www.cometsystem.com

User's Guide

PA8610
PA8611
PA8641
PA8652

Sensor with Ethernet communication

October 2026

© Copyright: COMET SYSTEM, s.r.o.

It is prohibited to copy or modify this manual without the explicit consent of COMET SYSTEM, s.r.o. All rights reserved.

COMET SYSTEM, s.r.o. continuously develops and improves its products. The manufacturer reserves the right to make technical changes to the device without prior notice. Misprints reserved.

This User's Guide applies to a range of products. Not all products support all features, such as different types of measured values. Screenshots and graphics may differ depending on the specific product and the computer operating system.

Contact the manufacturer of this device:

COMET SYSTEM, s.r.o.
Bezrucova 2901
756 61 Roznov pod Radhostem
Czech Republic
www.cometsystem.com

Table of contents

TABLE OF CONTENTS 3
INTRODUCTION 5
SAFETY PRECAUTIONS AND PROHIBITED HANDLING 6
INSTALLATION 8
- Hardware installation 8
- Initial device setup 10

FEATURES 12
- Dashboard 12
- Status LED 13

MODELS OF WEB SENSORS 14
DEVICE SETUP 16
- Conventions 16
- General settings 17
- Measurement settings 19
- Channel settings 20
- Alarm settings 22
- Network settings 22
- Protocols settings 26
- Cloud protocol settings 32

COMMUNICATION PROTOCOLS 36
- Modbus TCP 36
- Cloud protocol – JSON 39
- JSON and XML via http server 42
- SNMP protocol 45
- Syslog protocol 46

TROUBLESHOOTING 48
- Factory defaults 48
- Forgotten administrator password 48
- How to determine device IP address 48
- How to use newly connected probe 49
- Error codes at channels 49
- Wrong device time 51
- Device is restarting continuously 51
- Measurement accuracy issue 51
- Uploading a certificate or private key 51

RECOMMENDATIONS FOR OPERATION AND MAINTENANCE 52
- Operation in application fields 52
- Recommendations for calibration 53
- Recommendations for regular checks 53
- IT security advisories 54
- Firmware update 55
- Technical support and service 55

TECHNICAL SPECIFICATIONS 56
- Power supply 56

General parameters 56
Communication protocols 56
Parameters of inputs 58
Operating and storage conditions 61
Dimensions 61
Mechanical properties 63
End of operation 63
Declaration of Conformity 63
APPENDIX 64
REVISION HISTORY 72

Introduction

Web Sensors are designed for autonomous measurement, processing, and alarming of physical quantities. They support the measurement of temperature and relative humidity and may also be equipped with binary inputs. The available inputs and measurement ranges depend on the specific device model and cannot be changed by the end user. Device communication is carried out via an Ethernet network with support for multiple communication formats. Web Sensors can be powered by an external adapter or via Power over Ethernet (PoE).

Key features:

- Measurement using an internal temperature sensor or external temperature probes and temperature-humidity probes. The PA8652 device is additionally equipped with three binary inputs for monitoring binary signals.
- Monitoring and alarming of measured values based on preset limits. Two alarm limits are available for each measured quantity, with selectable direction.
- Minimum and maximum values for each measured quantity are recorded from device start-up. These values can be manually reset by the end user. The values are also cleared when the device is restarted.
- Communication is performed over an Ethernet network, enabling easy deployment in places where a LAN connection is available.
- The device can be powered either by an external power supply adapter or via Power over Ethernet (PoE), compliant with IEEE 802.3af. External power supply is available as optional accessories.
- Measured values can be displayed via the device web interface and transmitted to the COMET Cloud or COMET Database data acquisition systems.
- Integration with third-party data acquisition systems is supported through JSON, XML, Modbus TCP, and SNMP protocols.
- The device is equipped with integrated non-volatile internal memory, used for recording measured values in the event of connectivity outages.
- Alarm states can be reported via email or Syslog messages sent from the device.
- The device delivery includes a traceable calibration certificate. The declaration of metrological traceability of standards is based on the requirements of the EN ISO/IEC 17025 standard.

Safety precautions and prohibited handling

Please read the following safety precautions carefully before using the device and keep them in mind during use.

Installation, commissioning, and maintenance must only be carried out by a qualified person in accordance with applicable regulations and standards.

- **Operating and storage conditions:** Follow the recommended conditions specified in the technical parameters. Do not expose the device to temperatures outside the specified range. Avoid exposure to direct heat sources or sunlight.
- **Ingress protection:** The device is not protected against water, moisture, or dust ingress. Protect the device from dripping and splashing water. Do not use the device in environments where condensation may occur. In such conditions, the device must be installed in an enclosure providing a higher level of ingress protection. Such a box is available as an optional accessory.
- **Device cover:** Never operate the device without the cover. The device may contain hazardous voltage, and there is a risk of electric shock.
- **Aggressive environment:** Do not expose the device to aggressive environments, chemicals, or mechanical shock. Relative humidity sensors must not come into direct contact with water or any liquid. Do not remove the sensor cover or perform any actions that could cause mechanical damage to the sensors beneath the cover.
- **Fire and explosion hazard:** This device must not be used in hazardous areas, especially those at risk of explosion due to flammable gases, vapours, or dust.
- **Servicing, failures and maintenance:** Do not attempt to repair the device yourself. Any repairs may only be carried out by suitably trained service personnel. Use a soft cloth for cleaning only. Do not use solvents or other aggressive agents. If the device shows signs of unusual behaviour, switch it off immediately. Contact the distributor from whom you purchased the device.
- **Network infrastructure:** The device may be connected to network equipment compliant with applicable standards. For power over Ethernet (PoE), use IEEE 802.3af or IEEE 802.3at compliant switches. Do not use passive PoE injectors.
- **Power supply adapter:** Use a *power supply adapter recommended by the manufacturer* and approved according to relevant standards. Do not use an adapter with a higher output voltage than permitted. Before connecting the adapter, make sure that its housing and cables are not damaged.
- **Mounting:** Install the device in the recommended operating position. Installation must be performed on a stable surface to prevent falling or mechanical damage.
- **Cable connection:** Connect or disconnect the device properly. Do not disconnect the Ethernet cable or probes while the device is powered.

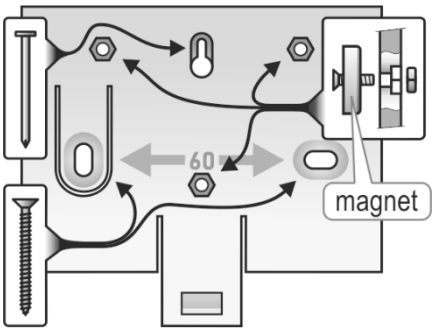
- **Serviceability:** Proper function of the device depends on the current state of required network services. The manufacturer is not responsible for data loss caused by improper use of the device, power failure, or failure of 4 network infrastructure. The device is not intended for use in applications where device malfunction could cause injury, loss of human life, or significant property damage. In such applications, a risk assessment must be carried out to determine the required level of redundancy.
- **Firmware update:** Upload firmware obtained only from the manufacturer or an official distributor. Firmware from unknown sources will compromise device security.
- **Recommended accessories:** Use only accessories recommended by the manufacturer. Make sure that accessories are not damaged before being connected to the device.

Installation

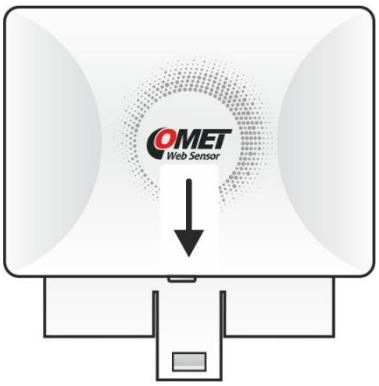
Hardware installation

- **Choose the correct location for the device** – verify that the environment in which the device is to be installed meets the specified *operating conditions*. The device is not protected against water and dust ingress. Do not use it in such environments. Ensure that the device is installed in the prescribed operating position.

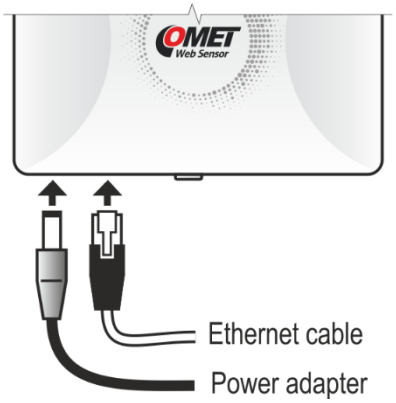
- **Secure the mounting plate** – use one of the recommended methods to install the supplied mounting plate. The bracket may be screwed directly onto a wall or another flat surface. Mounting materials, such as screws or wall plugs, are not included in the package. Use suitable fixing materials to prevent the device from falling and causing possible injury.



- **Place the device into the mounting plate** – slide the device downwards into the mounting plate until it locks into the lower position.

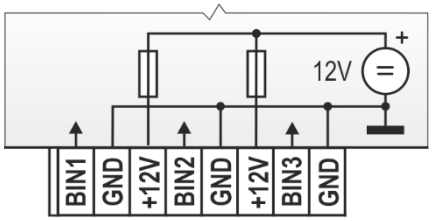


- **Connecting cables and probes** – connect the measuring probes, Ethernet cable, and binary inputs to the device. If PoE is not used for power supply, connect a suitable power adapter. Never place the probes or the Ethernet cable in cable trays shared with power cables.



- **Device binary inputs** – connect the cables of the binary sensors (dry-contact, voltage input, LD-81 flood detector) to the terminal block using the supplied SP013 tool (see *Appendix 5*).

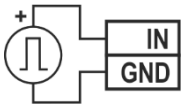
Internal wiring diagram of the inputs:



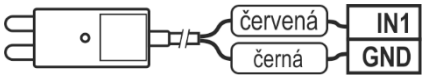
+12 V – power supply output for binary sensors, maximum output current 150 mA

Dry contact:

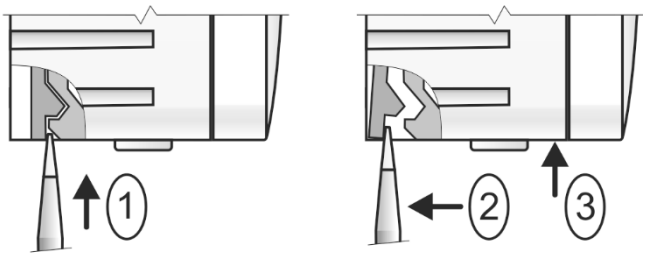
Voltage input:



Two-wire flood detector LD-81:



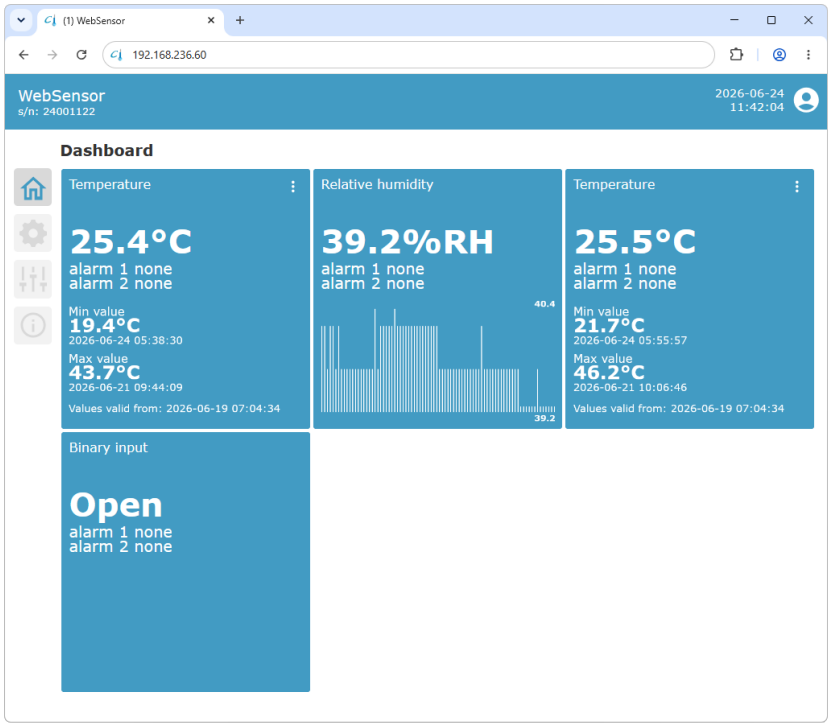
- **Removing the device** – use a suitable screwdriver to release the mounting plate latch and slide the device out of the mounting plate.



Initial device setup

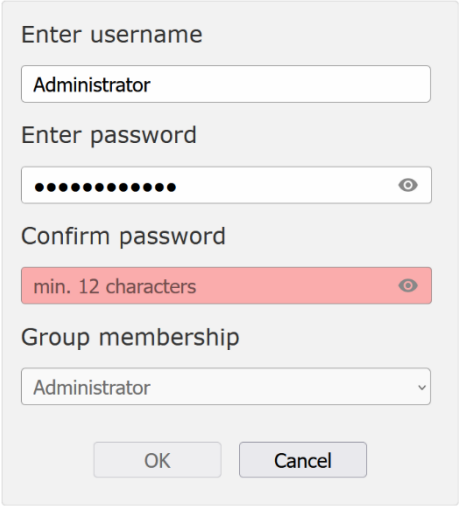
- **Determining the device IP address** – by default, the device IP address is assigned by a DHCP server. The orange LED on the right side of the RJ45 connector indicates that a valid IPv4 or IPv6 address is available. The device IP address can be found using the TSensor or COMET Vision software. For more information, see chapter *How to determine device IP address*.

- **Opening the device web page in a browser** – enter the device IP address obtained in the previous step into the browser. After entering the address, the device dashboard with the measured values will be displayed.

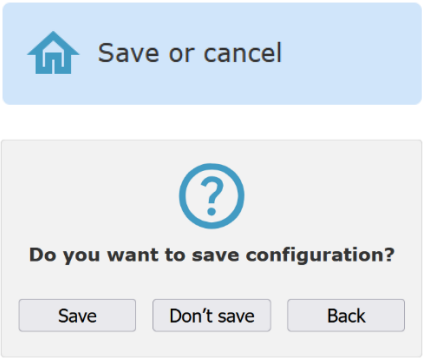


- **Select the Settings menu item**

- **Entering the administrator password** – in the first step of the setup, you will be prompted to enter the password for the administrator account. It is not possible to continue the setup without entering the password. Entering the administrator password is required during the initial device setup.



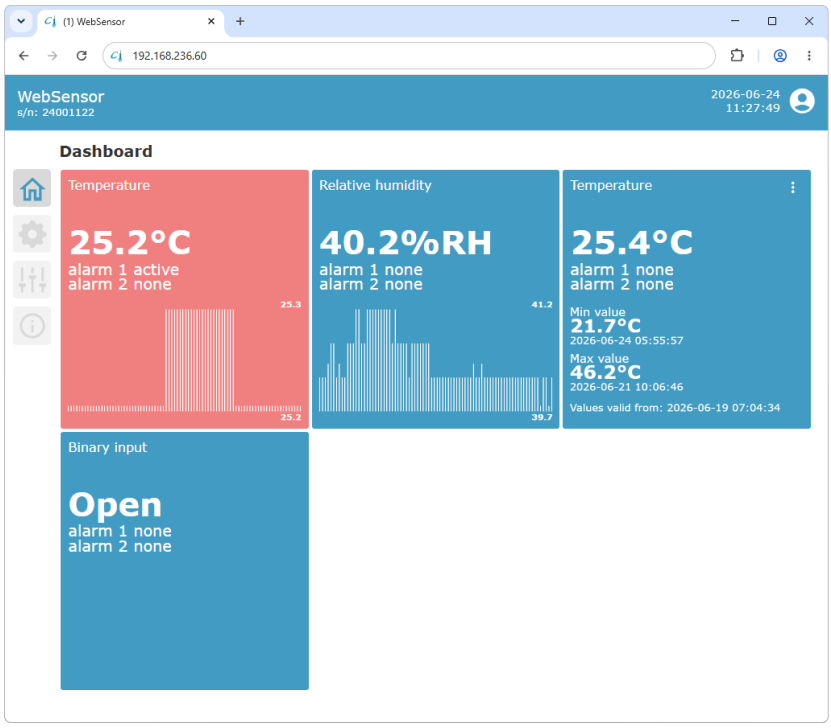
- **Other device settings** – configure the remaining device functions as needed. A description of individual functions can be found in the chapter *Device setup*.
- **Saving the settings** – after making the necessary changes, it is required to save the settings. This is done by selecting the “Save or cancel” menu option and confirming the selection in the following dialog window.



