Manual for 2 devices

- IP WatchDog2 Lite
- IP WatchDog2 Industrial

April 2025

The device complies with the standards in force in the Czech Republic, is operationally tested and is supplied in a serviceable condition. To keep the device in this state, it is necessary to follow the requirements on safety and maintenance of the device.

Do not use the device if:

- It is visibly damaged
- Is not working properly
- There are loose parts inside the device
- Been exposed to moisture or water
- It was repaired by unauthorized persons
- The power adaptor or its power cord are visibly damaged

The manufacturer is only responsible for the device if it's being powered by an approved or supplied 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.

Shipment contents

The complete package of the IP WatchDog2 product may include the following components. Please check the version of the product you are ordering:

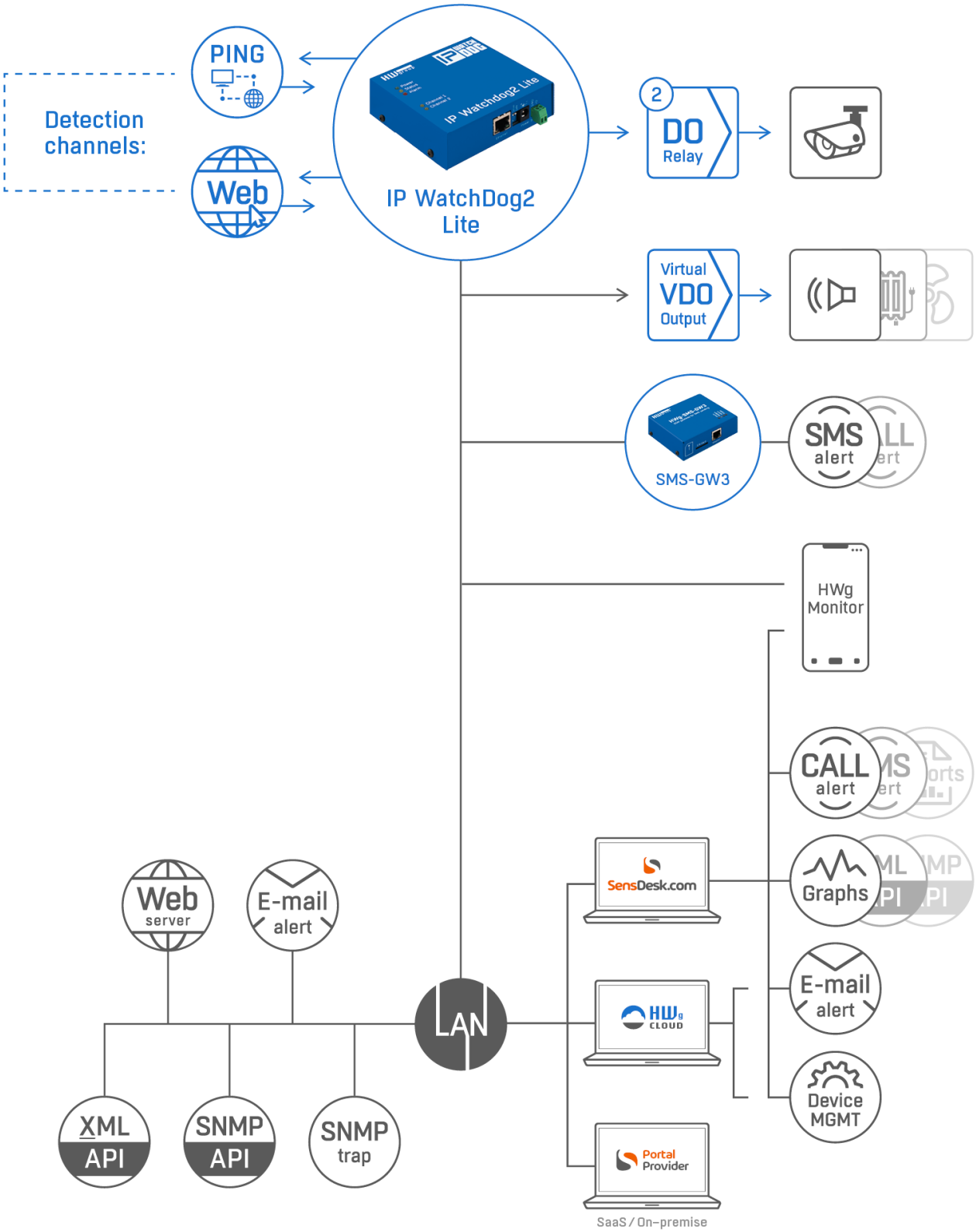
- IP WatchDog2 Industrial plain unit
- IP WatchDog2 Lite plain unit
- Printed manual
- Power adapter (12V, international – EU, UK, US)

Default network parameters configuration:

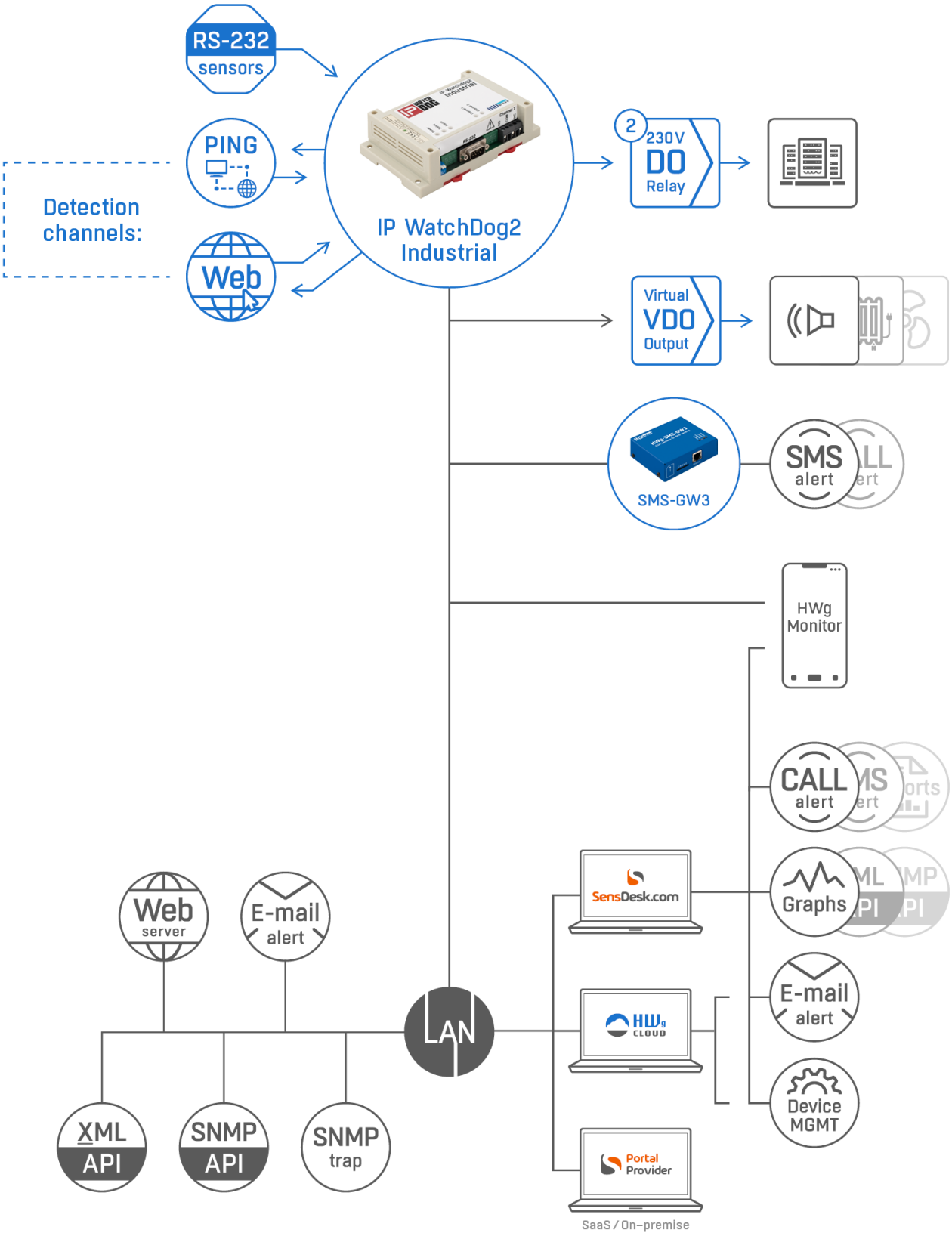
- IP configuration: Enabled by default
- IP address: DHCP by default (Fixed IP address available)
- Network mask: DHCP by default
- Default gateway: DHCP by default
- Username: Not set
- Password: Not set

Product usage scheme(s)

IP WatchDog2 Lite



IP WatchDog2 Industrial



IP WatchDog2 Lite / Industrial

	IP WatchDog2 Lite	IP WatchDog2 Industrial
Housing	Metal	Plastic
Relay outputs	max. 50V/1A	max 240V/16A (AC)
Serial line input (RS-232)	No	Yes
Manual output control	Yes	Yes
Monitoring methods	4 methods	5 methods

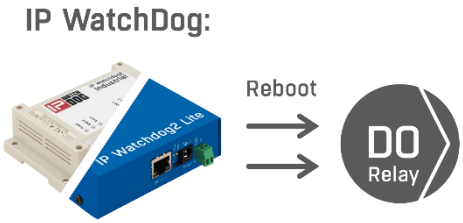
IP WatchDog2 Lite

IP WatchDog2 Industrial

5 Monitoring methods and their parameters

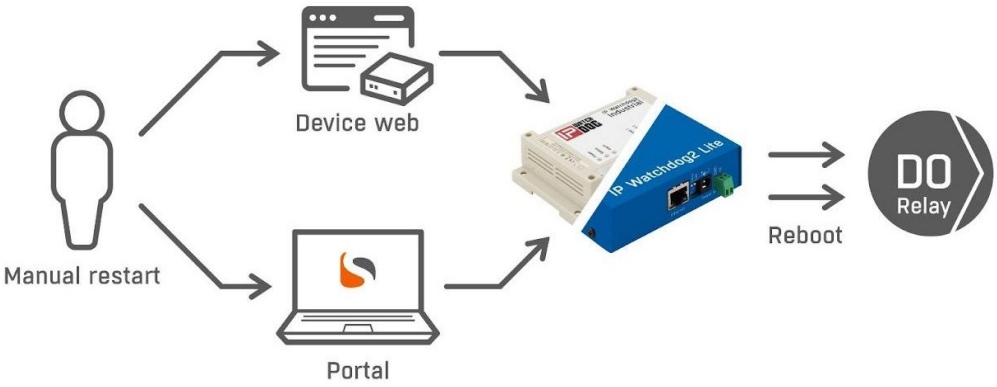
Outgoing Ping	**Primary target IP** – primary IP address where IP Watchdog2 sends the PING and from which it awaits reply. **Secondary target IP** – secondary IP address where IP WatchDog2 sends the PING and from which it awaits reply, if primary target does not responds. **Ping number** – Number of sent PINGs in timeout for reboot interval. **Timeout for reboot** – time interval, in range from 0-1800 s (0 =disabled), during this period, IP WatchDog2 sends PINGs to the monitored device. If there is no response, a RESET is performed.
Incoming Ping	**IP range** – range of IP addresses defined by IP and mask, from which the receiving PING can be accepted. **Timeout for reboot** – time interval, in range from 0-1800 s (0 =disabled), that IP WatchDog2 waits for incoming PING before causing RESET.
WWW Page request	**Server address** – IP address where IP WatchDog2 requires HTML page from. **Timeout for reboot** – time interval, in range from 0-1800 s (0 =disabled), during this period, IP WatchDog2 sends request for a HTML page. If there is no response, a RESET is performed. **Request number** – Number of requests in timeout for reboot interval.
WWW Page	**Ping address** (Heartbeat page request)– address of HTML page which is to be periodically requested from monitored system in heartbeat process. **Timeout for reboot** - interval in range from 0-1800 s (0 = disabled), for this time IP WatchDog2 waits for an request for a HTML page, then RESET is performed.
Requested RS232 String	**Requested string** – string in format ASCII, HEX or DEC awaits on port RS-232 (* represents random sign). **Timeout delay for reboot** – interval in range 0-1800 s (0 = disabled), for this time IP WatchDog2 waits for an request for a HTML page, then RESET is performed.
Manual control	**No parameters required** **Options:** a) Can be controlled from the portal b) IP WatchDog device web can be locked by password.

3x Rebooting mechanism scheme



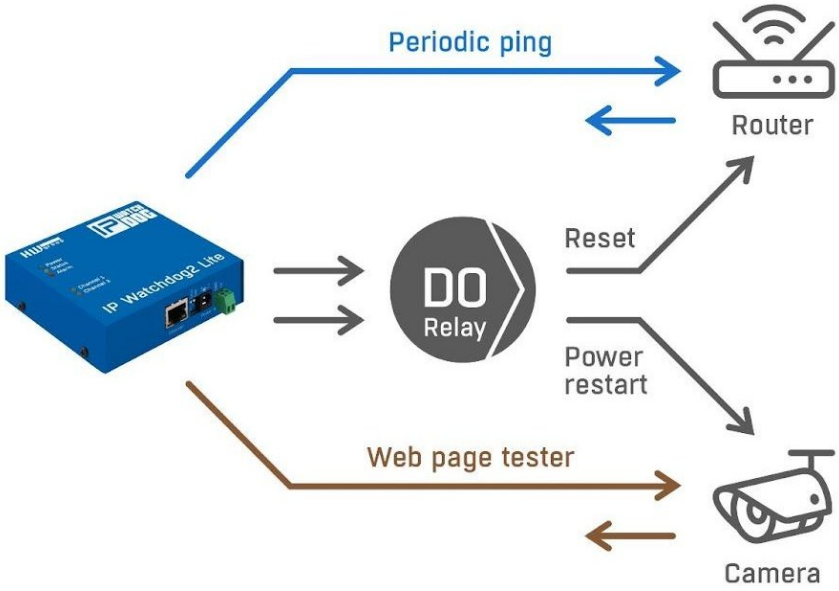
Manual reboot

A human operator can manually reboot the device using the web interface.



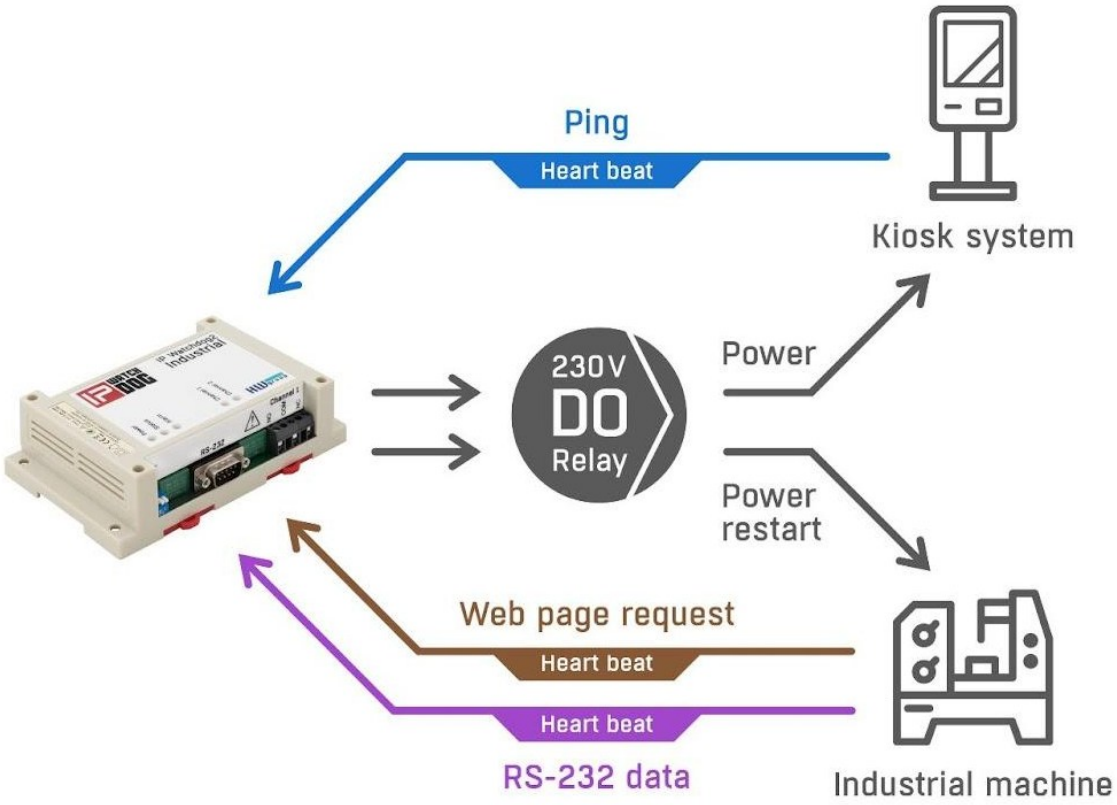
Automatic reboot – Failure detection

The automatic failure detection mechanism works without modifying the controlled system. You simply set up failure detection based on an existing parameter that is easy to monitor. For example, a web page request or PING detection can check the LAN connectivity of a specific device.



Automatic reboot – Heartbeat

Heartbeat mechanism reboots the device if no heartbeat signal is received within a defined time. The IP WatchDog can receive a PING request, a web page request, or a defined string in the serial port data stream.
This is a reliable WatchDog process, but you must ensure that the monitored system sends the heartbeat signal.



For more information about the mechanisms, please refer to the article:
https://www.hw-group.com/support/use-ip-watchdogs-remote-reboot-for-automatic-repair-or-full-system-restart

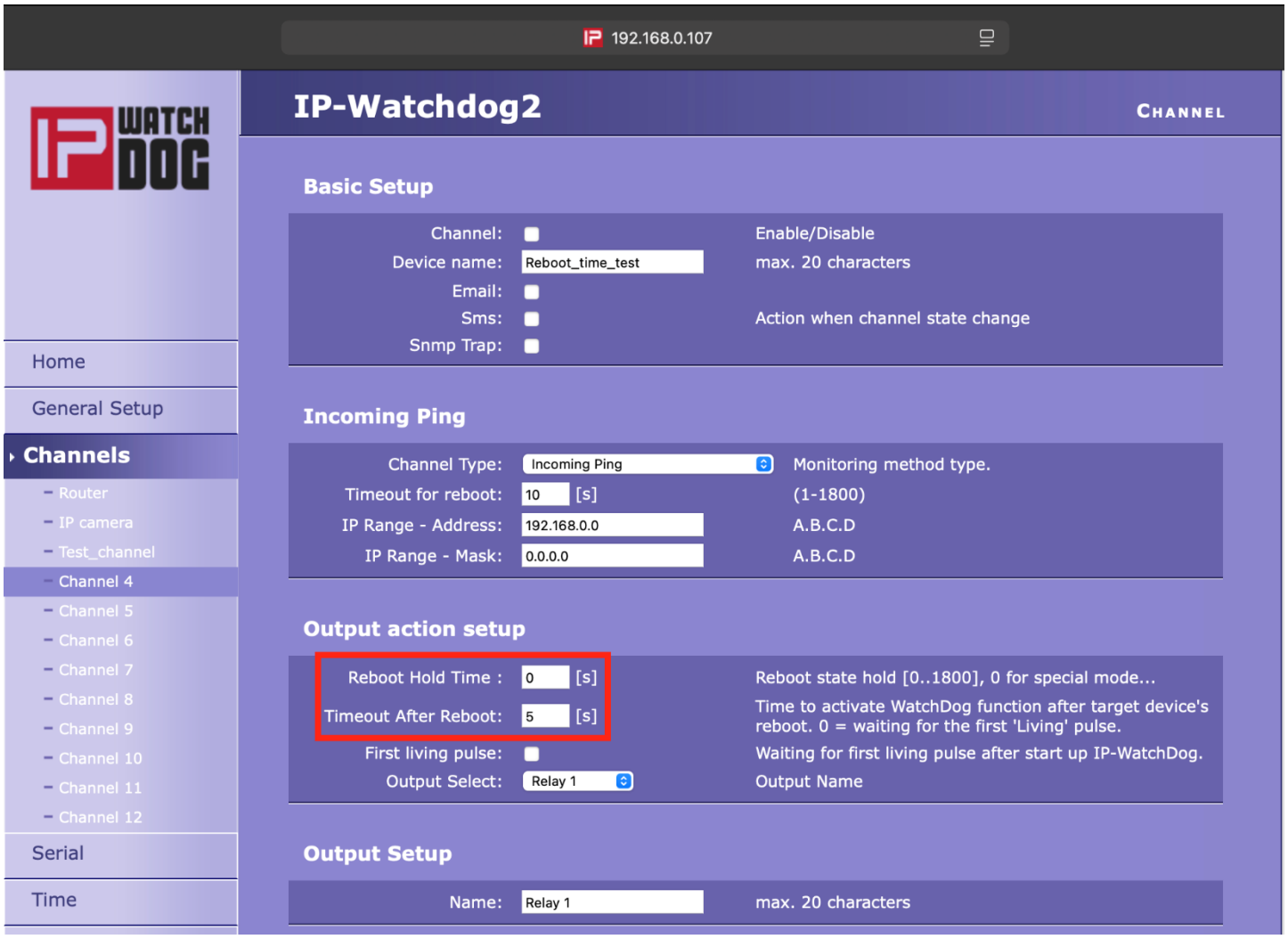
Application tips

Reboot Hold Time

Besides the classic reset of the monitored device and its following release IP WatchDog2 still a possibility of permanent Reset state in case the monitored device does not respond to the demands of IP WatchDog2 or does not send periodically refresh impulses. This mode is activated by setting the parameter *Reboot Hold Time* to 0. If in this case state is performed RESET, the channel (or its output) in this state until the monitored device reports itself again, or if no channel is deactivated.

The function is designed for cases where IP WatchDog2 does not reset directly monitored device or when one of the channels used to activate the backup device or other alarm system.

Note: *If the value Reboot Hold Time = 0, the IP WatchDog2 in a special mode Reset function and especially Manual Reset behave somewhat differently than described on the previous pages, because the Reset state cannot be ended by itself. This is especially true when using Manual Reset button with deactivated channel when there is no standard way how to reverse Reset state and the only way is to activate the channel and initialize the refresh impulse.*



RME - Remote Monitoring Ecosystem

HW group company is a manufacturer of the **Remote Monitoring Ecosystem**. Our devices, sensors and detectors could be combined into large industrial-grade, secure and reliable projects connected to the SensDesk Portal Technology.

Central SMS gateway for alerting

SMS-GW is a central gateway that allows all HWg devices
And any SensDesk Technology based portal sending SMS & Call alerts to any telephone number.
Just plug there SIM card from your local operator and use one SMS-GW device for alerting from all devices & software in the same LAN.
Every HWg Ecosystem device (Portal) using the SMS-GW for alerting to different telephone numbers.

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

The Portal

Each HWg device can be connected to one SensDesk Technology based portal. It can be a useful tool for long-term reliable alerting, central FW upgrade place etc..

www.HWg-cloug.com

The **HWg-cloud.com** Portal (on-line service) from HW group company is limited but free of charge service.

