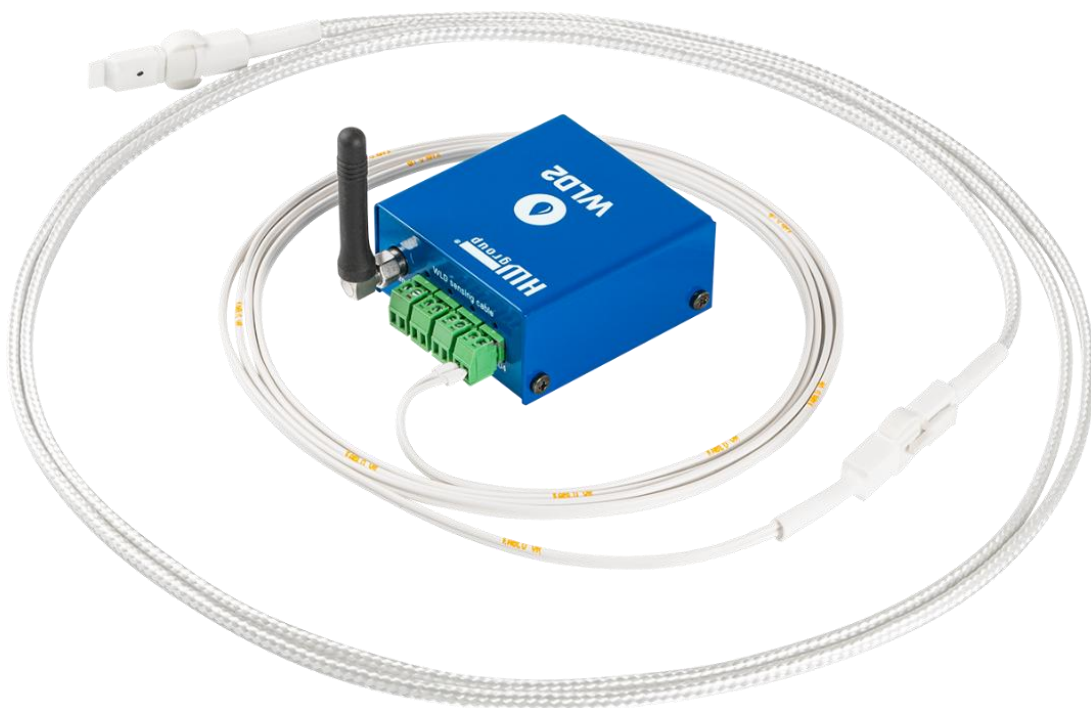




WLD2 – user manual

Safety warnings

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.

Improper use of the device may breach the safety protections provided by the manufacturer!

The power socket or point of disconnecting the device from power supply must be freely accessible! The device must not be used, particularly 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 repairs by unauthorized personnel.
- The power adapter or its supply cable are visible damaged.
- The manufacturer is only responsible for the device if it is being powered by an approved or supplied power source.

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

If you experience any difficulties with installing or starting up the device, please don't hesitate to reach out to our technical support team for assistance.

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 a precise model of your device (on the manufacturing label and the firmware version (see below), if you know it.

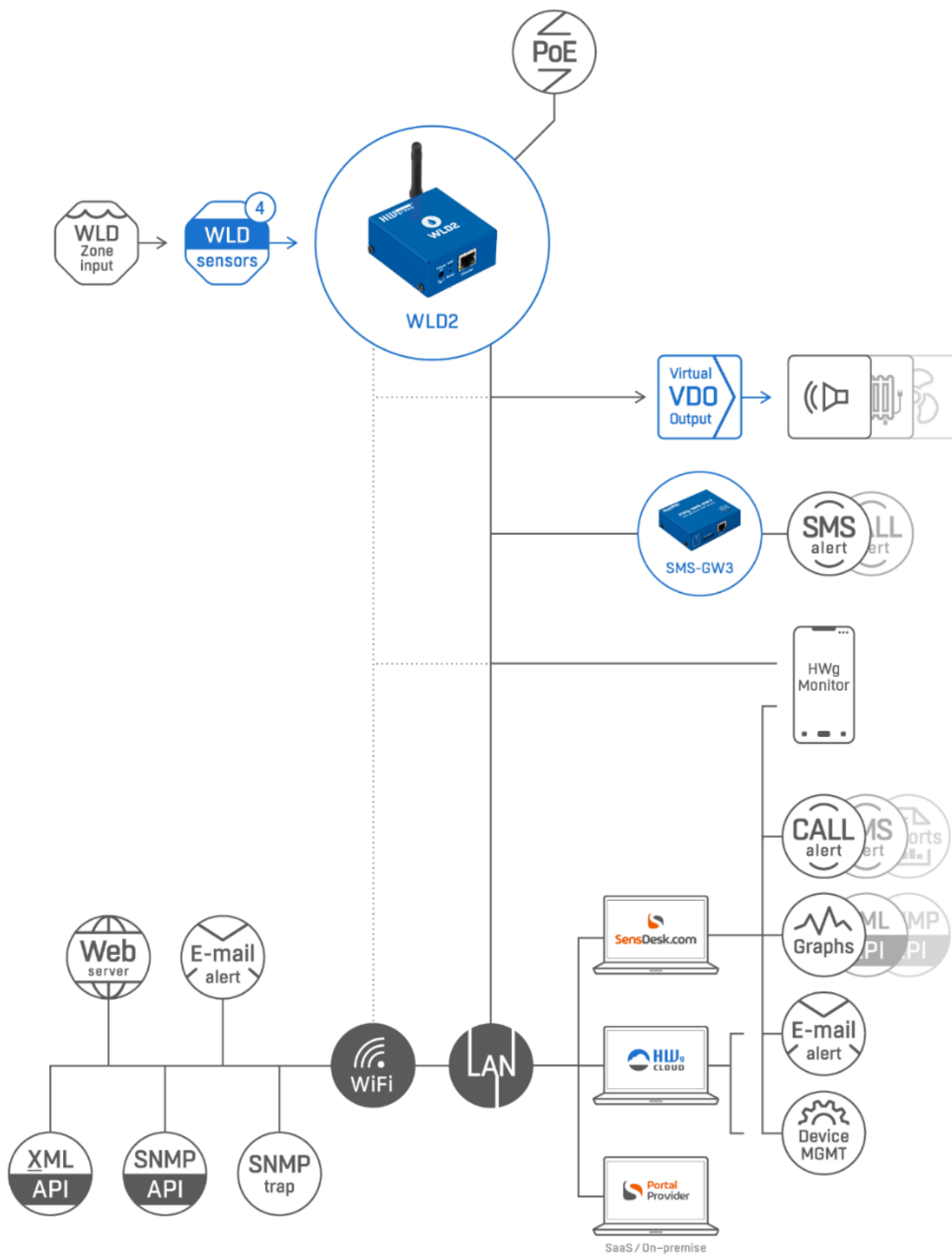
Table of Contents

WLD2 PRODUCT USAGE SCHEME.....	6
WLD2 FUNCTIONALITY	7
QUAD LEAK DETECTOR WITH WIFI AND ETHERNET	7
USAGE EXAMPLES.....	8
BASIC FEATURES.....	8
CONNECTORS AND INDICATORS	9
<i>Led Indicators</i>	9
<i>Reset Button</i>	9
<i>Connectors</i>	9
ZONES: WHAT THEY ARE AND HOW TO USE THEM.....	10
<i>What is a zone?</i>	10
<i>Creating and Extending Zones</i>	10
<i>Several water sensing segments in one Zone</i>	11
<i>Several Zones for independent Alerting</i>	11
TECHNICAL PARAMETERS	12
WIFI RADIO	13
WIFI SIGNAL STRENGTH	13
MECHANICAL DIMENSIONS OF WLD2 DEVICE.....	14
WLD SENSING CABLES	15
WLD SENSING CABLES TYPES.....	16
WLD SENSING CABLE OPTIONS	17
<i>WLD-Sensing cable A – 2 m / 10m / 50m</i>	17
<i>WLD-Sensing cable B – 2 m / 5m/ 10m / 50m</i>	17
<i>WLD-Connecting cable AB - 2 m</i>	17
<i>WLD-Extension cable AB - 5 m</i>	17
WLD2 FIRST STEPS	18
WLD SENSING CABLE CONNECTION (UP TO 4)	18
ETHERNET CONNECTIONS	18
SETTING OF THE IP ADDRESS - HWG-CONFIG	19
<i>Set device network parameters:</i>	20
<i>Note: The device provides two options for restoring the default settings:</i>	20
<i>Device built-in web server</i>	21
WLD2 DEVICE DISCOVERY (IPHONE / MAC).....	21
WWW INTERFACE.....	22
HOME TAB.....	22
<i>Base Information</i>	22
<i>Sensors</i>	22
GENERAL SETUP TAB	23
<i>General</i>	23
<i>Network</i>	23
<i>Device Admin</i>	24
SECURITY TAB	25
<i>HTTPS Server Certificate files</i>	25
<i>Generate the SSL key and certificate</i>	25
WIFI TAB	25
<i>WiFi modem state</i>	26
<i>Information</i>	26
<i>WiFi Setup</i>	27
<i>Network</i>	27
<i>WiFi Scan List</i>	27
<i>Connecting to find WiFi</i>	27

Scan API.....	28
SENSORS TAB	29
Sensors tab description:	30
OUTPUTS TAB	30
Virtual Output List.....	31
E-MAIL TAB.....	31
Sending alert via SMTP server	31
E-mail Settings	31
Email Test Log	32
SMS TAB	33
Remote SMS gateway.....	33
SMS Test Log.....	34
Set SMS messages from SMS-GW3 device.....	34
ALARMS TAB	37
Alarm Target.....	37
SNMP TAB.....	38
SNMP Settings	38
SNMP Access.....	38
SHOW OID KEYS TABLE	39
TIME TAB	40
SNTP Settings.....	40
Time Settings	40
SNTP Log.....	40
PORTAL TAB	41
Portal Message	41
Portal settings.....	41
AutoPush settings.....	42
What is AutoPush.....	42
Portal Debug Log.....	42
SYSTEM TAB	43
Download	43
System.....	43
Factory Default	44
System Restart	44
FIRMWARE UPGRADE FOR WLD2 UNITS.	45
REMOTE MONITORING ECOSYSTEM.....	46
CENTRAL SMS GATEWAY FOR ALERTING	46
THE PORTAL	46
www.SensDesk.com	47
www.HWg-cloud.com	47
Third-party Portals.....	47
WHY CONNECT WLD2 TO THE PORTAL?	48
HWG MONITOR: MOBILE APP FOR DISPLAYING CURRENT SENSOR VALUES.....	49
Specifics of selected SensDesk Technology portals	50
The HWg Monitor application can work with all portals from the SensDesk Technology family. However, not every portal has to support this application.	50
Support depends on whether the XML API is enabled on the portal. This feature can be enabled or disabled by the portal operator.	50
The HWg-cloud.com portal has this support disabled. XML API support is available only in the paid version of SensDesk.com. Portals operated by other providers may have different settings. Therefore, please contact your portal operator to confirm application support.	50
HOW TO CONNECT WLD2 TO THE HWG-CLOUD.COM PORTAL	51
WLD SYSTEM	53
THE MOST USABLE DEVICES WITH THE WLD SENSING CABLE	53
WLD DEVICE FAMILY OVERVIEW	54

WLD DEVICES FAMILY	54
<i>WLD Relay</i>	54
<i>NB-WLD</i>	54
<i>WLD2</i>	55
PERSEUS PLATFORM WITH A SINGLE WLD SENSING CABLE INPUT	55
<i>Perseus 150 and 155</i>	55
<i>Perseus 140 and 145</i>	55
<i>Perseus Energy 242</i>	55
<i>Perseus Energy 285</i>	55
WLD SYSTEM	56
WLD-SENSING CABLE A ACCESSORIES	57
WLD-SENSING CABLE B ACCESSORIES	57
MOUNTING ACCESSORIES	58
DIFFERENT WAYS TO SEND SMS ALERTS FROM THE WLD SYSTEM	59
HOW TO DESIGN WATER LEAK DETECTION SYSTEMS	60
DETECTION PRINCIPLE	60
INSTALLING THE WLD SENSING CABLE ON THE FLOOR	60
<i>Installation recommendations</i>	60
INSTALLING THE WLD SENSING CABLE ON PIPES	61
INSTALLING THE WLD SENSING CABLE ON STAIRS	61
INSTALLING THE WLD SENSING CABLE IN AN ELEVATOR SHAFT	61
WLD SYSTEM DESIGN RULES	62
<i>Zone design</i>	62
<i>WLD system Design Priorities</i>	63
<i>Alarm and Integration</i>	64

WLD2 product usage scheme



WLD2 functionality

Quad leak detector with WiFi and Ethernet

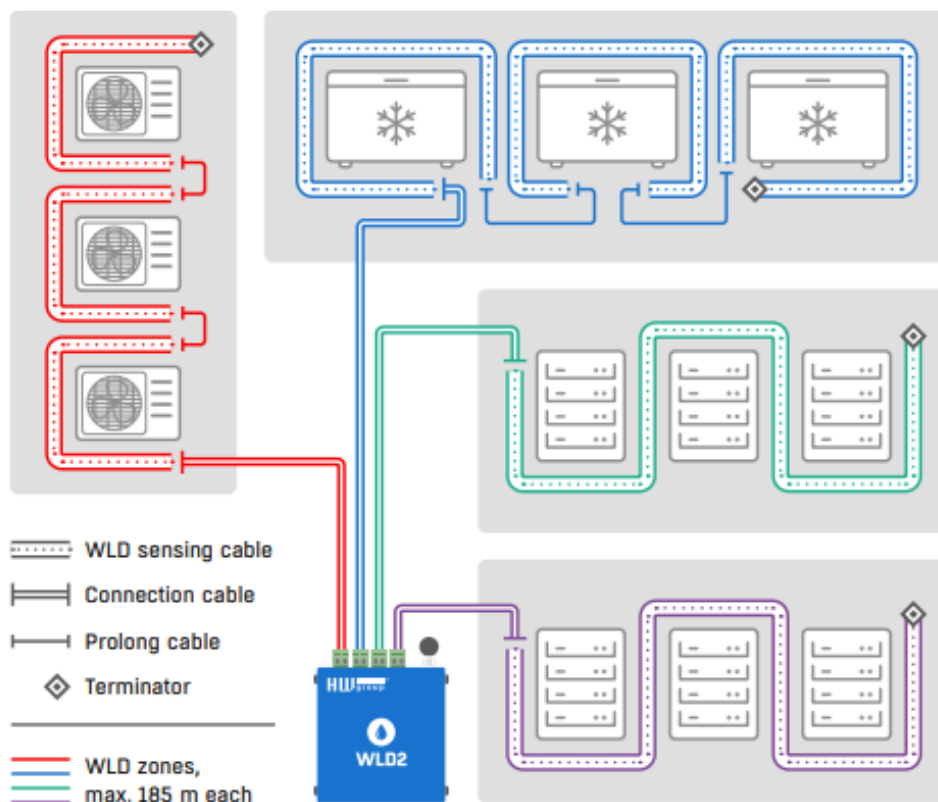
WLD2 is a LAN based WLD (Water Leak Detection) device with 4 external independent zones of WLD sensing cables. WLD2 can indicate water flooding along the entire length of WLD sensing cable for each zone. It is a standalone monitoring device with built-in web server, SNMP and email support (SMTP).

