WLD2

WLD2 – 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
Features 4
Usage examples 4
Basic features 5
Scalability 5
Comparison of HWg-WLD and WLD2 5
Connectors and connections 6
First start-up 7
WWW interface 9
Home tab 9
General Setup tab 10
Security tab 11
WiFi tab 12
Sensors tab 15
Outputs tab 16
E-mail tab 17
SMS tab 18
Alarms tab 19
SNMP tab 20
Time tab 22
Portal tab 23
System tab 25
Technical parameters 27
Physical dimensions 28
WiFi Radio 29
WiFi signal strength 29
Connecting WLD2 to the SensDesk portal 30
Using the mobile phone app 35
Firmware upgrade in WLD2 units 36

Features

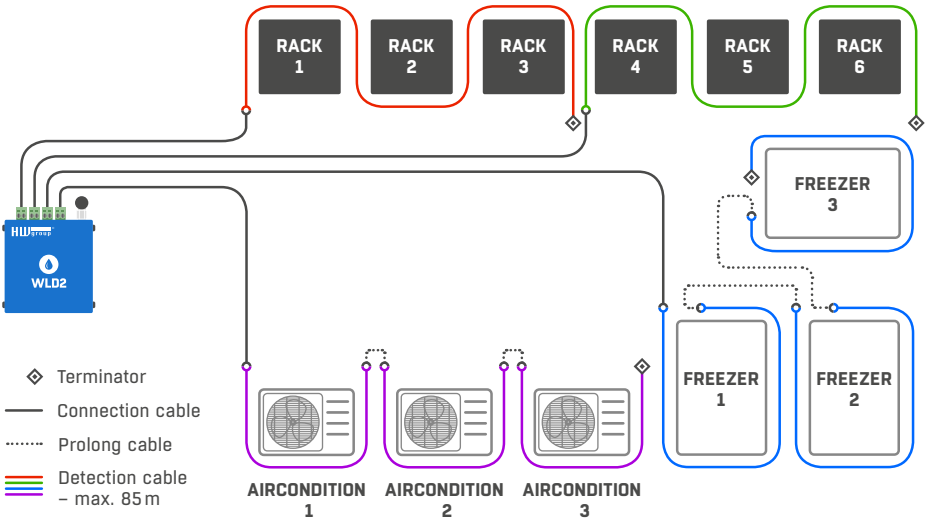
WLD 2 – Quad water leak detector with WiFi and Ethernet

WLD2 is a WiFi / Ethernet water leak detector with support for WWW, SNMP and PoE. To detect leaking liquids, it uses sensing cables. With braided liquid-absorbing cables, it is possible to detect even the smallest volumes of liquids, such as condensation from A/C pipes or water leaks in general – before a critical volume of water, ethylene glycol, or another conductive liquid forms and damages become costly. In addition to flooding, the detector also detects disconnected or damaged sensing cable for increased reliability.

Thanks to WiFi connectivity, the WLD2 WiFi water leak detector can be installed in hard-to-access places and, in case of flooding, send an alert via e-mail, SNMP trap, or – with an external SMS gateway by HW group – even send a text message or dial a phone number. Of course, in critical applications, it can also communicate via wired Ethernet and can be powered with PoE.

WLD2 can be connected to the SensDesk portal using the HWg-Push protocol, as well as to standard monitoring systems thanks to SNMP and SNMP Trap support. Flooding can be also indicated by switching a remote output (e.g. a relay) over the network (Box-2-Box mode with a Poseidon2 or Damocles2 unit), independently for each sensing cable.

Compared to HWg-WLD, up to 4 independent detecting cables can be connected to the WLD2 to help locate the leak more accurately.



Usage examples

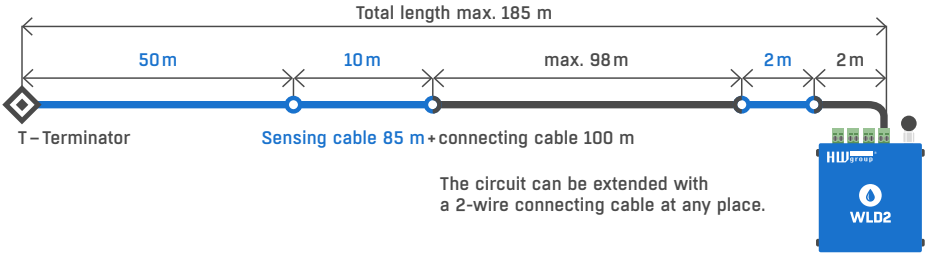
- Water detection under raised floors.
- Leaky pipe detection (cable wrapped along the pipe).
- Protection against floods from skylights – sensing cable routed along the walls.
- Detection of water leaks in drip trays.
- Detection of water leaks under air-conditioning outlets.

Basic features

- Simple installation, support for automatic network configuration via DHCP.
- Intuitive WWW interface for fast and easy installation.
- Ability to communicate over WiFi (external antenna for extended range, support for 2.4GHz, 2.11 b/g/n) and Ethernet at the same time.
- With support for up to 4 sensing cables (each max. 85m), detection capabilities can be scaled and the source of the leak more easily identified.
- The sensing cable can be fixed using clips or adhesive tape.
- WLD2 signals the following states: OK / Flooded / Sensing cable fault.
- Flooding alerts can be send as a standard e-mail, or as a text message (SMS) through a SMS gateway available from HW group.
- Detected leaks or WLD sensing cable disconnections can be signaled by activating a relay output at a Poseidon2 or Damocles2 unit over the Ethernet.
- WLD2 can be easily mounted on a wall or in a 19" cabinet.
- Powered over PoE or from an external adapter.

Scalability

WLD2 supports up to 4 independent sensing cables. This makes it easier to locate the source of the leak. Each detection circuit can consist of up to 85m of sensing cable + up to 100m of connecting cable.



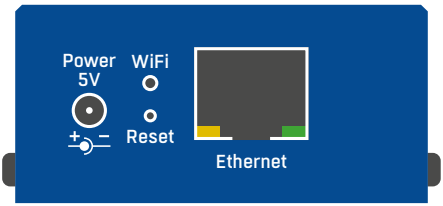
Comparison of HWg-WLD and WLD2

Function	HWg-WLD	WLD2
WLD circuits	1	4
Ethernet	✔	✔
WiFi	✖	✔
HTTPs	✖	✔
External antenna	✖	✔
TLS	✖	✔
SensDesk support	✖	✔
PoE	✖	✔
Remote outputs	1	4

Connectors and connections

Connectors

- *Ethernet* – for a wired internet connection in case of LAN operation, or for initial configuration in case of WiFi operation. Can be used to power the device via PoE (Power over Ethernet).
- *WLD1 – WLD4* – for connecting up to 4 liquid sensing cables.
- *Power* – connector for a 5V power supply if the device is powered from an external adapter.

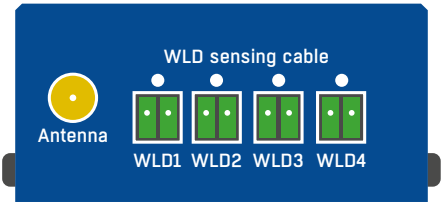


LED indicators

- *Link* – green LED indicates an active network connection.
- *Activity* – flashing yellow LED indicates ongoing communication over the wired network connection.
- *WiFi* – blue LED indicates an active connection to a WiFi Access Point. While establishing the connection, flashing LED indicates status.
- *WLD LED* – 4 red LEDs above the connectors for the sensing cable. When lit, the respective circuit is in Alarm – liquid is detected or the cable is disconnected.