- Device alerting (long-term reliable)
- Limited amount of devices per user account

www.SensDesk.com

The **SensDesk.com** Portal is paid service from HW group company. It's paid service with these benefits against HWg-cloud:

- SMS & Call alerts
- Graphs, reports, Open API (XML, SNMP)
- Mobile App (HWg mobile)
- Multi user accounts, Up to 2 years data history

3rd party Portals

You can be using your own even public, even private Portal based on **SensDesk Technology.**

- SaaS / On-premise version
- Make your own business model (mix of paid services)

Technical parameters

IP WatchDog2 Lite

Ethernet port	
+ Interface	RJ45 (10BASE-T / 100BASE-Tx)
+ Compatibility	Ethernet: Version 2.0/IEEE 802.3
+ Supported protocols	IP: ARP, TCP/IP, NVT, RFC2217, UDP/IP, SNTP

Relay contact ampacity	
DC voltage	max. 30V / 1A
AC voltage	max. 50V / 0,5A

Environment parameters	
+ Operation temperature	-30°C to +85°C
+ Storage temperature	-5 to +75 °C
+ Relative humidity	5 to 95 % (non-condensing)

Mechanical construction	
+ Mechanical construction	Metal, table construction with external wall bracket, DIN rail or Rack
+ Dimensions	100x94x31 / 260g
+ EMC	FCC Part 15, Class B, CE - EN 55022, EN 55024, EN 61000

Power Input	
+ Port	POWER 9-30V DC
+ Type	Main device power input (typically 250 mA) + Power Out
+ Connector	Jack (barrel, inner 2.5 mm outer 6.3 mm), Terminal Block

Power Output	
+ Voltage	Power OUT = Power In
+ Current	Max. Power Adaptor minus 250mA or 1000mA
+ Connector	Terminal Block

Connectors of the IP WatchDog2 Lite

Individual connectors and control elements as well as connection of the relays is shown on the picture below:

LED

- **Power (Green)** - lights, if connected and the device is working
- **Status (Yellow)** - blinks when signal is accepted from the monitored device, blinking quickly when being upgraded
- **Alarm (Red)** - lights, if some of device is unavailable and IP WatchDog2 is performing reset
- **Channel1/Channel2** - lights when channel is switched (reset or manual switch)

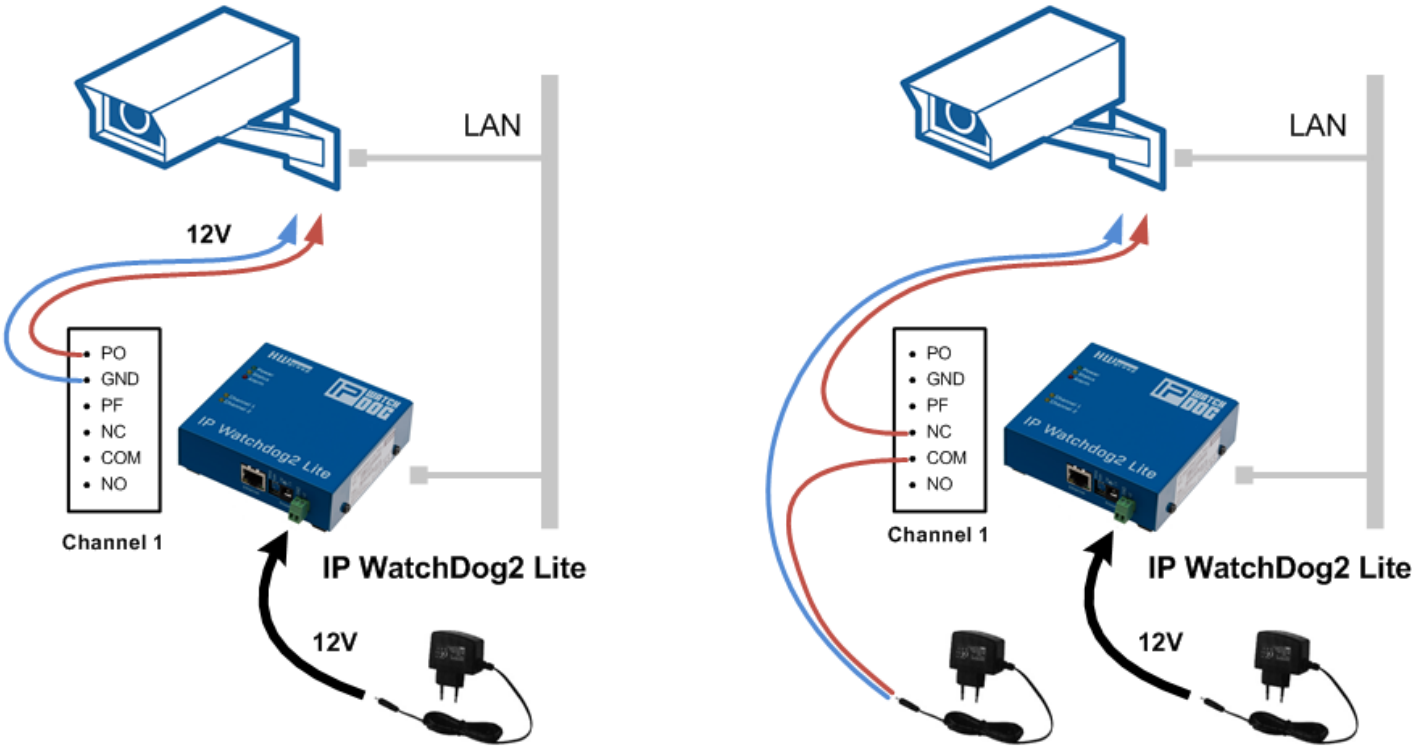
DIP switches

- **Setup** - is used to reset the device to the default configuration, if switched when the power supply is
- **Safe** - for manufacturer purposes only

Outputs Channel1 / Channel2

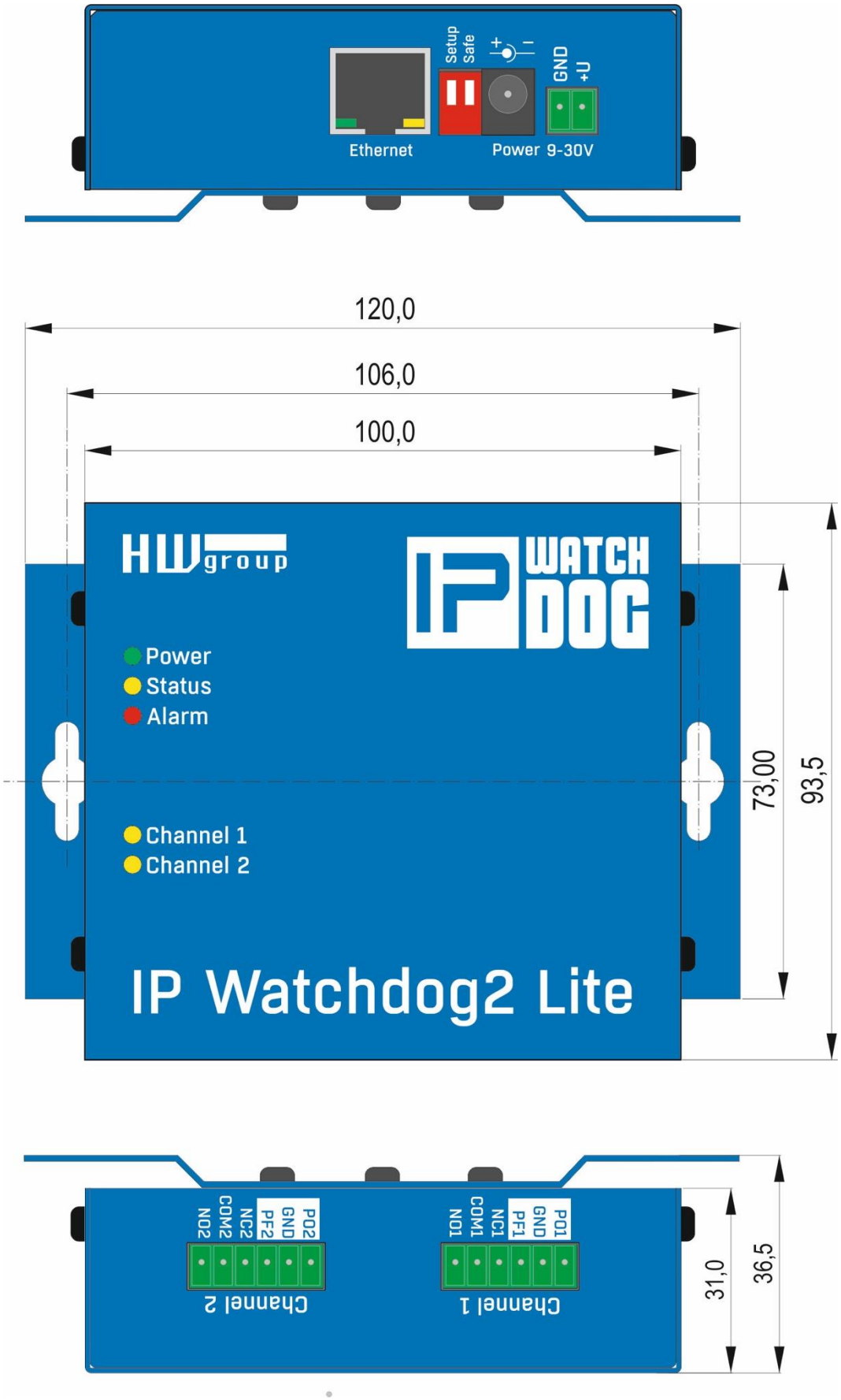
Terminal board description		
Pin	**Power**	**Function description**
PO	*Power On*	In the idle state this pin contains power supply of the IP Watchdog2 - axis of the power connector.
PF	*Power OFF*	In Reset mode this pin contains power supply of the IP Watchdog2 - axis of the power connector.
GND	*Ground*	Negative pole of the supply voltage. Is connected directly to GND.
NC	*Normally Close*	In Idle state this pin is connected with the appropriate COM pin
NO	*Normally Open*	In Reset state this pin is connected with the appropriate COM pin
COM	*Common*	Common pin - in case of switching contacts connected to relay housing

PF / PO Powered outputs usage



Mechanical dimensions of IP WatchDog2 Lite

The device is in metal box with option to mount on wall or DIN rail.



Technical parameters

IP WatchDog2 Industrial

Ethernet port	
+ Interface	RJ45 (10BASE-T / 100BASE-Tx)
+ Compatibility	Ethernet: Version 2.0/IEEE 802.3
+ Supported protocols	IP: ARP, TCP/IP, NVT, RFC2217, UDP/IP, SNTP

Serial port 1 – Channel 1	
+ Data bites	8
+ Stop bity	1
+ Parity	None
+ RS-232 interface	RxD,TxD, GND

Environment parameters	
+ Operation temperature	-30°C to +85°C
+ Storage temperature	-5 to +75 °C
+ Relative humidity	5 to 95 % (non-condensing)

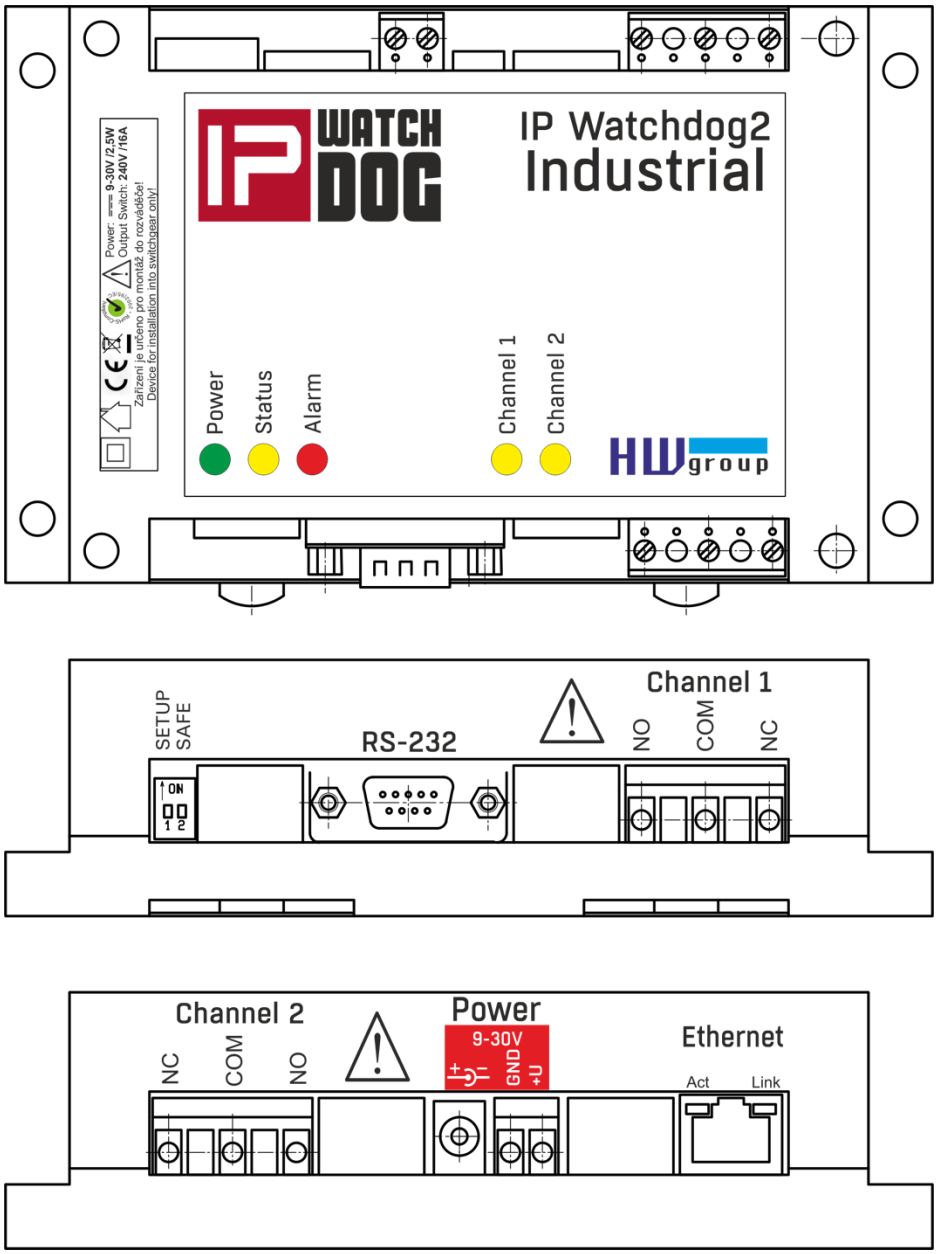
Mechanical construction	
+ Mechanical construction	Metal, table construction with external wall bracket, DIN rail or Rack
+ Dimensions	100x94x31 / 260g
+ EMC	FCC Part 15, Class B, CE - EN 55022, EN 55024, EN 61000

Power Input	
+ Port	POWER 9-30V DC
+ Type	Main device power input (typically 250 mA) + Power Out
+ Connector	Jack (barrel, inner 2.5 mm outer 6.3 mm), Terminal Block

Power Output	
+ Voltage	Power OUT = Power In
+ Current	Max. Power Adaptor minus 250mA or 1000mA
+ Connector	Terminal Block

Connectors of the IP WatchDog2 Industrial

Individual connectors and control elements as well as connection of the relays is shown on the picture below:



LED

- **Power (Green)** - lights, if connected and the device is working
- **Status (Yellow)** - blinks when signal is accepted from the monitored device, blinking quickly when being upgraded
- **Alarm (Red)** - lights, if some of device is unavailable and IP WatchDog2 is performing reset
- **Channel1/Channel2** - lights when channel is switched (reset or manual switch)

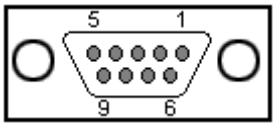
DIP switches

- **Setup** - is used to reset the device to the default configuration, if switched when the power supply is
- **Safe** - for manufacturer purposes only

Outputs Channel1 / Channel2

Description terminal board		
Pin	**Power**	**Function description**
NC	*Normally Close*	In Idle state this pin is connected with the appropriate COM pin
NO	*Normally Open*	In Reset state this pin is connected with the appropriate COM pin
COM	*Common*	Common pin - in case of switching contacts connected to relay housing

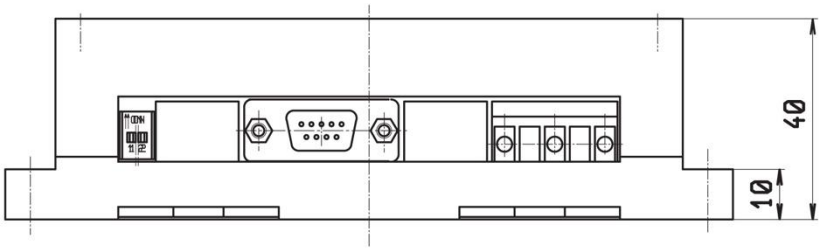
Serial - DB9M

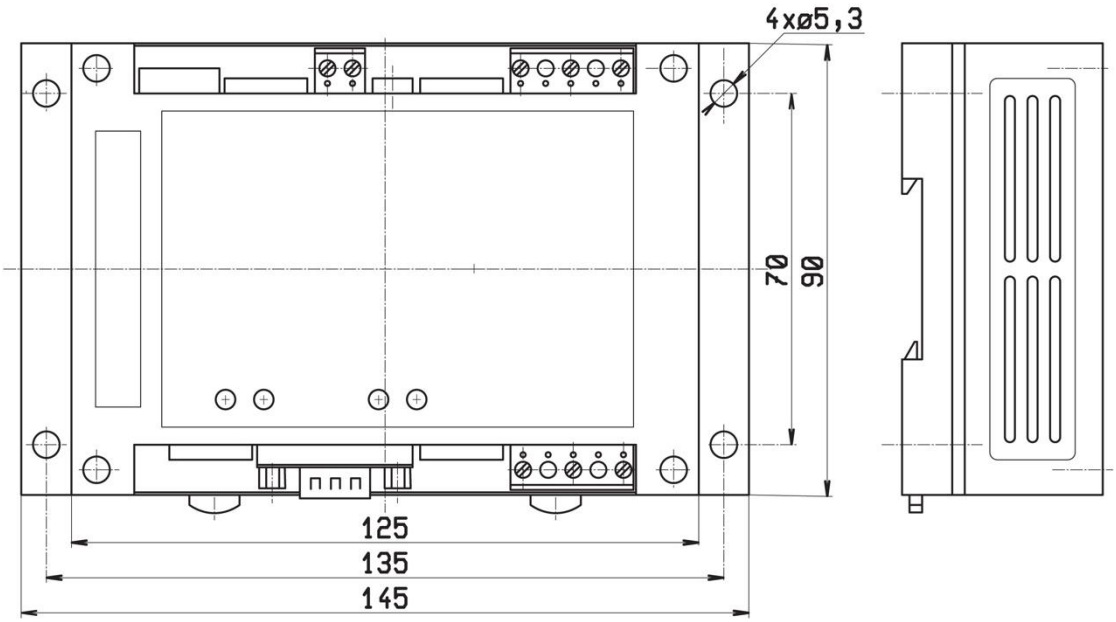


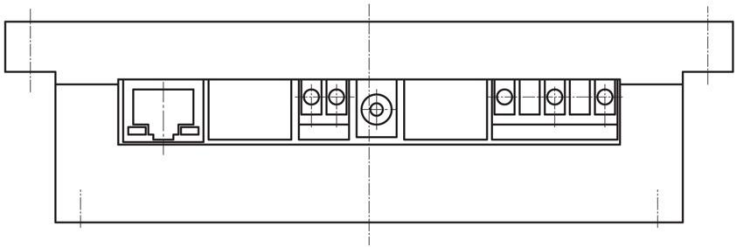
Connector DB9M (RS-232)				
	Channel1	Channel2		
1	DCD		IN	Unused
2	**RxD**		IN	Receive Data
3	**TxD**		OUT	Transmit Data
4	DTR		OUT	Unused
5	**GND**		---	System Ground
6	DSR		IN	Unused
7*	**RTS**		OUT	Clear to Send, (Receive Data)
8		RxD	IN	Request to Send
9	RI		IN	Unused

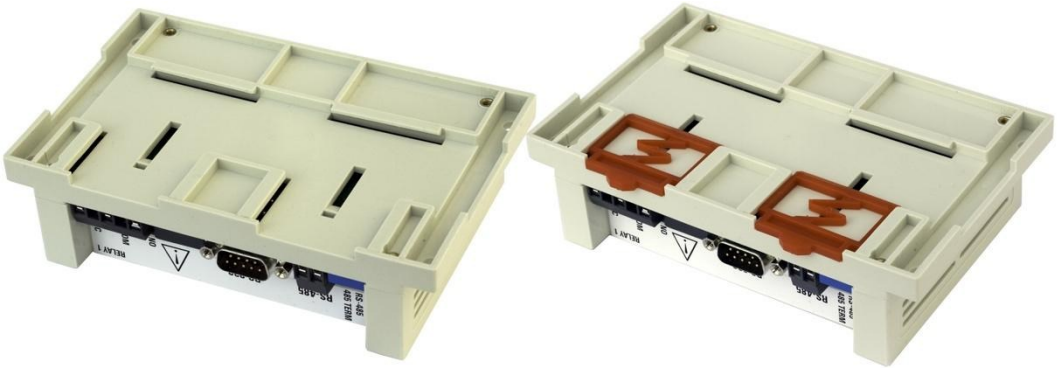
Mechanical dimensions IP WatchDog2 Industrial

The device is in solid box with option to mount on wall or DIN rail.









First steps

In this chapter, you will learn how to connect the IP WatchDog2 to your PC or company network, how to set it up and put it into service, and how to perform some basic operations.

Device connection

The following procedure is recommended for quick setup of the device. Detailed description of all parameters and commands can be found in chapter called *"Parameters description".*

Cable connection

- Set switches from DIP1 and DIP2 into OFF position.
- Connect IP WatchDog2 to the Ethernet 10/100 Mbit network.
- Connect the supplied power adaptor to power grid and plug the connector of the power adaptor into power connector of the IP relay. *The Power* LED indicator should light up.

If the Ethernet connection is OK, the LINK indicator should light up.

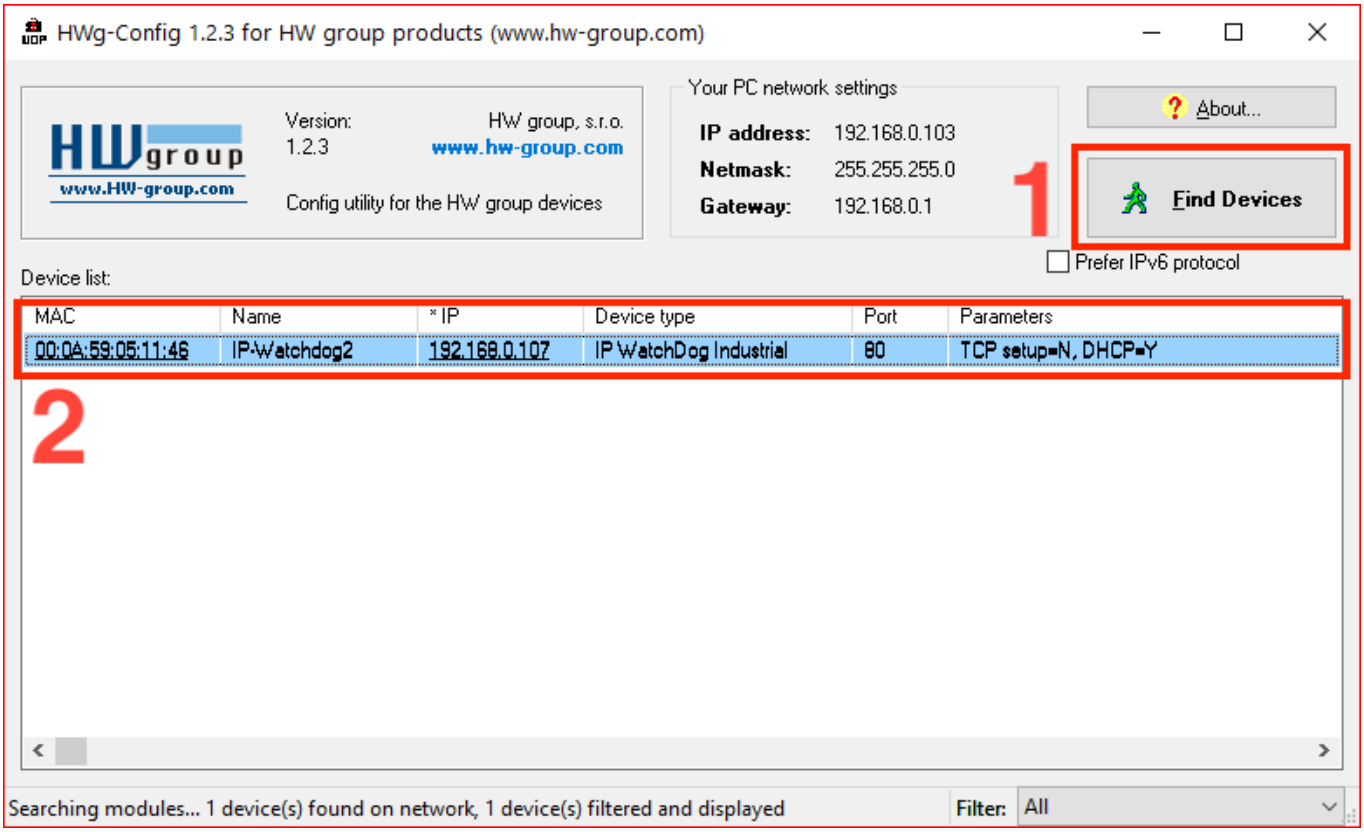
Primary configuration of Ethernet parameters

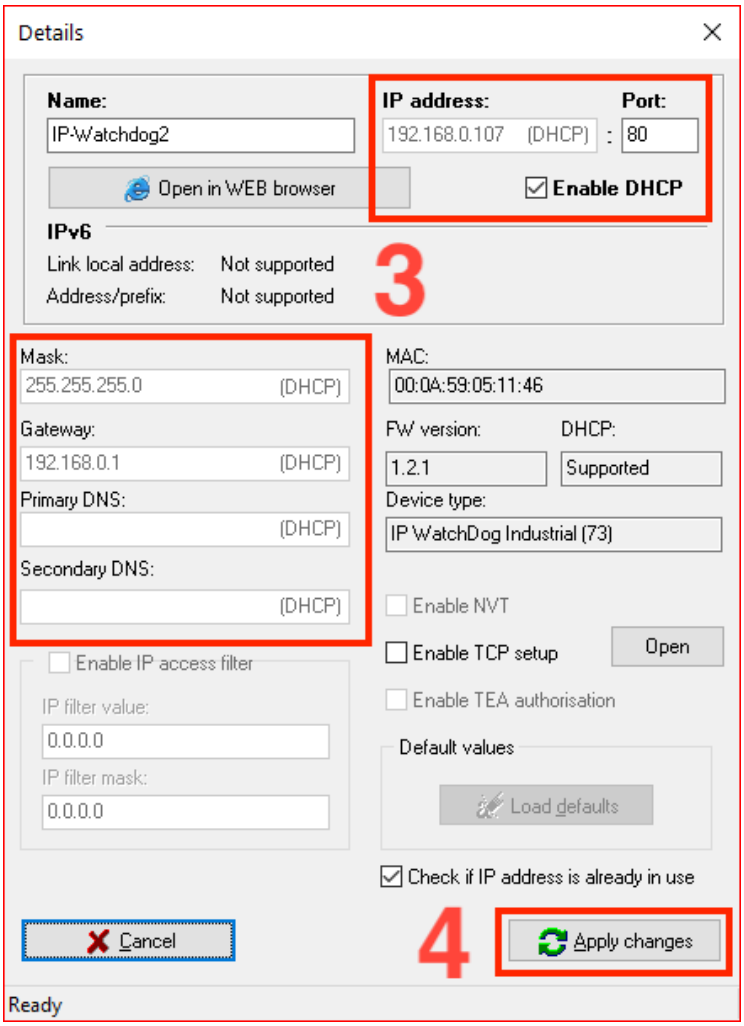
The initial LAN configuration of the IP WatchDog2 device (IP address, network mask, and gateway) can be read or defined using **HWg-Config** (for MS Windows). The PC running the software and the device must be on the same LAN segment..

