STE 2

User Manual

Safety warning

The device meets the requirements of standards valid in the Czech Republic, has undergone live testing and is delivered in operational condition. To maintain the device in this condition, it is necessary to observe the safety and device maintenance requirements set forth below.

If the device is not used in the manner recommended by the manufacturer, the security offered by the device may be breached!

The power socket or point of disconnecting the device from power supply must be freely accessible!

The device must not be used in particular if:

- it is visible damaged
- it does not work properly
- there are loose parts inside the device
- it was exposed to long-term humidity or got wet
- it underwent unqualified repair by unauthorised personnel
- the power adapter or its supply cable are visible damaged
- if the device is used in a manner other than the designated manner, the protection provided by the device may be breached
- the switch or fuse and other power surge protection resources must be part of the overall construction unit

The manufacturer is liable for the device only if it is powered by the supplied or approved power source.

Should you have any problems with installation and start-up, you can contact our technical support:

HW group s.r.o.
http://www.hw-group.com
email: support@HWg.cz

Rumunská 26/122
Prague, 120 00
Phone: +420 222 511 918

Before contacting technical support, prepare the precise model of your device (on the manufacturing label and the firmware version (see below), if you know it.

Contents

Safety warning 2
Contents 3
STE2 – Basic features 4
Basic features 5
Application 5
Connectors and wiring 6
Recommended connection 7
First start-up 8
WWW interface 10
Home tab 10
General Setup tab 11
Security tab 12
WiFi tab 13
Sensors tab 16
Digital Inputs tab 17
E-mail tab 18
SMS tab 19
Alarms 20
SNMP tab 21
Time tab 23
Portal tab 24
System tab 26
Technical parameters 28
Physical dimensions 29
WiFi Radio 30
WiFi signal strength 30
Impact of device position vis-à-vis the transmitter 31
Supported interfaces 32
Dry contact inputs 32
RJ11 – 1-Wire bus 32
Active / Passive 1-Wire port 33
Sensor Hysteresis 33
Connecting STE2 to the SensDesk portal 34
Using the mobile phone app 39
Firmware upgrade in STE2 units 40

STE2 – Basic features

STE2 is a thermometer with an Ethernet and WiFi interface, HTTPS support and option of connection to the SensDesk portal.

STE2 is a device with HTTPS and SNMP support designated for measuring temperature and humidity from external sensors, with the option of connection to the internet via classic cable or WiFi. If the permitted range of values is exceeded, it allows the sending of an alarm via e-mail, via the SensDesk portal or via SMS. Support of monitoring system is a matter of course and the device is supplied with free HWg-PDMS software to create graphs and export data to MS Excel. The packaging includes a power adapter and temperature sensor.

Basic features

- Contains classic Ethernet and WiFi – 802.11 b/g/n (2.4 GHz)
- Support of current Ethernet and WiFi operation (for easy configuration)
- 5V or PoE power supply
- Simple installation, supports DHCP
- Built-in WEB server with HTTPS support – no need for any software other than a standard internet browser
- Can be connected to NMS (SNMP MIB)
- Support for simultaneous traffic to both HTTP and HTTPS with the option of disabling one or the other protocol for security reasons
- Sends an e-mail if the temperature is too high / low
- Support of TLS authorisation (GMAIL)
- Password protected
- Supplied with Windows HWg-PDMS software for drawing graphs and exporting data to MS Excel

Application

A/C outages
Changes in temperature alert you to outages of the A/C cooling unit.

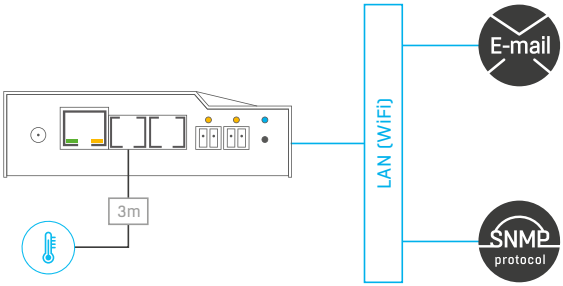
Heating monitoring
Remote monitoring of the heating system, alert via e-mail or SMS about the risk of freezing (e-mail-2-SMS).

Monitoring of provided services
Using the provided HWg-PDMS software, you can easily create reports with temperature graphs at one or several locations. You can have an overview of the quality of outsourced services.

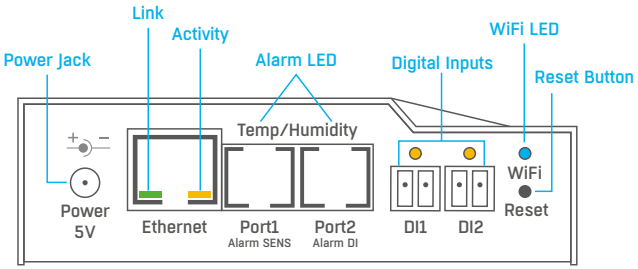
Fridge and freezer monitoring
Sends an e-mail to alert you of refrigerator outages. Logging of operation and storage conditions.

Heating optimisation
Cost savings for heating and A/C.

Food storage
Monitors optimal storage conditions. Protocols for HACCP can be created using the application software.



Connectors and wiring



Description of connectors

- *Ethernet* – Serves for internet connection via cable for operation in a classic computer network and for configuration of operation on WiFi. The connector supports power supply from the computer network via PoE.
- *Temp/Humidity* – Serves to connect up to 3 temperature or humidity sensors. The sensor length may be up to 60 metres in each port.
- *Power* – Connector for 5V power supply in the case of power supply from an external adapter.
- *Digital Inputs* – Serves to connect sensors with digital output.

LED diodes on the front panel

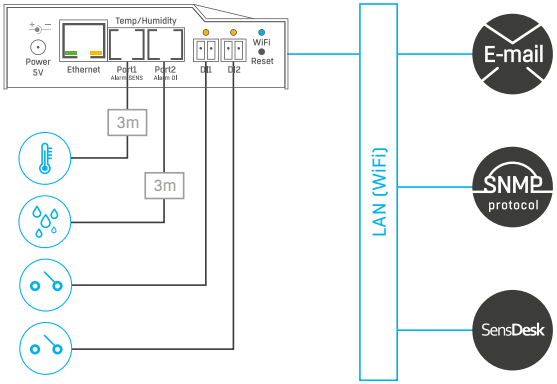
- *Link* – A green LED signalises connectivity to the computer network.
- *Activity* – A yellow flashing LED signalises ongoing communication on the cable connection to the computer network.
- *WiFi* – A blue LED signalises establishment of a connection to the WiFi connection point. When establishing a connection, it signalises the state by flashing.
- *Alarm LED* – Two LEDs hidden in the Port1 and Port2 connectors. Shining LEDs indicate Alarm state.
  - *Alarm SENS* – Shining LEDs signalises Alarm state on one of the temperature or humidity sensors.
  - *Alarm DI* – Shining signalises Alarm state on one of the digital inputs.

Description of button function

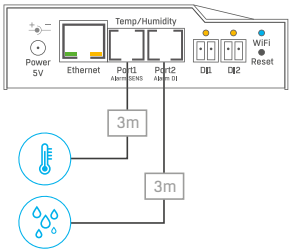
- *Reset* – serves to restore factory settings on the device.

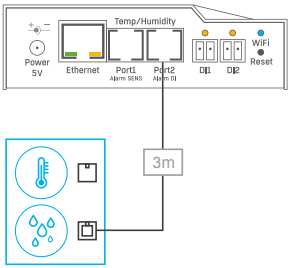
1. Switch the device off.
2. Press and hold the button.
3. Switch the device on and press the button for another 5 seconds.
4. All the LEDs will gradually light up.
5. Restart the device. Factory settings will be restored.

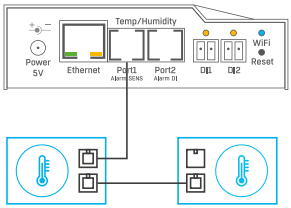
Recommended connection



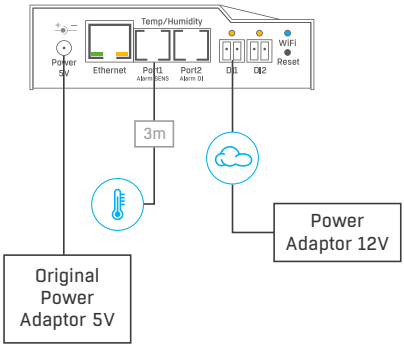
Sensor connection options:







Smoke sensor connection:



First start-up

First step

1 Cable connection

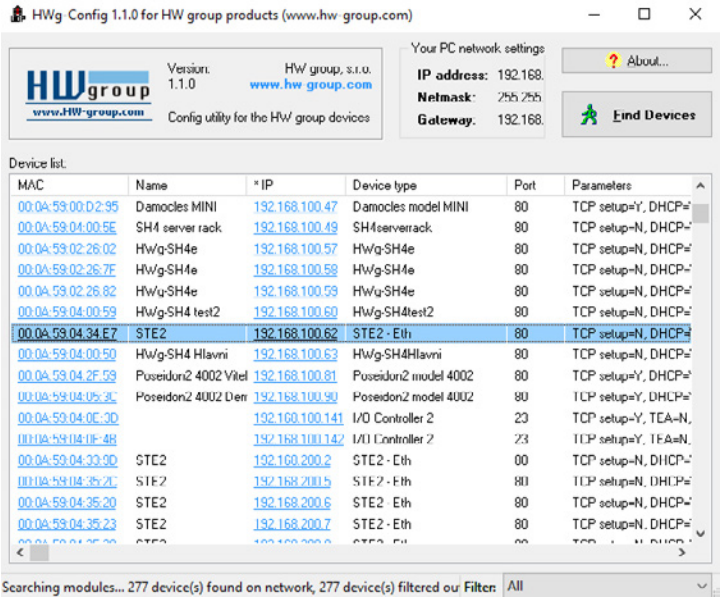
- Connect the device to the **Ethernet** (direct cable to the **switch**, crossed to PC).
- Connect the power adapter to the grid and connect it to the device power supply connector.
- The green LED in the **Power & Mode** RJ45 connector will light up.
- If connection to the **Ethernet**, is functional, the **LINK** (yellow) LED should light up shortly afterwards and switch off during data transfer to the Ethernet (Activity signalisation).
- A quickly flashing yellow **LINK** LED signalises communication with the DHCP server.

2 Setting of the IP address - HWg-Config

The **HWg-Config** program is located in the main director on the enclosed CD (version for Windows and Linux).

The program can be downloaded at www.HW-group.com Software -> HWg-Config.

