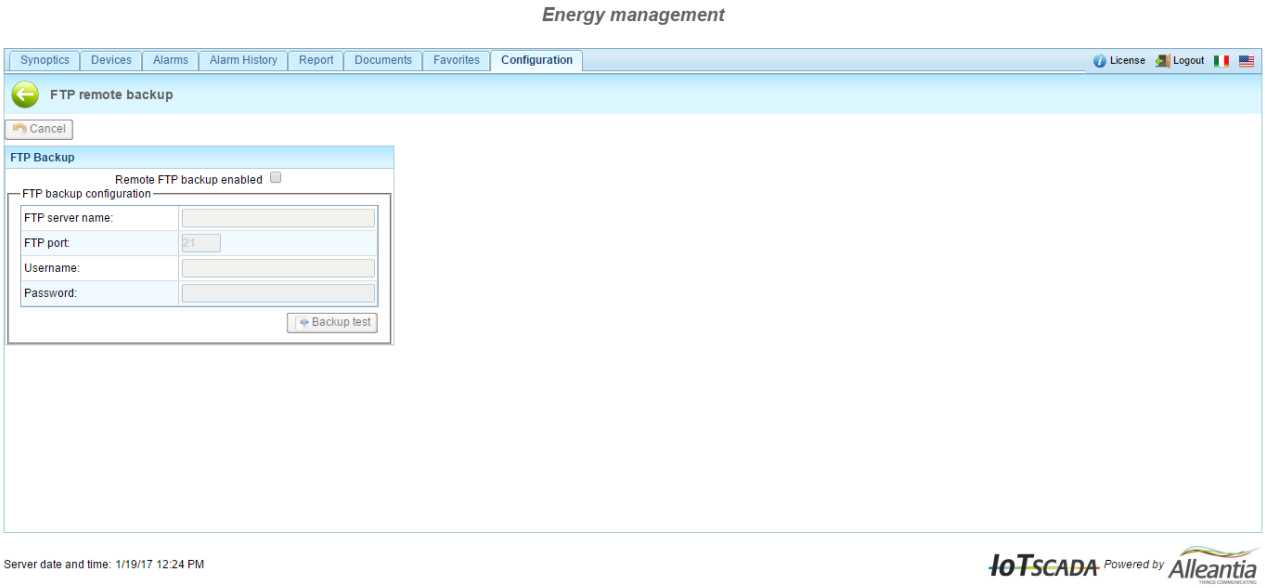


Figure 48 - FTP remote backup configuration

A test file can be sent to check the correctness of the settings entered by pressing the corresponding *"Backup test"* button.

5.4.4.1 Details of the transferred files

IOT SCADA will send 3 files every night called:
backup_*date*_*hour*.zip
backup_*date*_*hour*.zip.md5
backup_*date*_*hour*.zip.sig
in which *date* represents the date, and *hour* the UTC time in which the backup was made such as, for example, “backup_23062012_0144.zip”.

The file with the zip extension contains the CSV file with the IOT SCADA data and an encrypted file with its configuration.

CAUTION

The backup performed by this IOT SCADA SERVER feature is incremental. To rebuild the system in the event of failure all the files transferred over time are required. The remote backup can be interrupted at any time by disabling it in the dedicated configuration section. If subsequently re-enabled, it will resume the backup of your data from where it was last interrupted.

The file with the md5 extension contains a signature with the MD5 algorithm to verify the correct transfer of the file. The file with the .sig extension contains a RSA signature to verify that the file was actually generated by an Alleantia product and has not been manipulated to alter the content.

The remote backup function is incremental in respect to the previous backup.
If the previous backup is of the previous night, the zip will contain the data of a single day. If the previous backup does not exist, or it is the first run, the zip file will contain ALL the data of the system starting from the commissioning of the plant.

5.4.5 Connection to SQL Server

It is possible to indicate Microsoft SQL Server as a destination of all data, events and alarms collected from the IOT SCADA SERVER.
First, click the *"Download Script"* button to download the sql script, then carry it out on the machine with Microsoft SQL Server to create the database tables, where the IOT SCADA SERVER data will be downloaded. After, the connection parameters will be inserted in database in the configuration panel. You can test the correct configuration, clicking the *"Connection test"* button.
If everything works correctly, click the *"Save"* button to save the configuration.
From this moment on, the IOT SCADA SERVER will download its data in configured database. The refresh rate can be changed from interface.

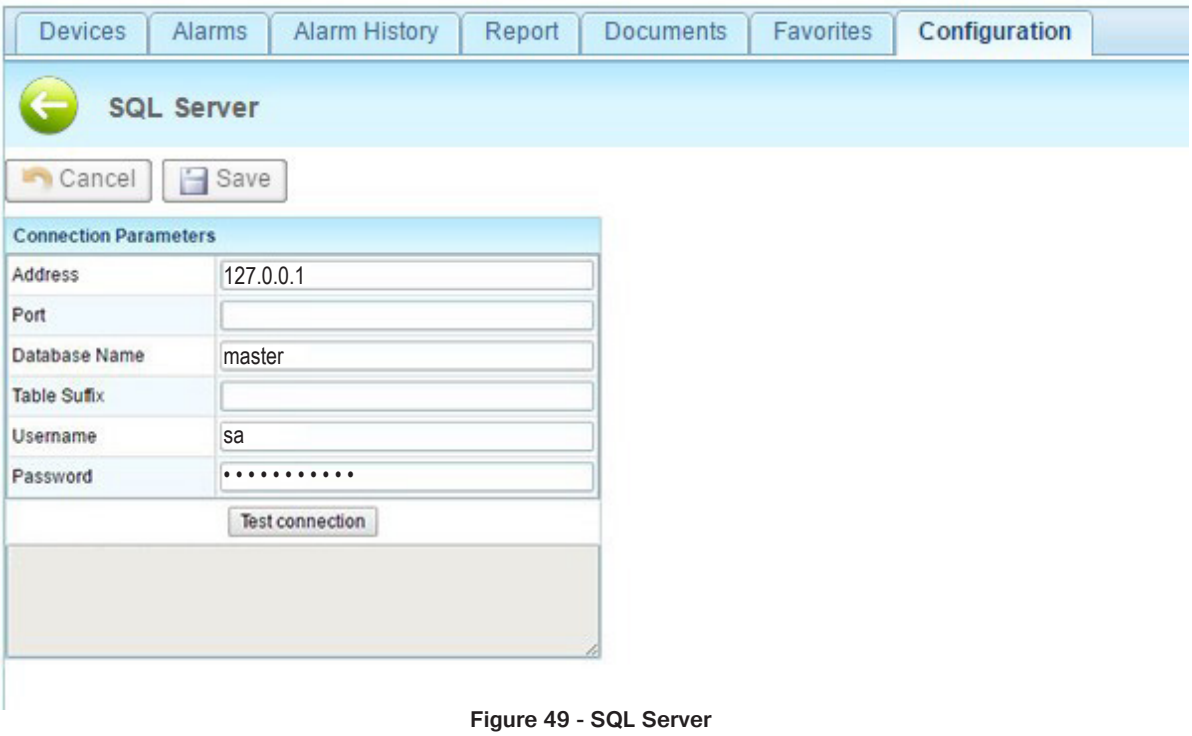


Figure 49 - SQL Server

5.4.6 Connection to Azure IoT Hub

In Microsoft Azure, after creating IoT Hub, get the connection string.