UDP Setup – Finding the Device via UDP

- Launch the HWg-Config program (download from www.HW-group.com).
- In the app, click "**Find Modules**" (Step 1, see picture). The device's MAC address should appear in the left column.
- Click on the **MAC address** (Step 2). The configured device parameters will appear in a new window named "Details."
- Click on the **IP address** (Step 2) to open the device's web interface in your browser.

Note:
If you wish to change these basic parameters (at a minimum, the IP address, port, mask, and gateway must be set), enter the desired values into the appropriate fields (Step 3), and press ***"Apply Changes."***
(Step 4) When manually entering the IP address and gateway, it is also necessary to ***disable DHCP*** *by unchecking the* ***"Enable DHCP"*** *field.*

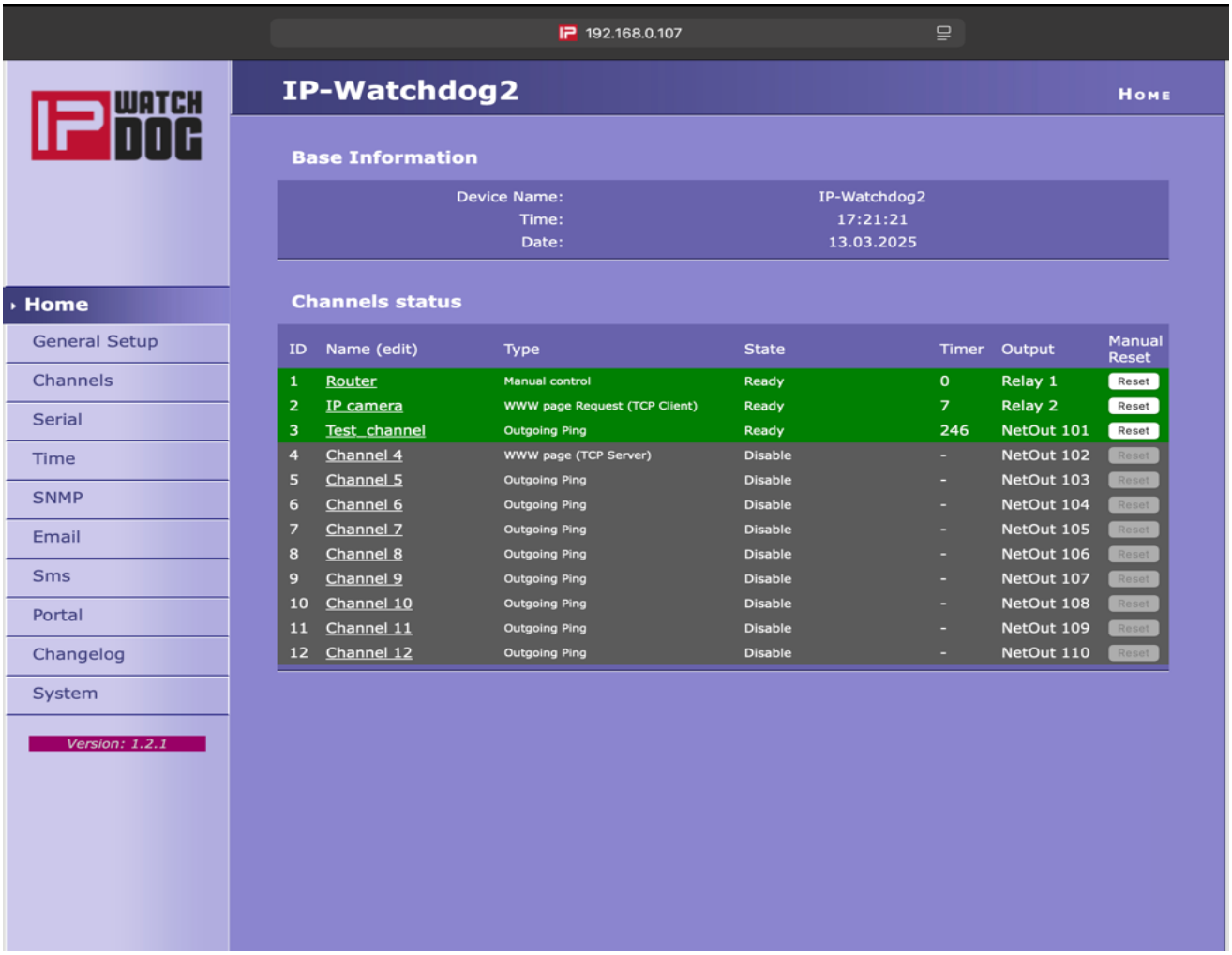

HWg-Config 1.2.3 for HW group products (www.hw-group.com)
Version:
1.2.3
HW group, s.r.o.
www.hw-group.com
Config utility for the HW group devices
Your PC network settings
IP address: 192.168.0.103
Netmask: 255.255.255.0
Gateway: 192.168.0.1
1
About...
Find Devices
Prefer IPv6 protocol
Device list:
MAC
Name
* IP
Device type
Port
Parameters
00:0A:59:05:11:46
IP-Watchdog2
192.168.0.107
IP WatchDog Industrial
80
TCP setup=N, DHCP=Y
2
Searching modules... 1 device(s) found on network, 1 device(s) filtered and displayed
Filter:
All


Details
Name:
IP-Watchdog2
IP address:
Port:
192.168.0.107 (DHCP)
80
Open in WEB browser
Enable DHCP
IPv6
Link local address: Not supported
Address/prefix: Not supported
3
Mask:
255.255.255.0 (DHCP)
Gateway:
192.168.0.1 (DHCP)
Primary DNS:
(DHCP)
Secondary DNS:
(DHCP)
MAC:
00:0A:59:05:11:46
FW version:
DHCP:
1.2.1
Supported
Device type:
IP WatchDog Industrial (73)
Enable NVT
Enable TCP setup
Open
Enable TEA authorisation
Enable IP access filter
IP filter value:
0.0.0.0
IP filter mask:
0.0.0.0
Default values
Load defaults
Check if IP address is already in use
Cancel
4
Apply changes
Ready

Device web interface

Enter the IP address of the device into your WWW browser. The Main Page of www interface will appear.

In the upper section of the window that opens, you will see the Base Information section, displaying the device name, current time, and date. Below this overview is a section called Channels Status, which provides an overview of all the channels. The left sidebar contains all the configurable options for your WatchDog. Detailed information on configuration methods over www interface can be found in the chapter called **Device configuration via WWW**.



Manual restart

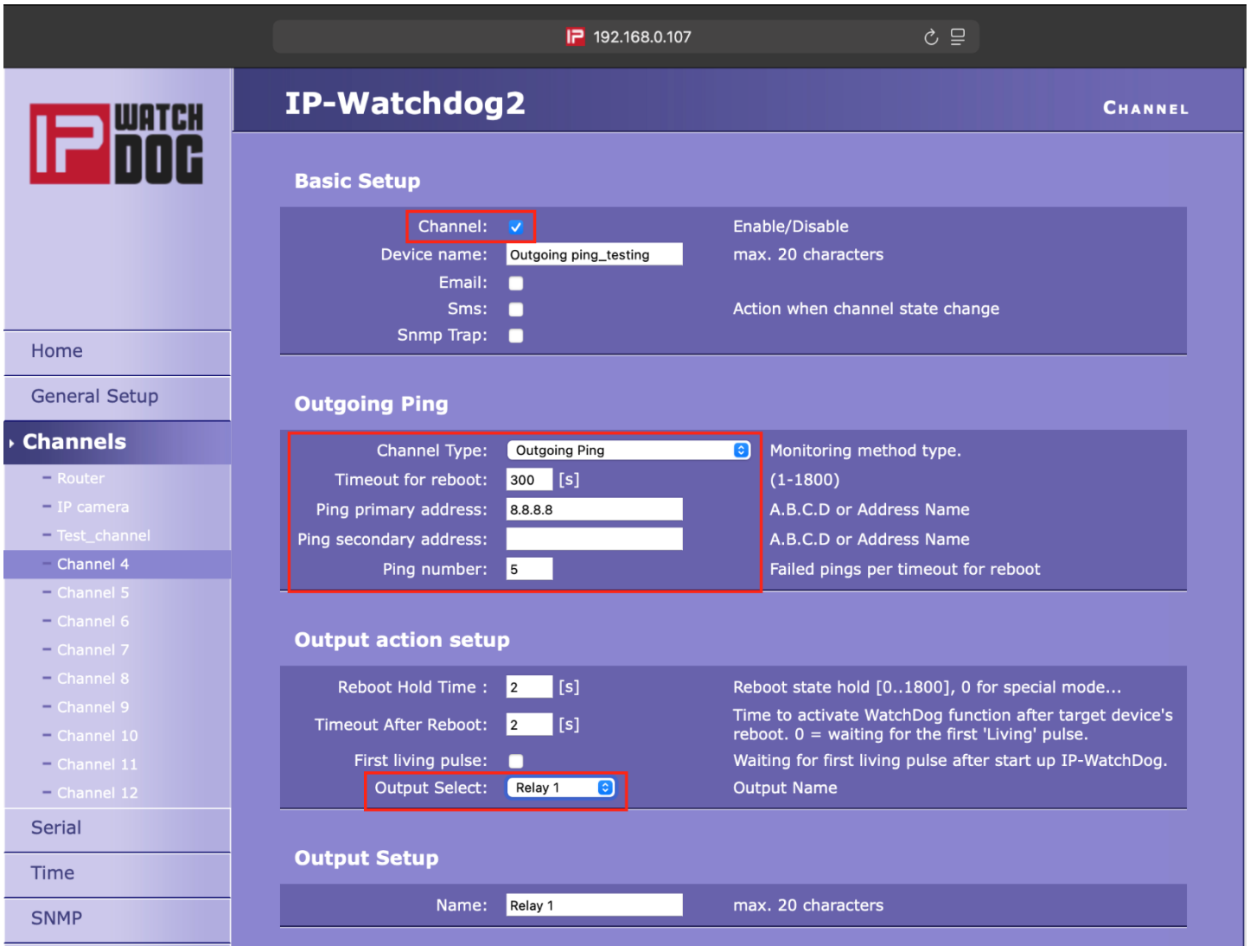
The first thing you can easily try is manually resetting **Channel 1**. Simply click the **Reset** button, and you should see a brief change in the channel status.

Outgoing ping

Another simple method for setting up a channel is using an **outgoing ping**. For this method, you need a WatchDog device connected to the LAN and access to the Internet. In the channel configuration, set the **Channel Type** to *Outgoing Ping*.

Set the **Ping Target** to 8.8.8.8 (Google's public DNS server). Configure the **Timeout for Reboot**, which is the time the WatchDog waits for a ping response before triggering a restart. The **Ping Number** defines how many ping attempts are made during the Timeout period.

For the output, select either **Relay 1** or **Relay 2**. Leave the remaining parameters at their default values.



Once these parameters are set, disconnect your router from the Internet. This should cause the ping to the IP address 8.8.8.8 to fail, and after the timeout period, the IP WatchDog will perform a reset.

Portal (based on SensDesk Technology)

The Portal is a server running a platform based on SensDesk Technology for remote monitoring. It can operate either as a public cloud service or be installed on-premise within a local network.

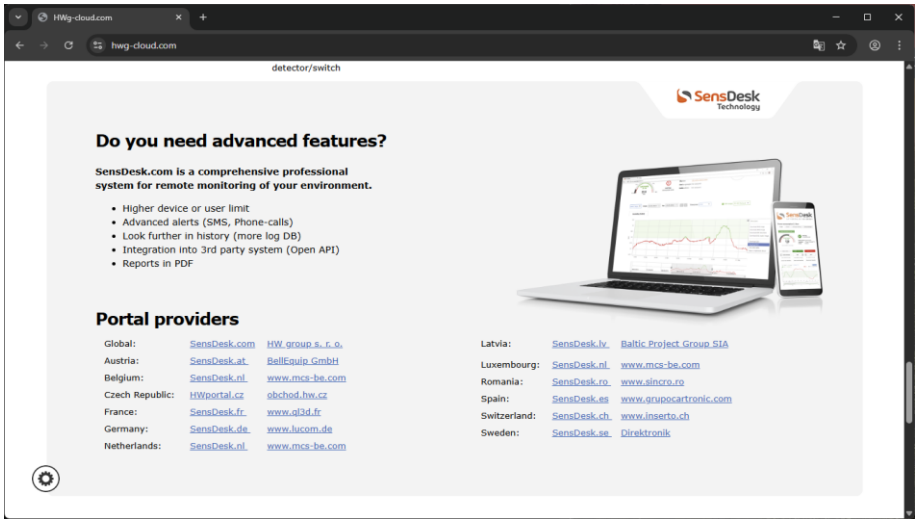
Several providers offer this type of Portal with various configurations:

- Free trial accounts + paid services (e.g., **hw-portal.cz**)
- Free accounts with limited features (e.g., **HWg-cloud.com**)
- Paid accounts only (e.g., **SensDesk.com**)

Currently, there are more than 50 installations of SensDesk Technology-based Portals in different countries and companies.

Portal Configurations May Vary In

- Type of alerts: Email only / SMS / Phone calls
- Single-user vs. multi-user permission groups settings
- Maximum number of devices per company account
- Data retention period (how long historical data is stored)
- Response time for control output actions
- Number of reports and multi-graphs that can be generated
- Compatibility with the HWg Mobile App



Why Connect an IP WatchDog to the Portal?

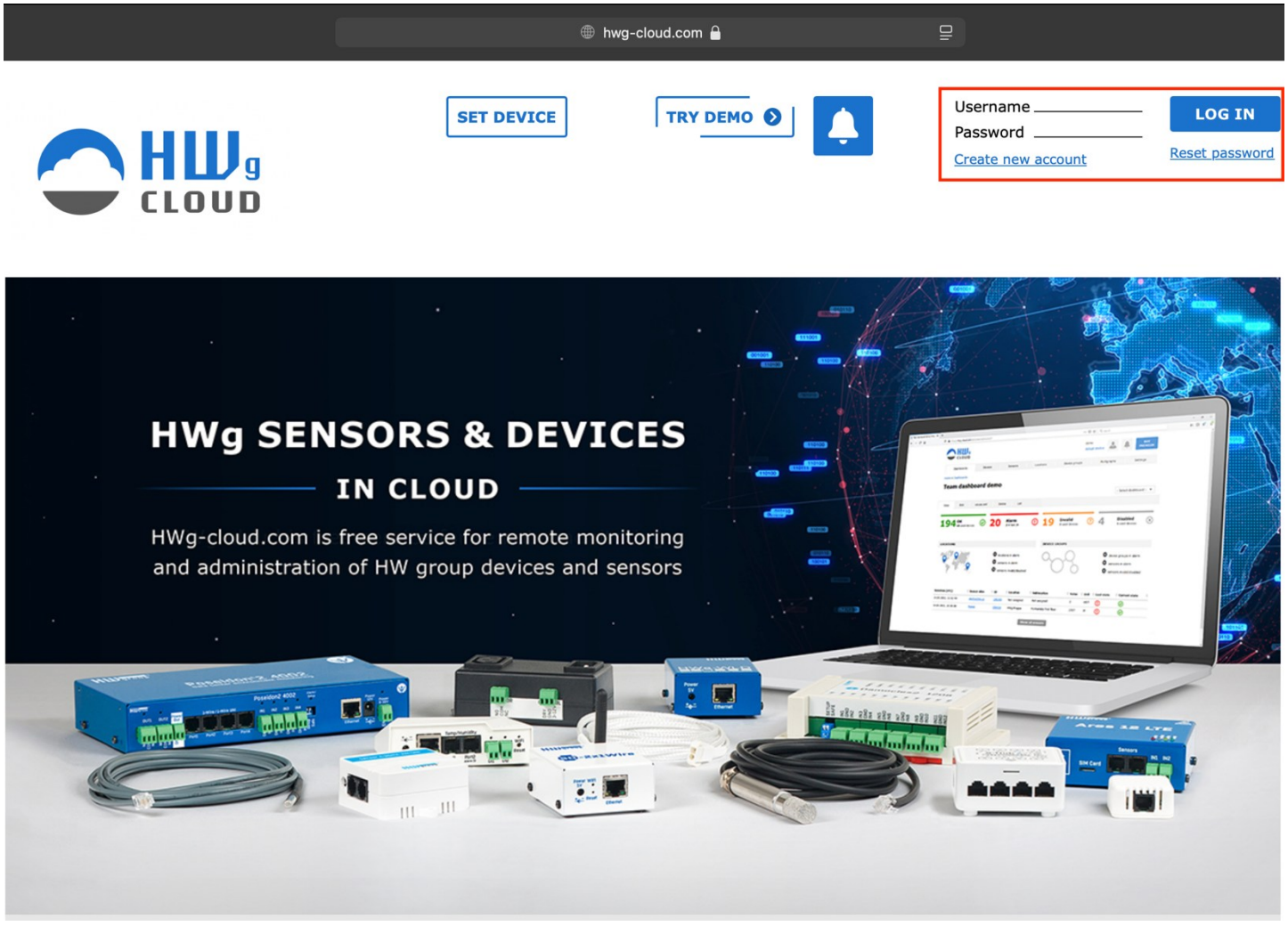
1) **Long-term reliable email lerting**
   Email alerts through public SMTP servers are outdated.
   Sending emails via public SMTP servers (like Gmail, Yahoo, or GMX) was acceptable in 1993—but not in 2025 and beyond. It's not a long-term reliable solution. Use portal-based alerting **instead of public SMTP servers**. HW group offers HWg-cloud.com as a free service.
2) **Device Invalid Alert via the Portal**
   The Portal can automatically notify you (via email) if the WatchDog device becomes unreachable for a certain period.
3) **Web-based access to control outputs remotely**
   The Portal website is always accessible, allowing you to remotely restart any WatchDog output from anywhere, anytime.
4) **Centralized alert management**
   With the Portal, it's easy to manage all alerts in one place.
   If the infrastructure manager leaves the company, will someone really update the alert settings on every individual device? With the Portal, it's simple and centralized.

Connecting IP Watchdog to the HWg-cloud

1) Creating an Account on HWg-Cloud

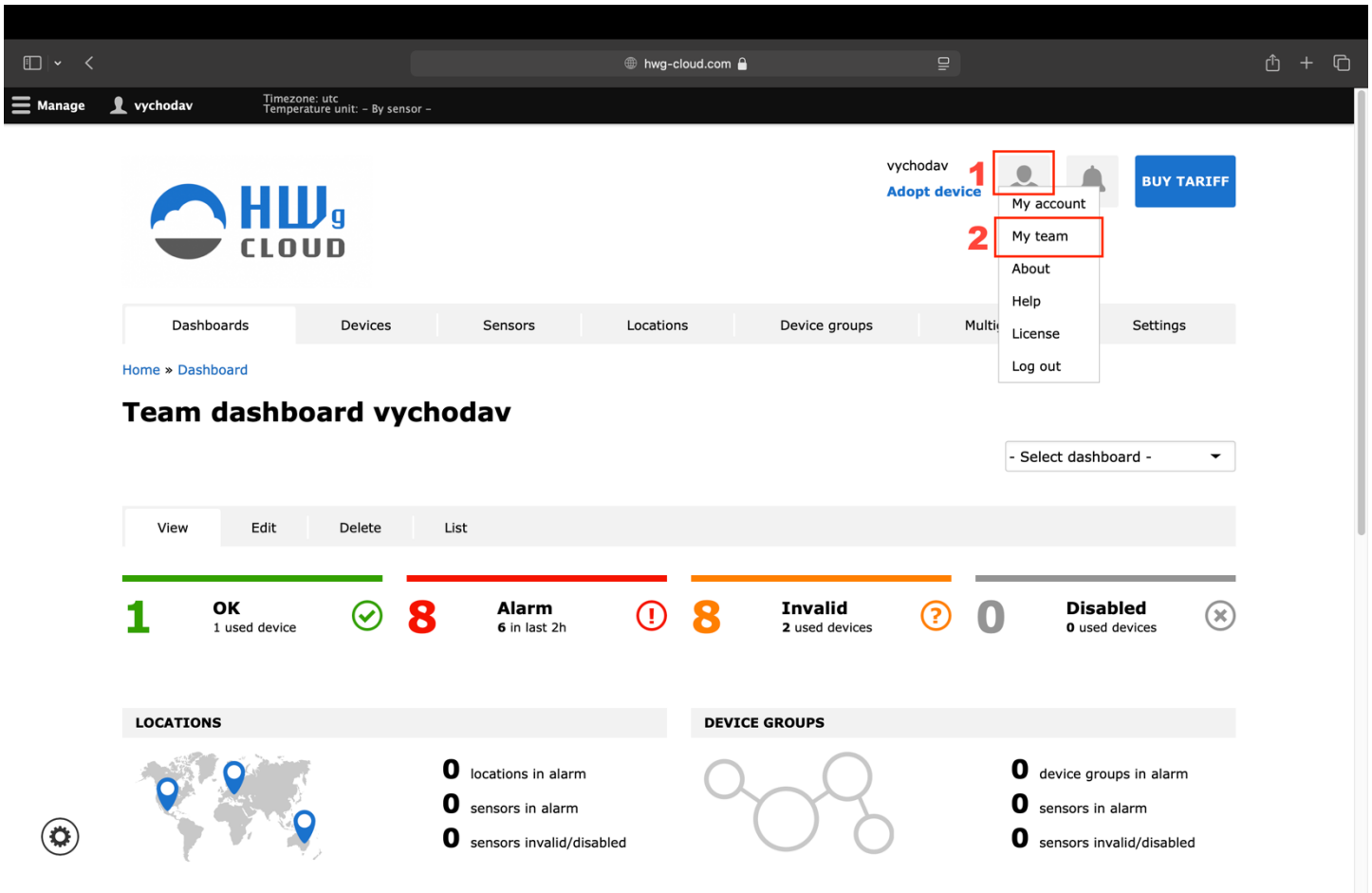
If you already have a user account, simply enter your login details — the device will be automatically assigned to your account.

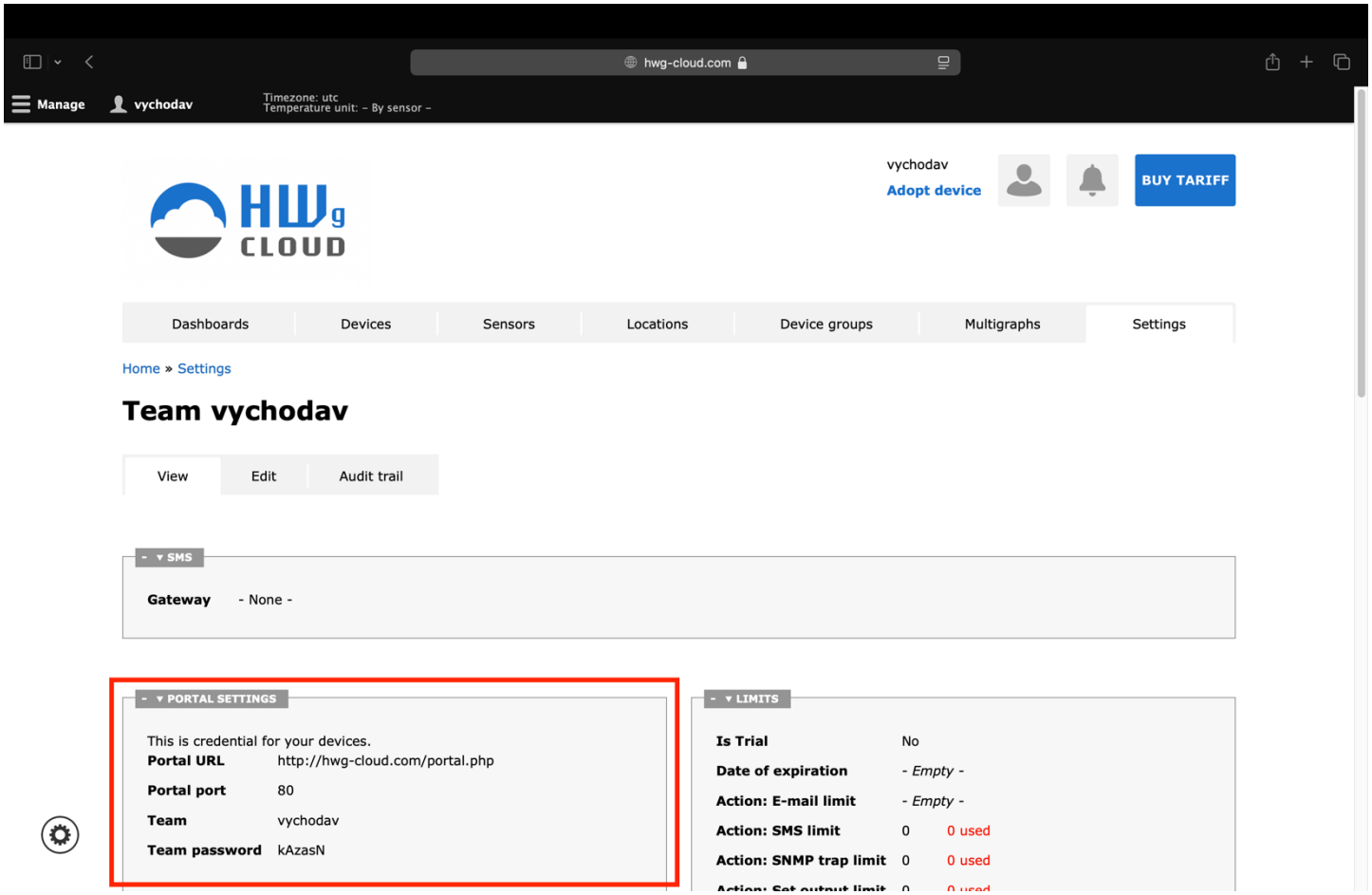
If you do not have an HWg-Cloud account yet, click the **Register** button to display the registration form.