- Click on the icon to launch the **HWg-Config** program – the program automatically searches for connected devices.
- Launch the search by clicking on the **Find Devices** icon.
- The program searches for devices in your local network. Click on the MAC address of the device to open the dialogue window for device settings.



First step

Set device network parameters:

- IP address / HTTP port (80 by standard)
- Your network ask
- IP address of your network gateway
- Device name (optional parameter)

Save the settings by clicking on **Apply Changes.**

Restore default settings:

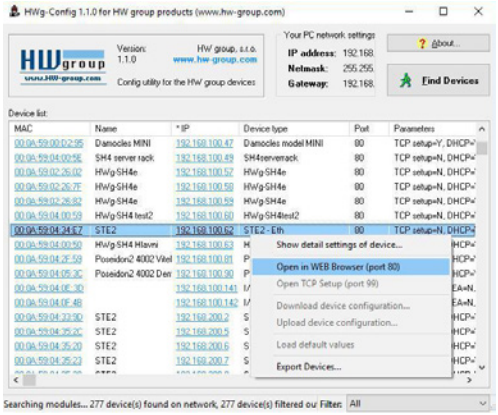
- Right-click on the device MAC address. The default values from the HWg-Config can be restored by software mode during the first 60 settings after start-up.

- Press the RESET button, hold it down and connect the power source. Hold the button down for another 5 seconds until all the LEDs light up.

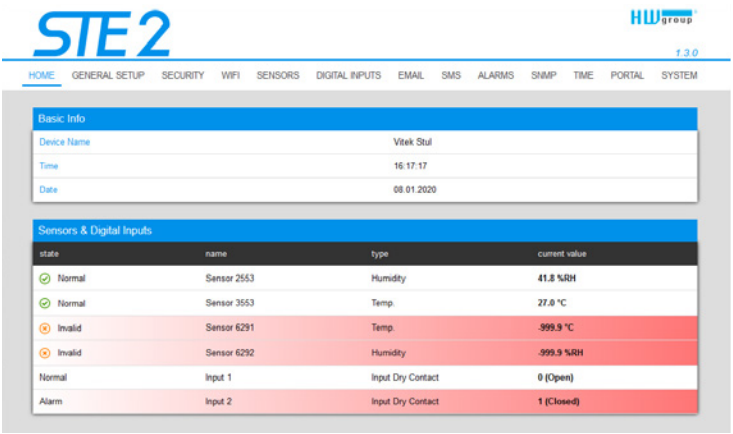
3 Device website

Options of opening the website:

- Enter the device IP address in the browser window.
- Click on the IP address in the HWg-Config program.
- Click on the underlined IP address in the HWg-Config application.



Home tab



— *Base Information section*

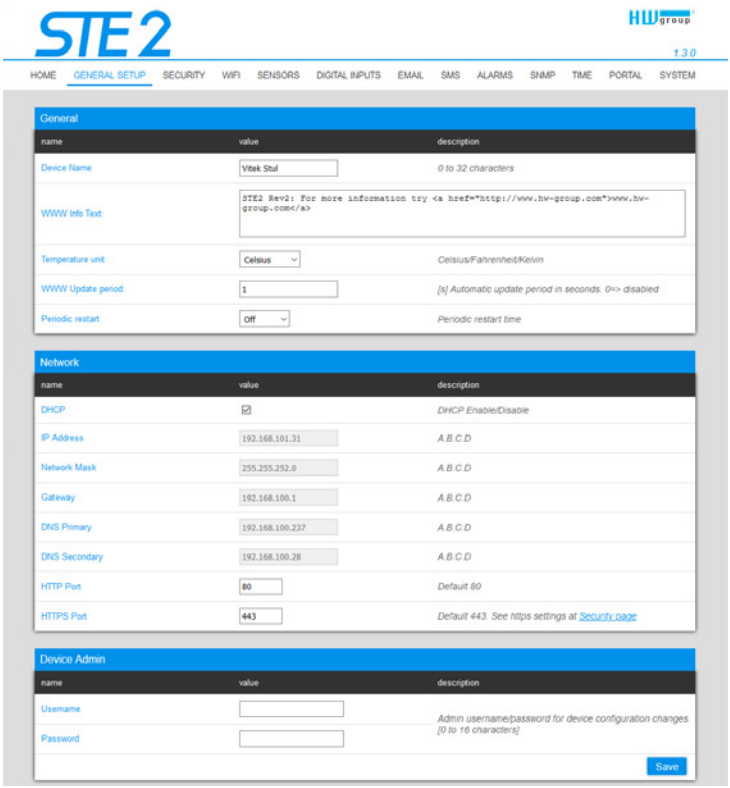
- *Device Name* – The device name serves to distinguish specific devices in larger installations. Can be set in the General Setup tab.
- *Time* – Current device time. The time can be set automatically from the internet or manually in the Time tab. In the case of automatic setting, the correct value is the indicator of device access to the internet.
- *Date* – Current device date. The date can be set automatically from the internet or manually in the Time tab. In the case of automatic setting, the correct value is the indicator of device access to the internet.

— *Sensors & Digital Inputs section*

Lists the current values of sensors and digital DI inputs (Dry contacts)

- *State* – Input or sensor state.
  - *Normal* – Idle state, all normal.
  - *Alarm High* – Value exceeded the permitted upper limit.
  - *Alarm Low* – Value dropped below lower bottom limit.
  - *Alarm* – Digital input in the Alarm state (according to the Alarm Alert setting at the Digital Inputs tab).
- *Name* – Sensor name for better identification in larger systems. The name can be set in the Sensors or Digital Input tab.
- *Type* – Sensor type; indicates what type of sensor is in question (temperature / humidity / digital input).
- *Current Value* – Current value including unit of measure.

General Setup tab



— *General section*

- *Device Name* – Device name (STE2), allow you to distinguish individual the device in the network.
- *WWW Info Text* – Text at the foot of the website.
- *Temperature Unit* – Unit for displaying temperature. You can choose between Celsius / Fahrenheit / Kelvin. The Safe Range values will automatically be converted based on this option.
- *Periodic Restart* – Function to improve device stability in exposed networks allowing regular automatic restart of the device.

— *Network section*

Only the cable connection parameters (RJ-45) are set here. Wireless connection parameters are set in the WiFi tab.

- *DHCP* – Permits the function of IP address setting by the DHCP server, if available. Enabling or disabling DHCP depends on the needs of the user and network administrator.
- *IP Address* – IP address of the device, allocated by the network administrator.
- *Network Mask* – Network mask, allocated by the network administrator.
- *Gateway* – IP address of the default gateway, allocated by the network administrator.
- *DNS Primary / DNS Secondary* – IP address of the DNS server, allocated by the network administrator.

- *HTTP Port* – Port number on which the built-in WWW server tunes in. A change of the port number is suitable e.g. for multiple devices accessible from the external network via a router. Consult the network administrator about potential changes. The default port is 80. You can turn off HTTP support by setting the port value to 0.

- *HTTPS Port* – The port number on which the embedded Web server listens for the secure HTTPS connection. Changing the port number is appropriate, for example, for multiple devices accesses from the external network via the router. Contact your network administrator for any change. The default port is 443. You can turn off HTTPS support by setting the port value to 0.

— *Device Admin section*

- *Username / Password* – Username and password to secure access to the device.

Security tab

— *HTTPS Server Certificate files*

Used to manage certificates needed for the HTTPS server. Allows you to upload or delete a public key, a private key, or a certificate of the certificate authority (CA) that has issued the public key certificate.

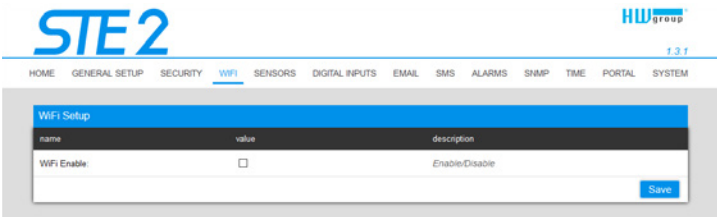
— *Generate the SSL key and certificate*

Generate a private SSL key and self-signed certificate for closed networks or testing purposes. The generated certificate is self-signed and will be displayed as untrusted. Please add the certificate

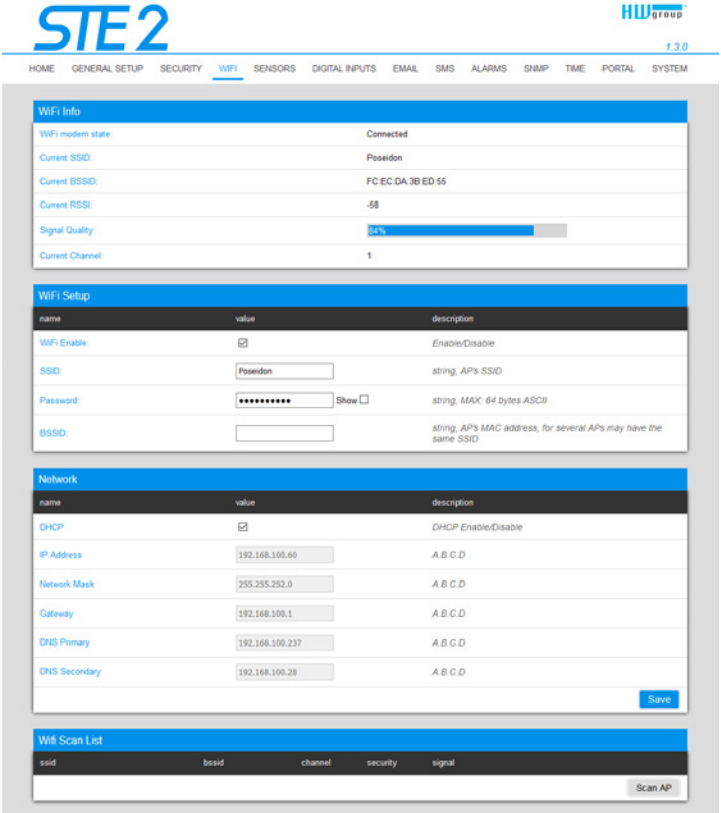
to the list of exceptions or use a certificate signed by a trusted certification authority. Please note that the generated data will replace the SSLCertificateFile and the SSLCertificateKeyFile. Generating the key can take up to 10 minutes. Do not restart the device and do not search for sensors. Otherwise the key generation will be interrupted.

WiFi tab

When WiFi is off, only the enable option is shown:



All the options are available after enabling:



— *WiFi modem state*

- *Disable* – Wifi is disabled.
- *Wait for power on* – Waits for WiFi module when power on.
- *Init* – Initializing of WiFi module.
- *Connecting* – Connecting.
- *SSID check* – SSID check.
- *Connected* – Connected to selected WiFi network.
- *Network WiFi scan* – Scan of available WiFi networks.
- *Wait for scan* – Waits for Network wifi scan.