To detect even a few drops of liquids, it uses external WLD sensing cables Type A or B. With braided liquid-absorbing cables, it is possible to detect even condensation from A/C pipes or water leaks in general. It's sensitive to water, ethylene glycol or other conductive liquid. Disconnected or damaged WLD sensing cable is also detected for each zone.

With WiFi connectivity, WLD2 can be installed in hard-to-reach locations. In case of flooding, it can send an alert via email, SNMP trap, or SMS/Voice Call (using external SMS gateway device).

WLD2 can be connected to any SensDesk Technology based portal (HWg-Push protocol). WLD2 can be used as a standalone monitoring system thanks to SNMP and SNMP Trap support.

WLD2 can indicate water flooding 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 WLD sensing zone.



Usage examples

- Data centers with raised floors
- Server rooms and electrical closets
- Utility substations/ Telecom base stations
- Industrial/production facilities
- Storage rooms with various goods
- Wooden constructions
- Hotels
- Water heaters and boilers
- Ceilings and roofs
- HVAC systems
- Basements and crawl spaces
- Restrooms and bathrooms
- Laundry rooms
- Kitchen and break rooms
- Archives and libraries
- Showrooms and exhibitions

Basic features

- **4 independent WLD sensing zones** (up to 185 m each), each with separate alerts
- Connectivity: **LAN** (Ethernet with PoE) and **WiFi**
- **Built-in web server** for device configuration and status monitoring
- WLD2 zone signals state: **OK / Flooded / Sensing cable disconnected**.
- In a **standalone mode**, WLD2 can send flooding alerts via standard **e-mail** or **SNMP trap**.
- **SMS** and **Voice Calls** are available with an external device **SMS-GW** or external **Portal** (SensDesk Technology)
- Detected water **leaks along the entire length** of the WLD cable can activate a relay output on **remote (LAN) Perseus, Poseidon2** or Damocles2 units via LAN
- Powered over **PoE** or via an **external adapter**.
- Simple installation with **DHCP** auto-configuration.
- WLD2 can be easily mounted on a **wall** or in a **19" cabinet**.
- Wide range of accessories

Connectors and indicators

Led Indicators

Link – green LED indicates an active network connection.

Activity– yellow LED and flashing green 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 mode—either liquid is detected, or the cable is disconnected.

Reset Button

Pressing this button resets the device to factory defaults. Turn the device off. Press and hold the button. Turn the device on and hold the button for another 5 seconds. All LEDs light up in sequence. Turn the device on again, factory defaults are restored.

Connectors

Ethernet – for a wired internet connection in case of LAN operation, or for initial configuration in case of WiFi operation. It can be used to power the device via PoE (Power over Ethernet).

WLD1 – WLD4 – connecting to 4 WLD sensing cables.

Power – connector for a 5V power supply if the device is powered by an external adapter.



ZONES: What They Are and How to Use Them

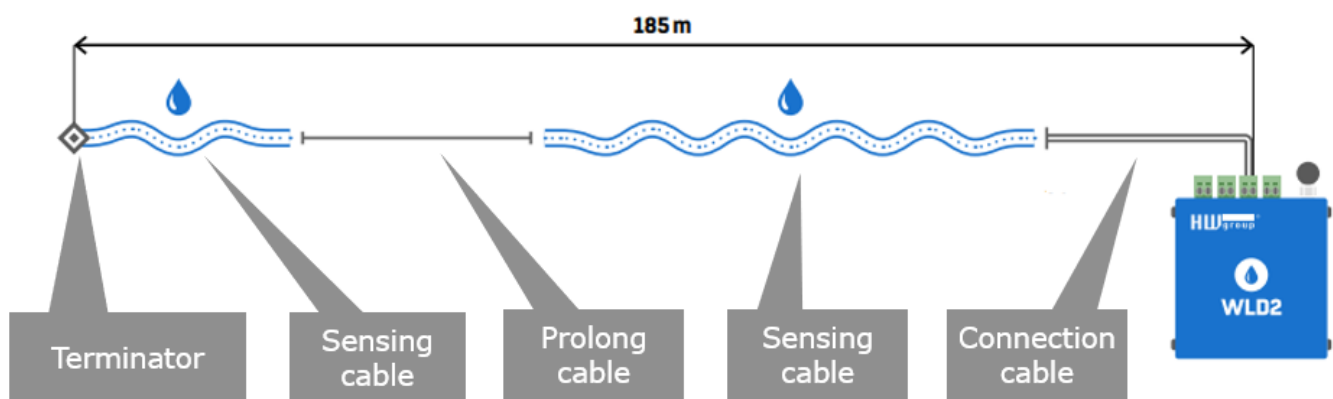
Water leak detection with the WLD2 depends on the connected sensing cable, which is an essential component of the whole product line.

Operation is not possible without connected external WLD Sensing cable.

What is a zone?

A zone is an independently monitored area composed of:

- WLD-Sensing cable A or B
- Connection cable
- Optional prolong cable (2m or 5m)
- With a terminator at the end



All cables are interconnected, starting with the connection cable, and are connected to a single input of the WLD2 device via the green terminal block.

Each zone operates as a distinct, monitored pathway for detecting the presence of water. WLD2 can support up to four zones, allowing separate areas of a facility to be monitored independently and simultaneously.

Creating and Extending Zones

You can mix and match sensing and prolong cables to create custom zones, providing long-range coverage with modular flexibility, optimizing the overall installation length. Each sensing zone can be extended up to 185 meters.

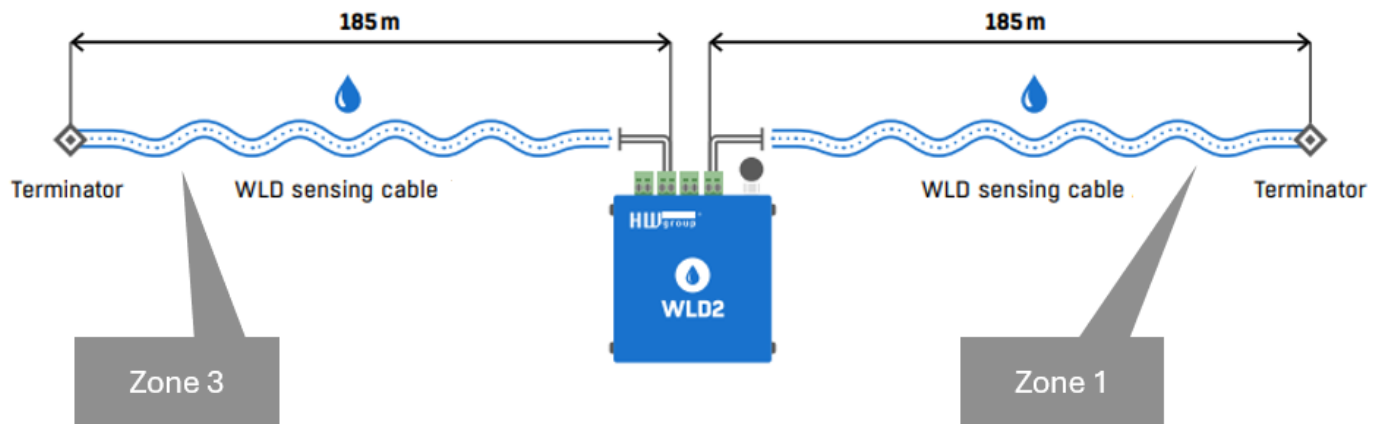
Plug-and-play setup simplifies the entire cable connection process, allowing the use of mixable cable lengths.

Several water sensing segments in one Zone

A cost-effective solution for monitoring long distances. Water is detected only in areas where leaks are likely to occur, while non-sensing (prolong) cable is used to bridge dry areas and extend the total length of the zone as needed.

Several Zones for independent Alerting

WLD2 supports up to 4 independent zones for each green terminal block input. Each detection zone can be configured to notify different responsible personnel. Multiple zones enable coverage of larger or segmented protected areas.



Technical parameters

Ethernet	
Interface	RJ45 (10/100BASE-T)
Supported protocols	SNMP, SNMP Trap, DHCP, HTTP, HTTPS, SMTP, SMTP TLS, XML
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 connector	SMA female
External sensors (WLD sensing cables)	
Number/Connectors	4 zones: WLD1, WLD2, WLD3, WLD4
Connector	Terminal block
Sensor states	0 = OK, 1 = Flooded, 2 = Cable damaged/disconnected
Sensing cable length	Each single area is max 185m (with non-sensing prolong cable included).
Cable extension	Sensing cable can be extended with a prolong cable, 185m in total per area.
Power supply	
Power voltage	5V / 250 mA
Connector	Jack Ø 3.5 × 1.35 / 10 [mm]
PoE	RJ45 - IEEE 802.3af Class 0
Other parameters	
Operating temperature	-30°C to 80°C / 0%RH ÷ 100%RH
Dimensions/weight	67 × 31 × 69 mm [WxHxD] / 151 g
EMC	
Elmag. radiation	CE / FCC Part 15, Class B
Elmag. compatibility	EN 55022, EN 55024, EN 61000
The device is designed to be used at a minimum distance of more than 20 cm respect to the user.	

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

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 milliwatt 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.

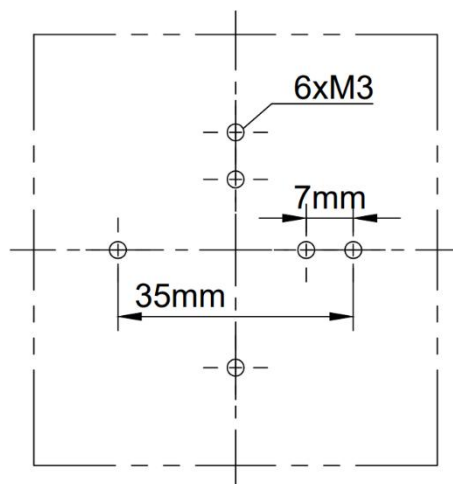
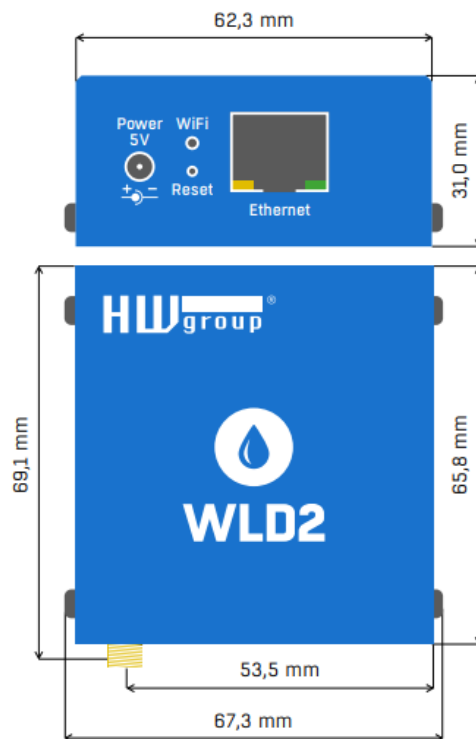
The decibel unit is non-dimensional and expresses the logarithm of a ratio of two values. In our case, it is the ratio of received output to an etalon of 1 mW:

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

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

Mechanical dimensions of WLD2 device.

The device is housed in a metal enclosure with options for various mounting methods, such as on a DIN rail, in a rack, or on a wall.



WLD sensing cables

The WLD2 device can detect water leakage only when connected to a sensing cable.

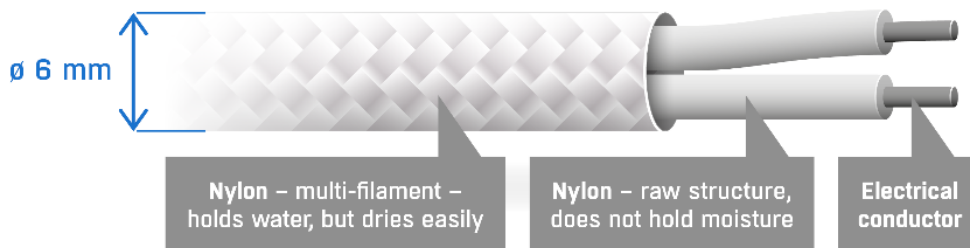
The WLD sensing cables is an integral part of the Water Leak Detection system. It provides easy installation and long-term reliability. Conductive liquids can be detected **along the entire length of the sensing cable**, and even a few drops of water are enough to trigger an alarm.