2) Accessing Portal Settings

In your HWg-Cloud account, click on the **person icon**, then select **"My Team"**. On this page, in the **Portal Settings** box, you will find all the information required to configure the IP WatchDog web interface.




hwg-cloud.com
Manage
vychodav
Timezone: utc
Temperature unit: – By sensor –
vychodav
Adopt device
BUY TARIFF
HWg CLOUD
Dashboards
Devices
Sensors
Locations
Device groups
Multigraphs
Settings
Home » Settings
Team vychodav
View
Edit
Audit trail
SMS
Gateway - None -
PORTAL SETTINGS
This is credential for your devices.
Portal URL http://hwg-cloud.com/portal.php
Portal port 80
Team vychodav
Team password kAzasN
LIMITS
Is Trial No
Date of expiration - Empty -
Action: E-mail limit - Empty -
Action: SMS limit 0 0 used
Action: SNMP trap limit 0 0 used

3) Configuring Portal Settings in the Device

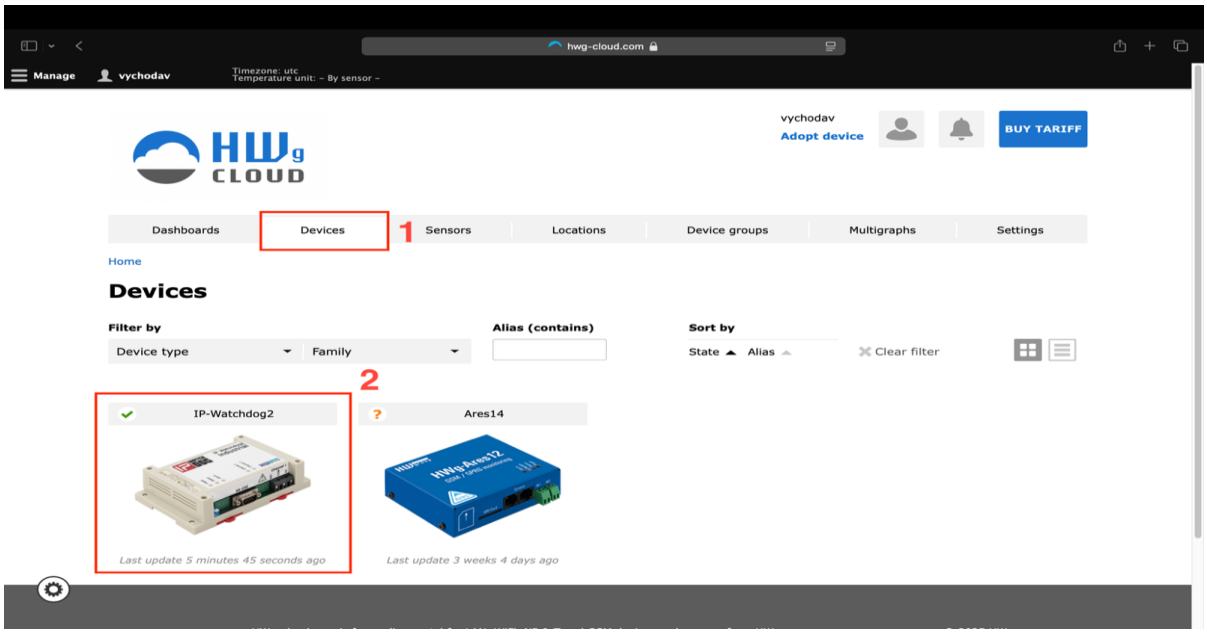
Go to the device's web interface as described earlier in this chapter. In the left sidebar, select **Portal**, and enter the credentials from your Portal (HWg-Cloud/SensDesk/Other) in the **Portal** section.

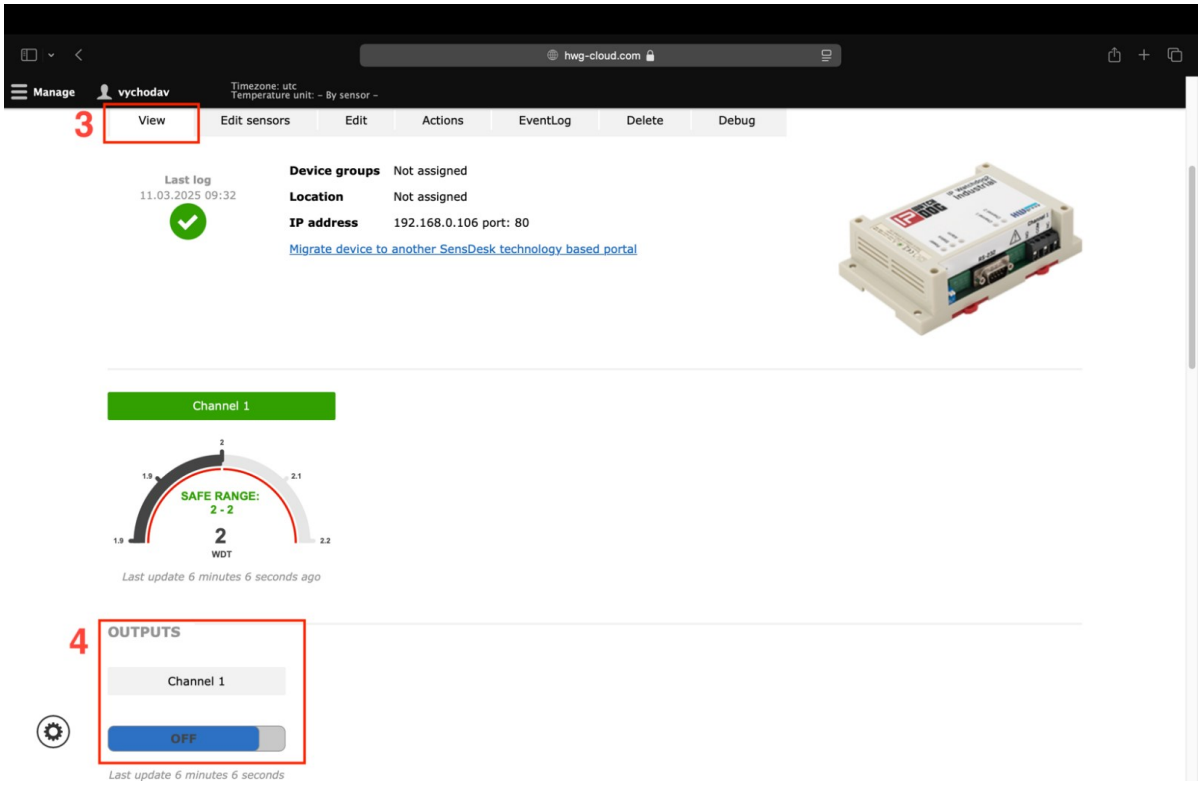
4) Check the Connection to the Portal Manually

Manually check the connection to the portal. The device should appear in the portal, and a link to your HWg-Cloud account will be displayed in the **Portal Message** section.

Manual restart from HWg-cloud portal

Using the HWg-Cloud portal, you have the option to manually restart a device connected to the WatchDog via its output. This can be done from the **device detail view** within the portal.

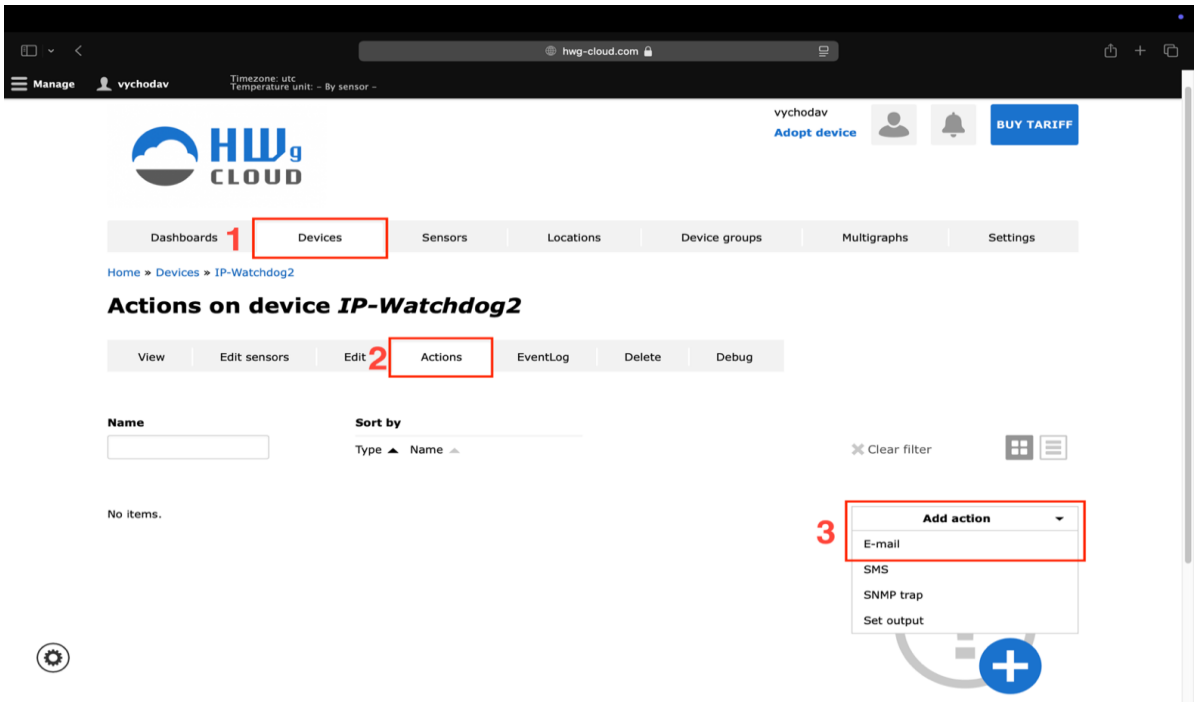


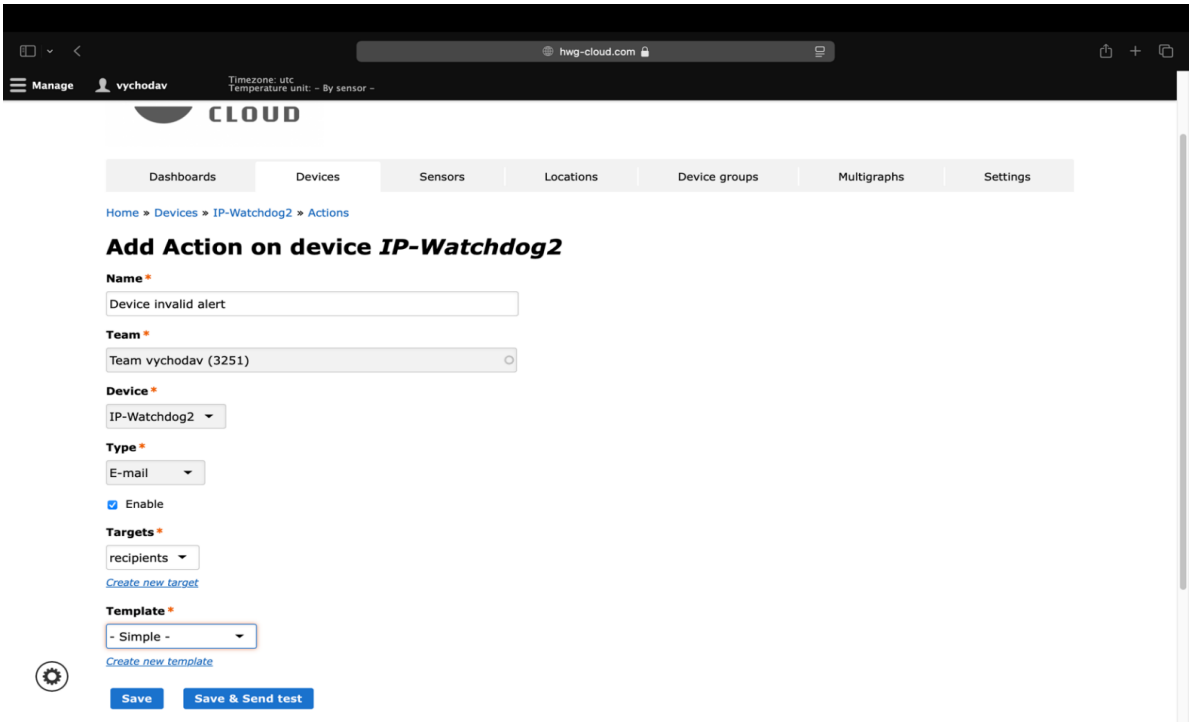


Alerting via HWg-cloud portal

Another important feature provided by the portal is **alerting**. This includes alerts for **channel status changes** as well as the equally important **device invalid alert**, which is triggered when your device becomes unreachable.

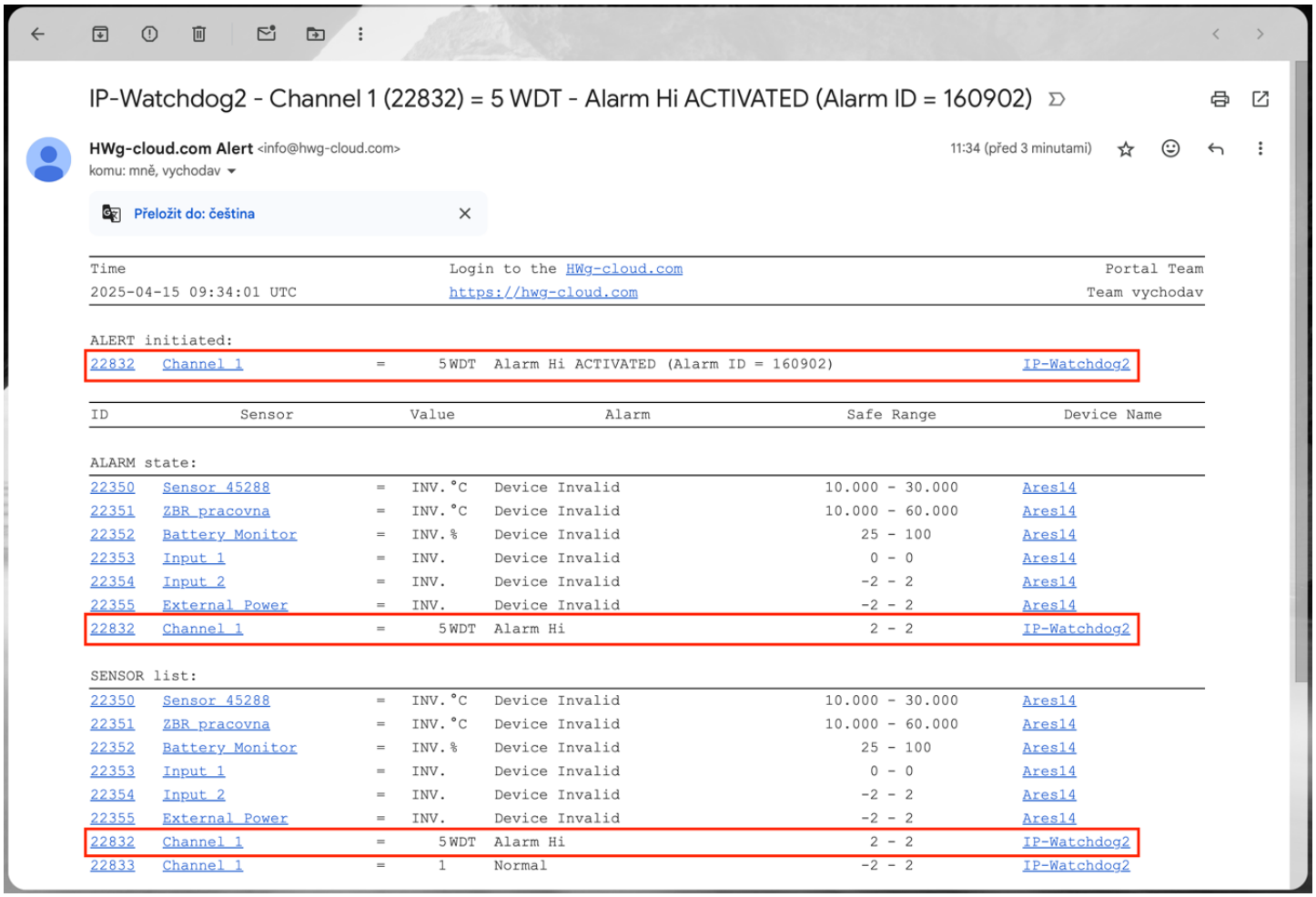
The **device invalid alert** can only be configured through the portal. To set it up, follow these steps:





Output restarted email alert example

The IP WatchDog device restarts the output autonomously. However, an email notification about the "Restart occurred" event can be sent from the portal.
Below is an example of an Outgoing Ping-based restart.



IP-Watchdog2 - Channel 1 (22832) = 5 WDT - Alarm Hi ACTIVATED (Alarm ID = 160902)

HWg-cloud.com Alert <info@hwg-cloud.com> 11:34 (před 3 minutami)
komu: mně, vychodav

Přeložit do: čeština

Time	Login to the HWg-cloud.com	Portal Team
2025-04-15 09:34:01 UTC	https://hwg-cloud.com	Team vychodav

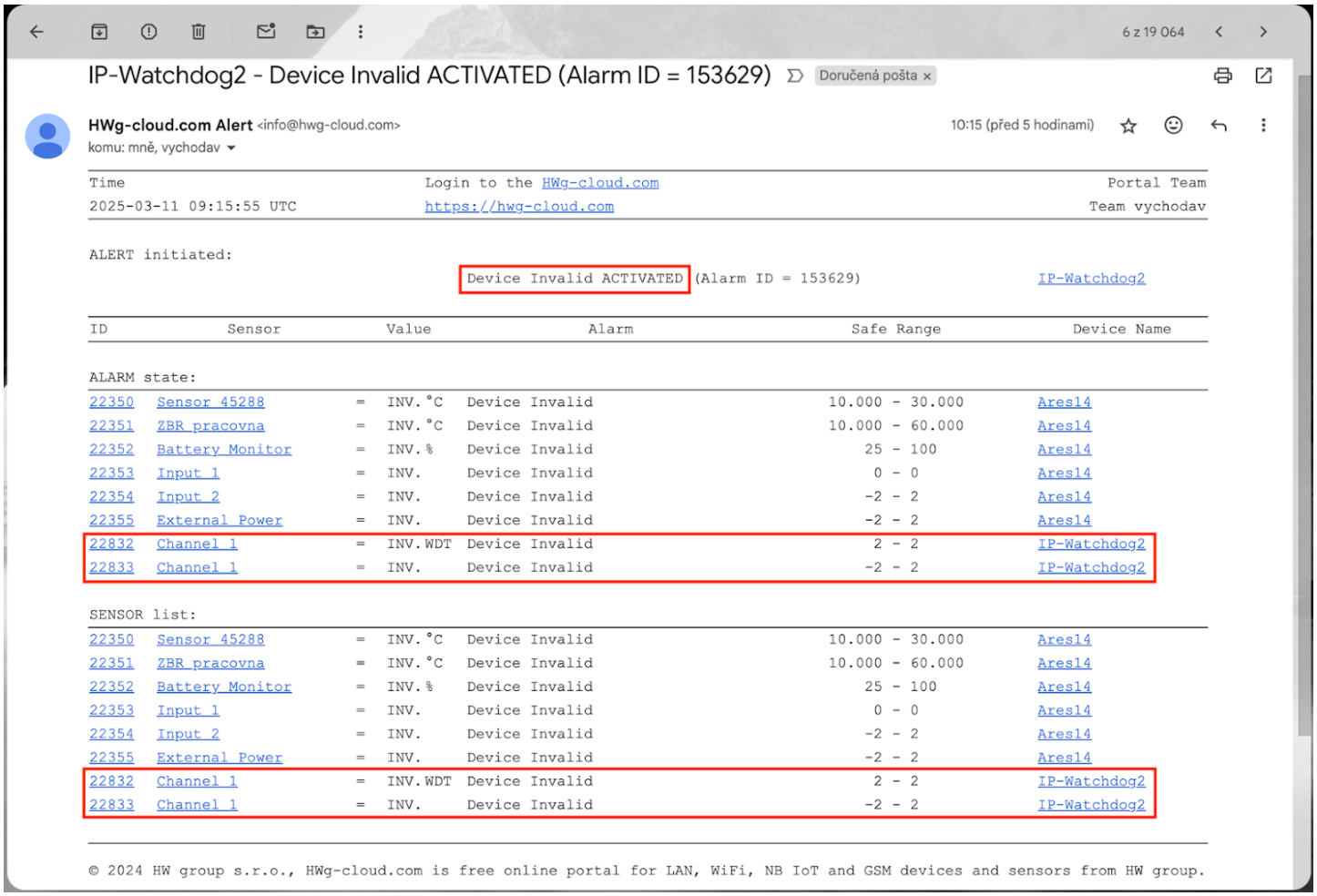
ALERT initiated:

22832	Channel 1	=	5 WDT	Alarm Hi ACTIVATED (Alarm ID = 160902)	IP-Watchdog2

ID	Sensor	Value	Alarm	Safe Range	Device Name
ALARM state:					
22350	Sensor 45288 =	INV. °C	Device Invalid	10.000 - 30.000	Ares14
22351	ZBR pracovna =	INV. °C	Device Invalid	10.000 - 60.000	Ares14
22352	Battery Monitor =	INV. %	Device Invalid	25 - 100	Ares14
22353	Input 1 =	INV.	Device Invalid	0 - 0	Ares14
22354	Input 2 =	INV.	Device Invalid	-2 - 2	Ares14
22355	External Power =	INV.	Device Invalid	-2 - 2	Ares14
22832	Channel 1 =	5 WDT	Alarm Hi	2 - 2	IP-Watchdog2
SENSOR list:					
22350	Sensor 45288 =	INV. °C	Device Invalid	10.000 - 30.000	Ares14
22351	ZBR pracovna =	INV. °C	Device Invalid	10.000 - 60.000	Ares14
22352	Battery Monitor =	INV. %	Device Invalid	25 - 100	Ares14
22353	Input 1 =	INV.	Device Invalid	0 - 0	Ares14
22354	Input 2 =	INV.	Device Invalid	-2 - 2	Ares14
22355	External Power =	INV.	Device Invalid	-2 - 2	Ares14
22832	Channel 1 =	5 WDT	Alarm Hi	2 - 2	IP-Watchdog2
22833	Channel 1 =	1	Normal	-2 - 2	IP-Watchdog2

The Invalid Alert email example

When the device is disconnected from the Portal (connectivity failure / device power failure), the Portal itself can alert you for this situation by sending "**Device Invalid alert**".
It's sent by the Portal after 30-60 minutes from last communication with the device.