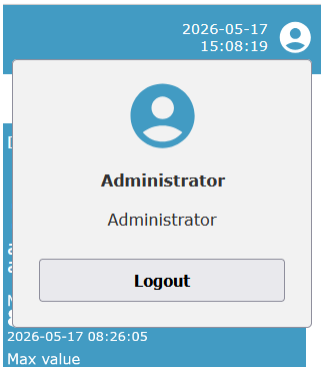
Features

Dashboard

The dashboard allows the display of trends in measured values as well as recorded minimum and maximum values for individual channels. You can switch between these views by pressing the tile. If an alarm is present on a measurement channel, the tile is displayed in red. The number of displayed tiles depends on the number of quantities measured by the device. The tile size automatically adapts to the screen resolution.

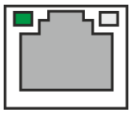
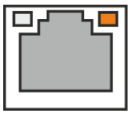


Tile	Description
	Menu item for displaying measured values, trend graphs, and recorded minimum and maximum values.
	Selecting this item starts a configuration session. During the session, the required configuration changes can be made. Only one configuration session can be active at a time.
	Service options menu. The content of this menu varies depending on the device model and the permissions of the currently logged-in user. Here, it is possible to detect probes, restart the device, perform a factory reset, update the firmware, and download a diagnostic log.
	Device information page. This menu item can also be used to download the SDK. This file contains technical information about the communication protocols used.

	This header item contains information about the logged-in user and allows the user to log out. 
	Allows clearing the minimum and maximum value memory. The reset can be performed selectively for individual channels or for all channels at once.

Status LED

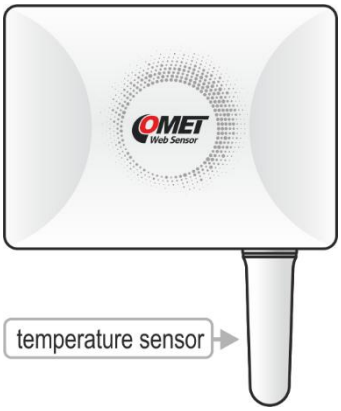
The status of the network communication is indicated by the LEDs on the RJ45 network connector.

LED	Description
	A flashing green LED on the left side of the connector indicates network activity.
	The orange LED on the right side of the connector indicates IP address availability. The LED is lit when the device has an active physical network connection and a valid IPv4 or IPv6 address. An IPv4 address may be statically assigned, obtained from a DHCP server, or assigned by the APIPA function if the DHCP server is unavailable.

Models of Web sensors

This section provides a list of available Web Sensor models. The differences between individual models lie in the type of sensors used and their measurement range. Each measured value is assigned to a single input channel. The device user cannot change the measurement range or the type of measured value.

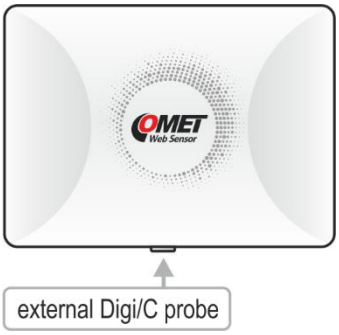
PA8610



Single-channel compact thermometer

This model measures temperature using a sensor stem that is integrated into the device. The device is designed for direct installation in the measured environment. The sensor stem should point downwards.

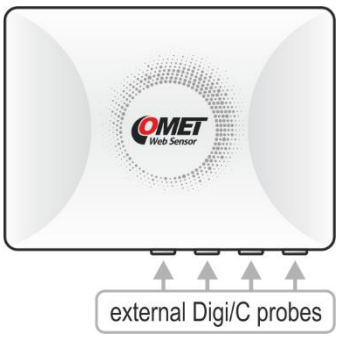
PA8611



Device for connecting one external probe

The device allows the connection of one temperature probe (DST, DST+) or one combined temperature-humidity probe (DSRH, DSRH+). The probe is not included with the device and can be ordered separately. It is recommended to install the device outside the monitored environment and place only the probe in the measurement area.

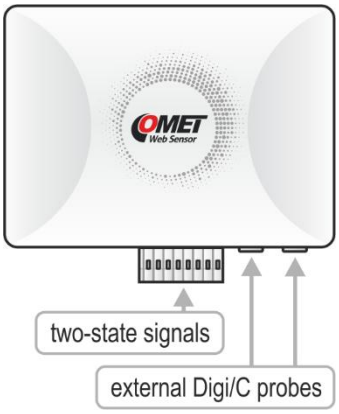
PA8641



Device for connecting up to four external probes

The device allows the connection of up to four temperature probes (DST, DST+) and/or combined temperature-humidity probes (DSRH, DSRH+). Any combination of external probes can be used. The probes are not included with the device and can be ordered separately. It is recommended to install the device outside the monitored environment and place only the probes in the measurement area.

PA8652



Device for connecting two external probes and three binary inputs

The device allows the connection of up to two temperature probes (DST, DST+) and/or combined temperature-humidity probes (DSRH, DSRH+). Any combination of external probes can be used. The probes are not included with the device and can be ordered separately. It is recommended to install the device outside the monitored environment and place only the probes in the measurement area. For monitoring binary (on/off) signals, the device is equipped with three binary inputs. The device can supply power to external binary detectors via two +12 V terminals.

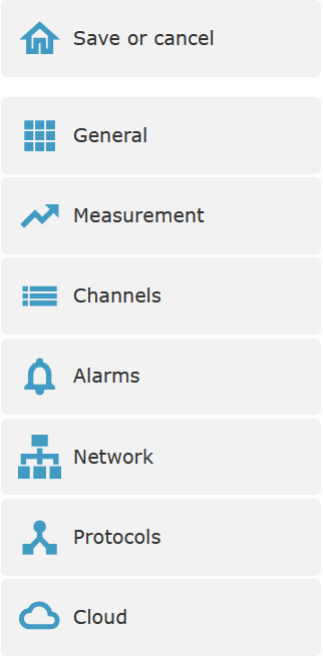
Device setup

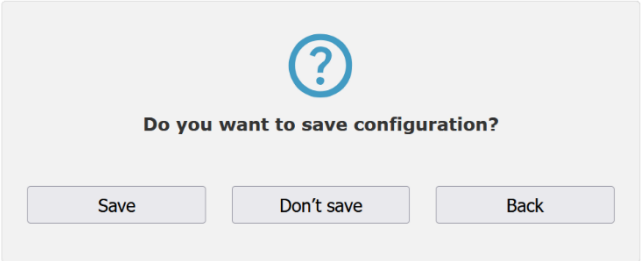
Conventions

Configuration session

Device setup uses a feature called a configuration session. Once a device setup is started, settings can be modified as needed. All setup changes are stored in temporary memory. Changes to settings are applied only after they are saved. Settings can be saved or discarded using the “Save or cancel” menu option. The same option is also used to cancel changes made during the configuration session.

Only one configuration session can be active at a time. This means that access to the settings from other locations is blocked for the duration of the session. Access is restored only after the previous session has ended. The inactivity timeout for a configuration session opened in a web browser is set to 20 minutes. If the browser window is closed, the session will terminate after 2 minutes. The structure of the settings is described in *Appendix 3*.

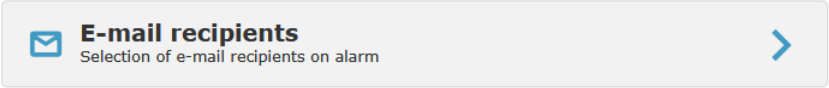




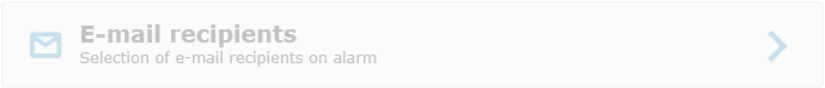
Globally disabled features

Some device functions can be enabled or disabled globally. One example is email notifications. Email notifications must be enabled globally before they can be used. For channel alarms, the email recipients must then be configured. If a function is disabled globally, the corresponding channel configuration tiles are displayed in a lighter color.

Feature is globally enabled:

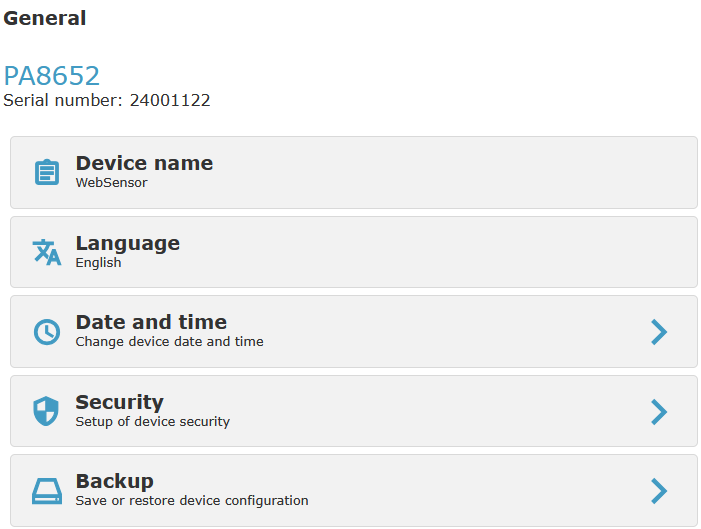


Feature is globally disabled:



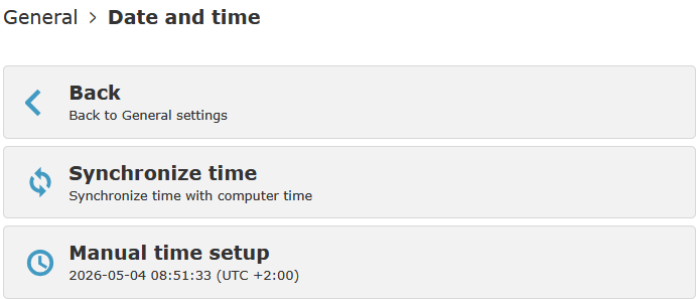
General settings

The general device settings allow configuration of the device name, time, security settings, language, and saving the configuration to a backup file. The device's graphical interface is fully localized into the following languages: English, Czech, Dutch, Polish, Spanish, French, German, and Italian.



Date and time

Settings of date and time for the device. Web Sensor devices are equipped with a real-time clock powered by an internal battery. This allows the device to maintain the current time even when powered off. The time can be synchronized with a computer or mobile phone using the “Synchronize time” option. The time zone (UTC offset) is set automatically after synchronization. The device time is updated after the settings are saved.



Be aware that improper changes to the time zone, without correctly adjusting the current time, may cause incorrect data interpretation in the COMET Cloud history.

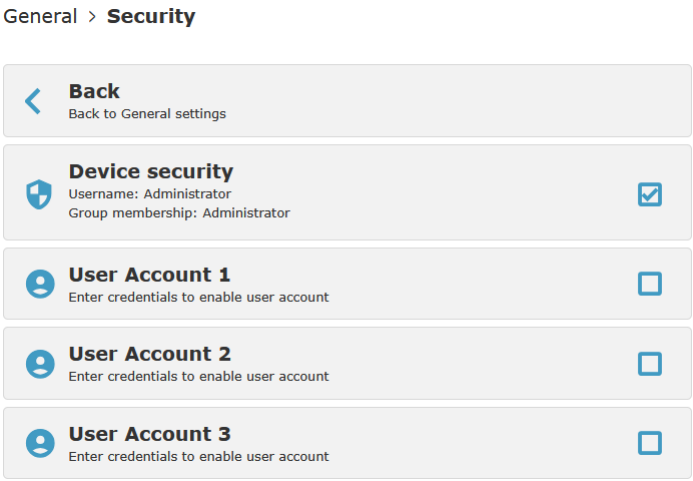
Security

Web Sensors have an integrated advanced security system. It is possible to set up to four user accounts, each assigned to one of three security levels. The privileges of the individual levels are described in the table below.

As part of the initial device setup, a password for the administrator account must be set. Without setting this password, it is not possible to proceed with the device configuration. Setting up the other user accounts is optional. The minimum password length is 12 characters.

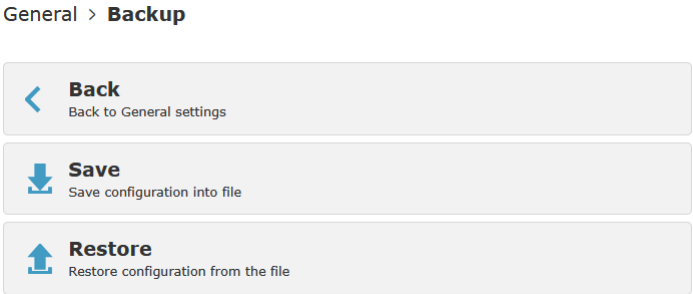
In case the administrator password is lost, the device must be restored using the *Factory defaults procedure*.

Feature	Administrator	Power user	User
Show current values	X	X	X
Clear min/max values	X	X	
Detect probes	X	X	
Device restart from web	X	X	
Factory defaults from web	X	X	
Device setup	X	X	
Security settings	X		
Firmware update	X		
Download diagnostic	X		



Backup

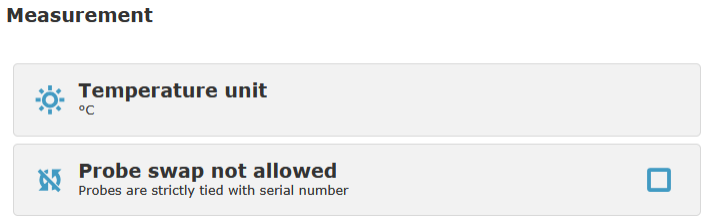
Device settings can be saved to a file and restored later. All device parameters are stored in this file, except for security settings. Please note that network parameters, such as the IP address, are also included in the saved data. When restoring the configuration to a different device, a conflict may occur if a static IP address is used. In such a case, the network parameters must be manually adjusted after restoration. The backup file does not include user-uploaded certificates. These certificates must be uploaded separately.



Measurement settings

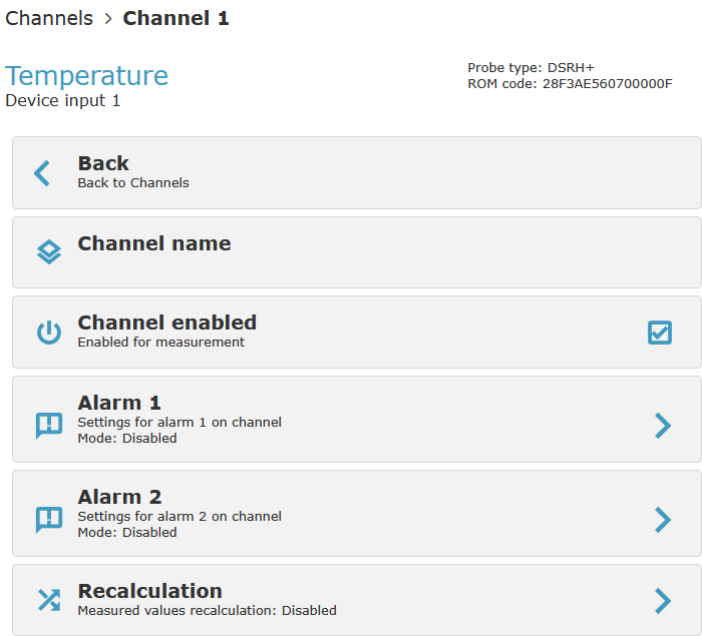
Settings related to the device measurement functions. Available features depend on the device model. The temperature unit can be selected as either °C or °F. Devices equipped with a CINCH (RCA) connector allow the connection of temperature probes (DST, DST+) and combined temperature-humidity probes (DSRH, DSRH+). For the device to measure using the probes, the probes must be detected. Probe detection is performed automatically when the device is restarted, provided that a different probe has not previously been detected on the input. Manual probe detection can be performed via Service Options / Detect Probes. The device supports automatic replacement of a probe with another probe of the same type, provided that the probe type has already been detected. This means that a temperature-humidity probe can be replaced with another temperature-humidity probe. The same applies to temperature probes. If this behaviour is not desired, automatic probe replacement can be disabled using the "Probe

swap not allowed" option. In this case, the device stores the probe serial number and allows operation only with that specific probe. If the probe is replaced, manual probe detection must be performed.