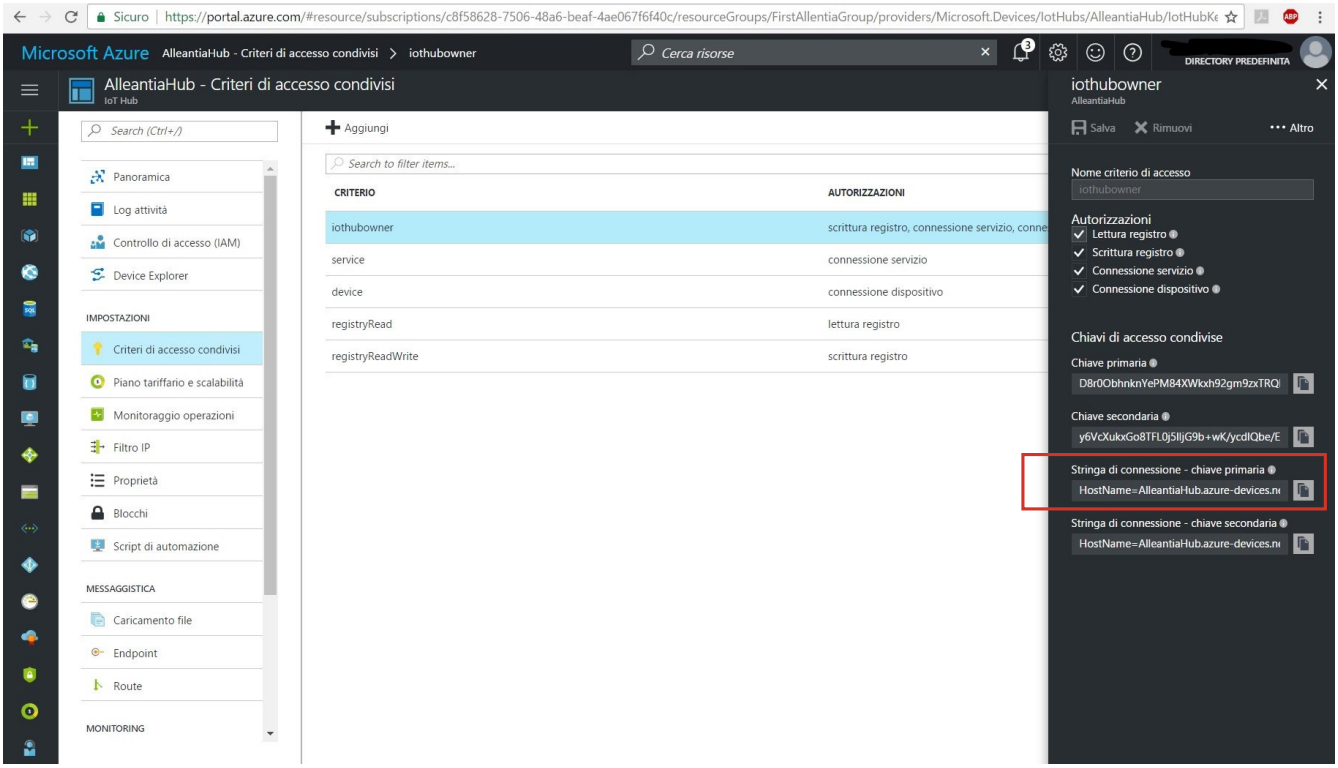


Figure 50 - Microsoft Azure

Insert the string into the box in configuration panel. Then press “Create IoT Hub Identity” button to register the device in IoT Hub.

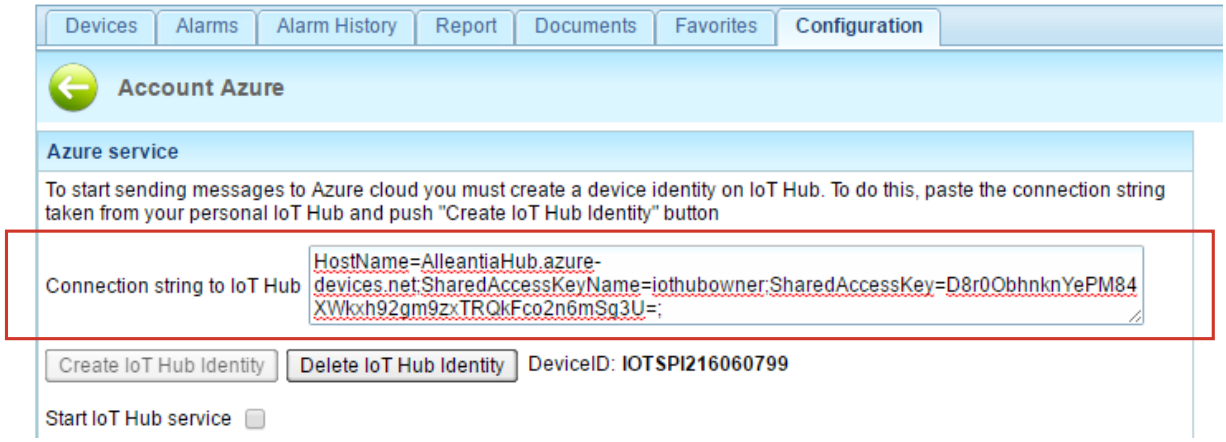


Figure 51 - Connection string

If the registration was successful, *Device ID* will be displayed next to the button.

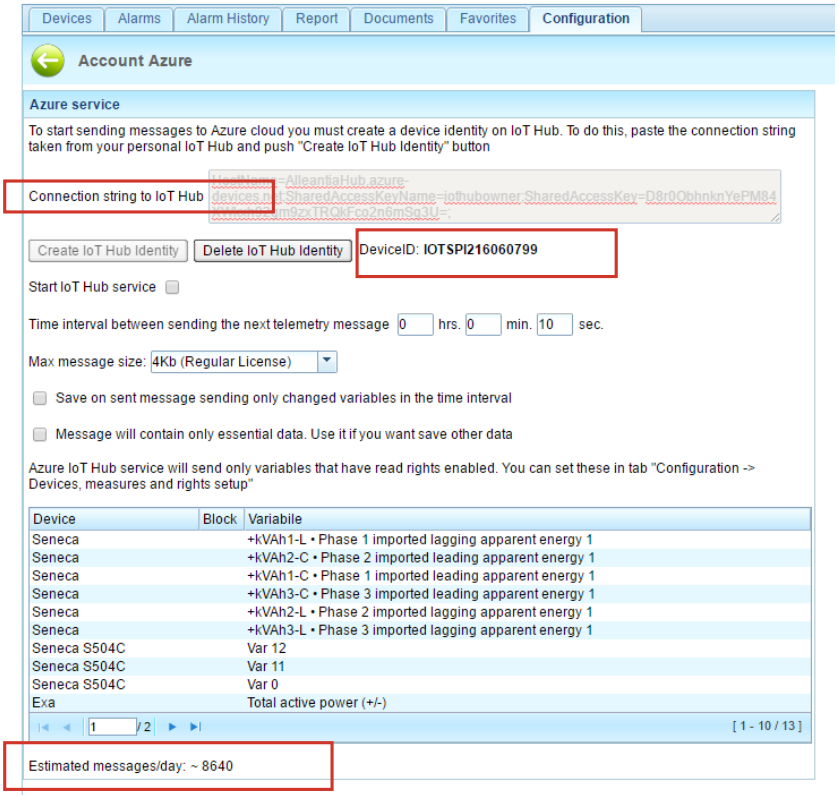


Figure 52 - Account Azure

Now you can set time interval between sending next telemetry message and mske other settings. It will send messages only for variables/alarms with read/write/alarm rights (Figure 53).

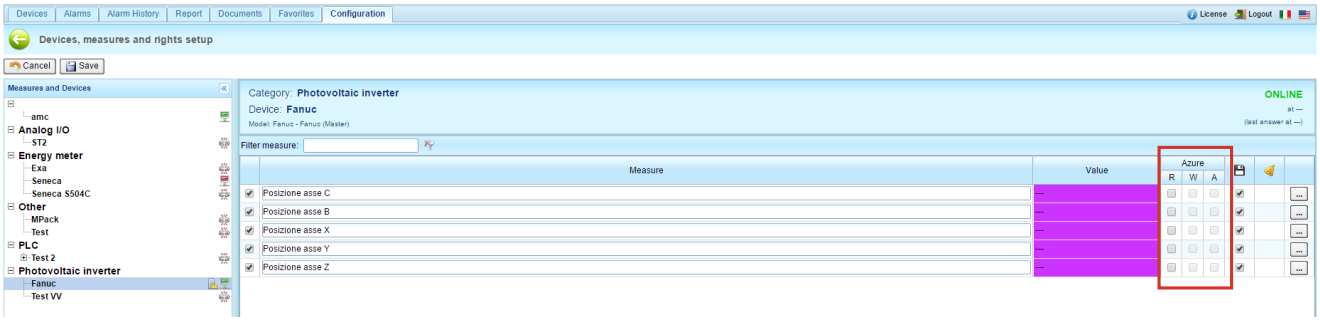


Figure 53 - Devices, measures and rights setup

You can set these rights in *"Devices, measures and rights setup"*, *"Synoptics measures configuration"* and *"Custom alarms"* sections.
Write permission can be enabled only for measures which can be modified from outside. The alarms' permissions (A) can be enabled only for measures defined as an alarm in Xmod driver.
Finally, check the checkbox *"Start IoT Hub service"* to activate. Depending on the selected options, estimated messages sent per day will be shown (Figure 52).