Button

- *Reset* – to reset the device to factory defaults.
  1. Turn the device off.
  2. Press and hold the button.
  3. Turn the device on and hold the button for another 5 seconds.
  4. All LEDs light up in sequence.
  5. Turn the device on again, factory defaults are restored.



First start-up

First step

1 Cable connection

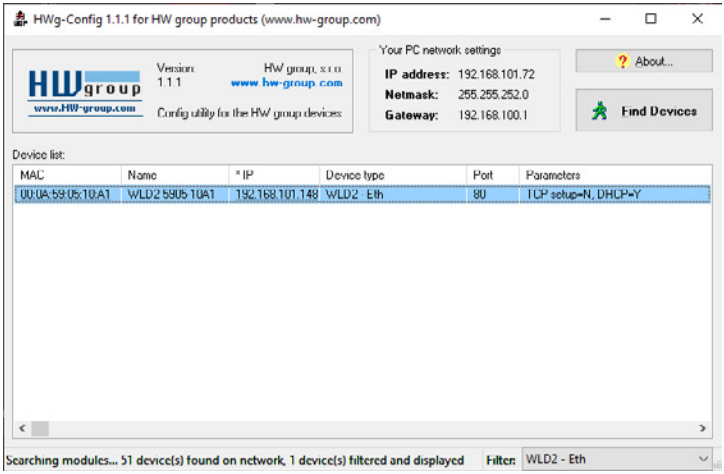
- Connect the device to the **Ethernet** (direct cable to the **switch**, crossed to PC).
- Connect the power adapter to the grid and connect it to the device power supply connector.
- The green LED in the **Power & Mode** RJ45 connector will light up.
- If connection to the **Ethernet**, is functional, 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.



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:

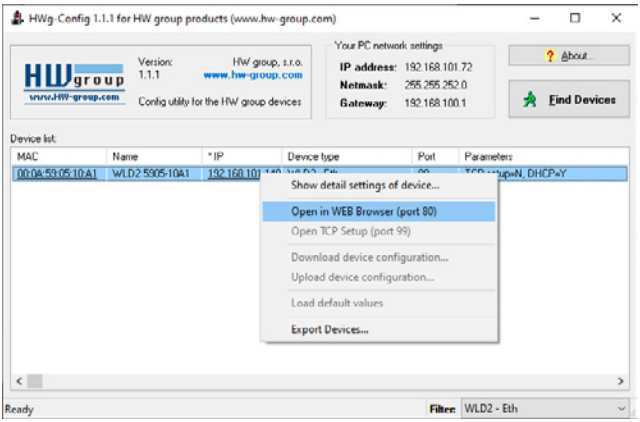
- Right-click on the device MAC address. The default values from the HWg-Config can be restored by software mode during the first 60 settings after start-up.

- 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

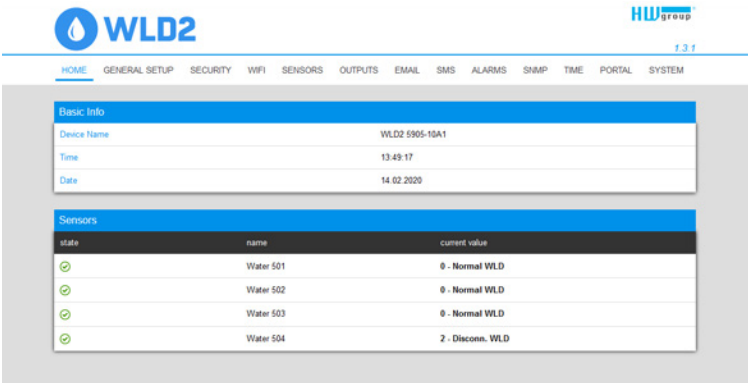
Options of opening the website:

- 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.



WWW interface

Home tab



— *Base Information section*

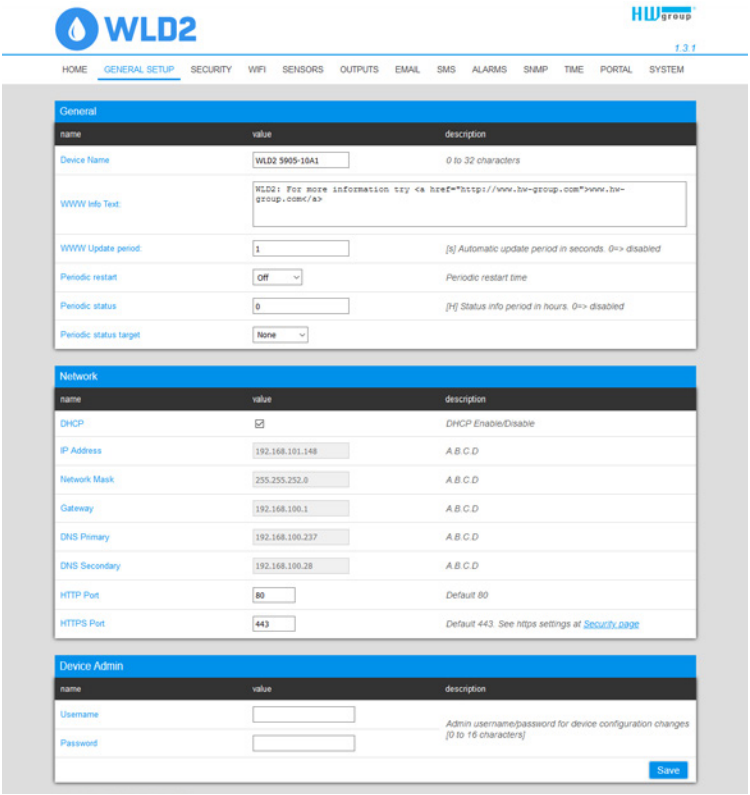
- *Device Name* – the device name serves to distinguish specific devices in larger installations. Can be set in the General Setup tab.
- *Time* – current device time. The time can be set automatically from the internet or manually in the Time tab. In the case of automatic setting, the correct value is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

Lists the current values of sensors.

- *State* – input or sensor state.
  - *Normal* – idle state, all normal.
  - *Disconnect* – the sensing cable is disconnected or damaged.
  - *Flooded* – liquid was detected.
- *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.

General Setup tab



— *General section*

- *Device Name* – device name (WLD2), 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.