Channel settings

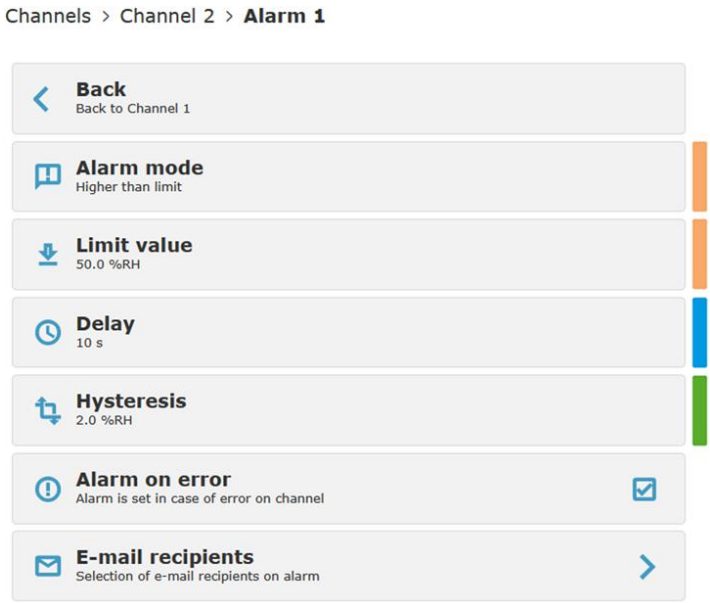
The device is equipped with a number of channels according to the model type. Channels can be enabled or disabled. If a channel is disabled, the measured values are not displayed on the dashboard. The channel name can be changed as required. If the channel name is left blank, the device automatically assigns a channel name according to the selected language. Please note that after changing a channel name, new channels are created in COMET Cloud and COMET Database. Each channel has two independent alarm limits, which can be configured separately. If required, the measured values can be recalculated using a linear equation (i.e. a correction of the measured values can be applied).



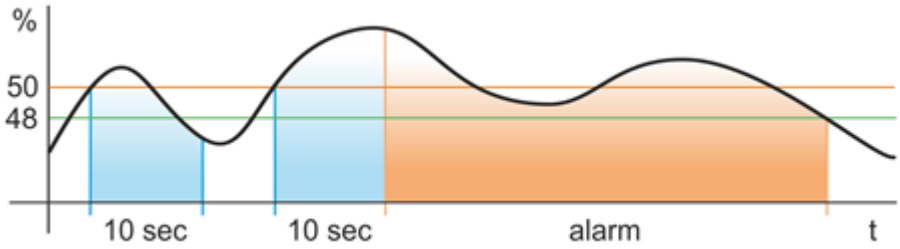
Settings alarm for a channel

Each channel allows configuration of two separate alarms. The alarm mode selects the alarm direction: Lower than limit, Higher than limit, or Disabled. The limit value defines the threshold for alarm activation. An alarm is activated when the measured value exceeds the selected limit for the period specified by the Delay option. The alarm state is cleared when the measured

value returns within the selected hysteresis range. Optionally, a channel alarm can also be triggered by a measurement error.



Web sensors support email notifications when a channel alarm is activated. Up to four email recipients can be configured. Recipient email addresses are configured in the *Email Protocol Settings* section. Each recipient can be enabled or disabled individually in the alarm settings.



The image above illustrates how the alarm settings work. The alarm limit is set to 50%, with a delay of 10 seconds and a hysteresis of 2%. Initially, the alarm is not activated because the measured value does not exceed the limit for the entire delay period. The alarm is then activated because the measured value remains above the limit longer than the configured delay time. The alarm state persists until the measured value falls below the limit minus the hysteresis value (50% − 2% = 48%).

Recalculation of measured values

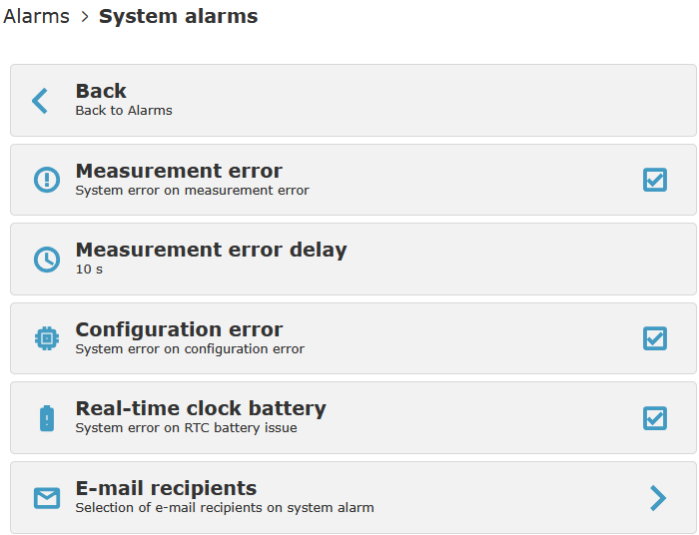
The measured values can be recalculated using a linear equation. This option can be enabled if a correction of the measured values is required. Enabling the recalculation does not affect the calibration constants of the device or the probes.

Alarm settings

System alarms

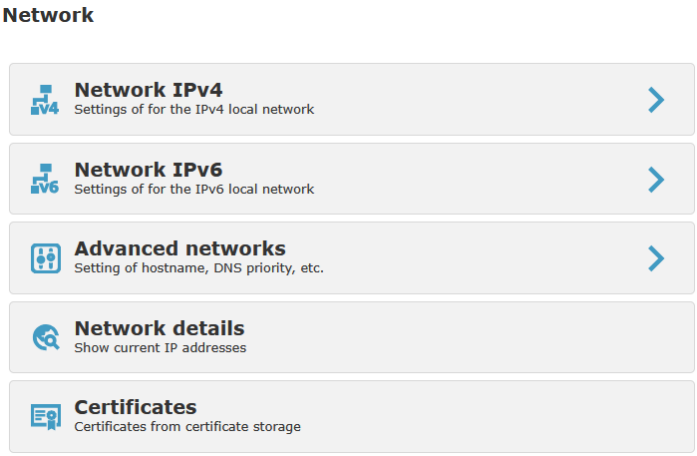
System alarms are used to monitor the correct operation of the measurement chain, including the device and probes. They indicate faults or abnormal conditions of the device and connected probes. Unlike measured value alarms, which indicate issues in the technology being monitored by the device, system alarms may be intended for a different group of users (e.g. maintenance personnel).

The device has three types of system alarms: a measurement channel error alarm, a configuration error alarm, and a real-time clock (RTC) battery error alarm. The measurement channel error alarm is activated if an error condition on any measurement channel persists for a period defined by the delay setting.



Network settings

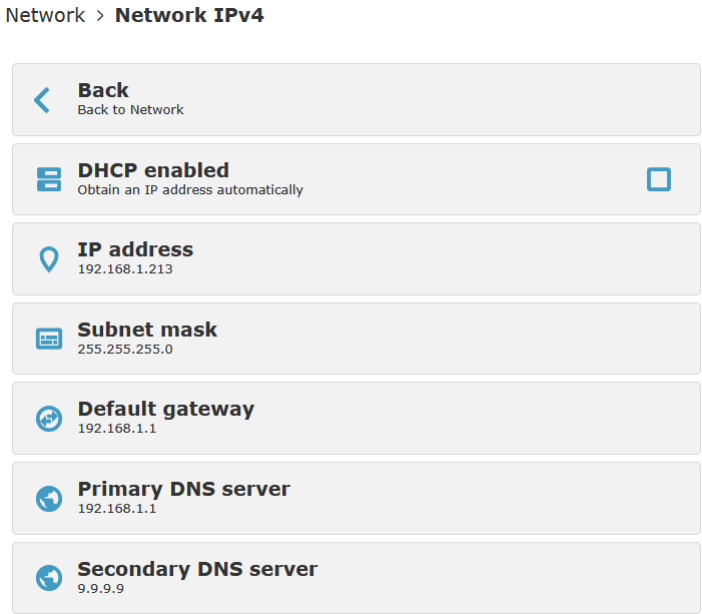
Web Sensor sensors support both IPv4 and IPv6 protocols. All services and communication protocols can operate over both IP versions, which may run simultaneously. By default, DHCP is enabled for IPv4 and IPv6 is configured to obtain an address automatically.



Current network parameters, such as IP addresses, can be viewed using the “Network details” menu item. The device allows user certificates to be uploaded for protocols using TLS connections. Certificates can be uploaded using the COMET Vision application once it becomes available. Information about the currently used certificates can be obtained via the “Certificates” menu item.

IPv4 network

By default, DHCP is enabled for IPv4. In this case, the device requests an IP address from a DHCP server. If a DHCP server is not available, the device temporarily assigns itself an address from the APIPA range (i.e. 169.254.0.1 to 169.254.255.254). This assignment takes place after approximately 40 seconds after device startup. Even after an APIPA address has been assigned, the sensor continues attempting to contact a DHCP server to obtain a valid IP address.



If required, a static IP address can be configured instead of DHCP. In such cases, contact your network administrator. Incorrect configuration of the IP

address, subnet mask, gateway address, or DNS settings may cause network communication problems. If the configured IP address is already in use on the network or falls within the DHCP server address range, IP address conflicts may occur and affect communication with other devices on the network. When configuring a static IP address, a basic check is performed to detect configuration conflicts. Possible error states are described in the table below.

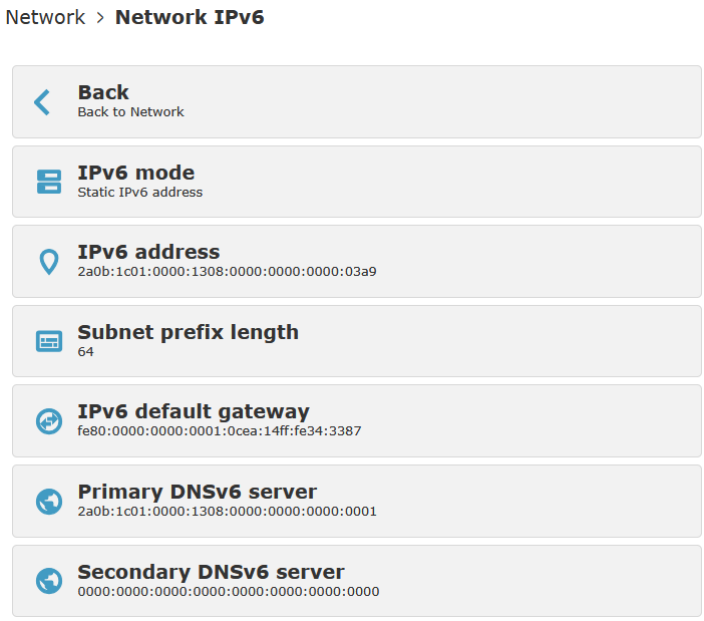
The local IP address of the sensor can be determined using the method described in the *How to determine device IP address* chapter.

Return code	Note
ERR_IP_IS_BROADCAST	The static IP address of the device is set to a broadcast address.
ERR_IP_GW_IS_SAME	The static IP address of the device is the same as the gateway IP address.
ERR_NOT_SAME_SUBNET	The static IP address of the device is not in the same subnet as the gateway address.

IPv6 network

The device is set by default to automatically obtain an IPv6 address. In this case, it uses either stateless address autoconfiguration (SLAAC) or DHCPv6, if available on the network. If SLAAC is used and it is not possible to obtain a DNS address from a DHCPv6 server, the “Backup DNSv6 server for SLAAC” setting is used. DNS via Router Advertisements (RFC 8106) is not supported. When IPv4 and IPv6 are used simultaneously, the IPv4 address assigned by the DHCP server is usually available sooner than the automatically assigned IPv6 address.

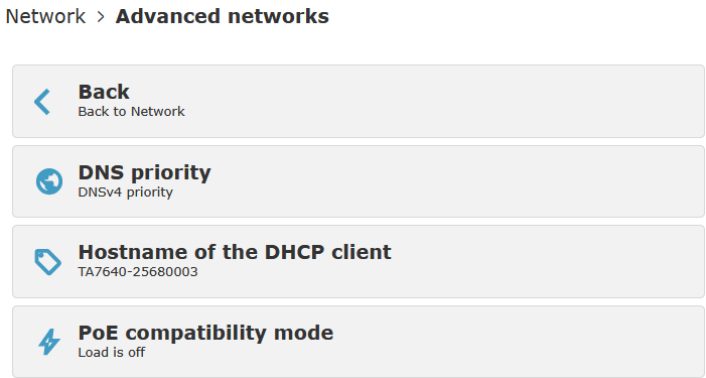
If necessary, a static IPv6 address can be configured, or IPv6 protocol support can be completely disabled. Disabling IPv6 is recommended only in cases where it is known that the local network does not support IPv6.



The device can be used in environments with IPv6-only deployment. Since the device does not allow IPv4 to be fully disabled, it is recommended in such deployments to configure a static IPv4 address to prevent any potential negative impact on network traffic.

Advanced networks

In advanced network settings, it is possible to specify whether IPv4 or IPv6 will be preferred for DNS. This determines whether DNSv4 or DNSv6 servers are used with priority, and whether A or AAAA records are requested preferentially. It is also possible to set the DHCP hostname and the PoE compatibility mode.



Some PoE switches incorrectly implement the IEEE 802.3af standard. In the case of low-power devices, such as Web Sensor sensors, these devices may not be able to provide proper power. This often results in continuous power cycling (i.e., repeated device restarts). For Web Sensor devices, a PoE compatibility mode can be enabled in such cases. This increases the device's power consumption, allowing it to operate even with these non-compliant network components.

When PoE compatibility mode is enabled, devices with a measuring probe may not meet the measurement accuracy specified in the technical documentation. If the device is powered exclusively by a power adapter, do not enable PoE compatibility mode.

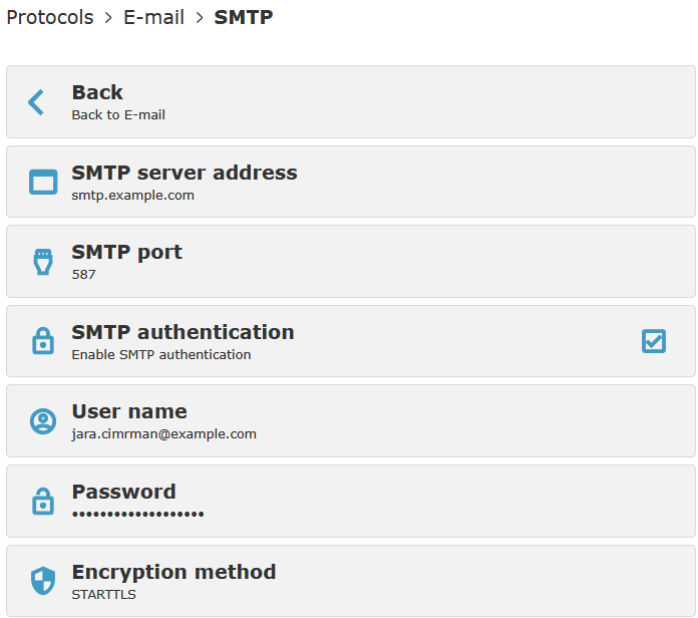
Protocols settings

Email

Web sensors can send alarm emails directly via an SMTP server. The device can send a warning email when an alarm occurs on a channel or when the alarm is cleared. Emails triggered by system alarms can provide information about measurement errors or other hardware-related issues. The device can also send keep-alive emails and repeat warning emails if an alarm on a channel persists.

If COMET Cloud or COMET Database is used, it is not necessary to configure email sending directly on the device. COMET Cloud and COMET Database provide their own independent methods for sending warning emails.

To enable email sending from Web sensors, the connection to the SMTP server must be properly configured. Information on how to set SMTP parameters can be provided by a network administrator. The SMTP server address and port must be set according to the server being used. If SMTP authentication is required, a username and password must be configured. The username is typically the same as the sender email address. If encrypted communication with the server is used, TLS or STARTTLS can be enabled. Common combinations of SMTP port, encryption, and authentication are shown in the table below.

