AWP serie

Manual

HITMA B.V.
Ampèrestraat 35-37
NL-1446 TR PURMEREND

T (+31) 0299 630 610
F (+31) 0299 630 611

E info@atal.nl
I www.atal.nl

Table of contents

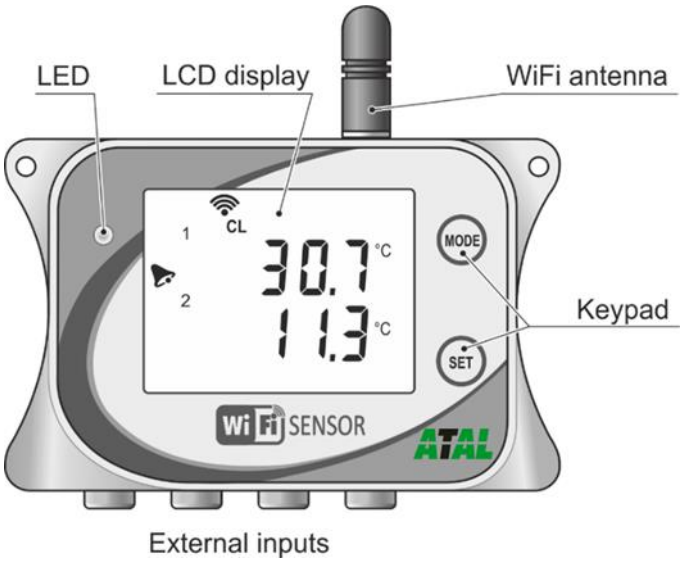
Introduction

Wi-Fi sensors are designed for autonomous measurements, processing, and alarming of the physical quantities. Measurement of temperature, relative humidity, barometric pressure, CO_2 concentration are supported. Inputs and measurement ranges depends on device model and cannot be changed by end-user. Device communication is done via Wi-Fi wireless network. Device needs to be powered from external adapter which is part of shipment.

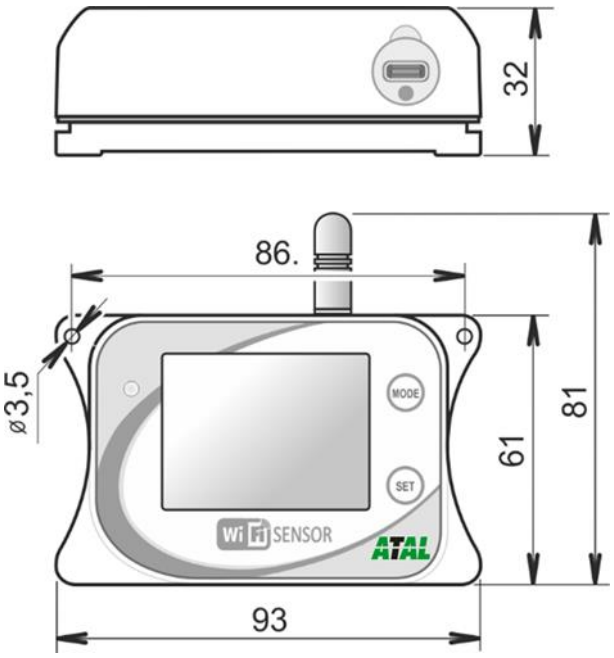
Key features:

- Measurement from external and internal sensors temperature, relative humidity, barometric pressure, CO_2 concentration. From relative humidity values are calculated additional humidity quantities like a dew point.
- Monitoring and alarming of the measured values to the pre-set limits. Two alarm limits are supported for each measured quantity with selectable direction.
- Acoustics and optical LED signalisation of the alarms.
- Measured values are shown on a large LCD display with backlight.
- Holding of minimum and maximum values from device start-up for each measured quantity. Minimum and maximum values can be reset by the end-user manually.
- Communication via 2.4 GHz Wi-Fi network. Device can be used with wireless infrastructure which is already available at place of installation.
- Device is equipped by the USB-C connector which is used for powering of the device. Same connector can be used for device configuration if needed.
- Measured values can be shown on device web pages and can be transferred into data acquisition system ATAL Cloud or ATAL Database.
- 3rd party data acquisition systems are supported via JSON, XML, Modbus TCP and SNMP protocols.
- Device has integrated internal non-volatile memory. Memory is used for recording measured values in case Wi-Fi or internet connection outage.
- Occurrence of alarm states can be reported by the email sent from the device.
- Device configuration via web pages from computer or cell phone. Initial device provisioning is done via access point mode.
- The device delivery includes traceable calibration certificate. Declaration of metrological traceability of etalons is based on requirements of EN ISO/IEC 17025 standard.

Schematic drawing of Wi-Fi sensor:


LED
LCD display
WiFi antenna
CL
1
2
30.7 °C
11.3 °C
MODE
SET
Keypad
Wi Fi SENSOR
ATAL
External inputs

Dimensions:


32
86.
ø3,5
MODE
SET
Wi Fi SENSOR
ATAL
61
81
93

Safety precautions and prohibited handling

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

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

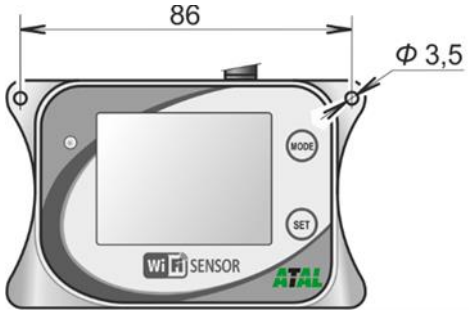
- **Legislative conditions.** The device includes a radio transmitter operating in the non-license Wi-Fi band. Used frequency and the transmit power are specified in the *Technical specification*. This band and transmit power are used in the European Union countries. If you are in another location, please make sure that usage of device is allowed before turning it on.
- **Electromagnetic interference.** Do not use the device in places where the usage of Wi-Fi devices is prohibited. Such as near to sensitive medical devices, on the aircraft or in localities where explosive materials are used.
- **Operating and storage conditions.** Follow the recommended operating and storage condition as stated in the *Technical specification*. Do not expose the device to direct radiation of heat sources and sun. Do not install the device more than 2 m above the floor to avoid the risk of injury in case of device fall from high.
- **Fire and explosion hazard.** It is not allowed to use this device within hazardous areas, especially those endangered by a potential explosion of combustible gases, vapours, or dust.
- **Device cover.** Never operate the device without the cover.
- **Aggressive environment.** Do not expose this device to aggressive environment any kind, chemicals, or mechanical shocks. Use soft tissue for cleaning only. Do not apply solvents or similar aggressive agents.
- **Failures and servicing.** Do not try to repair the device by yourself. Any repairs may be carried out by suitably instructed service personnel only. If the device shows signs of unusual behaviour, power off the device instantly. Contact the distributor from which was device purchased.
- **Ingress protection.** The device has not a protection against the ingress of water and dust. Do not operate it in unsatisfied conditions.
- **Serviceability.** This device operates a wireless communication in the unlicensed radio spectrum of the Wi-Fi network. From this reason the connection cannot be guaranteed under all circumstances. Never rely merely on the wireless equipment only for a critical communication system like a rescue systems or safety systems. Bear in mind that redundancy is essential for systems with high level of the functional safety. See e.g. IEC 61508 for more information.
- **Recommended accessories.** Use accessories recommended by the manufacturer only.