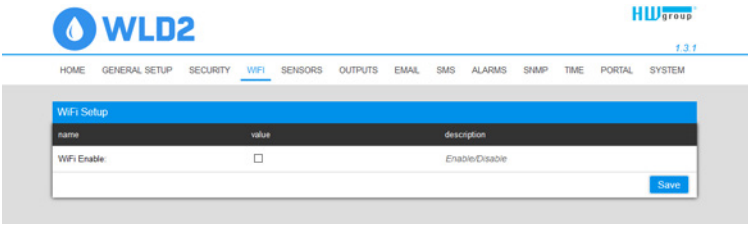
— *Generate the SSL key and certificate*

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

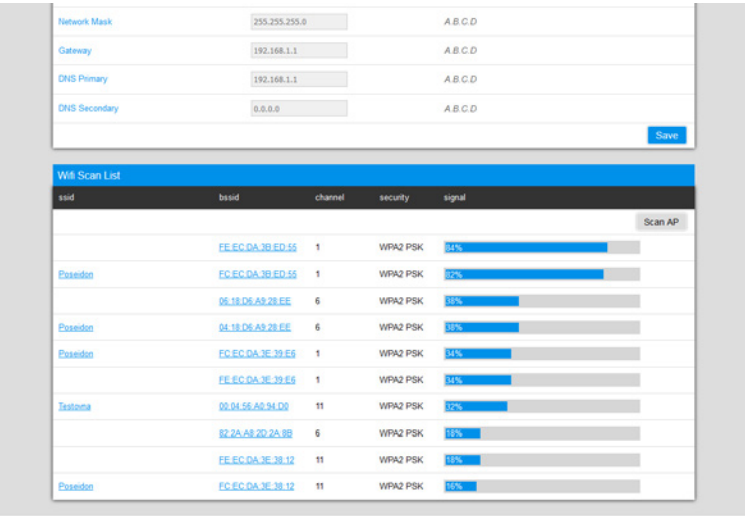
- ***SSID*** – name of found WiFi network.
- ***BSSID*** – connection point identifier (MAC address).
- ***Channel*** – WiFi channel on which the connection point operates.
- ***Security*** – type of secured WiFi communication.
- ***Signal*** – signal level in DB. The higher the value, the better. WARNING,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

Connecting to found WiFi

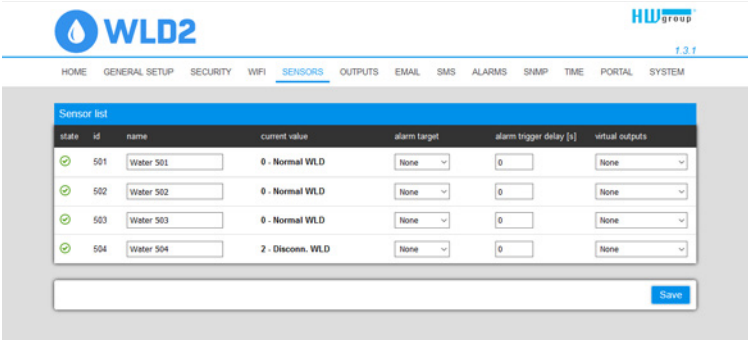
- Click on the SSID of the found network to prefill WiFi setting and just enter the Password. The BSSID remains empty. Standard setting. Reconnects automatically if AP is changed.

- 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



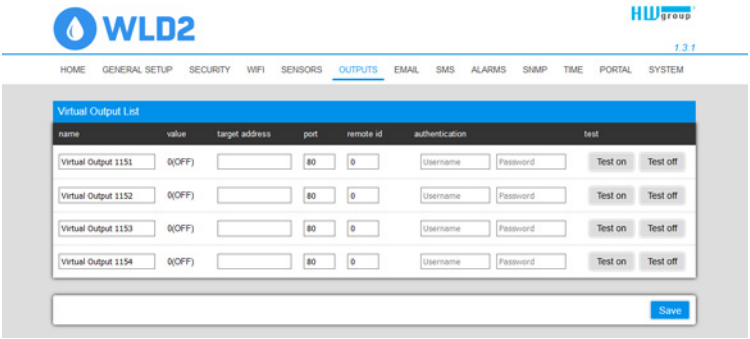
— *Sensor List section* *

- *State* – input or sensor state.
  - *Normal* – idle state, all normal.
  - *Disconnect* – the sensing cable is disconnected or damaged.
  - *Flooded* – liquid was detected.
- *ID* – sensor ID identical to ID in Poseidon2 and WLD2 units.
- *Name* – sensor name for better identification in larger systems. The name can be set in the Sensors tab.
- *Current Value* – current value including unit of measure.
- *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.
- *Virtual Outputs* – remote output that is switched (closed) whenever a liquid is detected or the sensing cable is disconnected. Configured at the Outputs tab.

** Sensors in Alarm state are highlighted.*

Outputs tab

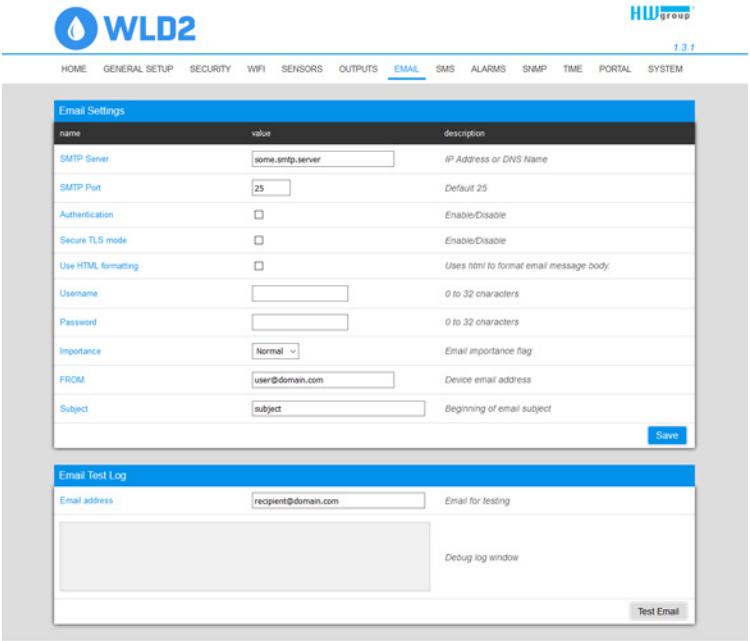
Defines the parameters of up to 4 remote outputs, usually relays (on Damocles or Poseidon units).



— *Virtual Output List*

- *Name* – name of the output. Shown at the Sensors page in the Virtual Outputs column.
- *Value* – current state of the output.
- *Target address* – IP address of the device with the controlled output.
- *Port* – TCP port where the device with the controlled output listens (usually 80).
- *Remote ID* – ID of the controlled output at the remote device.
- *Authentication* – username and passphrase for controlling the outputs, if set at the device.
- *Test On a Test off* – for testing the settings.

E-mail tab



— *E-mail Settings*

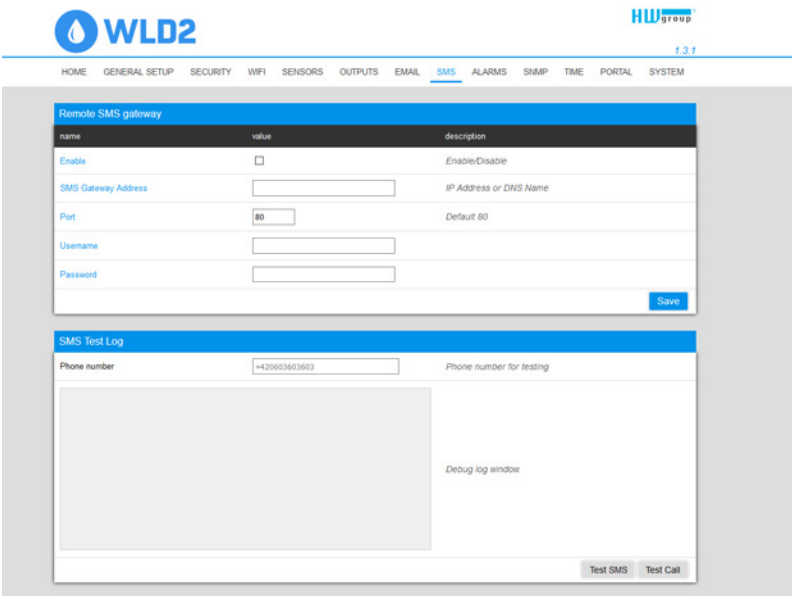
- ***SMTP Server*** – IP address or domain address of the SMTP server.
- ***SMTP Port*** – port number on which the e-mail server tunes in – 25 by standard.
- ***Authentication*** – enable authentication; check if the SMTP server requires authentication.
- ***Secure TLS mode*** – check if the SMTP server 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.