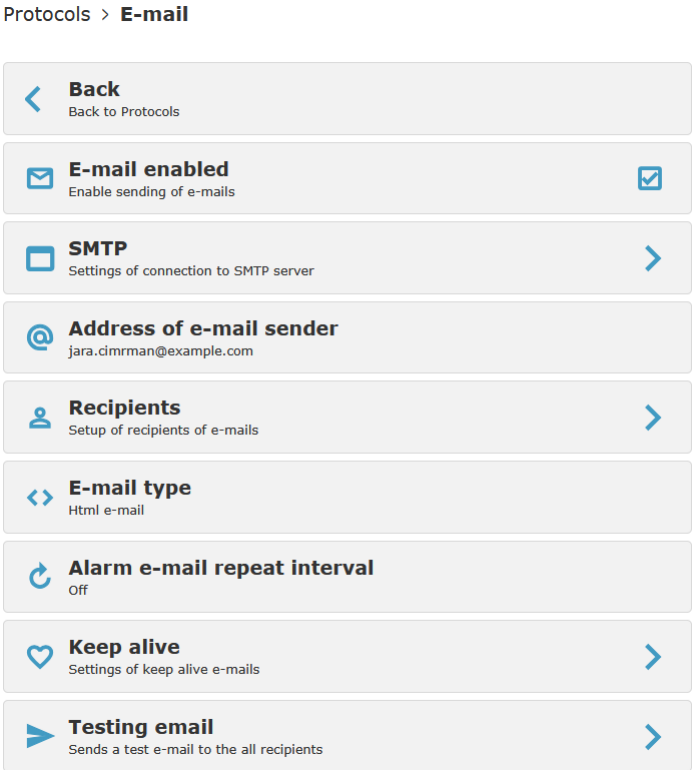


For proper SMTP communication, the sender address and recipient addresses must be configured. Web Sensor devices support up to four recipients, each of which can be independently assigned to different alarms.

Emails can be sent in either plain text or HTML format. The interval for repeated alarm emails can be set from 10 minutes to 12 hours. If this option is enabled, the device sends alarm emails repeatedly at the specified interval as long as the alarm persists.

Repeated emails indicating proper system operation can be sent at intervals from 1 to 12 hours, as needed.

SMTP server mode		SMTP port	Set username and password	Encryption method
No auth. with no encryption		25	No	No
Auth. with no encryption		25	Yes	No
Auth. with encryption	TLS	465	Yes	TLS
Auth. with encryption	Start TLS	587	Yes	STARTTLS
Auth. with encryption	OAuth	465	Not supported mode	
Auth. with encryption	OAuth	587		



The correctness of the SMTP server settings can be verified using a test email. The parameters of the test email are taken from the current configuration session. The progress of sending the test email is available under the “Diagnostics” section.

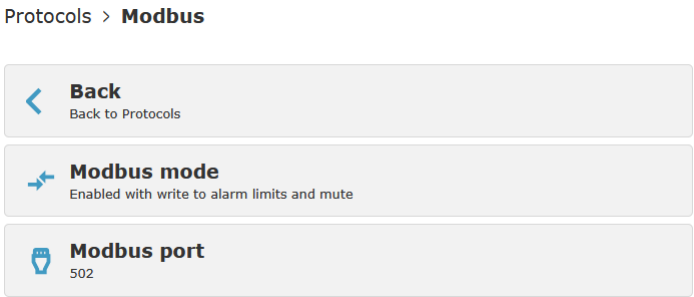
Return codes for the test email sending request are listed in the table below.

Return code	Description
ERR_MAIL_NET_NO	It is not possible to send a test email due to network connection issues.
ERR_MAIL_DNS	DNS resolution error. Ensure that the correct SMTP server address is entered and that the DNS server IP address is properly configured.
ERR_MAIL_SOCK_CREATE	Internal error: unable to create a network socket.
ERR_MAIL_SEC_CREATE	Internal error: unable to create TLS socket. This error may occur when an invalid user CA certificate has been uploaded.
ERR_MAIL_BIND	Internal error: socket bind error.
ERR_MAIL_CONNECT	Unable to establish a TCP connection to the SMTP server. Ensure that the correct SMTP server address and port are configured. Check whether outgoing connections are blocked by a firewall. If the SMTP server is in a different subnet (e.g. on the Internet), verify the correctness of network parameters such as the subnet mask and gateway IP address.
ERR_MAIL_TLS1	Unable to establish a TLS connection. Make sure the SMTP server is correctly configured and that the correct port is set. Port 465 is typically used for TLS encryption. This error may also occur if a user CA certificate is installed and the SMTP server could not be verified, or if the SMTP server does not support TLS 1.2.
ERR_MAIL_LOGIN	Invalid server response after the connection has been established. Ensure that the correct SMTP server address is entered and that the TCP port matches the selected encryption mode (e.g. whether the server expects STARTTLS while the device is configured for TLS, etc.).
ERR_MAIL_HELO	Invalid response to the HELO or EHLO command. It is possible that there is no SMTP server on the opposite side, or that the encryption mode is incorrectly configured. Verify whether TLS is required for the selected port.
ERR_MAIL_STARTTLS	Error while executing the STARTTLS command. Ensure that the SMTP server supports this command.

ERR_MAIL_TLS2	Unable to switch to a TLS connection after the STARTTLS command. This error may also occur if a user CA certificate is installed and the SMTP server cannot be verified, or if the SMTP server does not support TLS 1.2.
ERR_MAIL_AUTH_LOGIN	Authentication error. Error while sending the AUTH LOGIN command. Ensure that authentication is enabled on the SMTP server and that the AUTH LOGIN command is supported.
ERR_MAIL_AUTH_USER	Authentication error. Error while sending the username. Ensure that the correct username is entered.
ERR_MAIL_AUTH_PASSWORD	Authentication error. Error while sending the password. Verify that the correct password is entered for the configured user.
ERR_MAIL_SENDER	Error while sending the MAIL FROM command.
ERR_MAIL_RCPT	Error while sending the RCPT TO command.
ERR_MAIL_DATA	Error while sending the DATA command.
ERR_MAIL_BODY	Error while sending email message data.
ERR_MAIL_DATA_END	Error while sending the end-of-data marker (dot command).
ERR_MAIL_DATA_QUIT	Error while sending the QUIT command.
ERR_MAIL_AUTH_ERR	Authentication error. It is likely that an incorrect username or password is entered. Make sure the correct sender email address is set. The sender address is usually the same as the authentication username. Another possible cause is that the SMTP server rejected the connection for another reason (e.g. inability to connect from the given subnet).
ERR_MAIL_OTHER_ERR	Other error during communication with the SMTP server. It is likely that the email was not sent. More detailed information can be obtained from the communication log below.
ERR_MAIL_NO_WEB_CONFIG	The test email cannot be sent because there is no active configuration session.

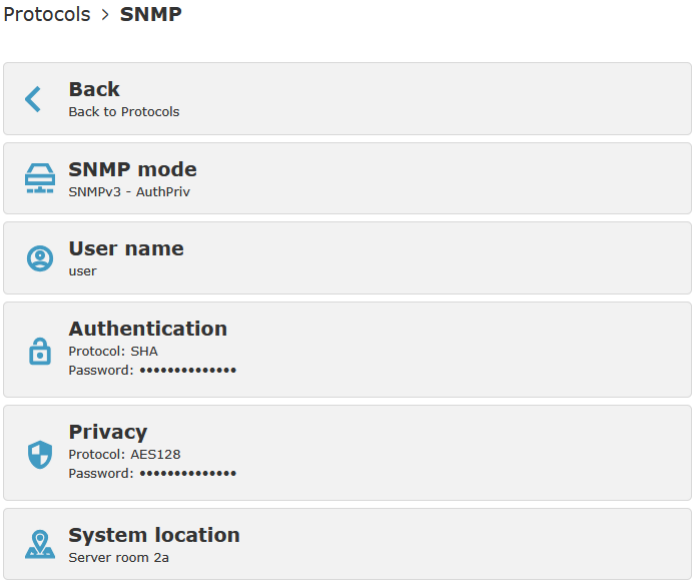
Modbus

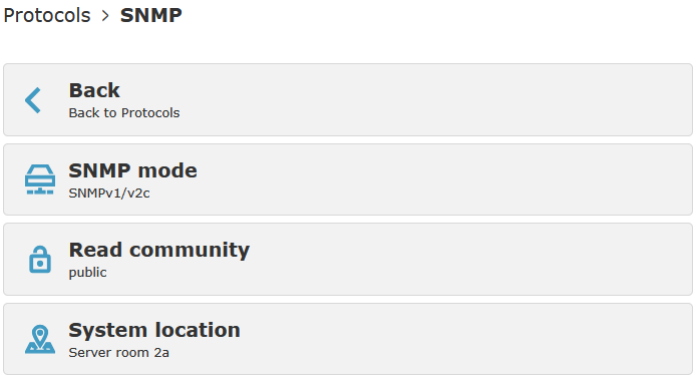
The device has an integrated Modbus TCP server that allows third-party systems (e.g., SCADA) to read current values. The server can handle two Modbus TCP connections simultaneously. By default, the protocol is enabled on port 502. The Modbus TCP server can be set to one of three modes: disabled, enabled in read-only mode and enabled with the ability to modify alarm limits. By default, read-only access is enabled. A description of the registers is provided in the Modbus TCP chapter *Modbus TCP*.



SNMP

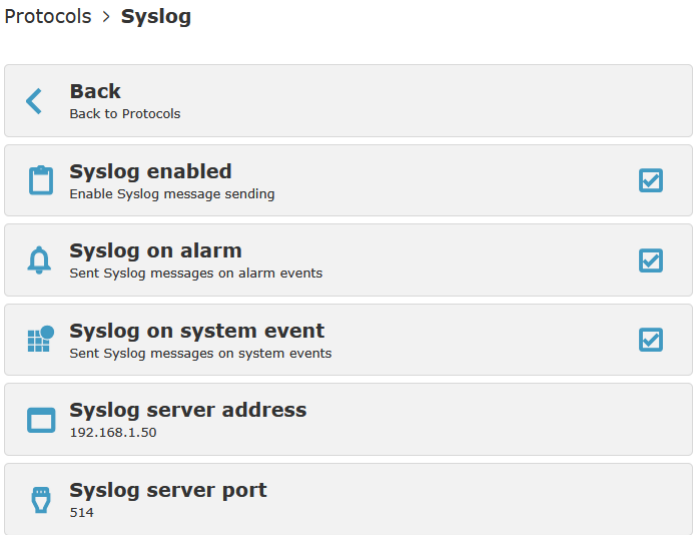
Web Sensor devices can provide measured values via the SNMP protocol. SNMP versions SNMPv1, SNMPv2c, and SNMPv3 are supported. The default SNMP mode is SNMPv1/v2c. The community string is set to “public” by default. SNMPv3 supports three security modes (NoAuthNoPriv, AuthNoPriv, and AuthPriv). Depending on the selected mode, a username, authentication password, and encryption password must be configured. The “System location” field can contain a more detailed specification of the device’s installation site. Writing via SNMP is not supported. A detailed description of the SNMP protocol, including OID keys, is provided in the chapter *SNMP protocol*.





Syslog

The sensors allow sending messages to a configured Syslog server. The UDP protocol is used for sending Syslog messages with a default port of 514. Syslog messages are divided into two classes – alarm messages and system event messages. A detailed description of the messages is provided in chapter *Syslog protocol*.

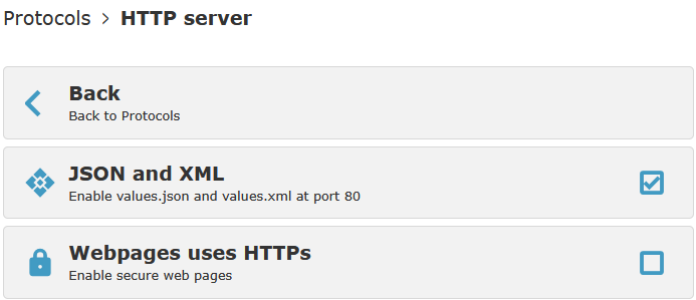


HTTP server

Measured values can be obtained using HTTP GET requests sent to the HTTP server running on the sensor on TCP port 80. Values can be provided in XML or JSON format via the files *values.xml*, *values.json and values-ex.json*. This function is independent of the device security settings and can be enabled or disabled as needed. By default, this functionality is disabled. Detailed information is provided in the chapter *JSON and XML via http server*.

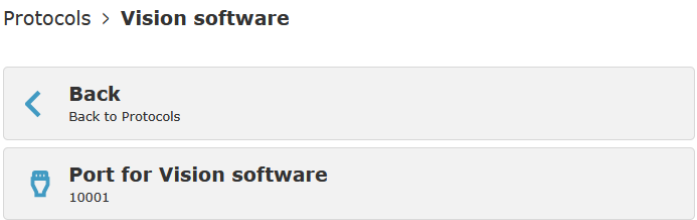
By default, the sensor does not have HTTPS enabled for the web server. If necessary, HTTPS can be enabled. After enabling the HTTPS server, the maximum number of simultaneously connected clients is reduced from four to three. When HTTPS is activated, a certificate signed by the COMET Root CA authority is used by default. For this reason, when accessing via

a web browser, it is necessary to approve a security exception. If needed, a user certificate can be uploaded.



Vision software

Configuration of the TCP port for communication with the COMET Vision software. The Web Sensor device functions here as a TCP server. The default port is set to 10001. Communication with the software is secured using the TLS protocol.

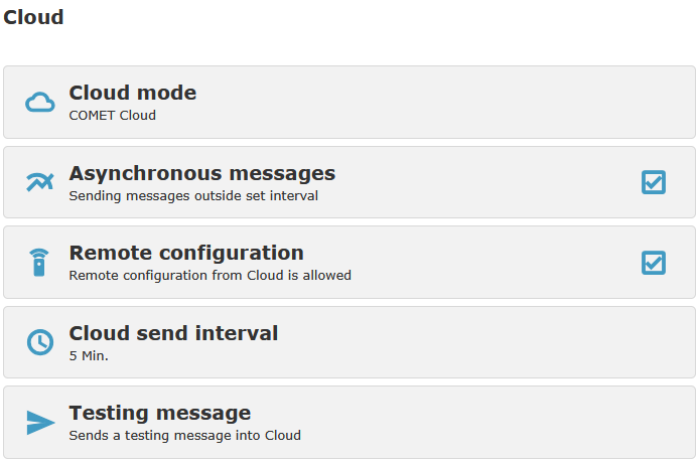


Cloud protocol settings

Web Sensor devices can send current measured values to a remote server using HTTP(S) POST requests in JSON format. This function can be used to transmit data to COMET Cloud, COMET Database, or a third-party system. A detailed protocol description is provided in *JSON structure* chapter. If measured values cannot be successfully delivered to the server, they are stored in internal memory and sent later. The memory capacity is 2,600 data sets. This feature prevents data loss in the event of network connectivity failure. Values stored in memory are retained even during power outages. Data are deleted after successful delivery via the cloud protocol or when the device settings are changed. The cloud protocol has two modes: “COMET Cloud” and “COMET Database / User Server”.

COMET Cloud mode

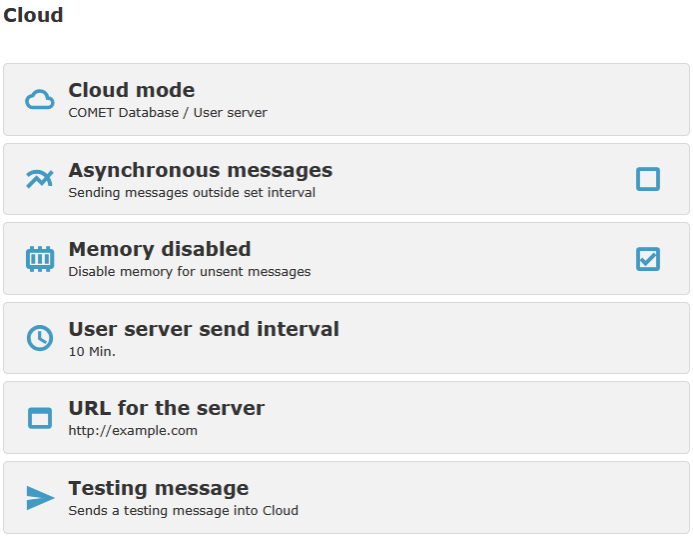
By enabling this mode, the device starts sending measured values directly to COMET Cloud. COMET Cloud is a paid service. With a newly purchased sensor, COMET Cloud can be used free of charge for three months. This trial period allows you to test the COMET Cloud features at no additional cost. To make the device visible in COMET Cloud, it must be registered. The registration procedure is described on the registration card supplied with the device.