— *Information section*

- *Current SSID* – Current name of the network to which the device is connected. If the parameter is missing, the device is not connected to any WiFi network.
- *Current BSSID* – Current identifier of the WiFi network connection point. If the parameter is missing, the device is not connected to any WiFi network.
- *Current RSSI* – Relative strength of signal input. The higher the RSSI, the stronger the signal.
- *Signal Quality* – Strength of WiFi signal in % with graphic indicator.
- *Current Channel* – WiFi channel on which the device communicates. If the parameter is missing, the device is not connected to any WiFi network.

— *WiFi Setup section*

- *WiFi Enable* – Enable or disable WiFi. By standard, the wireless interface is disabled. Device restart follows enabling.
- *SSID* – Name of the WiFi network to which should be the device connected. If you do not know your network name, use the Scan AP function at the bottom of the page.
- *Password* – Secured network password. If you do not know it, contact your network administrator.
- *BSSID* – Identifier of the WiFi network connection point (MAC address of the connection point). Optional data.

— *Network section*

WiFi network parameters. Only the wireless interface is set here. Cable Ethernet (RJ-45) is set in the General Setup tab.

- *DHCP* – Permits the function of IP address setting by the DHCP server, if available. Enabling or disabling DHCP depends on the needs of the user and network administrator.
- *IP Address* – IP address of the device, allocated by the network administrator.
- *Network Mask* – Network mask, allocated by the network administrator.
- *Gateway* – IP address of default gateway, allocated by the network administrator.
- *DNS Primary / DNS Secondary* – IP address of the DNS server, allocated by the network administrator.

WiFi Scan List

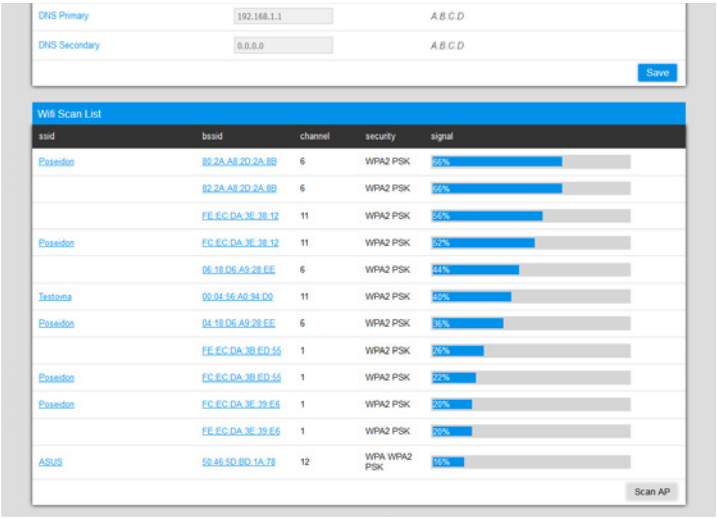
- *SSID* – Name of found WiFi network.
- *BSSID* – Connection point identifier (MAC address).
- *Channel* – WiFi channel on which the connection point operates.
- *Security* – Type of secured WiFi communication.
- *Signal* – Signal level in DB. The higher the value, the better. WARNING, -60 is more than -90! The highlighted row indicates the currently connected AP.

Connecting to found WiFi

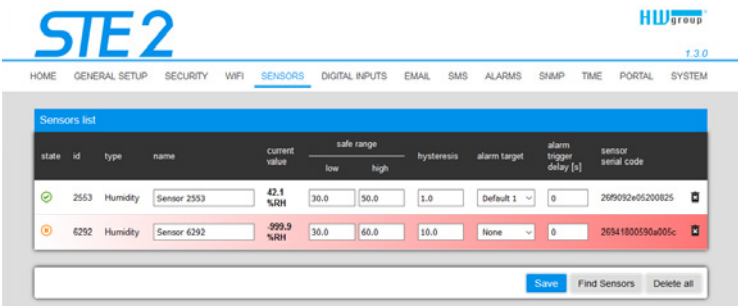
- Click on the SSID of the found network to prefill WiFi setting and just enter the Password. The BSSID remains empty. Standard setting. Reconnects automatically if AP is changed.

- Clicking on BSSID will prefill not only the network name (SSID), but also the MAC address of the specific AP (BSSID). The device then connects to this AP and will not try to reconnect in the case of aggregated networks.

Scan AP



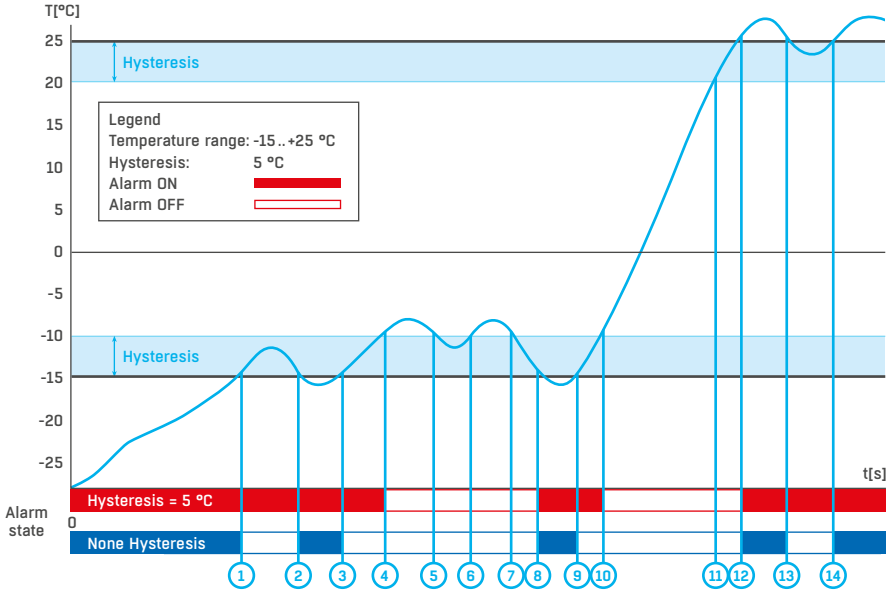
Sensors tab



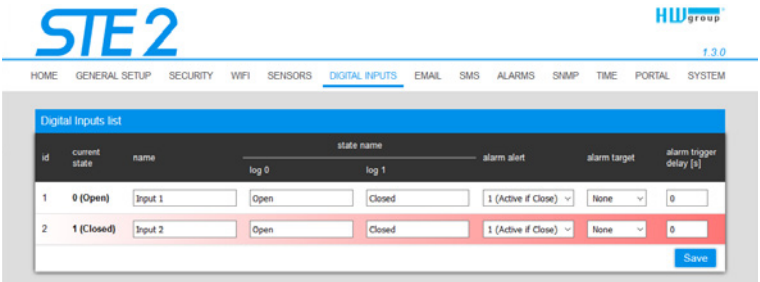
— *Sensor List section* *

- *State* – Input or sensor state.
  - *Normal* – Idle state, all normal.
  - *Alarm High* – Value has exceeded permitted upper limit.
  - *Alarm Low* – Value has dropped below permitted lower limit.
- *ID* – Sensor ID identical to ID in Poseidon2 and STE2 units.
- *Type* – Sensor type; determine what type of sensor is in question (temperature / humidity / DI input).
- *Name* – Sensor name for better identification in larger systems. The name can be set in the Sensors or Digital Input tab.
- *Current Value* – Current value including unit of measure.
- *Safe Range* – Range of permitted values. If the current value exceeds the Safe Range, an Alarm is activated.
- *Hysteresis* – Defines the insensitivity zone if the limit values are exceeded; prevents the activation of multiple alarms if the temperature oscillates around the limit value.
- *Alarm Target* – Specifies the targets for alarm alerts (SMS + E-mail). Target recipients are defined at the Alarms tab. The drop-down menu allows selecting an existing set of targets or creating a new one.
- *Alarm Trigger Delay [s]* – Delays the alarm start alert by a specified time.
- *Code* – Full ID of the 1-Wire sensor.
- *Delete* – Button to delete the specific sensor.

** Sensors in Alarm state are highlighted.*



Digital Inputs tab

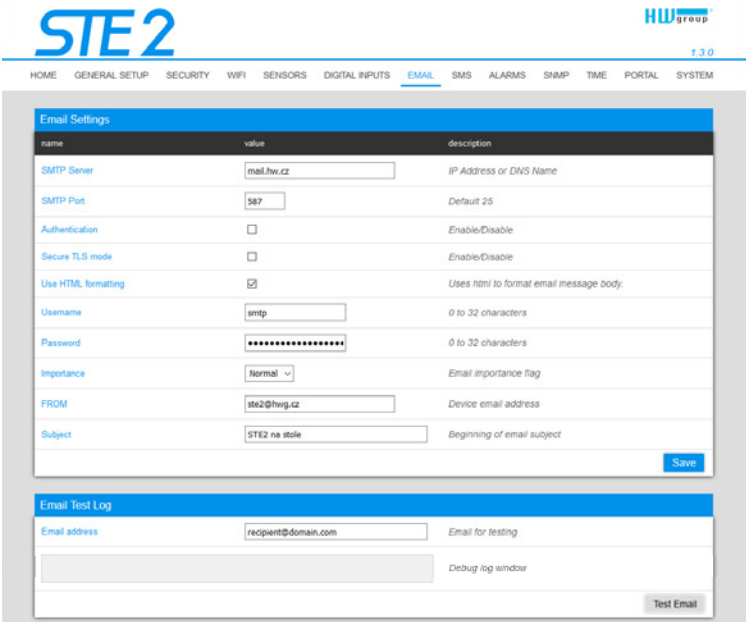


— *Sensor List section**

- *ID* – Indication of the input variable within the device.
- *Current State* – List of current input state ("0 (Off)" / "1 (On)").
- *Name* – Input name in 12 characters (e.g. "2F left door", "smoke section 1").
- *Alarm Alert* – Definition of Alarm state for each input.
- *Alarm Target* – Specifies the targets for alarm alerts (SMS + E-mail). Target recipients are defined at the Alarms tab. The drop-down menu allows selecting an existing set of targets or creating a new one.
  - *Active if Close* – Alarm active if the input is in state 1 (On).
  - *Active if Open* – Alarm active in input is in state 0 (Off).
  - *Disabled* – Input does not have a defined Alarm state.
- *Alarm Trigger Delay [s]* – Delays the alarm start alert by a specified time.