Installation

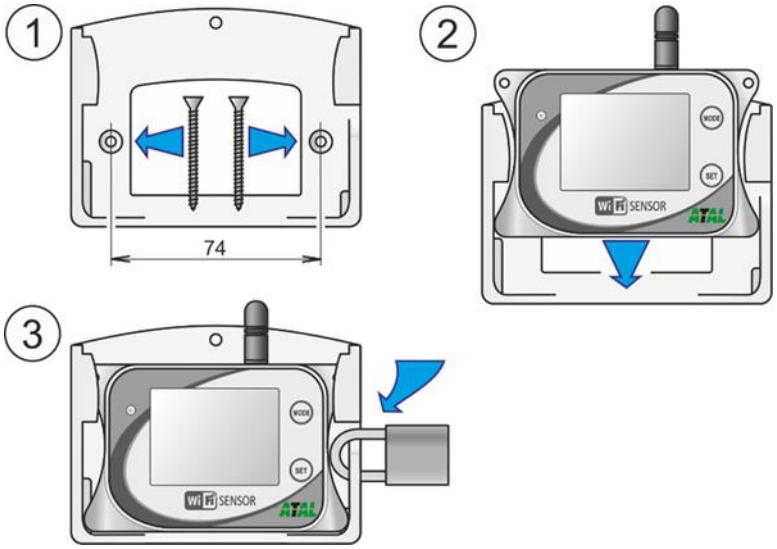
Hardware installation

- **Select proper location for the device** – bear in mind that the environmental conditions should meet requirement according to *Operating conditions*. Do not place device next to sources of electromagnetic interferences. The device has not a protection against the ingress of water and dust. Do not use device at places where such conditions can be expected.
- **Recommended working position** – device should be used at recommended working position. This position is with antenna up.

- **Test Wi-Fi signal strength at device location** – proper signal strength is essential for device function. Signal strength can be examined by another Wi-Fi device like a cell phone places at device location. Another way to determine signal strength is using procedure described at chapter *Wi-Fi connection issues*.
- **Fasten the device** – device can be screwed directly to wall or another solid surface. Do not fasten device to metal object directly. Installation material like a wall dowels and screws are not part of shipment. Use appropriate fasten material to mounting device securely. Avoid dropping of device and potential injury.



- **Device can be mounted onto wall by optional holder ATRU-AC02** – holder is available as optional accessory. ATRU-AC02 package contains holder itself, installation material (wall dowels and screws), lock and keys. For security reason do not install device to higher position than 2 m above floor.



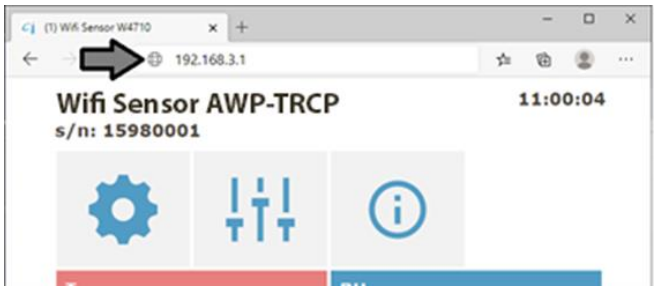
- **Mounting cables and probes** – connect probes to the device. Please follow recommended working positions for probes. Do not place probes together with electric-power distribution cables or devices.
- **Power on device** – connect power supply via USB-C cable (5V DC). Cable and adapter are part of shipment.

Provisioning and first setup

- **Access point mode** – newly purchased device is set into access point mode. Access point mode is signalised by symbol AP on the LCD display. In case this symbol is not shown or there is symbol CL, please switch device mode manually by the buttons according to chapter *Keyboard*.

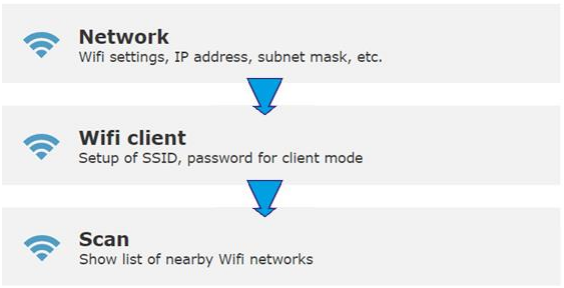
- **Connect by laptop or cell phone to access point** – enable Wi-Fi on laptop or cell phone and connect to the access point with name WiFiSensor_xxxxxxxx. If cell phone is used, it is recommended to switch off mobile data connection. Proper connection is signalised by following symbol at LCD display.

- **Open web browser and insert address of device** – *http://192.168.3.1* or *www.wifisensor.net*

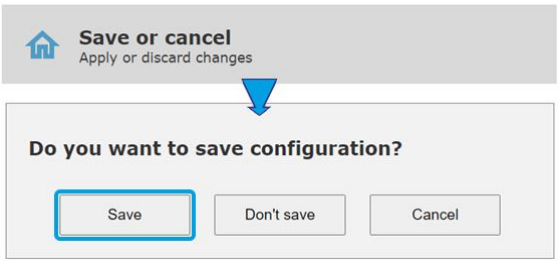


- **Enter device settings** – go to the settings menu to start configuration

- **Insert SSID and password for Wi-Fi network** – to be device connected into Wi-Fi network, it needs to be Wi-Fi network credentials inserted. This can be done at menu Network / Wi-Fi client / Scan.