The sending interval to COMET Cloud can be set from 5 minutes to 12 hours. The minimum recommended interval is 10 minutes. When asynchronous messages are enabled, alarm messages are also sent outside the selected interval. Messages are also sent when an alarm clears and when the device configuration is changed. Asynchronous messages are enabled by default. Web Sensor devices support remote configuration via COMET Cloud. If remote configuration is not desired, it can be disabled.

COMET Database / User server

This mode allows measured values to be sent to COMET Database or a third-party system. COMET Database is a data collection system based on an SQL database server, enabling data collection and analysis from a wide range of COMET devices. COMET Database can be used as an alternative to COMET Cloud in highly secure environments where cloud services cannot be used. A 30-day trial version of COMET Database is available. The procedure for connecting Web Sensor devices to COMET Database is described in the COMET Database manual.



The sending interval can be set from 10 s to 12 hours. When asynchronous messages are enabled, alarm messages are also sent outside the selected

interval. Messages are also sent when an alarm clears. Asynchronous messages are enabled by default. The device stores messages in internal memory if they cannot be delivered due to a connectivity outage. Once the connection is restored, these messages are sent. If this behaviour is not desired, message buffering can be disabled. In this case, messages will be lost during cloud connectivity outages. The URL must be set to the entry point of COMET Database or a third-party HTTP(S) server. User certificates can be uploaded if authentication of delivered messages via HTTPS is required when using a custom server.

Testing Cloud message

Sending messages to the cloud server can be tested using a test message. The parameters for the test message are taken from the current configuration session. Information about the result of the test message transmission is available under the “Diagnostics” menu item.

Error codes for the cloud server test message are listed in the table below.

Return code	Description
ERR_CLOUD_NET_NO	The test message cannot be sent due to network connectivity issues.
ERR_CLOUD_DNS_ERR	Error resolving DNS name. Make sure the cloud server URL is entered correctly and that the DNS server IP address is configured correctly.
ERR_CLOUD_SOCK_ERR	Internal error: unable to create network socket.
ERR_CLOUD_SSL_ERR	Internal error: unable to create TLS socket. This error may occur when invalid certificates are uploaded for cloud connection.
ERR_CLOUD_BIND_ERR	Internal error: socket bind error.
ERR_CLOUD_CONNECTION_ERR	Unable to establish a TCP connection to the cloud server. Make sure the cloud server address is entered correctly. Check whether outgoing connections are blocked by a firewall. If the cloud server is in a different subnet (e.g. on the internet), verify the network settings such as subnet mask and gateway IP address.
ERR_CLOUD_CONNECTION_TLS_ERR	Unable to establish a TLS connection. Make sure the cloud server address is correctly configured. This error may also occur if the connection is rejected due to certificate verification failure,

	or if the server does not support TLS 1.2.
ERR_CLOUD_TRANSFER_ERR	An error occurred during data transmission over the open network socket.
ERR_CLOUD_WRONG_HTTP_CODE	Invalid HTTP response code received from the server.

Communication protocols

Modbus TCP

Using the Modbus TCP protocol, measured values can be read from the device by third-party software, such as SCADA systems. The Modbus TCP server supports simultaneous connections from two clients. The default TCP port is 502. The Modbus device address (Unit Identifier) can be arbitrary. Writing is allowed to registers for alarm limit settings. Examples of reading via the Modbus TCP protocol in Python are available in the SDK (About / SDK). A detailed specification of the Modbus protocol is freely available at *www.modbus.org*.

Supported Modbus commands (functions):

Mode	Code	Description
Read only	0x03	Read 16-bit holding registers.
	0x04	Read 16-bit input registers.
With alarm limit write enabled	0x03	Read 16-bit holding registers.
	0x04	Read 16-bit input registers.
	0x10	Write 16-bit holding registers.

Depending on the communication library used, it may be necessary to use the register number instead of the register address. The register number is equal to the register address incremented by one. For example, register number 0x9C41 corresponds to Modbus address 0x9C40. In Modbus TCP protocol frames, the physical register address (numbered from 0) is transmitted.

Variable	Address [HEX]	Address [DEC]	Type	Variable
Device identification				
Serial number (The device serial number has 8 digits, which are split into four Modbus registers)	0x9C22	39970	RO	BCD
	0x9C23	39971	RO	BCD
	0x9C24	39972	RO	BCD
	0x9C25	39973	RO	BCD
Device type	0x9C26	39974	RO	HEX

Device states				
Configuration error	0x9C2A	39978	RO	INT
System alarm - measurement error	0x9C2B	39979	RO	INT
Low RTC battery voltage detected	0x9C2C	39980	RO	INT

Measured values				
Measured value on channel 1 … Measured value on channel 8	0x9C40 … 0x9C47	40000 … 40007	RO	INT*X
Alarm 1 state on channel 1 … Alarm 1 state on channel 8	0x9C48 … 0x9C4F	40008 … 40015	RO	INT
Alarm 2 state on channel 1 … Alarm 2 state on channel 8	0x9C50 … 0x9C57	40016 … 40023	RO	INT
Unit for channel 1 … Unit for channel 8	0x9C58 … 0x9C5F	40024 … 40031	RO	STR
Decimal places for the channel 1 … Decimal places for the channel 8	0x9C60 … 0x9C67	40032 … 40039	RO	INT
Measured value on the channel 1 … Measured value on the channel 8	0x9C68 … 0x9C77	40040 … 40055	RO	32b INT * (X+2)
Measured value on the channel 1 … Measured value on the channel 8	0x9C78 … 0x9C87	40056 … 40071	RO	IEEE 754 FLOAT
Minimum value for the channel 1 … Minimum value for the channel 8	0x9C88 … 0x9C8F	40072 … 40079	RO	INT*X
Maximum value for the channel 1 … Maximum value for the channel 8	0x9C90 … 0x9C97	40080 … 40087	RO	INT*X

Alarm limits				
Alarm 1 mode for channel 1 … Alarm 1 mode for channel 8	0x9CA4 … 0x9CAB	40100 … 40107	R/W	INT[1)]
Alarm 2 mode for channel 1 … Alarm 2 mode for channel 8	0x9CAC … 0x9CB3	40108 … 40115	R/W	INT[1)]
Alarm 1 limit for channel 1 … Alarm 1 limit for channel 8	0x9CB4 … 0x9CBB	40116 … 40123	R/W	INT*X
Alarm 2 limit for channel 1 … Alarm 2 limit for channel 8	0x9CBC … 0x9CC3	40124 … 40131	R/W	INT*X
Alarm 1 delay for channel 1 … Alarm 1 delay for channel 8	0x9CC4 … 0x9CCB	40132 … 40139	R/W	INT

Alarm 2 delay for channel 1 … Alarm 2 delay for channel 8	0x9CCC … 0x9CD3	40140 … 40147	R/W	INT
Alarm 1 hysteresis for channel 1 … Alarm 1 hysteresis for channel 8	0x9CD4 … 0x9CDB	40148 … 40155	R/W	INT*X
Alarm 2 hysteresis for channel 1 … Alarm 2 hysteresis for channel 8	0x9CDC … 0x9CE3	40156 … 40163	R/W	INT*X
Notes: **1)** Alarm modes: 0 – alarm disabled, 1 – alarm below limit, 2 – alarm above limit				

All registers for alarm limits support both read and write operations. To enable writing, the Modbus server mode must be set to “Enabled with write to alarm limits”. Writing to any of these registers triggers an update of the device alarm limits. For this reason, the interval between two consecutive write operations must not be shorter than 15 seconds. If writes are performed more frequently, the Modbus server will return a Modbus exception. When changing multiple alarm limits, it is recommended to use a read-modify-write approach across multiple registers at once.

Type of variables:

Type	Description
BCD	Register is at BCD format (16bit)
HEX	Number at HEX format (16bit)
INT	The register is a signed 16bit integer with a range from -32768 to 32767.
INT*X	The register is a signed 16-bit integer. To increase the resolution of the transmitted value, the measured value is multiplied by factor X. The number of decimal places can be obtained from registers 40032 – 40039 or from the table below. Example: if the number of decimal places is 1, a temperature value of 238 in the register corresponds to 23.8 °C. Error values are transmitted as numbers lower than -32000 (e.g. -32005 = Error 5).
STR	Two-byte text via a single 16bit Modbus register
INT*(X+2)	32bit measured value with resolution increased by a factor of 2. The value is transmitted via two 16-bit Modbus registers. The most significant part of the number is transmitted first (e.g. value 22.825 = reg1: 0, reg2: 22825). Error values are transmitted as numbers lower than -320000000 (e.g. -320000011 = Error 11).
IEEE 754	The value is a 32-bit IEEE 754 floating-point number transmitted via two Modbus registers. The value 22.704 is transmitted as reg1: 0xA317 and reg2: 0x41B5.

Table of decimal places for INT*X:

Measured value	Nr. of dec. places	Unit	Example
Temperature	1 (= *10)	°C or °F	125 = 12.5 °C
Relative humidity	1 (= *10)	%RH	801 = 80.1 %RH

Dew point Absolute humidity Specific humidity Mixing ratio Specific enthalpy Humidex Heat index	1 (= *10)	°C or °F g/m^3 g/kg g/kg kJ/kg	93 = 9.3 °C 85 = 8.5 g/m^3 76 = 7.6 g/kg 78 = 7.8 g/kg 445 = 44.5 kJ/kg 258 = 25.8
Barometric pressure	1 (= *10) 2 (= *100) 1 (= *10) 1 (= *10) 2 (= *100) 1 (= *10) 3 (= *1000) 1 (= *10)	hPa kPa mBar mmHg inHg inH_2O PSI oz/in^2	10117 = 1011.7 hPa 10117 = 101.17 kPa 10118 = 1011.8 mBar 7588 = 758.8 mmHg 2988 = 29.88 inHg 4062 = 406.2 inH_2O 14675 = 14.675 PSI 2348 = 234.8 oz/in^2
CO_2 concentration	0 (= *1)	ppm	890 = 890 ppm

Cloud protocol – JSON

Web Sensor can send measured values to a remote server using HTTP(S) POST requests with data in JSON format. A description of the JSON protocol can be found in this chapter. An example HTTP server for processing sensor messages in Python is available in the SDK (About / SDK). The cloud protocol supports two modes: COMET Cloud and COMET Database / User server. This chapter describes the format for the user server.

Measured values are transmitted using HTTP(S) POST requests with content in JSON format. The structure of the JSON message is described in the *JSON structure* chapter. Each message must be acknowledged by the server with an HTTP 200 response. If the server does not acknowledge the message, it is not marked as successfully sent. Unless the memory function for unsent messages is disabled, the message is stored and resent during the next connection attempt. Messages stored in memory are sent first. The memory capacity is 2600 message sets. The memory is cleared after changing the device settings. The sensor uses HTTP/1.1 transmission, which allows multiple POST requests (multiple JSON messages) to be sent within a single TCP (TLS) connection. If the server cannot correctly process this behaviour, the memory function must be disabled. The device supports both HTTP and HTTPS for JSON message transmission. If client authentication is required, it can be performed either using the COMET root CA certificate or by uploading user certificates through the COMET Vision application once it becomes available. The COMET root CA certificate is available in the SDK.

JSON structure

The structure of the JSON message is as follows:

```
{
  "JsonType": ...,
```

```
"JsonVersion": ...,
"OrderId": ...,
"MsgType": ...,
"MsgCache": ...,
"Sn": ...,
"Desc": ...,
"Kind": ...,
"AState": {
  "Reg": ...,
  "Mask": ...
},
"NConf": ...,
"ConfID": ...,
"Interval": ...,
"Time": {
  "Now": ...,
  "Sample": ...,
  "IsValid": ...
},
"LocalIP": ...,
"Channels": [
  {
    "Nr": ...,
    "En": ...,
    "Quant": ...,
    "Val": ...,
    "ValStr": ...,
    "Unit": ...,
    "Dec": ...,
    "Type": [ Static, Dynamic ],
    "Alarm": [ Al1, Al2 ],
    "AlarmMode": [ AlMode1, AlMode2 ],
    "BinDesc": [ "BinDescOn", "BinDescOff" ]
  },
    ...
    ...
  ]
}
```

Description of parameters inside JSON message:

Parameter	Type	Range	Description	
JsonType	INT		Type of the JSON message. For PA86xx sensors is set to 5.	
JsonVersion	INT		Version of JSON message. Currently set to 1.	
OrderId	INT	0 – 32bit unsigned	Message sequence number since device restart. First message is set to 0.	
MsgType	INT	0 – 2, 4 – 5	Message type:	
			0	first message after restart
			1	synchronous message
			2	asynchronous message
			4	testing message
			5	testing message initiated from the web
MsgCache	INT	0 – 7, 9 – 10	Reason code related to JSON non-volatile/cache memory:	
			0	direct message without using memory
			1	sent from memory (NO_NET)
			2	sent from memory (DNS_ERR)
			3	sent from memory (SOCK_ERR)
			4	sent from memory (SSL_ERR)
			5	sent from memory (BIND_ERR)
			6	sent from memory (CONNECTION_ERR)

				7	sent from memory (TLS_ERR)
				9	sent from memory (TRANSFER_ERR)
				10	sent from memory (WRONG_HTTP_CODE)
Sn		STR	8B length	Serial number of the device (e.g. 25686614)	
Desc		STR	64B length	Device name in UTF-8	
Kind		INT	128 – 131	Identification of device type:	
				128	PA8652 T, T+RH, BIN
				129	PA8611 T, T+RH
				130	PA8641 T, T+RH
				131	PA8610 T
AState	**AState** status register. Description of the **AState** register is in the table below.				
	Reg	INT	0 – 65535	Value of the **AState** register at the moment the request was created.	
	Mask	INT	0 – 65535	Mask of active bits in the **AState** register (only bit 12 used)	
NConf		INT	0 – 255	Configuration number	
ConfID		STR	16B length	Unique configuration ID (X-YYYYYYYY-ZZ-RR)	
Interval		INT	0 – 65535	Sending interval in seconds	
Time	Date and time				
	Now	STR	RFC3339	Time when the message was sent to the server	
	Sample	STR	RFC3339	Time when the values in the message were measured (i.e., the time may be earlier than **Now** when sending a message from memory).	
	IsValid	INT	0, 1	Indication whether the time is valid (1 = valid time).	
LocalIP		STR	64B length	IPv4 address of the device on the local network	
Channels	Measured values for the channel. If a channel is not available, it is not included in the message.				
	Nr	INT	1 – 8	Channel number	
	En	INT	0, 1	Whether the channel is enabled for measurement (1 = enabled).	
	Quant	STR	32B length	Channel name in UTF-8.	
	Val	STR	32B length	Measured value – transmitted as a floating-point number in hexadecimal format (FF8100NN = error code NN).	
	ValStr	STR	32B length	Measured value in string format (e.g., 12.8, n/a, Error X).	
	Unit	STR	16B length	Channel unit in UTF-8	
	Dec	INT	0 – 10	Number of decimal places	
	Type	Channel type information.			
		Static	INT	0 – 255	Static channel identifier
		Dynamic	INT	0 – 255	Channel identifier from channel detection
	Alarm	Channel alarm status (1 = alarm)			
		Al1	INT	0, 1	Channel alarm 1
		Al2	INT	0, 1	Channel alarm 2
	AlarmMode	Alarm mode.			
		AlMode1	INT	0 – 2	Alarm 1 mode (0 – alarm off, 1 – below limit, 2 – above limit).
		AlMode2	INT	0 – 2	Alarm 2 mode (0 – alarm off, 1 – below limit, 2 – above limit).