* *DI inputs in Alarm state are highlighted.*

E-mail tab



— *E-mail Settings*

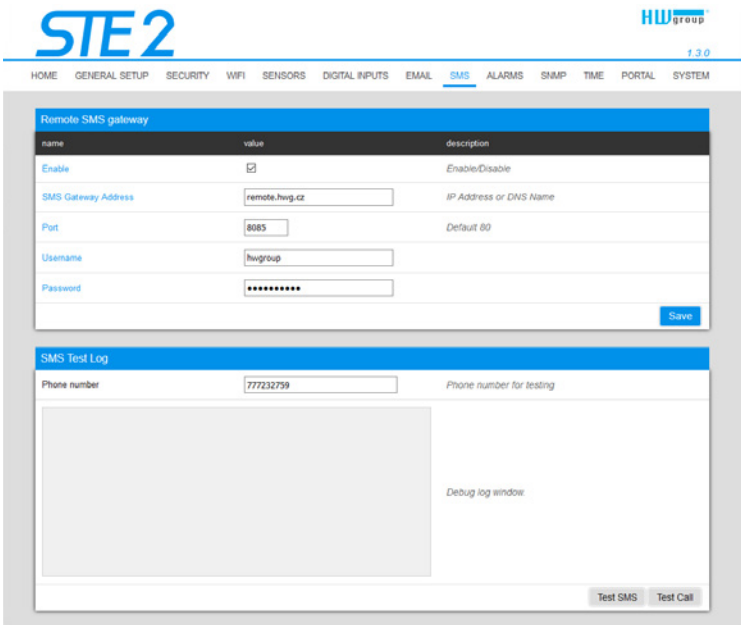
- ***SMTP Server*** – IP address or domain address of the SMTP server.
- ***SMTP Port*** – Port number on which the e-mail server tunes in – 25 by standard.
- ***Authentication*** – Enable authentication; check if the SMTP server requires authentication.
- ***Secure TLS mode*** – Check if the SMTP server requires secure communication via SSL/TLS.
- ***Username*** – Username for SMTP server authentication. If the Authentication field is not checked, the content of this field is irrelevant.
- ***Password*** – Password for SMTP server authentication. If the Authentication field is not checked, the content of this field is irrelevant.
- ***Importance*** – Sets priority of the e-mail message. Important for filtering and further processing of alarm messages.
- ***FROM*** – Sender's e-mail address, i.e. of the device. The address may be required by the SMTP servers and can be used to identify the device or to filter and further process alarm messages.
- ***Subject of e-mail*** – The field content can be used to identify the device, or for filtering and further processing of alarm messages.

— *Email Test Log section*

In this section, the SMTP server settings can be tested. Click Test Email to send a test e-mail to the specified Email address. The Debug log window shows the communication with the SMTP server.

SMS tab

With the Wifi turned off, only the power-on option is shown:



— *Remote SMS gateway*

- *Enable* – Turns on the SMS sending function. For sending, the SMS alarm action must be set at the sensor or input.
- *SMS Gateway Address* – IP address where "HWg-SMS-GW3" is located through which the device will send SMS. It can be set including service - typically /service.xml
- *Port* – The TCP port on which the gateway listens.
- *Username* – User name for authorization in SMS GW.
- *Password* – Password for authorization in SMS GW.
- *SMS + Ring When Alarm* – Enables sending a SMS and then dialing the number.

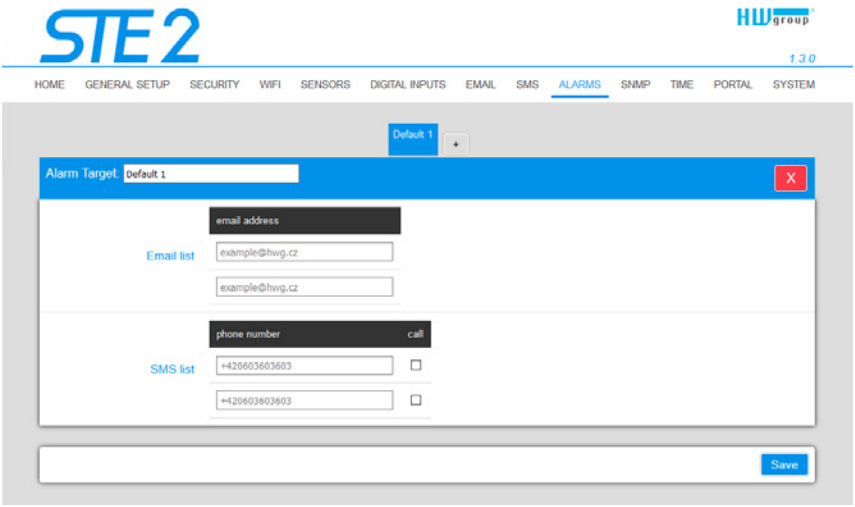
— *SMS Test Log*

In this section, the SMS gateway settings can be tested.

- *Test SMS* – Sends a test text message to the specified Phone number.
- *Test Call* – Dials the specified Phone number.
- *Debug log window* – Shows the communication with the SMS gateway.

Alarms tab

Alarm targets are defined at this tab. Up to 2 sets of targets can be created; each set can contain up to 2 addresses for e-mail alerts and 2 phone numbers for text message alerts and calls. These sets are then assigned to individual sensors and digital inputs. To create a set, click the + button at the Alarms tab, or select Add new... when editing a sensor or a digital input.



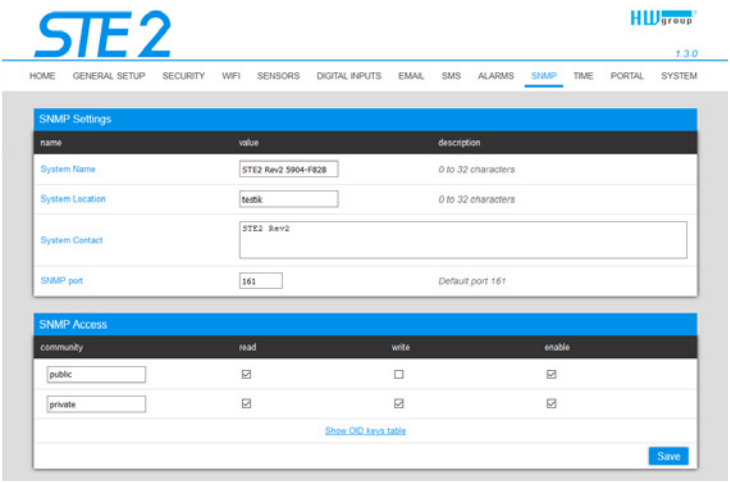
— *Alarm Target*

Set of targets. For clarity, the set can be given a custom name.

- ***Email list*** – E-mail addresses of alarm alert recipients. To send e-mails, the SMTP server must be properly configured at the Email tab.
  - ***Email address*** – Each field may contain only one e-mail address.
- ***SMS list*** – Phone numbers for text message alarm alerts. To send a message, the SMS gateway must be properly configured at the SMS tab.
  - ***Phone number*** – Each field may contain only one phone number.
  - ***Call*** – When checked, the phone number is dialed after the text message is sent (an incoming text alone can be easy to overlook).

SNMP tab

The SNMP tab sets the parameters for communication via SNMP protocol.



— *General SNMP Settings section*

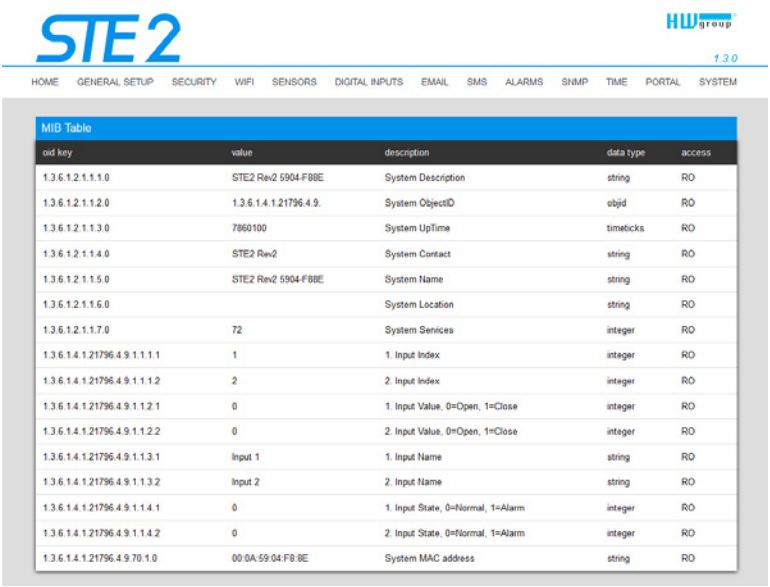
- *System Name* – Device name within SNMP.
- *System Location* – Device location within SNMP.
- *System Contact* – Contact of the device administrator within SNMP.
- *SNMP port* – Port number on which communication via SNMP is possible – 161 by standard.

— *SNMP Access section*

- *Community* – Name of SNMP community for access to the device via SNMP. 2 communities can be defined. For each Community you can define whether it has rights for:
  - *Read*
  - *Write*

— *Show OID keys table*

This function writes up the entire tree of variables with indication of the entire SNMP OID and explanations of the type of variable. For connecting the device to third-party monitoring systems, there is also an MIC file under the Download MIB file link.



MIB Table

oid key	value	description	data type	access
1.3.6.1.2.1.1.1.0	STE2 Rev2 5904-F88E	System Description	string	RO
1.3.6.1.2.1.1.2.0	1.3.6.1.4.1.21796.4.9.	System ObjectID	objid	RO
1.3.6.1.2.1.1.3.0	7860100	System UpTime	timeticks	RO
1.3.6.1.2.1.1.4.0	STE2 Rev2	System Contact	string	RO
1.3.6.1.2.1.1.5.0	STE2 Rev2 5904-F88E	System Name	string	RO
1.3.6.1.2.1.1.6.0		System Location	string	RO
1.3.6.1.2.1.1.7.0	72	System Services	integer	RO
1.3.6.1.4.1.21796.4.9.1.1.1.1	1	1. Input Index	integer	RO
1.3.6.1.4.1.21796.4.9.1.1.1.2	2	2. Input Index	integer	RO
1.3.6.1.4.1.21796.4.9.1.1.2.1	0	1. Input Value, 0=Open, 1=Close	integer	RO
1.3.6.1.4.1.21796.4.9.1.1.2.2	0	2. Input Value, 0=Open, 1=Close	integer	RO
1.3.6.1.4.1.21796.4.9.1.1.3.1	Input 1	1. Input Name	string	RO
1.3.6.1.4.1.21796.4.9.1.1.3.2	Input 2	2. Input Name	string	RO
1.3.6.1.4.1.21796.4.9.1.1.4.1	0	1. Input State, 0=Normal, 1=Alarm	integer	RO
1.3.6.1.4.1.21796.4.9.1.1.4.2	0	2. Input State, 0=Normal, 1=Alarm	integer	RO
1.3.6.1.4.1.21796.4.9.70.1.0	00:0A:59:04:F8:8E	System MAC address	string	RO

Time tab

The system time and parameters of optional automatic synchronisation via time servers is sent in the Time tab.