The WLD sensing cables from HW group is a unique solution with:

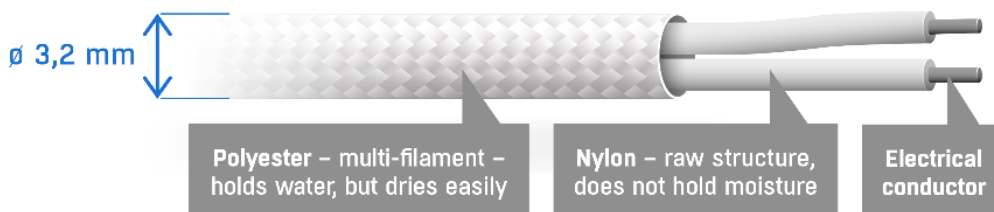
- No bend limit
- No grip limit
- No twist limit
- No reuse limit

Difference between WLD-Sensing cable A & B

WLD-Sensing cable A



WLD-Sensing cable B



WLD sensing cables types

	Type A	Type B
Sensing cable diameter (Ø)	6 mm	3,2 mm
Cable braiding material	Nylon multi-filament	Polyester multi-filament
Bending Angle limit	None	None
Sensing cable length options	2m / 10m / 50m	2m / 5m / 10m / 50m
Water Leak Detection	Entire length of the sensing cable	
WLD Zone max length	185m (with extension cable included)	
Zone states	0 =OK 1 =Flooded 2 =Cable disconnected	
Connector	2-pin (locking connector)	
Detection Media	Conductive liquid	
Reaction time	0.5 – 5 seconds	
Water Location (distance)	No	
Operating Environment	-10°C to 60 °C	
Cable to connect to device (terminator included)	WLD-Connecting cable AB 2m	
Extension (Non-sensing) cable	WLD-Extension cable AB 5m	

WLD Sensing cable options

WLD-Sensing cable A – 2 m / 10m / 50m



The WLD Sensing Cable Type A is a sensor cable used to detect the presence of any conductive liquid. The liquid is detected along the entire length of the WLD sensing cable, allowing an extended area to be monitored at once.

The cable can be routed under floors in data centres, along walls, or wrapped around pipes.

Even a very small amount of conductive liquid, such as water or ethylene glycol, can trigger an alarm. The sensing cable is an essential component of the WLD system.

WLD-Sensing cable B – 2 m / 5m/ 10m / 50m



The WLD Sensing Cable Type B is similar to Type A but has a smaller diameter. It also detects even a few drops of water along the entire length of the sensing cable, up to a maximum total length of 185 m.

In the event of water leakage or flooding, every minute counts. Early warning can help prevent significant damage and reduce costs. Long-term reliability of the entire system is essential.

WLD-Connecting cable AB - 2 m



The WLD Connecting Cable AB does not detect water. It is used to connect the WLD sensing cable to the WLD device.

The WLD Connecting Cable AB includes a green 2-pin terminal block, a 2 m cable, and a terminator.

WLD-Extension cable AB - 5 m



The WLD Extension Cable AB is a 5 m non-sensitive extension cable for the WLD system.

It is used to extend the WLD monitoring area, or zone, without adding sensing capability.

WLD2 first steps

WLD sensing cable connection (up to 4)

- Connect the connection cable to the green terminal block.
- Connect the sensing cable to the connection cable and add a terminator to the end.
- Or add a combination of prolong and sensing cables to the connection cable in any order, up to a total length of 185 meters with a terminator at the end.

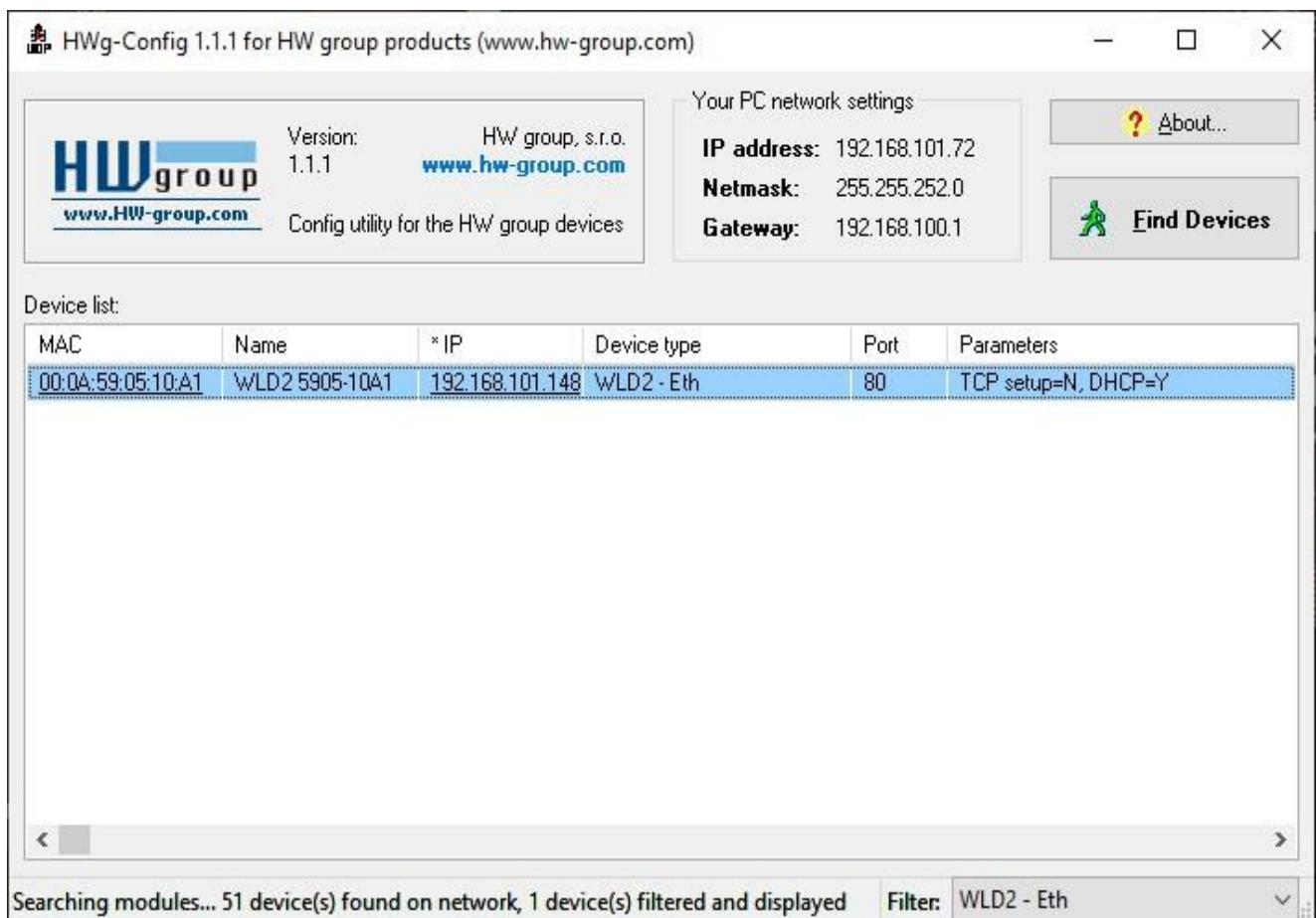
Ethernet connections

- 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 signalization).

Setting of the IP address - HWg-Config

The program can be downloaded at www.hw-group.com/software/hwg-config-udp-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 setting



Set device network parameters:

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

The screenshot shows a 'Details' configuration window with the following fields and controls:

- Name:** WLD2 5905-10A1
- IP address:** 192.168.101.14 (DHCP)
- Port:** 80
- Mask:** 255.255.252.0 (DHCP)
- Gateway:** 192.168.100.1 (DHCP)
- MAC:** 00:0A:59:05:10:A1
- FW version:** 1.3.1
- Device type:** WLD2 - Eth (89)
- DHCP:** Supported
- ☐ Enable IP access filter
- IP filter value:** 0.0.0.0
- IP filter mask:** 0.0.0.0
- Default values:** Load defaults
- ☒ Enable DHCP
- ☐ Enable NVT
- ☐ Enable TCP setup (with an 'Open' button)
- ☐ Enable TEA authentication
- ☒ Check if new IP address is empty
- Buttons:** Open in WEB Browser, Cancel, Apply changes

Save the settings by **Apply Changes**.

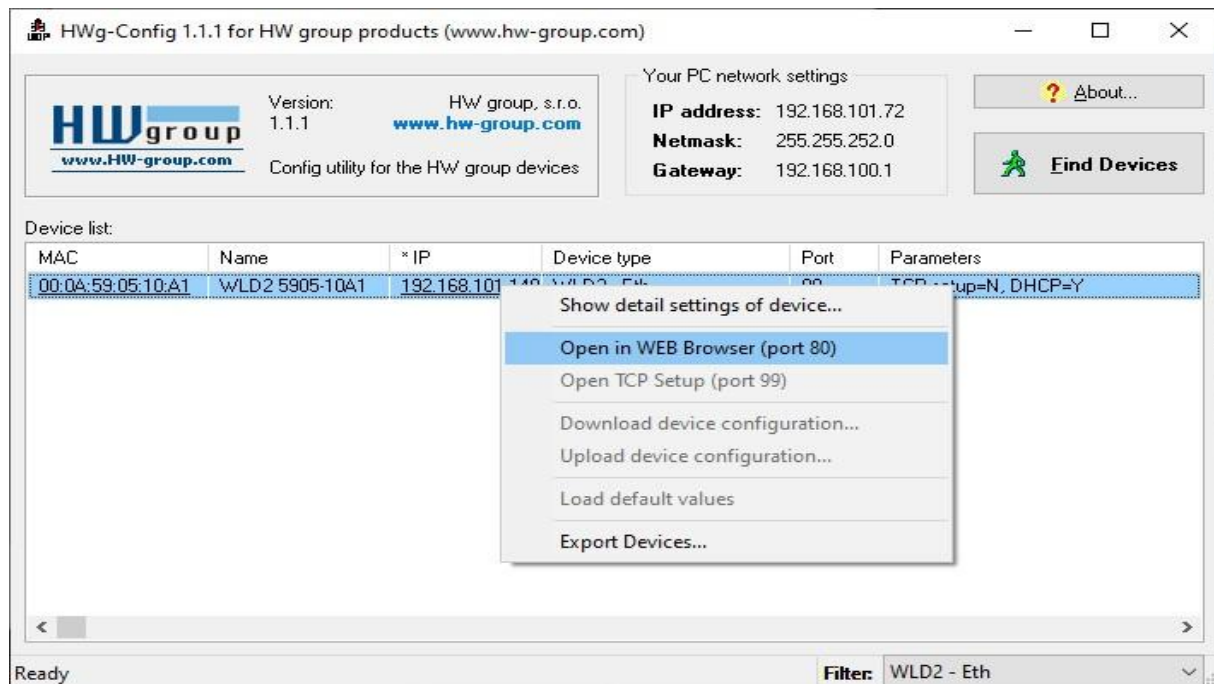
Note: The device provides two options for restoring the default settings:

- 1) **In HWg-Config**, right-click the device's MAC address and select Load default values.
Note: The default values can be restored from HWg-Config only during the first 60 seconds after the device is powered on.
- 2) Power off the device. Press and **hold the RESET button**, then connect the power adapter. Keep holding the button for at least 5 seconds, until all LEDs light up.

Device built-in web server

Options for opening device interface:

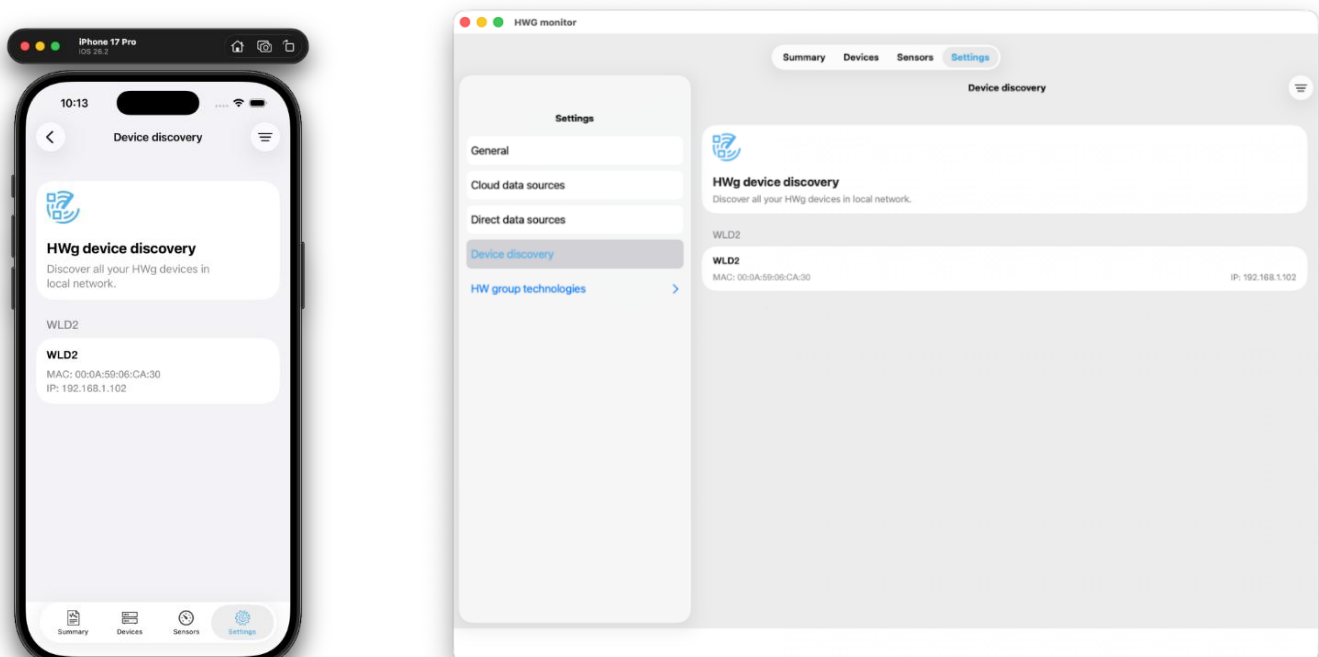
- Enter the device IP address in the browser window or click on the underlined IP address in the HWg-Config application.