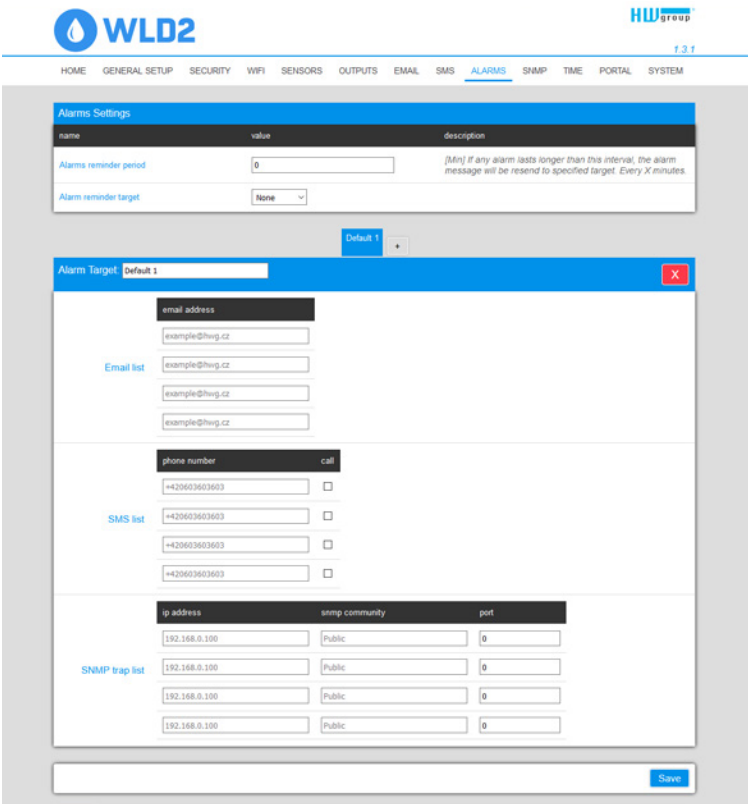
— *SMS Test Log*

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*

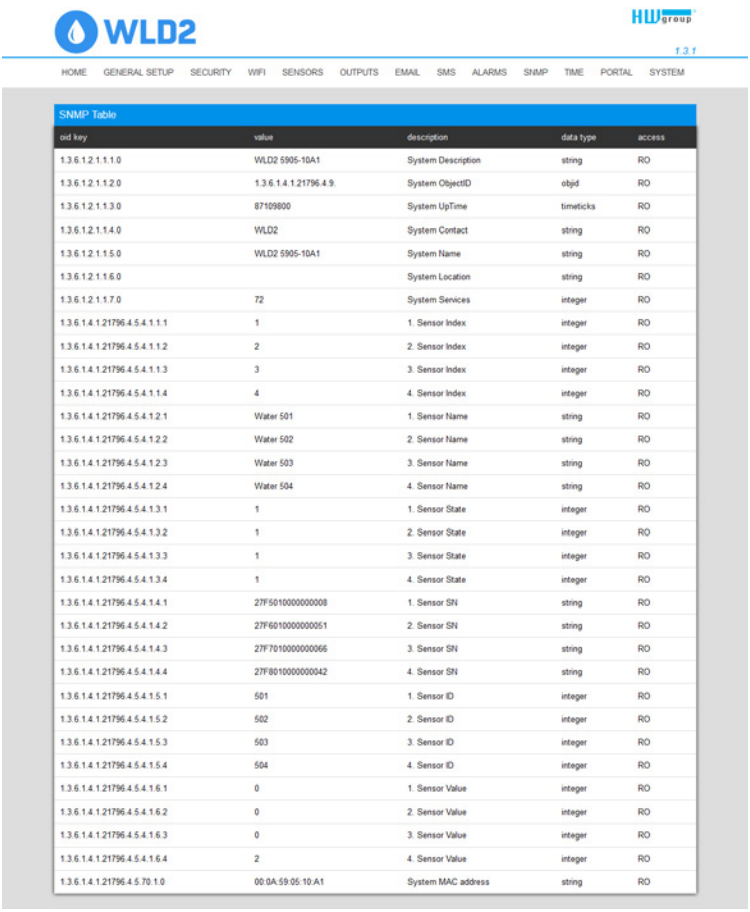
- *System Name* – device name within SNMP.
- *System Location* – device location within SNMP.
- *System Contact* – contact of the device administrator within SNMP.
- *SNMP port* – port number on which communication via SNMP is possible – 161 by standard.

— *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.