	BinDesc[1]	Binary input state description.			
		BinDesc On[1]	STR	32B length	On-state description (closed, voltage, flooded).
		BinDesc Off[1]	STR	32B length	Off-state description (open, low voltage, dry).

Notes:

1) The parameter is not available on binary channels in PA8652.

JSON field **AState** – **Reg** provides additional information for the message. Description of individual bits:

Bit	Description
bit0 – bit5	Unused
bit6	Internal hardware error (1 = Internal hardware error - RTC, EEPROM)
bit7	Device is connected to the LAN, meaning it has an IPv4 or IPv6 address (=1).
bit8 – bit10	Unused
bit11	RTC time may not be valid — low voltage detected on RTC (=1).
bit12	Measurement error on one of the channels (=1).
bit13	Configuration is invalid — configuration error (=1).
bit14 – bit15	Unused

JSON and XML via http server

Currently measured values can be obtained using HTTP GET requests sent to the HTTP server running in the sensor. Requests for the files *values.json*, *values-ex.json*, and *values.xml* can be sent to the server on port 80. This function is independent of the HTTP(S) server running on port 81 or 443 (if HTTPS is enabled), which is intended for user access. To use this function, it must be enabled in the device settings (Protocols / HTTP Server / JSON and XML). If the function is disabled, the server returns HTTP error code 403. Examples of reading JSON and XML files in Python are available in the SDK (About / SDK). Access to the files *values.json*, *values-ex.json*, and *values.xml* is independent of the device's security subsystem. The files are available on port 80 without any restrictions. Responses to HTTP GET requests for *values.json*, *values-ex.json*, and *values.xml* on port 80 are provided by an HTTP/1.0 server with support for a single TCP connection. The response time depends on the load of the HTTP server. The average response time is 10 ms. In case of communication issues or server overload, the response time may be longer.

XML structure

The XML file format can be validated against an XSD schema that is available in the SDK (About / SDK). Example XML files are also available in the same location. Description of tags at <root> key:

Parameter	Type	Range	Description
<devname>	STR	64B length	Device name
<devsn>	STR	8B length	Serial number of the device (e.g. 25686614)
<time>	STR	RFC3339	Current device time
<timeunix>	INT	32bit unsigned	Current device time as a Unix timestamp (seconds since 01/01/1970)
<synch>	INT	0, 1	Indicates whether the device time is valid (=1)
<acc>	INT	0, 1	The device does not support the acoustic function.
<ch1> … **<ch8>**			Element containing information about each channel with current measured values.

Description of tags for channels:

Parameter	Type	Range	Description
<name>	STR	32B length	Channel name (in English)
<unit>	STR	16B length	Channel unit
<value>	STR	32B length	Measured value in string format (e.g. 12.8, n/a, ErrorX)
<alarm1>	INT	0, 1	Alarm 1 state (1 = alarm)
<alarm2>	INT	0, 1	Alarm 2 state (1 = alarm)

JSON structure

The structure of the JSON file *values.json* is as follows:

```
{
  "devname": ...,
  "devsn": ...,
  "time": ...,
  "timeunix": ...,
  "synch": ...,
  "acc": ...,
  "ch": [
    {
      "name": ...,
      "unit": ...,
      "type": ...,
      "value": ...,
      "alarm1": ...,
      "alarm2": ...
    },
    ...
    ...
  ]
}
```

The structure of the JSON file *values-ex.json* is as follows:

```
{
  "devname": ...,
  "devsn": ...,
  "time": ...,
  "timeunix": ...,
  "synch": ...,
  "acc": ...,
```

```
  "ch": [
    {
      "name": ...,
      "namelang": ...,
      "unit": ...,
      "type": ...,
      "value": ...,
      "valuelang": ...,
      "alarm1": ...,
      "alarm2": ...,
      "timevalid": ...,
      "min": {
        "val": ...,
        "time": ...
      },
      "max": {
        "val": ...,
        "time": ...
      }
    },
    ...
    ...
  ]
}
```

where:

Parameter			Type	Range	Description
devname			STR	64B length	Device name
devsn			STR	8B length	Serial number of the device (e.g. 25686614)
time			STR	RFC3339	Current device time
timeunix			INT	32bit unsigned	Current device time as a Unix timestamp (seconds since 01/01/1970)
synch			INT	0, 1	Indicates whether the device time is valid (=1)
acc			INT	0, 1	This feature is not available on the device
ch	**name**		STR	32B length	Channel name (in English)
	namelang		STR	32B length	Channel name from device settings
	unit		STR	16B length	Channel unit
	type		INT	32bit unsigned	Channel type – a more detailed description can be found in the SDK.
	value		STR	32B length	Measured value in string format (e.g. 12.8, n/a, Error X).
	valuelang		STR	32B length	Measured value in string format in the selected language (e.g. 12.8, n/a, Error X).
	alarm1		INT	0, 1	Alarm 1 state (1 = alarm)
	alarm2		INT	0, 1	Alarm 2 state (1 = alarm)
	timevalid[1)]		STR	RFC3339	Timestamp from which the min/max values in memory are valid, available via the *values-ex.json* file.
	min	**val**[1)]	STR	32B length	Minimum value from memory (e.g., -2.4, n/a, Error X).
		time[1)]	STR	RFC3339	Time when the minimum value was measured.
	max	**val**[1)]	STR	32B length	Maximum value from memory (e.g., -2.4, n/a, Error X).
		time[1)]	STR	RFC3339	Time when the maximum value was measured.

Notes:

1) The parameter is not available on binary channels in PA8652.

SNMP protocol

Measured values, alarm states, and device status can be read using the SNMP protocol. All common versions are supported - SNMPv1, SNMPv2c, and SNMPv3. By default, a mixed mode is used, in which SNMPv1 and SNMPv2c can be used simultaneously. The SNMP protocol uses UDP port 161. The default community string is set to “public”. When switching to SNMPv3, SNMPv1 and SNMPv2c are disabled. Writing via the SNMP protocol is not supported. MIB tables are available in the SDK (About / SDK).

For SNMPv3, the following modes are supported: NoAuthNoPriv (no authentication and no encryption), AuthNoPriv (authentication without encryption), and AuthPriv (authentication with encryption). The supported authentication algorithms are MD5, SHA, and SHA256, and the supported encryption algorithms are DES, AES128, and AES256. All combinations of these algorithms are supported.

It is recommended to use the AuthPriv mode together with the SHA and AES128 algorithms. Authentication and encryption passwords should not be the same. Passwords should be at least 12 characters long and should not contain repeating characters or repeating groups of characters.

List of SNMP OID keys:

OID	Type	Description
Device identification		
.1.3.6.1.4.1.22626.1.9.1.1.0	STRING	Device name
.1.3.6.1.4.1.22626.1.9.1.2.0	STRING	Device serial number
.1.3.6.1.4.1.22626.1.9.1.3.0	INTEGER	Device type
.1.3.6.1.4.1.22626.1.9.1.4.0	STRING	Device model as string
Measured values (ch = 1 to 8)		
.1.3.6.1.4.1.22626.1.9.2.1.1.1.ch	INTEGER	Channel number (1 to 8)
.1.3.6.1.4.1.22626.1.9.2.1.1.2.ch	STRING	Channel name
.1.3.6.1.4.1.22626.1.9.2.1.1.3.ch	STRING	Measured value
.1.3.6.1.4.1.22626.1.9.2.1.1.4.ch	INT*X	Measured value at format INT*X
.1.3.6.1.4.1.22626.1.9.2.1.1.5.ch	INTEGER	Number of decimal points for value INT*X
.1.3.6.1.4.1.22626.1.9.2.1.1.6.ch	STRING	Channel unit
.1.3.6.1.4.1.22626.1.9.2.1.1.7.ch	INTEGER	State of alarm 1 at channel
.1.3.6.1.4.1.22626.1.9.2.1.1.8.ch	INTEGER	State of alarm 2 at channel
.1.3.6.1.4.1.22626.1.9.2.1.1.9.ch	STRING	Minimal value for channel
.1.3.6.1.4.1.22626.1.9.2.1.1.10.ch	STRING	Maximum value for channel
Device state		
.1.3.6.1.4.1.22626.1.9.3.4.0	STRING	Time according RFC3339
.1.3.6.1.4.1.22626.1.9.3.5.0	STRING	Time at Unix timestamp (sec. from 1.1.1970)
.1.3.6.1.4.1.22626.1.9.3.6.0	INTEGER	Time is valid
.1.3.6.1.4.1.22626.1.9.3.7.0	INTEGER	Device configuration error
.1.3.6.1.4.1.22626.1.9.3.8.0	INTEGER	Measurement error
.1.3.6.1.4.1.22626.1.9.3.9.0	INTEGER	Real-time clock battery error

List of supported OID keys for the MIB-II (RFC1213) table:

OID	Type	Description
.1.3.6.1.2.1.1.1.0	STRING	sysDescr (firmware version and hardware revision)
.1.3.6.1.2.1.1.2.0	OBJ. ID	sysObjectID (.1.3.6.1.4.1.22626)
.1.3.6.1.2.1.1.3.0	TICKS	sysUpTime (time since device startup)
.1.3.6.1.2.1.1.4.0	STRING	sysContact (set to"cometsystem.com")
.1.3.6.1.2.1.1.5.0	STRING	sysName (device name from settings)
.1.3.6.1.2.1.1.6.0	STRING	sysLocation (system location from device settings)
.1.3.6.1.2.1.1.7.0	INTEGER	sysServices (72=application services)

Syslog protocol

Web sensors support sending Syslog messages to a configured server. The message format complies with the RFC 5424 standard. The default UDP port is 514. Syslog messages are divided into two groups: system messages and alarm messages. Each group can be enabled independently. If an IPv6 Syslog server is used, initial Syslog messages related to IPv4 events (for example, IPv4 address assignment) may be lost.

List of system messages:

Message class	Facility	Severity	Message
Email	2	3	Email send error ERR_MAIL_CODE
	2	5	Test email sent successfully
Web	4	5	User logged in successfully
	4	4	User login failed
	4	5	User logged out successfully
System messages	0	5	WebSensor (fw: 11-x-x-x.xxxx) warm boot
	0	5	WebSensor (fw: 11-x-x-x.xxxx) cold boot
	0	5	Reboot requested
	0	5	Config re-init requested
	0	5	New probes detected
	0	5	All probes cleared
	0	5	Network re-init requested
Network messages	16	5	Ethernet link is up
	16	5	Ethernet link is down
	16	6	Static IPv4 address assigned
	16	6	IPv4 address assigned via DHCP
	16	6	IPv4 address assigned via APIPA
	16	6	Static IPv6 address assigned
	16	6	IPv6 assigned via SLAAC with backup DNS
	16	6	IPv6 assigned via SLAAC with DNS from DHCPv6
	16	6	IPv6 assigned via DHCPv6
	16	6	IPv6 assigned via DHCPv6 with backup DNS

List of alarm messages:

Message class	Facility	Severity	Message
Alarm messages from the channels	17	4	Alarm X on channel Y activated
	17	5	Alarm X on channel Y deactivated
System alarm messages	17	4	System alarm activated - measurement error
	17	5	System alarm deactivated - measurement error
	17	4	System alarm activated - configuration error
	17	4	System alarm activated - RTC battery error

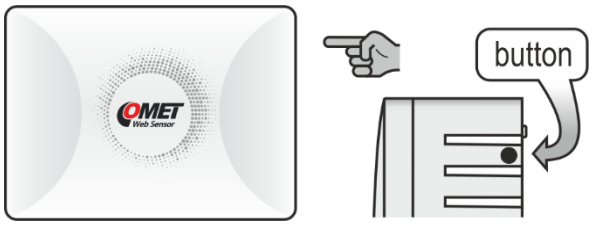
Troubleshooting

Factory defaults

Using the factory reset procedure restores the device configuration to the state of a newly purchased device. The current device settings are erased, including passwords and network parameters. User-uploaded certificates are also deleted during the factory reset. Detected probes and calibration constants are not affected by the factory reset procedure. If you need to restore the factory calibration constants, contact technical support.

Factory defaults procedure:

1. Disconnect the device from power (unplug the power adapter or the RJ45 cable if PoE is being used)
2. Press and hold the button on the device.



3. Reconnect power to the device.
4. Wait 5 seconds, then release the button.
5. The factory reset procedure is complete.

The factory reset procedure can also be performed via the web interface using the Service Options / Factory defaults menu item. In this case, the IPv4 and IPv6 network parameters will remain unchanged.

Forgotten administrator password

When the administrator password is forgotten and there is no access to the device, a *factory reset procedure* should be performed. The procedure is described in the chapter above.

How to determine device IP address

By default, the device uses DHCP for IPv4 addressing. The IPv4 address can also be configured manually as a static address. The device's IPv4 address can be determined in the following ways:

- The IP address can be determined by searching for the device on the network using the COMET Vision or TSensor software. Using COMET Vision, the device's IPv6 address can also be identified.
- The local IP address can be displayed in the COMET Cloud or COMET Database system. However, the device must already be connected to the data acquisition system.

- The web interface of the network router or firewall can be used if the device uses DHCP. The availability of this option depends on the network infrastructure used.

How to use newly connected probe

If Error 63, Error 69, Error 75, Error 80, or the message “n/a” is displayed after connecting a new probe (DST/DST+ or DSRH/DSRH+), it is necessary to perform a new probe detection. Probes are also detected after restarting the device, provided that no other probe was previously detected on the input. Manual probe detection can be performed in the Service Options / Detect Probes menu.

Error codes at channels

This chapter contains a list of error codes that may be shown on the channel(s). Please follow the recommendations below before contacting technical support. Error codes reported via Modbus TCP registers are represented as numbers lower than -32000 (e.g. -32005 = Error 5).

Error code	Description
Error 1	Measured value from the DS sensor is below the lower limit. Verify the measurement ranges of the connected probes.
Error 2	Measured value from the DS sensor is above the upper limit. Verify the measurement ranges of the connected probes.
Error 63 Error 69 Error 75 Error 80 or n/a	The measured value from the probe (DST/DST+ or DSRH/DSRH+) is not available. The probe is likely not connected. Connect the probe and perform probe detection.
Error 50	The device configuration for measurement channels is corrupted. The corrupted configuration can be repaired by restoring factory settings or by using COMET Vision software.
Error 52	The measured value cannot be displayed due to a value overflow during calculations.
Error 53 or n/a	The value is not available. This error is displayed for channels disabled in the configuration or when the value has not been measured yet.
Error 55	Value overflow occurred during conversion to a fixed number of decimal places. This error condition applies to Modbus TCP and SNMP protocols.
Error 60 Error 66	A short circuit has been detected on the input. Check whether the connected probe has damaged insulation or a damaged sensing element. Verify that a Pt1000 probe is

Error 74	not connected instead of a DST or DSRH probe. PA86xx device inputs do not support Pt1000 temperature probes.
Error 61 Error 67	CRC (checksum) error during communication with the memory in the probe. Verify that a compatible probe is connected, that the probe cable is not damaged, and that there are no sources of electromagnetic interference near the probe cable. The maximum probe cable length is 30 m. The SP010 extension cable may only be used with the DSRH/C probe.
Error 62 Error 68	The expected probe was not detected on the input. Verify whether the probe has been replaced. If necessary, perform probe detection.
Error 64	Other error during measurement from a DST probe. Contact technical support.
Error 65	Error during measurement from a DST probe. Follow the instructions provided for Error 61.
Error 70	Other error during measurement from a DSRH/DSRH+ probe. Contact technical support.
Error 71	Unsupported probe type connected. Verify that a compatible probe is connected. Update the device firmware.
Error 72	DSRH/DSRH+ probe power supply error. Contact technical support.
Error 73	The measured value from the DSRH/DSRH+ probe A/D converter is outside the expected range. Contact technical support.
Error 76	The measured value from the DST+ probe is not available, or a CRC error occurred during communication with the probe. Verify that the probe is properly connected, that the probe cable is not damaged, and that there are no sources of electromagnetic interference near the probe cable. The maximum probe cable length is 30 m. If necessary, perform probe detection.
Error 77	Communication error with the DST+ probe. Follow the instructions provided for Error 76.
Error 78	Other error during measurement from a DST+ probe. Contact technical support.
Error 79	Unknown probe type connected. Verify that a compatible probe is connected. Update the device firmware.