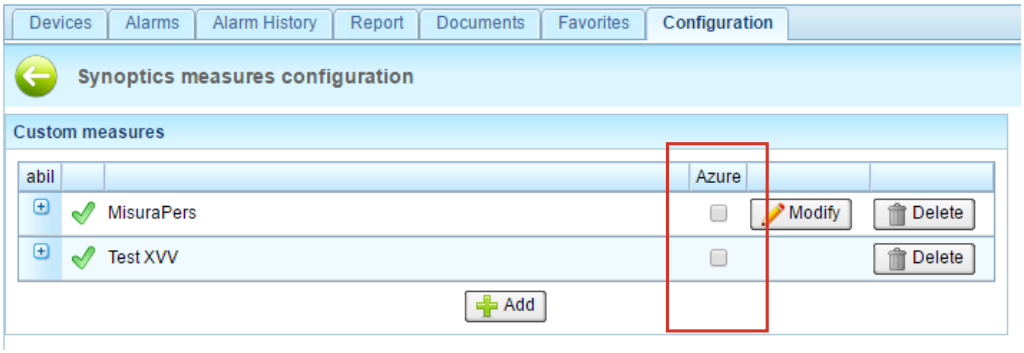


Figure 54 - Synoptics measures configuration

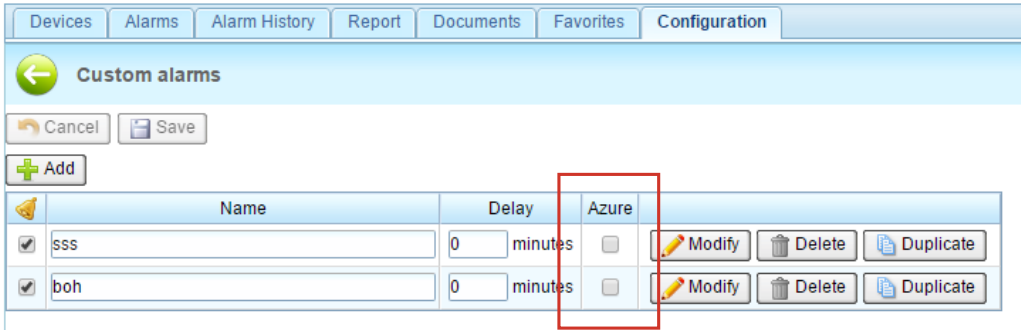


Figure 55 - Custom alarms

The service uses MQTT v3.1.1., to run this protocol the 8883 port or web socket of 443 port are needed. Make sure that these ports are open.

5.5 Information

In Section Information you can find information about the system and change such its data as licence and device catalogue.

5.5.1 Device catalogue

Every IOT SCADA SERVER system is released with database of connected devices with default configurations. This may contain not all the devices of the Alleantia's Library of Things, which is continuously updated and is available here http://cloud.alleantia.com/info/products.zul. Therefore you can download one or more .xmod files of devices configuration and upload it in the used IOT SCADA SERVER system, using the functionality of this section. The user can, in the same way, insert in the system ad hoc configured devices (e.g. PLC) using the Alleantia's tool
http://cloud.alleantia.com/xmod/convert.zul which creates an .xmod file for every device.
In section *"Information" -> "Device catalogue"* a window with the existing library of devices will open.

Figure 56 – Device catalogue

Pressing the *"Add"* button a popup window will open, that allows you to select different types of files: .xmod files of device's library to connect, and .pdf files for device's user manual.

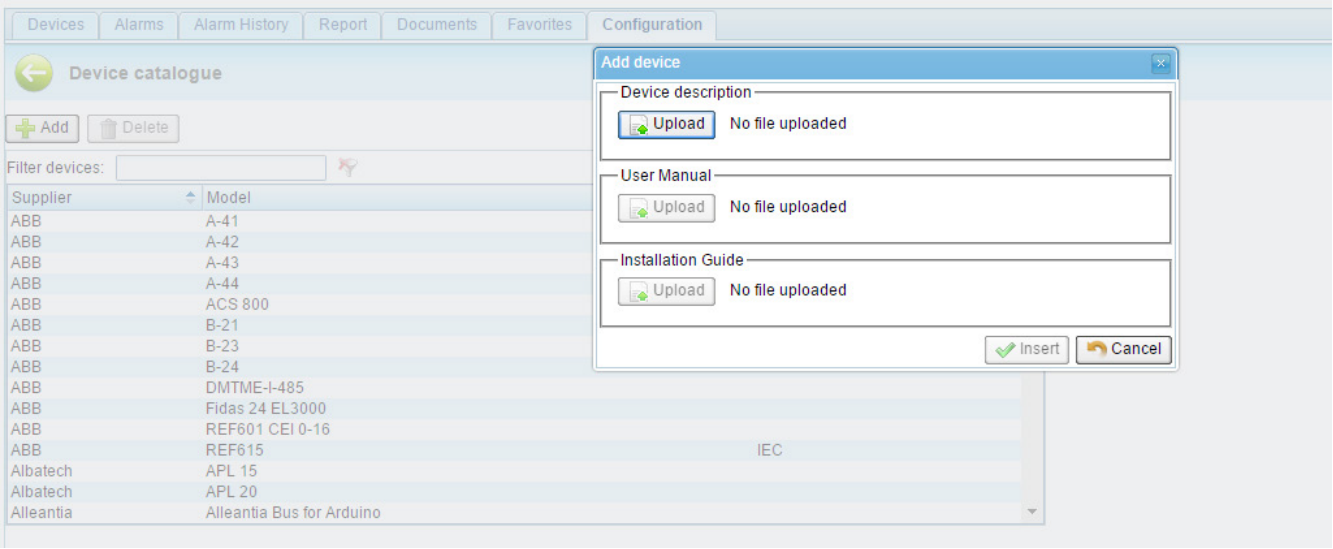


Figure 57 - Add device

Pressing the "Upload" button it will be possible to navigate the file system and select the file you need. For the .xmod file, the system recognizes and verifies correctness of the file and will permit or not to insert it in the IOT SCADA SERVER system's database.

5.5.2 License management

In this section you can verify the license key or insert a new license (e.g. of updating or upgrading) and insert the related activation key provided by Alleantia or by its vendor.

In section *"Information" -> "License management"* a popup window will open with the activation key, possibility to upload a new license and the installed license characteristics, and options:

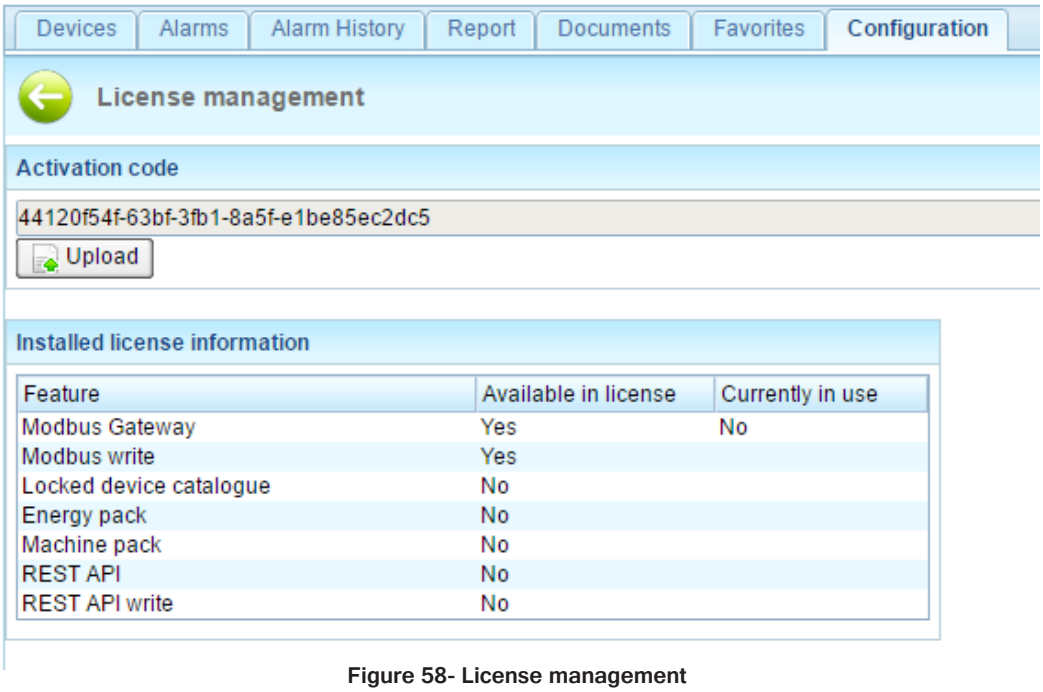


Figure 58- License management

5.5.3 Informations

In this section the version of installed software license is provided.

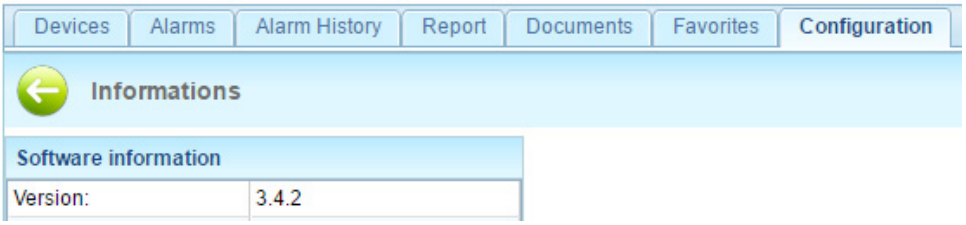


Figure 59 - Informations

5.5.4 Logs

It is possible to generate audit log in different sections of software, useful to debug problems in different levels: communication protocols, devices, user interfaces.

Go to section *"Information" -> "Logs"* a page for the logs configuration will open.