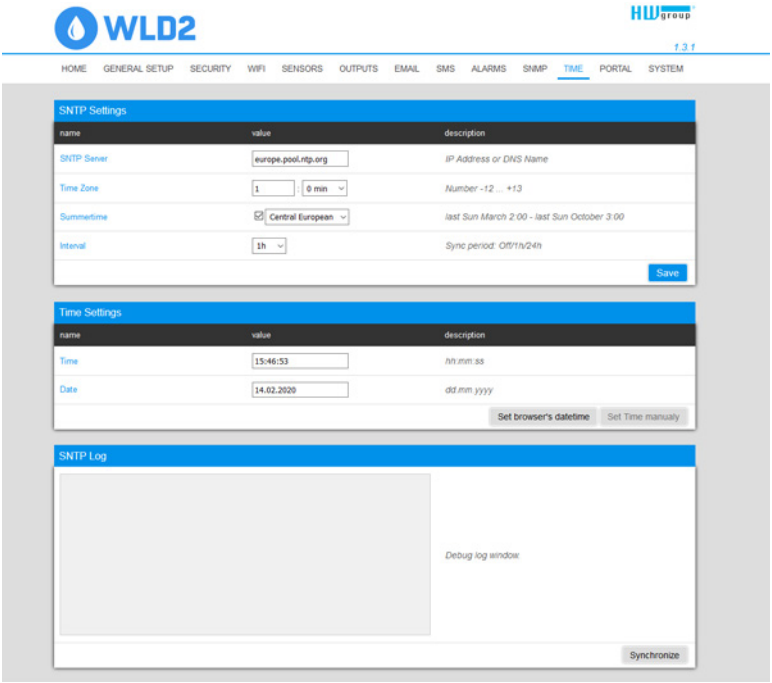


SNMP Table

oid key	value	description	data type	access
1.3.6.1.2.1.1.1.0	WLD2 5905-10A1	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	87109800	System UpTime	timeticks	RO
1.3.6.1.2.1.1.4.0	WLD2	System Contact	string	RO
1.3.6.1.2.1.1.5.0	WLD2 5905-10A1	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
1.3.6.1.4.1.21796.4.5.4.1.1.1	1	1. Sensor Index	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.1.2	2	2. Sensor Index	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.1.3	3	3. Sensor Index	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.1.4	4	4. Sensor Index	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.2.1	Water 501	1. Sensor Name	string	RO
1.3.6.1.4.1.21796.4.5.4.1.2.2	Water 502	2. Sensor Name	string	RO
1.3.6.1.4.1.21796.4.5.4.1.2.3	Water 503	3. Sensor Name	string	RO
1.3.6.1.4.1.21796.4.5.4.1.2.4	Water 504	4. Sensor Name	string	RO
1.3.6.1.4.1.21796.4.5.4.1.3.1	1	1. Sensor State	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.3.2	1	2. Sensor State	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.3.3	1	3. Sensor State	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.3.4	1	4. Sensor State	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.4.1	27F5010000000008	1. Sensor SN	string	RO
1.3.6.1.4.1.21796.4.5.4.1.4.2	27F6010000000051	2. Sensor SN	string	RO
1.3.6.1.4.1.21796.4.5.4.1.4.3	27F7010000000066	3. Sensor SN	string	RO
1.3.6.1.4.1.21796.4.5.4.1.4.4	27F8010000000042	4. Sensor SN	string	RO
1.3.6.1.4.1.21796.4.5.4.1.5.1	501	1. Sensor ID	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.5.2	502	2. Sensor ID	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.5.3	503	3. Sensor ID	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.5.4	504	4. Sensor ID	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.6.1	0	1. Sensor Value	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.6.2	0	2. Sensor Value	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.6.3	0	3. Sensor Value	integer	RO
1.3.6.1.4.1.21796.4.5.4.1.6.4	2	4. Sensor Value	integer	RO
1.3.6.1.4.1.21796.4.5.70.1.0	00:0A:59:05:10:A1	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*

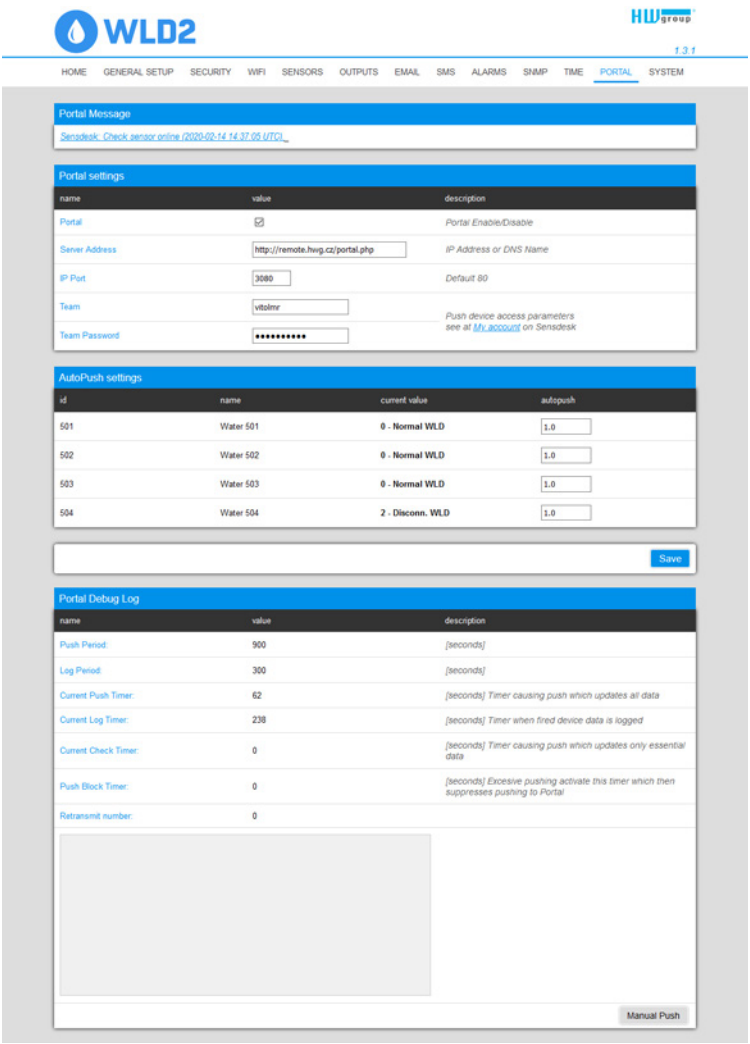
The Time Setup section enables filling in the current date and time manually, if synchronisation with the time server cannot be used.

— *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.

— *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.

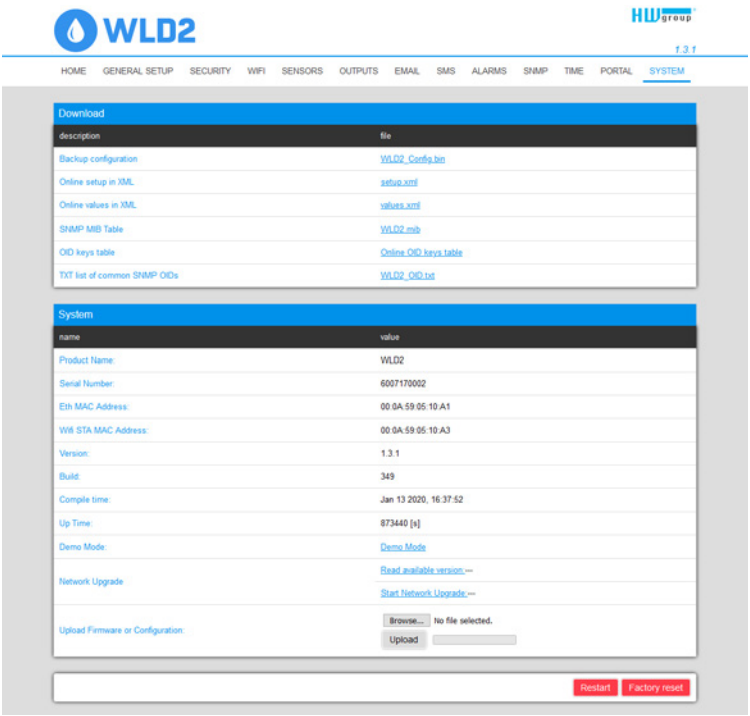
- ***Push Period*** – period of sending data to the remote portal. The period is determined by the portal and cannot be changed by the user.
- ***Log Period*** – period of storing data for the portal in the cache. The period is determined by the portal and cannot be changed by the user.
- ***Current 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	
Number/Connectors	WLD1, WLD2, WLD3, WLD4 / terminal blocks
Type	Moisture sensing cable
Connector	Terminal block
Sensor states	0 = OK, 1 = Flooded, 2 = Cable disconnected
Sensing cable length	Max 85 m
Cable extension	May be extended by at most 100 m, AWG 24

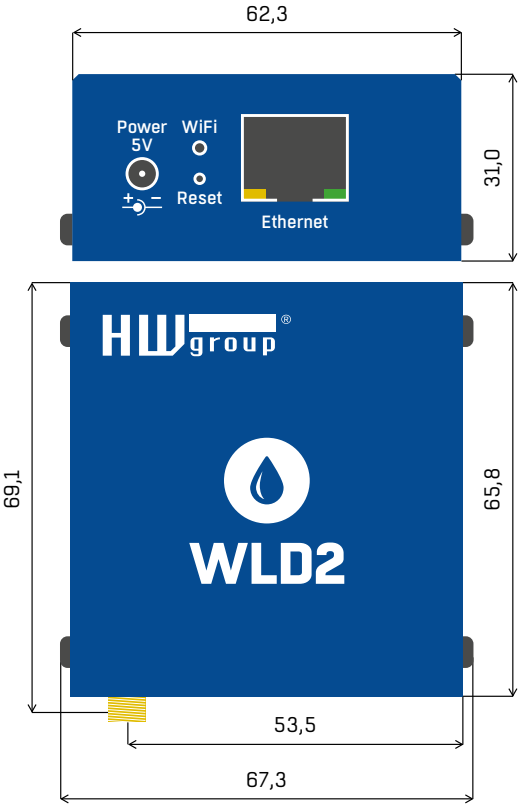
Power supply	
Power voltage	5V / 250 mA
Connector	Jack Ø 3.5×1.35 / 10 [mm]
PoE (Power over Ethernet)	RJ45 - IEEE 802.3af Class 0

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	65×80×30 [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.