— *SNTP Settings*

- ***SNTP Server*** – IP address or domain address of the time synchronisation server; default time.nist.gov.
- ***Time Zone*** – Setting of the time zone based on the device location. Serves to set the correct system time. Required for correct recording of measured values.
- ***Summertime*** – Enable summer time. Serves to set the correct system time. Required for correct recording of measured values.
- ***Interval*** – Interval of time synchronisation with the server.

— *Time Settings*

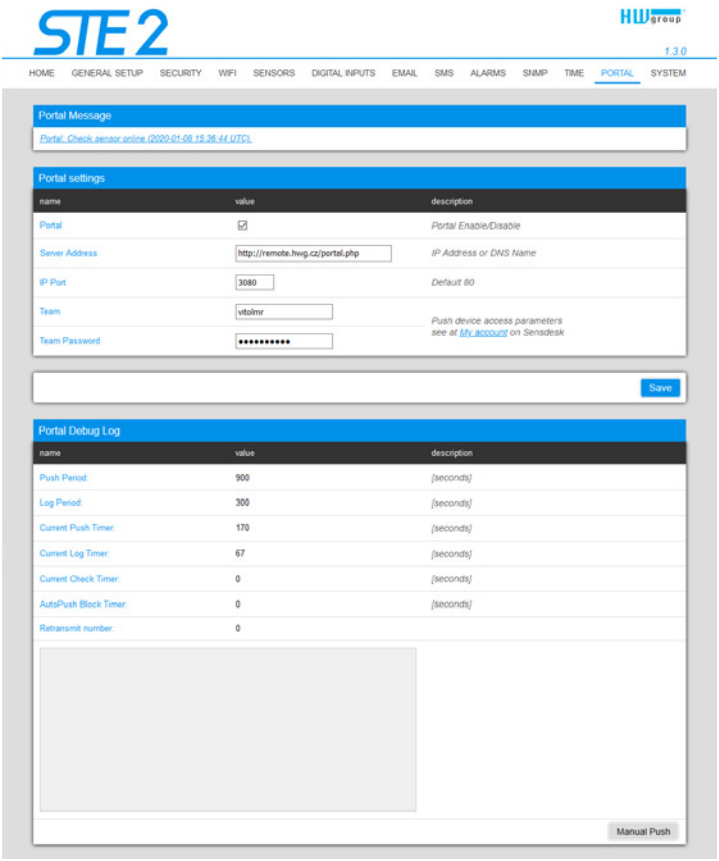
The Time Setup section enables filling in the current date and time manually, if synchronisation with the time server cannot be used.

— *SNTP Log*

The Sync button serves to perform instant synchronisation with the time server. It can also be used to test settings.

Portal tab

The tab serves to set parameters for sending data to a remote portal via HWg-PUSH protocol. More about the protocol or support of portal solutions is available on the website http://www.HW-group.com.



— *Portal Message section*

Feedback from the portal containing e.g. links to graphs, etc. Depends on the portal type.

— *Portal settings section*

- *Portal* – Enables or disables this function.
- *Server adress* – Complete URL of the remote server. Connection to the www.SensDesk.com is pre-set in the device.
- *IP Port* – Port which the portal tunes in to.
- *Team* – Name of the Team to which the device should be assigned.
- *Team Password* – Password of the Team to which the device should be assigned.

— *Input(s) AutoPush config section*

Sets the behaviour of AutoPush for DI inputs. During activation, the sending of information about changes in the input state to the portal is accelerated. The function can be enabled individually for each input.

— *Sensor(s) AutoPush config*

Sets the behaviour of the AutoPush function for individual sensors. The function accelerates the sending of information about fluctuating values to the portal. When the measured sensor value changes since last communication with the portal by more than the defined value, the device connects to the portal again and sends the new value.

— *Portal Debug Log section*

For debugging only. Event counters + Debug window for sending data to the portal.

- *Push Period* – Period of sending data to the remote portal. The period is determined by the portal and cannot be changed by the user.
- *Log Period* – Period of storing data for the portal in the cache. The period is determined by the portal and cannot be changed by the user.
- *Current Push Timer* – Timer indicating the time remaining until sending data to the portal.
- *Current Log Timer* – Timer indicating the time remaining until saving the data for the portal in the cache.
- *AutoPush Block Timer* – Time of incidents for AutoPush. If the permitted number of incidents for one Push period is exceeded, the AutoPush function will be blocked.
- *Retransmit number* – Counts the number of invalid Push attempts.
- *Manual Push* – Button for instant sending of data to the portal.

— *What is AutoPush*

- *AutoPush* – By default, the device thermometer sends data to the portal at a fixed interval defined by the relevant portal (in the case of the SensDesk portal, once every 15 minutes) and the user cannot change this value. A special case is the start and end of Alarms, when extraordinary sending will occur. AutoPush serves for the extraordinary sending of values also whenever the sensor value changes by more than the defined AutoPush value.

This concerns only the setting of communication between the device and the online portal. The values of local alarms are set in the portal.

System tab

— *Download section*

- *Backup configuration* – Configuration backup in BIN format. Click on the link to save the current device configuration after its final settings for potential restore purposes.
- *Online setup in XML* – Configuration backup in XML format. Click on the link to save the current device configuration after its final settings for potential restore purposes.
- *Online values in XML* – Current values in XML format. Click on the link to save the current device configuration after its final settings for potential restore purposes.
- *SNMP MIB Table* – SNMP MIB file. MIB file address containing the definition of SNMP variables.
- *OID keys table* – The function will draw up the entire tree of variables with indication of the entire SNMP OID and explanations of the variable type.
- *TXT list of common SNMP OIDs* – Overview of most important OID from the MIB table.

— *System section*

- *Product Name* – Device name (type).
- *Serial Number* – Device serial number.
- *Eth MAC Address* – MAC address of device for cable connection.
- *WiFi STA MAC Address* – MAC address of device for WiFi connection.
- *Version* – Firmware version. Serves for diagnostic purposes when solving problems.
- *Build* – Serves for diagnostic purposes when solving problems.
- *Compile time* – Firmware compile time. Serves for diagnostic purposes when solving problems.
- *UpTime* – Runtime of the device since last switching on or restart. Serves for diagnostic purposes when solving problems.
- *Demo mode* – Active demo mode prevents any changes in your device configuration. In this mode, users can browse and view all the web interface pages, but they are not allowed to change any values. A device with this setting can be placed on the public internet with no risk of changes in its configuration.
- *Read available version* – Lists the latest version of firmware on the HW group update server.
- *Start Network Upgrade* – Launches a firmware upgrade from the HW group update server.
- *Upload Firmware or Configuration* – Install newer firmware or configuration files to the device. Restore configuration may not work if there is too large a difference in firmware versions.

— *Factory Default section*

Restores factory settings. The default IP address is 192.168.10.20 and the username and password are not defined.

— *System Restart section*

Restarts the device.

Technical parameters

Ethernet	
Interface	RJ45 (10/100BASE-T)
Supported protocols	IP: ARP, TCP/IP (HTTP, HTTPS, SNTP, SMTP, HWg-Push, netGSM, TLS), UDP/IP (SNMP)
SNMP	Version 1 fully supported, some parts version 2

WiFi	
Supported standards	802.11 b/g/n
Frequency	2,4GHz
Output	+19.5 dBm output power in 802.11b mode +16 dBm for 802.11n
Security	WEP / WPA / WPA2 PSK / WPA2 TSK / WPS
Antenna	Internal

External sensors	
Port / connector	Port1, Port2 / RJ11 (1-Wire)
Connectability	Three external temperature or humidity sensors. One combined temperature + humidity sensor can be connected.
Sensor type	Only sensors from HW group s.r.o.
Sensors / distance	Max 3 sensors / Max 60 metres total length

DI INPUTS (Dry Contact Inputs)	
Port / connector	I1, I2 / ø 2 mm bracket
Type	Digital Input (supports NO/NC Dry contact)
Sensitivity	1 (On) = 0-500 Ohm (Right pin on the terminal block can be connected to 12V GND)
Max. distance	Up to 50m

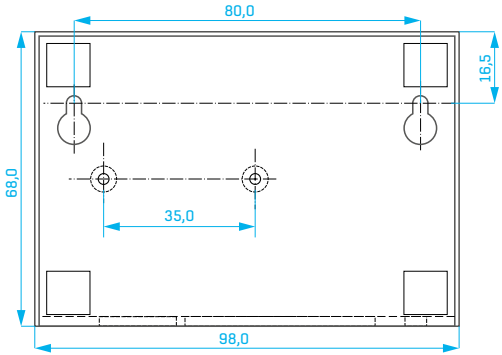
Power supply	
Power voltage	5V / 250 mA
Connector	Jack Ø3.5 x 1.35 / 10 [mm]
PoE (Power over Ethernet)	RJ45 - IEEE 802.3af Class 0

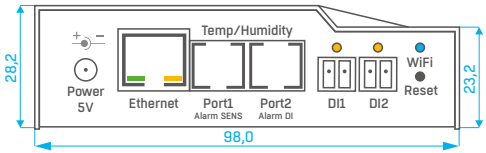
LED	
LINK	Green – Ethernet connection state
Activity	Yellow – Ethernet activity
Alarm	Port 1 – Alarm SENS – Shines if alarm active on sensor Port 2 – Alarm DI – Shines if alarm active on sensor
IN	Yellow – activation of the contact
WiFi	Blue – connection state in operation (shining), search indicator (flashing slowly) and connection (flashing quickly)

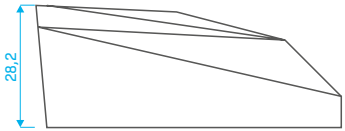
Button	
Reset	Restore default settings: hold or 5 seconds after connecting power supply.