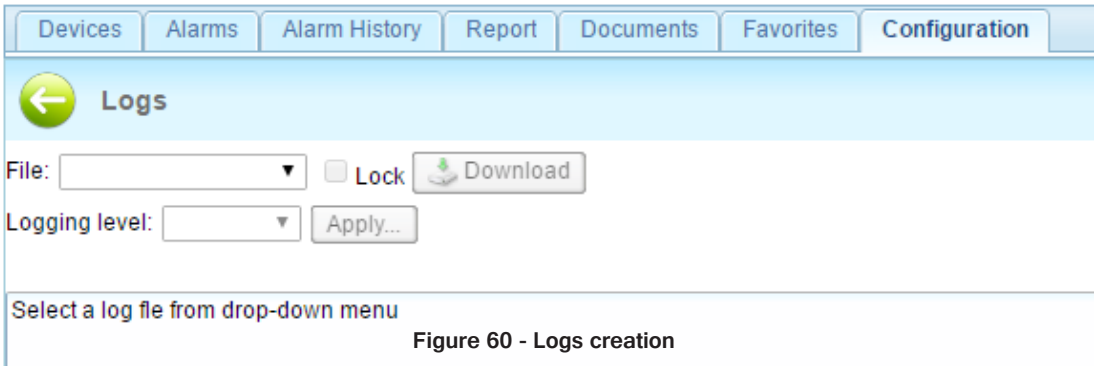


Figure 60 - Logs creation

3 logs files can be generated: "Logging engine", "Graphic interface" e "Protocol traffic". The levels of logging that can be selected are: ERROR, WARN and DEBUG. It is possible to download generated logs files, clicking the *"Download"* button.

6 User interface

6.1 Synoptics

Figure 55 shows a complete synopsis of a system in which the 2 synoptics have been created in section *"Configuration" -> "Customization" -> "Synoptics configuration"* (see Section 5.3)

Figure 61 - Home page with synoptics

This screen is automatically displayed on the HDMI output of the IOT SCADA SERVER.
The *"Synoptics"* tab is not shown if there are no configured synoptics, in which case the IOT SCADA SERVER home page becomes that of the *"Devices"* tab.

If a device in the system is in alarm, the *"Alarms"* text in the respective tab turns red.

The background of the text measures turns purple if at least one device from which they draw a value does not respond to requests.

6 User interface

6.2 Devices

6.2.1 System measures display

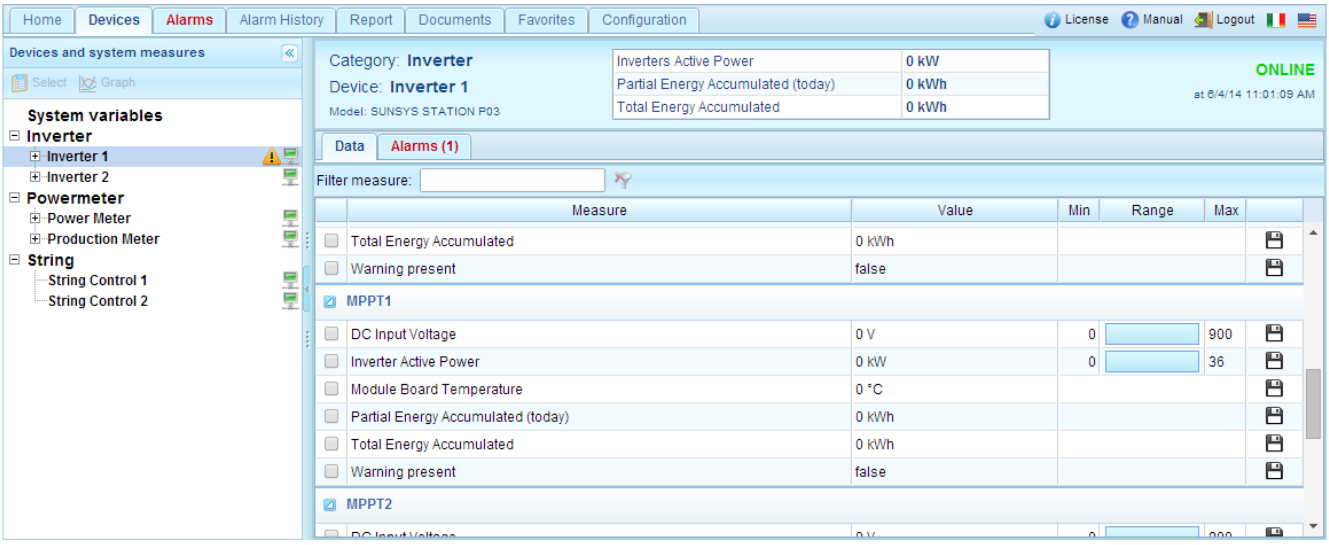
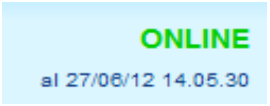
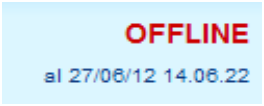


Figure 62 - System measures display

All of the devices being polled by the IOT SCADA SERVER can be seen in the tree menu structure on the left, sorted by category, and beside each device there is an icon that represents the reachability state. If operating normally the  icon will appear, and if the device is not reachable the  icon will appear; if there are alarms for a device, an additional warning icon  will appear next to the name, and if some measures were not read correctly the  icon will appear.

Once you select a device, the reachability state will be replicated in area on the right as well, together with the date and time of the last communication attempt made:





CAUTION
If the device is not reachable, first ensure that the device is turned on, then check the wiring and finally the configuration of the IOT SCADA SERVER.

6.2.1.1 Data and alarms display

The device measures read are divided into the two tabs *"Data"* and *"Alarms"*. Information and icons can be associated with each:


Logging enabled


Logging disabled


Alarm enabled


Alarm disabled


Active alarm

During normal operation the *"Alarms"* tab will look the same as the *"Data"* tab. In the presence of active alarms, however, the text of the *"Alarm"* tab will appear in red and the number of active alarms will be indicated. Selecting this tab will display all the measures associated with an alarm and those in active alarm condition will have a red background:

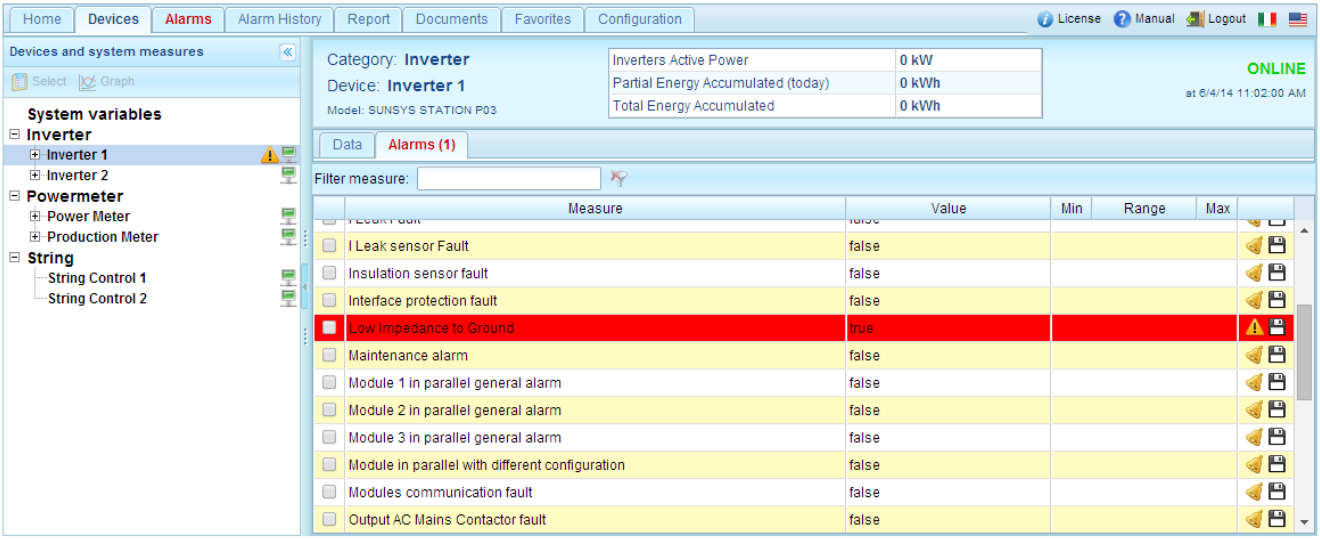


Figure 63 - Measures in alarm state

In the event that the device is offline, the background colour of all its measures will be purple and the value displayed will be that related to the last valid reading, or a series of dashes if there has been no communication:

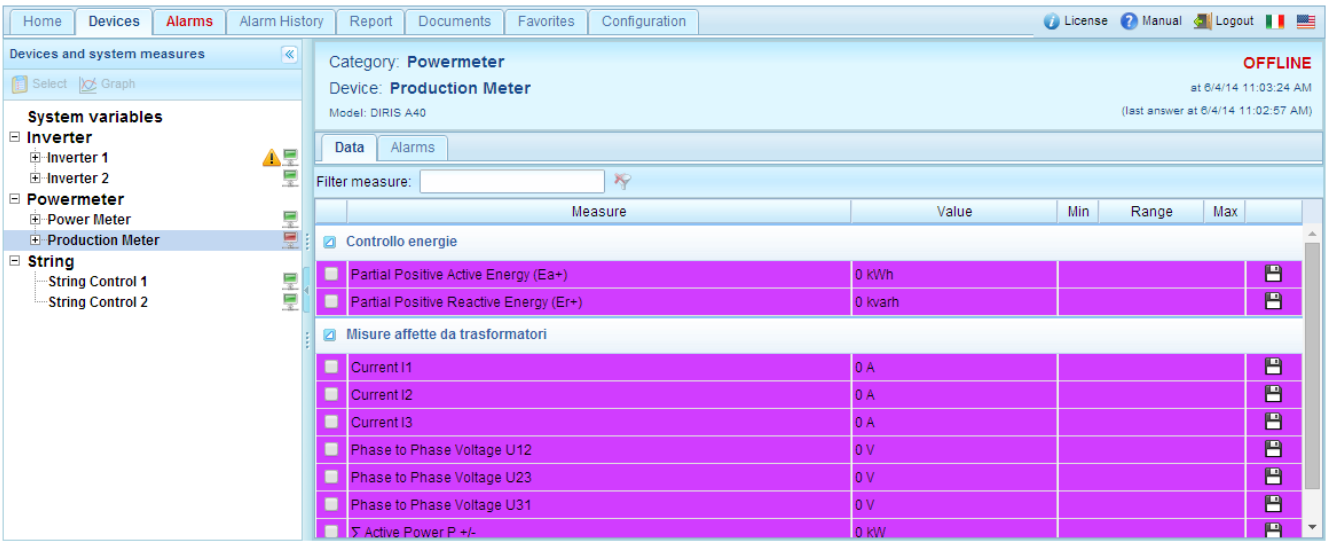


Figure 64 - Communication error device

To facilitate the search for a measure, it can be filtered by name with the appropriate field:

Figure 65 - Measure name filter

Or use the breakdown in sections, if any, selecting a single section from the tree menu structure on the left, such as, for example, “MPPT2”, which will result in the closure of all the sections except that selected, making visible only part of the device measures:

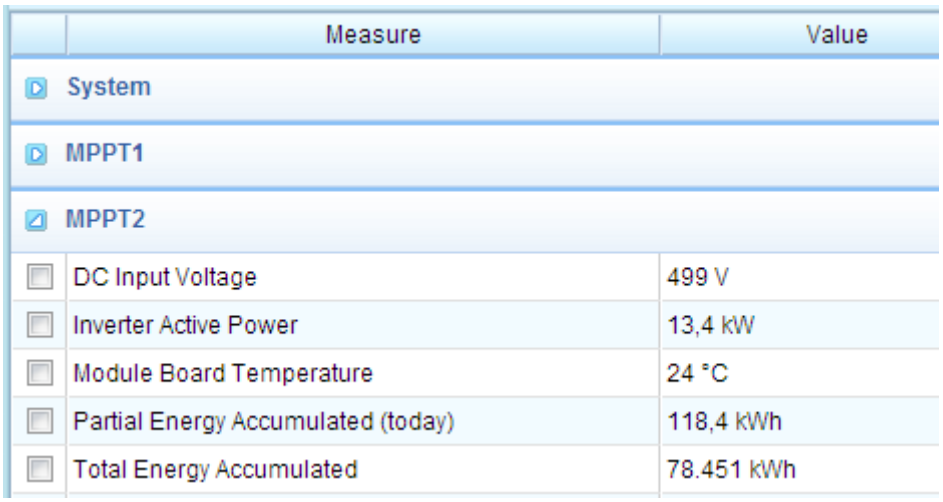
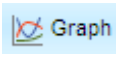


Figure 66 - Device sections

6.2.2 Graphs

To generate a graph of the time trend of one or more measures, select measures of interest by checking the appropriate box and then press the button:



CAUTION

The graph can only be generated for measures that were recorded in the time interval chosen. To change the recording state of a measure see Section 5.2.3.

A screen will appear as in Figure 61:

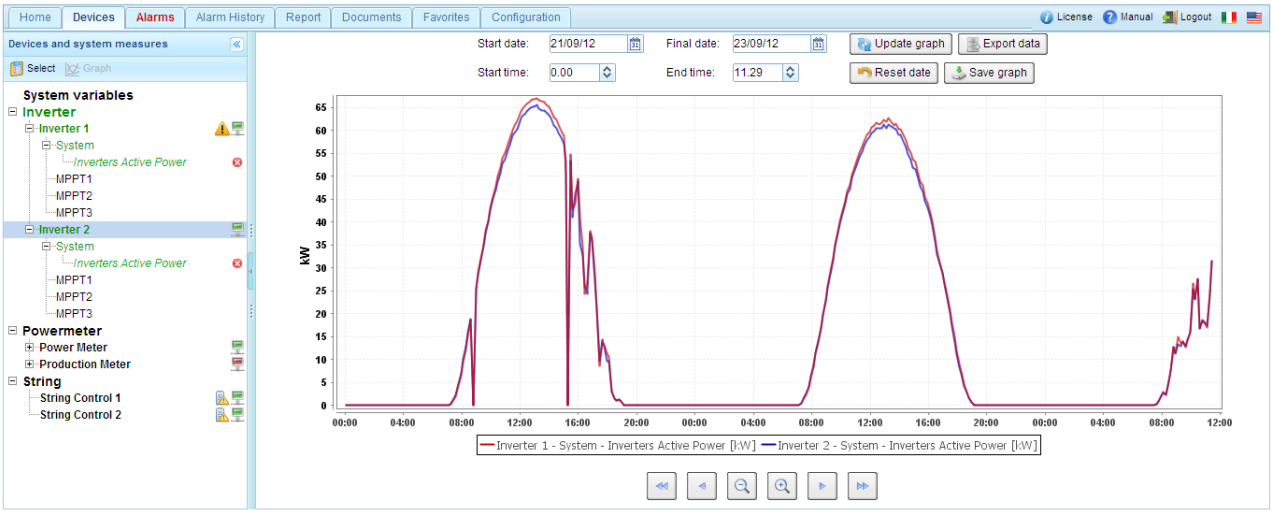


Figure 67 - Graphs

The temporal controls for the generation of the graph are located at the top. The default date and time interval runs from the current date and time to midnight on the previous day. These can, however, be edited and a new graph generated by pressing the *"Update graph"* button.
To restore the default interval, press the *"Reset date"* button.

Once a graph has been created, the reference time interval can be changed using the buttons below:

 moves the time interval back by 90%

 moves the time interval back by 40%

 decreases the time interval by 20%

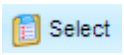
 increases the time interval by 20%

 moves the time interval forward by 40%

 moves the time interval forward by 90%

The graph is automatically regenerated after pressing one of these buttons.

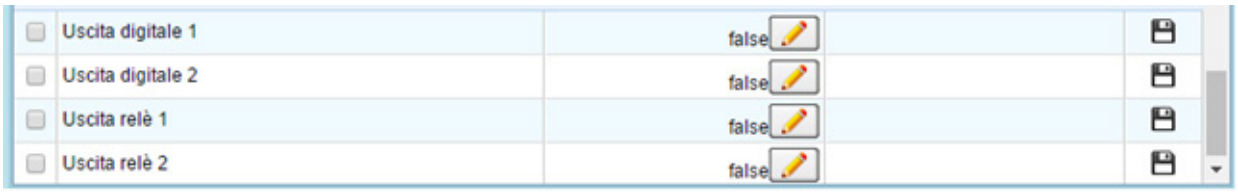
To change the selection of the measures to be plotted, return to the system and device measures display screen by pressing the button:



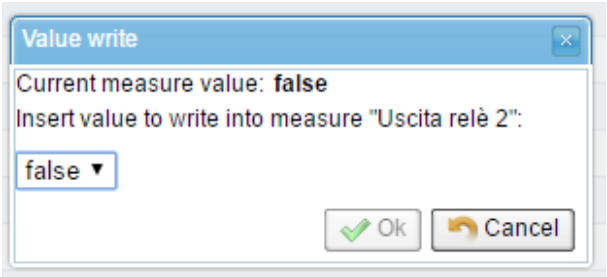
Select or clear the measure by using the check box again.
The measures currently selected are listed in the tree menu structure on the left. These can also be removed by pressing the icon:

6.2.3 Measure write

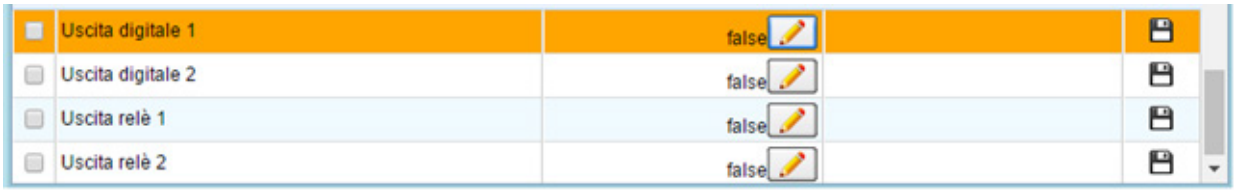
Some measures can be written, therefore it is possible to insert value to write into measure. To do it you should be authorized by logging in with user/password: go to section *"Configuration"*, login, and return to section *"Devices"*. Select a device to open the measures list. The writeable ones can be identified by the presence of a button on the row, see figure below.