6 z 19 064

IP-Watchdog2 - Device Invalid ACTIVATED (Alarm ID = 153629) Doručená pošta ×

HWg-cloud.com Alert <info@hwg-cloud.com> 10:15 (před 5 hodinami)
komu: mně, vychodav

Time	Login to the HWg-cloud.com	Portal Team
2025-03-11 09:15:55 UTC	https://hwg-cloud.com	Team vychodav

ALERT initiated:

Device Invalid ACTIVATED (Alarm ID = 153629) IP-Watchdog2

ID	Sensor		Value	Alarm	Safe Range	Device Name
ALARM state:						
22350	Sensor 45288	=	INV. °C	Device Invalid	10.000 - 30.000	Ares14
22351	ZBR pracovna	=	INV. °C	Device Invalid	10.000 - 60.000	Ares14
22352	Battery Monitor	=	INV. %	Device Invalid	25 - 100	Ares14
22353	Input 1	=	INV.	Device Invalid	0 - 0	Ares14
22354	Input 2	=	INV.	Device Invalid	-2 - 2	Ares14
22355	External Power	=	INV.	Device Invalid	-2 - 2	Ares14
22832	Channel 1	=	INV. WDT	Device Invalid	2 - 2	IP-Watchdog2
22833	Channel 1	=	INV.	Device Invalid	-2 - 2	IP-Watchdog2
SENSOR list:						
22350	Sensor 45288	=	INV. °C	Device Invalid	10.000 - 30.000	Ares14
22351	ZBR pracovna	=	INV. °C	Device Invalid	10.000 - 60.000	Ares14
22352	Battery Monitor	=	INV. %	Device Invalid	25 - 100	Ares14
22353	Input 1	=	INV.	Device Invalid	0 - 0	Ares14
22354	Input 2	=	INV.	Device Invalid	-2 - 2	Ares14
22355	External Power	=	INV.	Device Invalid	-2 - 2	Ares14
22832	Channel 1	=	INV. WDT	Device Invalid	2 - 2	IP-Watchdog2
22833	Channel 1	=	INV.	Device Invalid	-2 - 2	IP-Watchdog2

© 2024 HW group s.r.o., HWg-cloud.com is free online portal for LAN, WiFi, NB IoT and GSM devices and sensors from HW group.

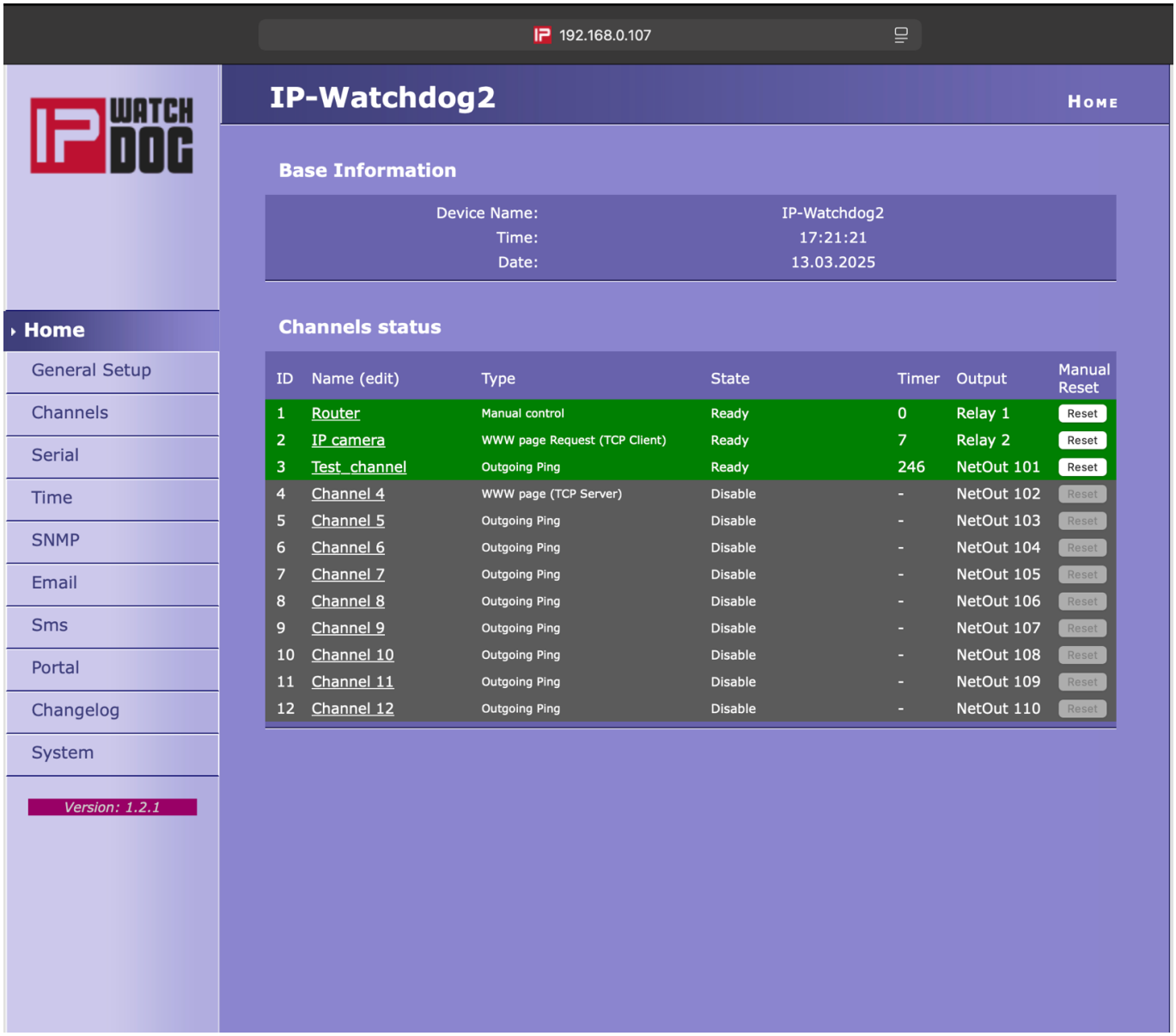
Device configuration via WWW

IP WatchDog2 contains a WWW interface allowing easy and detailed attendance of the device activity. The interface consists of four HTML pages which can be called by entering IP address of the device from your web browser.

IP WatchDog2 Main Page

After entering the IP address of the WatchDog2 into your web browser, the device's main page will appear. At the top of the window, you'll see the **Base Information** section, which displays the device name, current time, and date.

Below that is the **Channel Status** section, providing an overview of all channels. The **left sidebar** contains all the configurable options for your WatchDog2 device.



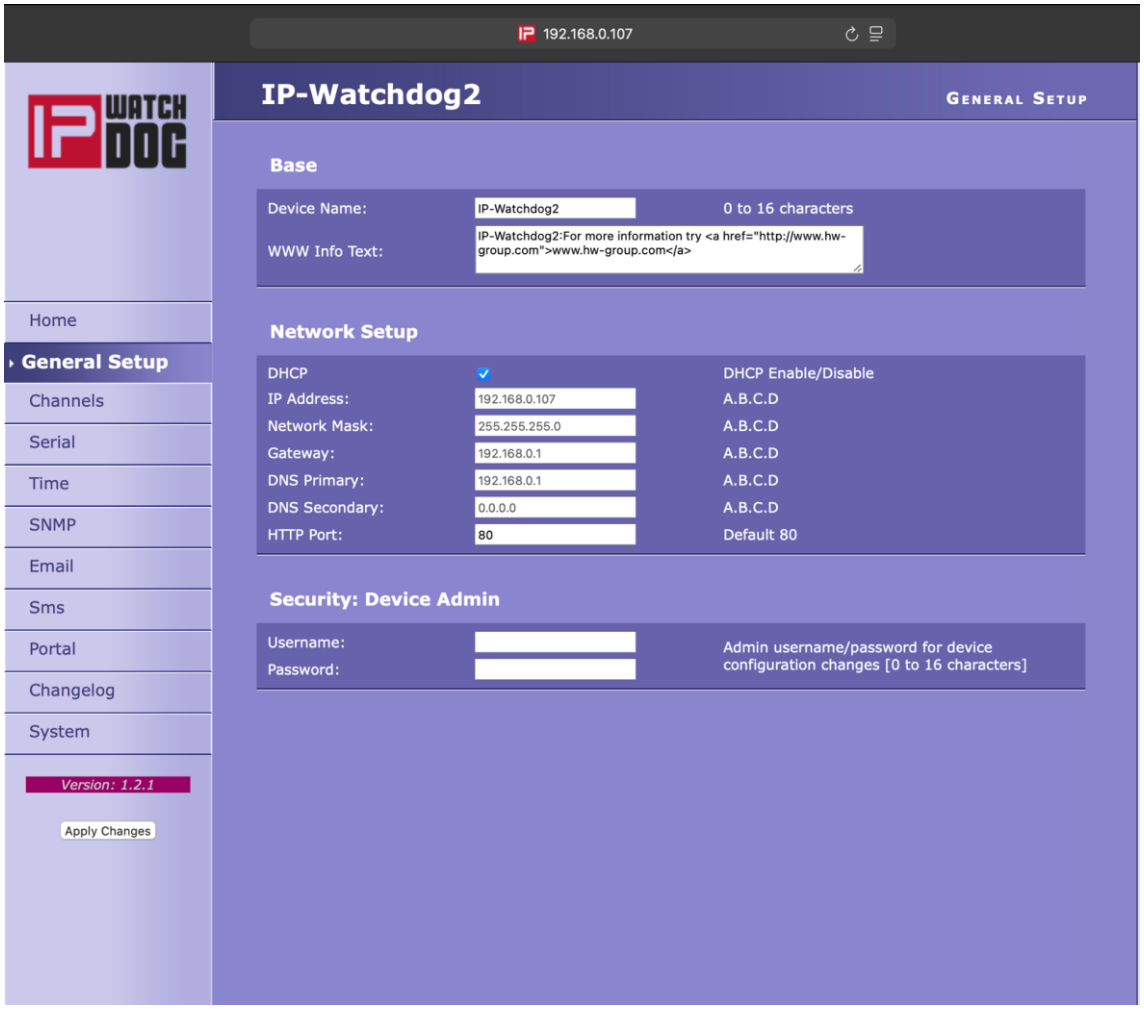
Section Base Information

- Device name – User name of the device. Can be modified in the tab General Setup
- Time – Machine time of the device – configuration can be changed in the tab Time. The valid time is usually taken from the Internet
- Date - Machine date of the device – configuration can be changed in the tab Time. The date is usually taken from the Internet

Section Channel Status

- *Name* – name of the monitored device (see *Channels*).
- *Type* – actual assigned function to the channel (see *Channels*):
  - ***Incoming Ping*** - IP WatchDog2 waits for ICMP command - PING Request from the defined address or range of addresses defined by IP and mask.
  - ***Outgoing Ping*** - IP WatchDog2 sends the ICMP command PING Request to the defined primary IP addresses and awaits response. If not received, the same command is sent to the secondary IP.
  - **WWW Page Request** - IP WatchDog2 waits for download HTML page from WWW server which is situated on defined IP address.
  - **WWW Page** - IP WatchDog2 waits requesting own WWW page from monitored device defined with IP address.
  - **Requested RS232 String** - IP WatchDog2 monitor dates on appropriate port RS-232 and awaits requested string.
- *State* – information about actual state of channel:
  - **Disable** (grey) – channel is deactivated. Allows manual operation of the relay through Channels
  - **Wait for Living pulse** (orange) - channel waits for arrival of the booting (first) pulse.
  - **Wait for pulse** (green) – channel waits for arrival refreshing pulse.
  - **Device Idle** (orange) – channel was reset. Awaiting first refreshing pulse.
  - **Reseting device now** (red) - channel being reseted.
  - **Device starting timeout** (orange) – waiting for the end of mandatory period after reset channel
  - **Manual Reset** (red) – channel was annulled manually
- **Config change** (green) – the process of changing the channel configuration
- *Timer* – Depends on the state of the channel – viz upper part – and determines how long the state will end.
- *Output* – Depended Output
- *Manual Reset* – button for manual Reset.

General Setup



Section Base

- *Device Name* – the name of the device (IP-WatchDog2) - allows to distinguish individual IP WatchDog2 in network.
  The device name can have a maximum of 16 characters.
- *WWW Info Text* – text of the footer WWW pages – suitable for contact information for example the data centre manager.

Section Network

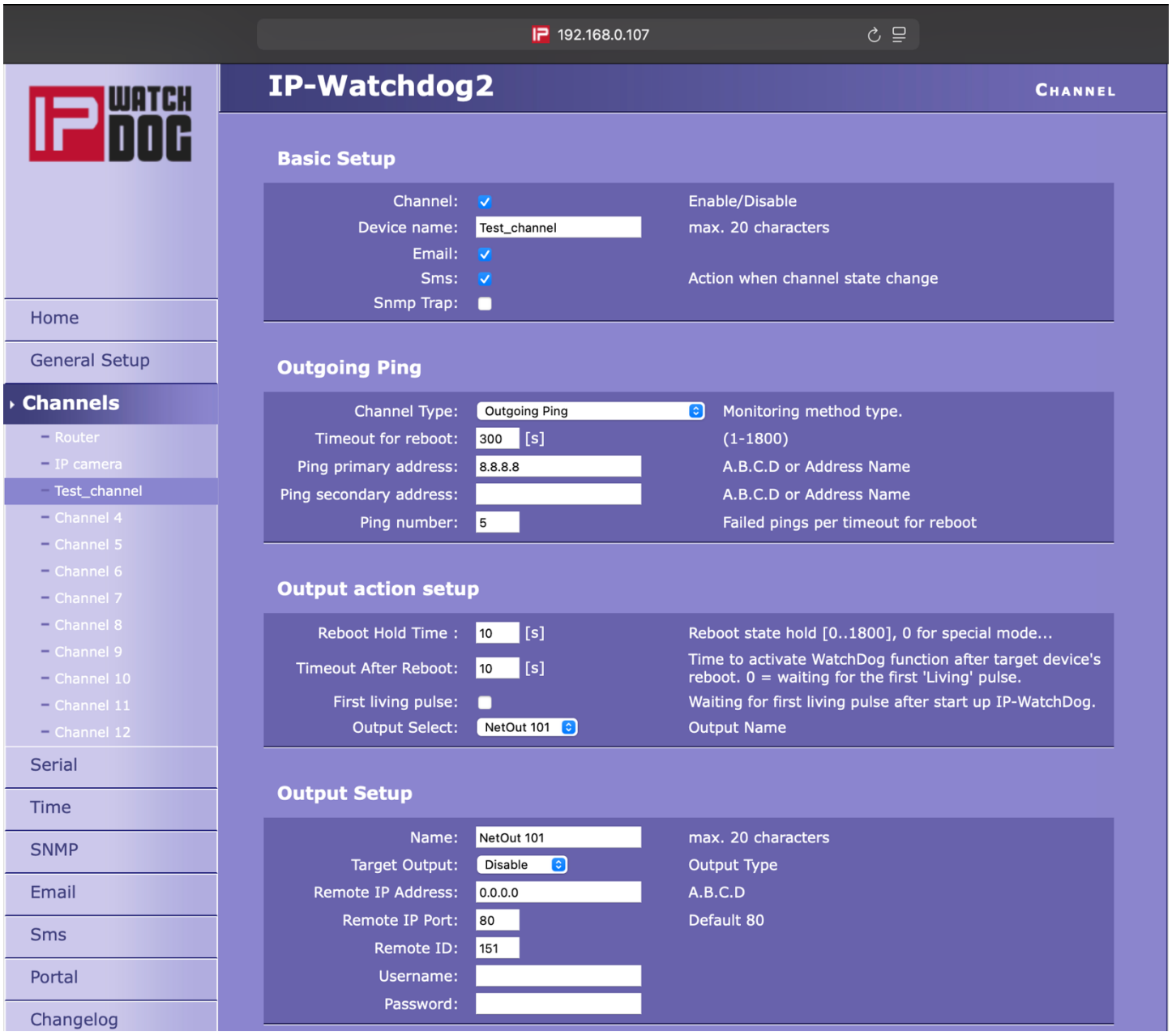
- *DHCP* – enable setting of an IP address with DHCP server, if available – switch on or off DHCP, depends on user and administrator needs.
- *IP Address* – IP address of IP WatchDog2 – assigned by the administrator of the network.
- *Network Mask* – mask of network – assigned by the administrator of the network.
- *Gateway* - IP address of default gateway - assigned by the administrator of the network.
- *DNS Primary / DNS Secondary* – IP address of DNS server – assigned by the administrator of the network.
- *HTTP Port* - number of port, where the built in WWW server is listening - change the number to have more IP WatchDog2 devices accessible from an external network via the router. Ask your network administrator about any changes. The default port is 80.

Security section: Device Admin

- Username / Password - username and password for security access to IP WatchDog2.

Channels

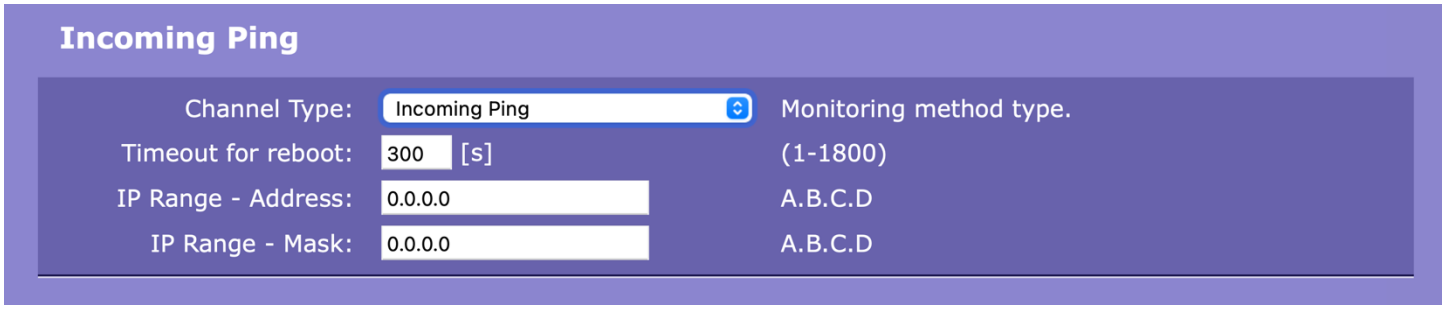
HTML pages *Channels* provides complete management of the monitoring channels.



Section Basic Setup

- Channel enabled/disabled - switch the channel on / off
- Channel name – name of the device. Makes configuring channels and solving the issues with monitored devices easier. Name can contain up to 20 symbols.
- Email – alert when channel state change
- SMS – alert when channel state change
- SNMP trap – alert when channel state change

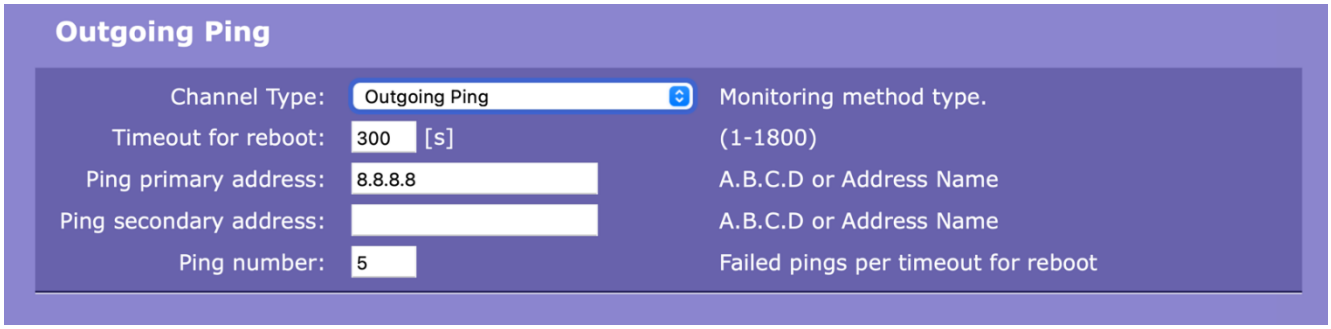
Section Incoming Ping (displayed depending on the Channel Type)



- **Timeout for reboot** – time interval that *IP WatchDog*2 waits for incoming PING before causing RESET.

- **IP range** - range of IP addresses defined by IP and mask, from which the receiving PING can be accepted.

Reset by Ping – Outgoing Ping (displayed depending on the Channel Type)

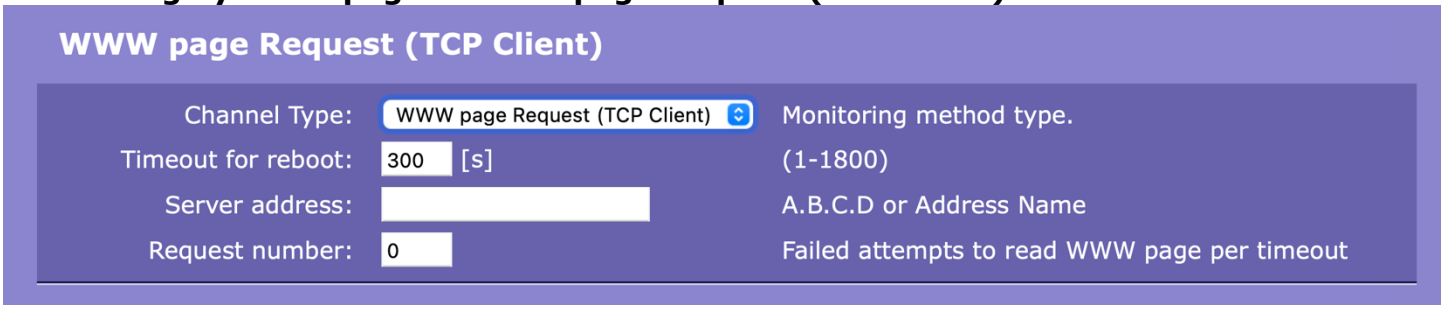


- **Timeout for reboot** – interval for sending requested PINGs.
- **Ping primary address** – primary address of the target device. The IP address and domain name can be specified.
- **Ping secondary address** – secondary address of the target device. The IP address and domain name can be specified. If only one device is monitored (or one address, the secondary address is left blank.
- **Ping Number** – number of sent PINGs in interval *Timeout for reboot*. At least one must have an answer or state *Reset* will follow.
- **Example**: The settings shown in the screenshot indicate that the IP Watchdog will ping the primary IP address every 360 seconds. (This interval is determined by dividing the total reboot timeout (3600 seconds) by the required number of ping failures (10), so 3600 / 10 = 360 seconds). If no successful ping response is received during the entire 3600 second period, the IP Watchdog will reboot the device.

Monitoring by HTML page – HTML page (TCP Server)

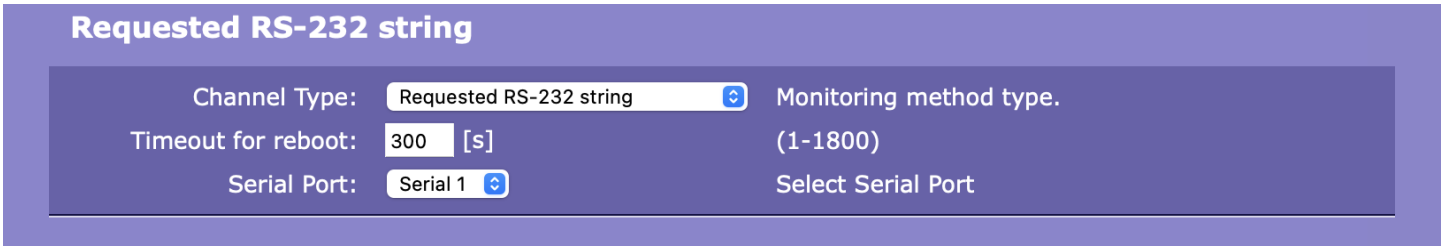
- **Timeout for reboot** – time interval that *IP WatchDog*2 waits for incoming PING before causing RESET.
- **Request Page** – WWW page http address that must be requested from the IP WatchDog2 by the remote device, or Reset will follow

Monitoring by HTML page – WWW page Request (TCP Client)



- **Timeout for reboot** – time interval that *IP WatchDog*2 waits for incoming PING before causing RESET. This parameter should be chosen with regards to the speed of the transmission line and server load.
- **Server address** - address of the target page (URL), which will be requested.
- **Request Number** – number of requests sent during the interval *Timeout for reboot.* At least one answer must come otherwise the *Reset* state will follow.

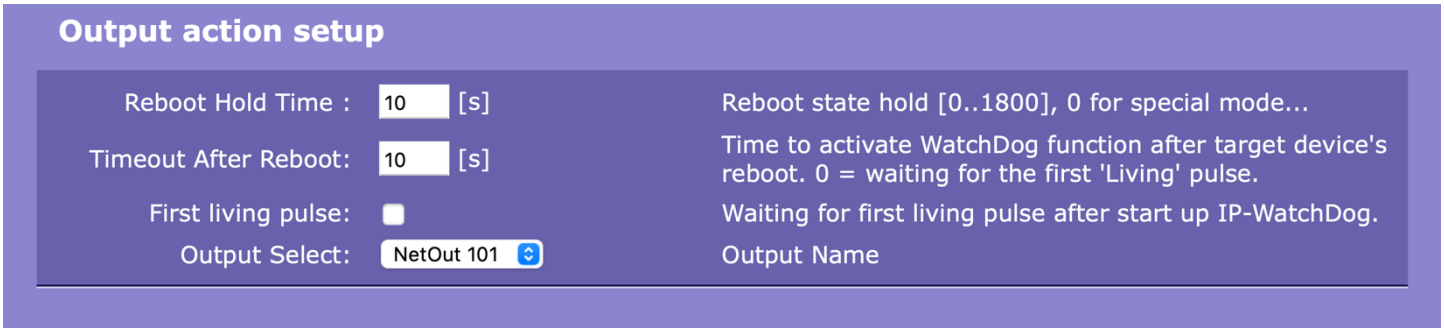
Monitoring by RS-232 String



- **Timeout for reboot** – time interval that *IP WatchDog*2 waits for incoming PING before causing RESET.
- **Requested string** - sets the monitored. HEX, DEC or ASCII format is available. Combining HEX, DEC and ASCII characters can be achieved using prefixes:
  - **$** - For HEX characters (example: $4F$4B$0D$0A or $4f$4b$0d$0a);
  - **#** - Escaped DEC characters – 3numbers (#079#075#013#010);
  - <string> - for ASCII characters.