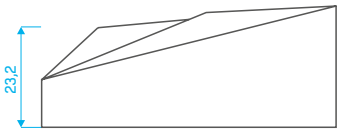
Other parameters	
Operating temperature	-10 to 60 °C (range of device operating temperatures – may not correspond to sensor range)
Dimensions/weight	65 x 80 x 30 [mm] / 500 g
Elmag. radiation	CE / FCC Part 15, Class B
Elmag. compatibility	EN 55022, EN 55024, EN 61000

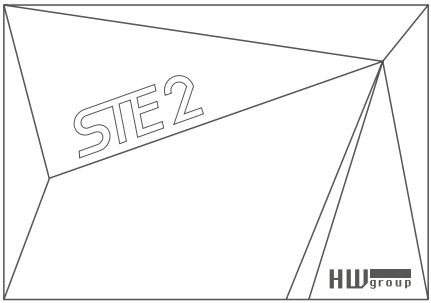
Physical dimensions











WiFi Radio

Description	Min	Typical	Max	Unit
Input frequency	2412	-	2484	MHz
Tx power				
Output power of PA for 72.2 Mbps	13	14	15	dBm
Output power of PA for 11b mode	19,5	20	20,5	dBm
Sensitivity				
DSSS, 1 Mbps	-	–98	-	dBm
CCK, 11 Mbps	-	–91	-	dBm
OFDM, 6 Mbps	-	–93	-	dBm
OFDM, 54 Mbps	-	–75	-	dBm
HT20, MCS0	-	–93	-	dBm
HT20, MCS7	-	–73	-	dBm
HT40, MCS0	-	–90	-	dBm
HT40, MCS7	-	–70	-	dBm
MCS32	-	–89	-	dBm
Adjacent Channel Rejection				
OFDM, 6Mbps		37		dB
OFDM, 54Mbps		21		dB
HT20, MCS0		37		dB
HT20, MCS7		20		dB

WiFi signal strength

What is signals strength

WiFi is a radio signal and it has limitations in reach given firstly by the transmission output and by the quality and shape of the antennas. Signal strength is indicated in decibels per miliwatt of output (dBm), often (incorrectly) simplified to "dB". Signal strength has a negative value and it applies that the lower the value (a higher number after the negative sign), the worse.

The decibel unit is non-dimensional and expresses the logarithm of a ratio of two values. In our case, it is the ratio of received output to an etalon of 1 mW:

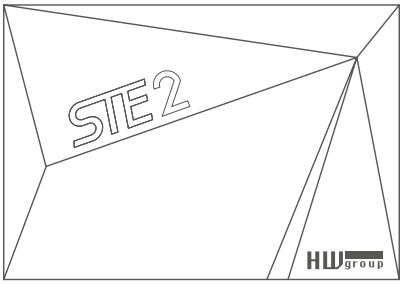
$$dBm = 10 * \log_{10} \frac{P_1}{1\ mW}$$

This means that if you have a signal of -54 dBm, it is higher (better) than a value of -82 dBm.

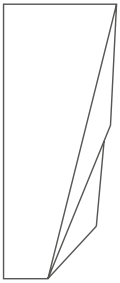
Impact of device position vis-à-vis the transmitter (router or AP)

The device uses a flat antenna similar to mobile telephones or laptops, while the connection points generally use multi-directional antennas (rods). Flat antennas have the same or better sensitivity as multi-directional antennas (the transition connector is omitted), but its primary disadvantages include sensitivity to the positioning of the device vis-à-vis the connection point.

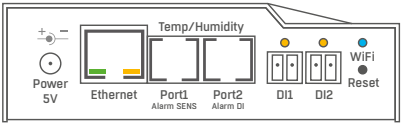
WiFi AP



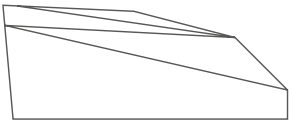
WiFi AP



WiFi AP



WiFi AP



Supported interfaces

Dry contact Inputs

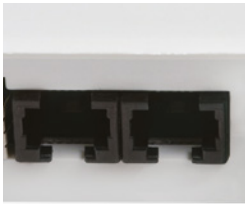
Dry contacts can be connected to the brackets.
For instance door contacts.
The inputs are galvanically connected to the power supply.

- *Unconnected input* has a value of „**0 (Off)**".
- *Active input* is identified as „**1 (On)**", Ohmic resistance of the input against the Common bracket must range between 0 Ω and 500 Ω.

— *Connection parameters:*

- *Maximum cable length:* 50 metres.
- *Supported sensors:* Any dry contact.
- *Alarm setting for each DI input*
  - Alarm inactive.
  - Alarm state when the contact is activated or deactivated.
  - Alarm state when the contact is deactivated.
- *Options for reacting to Alarm state:* Common settings for all inputs.
  - No reaction.
  - Notify of Alarm by sending e-mail or SMS.
- *Reading period:* 800 ms.
- *Range of ID sensors:* Inputs use address ID in the range of 1 to 9.
- *Sensor name:* The sensor can be named independently with up to 12 characters.
- *Sensor disconnection detection:* No, the disconnected sensor returns to the value „**0 (Off)**".

RJ11 – 1-Wire bus



Digital bus by Dallas Semiconductor, each sensor has a unique ID.

We recommend lines up to a total length of 60 m. There are known cases of experimentation with bus function up to a distance of tens to hundreds of metres.

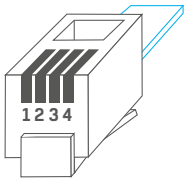
Flawless functioning cannot be guarantee for cables lines than 60 m from one connector on the device. It depends on the make of the cable, topology of the line and environment where the line is installed.

Active / Passive 1-Wire port

- *Active port:* RJ11 connector on the device. It guarantees full maximum distance of the sensors and power supply for all sensors.

When you reconnected the connected sensor from one active port to another, the sensor shows up as disconnected. You must restart automatic sensor detection.

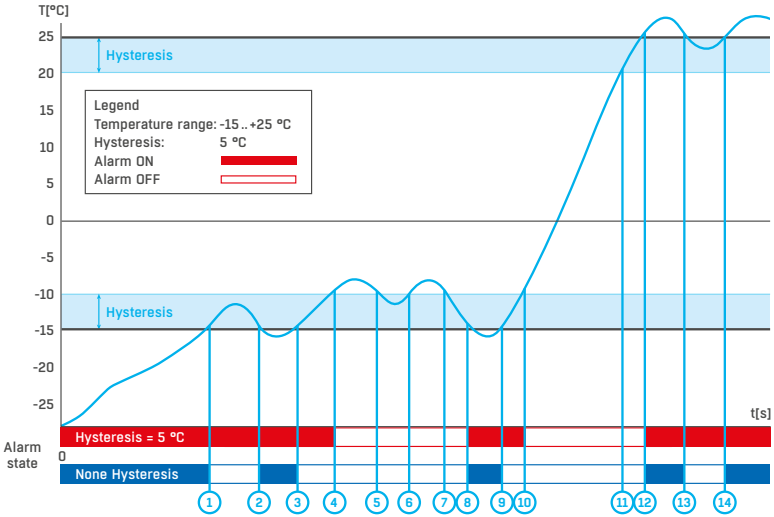
- *Passive port:* RJ11 connector on the T-Hub router or RJ11 connector from the sensor (if sensors are chained).



RJ11		
1	-	Not used
2	Data	Transmit Data
3	GND	Ground
4	+5V	Power

Sensor Hysteresis

The Hysteresis value defines the width of the tolerance range for sending an alarm. The function prevents the occurrence of multiple alarms in cases when the value oscillates around the defined value. The function is apparent from the graph.

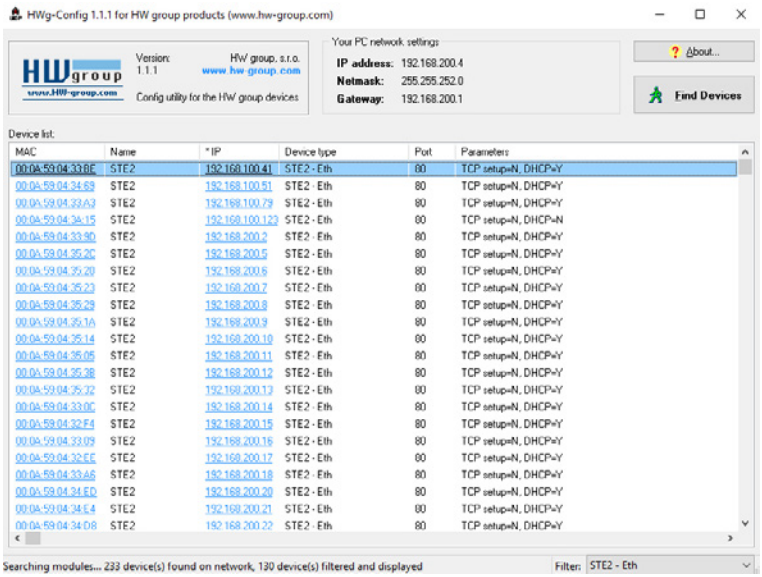


Within the internal 5°C hysteresis band, the alarm would be activated in **point 8** and would end in **point 9**. Because of the hysteresis function, the alarm is extended until the temperature reaches the end of the hysteresis zone (point 10) 5 °C + (-15 °C) = -10 °C.

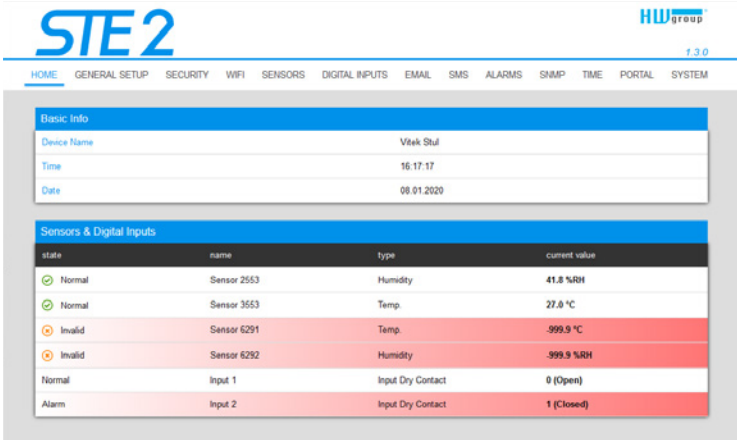
- *Hysteresis (=5 °C):* The unit sends **3** e-mails (**SMS**)
  Alarm at points **0..4**, **8..10**, **12** and upwards.
- *Without hysteresis (0 °C):* The unit sends **8** e-mails (**SMS**)
  Alarm at points **0..1**, **2..3**, **8..9**, **12..13**, **14** and upwards.