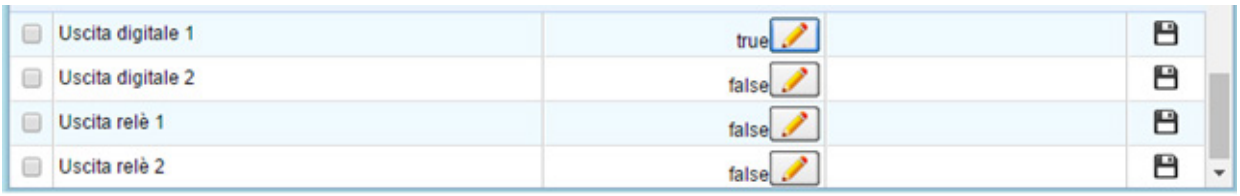
Pressing the button a popup window will open that allows to insert new value.



Writing is carried out in few seconds and while waiting the selected measure's line turns orange, keeping the old value.

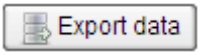


Once writing is complete, the line turns white again and the value is updated.



6.2.4 Exporting data to Excel

Once a graph has been generated, the data can be exported in Excel format by pressing the button:



You will be prompted to save the dataExport.xlsx file containing ALL of the values recorded by IOT SCADA SERVER for the measures that are currently selected within the selected time interval in Excel 2007 format. N.B. Excel 2007 limits the number of rows in an Excel spreadsheet to 65536. If the number of data exported is greater, the “excess” data will be automatically deleted.

6.3 Alarms

The current active alarms on all devices to which the IOT SCADA SERVER is connected can be viewed in the *“Alarms”* section. The list is sorted by date and time, but the order in any column can be changed by clicking on the corresponding heading.

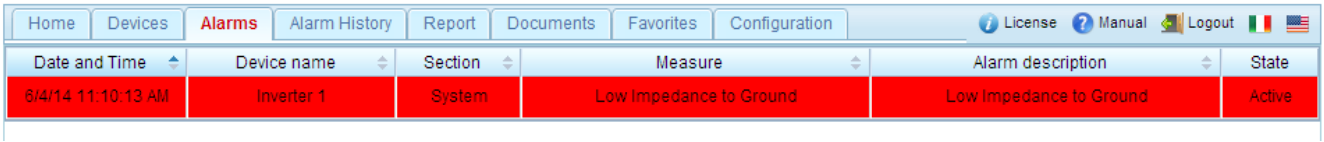


Figure 68 - Active alarms

If there is no alarm the message *“No active alarm”* will be displayed. If alarms are present, the text in the *“Alarms”* tab will be red, even when the tab is not open.

Custom alarms are also reported in this section.

6.4 Alarms history

To display a history of the alarms that were triggered in the devices connected to IOT SCADA SERVER enter the *"Alarm history"* section. If alarms are present, the screen that appears is like that in Figure 63:

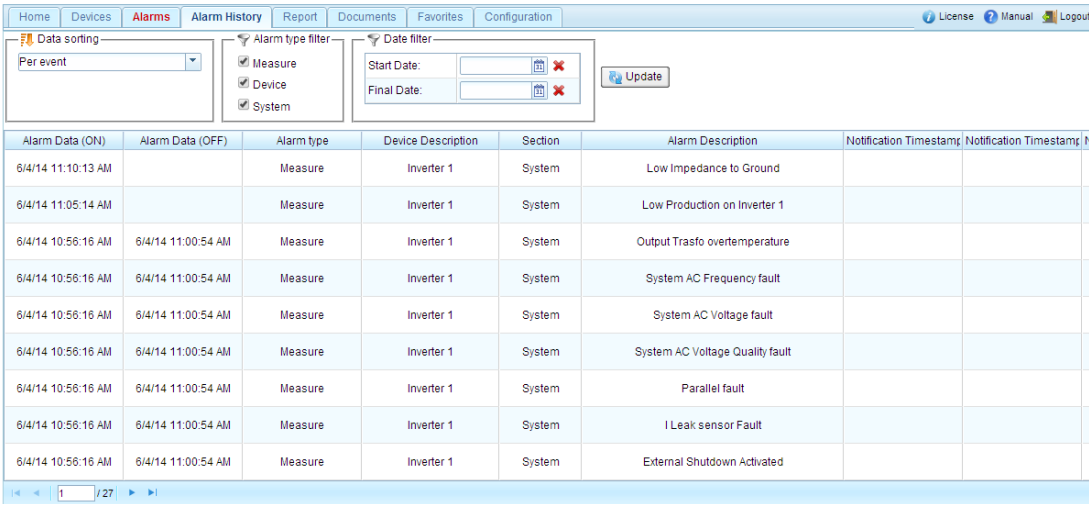


Figure 69 - Alarm history per event

The list is sorted by date and time in descending order and the alarms displayed can be filtered based on a date interval to be specified in the *"Date Filter"* fields, and on the type of alarm, to be specified in the *"Alarm type filter"* box. Thereafter the alarm corresponding to the filters set will be displayed by clicking on the *"Update"* button.

There are 3 types of alarms in IOT SCADA:

- Measure alarms
  - o These are default alarms set on catalogue device measures, or defined by the user as shown in Section 5.3.3.
- Device alarms
  - o These are generated when a device does not respond to requests and becomes offline
- System alarms
  - o These are generated by multiple abnormal situations, such as a backup failure, an improper shutdown of the IOT SCADA SERVER, an error while sending a notification, etc.

In Figure 63, *"Per event"* selected in the *"Data sorting"* box, the alarm ON and the corresponding OFF alarm, if any, are grouped together in the same row, thereby facilitating the relationship between alarm events.
If it is not possible to display all the alarms on the same page, the list can be scrolled by means of the page navigation controls at the bottom.
If the alarm notification has been configured (see Section 5.4.1), there is a  button at the end of each row. If this is pressed, a popup window as in Figure 64 will be displayed, with details on the forwarding of the notification.

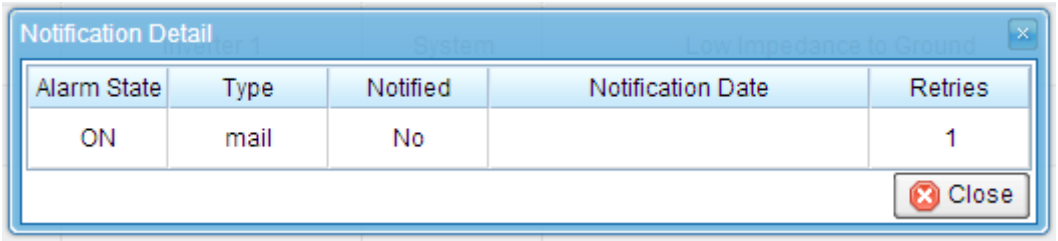


Figure 70 - Notification details

The alarm history can also be viewed by sorting the data in a chronological manner (i.e. selecting the option *"Chronology"*) in which the alarms are presented in the reverse order in which they occurred, that is with the most recent at the top of the list together with the information about the state of the alarm ON (device in alarm) separate from that of the alarm OFF status (device alarm over), as in Figure 65:

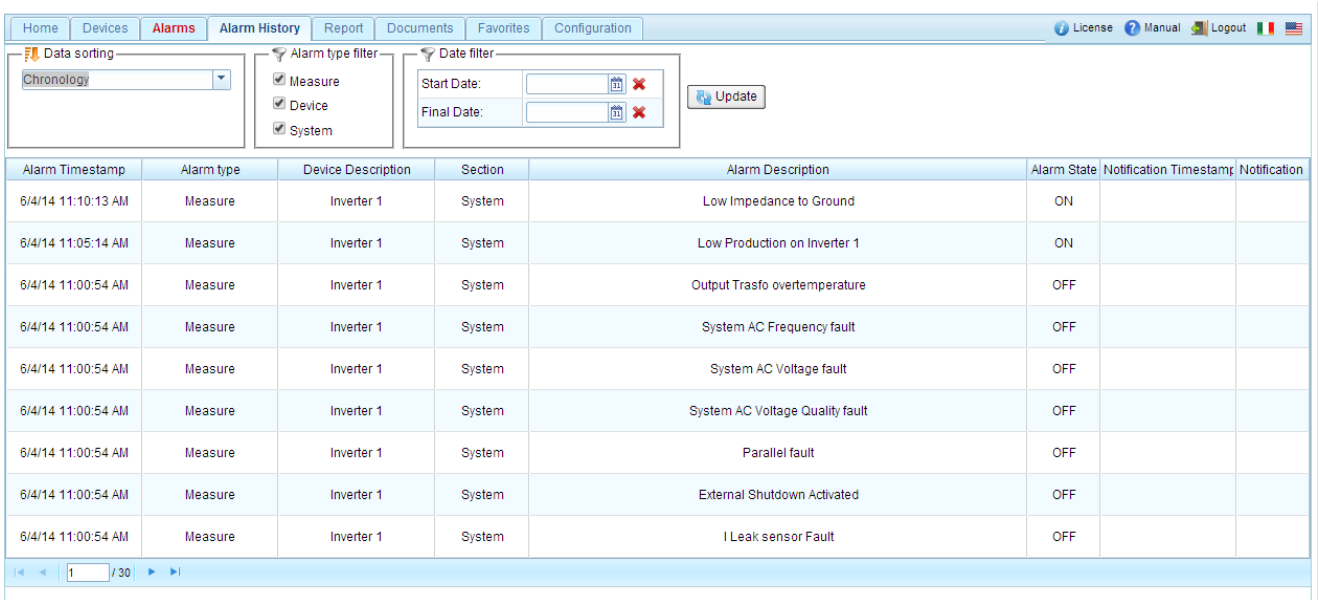


Figure 71 - Chronological alarms history

6.5 Report

In the *"Report"* section of the main menu it is possible to choose the type of report to generate:

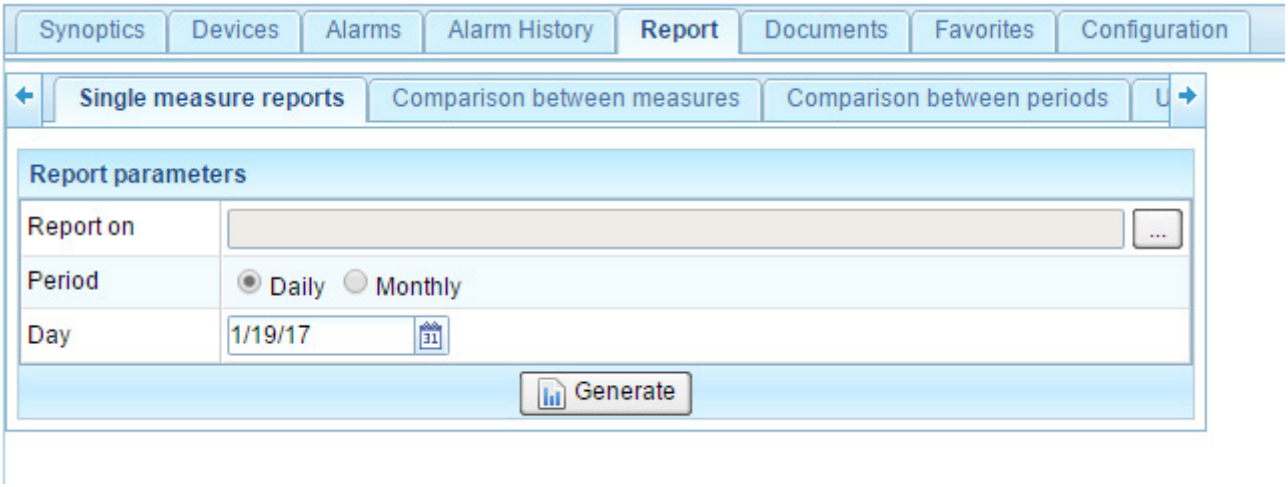


Figure 72 - Types of report

Energy reports can be generated (growing monotonic measures), enabling the daily or monthly progress of the energy measures to be analysed in different ways:

- the single measure energy report represents the simplest type of energy reports focusing the analysis on a single energy measure. This is the most compact of the various reports as it is composed of a single page with a bar graph and data table.
- the energy report "comparison between measures" highlights the differences between energy measures over the same period of time. This is useful in comparing energy production and consumption in a system, as well as for discovering any inefficiencies in devices regarded as similar (e.g. different production by inverter of the same model connected to the same number of strings). This contains a line graph and one or more data comparison tables between different measures.
- the energy report "comparison between periods" analyses the performance of one energy measure over several days or several months. It enables, for example, the comparison between the energy produced in July 2012 with that produced in the same month of 2013. It contains a line graph and one or more data comparison tables between different periods.

The measures and the periods over which the analysis is to be performed must be defined in each of these reports by filling in a special form of input parameters.

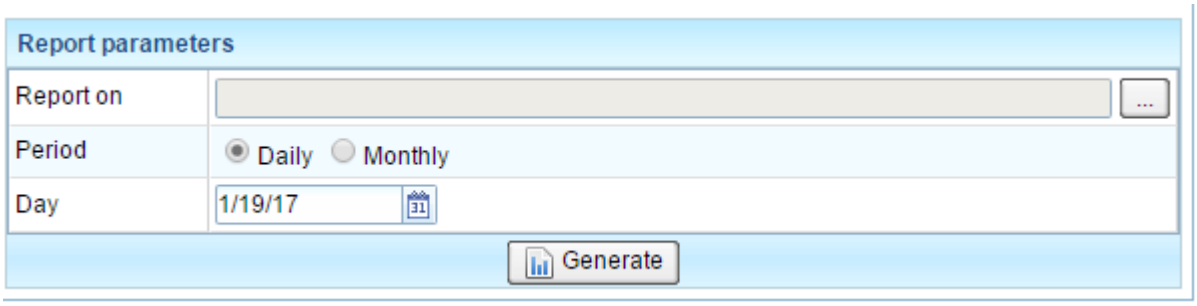


Figure 73 - Input parameters form for the single measure report

If the report is a comparison of several measures, then more than one measure can be chosen. Similarly, for the comparison report between several periods more than one period can be chosen.

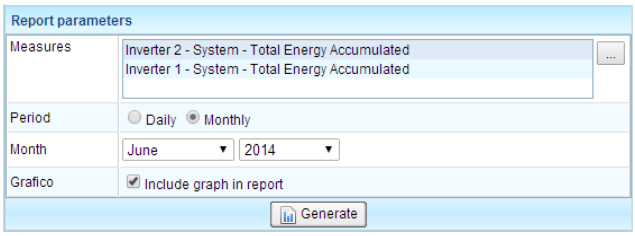


Figure 74 – Choice of multiple measures for the comparison report between different measures

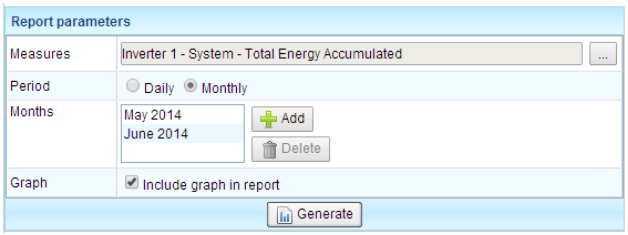


Figure 75 – Choice of multiple periods for the comparison report between different measures

After filling in the parameter input form, a preview of the report can be generated by pressing the *"Generate"* button. A few moments later a popup window will open displaying the generated document consisting of a graph and one or more tables; at the bottom of the popup window there are buttons that are used to save or forward the report displayed via email. The email forwarding occurs after the recipients of the mail have been entered in the appropriate popup window that appears after the *"Send"* button is pressed. To use this feature the notification parameters must be configured, as described in Section 5.4.1.