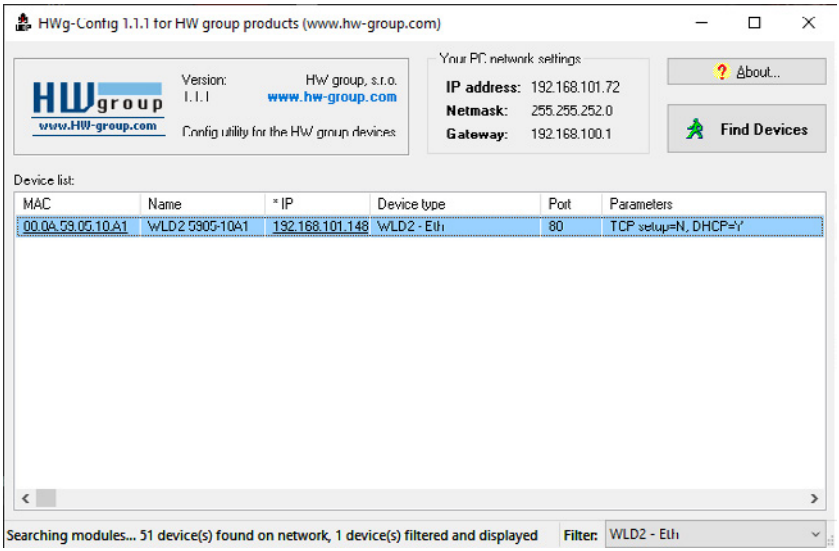
The decibel unit is non-dimensional and expresses the logarithm of a ratio of two values. In our case, it is the ratio of received output to an etalon of 1 mW:

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

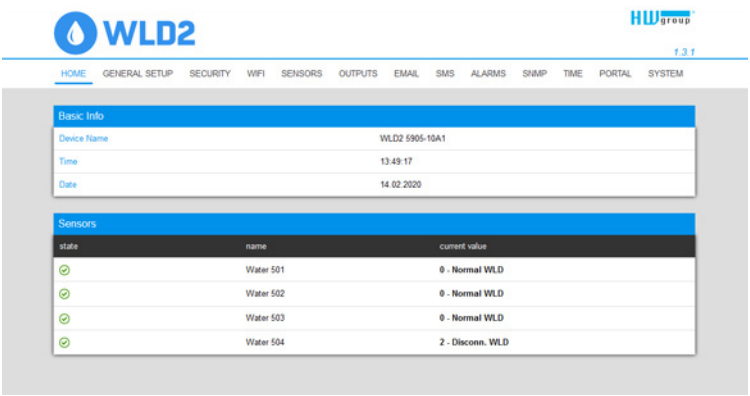
This means that if you have a signal of -54 dBm, it is higher (better) than a value of -82 dBm.

Connecting WLD2 to the SensDesk portal

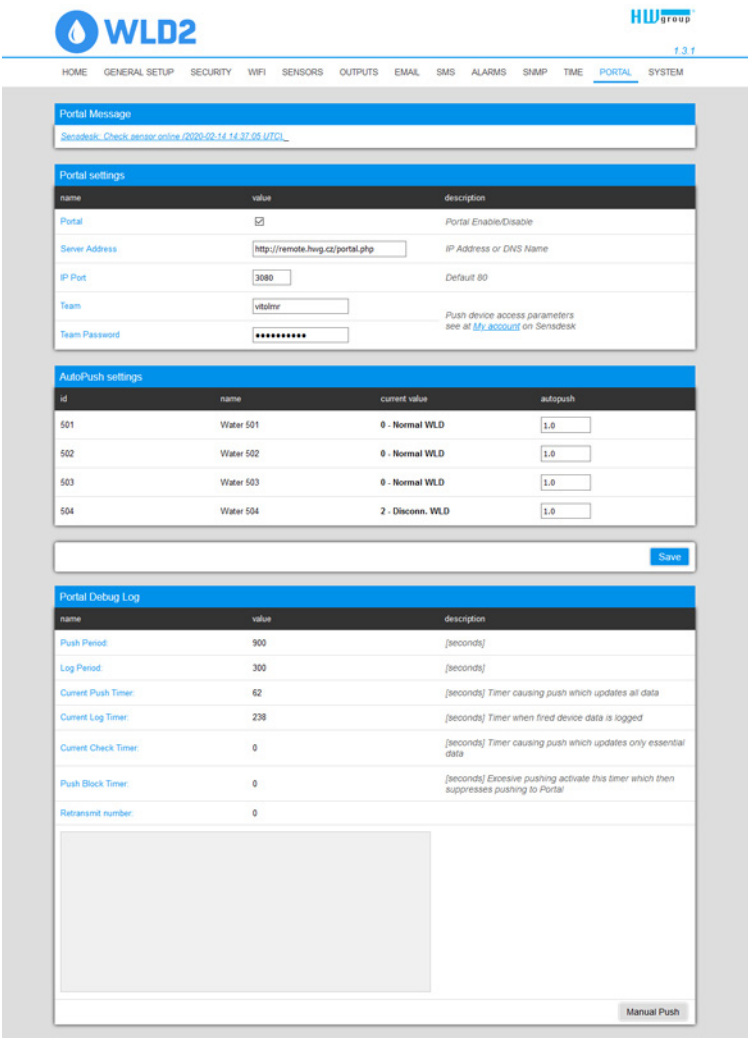
1 Connect the device to the computer network and set the network parameters (see the **First Steps** chapter).