Note: Characters can also be represented by ***?*** for any single character and * for any number of characters - for example if **IP-WTD** is set, *IP_WTD **$**10**$**13 is accepted.

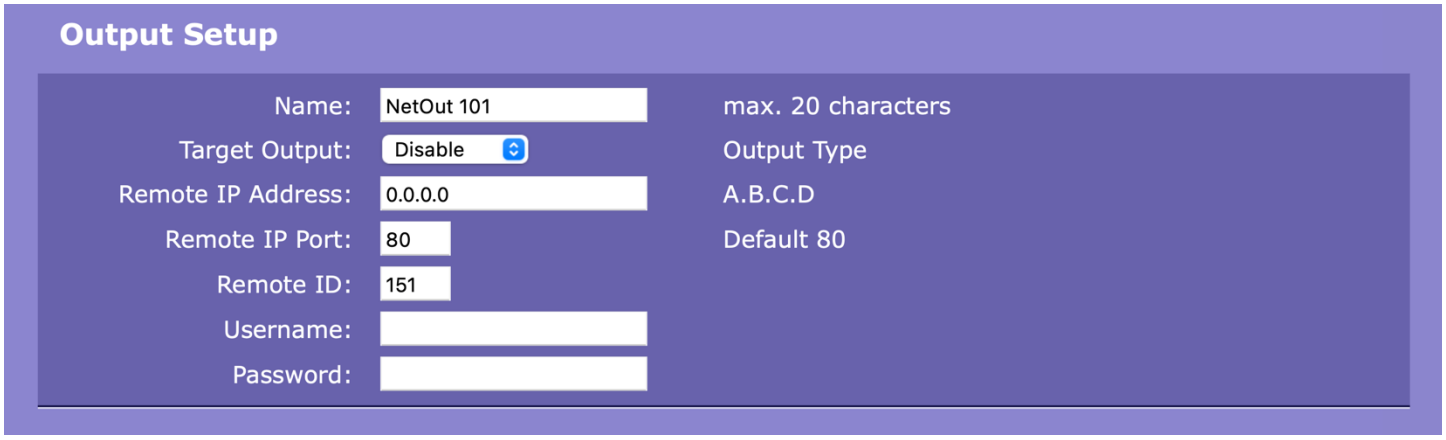
Section Output action Setup



- *Reboot Hold Time* – Reset length. Allows you to set the time when the channel (relay), is in reset status (manual and automatic) Interval can be in the range of 0-1800 seconds. If ***Reboot Hold Time* = 0**, then the Reset state lasts until the next refreshing impulse. This mode is designed to activate the backup device or identify the error state using other signalization means. Find more in the *Reboot Hold Time* - ***Application tips*** chapter.

- *Timeout After Reboot* – time interval that *IP WatchDog2* waits before causing other Reset after the previous one (or after first launch of the device), if monitored data are not received. The interval can be from in range of 0-1800 seconds. The "0" value causes device to wait for first incoming data from the monitored device.
- *First living pulse* – waiting for the arrival of the first data from the monitored device, and then the Time for reboot countdown starts (see below).
- *Output Select* – selects the output (relay) which will reset the monitored device. There is a list of available physical (*Relay1 or Relay2*) and virtual outputs (*NetOut1xx*). Virtual outputs are set to **Output Setup** section.
- *Send e-mail when reboot (in future)* – send e-mail in case of the device reset.
- *Send SMS when reboot (in future)* - send SMS in case of the device reset.
- *Beeper Enable (in future)* – activate sound signalization in case of reset the device reset. If checked, you will hear 3x short beeps at the time of switching the output.
- *During Beeper on Reset (in future)* - The sound signalization during the device reset

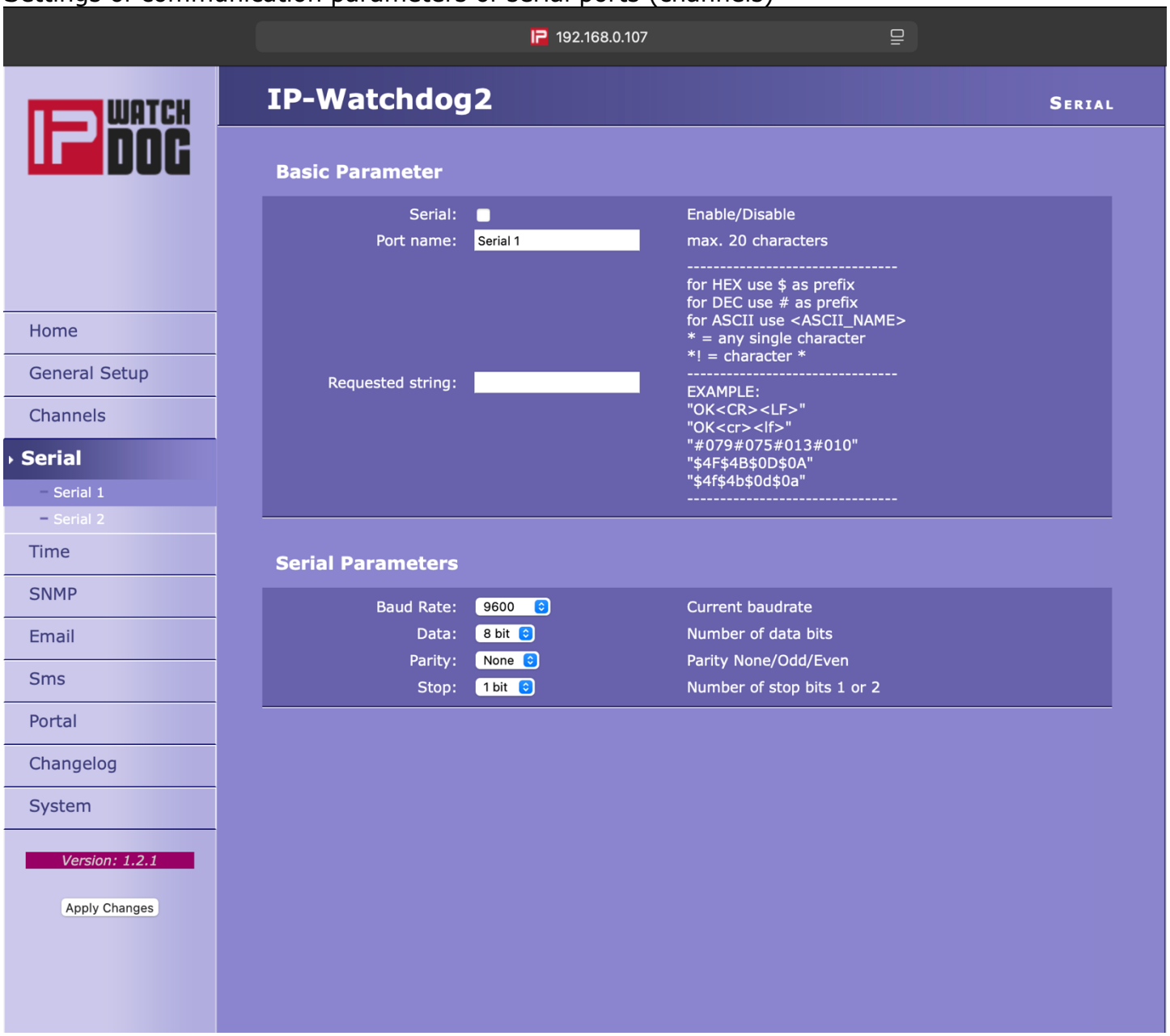
Section Output Setup (*Virtual outputs only*)



- *Name* – name of Outputs
- *Target Outputs* – type of remote Device
- *Remote IP Address* – address of the remote device
- *Remote IP Port* – HTTP port remote device`s
- *Remote ID* – ID of remote Outputs.
- *Username* – if the remote device is protected by a username and password
- *Password* – if the remote device is protected by a username and password

Serial

Settings of communication parameters of serial ports (channels)



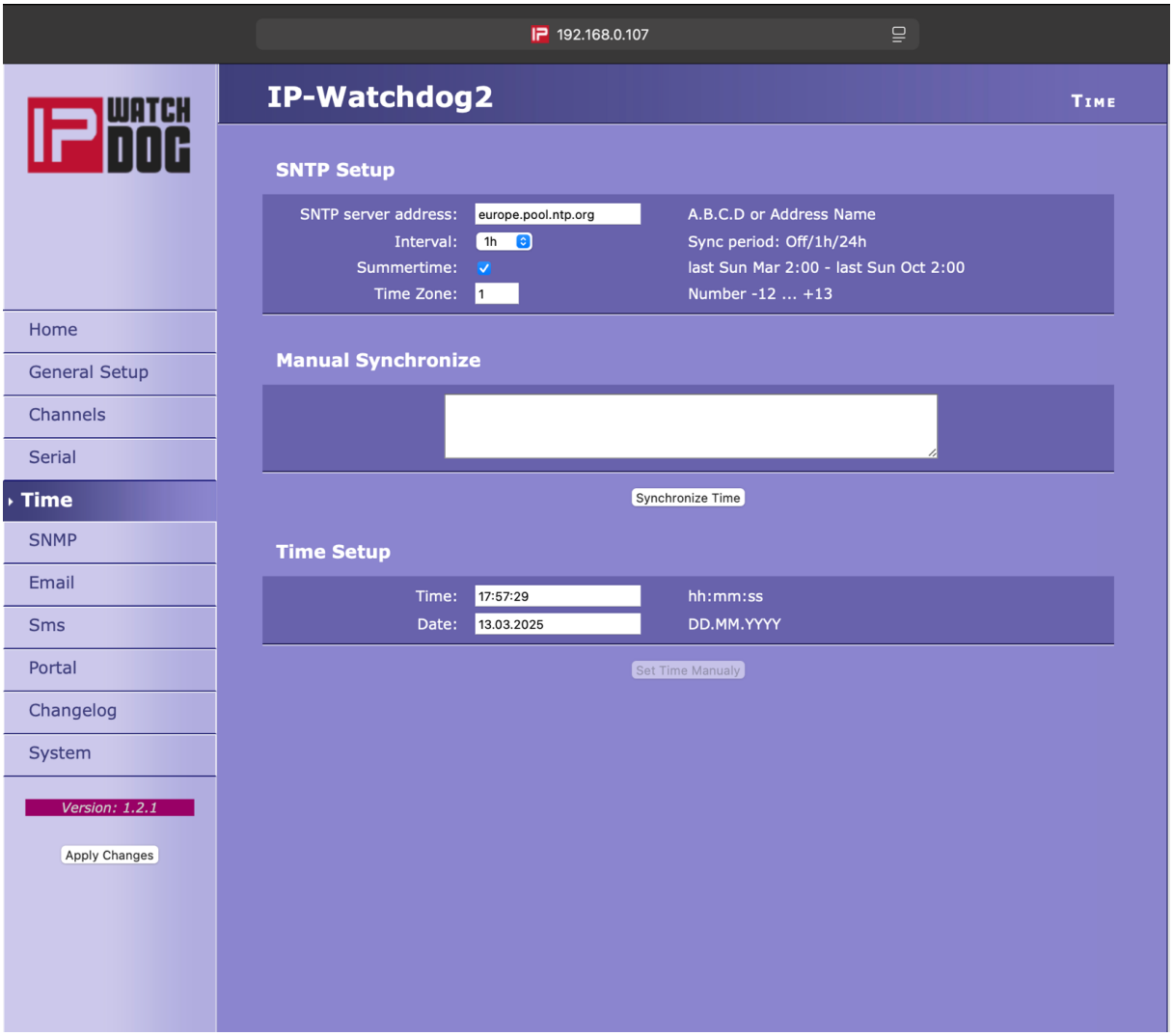
Basic Parameter

- Serial - Enable or disable port
- Port name - name of the port. Makes configuring channels and solving the issues with monitored devices easier. Name can contain up to 20 symbols.
- Requested string - Searched string in the data flow. Finding the required string it is deemed to constitute proper operation of the monitored equipment

Serial Parameters

- *Baud Rate* - Current baudrate
- *Data* - Number of data bits
- *Parity* - Parity None/Odd/Even
- *Stop* - Number of stop bits 1 or 2

Time



Section SNTP Setup

- SNTP Server – IP address or domain address of server for time synchronization
- Interval – interval of time synchronization with the server.
- Summertime - enable automatic switching between summer and winter time (DST) - used to set the correct system time.
- Time Zone – setting the time zone location IP WatchDog2 - used to set the correct system time.

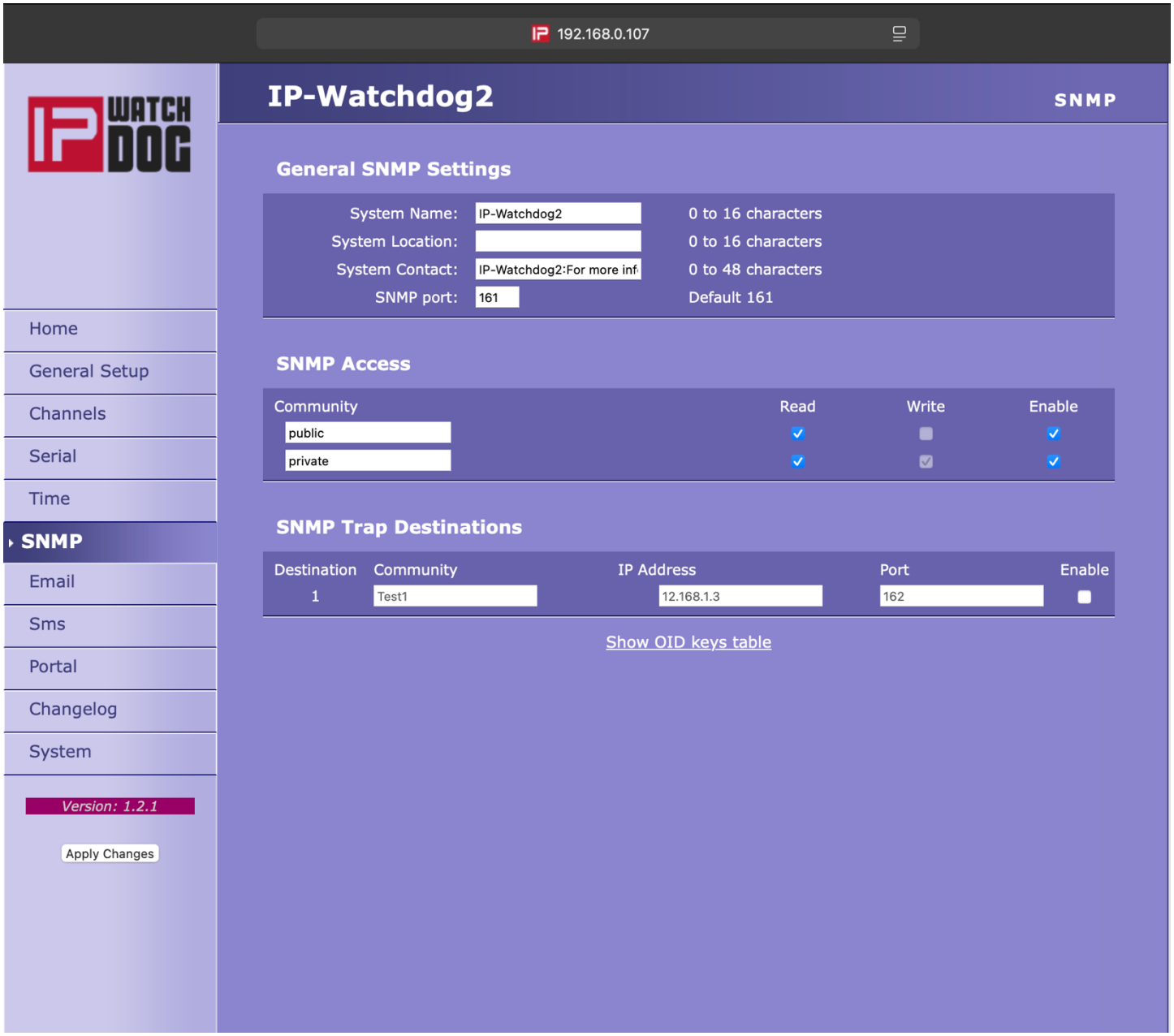
Manual synchronize

- Debug Window
- *Synchronize Time* is used to perform an immediate synchronization with the time server. Can also be used to test the settings.

Section Time Setup

Session Time Setup allows you to fill the current date and time manually when you can not use synchronization with the time server. After the loss of power this information may be lost.

SNMP



General SNMP Settings

- *System Name* – The device name coincides with the name of the device
- *Systém Location* – system location, such as "IT room, floor 2".
- *System Contact* – Contact the system administrator, for example, e-mail address
- *SNMP port* – Port settings for communication within the SNMP **[161]**.

SNMP Access

Defines the permissions and name groups of users can work with the Poseidon.

- *Community* – Text the name of the group that are assigned rights (default **Public** and **Private**)
- *Read* – add permission to the community to read variables over SNMP
- *Write* – add permission to the community writing values to variables over SNMP
- *Enable* – enable or disable the group

SNMP Trap Destination

Defines the destination for sending SNMP traps.

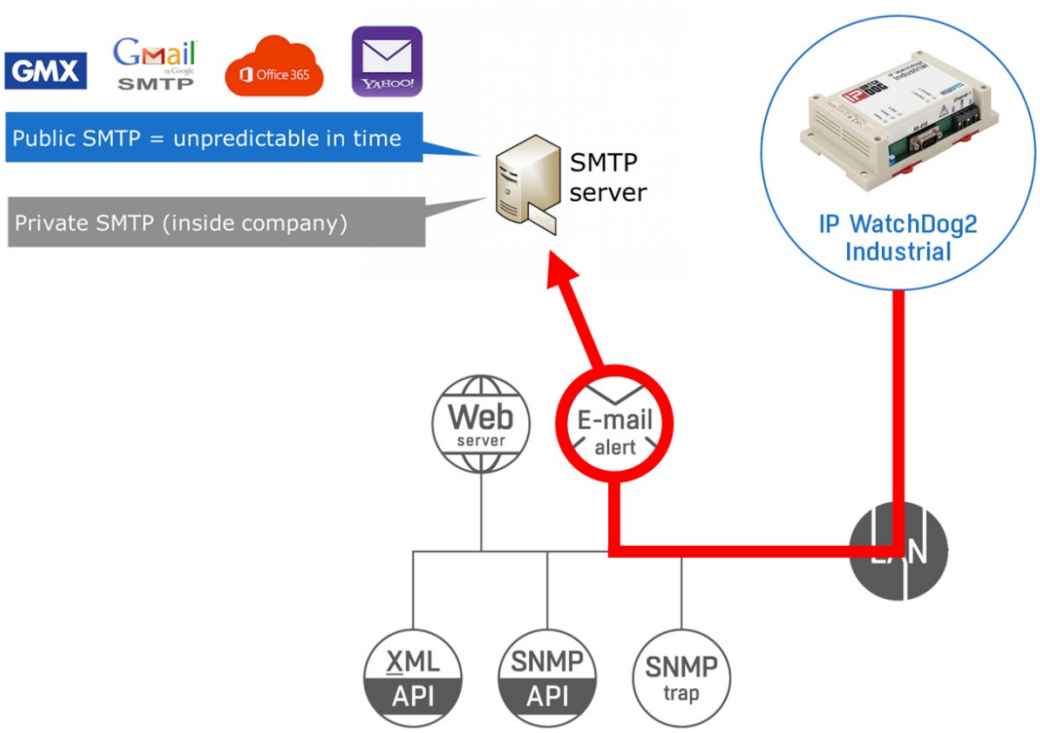
- *Community* – Text the name of the group SNMP Trap
- *IP address* –Destination address which will be sent SNMP traps.
- *Port* – The destination port to which traps will be sent.
- *Enable* – Enables transmission of SNMP traps to this destination.

E-mail

Sending alert via SMTP server

We do not recommend using public SMTP servers for email alerts. This solution lacks long-term reliability – what works today may not work in one year. Instead, use a private SMTP server for your email alerts. The best option is to take advantage of the free HWg cloud service and set up email alerting through the HWg cloud.

Use a public SMTP server: Not recommended



To send emails directly from the Watchdog device, you need a private SMTP server. Using a public SMTP server is not recommended, as it is not a long-term reliable solution due to the rapid evolution of security protocols. (You can read more about this issue in this article: Use a Public SMTP Server – Not Recommended.)

Pros:

✓ No dependency on external cloud services

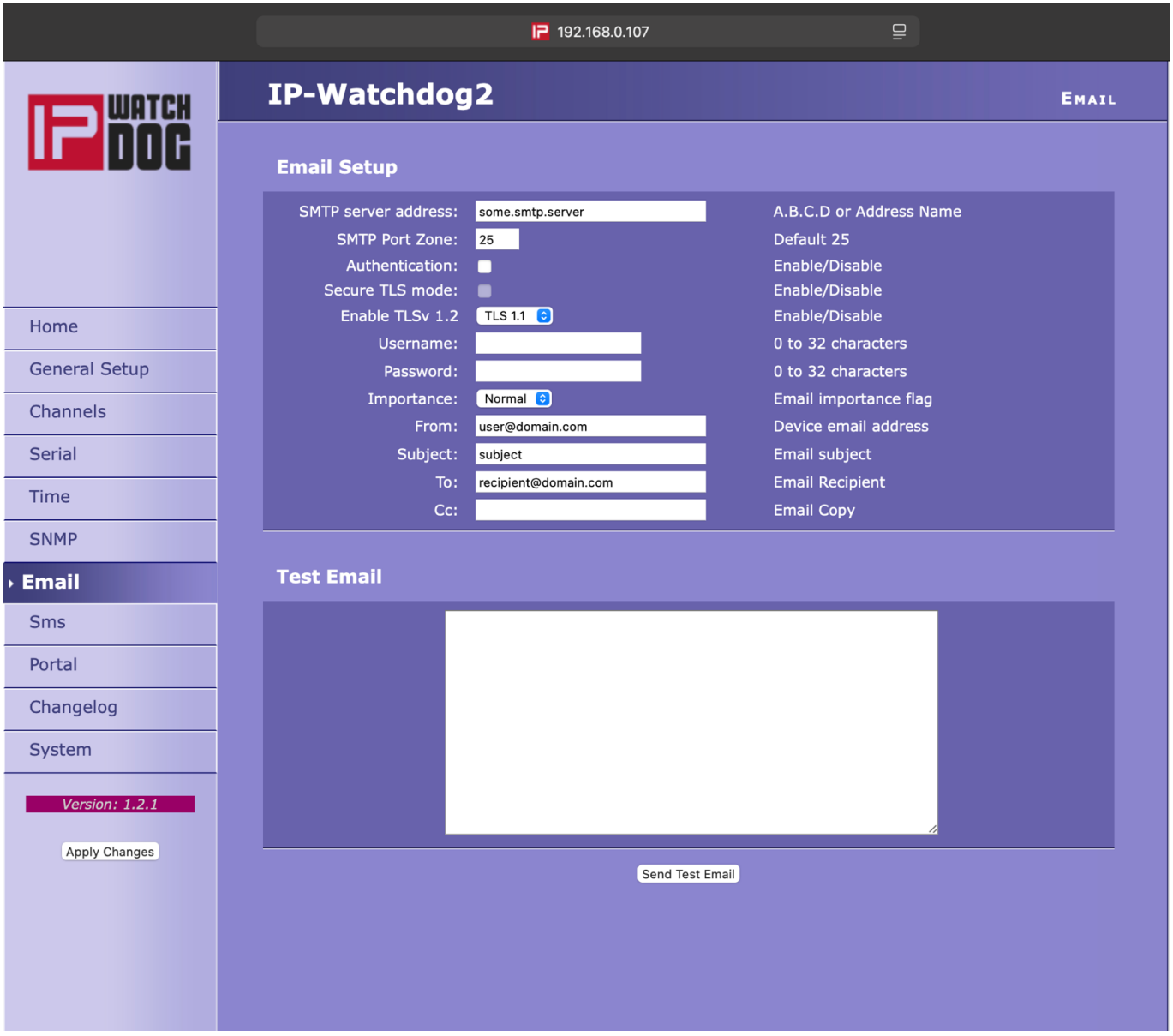
Cons:

✖ Requires setting up and maintaining a private SMTP server

✖ Public SMTP servers may stop working due to security updates

✖ No alert if the device itself goes offline

Email (SMTP Settings)



Email Setup Section

- *SMTP Server* – IP address or domain address of the SMTP server.
- *SMTP Port* – port number on which listens e-mail server - default 25.
- *Secure TLS mode - check if SMTP server requires a secure communications using SSL / TLS.*
- Authentication - enabled authentication- check if the SMTP server requires authentication.
- *Username* – user name for authentication to SMTP server. Unless Authentication check box is selected, the content of this field is irrelevant.
- *Password* – authorization password for the SMTP server. Unless Authentication check box is selected, the content of this field is irrelevant.
- *Importance* – sets the priority e-mail messages. Important for filtering and further processing alarm messages.