Connecting STE2 to the SensDesk portal

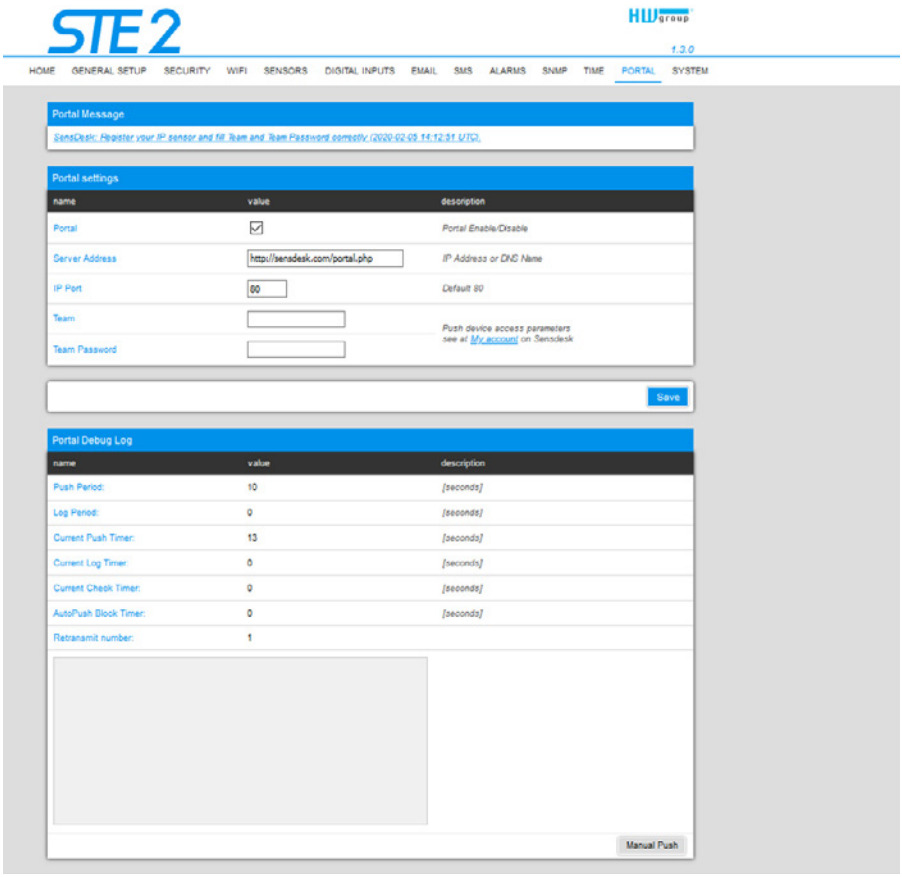
1 Connect the device to the computer network and set the network parameters (see the **First Steps** chapter).

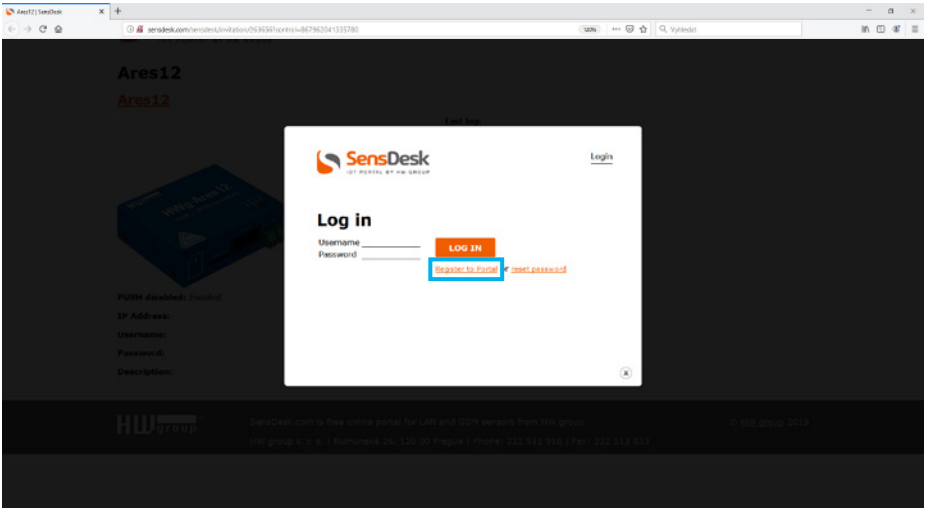


2 Check the device website:

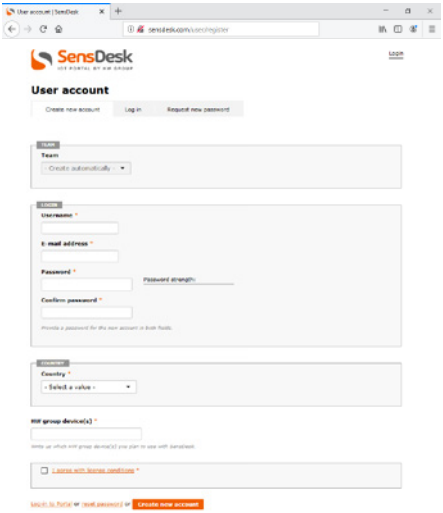


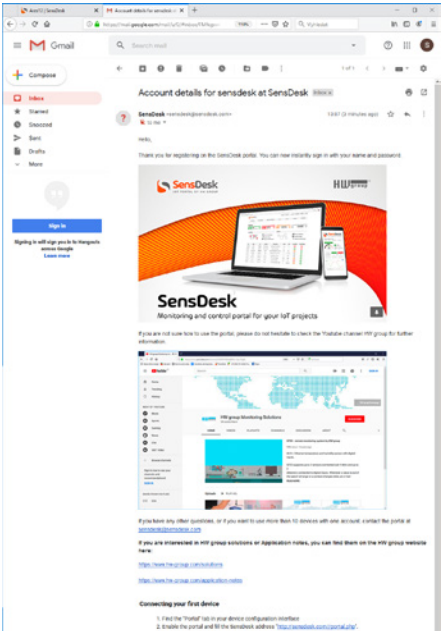
3 Tick the *Enable Portal* option and save the changes using the *Save* button in the bottom right corner of the window. Then click the *Manual Push* button in order to activate the portal function. Instead of "Portal disabled", a link *SensDesk.com: register your IP sensor* should appear in the *Portal Message* field. Click this link in order to get to the *SensDesk.com* portal.



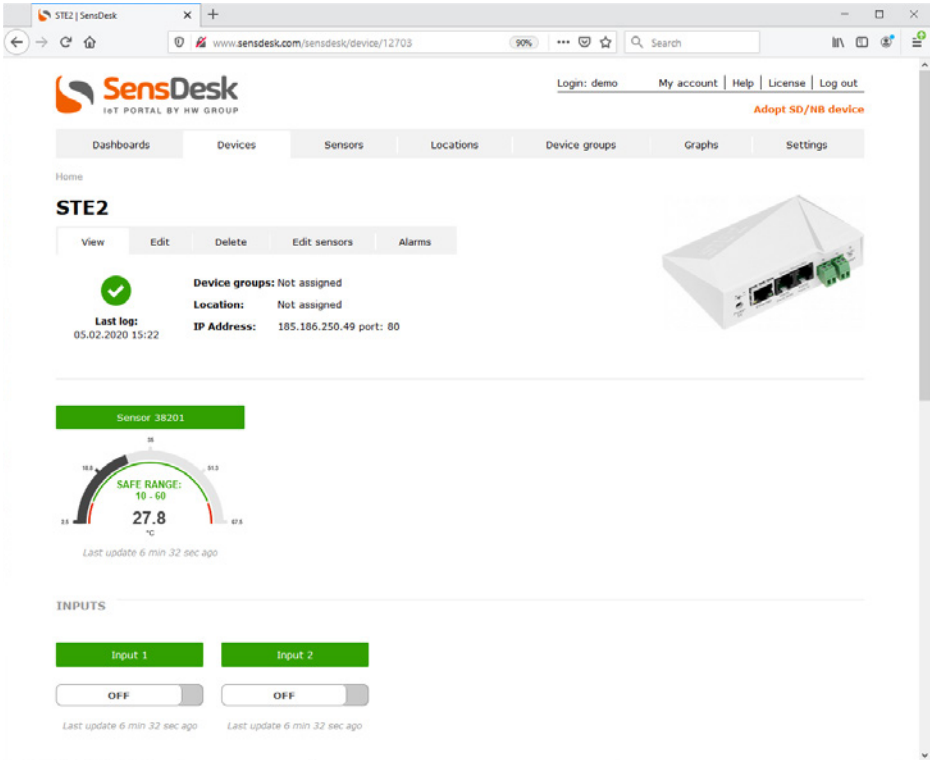


4 In case you already have a user account, please enter your login details and the device will be automatically assigned to your account. If you do not have a SensDesk account yet, click the *Register* and a registration form will be shown.

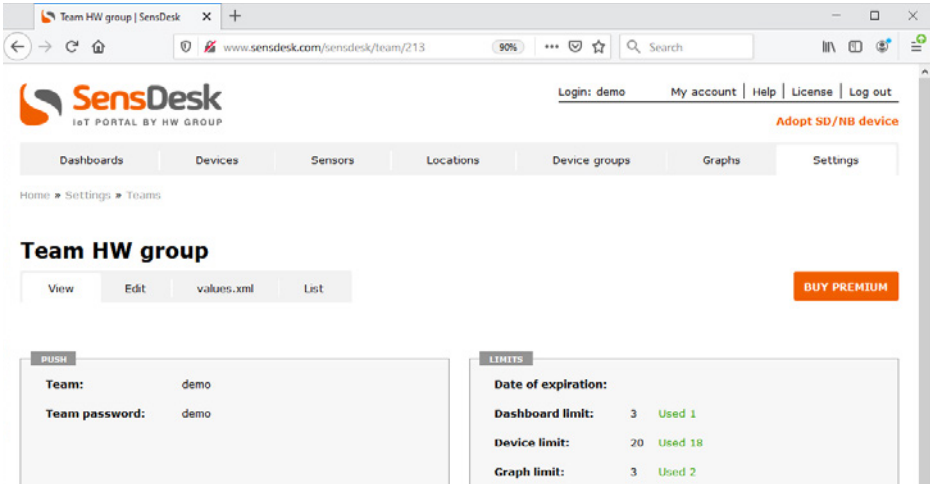




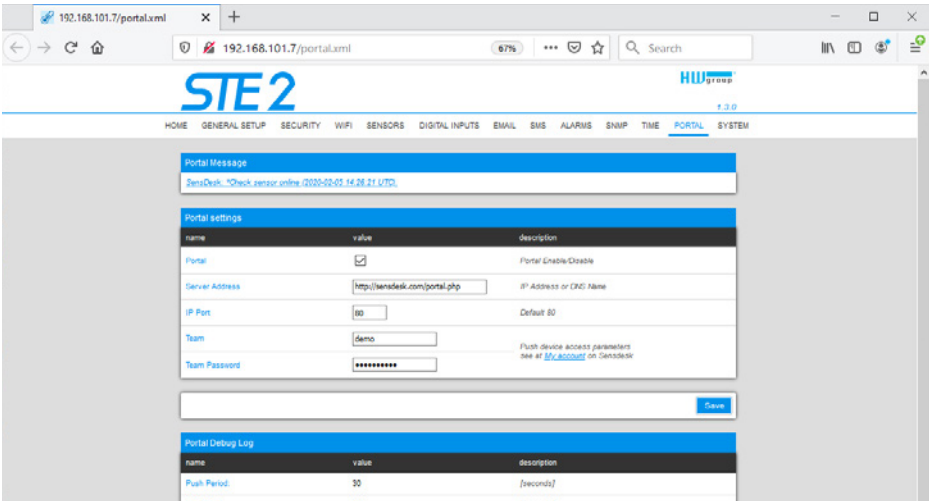
5 Enter the login details for your new account and a correct e-mail address. This e-mail address has to be unique for the server (cannot be already registered by another user).