WLD2 device discovery (iPhone / MAC)

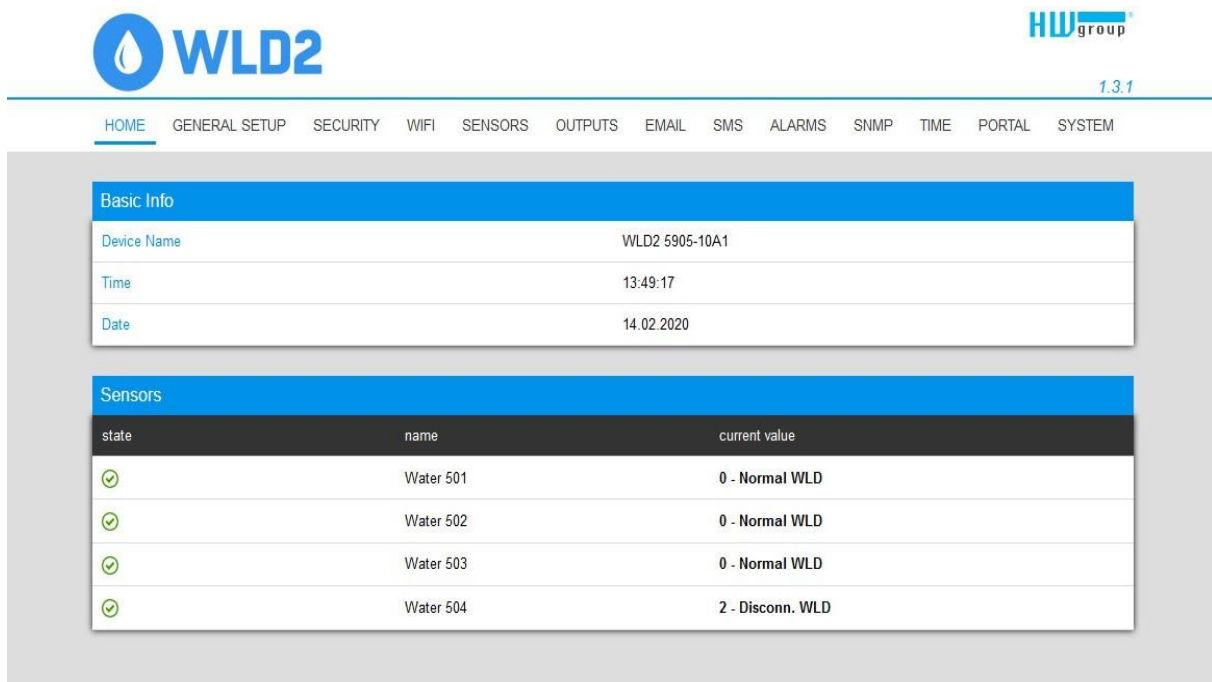
The HWg-Config is not available for iPhone or Mac computers.

On iOS, you can use the HWg Monitor mobile application, which includes the HWg Device Discovery feature. This feature automatically finds the WLD2 device on the local network.



WWW interface

Home tab



Basic Info		
Device Name	WLD2 5905-10A1	
Time	13:49:17	
Date	14.02.2020	

Sensors		
state	name	current value
✓	Water 501	0 - Normal WLD
✓	Water 502	0 - Normal WLD
✓	Water 503	0 - Normal WLD
✓	Water 504	2 - Disconn. WLD

Base Information

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

1.3.1

HOMEGENERAL SETUPSECURITYWIFISENSORSOUTPUTSEMAILSMSEMAILSMSALARMSNMPTIMEPORTALSYSTEM

General

name	value	description
Device Name	WLD2 5905-10A1	0 to 32 characters
WWW Info Text:	WLD2: For more information try http://www.hw-group.com	
WWW Update period:	1	[s] Automatic update period in seconds. 0=> disabled
Periodic restart	Off	Periodic restart time
Periodic status	0	[H] Status info period in hours. 0=> disabled
Periodic status target	None	

Network

name	value	description
DHCP	☒	DHCP Enable/Disable
IP Address	192.168.101.148	A.B.C.D
Network Mask	255.255.252.0	A.B.C.D
Gateway	192.168.100.1	A.B.C.D
DNS Primary	192.168.100.237	A.B.C.D
DNS Secondary	192.168.100.28	A.B.C.D
HTTP Port	80	Default 80
HTTPS Port	443	Default 443. See https settings at Security page

Device Admin

name	value	description
Username		Admin username/password for device configuration changes [0 to 16 characters]
Password		

Save

General

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

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.

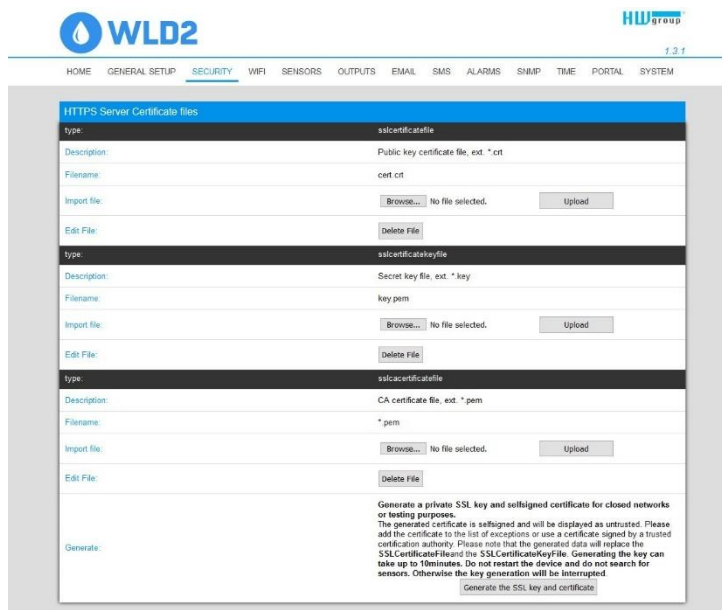
HTTP Port – port number on which the built-in WWW server tunes in. A change of port number is suitable e.g. for multiple devices accessible from the external network via a router. Consult the network administrator about potential changes. The default port is 80. You can turn off HTTP support by setting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

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

Security tab



The screenshot shows the WLD2 web interface with the 'SECURITY' tab selected. Under the 'HTTPS Server Certificate files' section, there are three entries for managing certificates:

- sslcertificatefile**: Public key certificate file, ext. *.cer. Filename: cert.cer. Includes 'Import file' (Browse...), 'Delete File', and 'Upload' buttons.
- sslcertificatekeyfile**: Secret key file, ext. *.key. Filename: key.pem. Includes 'Import file' (Browse...), 'Delete File', and 'Upload' buttons.
- sslcertificatefile**: CA certificate file, ext. *.pem. Filename: *.pem. Includes 'Import file' (Browse...), 'Delete File', and 'Upload' buttons.

At the bottom, there is a 'Generate' button and a detailed instruction: 'Generate a private SSL key and selfsigned certificate for closed networks or testing purposes. The generated certificate is selfsigned 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.' A 'Generate the SSL key and certificate' button is also present.

HTTPS Server Certificate files

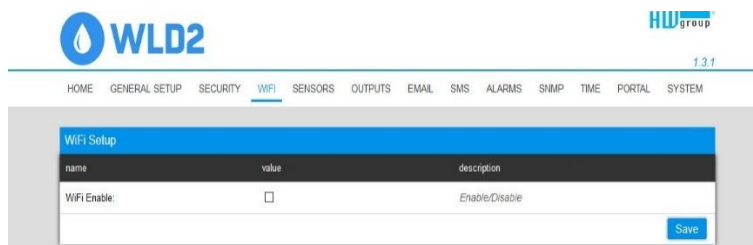
Used to manage certificates needed for the HTTPS server. Allows you to upload or delete a public key, a private key, or a certificate of the certificate authority (CA) that has issued the public key certificate.

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:



The screenshot shows the WLD2 web interface with the 'WiFi' tab selected. The 'WiFi Setup' section contains a table with the following data:

name	value	description
WiFi Enable	☐	Enable/Disable

A 'Save' button is located at the bottom right of the table.

All the options are available after enabling:

The screenshot displays the WLD2 web interface with the 'WIFI' tab selected. The interface is divided into three main sections: 'WiFi Info', 'WiFi Setup', and 'Network'. The 'WiFi Info' section shows the current state as 'Connecting', with fields for SSID, BSSID, RSSI, Signal Quality (0%), and Channel (0). The 'WiFi Setup' section contains fields for enabling WiFi, setting the SSID, password, and BSSID. The 'Network' section includes fields for enabling DHCP, setting IP address, network mask, gateway, and DNS servers. A 'WiFi Scan List' table is at the bottom, with columns for ssid, bssid, channel, security, and signal, and a 'Scan AP' button.

name	value	description
WiFi Enable	☒	Enable/Disable
SSID		string, AP's SSID
Password	Show	string, MAX: 64 bytes ASCII
BSSID		string, AP's MAC address, for several APs may have the same SSID

name	value	description
DHCP	☒	DHCP Enable/Disable
IP Address	192.168.1.91	A.B.C.D
Network Mask	255.255.255.0	A.B.C.D
Gateway	192.168.1.1	A.B.C.D
DNS Primary	192.168.1.1	A.B.C.D
DNS Secondary	0.0.0.0	A.B.C.D

ssid	bssid	channel	security	signal
------	-------	---------	----------	--------

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

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

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

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 find WiFi

Click on the SSID of the found network to prefill WiFi setting and just enter the Password. The BSSID remains empty. Standard setting. Reconnect 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 API

Network Mask

255.255.255.0

A.B.C.D

Gateway

192.168.1.1

A.B.C.D

DNS Primary

192.168.1.1

A.B.C.D

DNS Secondary

0.0.0.0

A.B.C.D

Save

WiFi Scan List

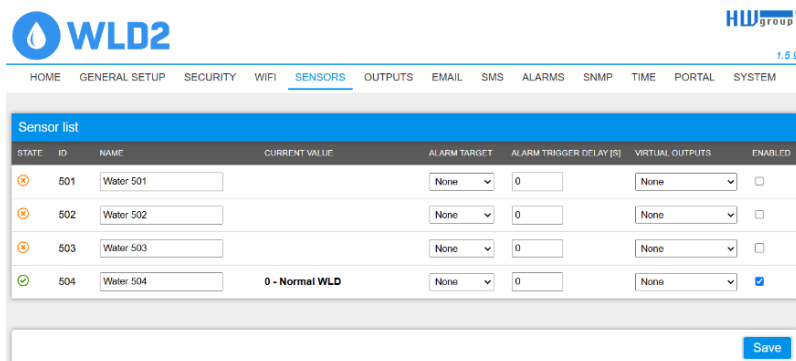
ssid	bssid	channel	security	signal
	FE:EC:DA:3E:ED:55	1	WPA2 PSK	94%
Poseidon	FC:EC:DA:3B:ED:55	1	WPA2 PSK	92%
	06:18:06:A9:28:EE	6	WPA2 PSK	88%
Poseidon	04:18:06:A9:28:EE	6	WPA2 PSK	86%
Poseidon	FC:EC:DA:3E:39:E8	1	WPA2 PSK	84%
	FE:EC:DA:3E:39:E8	1	WPA2 PSK	84%
Testona	00:04:56:A0:94:D0	11	WPA2 PSK	82%
	82:2A:A8:2D:2A:8B	6	WPA2 PSK	78%
	FE:EC:DA:3E:38:12	11	WPA2 PSK	76%
Poseidon	FC:EC:DA:3E:38:12	11	WPA2 PSK	76%

Scan AP

Sensors tab

If you are not using all 4 WLD inputs, you need to uncheck the unused ones from the interface to prevent them from reporting a disconnected status from the start.

One WLD sensing cable:

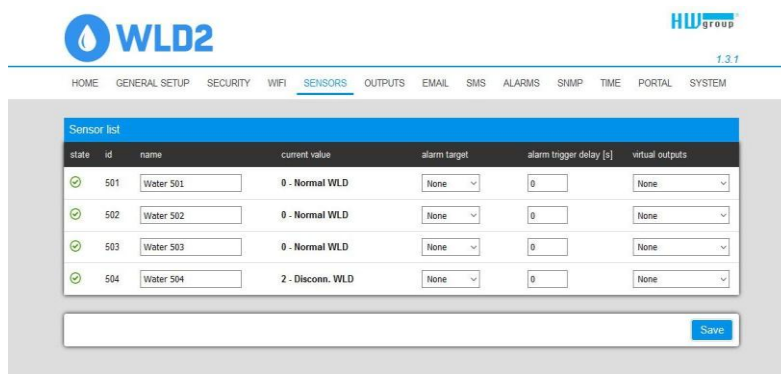


The screenshot shows the WLD2 web interface with the 'SENSORS' tab selected. The 'Sensor list' table has the following data:

STATE	ID	NAME	CURRENT VALUE	ALARM TARGET	ALARM TRIGGER DELAY [s]	VIRTUAL OUTPUTS	ENABLED
⚠	501	Water 501		None	0	None	☐
⚠	502	Water 502		None	0	None	☐
⚠	503	Water 503		None	0	None	☐
✅	504	Water 504	0 - Normal WLD	None	0	None	☒

A 'Save' button is located at the bottom right of the table.