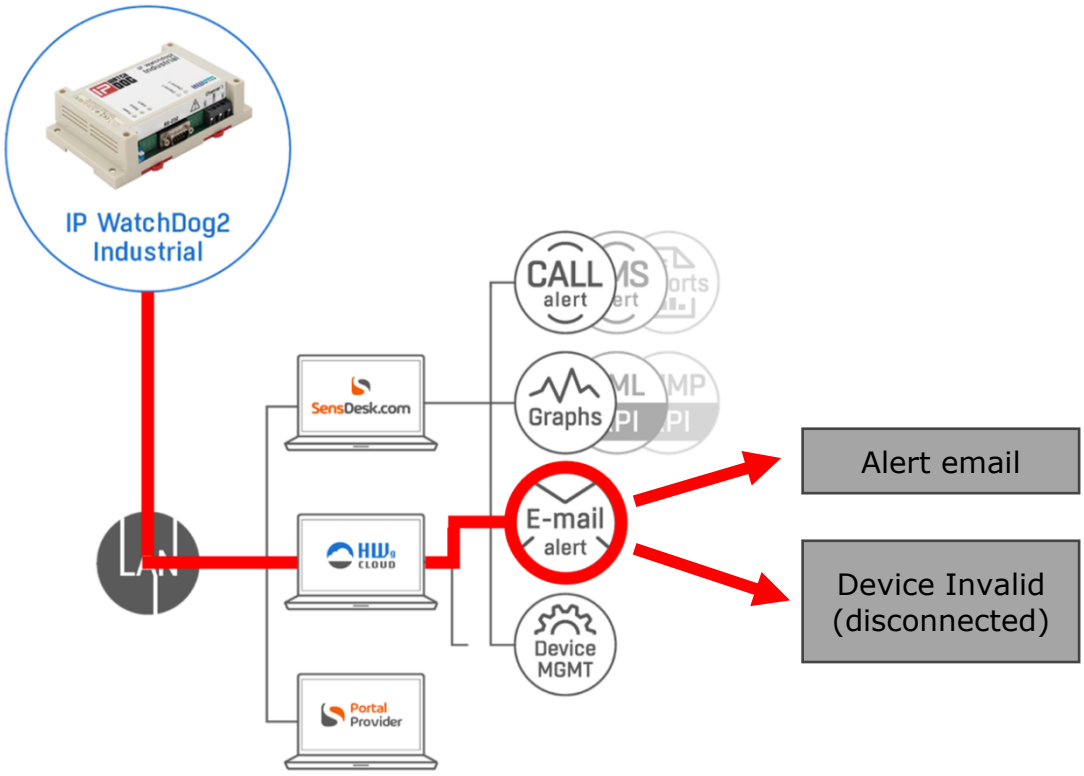
- *FROM* – from - e-mail address of the sender, ie units IP WatchDog2. Address may be required from SMTP servers and can be used to identify the units IP WatchDog2, possibly for filtering and processing of alarm messages.
- *Subject* - the subject of e-mail - the contents of the field can be used to identify the units IP WatchDog2, possibly for filtering and processing of alarm messages.
- *TO* – To - The e-mail address to be sent alarm e-mail.
- *CC* – copy - e-mail address to be sent a copy of alarm e-mail.

Check for sending Email

- Correct IP address for **IP Gateway**
- **DNS server** in the network settings
- **SMTP server** and its port
- Turning on **authentication** and correct **name** and **password**
- Off **Spam filter** in mail box

Sending alert via HWg-Cloud (portal)

Email alerts can be sent directly from the portal. It's more stable in the long term compared to using public SMTP servers. Additionally, it offers useful features such as Device Invalid Alerts..



Using cloud-based email alerting offers an advantage over direct device emailing: it includes device invalid alerts (notifications when the device is disconnected, powered down, or otherwise unreachable). This makes cloud-based alerting a more reliable long-term solution, as you always stay informed about the device status.

Pros:

✓ Reliable long-term alerting, even if the device is offline

✓ No need to configure an SMTP server

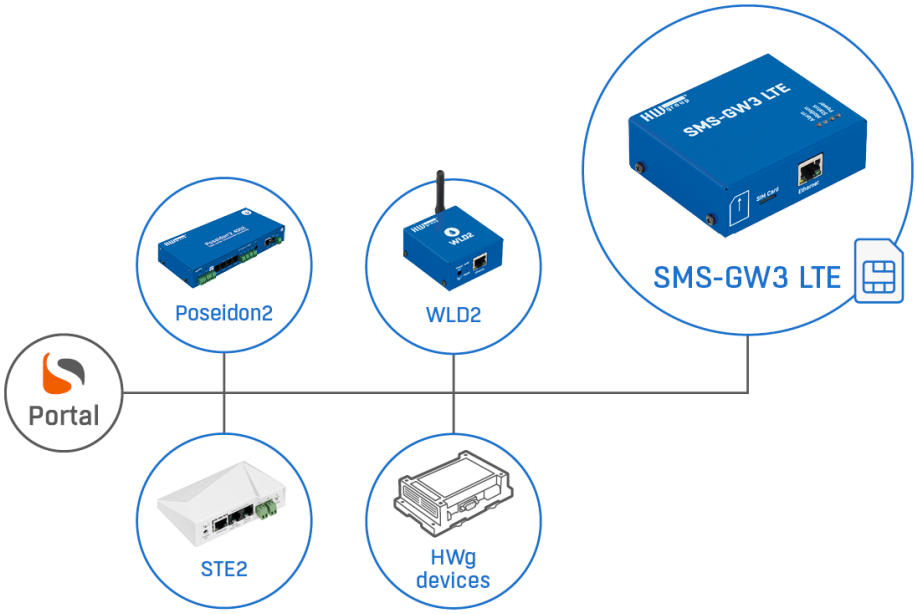
Cons:

✖ Relies on an external cloud service, which may have downtimes

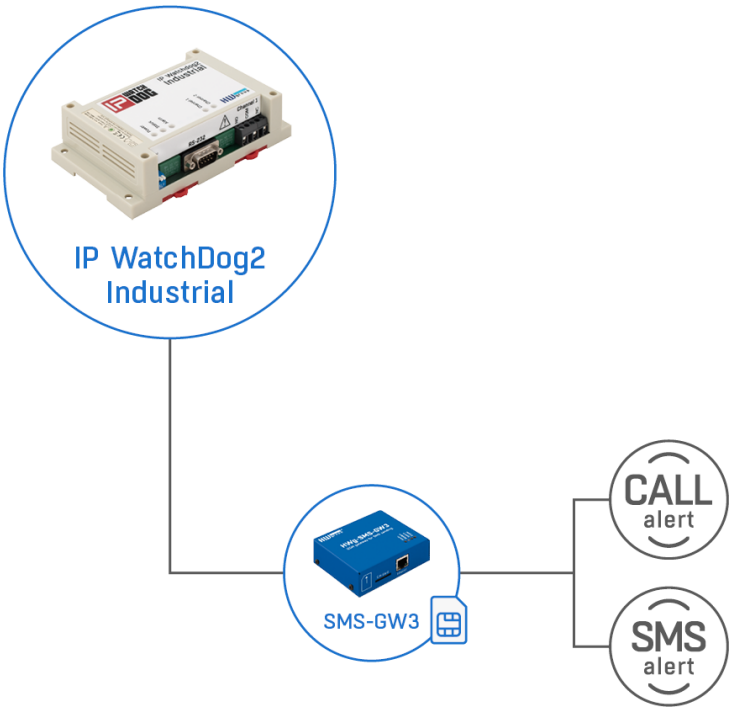
SMS alerts

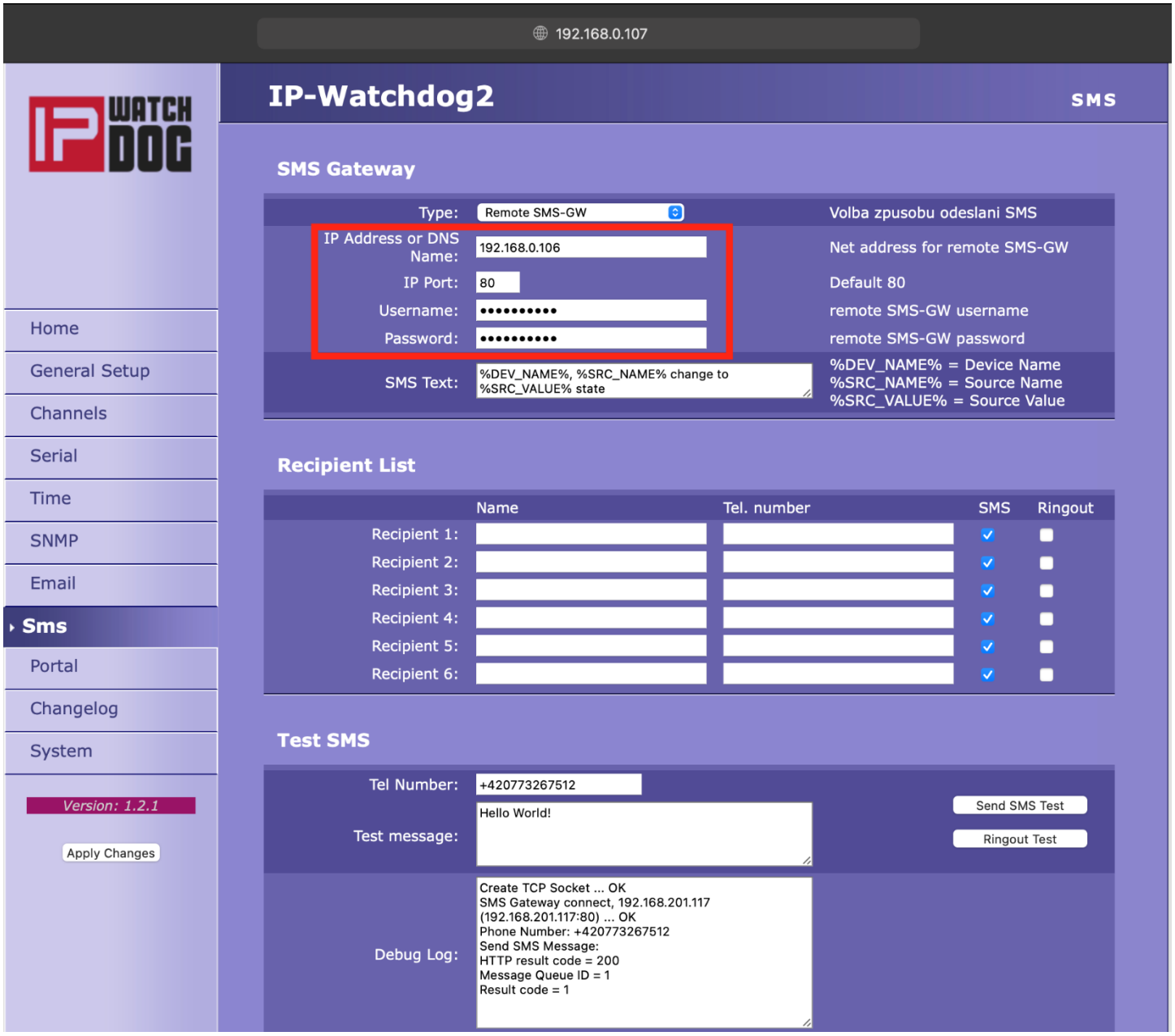
To send SMS alerts, you have to connect IP WatchDog device to the SMS-GW (device) over LAN. Second option is to sending SMS via the Portal, but it have to be Portal feature (SensDesk.com for example.

SMS alerts via external SMS-GW



SMS-GW device have to be LAN accessible, anyway it can be located in different building..





SMS gateway section

- **Type** – choose device for SMS sending: Local GSM modem on serial line (only for Industrial version) or Remote SMS gateway
  - **Local GSM modem**:
    - **SIM pin** – PIN of the SIM card used in the modem
    - **SMS text** – text that will be sent in the SMS. You can use these tags: %DEV_NAME% = Device Name; %SRC_NAME% = Source Name; %SRC_VALUE% = Source Value
  - **Remote SMS gateway**: (The credentials highlighted in the red box can be found in the SMS Gateway device's web interface, under the General Setup tab)
    - **IP Address or DNS name** – the IP Address of SMS gateway (can be found in the web interface of SMS gateway under the General Setup tab)
    - **IP Port** – IP port for communication (default value is port 80)
    - **Username** – the username set in SMS gateway under the General Setup tab in the NetGSM (SOAP) security box

- **Password** – the password set in SMS gateway under the General Setup tab in the NetGSM (SOAP) security box
- **SMS text** – text that will be sent in the SMS. You can use these tags: %DEV_NAME% = Device Name; %SRC_NAME% = Source Name; %SRC_VALUE% = Source Value

Section recipient list

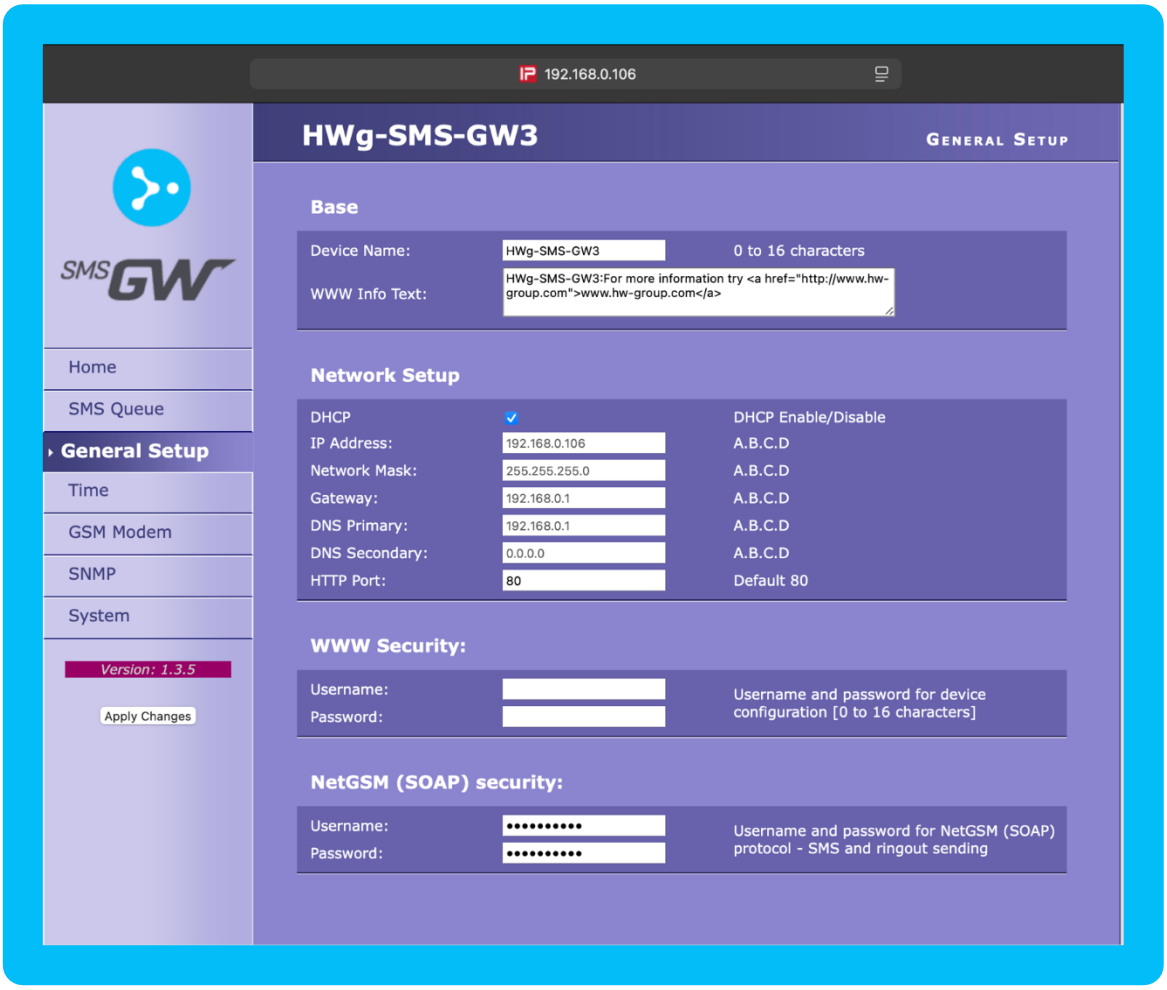
- **Recipient** – the name of the recipient and phone number. Select from options to send an SMS, Ringout call, or both

Section test SMS

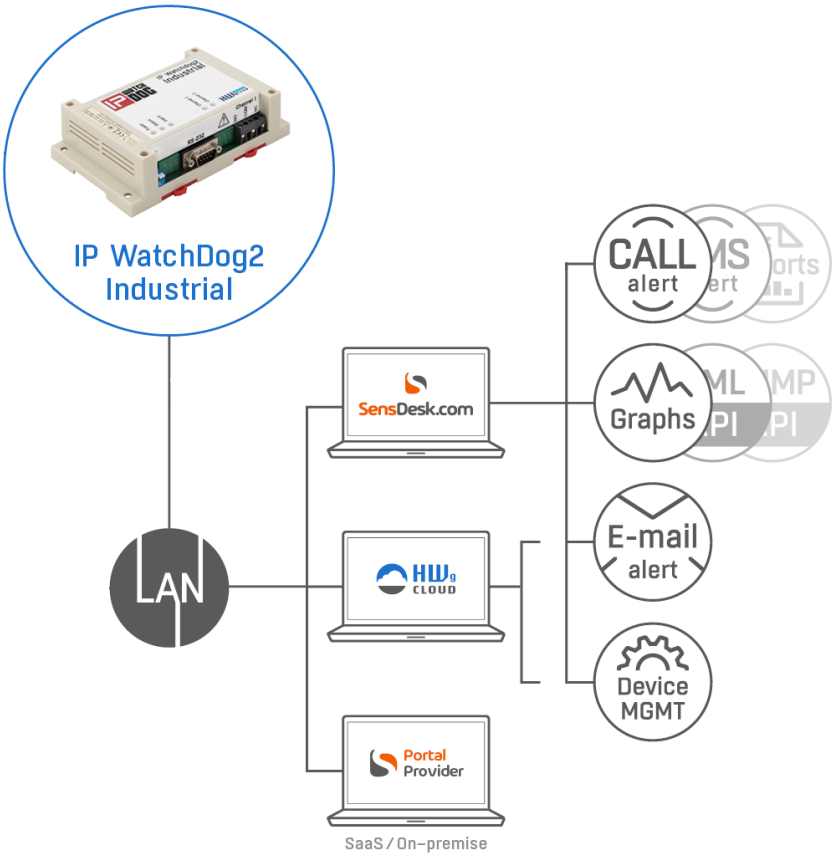
- **Tel number** – the telephone number to which the test SMS will be sent or Ringout call made
- **Test message** – the text of the message sent as a test
- **Debug log** - shows the communication with the SMS gateway

WEB GUI of the SMS-GW device

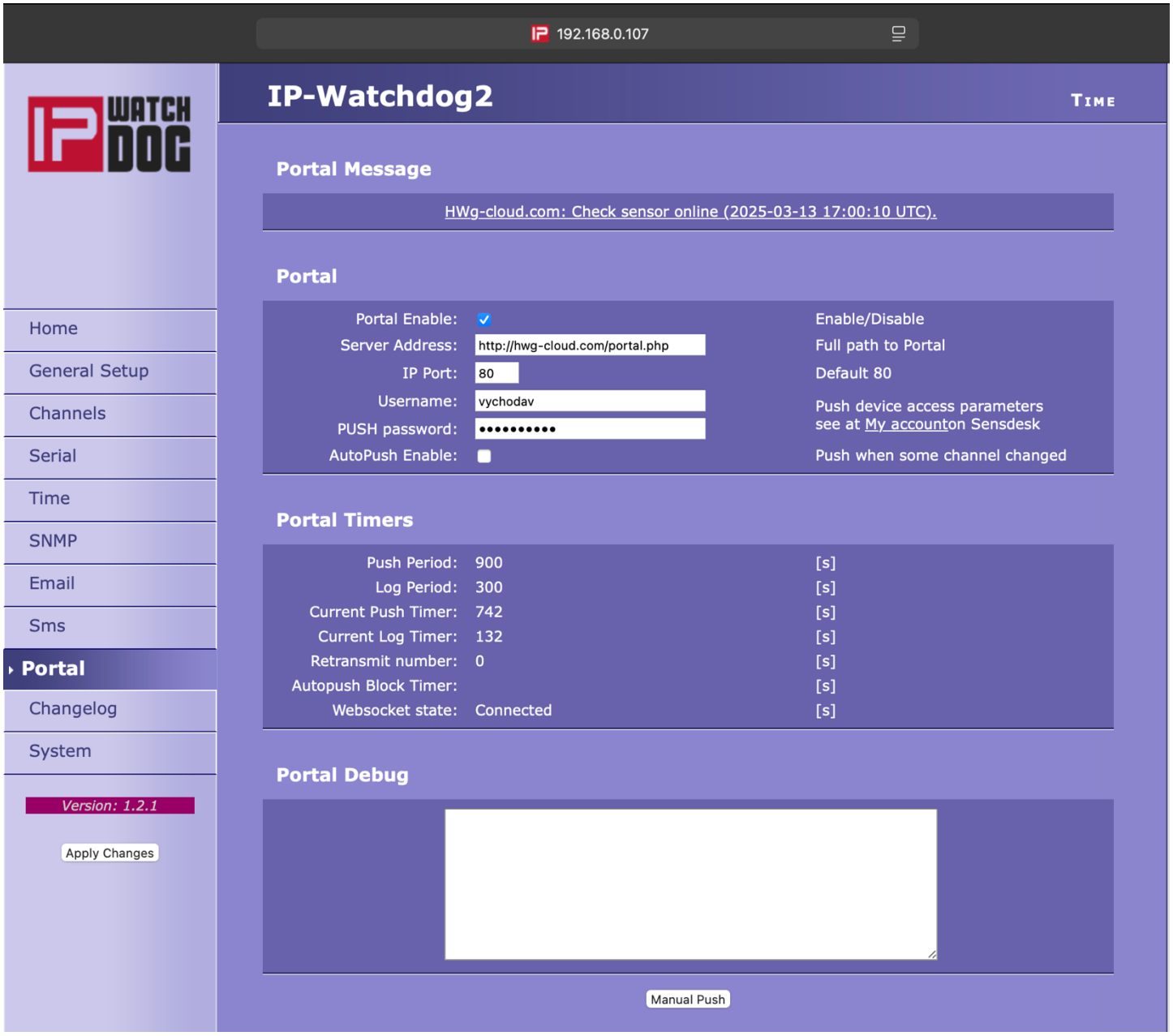
You can see the IP address of the SMS GW (192.168.xx.xx) is configured in the IP WatchDog2 device.



Portal



This page is used to set parameters for sending data to a remote HWg-PUSH portal. For more information about protocol or portal solutions, please visit http://www.hw-group.com



Portal Message Section

The message from the portal, contains links to graphs etc. It depends on the type of website.

Section Portal

- **Portal** – Enable or disable this feature
- **Push Period** – Period of sending data to a remote server. The period is adjusted retrospectively from the portal
- **Server address** – the full URL of the remote server
- **IP Port** – Port on which the portal listens
- **Username** – User name for assigning IP WatchDog2 to user. Receive from the portal administrator.
- **Password** – Password for assigning IP WatchDog2 to user. Receive from the portal administrator

Portal Timers

For debugging purposes only

- *Push Period* - The period for sending data to a remote portal. A period determined by the portal and can not be changed by the user.
- *Log Period* - The period of storage of data for portal into a cache. A period determined by the portal and can not be changed by the user.
- *Current Push Timer* - The timer indicates for how long the data will be sent to a portal
- *Current Log Timer* – The timer indicates for how long the data will be stored for portal into a cache.
- *Autopush Block Timer* - Event counter for Autopush. In the case of exceeding the allowed number of events per cycle of Push, the AutoPush feature will be blocked.