- **Other settings** – during initial device configuration other settings can be changed. Detail information about device settings is available in chapter *Device setup*.
- **Save settings** – For settings changes to be applied, it needs to be saved using the field Save or cancel.



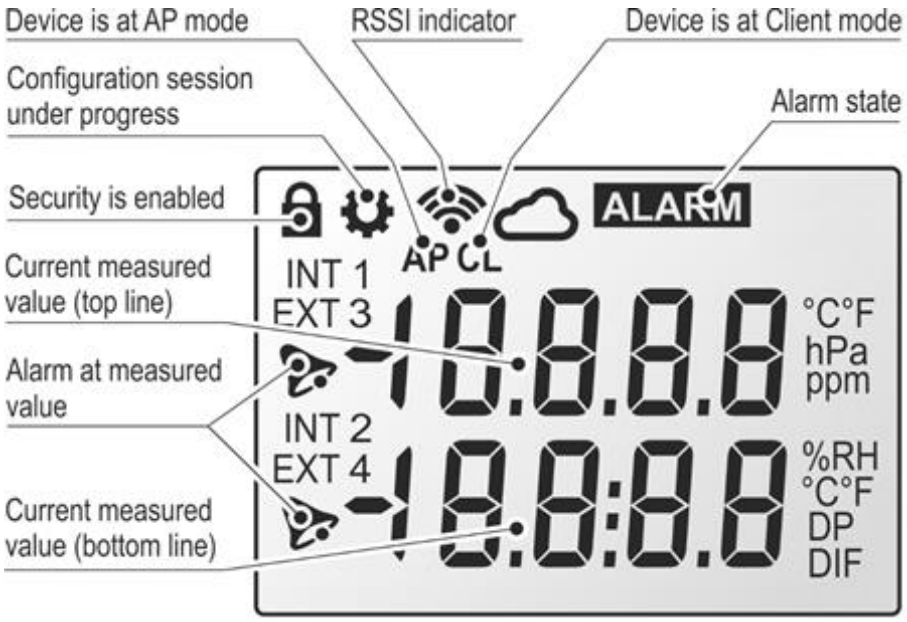
- **Connected to Wi-Fi** – after saving of settings, device will be connected into Wi-Fi network automatically. This will be signalled by symbol CL.

- **Device IP address** – after connection into Wi-Fi network, the device will be assigned new IP address. This IP address can be determined by pressing the MODE button or using procedures described at chapter *How to determine device IP address*.

Features

LCD display

Wi-Fi sensors are equipped with LCD display for showing current measured values and device state information. Showing of measured values at LCD display can be enabled for each value separately. When LCD display is deactivated and buttons are pressed, LCD display is temporarily activated with status information. LCD display backlight is configurable into one of three modes (off, always on or when key is pressed).



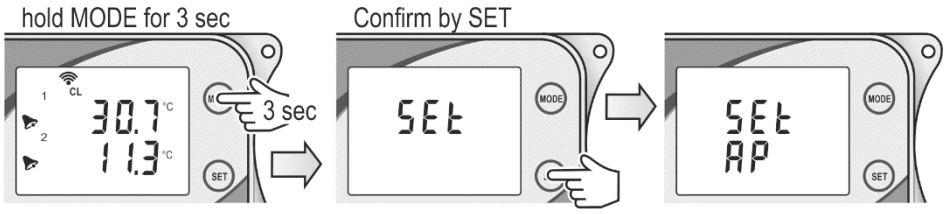
Feature	Description
Current measured value(s)	Current measured value at device channel. Units and value position at LCD display depends on each measured value. Measured value position at display is not configurable by end-user. Screens with measured values are switched with interval 4 sec.
Alarm at measured value 	Alarm state (Alarm 1 or Alarm 2) at measured value is signalised by “bell” icon before measured value.
Alarm state ALARM	Signalisation if there is any alarm on device. Alarm state comes from alarms on channel(s) or from system alarms. *System alarms* are designed for diagnostic of the device failure.
Security enabled 	This symbol is shown when device security is enabled.

Configuration session 	This symbol is shown when configuration session is under progress. Only one configuration session is possible at one moment. That means setup from other places is blocked when configuration session is started.	
Cloud connection 	Sending data via Cloud protocol is under progress currently.	
Acoustic active 	Device acoustic is active now.	
Acoustic mute 	Device acoustic was muted by web (software) or via keyboard.	
Values inside memory 	There are values inside memory for Cloud protocol. That means not all values for Cloud are sent yet.	
RSSI indicator and mode 		Device is at client mode and connection attempt into Wi-Fi network is under progress.
		Device is at client mode and connected into Wi-Fi network. RSSI value is not available yet.
		Connected into Wi-Fi network. Signal strength is poor (RSSI < -69 dBm).
		Connected into Wi-Fi network. Signal strength is sufficient.
		Connected into Wi-Fi network. Signal strength is good (RSSI > -59 dBm).
		Device is at AP mode. No client is connected.
		Device is at AP mode. At least one client is connected.

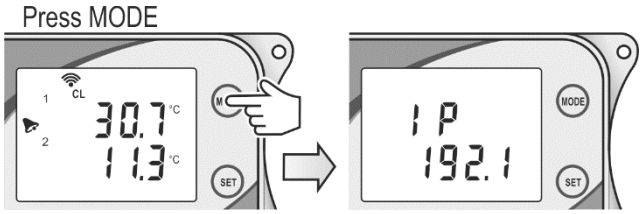
Keyboard

At the device body are two buttons MODE and SET. These buttons can be used for following actions:

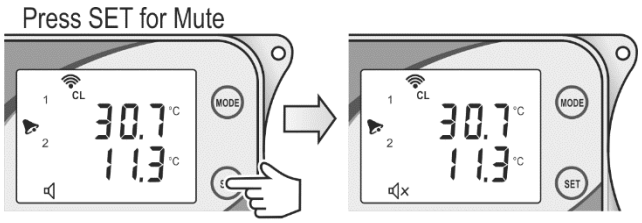
- Manual switching between Client and Access point mode