Four WLD sensing cables:

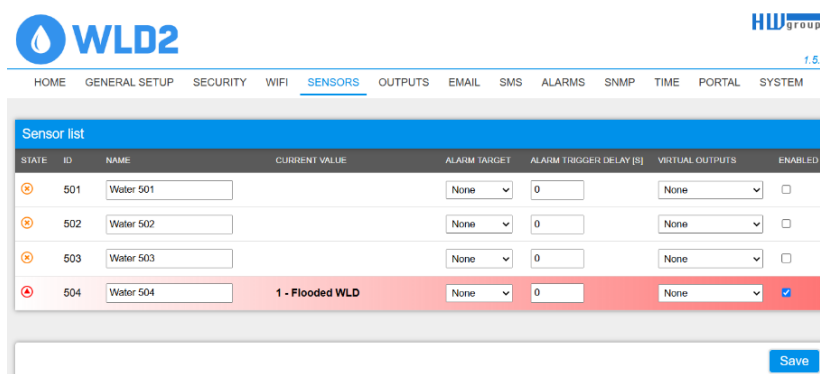


The screenshot shows the WLD2 web interface with the 'SENSORS' tab selected. The 'Sensor list' table has the following data:

state	id	name	current value	alarm target	alarm trigger delay [s]	virtual outputs
✅	501	Water 501	0 - Normal WLD	None	0	None
✅	502	Water 502	0 - Normal WLD	None	0	None
✅	503	Water 503	0 - Normal WLD	None	0	None
✅	504	Water 504	2 - Disconn. WLD	None	0	None

A 'Save' button is located at the bottom right of the table.

One flooded WLD sensing cables:



The screenshot shows the WLD2 web interface with the 'SENSORS' tab selected. The 'Sensor list' table has the following data:

STATE	ID	NAME	CURRENT VALUE	ALARM TARGET	ALARM TRIGGER DELAY [s]	VIRTUAL OUTPUTS	ENABLED
⚠	501	Water 501		None	0	None	☐
⚠	502	Water 502		None	0	None	☐
⚠	503	Water 503		None	0	None	☐
🔴	504	Water 504	1 - Flooded WLD	None	0	None	☒

A 'Save' button is located at the bottom right of the table.

Sensors tab description:

State – sensor state is signaled for each WLD zone independently.

✓ **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

Current Value – current value including unit of measure.

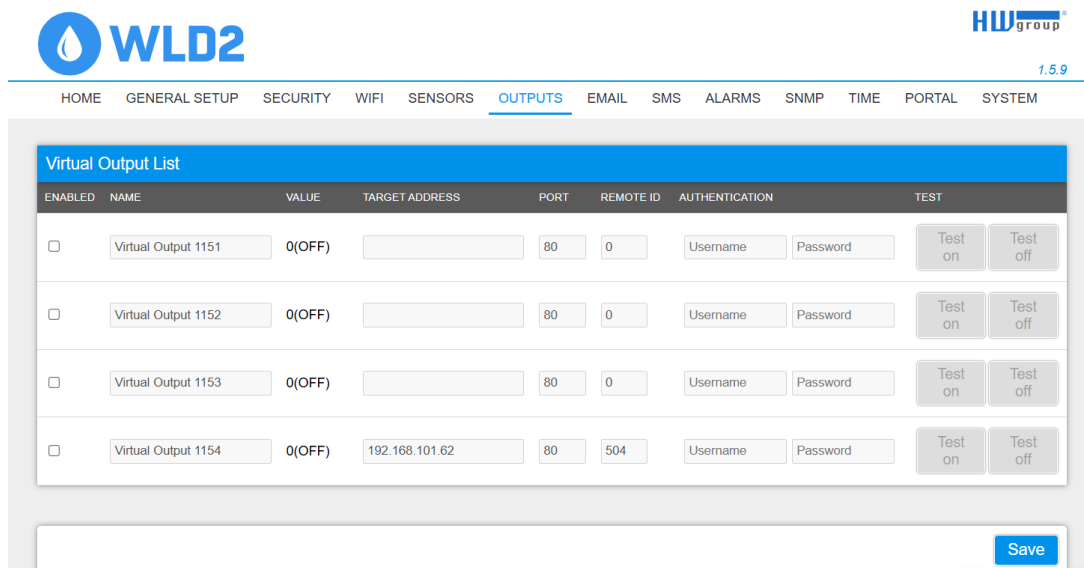
Alarm Target – specifies the targets for alarm alerts (SMS + E-mail). Target recipients are defined at the Alarms tab. The drop-down menu allows selecting an existing set of targets or creating a new one.

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.

Outputs tab

Defines the parameters of up to 4 remote outputs, usually relays (on Damocles2 or Poseidon2 units).



The screenshot shows the WLD2 web interface with the 'OUTPUTS' tab selected. The 'Virtual Output List' table contains four rows of configuration for virtual outputs 1151 through 1154. Each row includes checkboxes for enabling the output, input fields for name, value, target address, port, and remote ID, authentication fields for username and password, and buttons to test the output on or off. A 'Save' button is located at the bottom right of the configuration area.

ENABLED	NAME	VALUE	TARGET ADDRESS	PORT	REMOTE ID	AUTHENTICATION	TEST
☐	Virtual Output 1151	0(OFF)		80	0	Username Password	Test on Test off
☐	Virtual Output 1152	0(OFF)		80	0	Username Password	Test on Test off
☐	Virtual Output 1153	0(OFF)		80	0	Username Password	Test on Test off
☐	Virtual Output 1154	0(OFF)	192.168.101.62	80	504	Username Password	Test on Test off

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 and Test off – for testing the settings.

E-mail tab

Sending alert via SMTP server

Note that [SMTP server reliability is not guaranteed in the long term](#) due to potential outages, blacklisting, or configuration changes. For long-term reliable solutions of email alerts, SMS and phone calls, the SensDesk technology portal is recommended. If you want to receive email alarms, you need to add your email to the ALARMS tab, and they will then start arriving.

The screenshot shows the WLD2 web interface with the 'EMAIL' tab selected. The 'Email Settings' section contains a table with the following fields:

name	value	description
SMTP Server	some.smtp.server	IP Address or DNS Name
SMTP Port	25	Default 25
Authentication	☐	Enable/Disable
Secure TLS mode	☐	Enable/Disable
Use HTML formatting	☐	Uses html to format email message body
Username		0 to 32 characters
Password		0 to 32 characters
Importance	Normal	Email importance flag
FROM	user@domain.com	Device email address
Subject	subject	Beginning of email subject

A 'Save' button is located at the bottom right of the 'Email Settings' section.

The 'Email Test Log' section below it contains an 'Email address' field with the value 'recipient@domain.com' and a 'Test Email' button. There is also a 'Debug log window' area.

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.

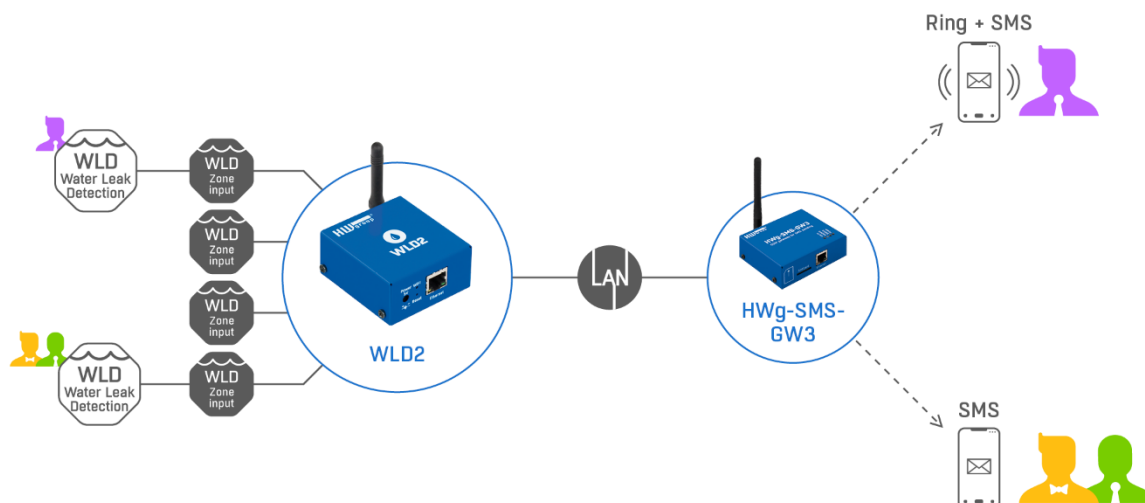
Email Test Log

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 communication with the SMTP server.

For reliable long-term email alerts, SMS, and phone call notifications, we reiterate that the SensDesk Technology portal is the recommended solution.

SMS tab

Remote SMS gateway



SMS alert and phone calls can be sent via an external device SMS-GW3 (GSM/LTE) gateway. It is a central gateway that allows HWg devices to send SMS and make voice calls alerts.

The screenshot shows the 'SMS' tab configuration interface for the WLD2 device. The interface includes a navigation bar at the top with links: HOME, GENERAL SETUP, SECURITY, WIFI, SENSORS, OUTPUTS, EMAIL, SMS, ALARMS, SNMP, TIME, PORTAL, SYSTEM. The 'SMS' tab is selected. The main configuration area is titled 'Remote SMS gateway' and contains the following fields:

name	value	description
Enable	☐	Enable/Disable
SMS Gateway Address		IP Address or DNS Name
Port	80	Default 80
Username		
Password		

Below the configuration fields is a 'Save' button. Underneath is the 'SMS Test Log' section, which includes a 'Phone number' field with a dropdown menu showing '+420603090000' and a 'Phone number for testing' field. Below these fields is a large grey area labeled 'Display log window'. At the bottom right of the log window are 'Test SMS' and 'Test Call' buttons.

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 – username 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

Set SMS messages from SMS-GW3 device

- In the Alarms tab, set the alarm reminder period and enter phone numbers in the SMS list. Select the CALL checkbox for calls. Then press the SAVE button.

WLD2 HWgroup 1.3.9

HOME GENERAL SETUP SECURITY WIFI SENSORS OUTPUTS EMAIL SMS **ALARMS** SNMP TIME PORTAL SYSTEM

Alarms Settings

NAME	VALUE	DESCRIPTION
Alarms reminder period	1	[Min] If any alarm lasts longer than this interval, the alarm message will be resend to specified target. Every X minutes.
Alarm reminder target	Default 1	

Default 1 +

Alarm Target: Default 1 DELETE

EMAIL ADDRESS

example@hwg.cz

Email list

example@hwg.cz

example@hwg.cz

example@hwg.cz

example@hwg.cz

PHONE NUMBER CALL

+123456789123 ☐

SMS list

+429603603603 ☐

+429603603603 ☐

+429603603603 ☐

+429603603603 ☐

- Copy an IP address of the SMS-GW3 from its web interface.

Eva HWg-SMS-GW3 GENERAL SETUP

Base

Device Name: Eva HWg-SMS-GW3 0 to 16 characters

WWW Info Text: HWg-SMS-GW3: For more information try www.hw-group.com

Network Setup

DHCP ☒ DHCP Enable/Disable

IP Address: 192.168.103.85 A.B.C.D

Network Mask: 255.255.252.0 A.B.C.D

Gateway: 192.168.100.1 A.B.C.D

DNS Primary: 192.168.100.237 A.B.C.D

DNS Secondary: 192.168.100.28 A.B.C.D

HTTP Port: 80 Default 80

WWW Security:

Username: Password: Username and password for device configuration [0 to 16 characters]

NetGSM (SOAP) security:

Username: Password: Username and password for NetGSM (SOAP) protocol - SMS and ringout sending

- Then enter it into the SMS Gateway Address field in the SMS tab of the WLD2 web interface, then click the Save button.

WLD2 1.5.9

HOME GENERAL SETUP SECURITY WIFI SENSORS OUTPUTS EMAIL **SMS** ALARMS SNMP TIME PORTAL SYSTEM

Remote SMS gateway

NAME	VALUE	DESCRIPTION
Enable	☒	Enable/Disable
SMS Gateway Address	192.168.103.85	IP Address or DNS Name
Port	80	Default 80
Username		
Password		

Save

- Fill in SIM Card Pin, Tel Number, Text and press Apply Changes in GSM-Modem tab of SMS-GW3 web interface. Then press Restart button.

SMS GW3

Home SMS Queue General Setup Time

GSM Modem

SNMP System

Version: 1.3.5

Apply Changes

GSM MODEM

Please Restart **Restart**

Information

Network Registration:	Unknown
Signal Quality:	Not known or not detectable
Operator Name:	
SMS Service Center Address:	
Number of SMS:	0
Number of failures SMS:	0
Number of Ringout:	0
Number of failures Ringout:	0

Clear counters

Configuration

SIM card PIN Status:	Please enter a valid PIN	PIN managemant
SIM Card Pin:	1234	PIN number [4 to 8 characters]
Roaming Enable:	☒	Allow users to send SMS even when home network is not available
SMS http GET Enable:	☐	Enable http GET API
Manual Network:	☐	Manual Set Network enable/disable

Test SMS

Tel Number:	+123456789123	Send SMS Test
Text:	Test text	Ringout Test

- In SMS tab of WLD2 web interface set phone number and try to test it by pressing Test SMS button.

The screenshot shows the WLD2 web interface. At the top, there is a navigation bar with the WLD2 logo and the HW group logo. The 'SMS' tab is highlighted in the navigation bar. Below the navigation bar, there is a 'Remote SMS gateway' section with a table of configuration parameters:

NAME	VALUE	DESCRIPTION
Enable	☒	Enable/Disable
SMS Gateway Address	192.168.103.85	IP Address or DNS Name
Port	80	Default 80
Username		
Password		

Below the configuration table is a 'Save' button. Underneath is the 'SMS Test Log' section. It contains a 'Phone number' field with the value '+123456789123' and a 'Phone number for testing' label. Below this is a 'Debug log window' showing the following text:

```
Phone Number: +123456789123
SMS Message:
<?xml version="1.0" encoding="utf-8"><soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:pos="poselidonService.xsd"><soapenv:Header/><soapenv:Body><pos:QueueAdd>
<Queue>GsmOut</Queue><Gsm><Cmd>SMS</Cmd><Nm>+123456789123</Nm><Text>EVA WLD2 5906-
7288: TEST. This is a test message.</Text></Gsm></pos:QueueAdd></soapenv:Body>
</soapenv:Envelope>

Connecting to SMS Gateway, 192.168.103.85 ...
Http result: 200 Ok
QueueAddResponse: 1 Ok
Sending test SMS succeeded.
```

At the bottom right of the 'SMS Test Log' section, there are two buttons: 'Test SMS' and 'Test Call'.