Wrong device time

Device time is maintained by an internal RTC (real-time clock) circuit with a coin-cell backup battery. The battery lifetime is designed to match the device lifetime, and it is not replaceable by the end user.

If the incorrect time symbol appears in the web interface, the current device time may not be correct. Set the correct time in the device configuration and save the settings. Then disconnect the device from the power supply and wait 5 minutes to verify the proper function of the backup battery. If the symbol is still displayed after the device is powered on again, contact technical support.

Device is restarting continuously

If the device is continuously restarting, this usually indicates a power supply issue.

If the device is powered by an adapter, replace it. The specifications of the power adapter can be found in the *Power supply* section. If the issue cannot be resolved by replacing the power adapter, contact technical support.

If the device is powered via a PoE switch compatible with the IEEE 802.3af standard, set the PoE compatibility mode according to *Advanced networks* chapter. If the issue cannot be resolved even in “very high load” mode, contact technical support.

Measurement accuracy issue

Measurement accuracy issues for temperature and relative humidity are commonly caused by incorrect probe placement or improper measurement methodology. Please follow the recommendations described in the chapter *Operation in application areas*. In case an error is shown on a measurement channel, please refer to the recommendations in *Error codes at channels*.

Another group of issues involves random spikes in measured values. A common cause of such issues is a source of electromagnetic interference near the cable or the device itself. Other causes may include damaged cable insulation. Please also ensure that the probe shielding is properly connected.

Uploading a certificate or private key

Certificates, CA certificates, and private keys in DER format are supported. If these files are available in PEM format, they must be converted to DER format before uploading.

Private keys can only be uploaded in PKCS#1 format. Uploading a private key in PKCS#8 format is not supported. An RSA private key in PKCS#8 format must be converted to PKCS#1 format before uploading.

Recommendations for operation and maintenance

Operation in application fields

Before putting the device into operation, it is recommended to consider whether it is suitable for the intended purpose. Device settings should be defined according to the intended use case. If the device is part of a larger measurement system, instructions for its metrological and operational checks should be developed.

Inadvisable or hazardous applications: This device is not intended for applications in which a malfunction could directly endanger human or animal life and health or affect the operation of other equipment performing critical functions. In applications where a device failure or malfunction could cause property damage, it is recommended to equip the system with suitable independent signalling equipment. This independent system will be able to detect such a failure and prevent material damage.

Device positioning: Follow the rules and principles described in this manual. Choose a suitable location for the device where the influence of environmental conditions is minimized. When measurements are performed in refrigerators, metal boxes or climate chambers, it is recommended to place the device outside the space and leave only the sensors and probes inside the measured environment.

Positioning of temperature sensors: These sensors should be placed in locations with sufficient air circulation and at the most critical point according to the application requirements. To prevent heat conduction through sensor cables from affecting the measured values, the sensor must be properly inserted into the measured environment. When monitoring temperature distribution in an air-conditioned storage facility, do not place the sensor in the direct airflow from the air-conditioning unit. In large chamber refrigerators, the temperature distribution may be highly inhomogeneous, and temperature differences may reach up to 10 °C. Similar variations can be found inside deep-freeze boxes (e.g. those used for blood preservation by deep freezing).

Positioning of humidity sensors: The positioning of humidity sensors also depends on the application requirements. Humidity measurements in refrigerators without additional humidity stabilization can be unreliable. When cooling is switched on and off, significant variations in humidity may occur, in the range of tens of percent, even if the mean value remains correct. Moisture condensation on freezer walls is a common phenomenon.

Recommendations for calibration

Metrological verification should be carried out according to the requirements of the application, at intervals defined by the user. The recommended calibration interval is stated in the *technical specification* for each device type. In some applications, legal requirements may require calibration to be performed by an independent accredited laboratory. Calibration requirements are determined by the organization's metrology department.

Recommendations for regular checks

It is recommended to check the measurement chain in which the instrument is integrated on a regular basis. The inspection interval and scope depend on the application and the user's internal regulations. The results of each inspection should be recorded. Any identified problems should be addressed according to their severity. In fixed installations, the following checks are recommended:

- Overall visual inspection of the device, including cover integrity and the condition of connectors.
- Inspection of cabling and probes. Cable connections, cable surface integrity, and proper cable routing should be checked (e.g. whether new high-voltage or high-current cables have been installed in parallel with the device cabling).
- Inspection of all probes and sensing elements. Visual check for water ingress into probes. Verification of the installation location of probes with respect to correct measurement conditions.
- Functionality check of the entire measurement chain (verification of features used by the application):
    a) Check whether the measured values are as expected. Measured values can be observed on the device's web interface.
    b) Check whether the measured values are properly transferred to a data acquisition platform such as COMET Cloud or COMET Database. Data are transmitted according to the selected measurement interval.
    c) Check the historical data in the data acquisition platform for any unexpected data outages or alarm states.
    d) Functionality check of alarm functions. This should be done by changing the measured input so that an alarm is triggered. The alarm state should be indicated on the device's web interface, and an alarm email should be delivered (if this feature is enabled).

IT security advisories

IT security is an important aspect of deploying any device connected to wired or wireless networks. It is important not only from the perspective of the application and measurement device, but also for the overall integrity of the network infrastructure. Any inadequately secured network or IoT device may compromise network security. The following chapter contains a list of recommendations on how to use Web Sensor securely.

Web Sensor security: Web Sensors include advanced security features. There are three types of user accounts, each with predefined rules. These rules are described in the *Security* chapter. Web Sensors are shipped without a default password. During the initial setup, a password must be set for the administrator account. Without configuring the administrator account, the device cannot be set up. The minimum password length is 12 characters. It is strongly recommended to use longer passwords, including numbers and special characters. Never use the same password for multiple devices or accounts.

HTTPS for the web interface is disabled by default. It is recommended to enable HTTPS for the web interface. By default, Web Sensors include a certificate signed by the COMET Root CA. This CA file is available in DER and PEM formats within the SDK package. To improve security, user certificates can be uploaded to the device.

Web Sensors support multiple communication protocols. It is recommended to disable any protocols that are not used. This can be done in the settings.

The device does not use the UPnP feature. A list of ingress ports on the device can be found in *Appendix 1*. It is recommended to connect Web Sensors to a separate VLAN to minimize the attack surface. Please ensure that the VLAN is properly isolated in the firewall settings.

Access from another location: If access to the Web Sensor from outside the local network is required, it is strongly recommended to use a VPN. Do not expose the device directly to the internet via port forwarding on the gateway or NAT. This approach helps prevent potential direct attacks on the device.

Firmware update: It is recommended to use the latest firmware on the device. The firmware file should be obtained only from official sources, such as the manufacturer's website or directly from technical support. Never use firmware from unofficial sources, as it may affect the proper function of the device or compromise its security.

Decommission: In case of device decommissioning, sale, or relocation, be aware that the device may contain confidential information. *Factory defaults procedure* is the recommended way to prevent such data leakage. The factory reset procedure restores the device to its default state and removes user certificates and private keys. Detected probes and system counters are not cleared.

Device backup configuration file: The device configuration can be saved to a file for future restoration. Be aware that the backup file contains confidential data, including passwords for communication protocols such as SNMPv3 and SMTP. It does not contain credentials used to secure access

to the device (i.e., usernames and passwords for web access). Backup files are not encrypted.

IT Security Technical Support: Technical support can be contacted with any questions regarding the security of our products. Information on security vulnerabilities and advisories is available on the COMET website under *Security policy and Security Advisories*. This section also describes the process for reporting newly discovered vulnerabilities and security incidents. The Software Bill of Materials (SBOM) is available upon request.

Firmware update

Device firmware can be updated via the web interface under Service options / Firmware update. Administrator privileges are required to perform a firmware update. Firmware downgrade is not supported. The authenticity and integrity of the firmware are cryptographically verified during the update process.

The latest firmware version can be obtained from the manufacturer's website or from technical support. Before starting the update, please read the update instructions carefully.

Technical support and service

Technical support is provided by the device distributor. Contact details for the distributor are listed on the warranty card included with the product. When submitting a support request, it is recommended to attach a diagnostic file downloaded from the device. The diagnostic file can be downloaded from the Service options / Diagnostics menu. The diagnostic file contains important technical information about the operation of the device. It may contain confidential information, such as the device's IP address. It does not contain passwords.

Warning. Do not attempt to repair the device yourself. Repairs may only be carried out by suitably trained and qualified service personnel. Improper installation, operation, or interference with the device may result in the loss of warranty. The manufacturer reserves the right to refuse free-of-charge warranty repairs for devices damaged in this way.

Technical specifications

Power supply

Power adapter:

PA8610, PA8611, PA8641: 5 V to 24 V DC

PA8652: 15 V to 24 V DC

coaxial connector Ø 5.5 x 2.1 mm, center-positive

Power-over-Ethernet (PoE) power supply:

Power supply according to IEEE 802.3af, PD Class 0 (max. 12.95 W), supply voltage 36–57 V DC. Power is delivered over either pairs 1, 2 and 3, 6 or pairs 4, 5 and 7, 8. Passive PoE is not supported.

Consumption:

Typical 1 W (not including the power consumption of external sensors supplied from the PA8652 +12 V terminals)

Power supply for external sensors (P8652):

Two +12 V (±1 V) terminals, each providing a maximum output current of 150 mA. The output is equipped with PTC protection.

Recommended power supply adapter:

PA810, PA8611, PA8641: A1825 (5 V, 2.1 A)

PA8652: A1941 (24 V, 1A)

General parameters

Measurement interval:

2 sec

Realtime clock:

With internal backup battery, maximum deviation ±13 s/month

Communication interface:

RJ45 connector, 10Base-T/100Base-TX Ethernet with Auto MDI/MDIX support

Recommended communication cable:

CAT6 FTP with maximum length 100 m

Communication protocols

Supported protocols:

TCP, UDP, IPv4, IPv6, ARP, ICMP, DHCP, DNS

HTTP, HTTPS, SMTP, Modbus TCP, SNMP, Syslog

IPv4:

Static IP address, DHCP, APIPA

IPv6:

Static IPv6 address, SLAAC, DHCPv6. DNS via Router Advertisements (RFC 8106) is not supported.

Supported automatic configuration modes: SLAAC only, SLAAC with stateless DHCPv6 (DNS configuration) and stateful DHCPv6 (address and DNS configuration). Mode is determined automatically according to Router Advertisement (RA) flags.

Webserver:

HTTP/1.1 server with HTTPS support (TLS 1.2)

Max. 4 simultaneous HTTP client connections

Max. 3 simultaneous HTTPS client connections

HTTP requests on port 80 can be redirected to TCP port 81 (HTTP) or 443 (HTTPS)

Supports uploading of a certificate and private key for HTTPS

Supported browsers: Mozilla Firefox, Google Chrome, Microsoft Edge.

JSON and XML over HTTP server:

Current readings are available via HTTP GET on port 80 at /values.json, values-ex.json and /values.xml

SMTP – Email:

Supported authentication: AUTH LOGIN

Supported security (TLS 1.2): TLS, STARTTLS

Supports uploading of a CA certificate for server verification

OAuth 1.0 or 2.0 is not supported

Cloud protocol:

HTTP/1.1 or HTTPS POST with JSON data structure

HTTPS with TLS 1.2

Supports uploading a certificate, private key and CA certificate for HTTPS verification. Supports mutual authentication.

Remote configuration supported via COMET Cloud

Non-volatile memory for up to 2600 stored value sets

Modbus TCP protocol:

Up to two clients can be connected to the server simultaneously

SNMP protocol:

Supported versions: SNMPv1, SNMPv2c, SNMPv3

Partial support for MIB-II table (RFC1213) – system group only

SNMPv3 authentication: MD5, SHA, SHA256

SNMPv3 privacy: DES, AES128, AES256

AES-256 key extension: Blumenthal

SNMP traps are not supported

Supported cipher suites for TLS 1.2:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA256

Certificates support:

Supported DER format for certificates, CA cert. and private keys. Only PKCS#1 RSA private keys are supported

Parameters of inputs

PA8610

Measured values:

Compact design – temperature from the sensor stem

Range:

-30 °C to +60 °C

Accuracy:

±0.6 °C

Resolution:

0.1 °C

Response time (at air flow ~1 m/s):

t_{95} < 6 min (temperature step 40 °C)

Operating position:

Sensor stem pointing downwards

Recommended calibration interval:

2 years

PA8611

Measured values:

The device is equipped with one connector for connecting an external temperature (DST, DST+) or temperature-humidity probe (DSRH, DSRH+).

Accuracy, range and response time:

See the manual for the used probe

Resolution:

Temperature: 0.1 °C

Relative humidity: 0.1 %RH

Probe connection:

The probe is connected via a CINCH (RCA) connector.

The maximum cable length for the probe must not exceed 30 m.

Operating position:

Any mounting position

Recommended calibration interval:

1 year for temperature and relative humidity probe

2 years for temperature probe

PA8641

Measured values:

The device is equipped with four connectors for external temperature probes (DST, DST+) or temperature-humidity probes (DSRH, DSRH+).

Accuracy, range and response time:

See the manual for the used probes

Resolution:

Temperature: 0.1 °C

Relative humidity: 0.1 %RH

Probe connection:

The probe is connected via a CINCH (RCA) connector.

The maximum cable length for the probe must not exceed 30 m.

Operating position:

Any mounting position

Recommended calibration interval:

1 year for temperature and relative humidity probes

2 years for temperature probes

PA8652

Measured values:

The device is equipped with two connectors for connecting temperature probes (DST, DST+) or temperature-humidity probes (DSRH, DSRH+). The device is also equipped with three digital inputs for monitoring binary (two-state) signals.

Accuracy, range and response time:

See the manual for the used probe

Resolution:

Temperature: 0.1 °C

Relative humidity: 0.1 %RH

Probe connection:

The probe is connected via a CINCH (RCA) connector.

The maximum cable length for the probe must not exceed 30 m.

Binary inputs:

BIN1 input: Three selectable operating modes are available: flood detector (LD-81), dry-contact input, or voltage input. The LD-81 flood detector is available as an optional accessory. The input is not protected against reverse polarity.

BIN2 and BIN3 inputs: Two selectable operating modes are available: dry-contact input or voltage input. The inputs are protected against reverse polarity.