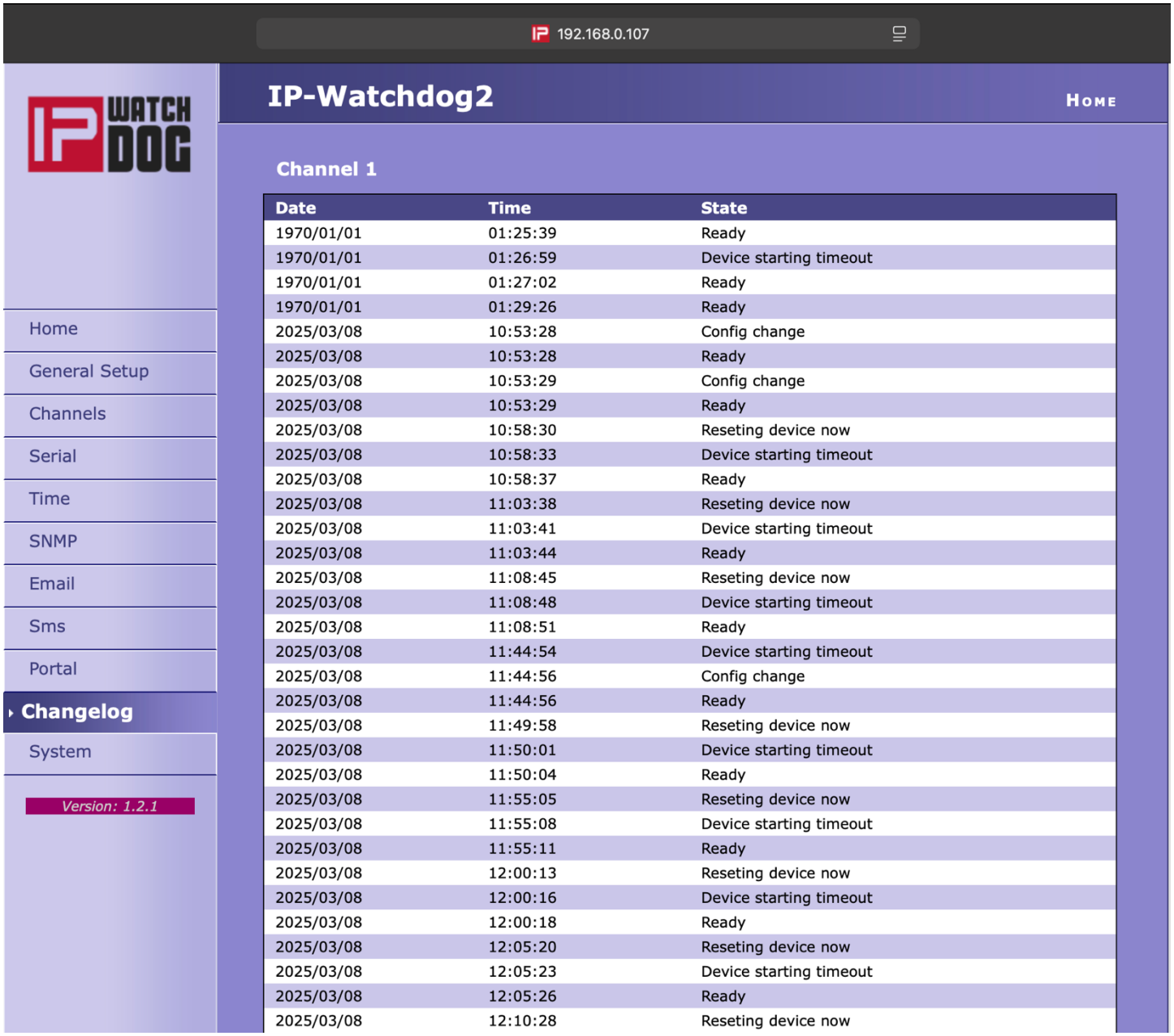
Portal Debug

- *Debug window* of sending data to the portal
- *Manual Push* - button for immediate shipment of the data to a portal

Adding IP Watchdog to HWg-cloud

To add the IP Watchdog to the portal, follow the steps in chapter First steps, subchapter Connecting IP Watchdog to the HWg cloud.

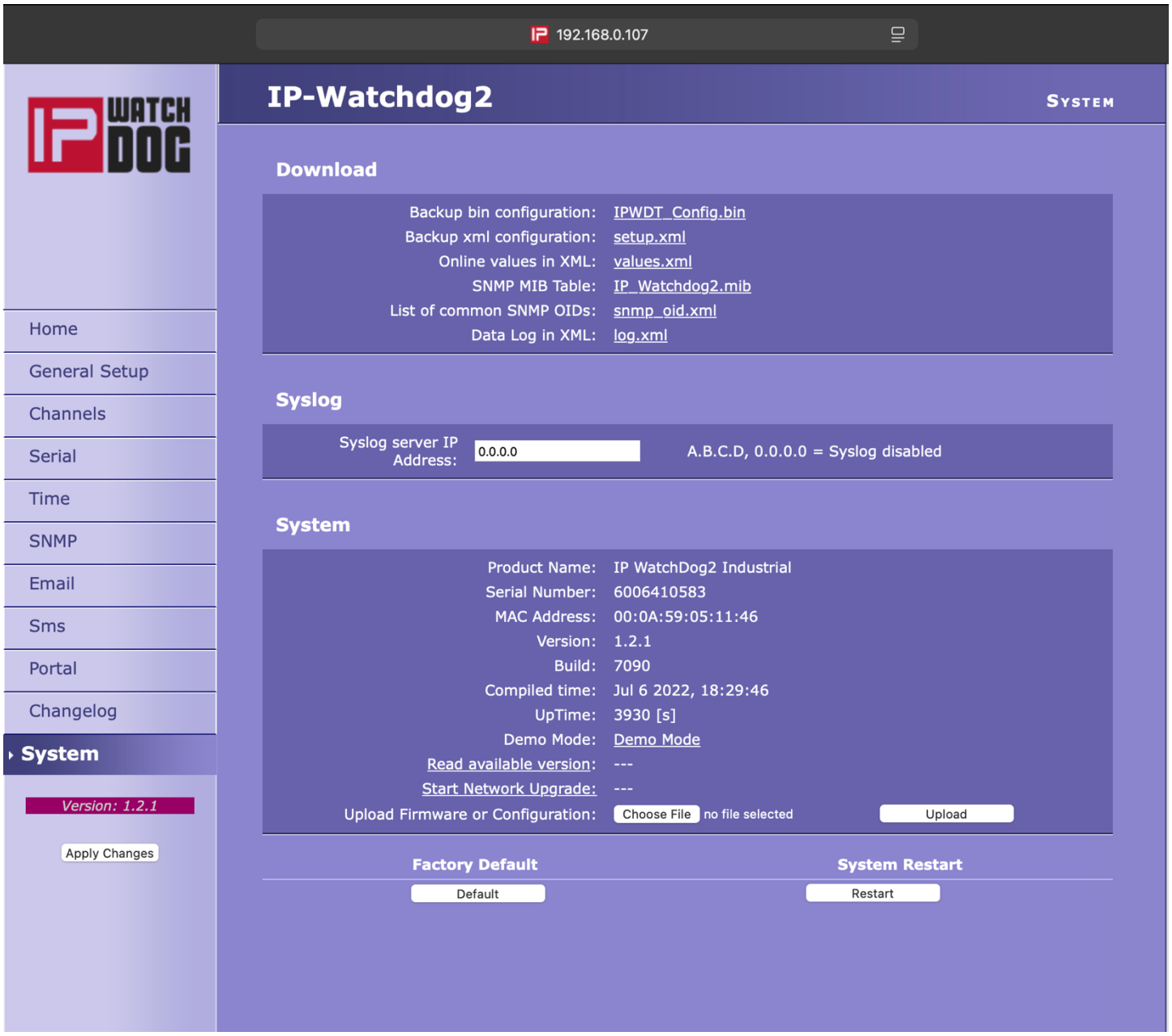
Changelog



Date	Time	State
1970/01/01	01:25:39	Ready
1970/01/01	01:26:59	Device starting timeout
1970/01/01	01:27:02	Ready
1970/01/01	01:29:26	Ready
2025/03/08	10:53:28	Config change
2025/03/08	10:53:28	Ready
2025/03/08	10:53:29	Config change
2025/03/08	10:53:29	Ready
2025/03/08	10:58:30	Reseting device now
2025/03/08	10:58:33	Device starting timeout
2025/03/08	10:58:37	Ready
2025/03/08	11:03:38	Reseting device now
2025/03/08	11:03:41	Device starting timeout
2025/03/08	11:03:44	Ready
2025/03/08	11:08:45	Reseting device now
2025/03/08	11:08:48	Device starting timeout
2025/03/08	11:08:51	Ready
2025/03/08	11:44:54	Device starting timeout
2025/03/08	11:44:56	Config change
2025/03/08	11:44:56	Ready
2025/03/08	11:49:58	Reseting device now
2025/03/08	11:50:01	Device starting timeout
2025/03/08	11:50:04	Ready
2025/03/08	11:55:05	Reseting device now
2025/03/08	11:55:08	Device starting timeout
2025/03/08	11:55:11	Ready
2025/03/08	12:00:13	Reseting device now
2025/03/08	12:00:16	Device starting timeout
2025/03/08	12:00:18	Ready
2025/03/08	12:05:20	Reseting device now
2025/03/08	12:05:23	Device starting timeout
2025/03/08	12:05:26	Ready
2025/03/08	12:10:28	Reseting device now

System

System tab grant users access to the most important system information such as operating time or firmware version, and operations such as restart IP WatchDog2 or upgrade firmware.



Download

- *Backup bin configuration* – backup of configuration in format BIN - click on the link to save the current configuration of IP WatchDog2 after its final setting in case it needs restoration.
- *Backup XML configuration* – backup configuration in XML format - click on the link to save the current configuration of IP WatchDog2 after its final setting in case it needs restoration.
- *SNMP MIB Table* – SNMP MIB file - address of MIB file containing the definition of SNMP variables.
- *List of common SNMP OIDs* – an overview of the most important OID MIB table.
- *Data Log in XML* – List of recent events in XML

Syslog

- *Syslog server IP Address* – Address of Syslog server

System Section

- *Version* – firmware version. Used for diagnostic purposes in case of problem solving.
- *Compile time* – Time compilation firmware. Used for diagnostic purposes in case of problem solving.
- *Build* – compilation. Used for diagnostic purposes in case of problem solving.
- *UpTime* – running time of the device since the last start or reboot. Used for diagnostic purposes in case of problem solving.
- *Demo mode* - activated demo mode prevents any change in the configuration of your equipment.
  In this mode, visitors can freely browse and view all pages of the web interface, but changing values, they are not allowed. Thus setting the device can be placed on the public internet without the risk of changes in its configuration.
- *Upload Firmware or Configuration* – allows download into the device a newer firmware or configuration file. Restoring configuration may fail if it is too much difference in firmware versions.

Factory Default Section

Restores the factory settings. Default IP address is 192.168.10.20 and the user name and password are not defined.

System Restart Section

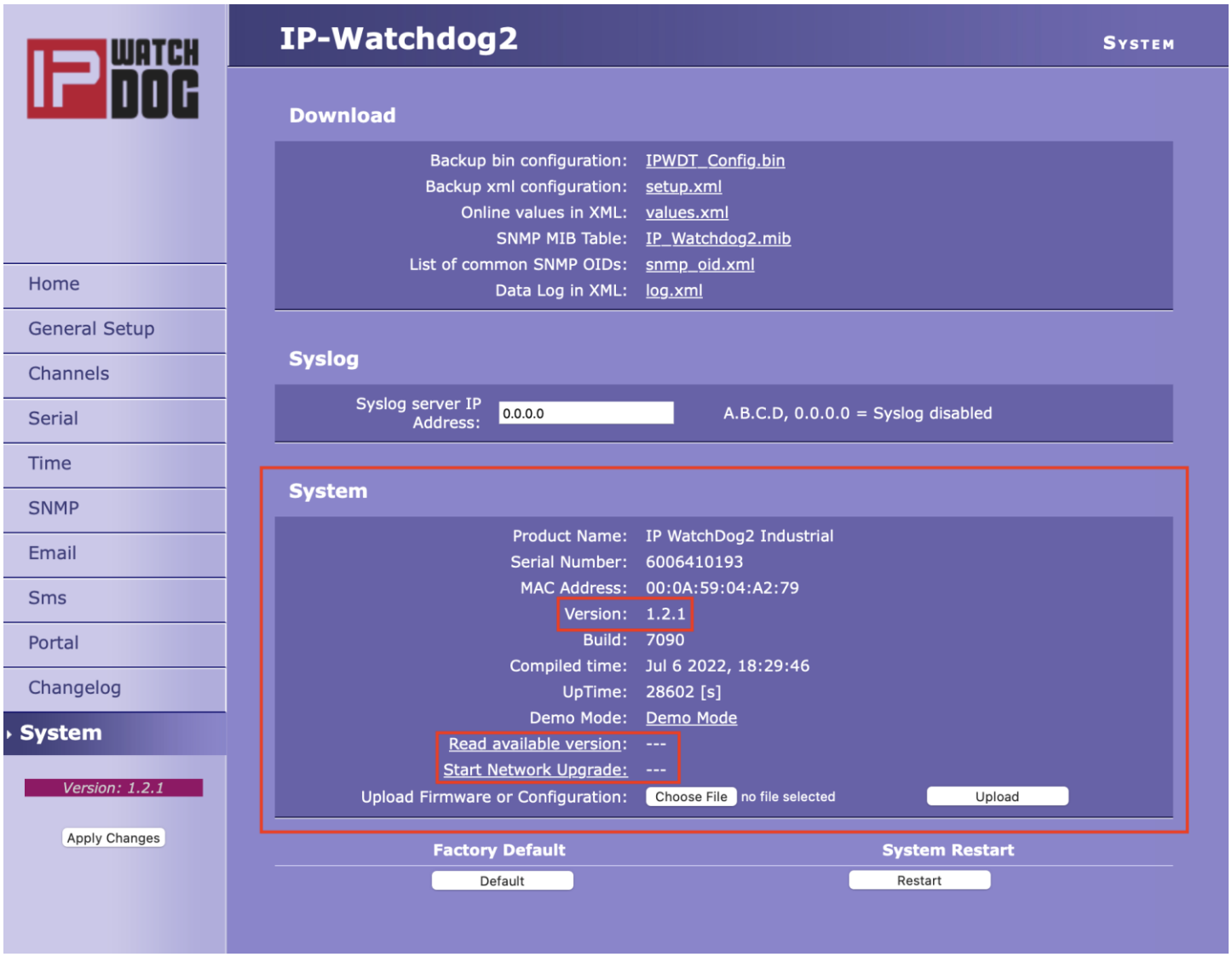
Reboot the device.

Firmware update and loading defaults

Firmware update

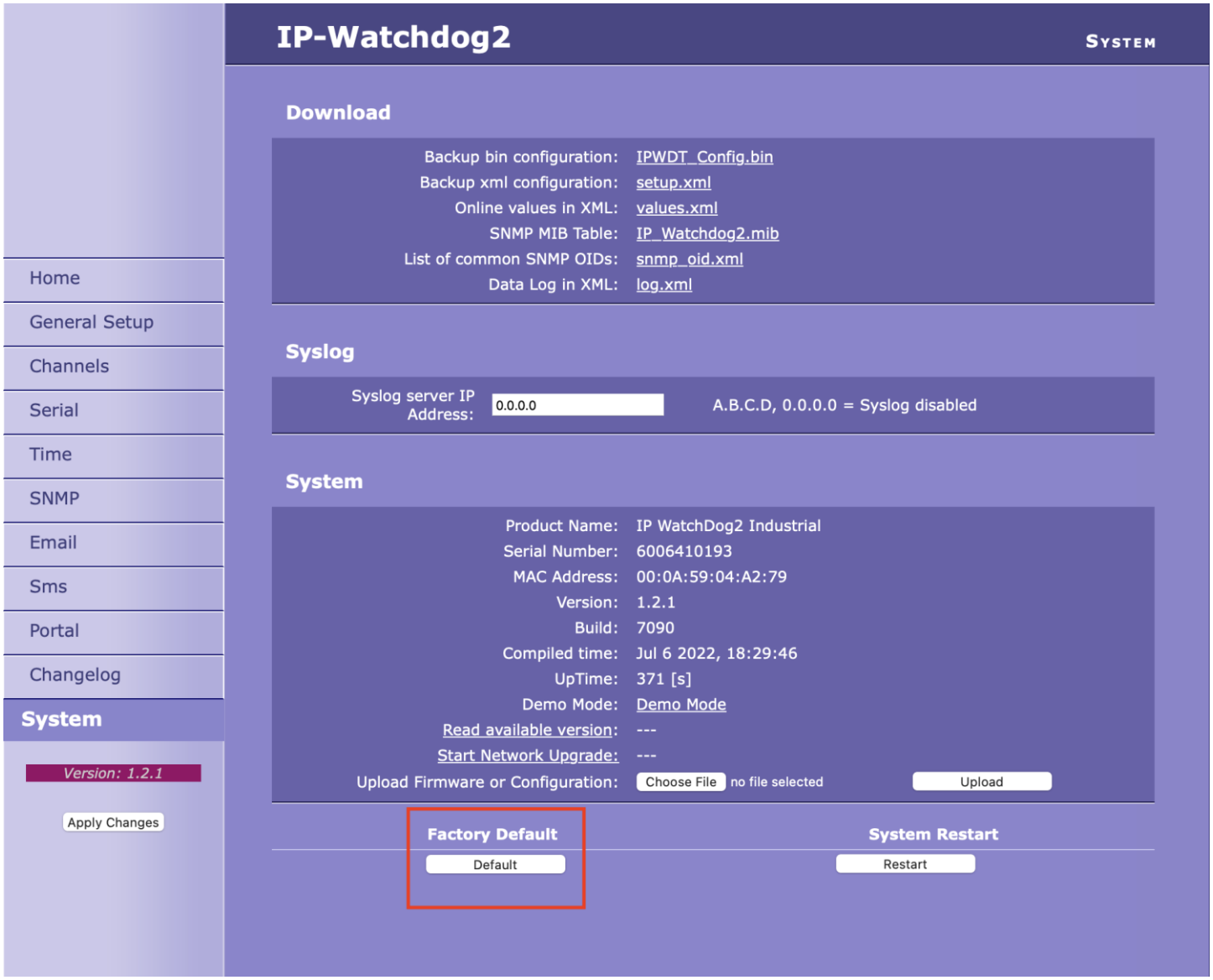
The latest firmware is available at: (https://www.hw-group.com/revision-overview/firmware). You can upload new firmware through the web interface of the IP Watchdog device in the System tab, which provides options to upload firmware or configuration files. You can also follow these steps to update the firmware:

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. Click 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.



Loading defaults

To load the default settings for the IP Watchdog device, navigate to the System tab in the web interface. Under the Factory Default section, you will find a "Default" button. Clicking this button will restore the device to its factory default settings.



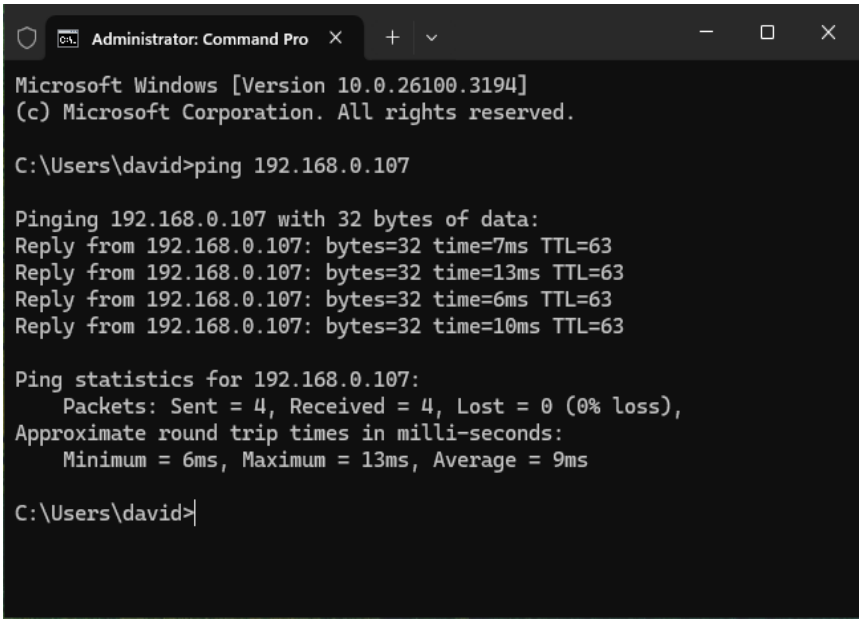
Testing and operation hints for Windows and Linux

Test functions Incoming Ping

Test command functions Incoming Ping for Windows

Application of the ICMP PING function in Windows is very simple but can be little tricky. Ping testing can be managed via the Start menu, select Run, Windows command line cmd and press OK. Application opens a command prompt (in older versions of MS Windows MS-DOS window). Write inside

`Ping ip_address_of_watchdog`, for example **`ping 192.168.5.60`**



The result will be roughly the following statement:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Vít Olmr>ping 192.168.5.60

Command PING on 192.168.5.60 with length 32 bytes:

Answer from 192.168.5.60: bytes=32 time=1ms TTL=64
Answer from 192.168.5.60: bytes=32 time < 1ms TTL=64
Answer from 192.168.5.60: bytes=32 time=1ms TTL=64
Answer from 192.168.5.60: bytes=32 time < 1ms TTL=64

Statistics for ping 192.168.5.60:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate time of the adoption of the response in milliseconds:
    Minimum = 0ms, Maximum = 1ms, Average= 0ms
```

If you want to send the PING permanently, enter the command with the -t:

`Ping 192.168.5.60 –t`

Command line can also be launched using the standard windows shortcuts:

- **Windows 8:** Press Windows Key + S, type CMD, then select Command Prompt.
- **Windows 10/11:** Right-click the Start button > Windows Terminal or Command Prompt, or type CMD in the Start/search menu.

The PING command relies on ICMP protocol (Echo Request/Reply), which may be blocked by:

1. Firewalls: Modern firewalls (e.g., Windows Defender Firewall) often disable ICMP by default. To resolve:
   - Open Windows Defender Firewall with Advanced Security.
   - Enable ICMPv4 and ICMPv6 inbound/outbound rules under Custom Settings.

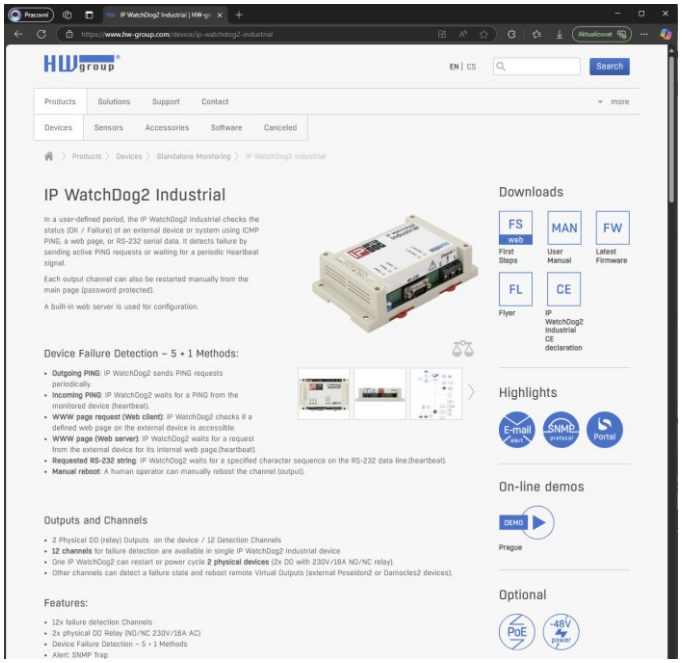
2. Remote Server Restrictions: Servers may block ICMP to prevent abuse (e.g., DDoS attacks).
   - If PING fails, use alternative monitoring methods (e.g., Page requests via a web browser).

Test command for Incoming Ping under Linux/Unix

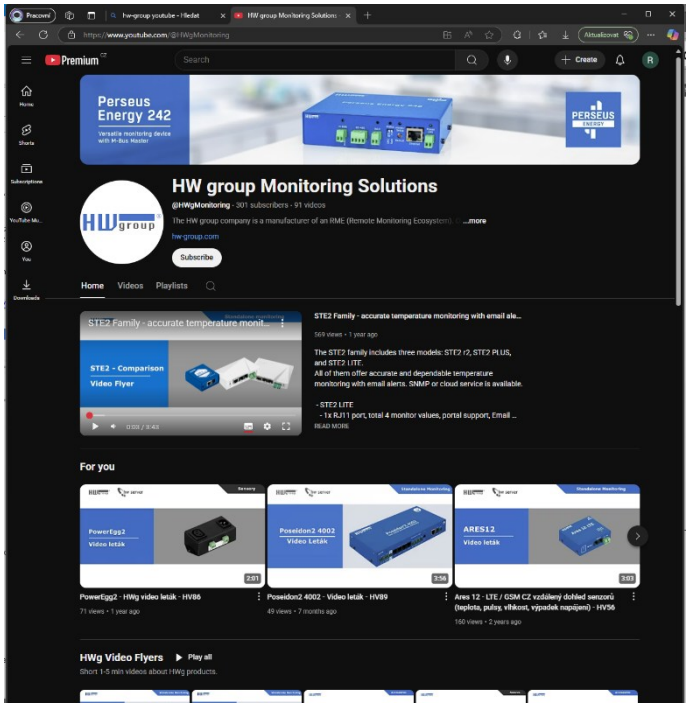
Using PING command under Unix and Linux OS is as simple as in the case of Windows, maybe even easier because you don't have to run the command line. Just enter the following into the console:

```
Ping 192.168.5.60
```

More information



www.HW-group.com



HW group YouTube

HW group, s.r.o.

Rumunská 26/122
Praha 2, 120 00
Česká republika

Tel.: +420 222 511 918
Fax: +420 222 513 833

www.HW-group.com

manual version: April 2025