- In GSM-Modem tab of SMS-GW3 web interface press Send SMS Test and check its delivery.

The screenshot shows the SMS-GW3 web interface. On the left is a sidebar with the SMS-GW logo and a list of navigation items: Home, SMS Queue, General Setup, Time, GSM Modem (highlighted), SNMP, and System. Below the sidebar is a 'Version: 1.3.5' label and an 'Apply Changes' button. The main content area is titled 'GSM MODEM' and contains three sections:

Information

Network Registration:	Registered, home network
Signal Quality:	-53 dBm (96 %)
Operator Name:	T-Mobile CZ
SMS Service Center Address:	+420603052000
Number of SMS:	27
Number of failures SMS:	0
Number of Ringout:	3
Number of failures Ringout:	0

There is a 'Clear counters' button next to the 'Number of Ringout' value.

Configuration

SIM card PIN Status:	Ready	PIN managemant
SIM Card Pin:	1234	PIN number [4 to 8 characters]
Roaming Enable:	☒	Allow users to send SMS even when home network is not available
SMS http GET Enable:	☐	Enable http GET API
Manual Network:	☐	Manual Set Network enable/disable

Test SMS

There is a 'Tel Number' field with the value '+123456789123' and a 'Test text' field. Below the 'Test text' field is a 'Ringout Test' button. To the right of the 'Test text' field is a 'Send SMS Test' button, which is highlighted with a red box.

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.

The screenshot displays the WLD2 web interface for configuring alarms. At the top, the 'ALARMS' tab is selected in the navigation menu. The 'Alarms Settings' section includes a table with columns 'name', 'value', and 'description'. It contains two rows: 'Alarms reminder period' with a value of '0' and a description about alarm resend intervals, and 'Alarm reminder target' with a value of 'None'. Below this, an 'Alarm Target' modal is open for 'Default 1'. This modal has three main sections: 'Email list' with four input fields for email addresses (all containing 'example@hwg.cz'), 'SMS list' with four input fields for phone numbers (all containing '+420603603603') and checkboxes for 'call' (all unchecked), and 'SNMP trap list' with four rows of input fields for IP address, snmp community, and port (all containing '192.168.0.100', 'public', and '0' respectively). A 'Save' button is located at the bottom right of the modal.

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 on 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.

name	value	description
System Name	WLD2 5905-10A1	0 to 32 characters
System Location		0 to 32 characters
System Contact	WLD2	
SNMP port	161	Default port 161

community	read	write	enable
public	☒	☐	☒
private	☒	☒	☒

[Show OID keys table](#) Save

SNMP Settings

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

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.



1.3.1

HOME GENERAL SETUP SECURITY WIFI SENSORS OUTPUTS EMAIL SMS ALARMS SHMP TIME PORTAL SYSTEM

oid key	value	description	data type	access
1.3.6.1.2.1.1.0	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	27F5010000000000	1. Sensor SH	string	RO
1.3.6.1.4.1.21796.4.5.4.1.4.2	27F601000000000051	2. Sensor SH	string	RO
1.3.6.1.4.1.21796.4.5.4.1.4.3	27F701000000000066	3. Sensor SH	string	RO
1.3.6.1.4.1.21796.4.5.4.1.4.4	27F801000000000042	4. Sensor SH	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 synchronization via time servers are sent in the Time tab.

The screenshot displays the 'TIME' tab in the WLD2 web interface. The top navigation bar includes links for HOME, GENERAL SETUP, SECURITY, WIFI, SENSORS, OUTPUTS, EMAIL, SMS, ALARMS, SNMP, TIME (selected), PORTAL, and SYSTEM. The version number 1.3.1 is shown in the top right corner.

SNTP Settings

name	value	description
SNTP Server	europa.pool.ntp.org	IP Address or DNS Name
Time Zone	1 0 min	Number -12 ... +13
Summertime	☒ Central European	last Sun March 2:00 - last Sun October 3:00
Interval	1h	Sync period: 0h/1h/24h

Save

Time Settings

name	value	description
Time	15:46:53	hh:mm:ss
Date	14.02.2020	dd.mm.yyyy

Set browser's datetime Set Time manually

SNTP Log

Debug log window

Synchronize

SNTP Settings

SNTP Server – IP address or domain address of the time synchronization 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 summertime. Serves to set the correct system time. Required for correct recording of measured values.

Interval – interval of time synchronization with the server.

Time Settings

The Time Setup section enables you to fill in the current date and time manually, if synchronization with the time server cannot be used.

SNTP Log

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

Portal tab

The device can be connected to the SensDesk Technology based portal. Default portal is HWg-cloud.com provided for free by HW group.

In this tab you set parameters for sending data to a remote portal via HWg-PUSH protocol. More about the protocol or portal(s) is available on the website www.HW-group.com or in the **Portals (SensDesk Technology Based)** separate chapter below.

The screenshot shows the WLD2 web interface with the 'PORTAL' tab selected. The interface includes a top navigation bar with links like HOME, GENERAL SETUP, SECURITY, WIFI, SENSORS, OUTPUTS, EMAIL, SMS, ALARMS, SHMP, TIME, PORTAL, and SYSTEM. The main content area is divided into four sections:

- Portal Message:** Displays a message from HWg-cloud: "Check sensor online (2022-05-26 07:26:02 UTC)".
- Portal settings:** A form with fields for Portal (checked), Server Address (http://hwg-cloud.com/portal.php), IP Port (80), Team (Jen Chai), and Team Password (masked). A 'Save' button is at the bottom right.
- AutoPush settings:** A table with columns ID, NAME, TYPE, CURRENT VALUE, and AUTOPUSH. It lists four items: Water Floor 1 (WLD, 0 - Normal WLD), Water Floor 2 (WLD, 1 - Flooded WLD), Water Rack A (WLD, 0 - Normal WLD), and Water Rack B (WLD, 2 - Disconn. WLD). Each item has an '1.0' value in the AUTOPUSH column.
- Portal Debug Log:** A table with columns NAME, VALUE, and DESCRIPTION. It lists various timers and periods: Push Period (900), Log Period (300), Current Push Timer (343), Current Log Timer (164), Current Check Timer (0), AutoPush Block Timer (0), and Retransmit number (0). A 'Manual Push' button is at the bottom right.

Portal Message

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

Portal settings

Portal – enables or disables this function.

Server address – complete URL of the remote server. Connection to the HWg-cloud.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.

AutoPush settings

Sets the behavior 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.

What is AutoPush

AutoPush – By default, the device sends data to the portal at a fixed interval defined by the relevant portal (in the case of the [HWg-cloud.com](https://hwg-cloud.com) 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.

Portal Debug Log

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 porta

System tab

Download

description	file
Backup configuration	WLD2_Configs.bin
Online setup in XML	setup.xml
Online values in XML	values.xml
SNMP MIB Table	WLD2.mib
OID keys table	Online OID keys table
TXT list of common SNMP OIDs	WLD2_OID.txt

System

name	value
Product Name:	WLD2
Serial Number:	6007170002
Eth MAC Address:	00:0A:59:05:10:A1
WiFi STA MAC Address:	00:0A:59:05:10:A3
Version:	1.3.1
Build:	349
Compile time:	Jan 13 2020, 16:37:52
Up Time:	873440 [s]
Demo Mode:	Demo Mode
Network Upgrade:	Read available version--- Start Network Upgrade---
Upload Firmware or Configuration:	Browse... No file selected. Upload

Download

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

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.

Up Time – 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

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

System Restart

Restarts the device.

Firmware upgrade for WLD2 units.

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

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

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

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

System	
NAME	VALUE
Product Name:	WLD2
Serial Number:	6007171085
Eth MAC Address:	00:0A:59:06:72:BB
Wifi STA MAC Address:	00:0A:59:06:72:BC
Version:	1.5.9
Build:	2478
Compile time:	Jul 4 2024, 09:08:20
Up Time:	29 [s]
Demo Mode:	Demo Mode
	Read available version:---
Network Upgrade	Start Network Upgrade:---
Upload Firmware or Configuration:	Vybrat soubor Soubor nevybrán Upload

After the upgrade, the user is requested to restart the device manually by pressing the **Restart** button. **The device will not restart automatically; it must be restarted manually.** Check the firmware version after the restart.

System	
NAME	VALUE
Product Name:	STE2 r2
Serial Number:	60069911125
Eth MAC Address:	00:0A:59:06:65:B1
Wifi STA MAC Address:	00:0A:59:06:65:B2
Version:	1.5.9
Build:	2478
Compile time:	Jul 4 2024, 09:08:20
Up Time:	3443507 [s]
Demo Mode:	Demo Mode
	Read available version:---
Network Upgrade	Start Network Upgrade:---
Upload Firmware or Configuration:	Vybrat soubor Soubor nevybrán Upload

Factory reset

Restart

Remote Monitoring Ecosystem



HWg RME (Remote Monitoring Ecosystem) is a complete approach for designing long-term reliable remote monitoring systems using HWg components, including sensors, LAN/LTE devices, cloud or on-premise services, and mobile applications.

The system may or may not use a cloud portal or SMS/Call alerts, but it is designed to be easy to install, centrally managed, and maintainable over time.

The key benefit of HWg RME is **long-term reliability**: a monitoring system designed according to HWg RME principles helps customers react to critical situations even years after installation, while simplifying multi-site management, alarm settings, notifications, user rights, and reducing the need for manual checks and service interventions.

Central SMS gateway for alerting

SMS-GW is a central gateway that allows HW group devices to send SMS and Call alerts to selected phone numbers.

Insert a SIM card from your local mobile operator into the SMS-GW device. Once configured, it can work as a central SMS gateway for all compatible HW group devices in the same LAN. Multiple devices can use one SMS-GW to send alarm alerts by SMS or voice call to different recipients.



- SMS-GW3 (GSM/2G)
- SMS-GW3 LTE

The Portal

Each HW group device can be connected to a portal based on SensDesk Technology, developed and maintained by HW group. The portal is recommended for long-term reliable alerting, device availability monitoring, central firmware management, alert escalation, reporting, and remote device management.

Main benefits of using the portal:

- Central management of alarms from multiple devices
- Device Invalid Alert when a device is disconnected
- Alert history, graphs, multigraphs, and PDF reports
- Email, SMS, and Call alert escalation
- User and team management

- Open API and data export to third-party systems
- Central dashboard with filtering by site, device, or sensor

www.SensDesk.com

The SensDesk.com is a paid online portal service from HW group.

- Email, SMS, and Call alerts
- Device Invalid Alerts
- Graphs, reports, and Open API
- XML, SNMP, and JSON data access
- Mobile app support
- Multi-user accounts
- Up to 2 years of data historyof data history



www.HWg-cloud.com

The HWg-cloud.com is a limited free online portal service from HW group.

- Reliable email alerting without using public SMTP servers
- Device Invalid Alerts
- Limited number of devices per user account



Third-party Portals

You can also use your own public or private portal based on SensDesk Technology.

- SaaS or On-premises (Virtual appliance)
- Custom business model with selected paid services
- Own branding and service structure, depending on the portal operator)



SaaS / On-premise

Why connect WLD2 to the Portal?

Reliable alerting

Public SMTP servers are not a reliable solution for long-term alerting. Services such as Gmail, Yahoo, or GMX are designed for personal email use, not continuous system monitoring. Security policy changes, rate limits, and authentication updates may interrupt automatic email delivery. Portal-based notifications provide a more stable solution.

Device Invalid Alert

The portal can automatically send an email notification if the WLD2 device is disconnected from the network.

Remote access

The portal provides web-based remote access to the WLD2 device status. Where supported, it can also be used for remote output control or restarting connected technology.

Centralized alert management

The portal enables centralized management of alerts from one interface. Instead of configuring alert settings separately on each device, users can manage alerts, recipients, escalation rules, and user rights centrally. This is especially useful when personnel changes occur, because alerting can be updated without reconfiguring every device individually.

HWg Monitor: Mobile App for Displaying Current Sensor Values

The **HWg Monitor** is a unique mobile application for Android and iOS that displays current values from sensors, inputs, and outputs.

It can display values not only from **SensDesk Technology portals**, but also directly from connected **HW group monitoring devices** over WiFi or Ethernet.

The current iOS version of the application also supports discovery of the **WLD2** device on the local network using the **HWg Device Discovery** feature.

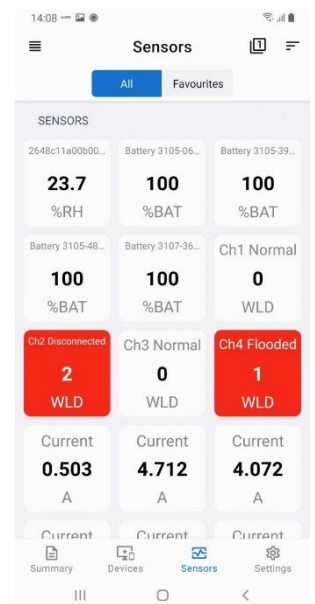


Note: HWg Monitor does not support the free HWg-cloud portal

The HWg Monitor application allows users to periodically retrieve values from one or more devices from the WLD2, Perseus, STE2, Poseidon2, Damocles2, PWR, and other HW group product families. It can also periodically download and display values from HW group cloud servers.

For each data source, such as a device or a portal from the SensDesk Technology family, a custom data refresh interval can be configured. The application also allows users to easily sort sensors by device or select preferred sensors for priority display.

The software downloads and displays data at user-defined intervals, including status indication with colour coding according to the severity of the condition. Red means that the sensor is in Alarm state. Yellow means that the sensor is in Disconnected state.