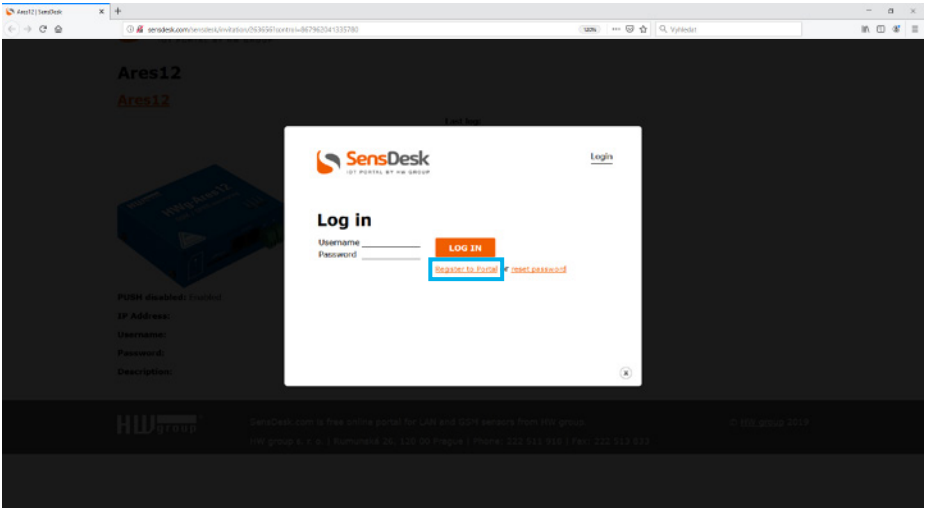


2 Check the device website:

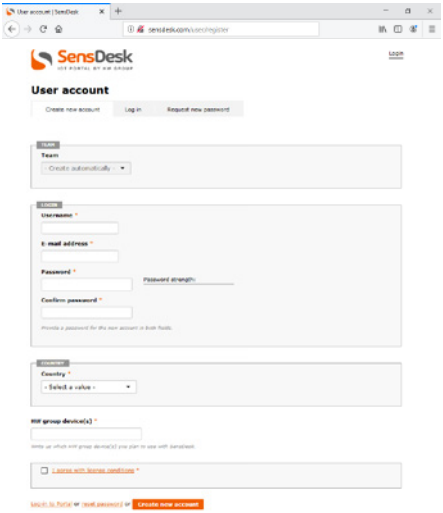


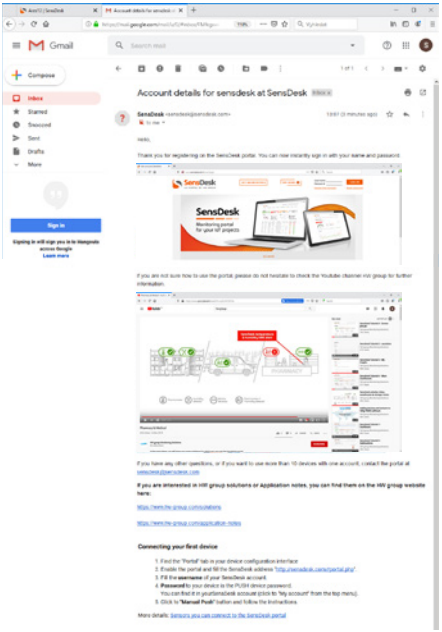
3 Tick the *Enable Portal* option and save the changes using the *Save* button in the bottom right corner of the window. Then click the *Manual Push* button in order to activate the portal function. Instead of "Portal disabled", a link *SensDesk.com: register your IP sensor* should appear in the *Portal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



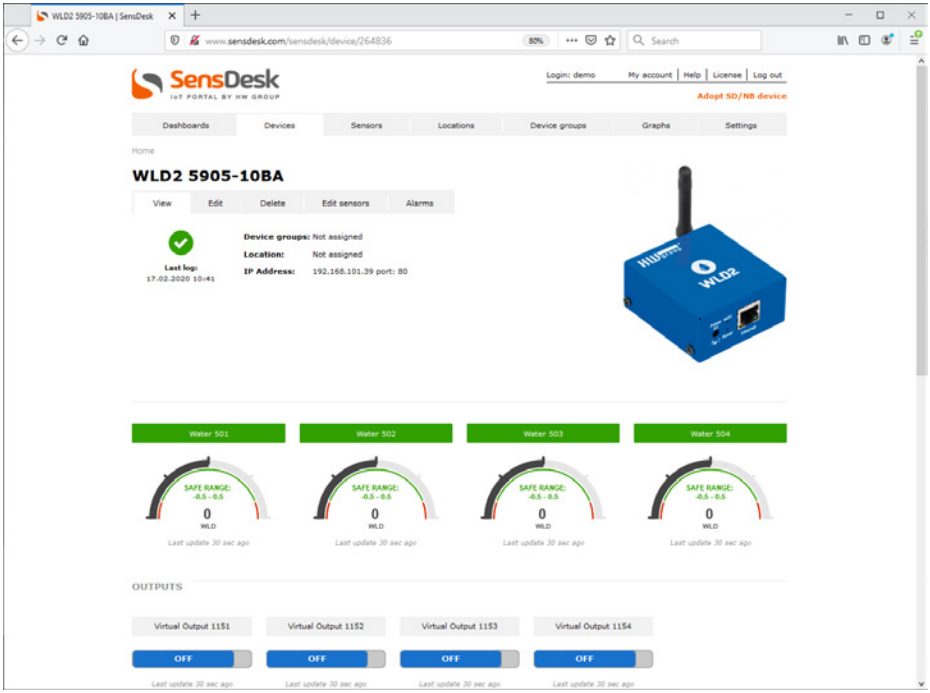


4 In case you already have a user account, please enter your login details and the device will be automatically assigned to your account. If you do not have a SensDesk account yet, click the *Register* and a registration form will be shown.

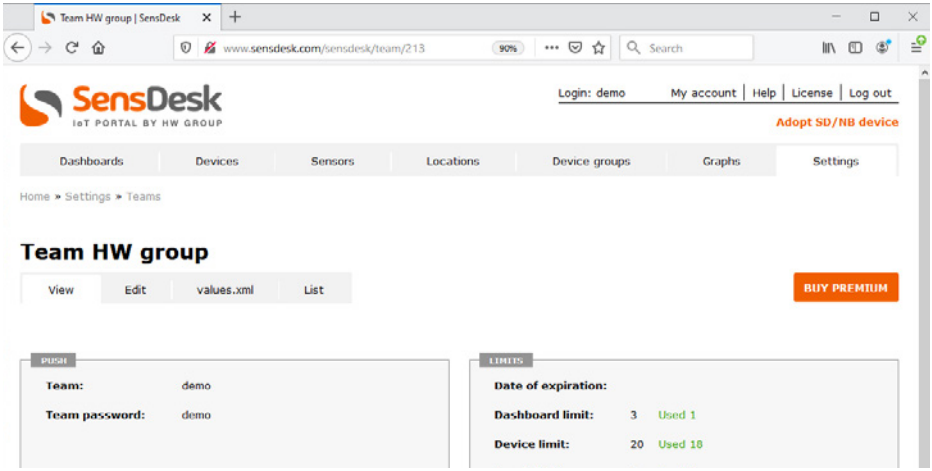




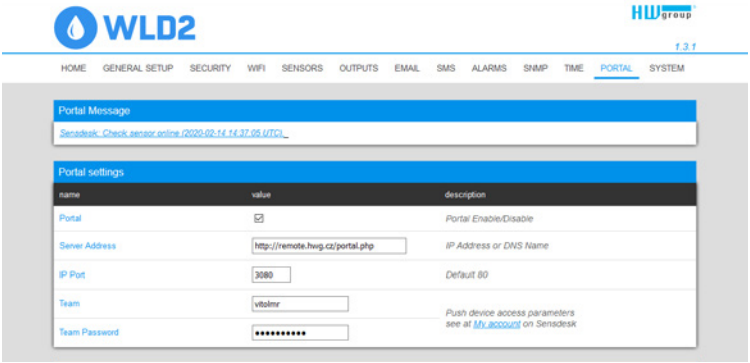
5 Enter the login details for your new account and a correct e-mail address. This e-mail address has to be unique for the server (cannot be already registered by another user).