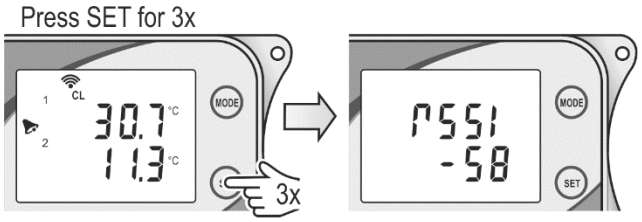
- Showing of device IP address



- Mute of the acoustic



- Showing RSSI value at LCD display



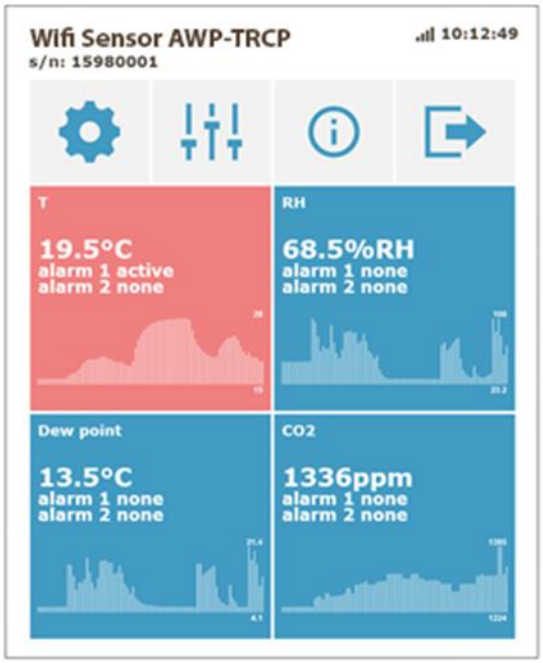
Wi-Fi Modes

Device supports two Wi-Fi modes. AP mode which in intended for initial provisioning into Wi-Fi network and Client mode. Client mode is used when device is connected to infrastructure access point. When Client SSID is blank device is automatically switched into AP mode. Newly purchased device has blank SSID. Device supports up to four Wi-Fi clients (computer, cell phone) when is at AP mode. If it is needed, device can be switched from Client mode into AP mode manually by keyboard. Procedure is described at chapter *Keyboard*.

When device is switched into AP mode by buttons and there is no other communication with Wi-Fi sensor, device is switched back to client mode automatically after 10 minutes.

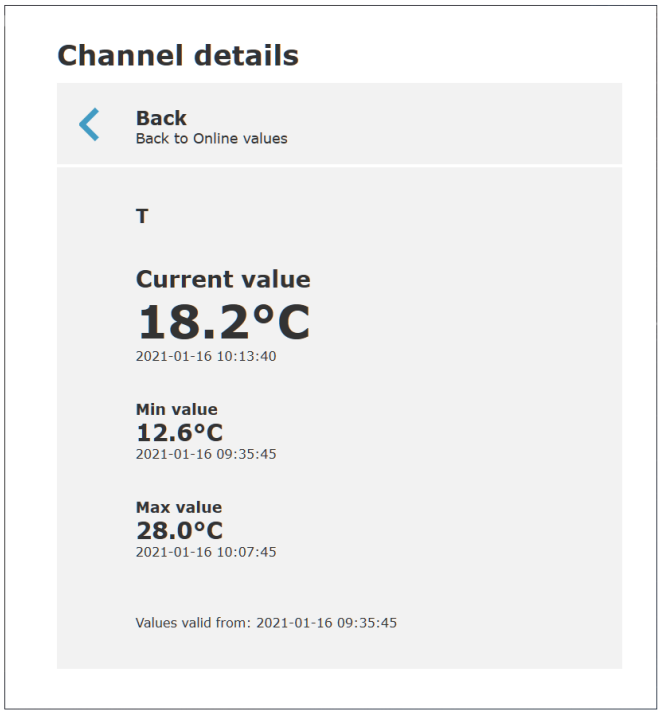
Main page

The Main page allows monitoring of online values for the device channels. After entering device IP address into web browser is Main page shown. Size of tiles is adjusted according to screen resolution automatically.



Tile	Description
	This tile starts Settings of the device.
	Advanced options menu. At this menu can be Mute of acoustic done, testing email and testing cloud message can be sent. There are accessible service options like a detection of Digi probes, firmware update and download of diagnostic file.
	About page shows important information about the device. Via About page is Library page accessible. Library page contains description of communication protocols.
	Logout option. This tile is available when device security is enabled.

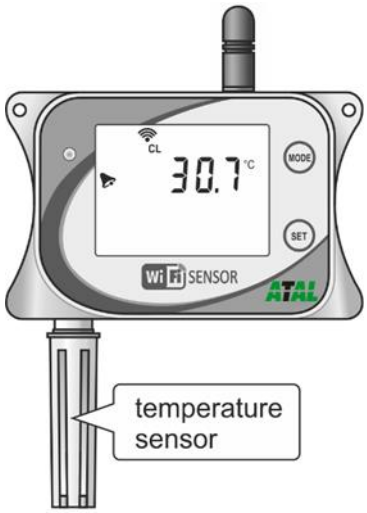
After clicking on the channel with online values, details of channel are shown. At this page are information about minimum and maximum values with timestamps. Minimum and maximum values can be reset by click to Current value tile.



Models of Wi-Fi sensors

This chapter contains list of available models of Wi-Fi sensors. Difference between models are types of inputs and ranges of measured values. Each measured quantity has assigned input channel. End-user cannot change type or range of measured quantities.

AWP-T



Single channel compact thermometer

This model of device measures temperature from probe which is connected to bottom part of the device. Temperature probe is part of shipment and may to be detached from device body. Device should be located into measured environment directly.

AWP-TR

Compact thermometer-hygrometer

This model is designed to measurement of temperature and relative humidity from probe connected to bottom part of the device. Probe is a part of shipment and may to be detached from device body. It can be selected one of the computed humidity values (dew point, absolute humidity, specific humidity, mixing ratio, specific enthalpy, or humidex). Device should be located into measured environment directly.

AWP-T1P

Single channel thermometer for external Pt1000 probe

This model is designed to measurement from one external probe Pt1000. Probe is not a part of shipment and can be ordered separately. Device is suitable for monitoring places where probe is placed only, and device body is located outside the measured environment. Maximum recommended probe length is up to 15 m.