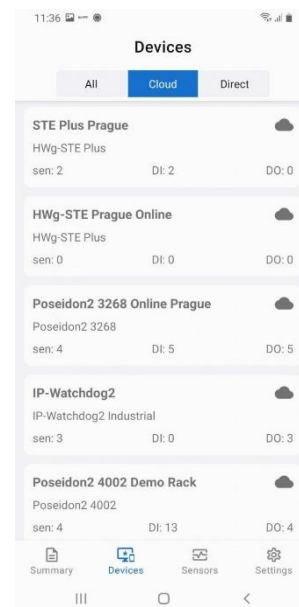
HWg Monitor can also remotely control outputs on directly connected Perseus, Poseidon2, and Damocles2 units. Remote output control is not available for units connected via a SensDesk Technology portal

Specifics of selected SensDesk Technology portals

The HWg Monitor application can work with all portals from the SensDesk Technology family. However, not every portal has to support this application.

Support depends on whether the XML API is enabled on the portal. This feature can be enabled or disabled by the portal operator.

The HWg-cloud.com portal has this support disabled. XML API support is available only in the paid version of SensDesk.com. Portals operated by other providers may have different settings. Therefore, please contact your portal operator to confirm application support.



How to connect WLD2 to the HWg-cloud.com portal

- Create a user account on HWg-cloud. If you already have one, enter your login details, and log in. If you do not have an HWg-cloud account yet, click the 'Register' button to display the registration form.
- After logging in or registering in your HWg-cloud account, click on the person icon, then select the 'My Team' option.
- On this page, in the portal tab Settings, you will find all the entries required to configure the WLD2 web interface.

The screenshot shows the HWg-cloud portal interface. At the top, there's a navigation bar with the HWg CLOUD logo, a language selector set to 'es', and buttons for 'Adopt device', a user profile icon, a notification bell, and a 'BUY TARIFF' button. Below this is a horizontal menu with tabs: Dashboards, Devices, Sensors, Locations, Device groups, Multigraphs, and Settings. The 'Settings' tab is active, and the breadcrumb 'Home > Settings' is shown. The main heading is 'Team for es'. Below it are buttons for 'View', 'Edit', and 'Audit trail'. A 'SMS' tab is visible, showing a 'Gateway' dropdown set to '- None -'. Below that, there are two sections: 'PORTAL SETTINGS' and 'LIMITS'. The 'PORTAL SETTINGS' section is highlighted with a red box and contains the following information: 'This is credential for your devices.', 'Portal URL: http://hwg-cloud.com/portal.php', 'Portal port: 80', 'Team: es', and 'Team password: TKD7TH'. The 'LIMITS' section shows settings for 'Is Trial' (No), 'Date of expiration' (- Empty -), 'Action: E-mail limit' (- Empty -), 'Action: SMS limit' (0, 0 used), and 'Action: SNMP trap limit' (0, 0 used).

- On the Portal tab of the device interface choose the *Enable Portal* option and save the changes using the *Save* button in the right bottom corner of the window.

The screenshot shows the 'Portal settings' and 'AutoPush settings' interface. The 'Portal settings' section has a table with columns 'NAME', 'VALUE', and 'DESCRIPTION'. The 'Portal' row has a checked checkbox in the 'VALUE' column, highlighted with a red box. Other rows include 'Server Address' (http://hwg-cloud.com/portal.php), 'IP Port' (80), 'Team (provided by portal)' (es), and 'Team Password (provided by portal)' (masked). Below this is the 'AutoPush settings' section with a table with columns 'ID', 'NAME', 'TYPE', 'CURRENT VALUE', and 'AUTOPUSH'. It lists four entries: 'Water 501', 'Water 502', 'Water 503', and 'Water 504' (WLD), each with a 'CURRENT VALUE' of '0 - Normal WLD' and an 'AUTOPUSH' value of '1.0'. At the bottom right, there is a 'Save' button highlighted with a red box.

- Click the *Manual Push* button to activate the portal function.

Portal Debug Log

NAME	VALUE	DESCRIPTION
Push Period:	900	[seconds]
Log Period:	300	[seconds]
Current Push Timer:	5	[seconds]
Current Log Timer:	244	[seconds]
Current Check Timer:	0	[seconds]
AutoPush Block Timer:	0	[seconds]
Retransmit number:	1	

26.03.2025, 14:34:40
Push delta start
Server Address: http://hwg-cloud.com/portal.php
Push SUCCESS

Manual Push

- Instead of *Portal disabled*, a link *hwg-cloud.com: register your IP sensor* should appear in the *Portal Message* field. Click on this link to get to the portal.

HWgroup

1.5.9

HOME GENERAL SETUP SECURITY WIFI SENSORS OUTPUTS EMAIL SMS ALARMS SNMP TIME PORTAL SYSTEM

Portal Message

HWg-cloud.com: Register your IP sensor and fill Team and Team Password correctly. (2025-03-26 13:36:01 UTC)_

Portal settings

NAME	VALUE	DESCRIPTION
Portal	☒	Portal Enable/Disable
Server Address	http://hwg-cloud.com/portal.php	IP Address or DNS Name
IP Port	80	Default 80
Team (provided by portal)	es	Push device access parameters
Team Password (provided by portal)	*****	Please have a look at My Team on Sensdesk

- The portal will open, and the device will be automatically assigned to your account.

es
Adopt device

BUY TARIFF

Dashboards Devices Sensors Locations Device groups Multigraphs Settings

Home

Devices

Filter by

Device type
Family

Alias (contains)

Sort by

State
Alias

Clear filter

EVA WLD2 5906-72BB

Last update 2 min 23 sec ago

WLD System

The most usable devices with the WLD sensing cable



Perseus 140



Perseus 145



Perseus 150



Perseus 155



Perseus Energy 242



Perseus Energy 285



WLD-Relay



WLD2



NB-WLD



WLD-ECHO

You will find more information at the end of the manual.

WLD device family overview

	WLD2	NB-WLD	PERSEUS LAN only	PERSEUS LAN & SIM	WLD- ECHO
WLD ports (zones)	4	1	1	1	2
Max length of a sensing cable	185 m	60 m	185 m	185 m	185 m
Sensing cable type	A, B	A, B	A, B	A, B	A, B
Location detection	-	-	-	-	-
Ethernet	YES	-	YES	YES	-
WiFi	YES	-	-	-	-
Mobile (cellular) networks	-	NB-IoT	-	YES	-
Web Interface	YES	Portal only	YES	YES	-
SMS-GW (for alerting)	YES	-	YES	YES	-
Portal (SensDesk Technology)	YES	YES	YES	YES	-
Relay output alerts	VDO*, PVDO* *	PVDO**	Some models	Some models	YES
Email Alerts	YES	Portal only	YES	YES	-
SMS/Call alerts (Independent)	-	-	-	YES	-
SMS/Call alerts(Portal/SMS- GW)	YES	YES	YES	YES	-
Alerts reminder	YES	Portal only	YES	YES	-
Alerts escalation	Portal only	Portal only	YES	YES	-
Open API	YES	-	YES	YES	-

*VDO - Virtual Digital Output

**PVDO – Portal Virtual Digital Output

WLD devices family

WLD Relay

The Sensor WLD Relay 1W-UNI can **operate independently** with a 12V power supply as a **relay output**, or it can be used **as a sensor connected** via 1-Wire UNI **to any HW group device** (STE2, Poseidon, Ares etc.). The relay output signals both water detection and sensing cable disconnection.



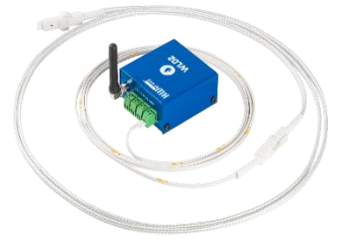
NB-WLD

NB-WLD is a remote monitoring detector with **one WLD zone**, an internal battery, and **NB-IoT** (NarrowBand IoT) connectivity (SIM card included). NB-WLD must be connected to the **SensDesk Technology**-based portal.



WLD2

WLD2 is a standalone monitoring detector with **four WLD zones**, Ethernet and WiFi connectivity, with PoE or external adapter power supply.



WLD-ECHO

WLD-ECHO is a compact water leak detector for WLD-Sensing cables A/B (up to 185 m). This external sensing cable detects water along its entire length, and even a few drops trigger an alarm and activate the relay output. Powered by 2 × AA batteries or 12 V DC.



Perseus Platform with a single WLD sensing cable input

Perseus 150 and 155

Perseus Monitoring 150 and 155 are complex 1U solutions for a 19" rack remote monitoring system. Connect external physical sensors (°C, %RH, A, V) or detectors (relay / dry contact. 3rd party meters (sensors) can also be connected via LAN or Modbus/RTU.



Perseus 140 and 145

Perseus Monitoring 140 and 145 are solutions for remote monitoring on site with LAN and LTE (only Perseus Monitoring 145). External sensors (up to 1000 variables) - RJ11 ports (1W-UNI) or RS-485 (Modbus/RTU). Multiple DI / DO (relay) and a WLD port.



Perseus Energy 242

Perseus Energy 242 is a LAN device in a metal case for environmental monitoring of a site of any size and complexity. Up to 100 external meters (and sensors) with 1000 values (variables) can be connected.

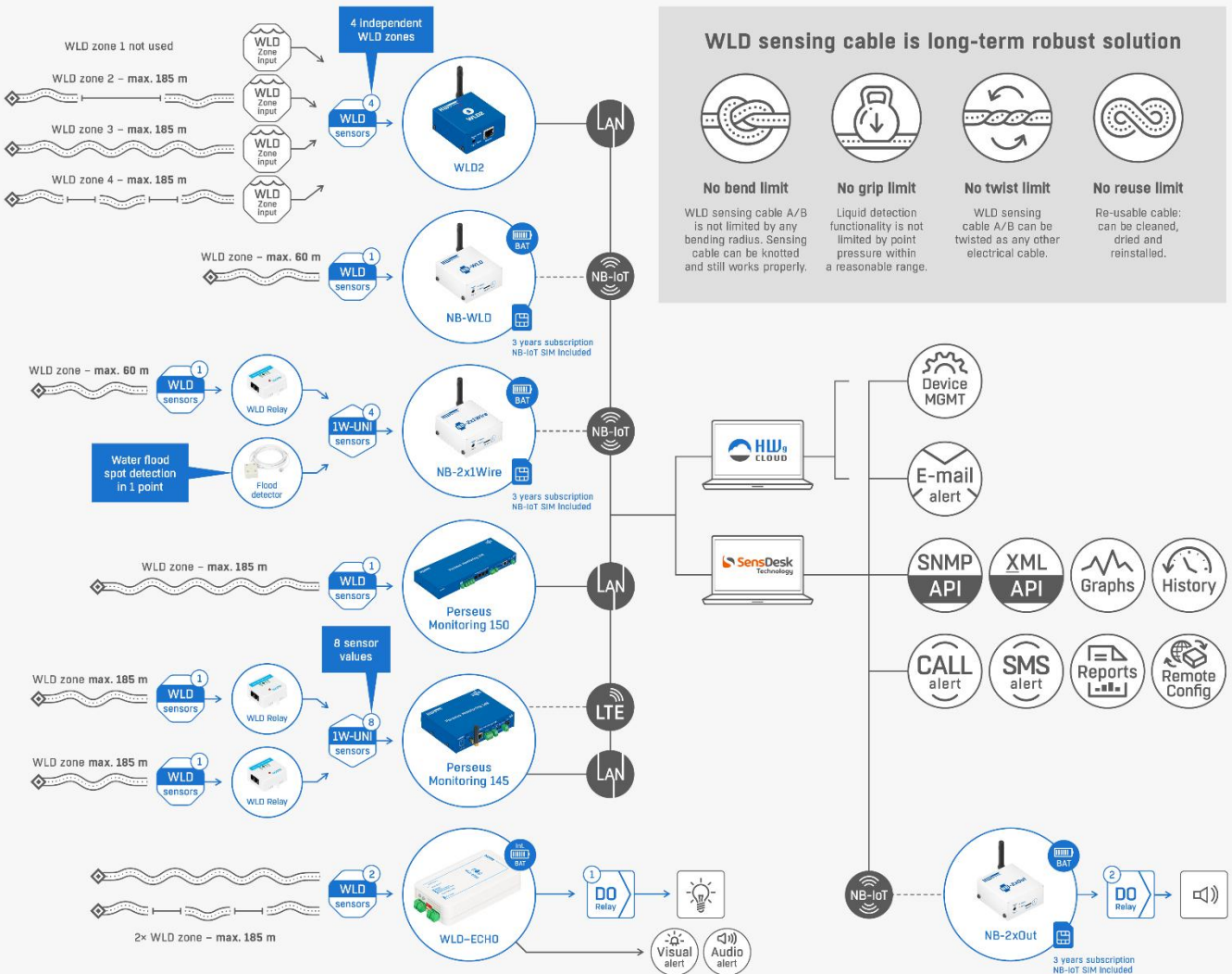


Perseus Energy 285

Perseus Energy 285 is a DIN rail LAN and LTE solution for remote energy monitoring and control applications with M-Bus Master. Connect external physical sensors (°C, %RH, A, V), detectors (relay/dry contact) and 3rd party meters (sensors) can also be connected via LAN or Modbus/RTU.



WLD System



WLD-Sensing cable A accessories

WLD-Sensing cable A – Accessories



WLD-Sensing cable A
2m / 10m / 50m

Water is detected along the entire length of the WLD sensing cable.



WLD-Cover Strip A 35 5m
Cover strip for WLD sensing cable A.



WLD-Poro Tape 5m
Adhesive tape with holes for attaching WLD sensing cable.



WLD-Extension cable AB 5m
Prolong non-sensitive cable 5m for WLD type A and B.



WLD-Connecting cable AB 2m
2m cable for connecting the WLD sensing cable with WLD zone input on the device. Terminator included.

WLD-Sensing cable B accessories

WLD-Sensing cable B – Accessories



WLD-Sensing cable B
2m / 5m / 10m / 50m

Water is detected along the entire length of the WLD sensing cable.



WLD-Cover Strip B 30 5m
Cover strip for WLD sensing cable B.



WLD-Poro Tape 5m
Adhesive tape with holes for attaching WLD sensing cable.