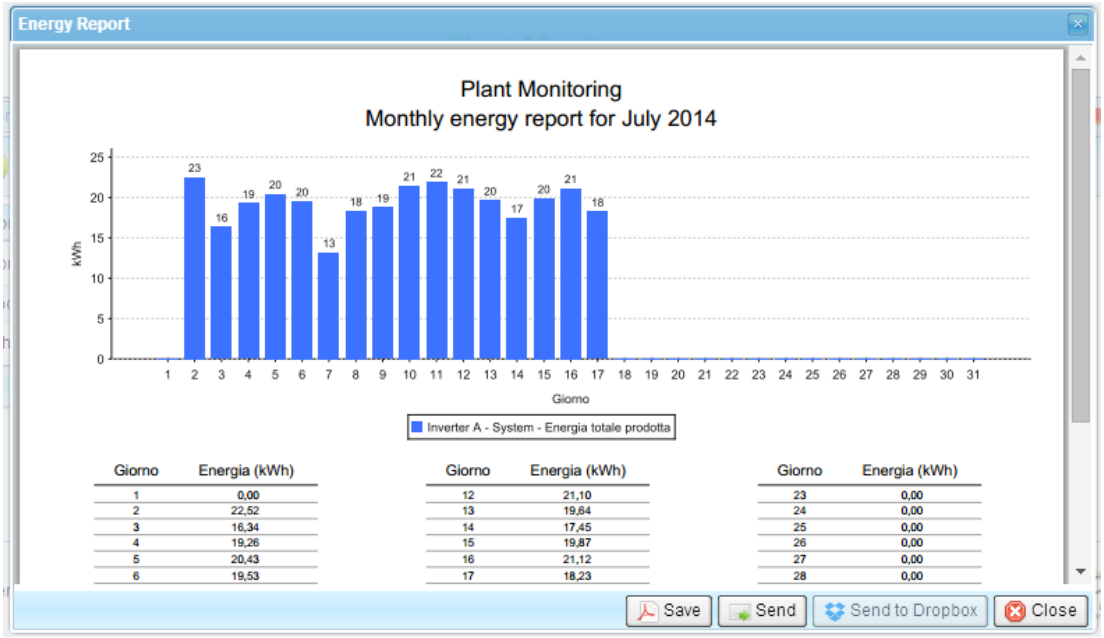


Figure 76 - Single measure energy report

6.6 Documents

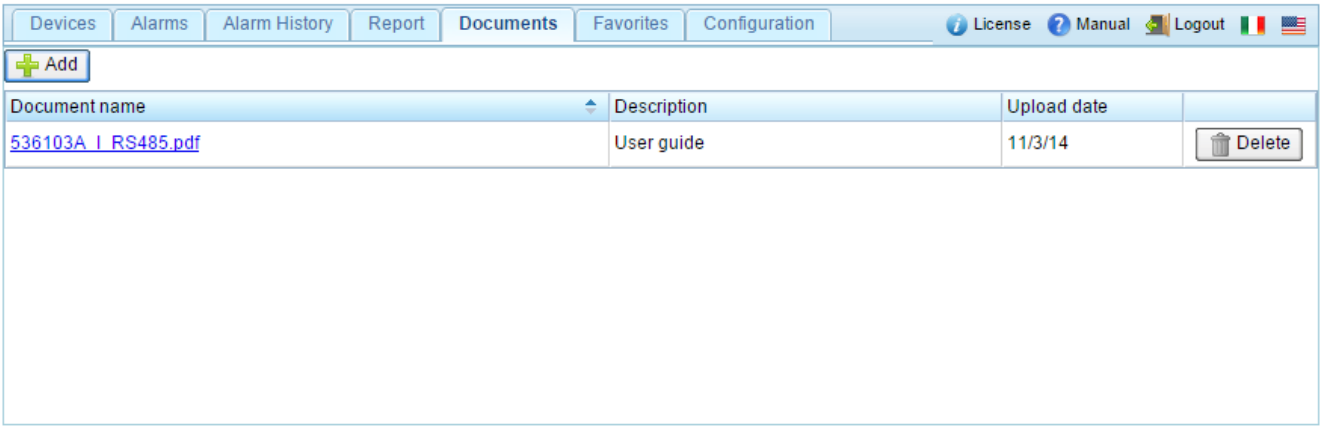


Figure 77 - System documents

For convenience, documents that are deemed useful to the system being monitored, such as wiring diagrams or other, can be loaded in IOT SCADA SERVER.
A popup window, as shown in Figure 72, opens when the *"Add"* button is pressed. Thereafter the *"Upload"* button must be pressed and the document to be loaded chosen. A description, such as *"System Wiring"* must be entered and subsequently the *"Ok"* button pressed.
You must be logged in to delete a document, in which case the *"Delete"* button next to each document will appear.

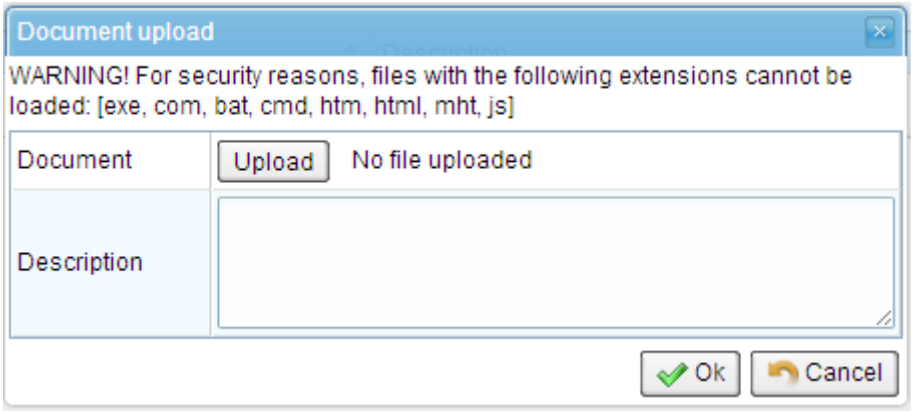


Figure 78 - Document upload

6.7 Favourites

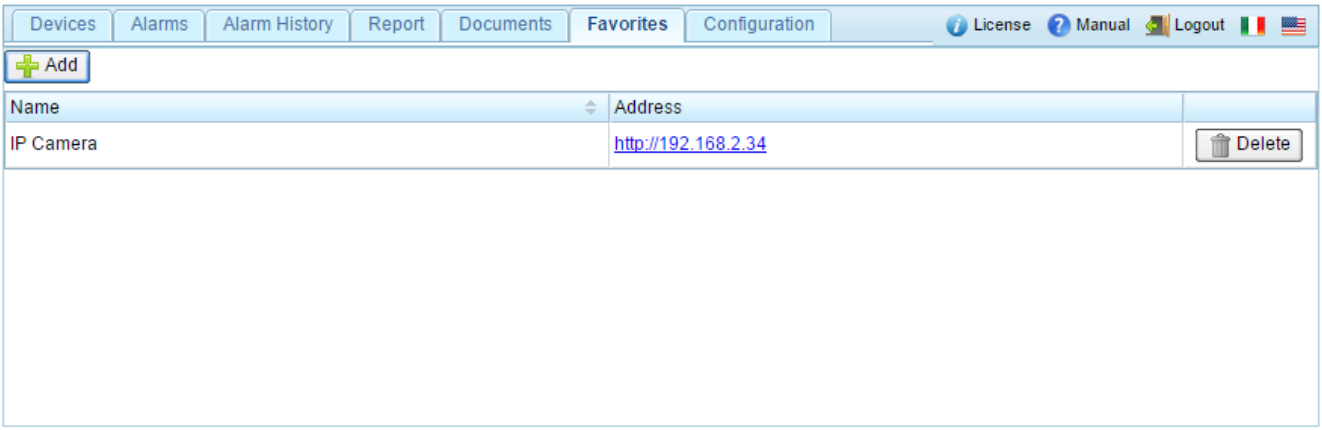


Figure 79 - Favourite addresses

"Favourites", that is addresses of IP cameras present in the system or of other sites that are of interest, can be entered in the IOT SCADA SERVER configuration.
By pressing the *"Add"* button a popup window opens as shown in Figure 74. A name must be entered to help understanding, such as *"System cameras"*, the address itself, and then the *"Ok"* button must be pressed.
You must be logged in to delete a favourite, in which case the *"Delete"* button next to each document will appear.

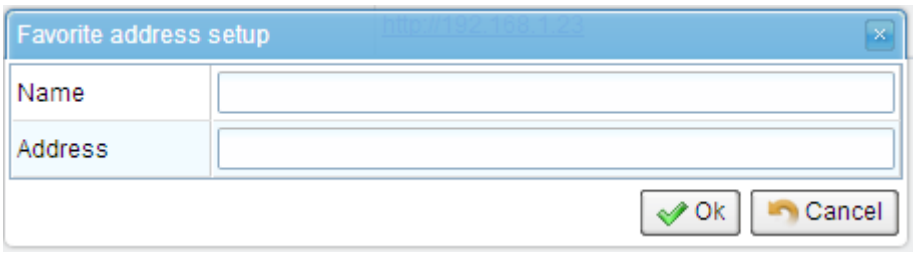


Figure 80 - Favourite addresses insertion

This will open in a new browser window when clicking on the address.

7 Troubleshooting – FAQ

7.1 IOT SCADA SERVER does not switch on

For the Base and UPS models (code IxS_1y1), check there is 12 V direct current on jack with terminal positive on DC+ and negative on DC-. If voltage is over or below 12 V, change power supply or, if possible, adjust output voltage of existing one.
For the Multi and Multi+UPS models (code IxS_1y2, IxS_1y3), check there is between 12 V and 24 V direct current or between 15 V and 26 V alternating current on terminal DC+ and DC-. If the measured voltage is not comprised in the specified intervals, change power supply or, if possible, adjust output voltage of existing one.

7.2 Unable to complete Internet communication test

Verify that the Ethernet or Wi-Fi connections have been made correctly and check activity state of LED LAN or Wi-Fi on the IOT SCADA SERVER (Section 2.3.1) and the switch/router. If the IP address has been manually configured, verify the parameter configuration with your network administrator or with the router.

7.3 Communication problems with serial devices

In the event of communication problems with serial devices, refer to the troubleshooting guide in the section “Configuration” -> “Installation” -> “Devices configuration” that can be downloaded by pressing the button:

7.4 Unable to access IOT SCADA SERVER from the local network

Check that the IP address and subnet mask of the device from which you want to reach IOT SCADA SERVER are compatible with the IP address and the subnet mask of the IOT SCADA SERVER itself (see Sections 4.4 e 5.1)

7.5 Unable to access IOT SCADA SERVER from the Internet

Check that “NAT” has been configured on the local router on port 80 of the IP address of the IOT SCADA SERVER.
In the event that you are trying to access the IOT SCADA SERVER through a name, and not through an IP address (e.g. mioimpianto.no-ip.org), check the DDNS configuration of the router.

8 Contacts

Alleantia s.r.l.

http://www.alleantia.com

Registered offices: Via Tosco Romagnola, 136 56025 Pontedera (PI)
Operating headquarters: via Umberto Forti, 24/14 56121 Pisa
VAT code/Tax code: IT 02011550502

info@alleantia.com


Alleantia
ALL <THINGS> JOINED

Alleantia s.r.l

www.alleantia.com

Tel: (+39) 050 9911933
Fax: (+39) 050 9655139
@: info@alleantia.com

M-ISS-0417-EN