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

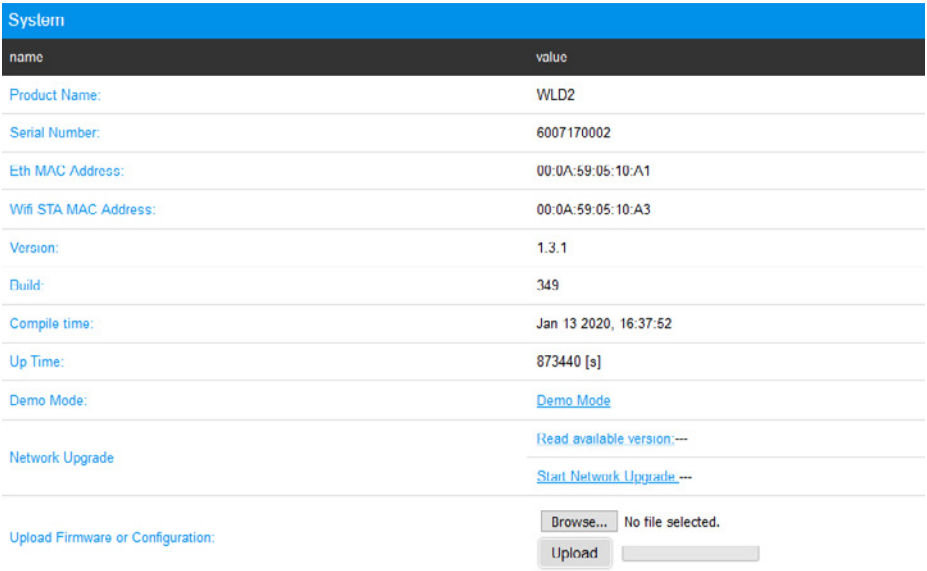
The **Username** and **PUSH Device** password can also be used in the application settings on mobile phones.

Firmware upgrade in WLD2 units

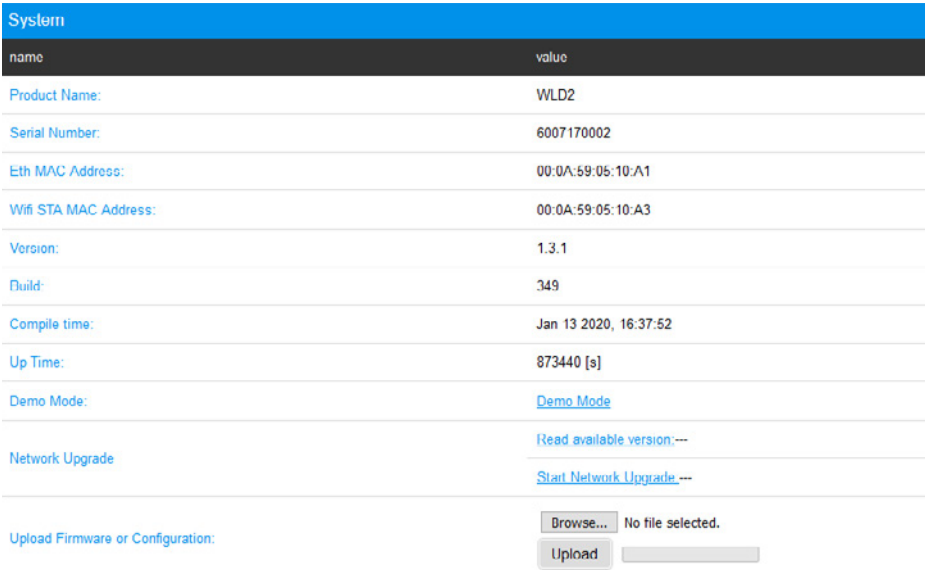
1 Open the device web interface in the *System* tab.

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

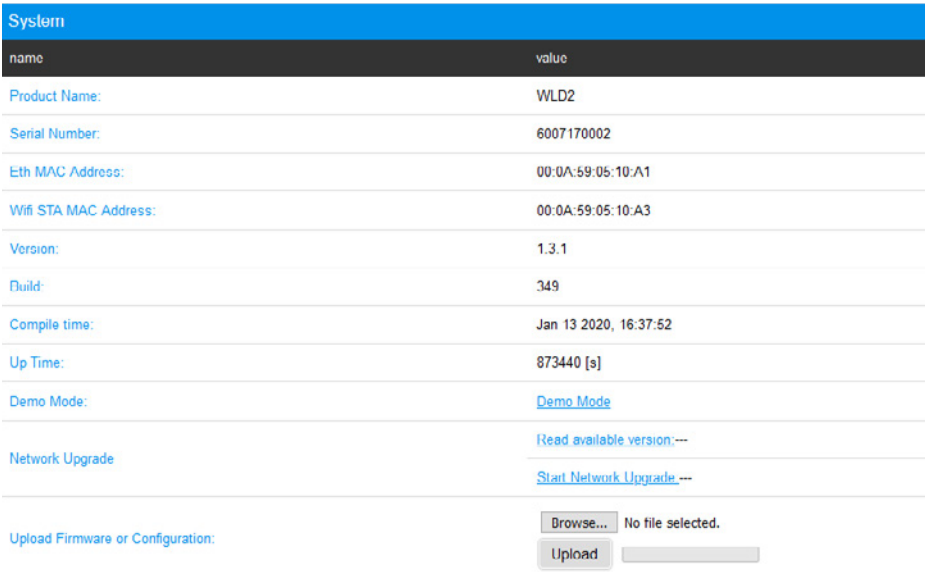
3 *Read available version* – serves to identify and display the current firmware version on the update server. Clock on the *Read available version* link.



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.

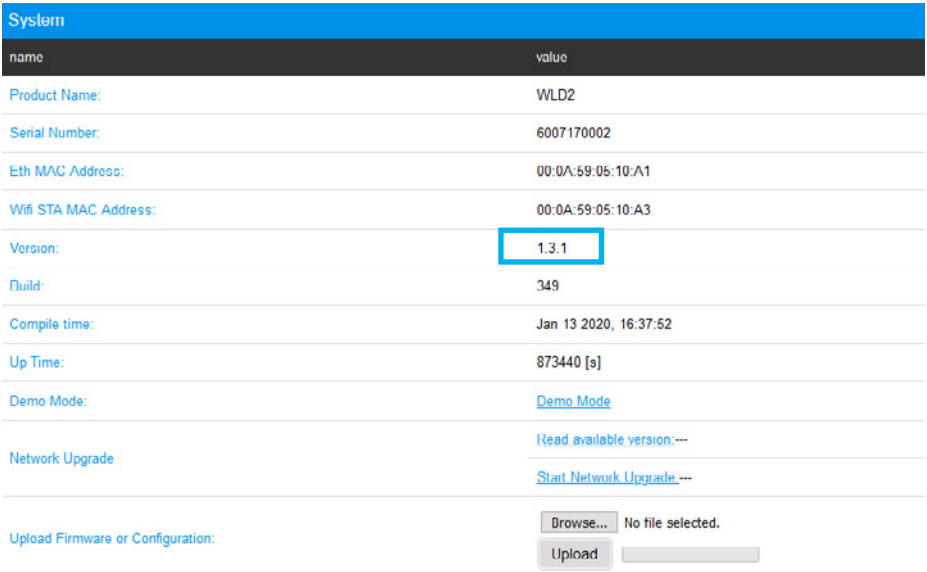


5 After the upgrade, the user is requested to restart the device manually.



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