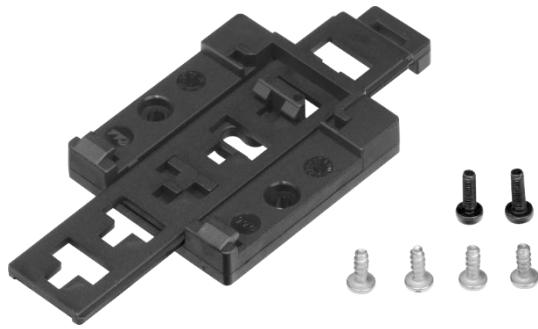


WLD-Extension cable AB 5m
Prolong non-sensitive cable 5m for WLD type A and B.



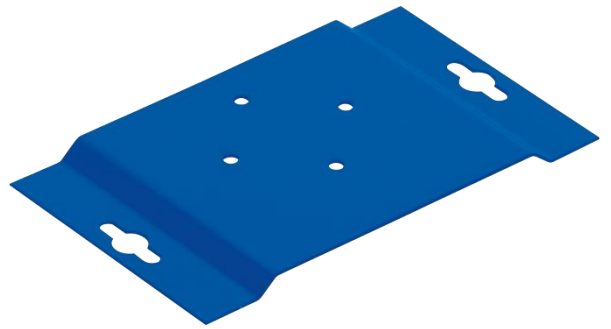
WLD-Connecting cable AB 2m
2m cable for connecting the WLD sensing cable with WLD zone input on the device. Terminator included.

Mounting accessories



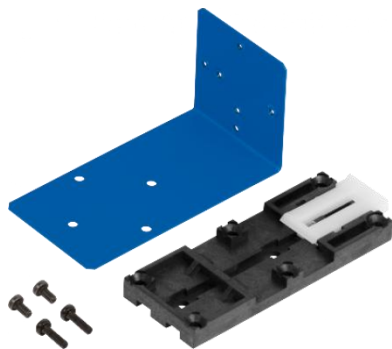
DIN Rail box set

A mounting kit for installing HWg devices to a DIN rail.



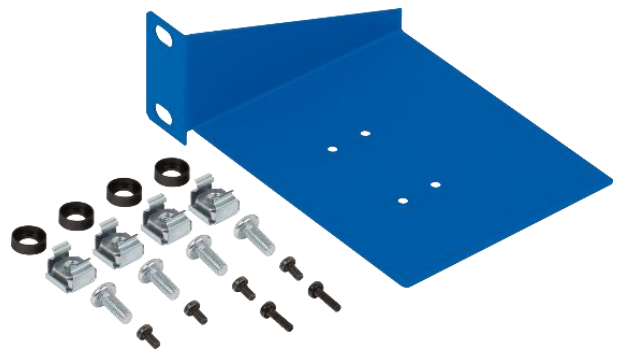
Mount plate D

Wall mount support



Mount plate L DIN Rail

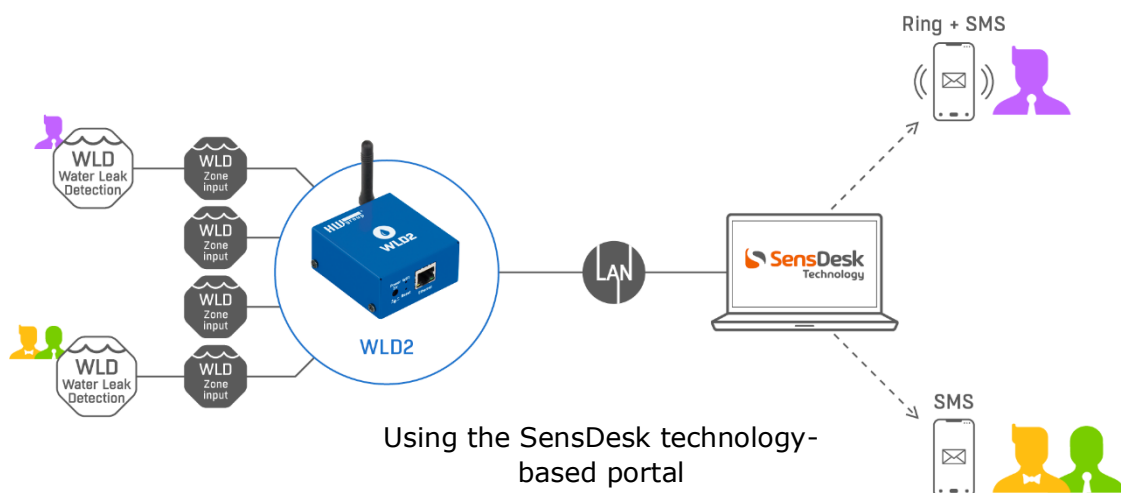
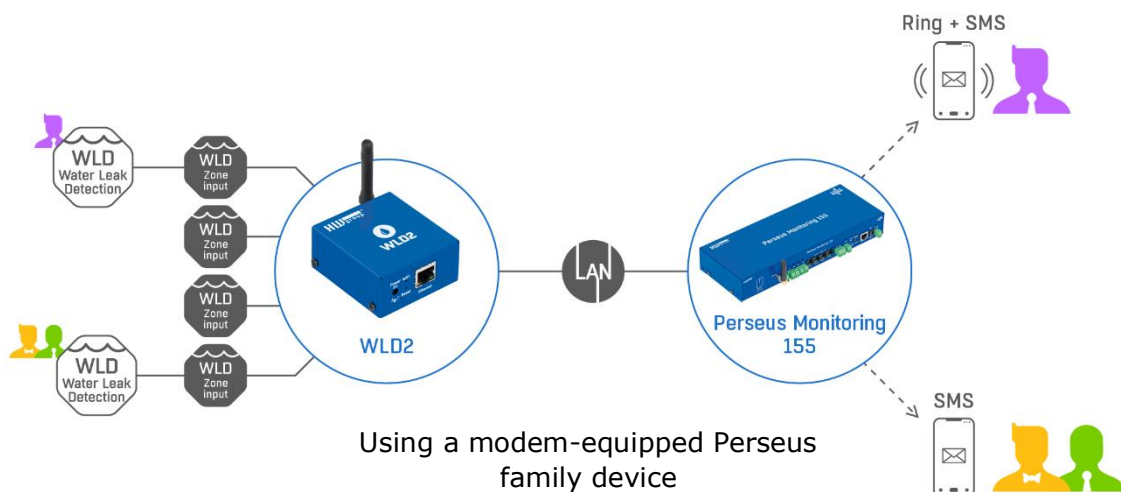
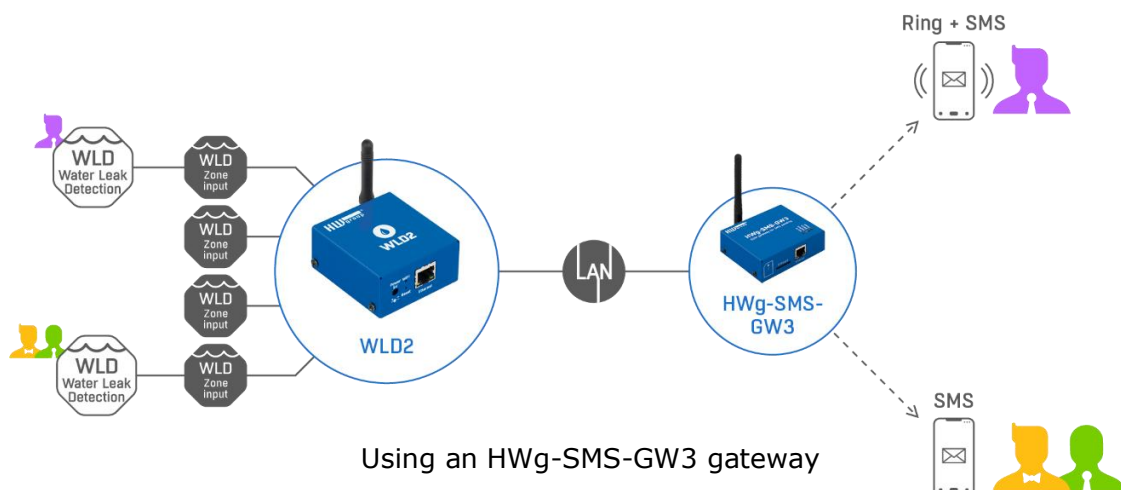
DIN Rail mount plate



Mount plate E- 1U

Rack (cabinet) mount plate

Different Ways to Send SMS Alerts from the WLD System



How to Design Water Leak Detection Systems

Detection Principle

The WLD system is designed to detect even a few drops of water as quickly as possible.

The two most important design goals are:

1. **Minimize the time between the first leak and alarm delivery**
2. **Avoid false alarms**

The WLD system detects the presence of water along the sensing cable. It is not intended to measure the height of the water level.

Installing the WLD Sensing Cable on the Floor

Install the WLD sensing cable around the perimeter of the room or around areas where water may appear.

The cable should be slightly loose. A good rule is to use approximately **1.3 m of cable for every 1 m of monitored distance**. A zig-zag layout is recommended.

The sensing cable should be installed directly on the floor, ideally below other cables, and fixed using **J-clips**, **WLD-Poro Tape**, or **WLD-Cover Strip**.

Installation recommendations

- 1) Avoid oily areas. Oil and dust can contaminate the cable and increase the detection time.
- 2) Do not install the cable directly behind air-conditioning units. Keep at least **1 m distance** to avoid false alarms caused by humidity or condensation.
- 3) The WLD sensing cable Type A and Type B is mechanically durable and flexible. However, avoid installation on vibrating parts.
- 4) The cable can be installed on metal floors. Use a cover strip or perforated tape for mechanical fixing.
- 5) Install the cable away from foot traffic whenever possible. In walk-through areas, protect the cable with a cover strip.
- 6) Use self-adhesive J-clips every **1 to 2 m**. Additional clips may be needed in corners or bends.
- 7) On porous concrete floors, the adhesive base of the J-clip may not hold reliably. Use silicone or another non-conductive adhesive.
- 8) Always make sure that the sensing cable is installed directly on the floor, not suspended above it.

Installing the WLD Sensing Cable on Pipes

WLD sensing cables Type A and Type B absorb water and react quickly to a few drops. For this reason, they are suitable for leak detection on pipes.

Vertical pipes

Wrap the WLD sensing cable around the pipe at an angle of **30–45°**. Repeat the angle along the pipe as needed.

Fix the cable using **WLD-Poro Tape** or cable ties every **0.9 to 1.5 m**.

Horizontal pipes

Route the WLD sensing cable Type A or Type B along the lower side of the pipe.

Fix it with **WLD-Poro Tape** or cable ties every **0.5 to 1 m**.

Note: *If the cable is installed on chilled-water pipes, insulate the pipe after installation. This helps reduce condensation and prevents false alarms.*

Installing the WLD Sensing Cable on Stairs

Stairs are a typical path for water during flooding. They are important detection points, especially at the top or bottom of staircases.

Recommended installation rules:

- The WLD sensing cable can be installed on the vertical edge of stairs if protected by **WLD-Cover Strip**.
- The most critical point is the **bottom of the staircase**, where water from upper floors usually collects.
- Do not install the cable too high above the floor. This may delay detection by valuable seconds or minutes.
- If the cable is routed along the side wall of a staircase, keep it as close to the floor as possible. Direct floor contact is preferred.

Installing the WLD Sensing Cable in an Elevator Shaft

In elevator shafts, the WLD sensing cable is usually installed in the **elevator pit**, where water is most likely to collect.

Install the cable directly on the floor, ideally around the perimeter of the pit, so that it can detect water running down the shaft walls.

The installation must avoid mechanical damage, collision with moving elevator parts, and must allow easy service access.

Installation rules:

- Do not install the WLD cable on elevator guide rails.
- Avoid oil collection areas.
- Route the cable exit from the shaft in a protective conduit along the wall.
- Install the WLD device outside the flood zone and outside the elevator shaft.

WLD System Design Rules

Correct design means: **maximum coverage of risk areas + minimum detection time + minimum false alarms**

Zone design

Divide the monitored area into zones.

- **1 WLD input = 1 WLD zone**
- Standard maximum zone length: **200 m**
- NB-WLD maximum zone length: **60 m**
- Large areas should be divided into multiple zones for faster remote identification of the leak area

WLD sensing Cable Topology

Required order: **Device → Connecting Cable → Sensing Cable → optional Extension Cable → Sensing Cable → Terminator**

Rules:

- The terminator must always be installed at the end of the WLD zone.
- The terminator is included with the WLD Connecting Cable.
- The WLD Location cable cannot be extended.
- Use extension cable only in areas where water detection is not required.

Cable Placement

Route the WLD sensing cable:

- around the perimeter of the room
- around racks, pipes, and other risk areas
- directly on the floor
- below other cabling
- preferably in a zig-zag pattern

Recommended ratio: 1.3 m of WLD sensing cable per 1 m of monitored distance

WLD system Design Priorities

1. Minimize detection time

- Cover all areas where water may appear or flow.
- Avoid blind spots.
- Do not save cable length in critical areas.

2. Minimize false alarms

- Use correct cable placement.
- Avoid unsuitable environments.
- Protect the cable in walk-through areas.

Areas to Avoid

Avoid installing the WLD sensing cable:

- directly behind air-conditioning units — keep at least **1 m distance**
- in oily or dusty areas
- on vibrating parts
- in condensation areas without insulation
- in oil collection areas, for example in elevator shafts

Mechanical Installation

Recommended fixing methods:

- **J-clips** every **1–2 m**
- **WLD-Poro Tape**
- **WLD-Cover Strip** in walk-through areas

For concrete floors, use silicone or another suitable non-conductive adhesive.

Always protect the cable in areas with foot traffic.

Alarm and Integration

The WLD system can be integrated with:

- Email alerts
- SMS alerts
- Call alerts
- SensDesk Technology portal
- Relay outputs, for example to security systems
- BACnet systems
- SNMP monitoring systems
- SNMP traps for IT monitoring systems

The goal is immediate alarm escalation within seconds or minutes and long-term reliable alarm delivery, even many years after installation.



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

manual version: 1.0.16