AWP-T4P

Four channels thermometer for external Pt1000 probes

This model is designed to measurement up to four external probes Pt1000. Probes are not a part of shipment and can be ordered separately. Device is suitable for monitoring places where probes are placed only, and device body is located outside the measured environment. Maximum recommended length of each probe is up to 15 m.

AWP-TR1D

Thermometer-hygrometer for one external probe

This model is designed to measurement of temperature and relative humidity from one TRHD-xxxE probe. Probe is not a part of shipment and can be ordered separately. It can be selected one of the computed humidity values (dew point, absolute humidity, specific humidity, mixing ratio, specific enthalpy, or humidex). There are available probes with maximum length up to 15 m. TRHD-xxxE probes provides calibrated values and are exchangeable without needs to change device setup. Device is suitable for monitoring places where probe is placed only, and device body is located outside the measured environment.

AWP-TR2D

Thermometer-hygrometer for two external probes

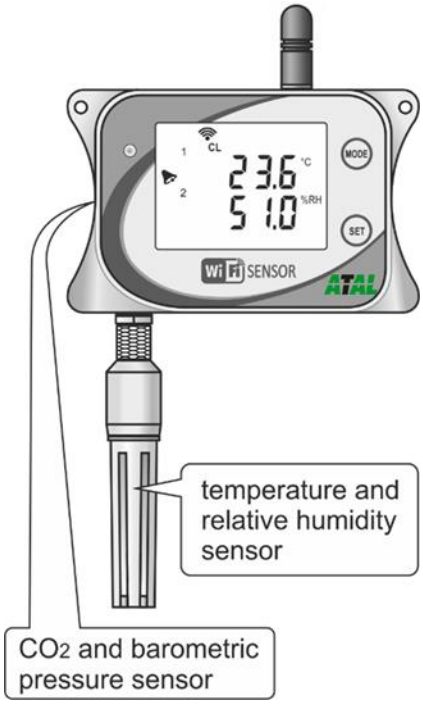
This model is designed to measurement of temperature and relative humidity from two TRHD-xxxE probes. Probes are not a part of shipment and can be ordered separately. It can be selected one of the computed humidity values (dew point, absolute humidity, specific humidity, mixing ratio, specific enthalpy, or humidex). There are available probes with maximum length up to 15 m. TRHD-xxxE probes provides calibrated values and are exchangeable without needs to change device setup. Device is suitable for monitoring places where probes are placed only, and device body is located outside the measured environment.

AWP-TR1D-T3P

Thermometer-hygrometer for one external probe and for three additional external Pt1000 temperature probes

This model is designed to measurement of temperature and relative humidity from one TRHD-xxxE probe and temperature from up to three Pt1000 probes. Probes are not a part of shipment and can be ordered separately. It can be selected one of the computed humidity values (dew point, absolute humidity, specific humidity, mixing ratio, specific enthalpy, or humidex). There are available TRHD-xxxE probes with maximum length up to 15 m. TRHD-xxxE probes provides calibrated values and are exchangeable without needs to change device setup. Maximum recommended length of each Pt1000 probe is up to 15 m. Device is suitable for monitoring places where probe is placed only, and device body is located outside the measured environment.

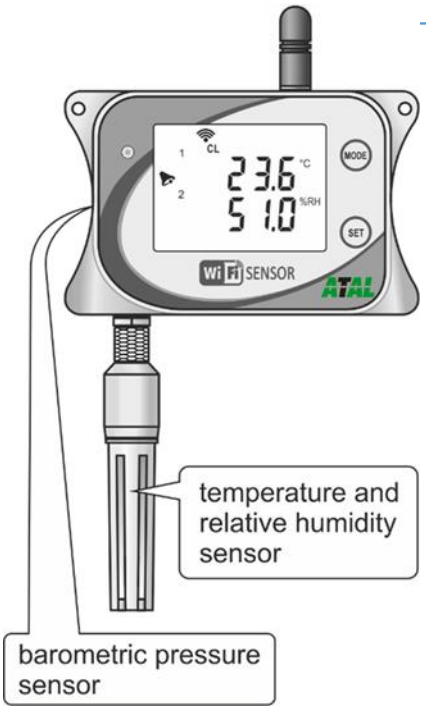
AWP-TRCP



Compact sensor with temperature, relative humidity, barometric pressure and CO_2 concentration measurement

This model is designed to measurement of temperature, relative humidity, barometric pressure, and CO_2 concentration of air. Temperature and relative humidity are measured by probe which is part of shipment and may to be detached from device body. Barometric pressure and CO_2 concentration of air are measured by internal sensors. It can be selected one of the computed humidity values (dew point, absolute humidity, specific humidity, mixing ratio, specific enthalpy, or humidex). Barometric pressure can be measured as absolute or compensated to the sea level. Device should be located into measured environment directly.

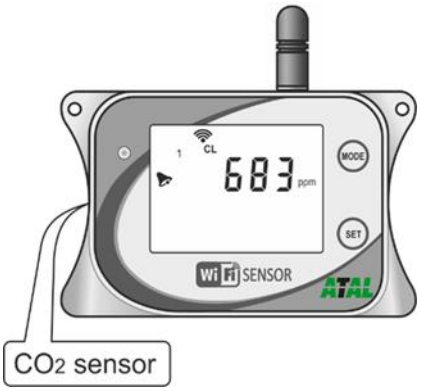
AWP-TRP



Compact sensor with temperature, relative humidity, and barometric pressure measurement

This model is designed to measurement of temperature, relative humidity, and barometric pressure. Temperature and relative humidity are measured by probe which is part of shipment and may to be detached from device body. Barometric pressure is measured by internal sensor. It can be selected one of the computed humidity values (dew point, absolute humidity, specific humidity, mixing ratio, specific enthalpy, or humidex). Barometric pressure can be measured as absolute or compensated to the sea level. Device should be located into measured environment directly.

AWP-C



Compact sensor for measurement of CO_2 concentrarion

This model measure CO_2 concentrarion of the air from internal sensor. Device should be located into measured environment directly.