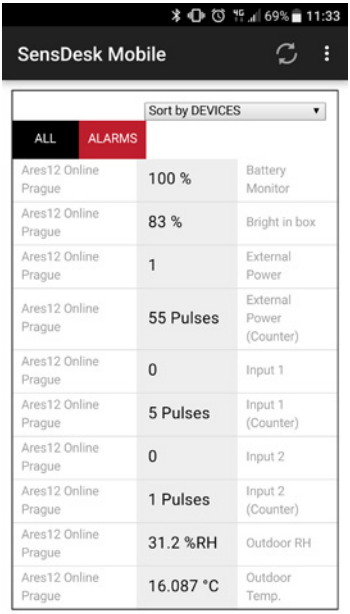
6 By activating the account, you will be redirected to the *Devices* > *View* page. At this moment, the data-sending period is set to 10 seconds to show the sensors functionality. This page is active only for approximately 15 minutes after the activation, then the logging period changes to 15 minutes.



7 If you check *Teams* link, you will find your *Team Password*. This password, together with your login name, identifies the device in communication with your account and in communication of mobile applications with SensDesk. The password cannot be changed and for a security reason it is different to the login password.



8 *Team Password* can be used in devices to skip the logging procedure during assigning the device to your portal account, or in mobile applications:

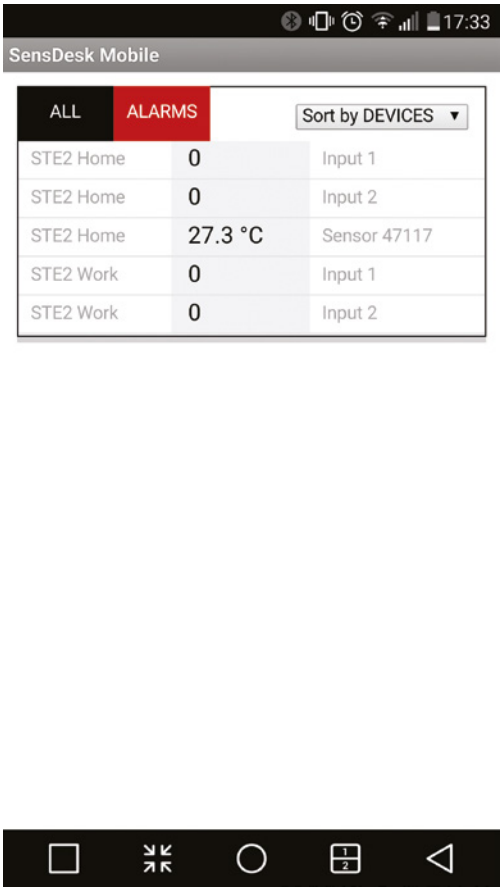


Portal function periodically sends the data to a remote server and the sending period is set by this server.

AutoPush is a function allowing unusual measured data sending, beside the periodical logging, in case that the value change is higher than the AutoPush delta parameter.

Using the mobile phone app

The **Username** and **PUSH Device** password can also be used in the application settings on mobile phones.

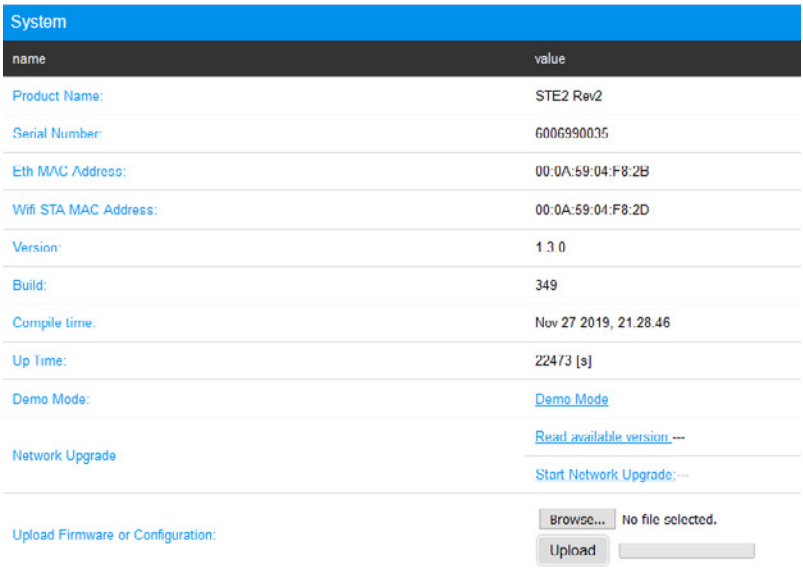


Firmware upgrade in STE2 units

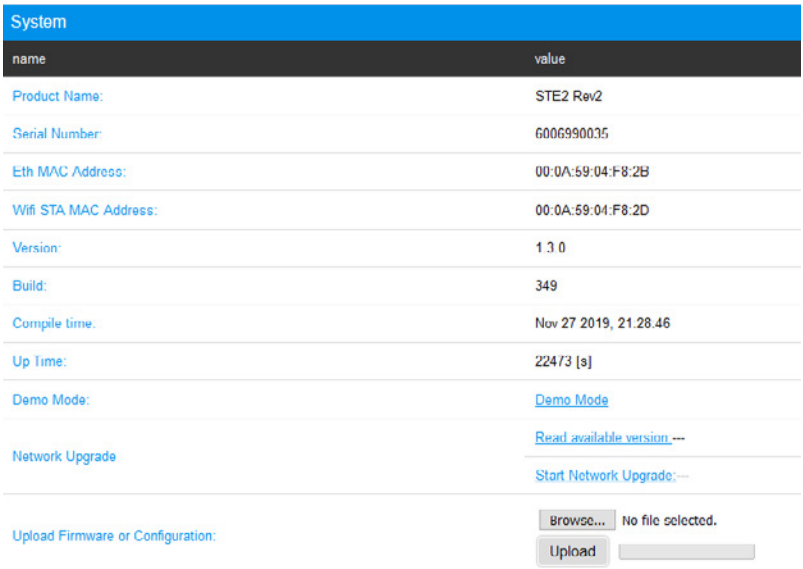
1 Open the device web interface in the *System* tab.

2 The *System* section contains items to identify and download the current FW version.

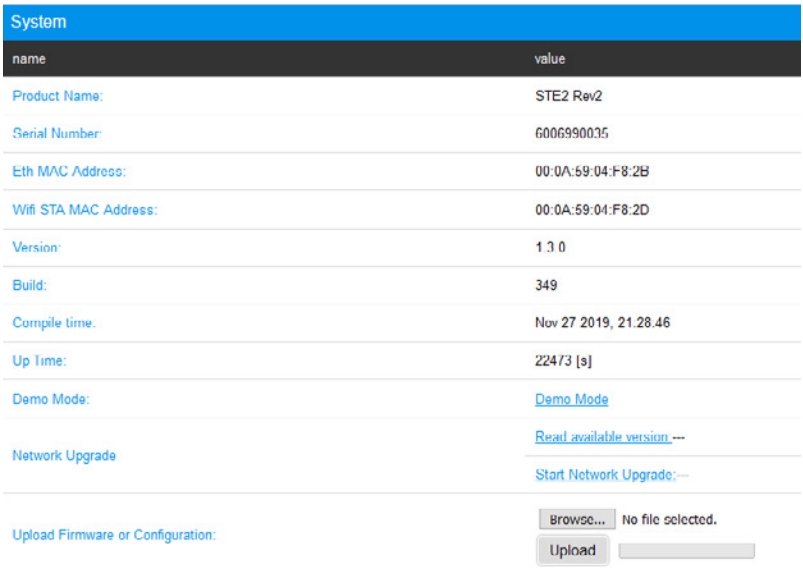
3 *Read available version* – Serves to identify and display the current firmware version on the update server. Clock on the *Read available version* link.



4 *Start Network Upgrade* – Serves to upgrade firmware to the device. The download progress is displayed while upgrading. Click on the *Start Network Upgrade* link.

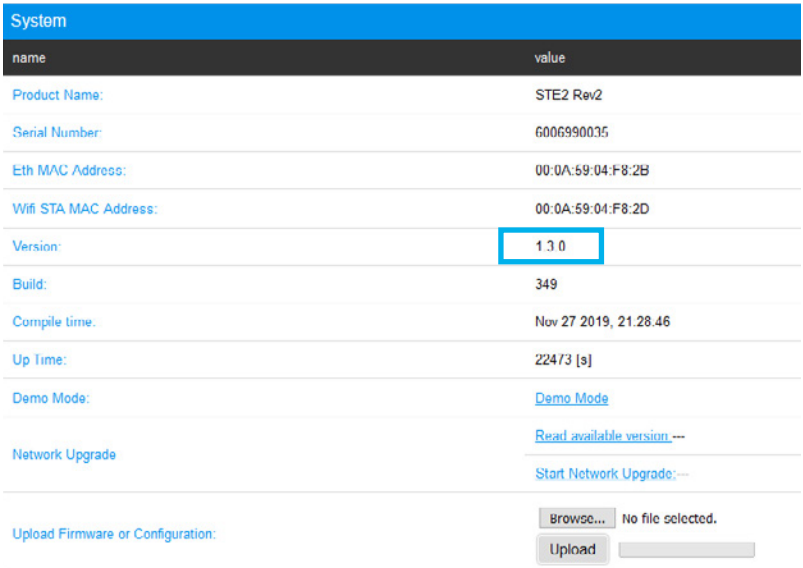


5 After the upgrade, the user is requested to restart the device manually.



To do this, press the *Restart* button. **The device will not restart automatically and this must be done manually.**

Check the firmware version after restart.



HW group s.r.o.
Rumunská 26/122
Prague, 120 00
Czech Republic

Phone: +420 222 511 918
Fax: +420 222 513 833

www.HW-group.com