Dry-contact input:

Voltage at the terminals with the open contact: 3.3 V

Current through the closed contact: < 0.1 mA

Closed-contact resistance: < 5 kΩ

Voltage input:

LOW-level input voltage: < 1.0 V

HIGH-level input voltage: > 2.5 V

Voltage source internal resistance: < 2 kΩ

Input voltage range: 0 to 30 V

Operating position:

Any mounting position

Recommended calibration interval:

1 year for temperature and relative humidity probes

2 years for temperature probes

Operating and storage conditions

Operating temperature:

-30 °C to +60 °C

Operating humidity:

0 %RH to 100 %RH without condensation

Operating environment:

chemically non-aggressive

Storage temperature:

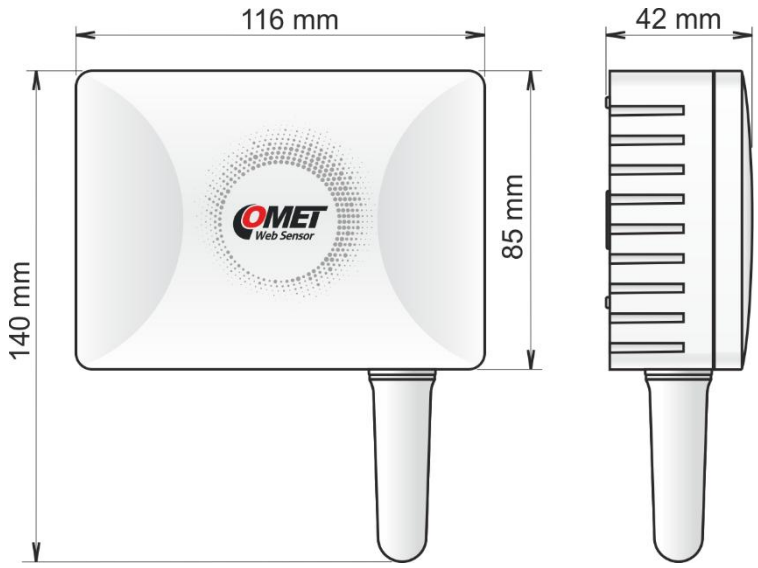
-30 °C to +60 °C

Storage humidity:

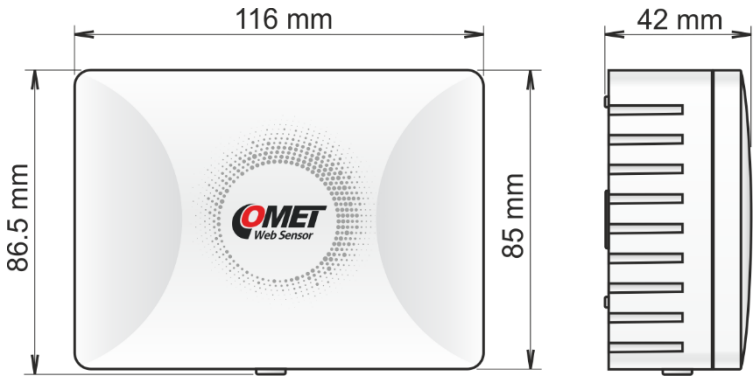
0 %RH to 85 %RH

Dimensions

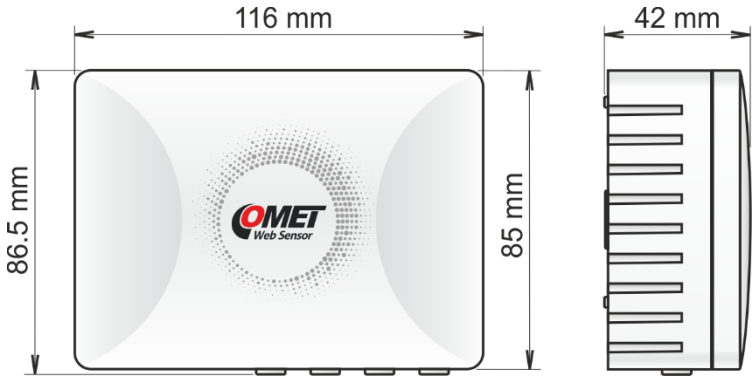
PA8610:



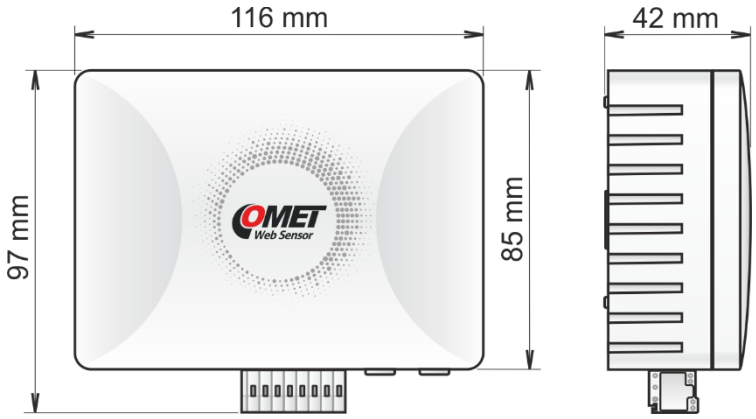
PA8611:



PA8641:



PA8652:



Mechanical properties

Mass:

~ 180 g až 190 g (according to device type)

Case material:

Starex® ASA WR-9100

Ingress protection:

IP30

End of operation

In case of device decommissioning, be aware that the device may contain confidential information (e.g. passwords). For this reason, it is recommended to perform the *Factory defaults procedure* before disposing of the device as electronic waste.

Disconnect the power supply from the device. Dispose of the device in accordance with local regulations. Do not dispose of the device as unsorted municipal waste. The device contains an integrated primary lithium coin cell battery with a capacity of 48 mAh. The battery is not user replaceable.

Declaration of Conformity

EU Declaration of Conformity

Hereby, COMET SYSTEM, s.r.o. declares that the PA86xx sensor family complies with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address:

https://www.cometsystem.com/declaration-conformity/ae-snc-paxxxxtaxxxx.pdf

Appendix

Appendix 1: List of used ports

This table shows the list of ingress ports used by Web Sensors.

Protocol	Port number	Usage
TCP	80	HTTP web server redirection port. It is also used to retrieve current values via values.xml, values.json and values-ex.json.
TCP	81	HTTP webserver
TCP	443	HTTPS web server, available when HTTPS is enabled for the web server.
TCP	502	Modbus TCP port (default port)
TCP	10001	Communication with Vision software (default port)
UDP	30718	COMET discovery protocol
UDP	161	SNMP protocol

Note: ICMP Echo (ping) is enabled at Web Sensors.

Appendix 2: Tests with 3rd party SMTP services

Web Sensors with firmware version 11.0.1.0 have been successfully validated with the following third-party email services. This list is valid as of the date of creation (2026-04-07). Not all services may be available in all countries. As these email services are provided by third parties, we do not guarantee proper functionality with Web Sensors or compatibility of any kind.

Service	SMTP server address	Port	Encryption	Note
Gmail	smtp.gmail.com	465	TLS	Note 1
		587	STARTTLS	
AOL Mail	smtp.aol.com	465	TLS	Note 2
		587	STARTTLS	
Yahoo! Mail	smtp.mail.yahoo.com	465	TLS	Note 3
		587	STARTTLS	
Seznam.cz	smtp.seznam.cz	25	No	
		465	TLS	
		587	STARTTLS	
Centrum.cz	smtp.centrum.cz	465	TLS	
		587	STARTTLS	

Note 1: To support TLS encryption using STARTTLS with the Gmail SMTP server, it is mandatory to enable 2-Step Verification. Once this verification is enabled, an App Password can be generated and used for SMTP authentication.

Note 2: To send emails via the AOL SMTP server, an App Password must be enabled.

Note 3: To send emails via the Yahoo SMTP server, an App Password must be enabled.

Appendix 3: Structure of settings menu

The structure of the Settings menu in Web Sensors is as follows. The structure may differ depending on the device type.

```
General
 ├─Device name
 ├─Language
 ├─Date and time
 │  ├─Synchronize time
 │  └─Manual time setup
 ├─Security
 │  ├─Device security
 │  ├─User Account 1
 │  ├─User Account 2
 │  └─User Account 3
 └─Backup
    ├─Save
    └─Restore

Measurement
 ├─Temperature unit
 └─Probe swap not allowed

Channels
 ├─Channel 1
 │   ...
 └─Channel 8
    ├─Channel name
    ├─Channel enabled
    ├─Alarm 1, 2
    │  ├─Alarm mode
    │  ├─Limit value
    │  ├─Delay
    │  ├─Hysteresis
    │  ├─Alarm on error
    │  └─E-mail recipients
    │     ├─Recipient 1
    │     ├─Recipient 2
    │     ├─Recipient 3
    │     └─Recipient 4
    └─Recalculation
       ├─Recalculation
       ├─Point 1
       └─Point 2
Alarms
 └─System alarms
    ├─Measurement error
    ├─Measurement error delay
    ├─Configuration error
    ├─Real-time clock battery
    └─E-mail recipients
       ├─Recipient 1
       ├─Recipient 2
       ├─Recipient 3
       └─Recipient 4
```

```
Network
├─Network IPv4
│  ├─DHCP enabled
│  ├─IP address
│  ├─Subnet mask
│  ├─Default gateway
│  ├─Primary DNS server
│  └─Secondary DNS server
├─Network IPv6
│  ├─IPv6 mode
│  ├─IPv6 address
│  ├─Subnet prefix length
│  ├─IPv6 default gateway
│  ├─Primary DNSv6 server
│  ├─Secondary DNSv6 server
│  └─Backup DNSv6 server for SLAAC
├─Advanced networks
│  ├─DNS priority
│  ├─Hostname of the DHCP client
│  └─PoE compatibility mode
├─Network details
└─Certificates

Protocols
├─E-mail
│  ├─E-mail enabled
│  ├─SMTP
│  │  ├─SMTP server address
│  │  ├─SMTP port
│  │  ├─SMTP authentication
│  │  ├─User name
│  │  ├─Password
│  │  └─Encryption method
│  ├─Address of e-mail sender
│  ├─Recipients
│  │  ├─Recipient 1
│  │  ├─Recipient 2
│  │  ├─Recipient 3
│  │  └─Recipient 4
│  ├─E-mail type
│  ├─Alarm e-mail repeat interval
│  ├─Keep alive
│  │  ├─Keep alive e-mails interval
│  │  ├─Recipient 1
│  │  ├─Recipient 2
│  │  ├─Recipient 3
│  │  └─Recipient 4
│  └─Testing email
│     ├─Testing email
│     └─Diagnostics
├─Modbus
│  ├─Modbus mode
│  └─Modbus port
├─SNMP
│  ├─SNMP mode
│  ├─Read community
│  ├─User name
│  ├─Authentication
```

```
│   ├─Privacy
│   └─System location
├─Syslog
│   ├─Syslog enabled
│   ├─Syslog on alarm
│   ├─Syslog on system event
│   ├─Syslog server address
│   └─Syslog server port
├─HTTP server
│   ├─JSON and XML
│   └─Webpages uses HTTPs
└─Vision software
    └─Port for Vision software

Cloud
├─Cloud mode - COMET Cloud
│   ├─Asynchronous messages
│   ├─Remote configuration
│   └─Cloud send interval
├─Cloud mode - COMET Database / User server
│   ├─Asynchronous messages
│   ├─Memory disabled
│   ├─User server send interval
│   └─URL for the server
└─Testing message
    ├─Testing message
    └─Diagnostics
```

Appendix 4: Channel mapping for individual models

Channels are mapped for individual device models according to the table.

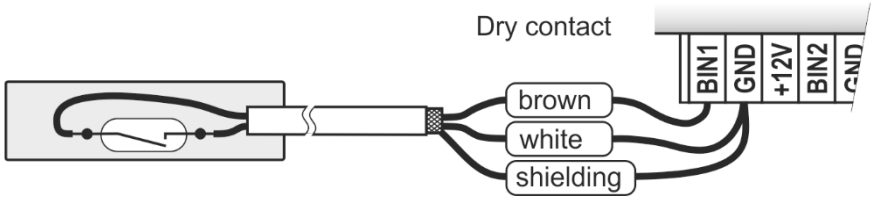
Model	Device channel							
	CH1	CH2	CH3	CH4	CH5	CH6	CH7	CH8
PA8610	T stem	--	--	--	--	--	--	--
PA8611	DS1 val1	DS1 val2	--	--	--	--	--	--
PA8641	DS1 val1	DS1 val2	DS2 val1	DS2 val2	DS3 val1	DS3 val2	DS4 val1	DS4 val2
PA8652	DS1 val1	DS1 val2	DS2 val1	DS2 val2	BIN1	BIN2	BIN3	--

Description:

T stem	Temperature from measurement stem
DS1, DS2, DS3, DS4	Measured values from the DS probe connected to input 1 (or inputs 2–4, respectively). Each probe can provide up to two measured values, which are assigned to specific device channels. Temperature probe DST or DST+: val1 – temperature val2 – unused Temperature and relative humidity probe DSRH or DSRH+: val1 – temperature val2 – relative humidity
BIN1, BIN2, BIN3	Binary inputs for monitoring two-state signals. Connected binary sensors and detectors can be powered from two +12 V terminals, each providing a maximum output current of up to 150 mA. BIN1 – the input supports three selectable operating modes: voltage input, dry-contact input, and a mode for the LD-81 two-wire flood detector BIN2 – the input supports two selectable operating modes: voltage input, dry-contact input BIN3 – the input supports two selectable operating modes: voltage input, dry-contact input

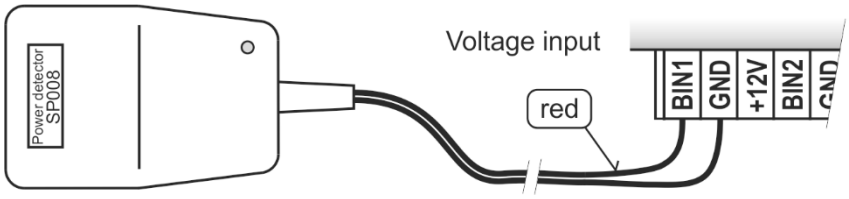
Appendix 5: Connection of binary sensors

SA200A magnetic contact with cable



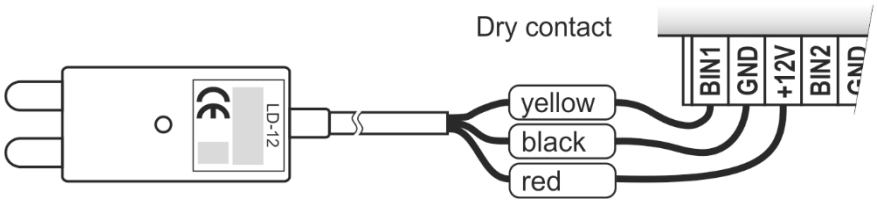
SP008 mains voltage failure detector

The detector is designed to indicate the presence of voltage in an AC mains outlet. Input voltage: 230 V AC / 50 Hz, Plug type: Type C, Response time: approx. 1 s



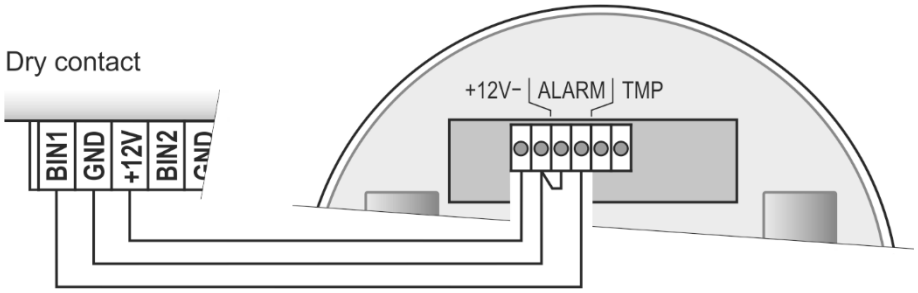
LD-12 flood detector

The detector is designed to detect flooding caused by water. The detector LD-12 uses a three-wire connection. When installing the detector, follow the instructions provided in the attached manual.



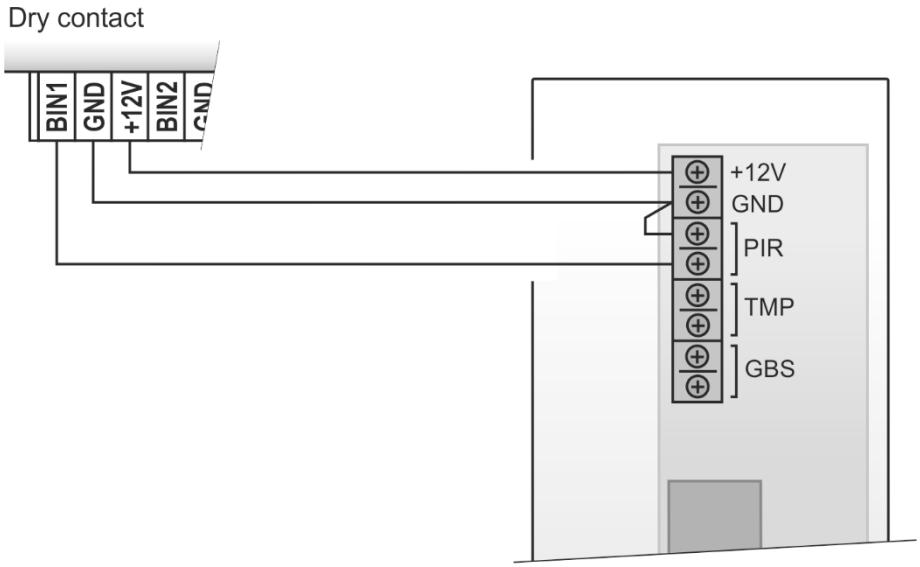
SD280 optical smoke detector

The optical detector is designed to detect fire hazards in residential and commercial buildings. When installing the detector, follow the instructions provided in the attached manual.



JS20 PIR motion detector

The detector is designed for premises protection. When installing the detector, follow the instructions provided in the attached manual.



Revision history

Document version	Date	Note
IE-SNC-PA86xx-01	June 2026	Initial document revision for devices with firmware version 11.0.1.0.
IE-SNC-PA86xx-02	October 2026	Corrections and clarification of default settings.

Note: Page numbers may differ between document versions.