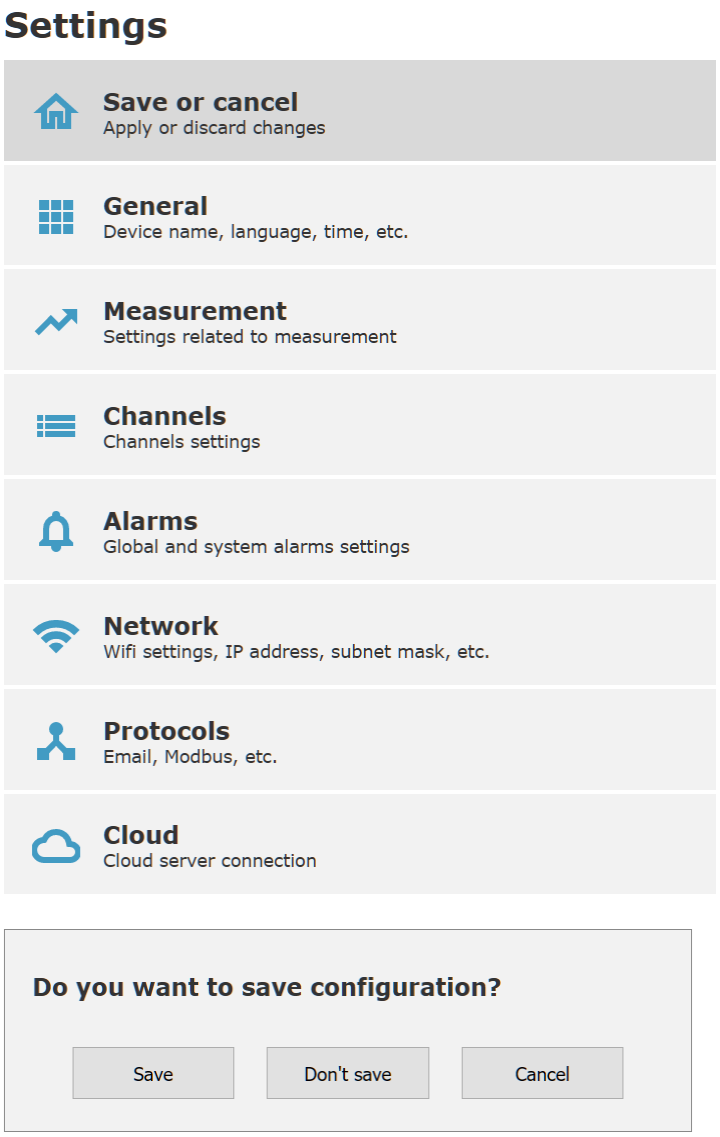
Device setup

Conventions

Configuration session

Device setup uses a feature called configuration session. Once a device setup is started settings can be changed according to needs. All changes of setup are kept inside temporary memory. Settings changes are applied after saving. Settings are saved under menu item Save or cancel. Same field is used to discard changes done during configuration session.

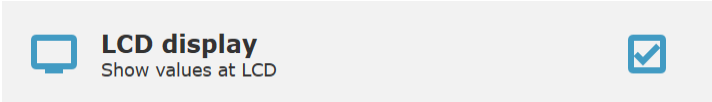
Only one configuration session is possible concurrently. That means setup from other places is blocked when configuration session is started. Access is possible again when configuration session is saved or cancelled. Structure of Settings menu is described at *Appendix 10*.



Globally disabled features

Some device features can be globally enabled or disabled. Good example of such feature is LCD display. It can be globally disabled at General settings. Showing measured values at LCD display can be disabled for each channel separately. When showing measured value on display is required, LCD display needs to be enabled globally and enabled at channel as well. When feature is globally disabled, it is shown by the tile with transparency at channel page.

Feature is globally enabled:

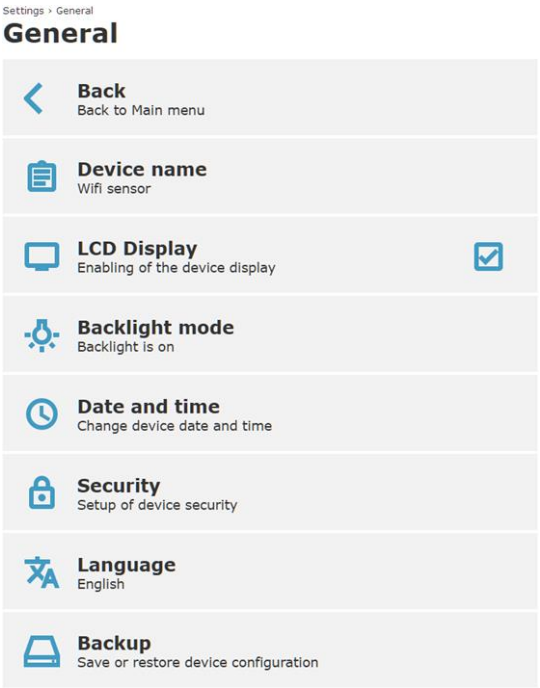


Feature is globally disabled:

General settings

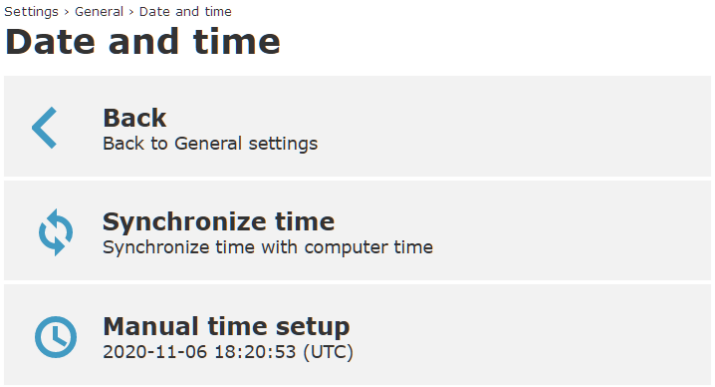
General settings of the Wi-Fi sensor allow to change device name, setup LCD display, set current time, enable security, change language, and backup device settings into file.

LCD display can be disabled if needed. When LCD display is disabled, measured values are not shown on display, but after the button is pressed, the LCD display is activated temporarily. Display backlights is set to one of three modes. Backlight can be permanently off, permanently on, or can be activated after button press. Supported languages are English, Czech, Dutch, Polish, Spanish, and French.



Date and time

Settings of date and time for the device. Wi-Fi sensors contains real time clock circuit which is powered by internal battery. Device maintains current time even is powered off. Current time can be synchronised with time at the computer or cell phone using option the Synchronize time. Time zone (UTC offset) is set automatically after time synchronizing. Change of device time is applied after saving whole settings.



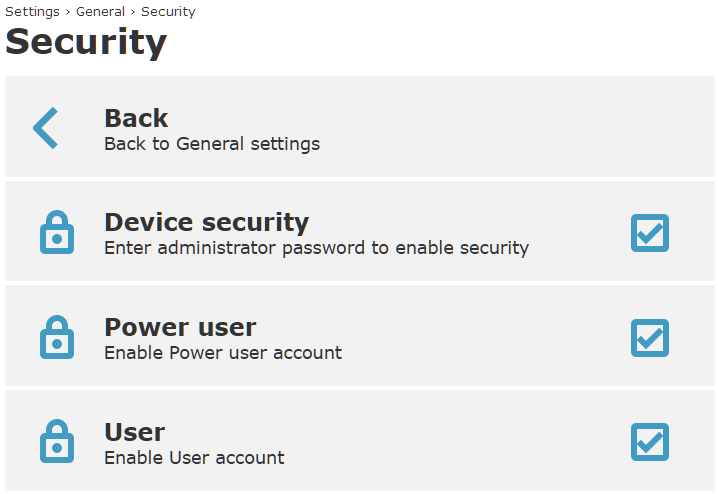
Be aware that improper changing of time zone without proper changing current time can cause wrong data interpretation at ATAL Cloud history.

Security

Wi-Fi sensors have integrated advanced security system. There are three types of user accounts - Administrator, Power user and User. Each user has assigned permissions to actions according to table below. Password for Administrator need to be set in case of security is enabled. Other user accounts are optional and can be disabled if needed. It is strongly recommended to enable device security when device is used at the final deployment.

When security is enabled, web server is switched to https mode automatically. Due to natural behaviour of https and certificates at local networks it may to be needed assign security exception at web browser.

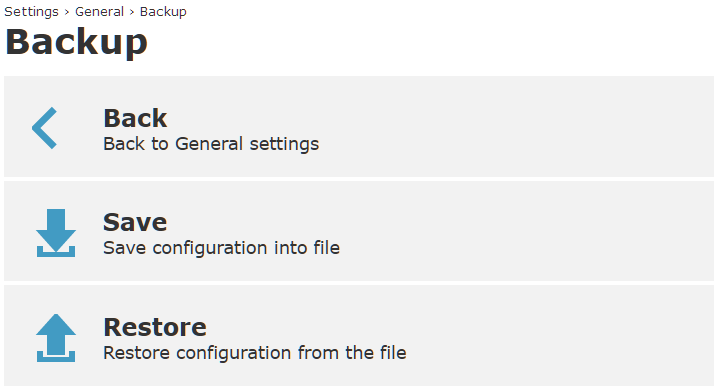
Be aware in case of administrator password is lost, device need to be restored by *Factory defaults procedure*.



Feature	Administrator	Power user	User
Mute	X	X	X
Detect Digi probes	X	X	
Restart from web	X	X	
Testing messages	X	X	
Setup	X	X	
Security setup	X		
Firmware update	X		
Download diagnostic	X		

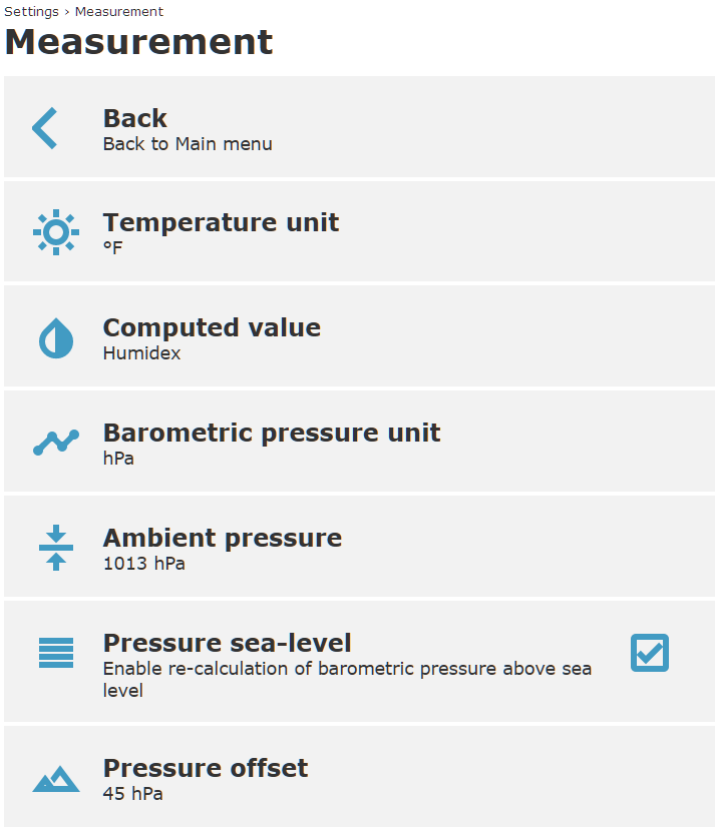
Backup

Device settings can be saved into file and restored from them later. All parameters of device are saved into file excluding security settings. Be aware that network parameters like IP address are saved as well. When settings are restored from another device, it may to cause IP address conflict when static IP address is used. In case of static address is used, network parameters should be changed after restoring from file. Backup file does not contain certificates used for WPA2-EAP security. These files need to be uploaded separately.



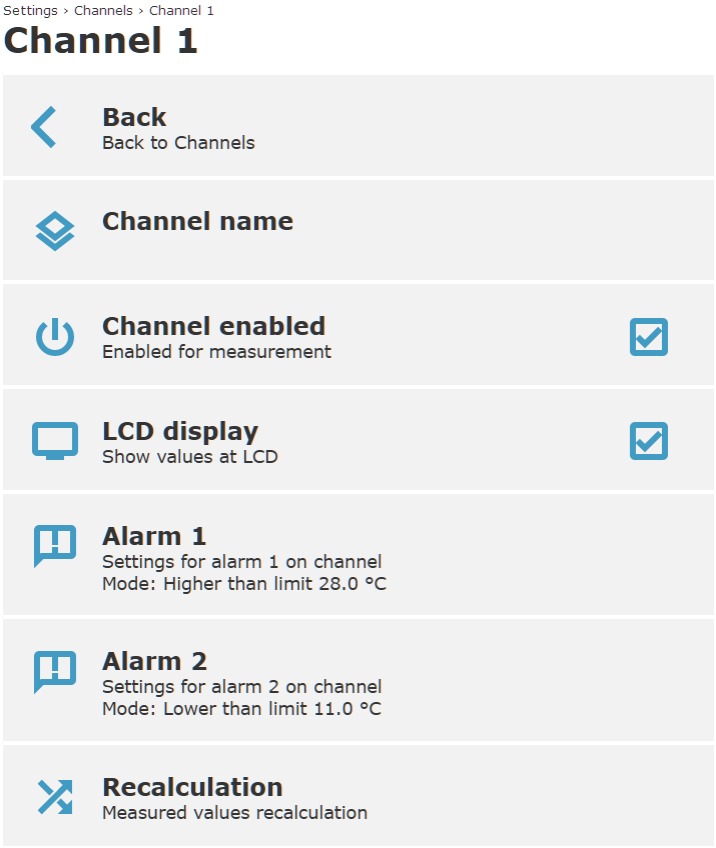
Measurement settings

Settings of global features related to measurement. Available setup options depend on device type. At the devices with temperature measurement can select between °C and °F. Dew point unit is same as temperature unit. Devices with humidity measurement allow to select one of computed values from the list: Dew point, Absolute humidity, Specific humidity, Mixing ratio, Specific enthalpy, or Humidex. Barometric pressure units can be switched between units: hPa, kPa, mBar, mmHg, inHg, inH_2O, PSI, or oz/in^2. Ambient pressure option is available at devices without barometric pressure sensor. Value is used for calculation of Specific humidity, Mixing ratio, and Specific enthalpy. Devices with barometric pressure measurement allow to set the pressure offset for conversion to the equivalent sea level pressure.



Channel settings

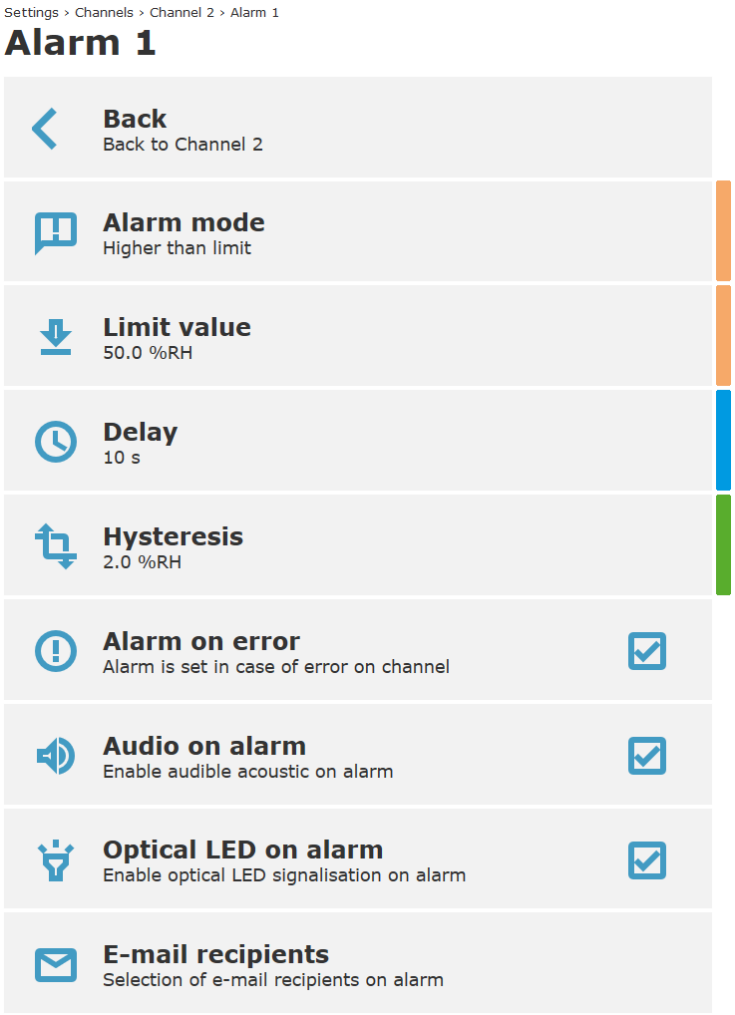
Device is equipped by number of channels according to model type. Channel can be enabled or disabled. When channel is disabled, it is not shown on device main page. Showing measured values from channel at the LCD display can be deactivated separately if needed. Channel name can be changed according needs. In case of channel name is left blank, default channel name according to selected language is used. Be aware that after changing channel name, a new channel is created inside ATAL Cloud or ATAL Database. Each channel can have two independent alarms thresholds which can be configured separately. Measured values can be re-calculated using linear equation if needed.



Settings alarm for a channel

Each channel allows configuration of two separate alarms. Alarm mode selects direction of alarm – Lower than limit, Higher than limit, or Disabled. Limit value is a threshold for activation of alarm. Alarm is activated when measured value exceed selected limit for a quantum of time set by Delay option. Alarm state is cleared when measured value returns under set limit with selected Hysteresis. When alarm is activated, it can be acoustic or optical LED signalisation activated. Alarm on channel can be activated optionally when measurement error on channel occurred.

Wi-Fi sensors have capability to send email in case of alarm on channel is activated. Up to four email recipients can be configured. Addresses of email recipients are configurable at *Email protocol settings*. Each recipient can be enabled or disabled separately at alarm settings.



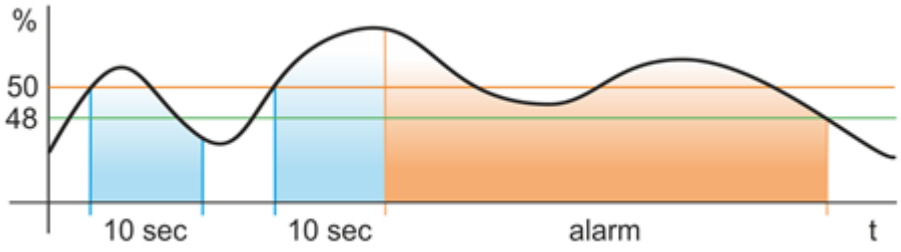
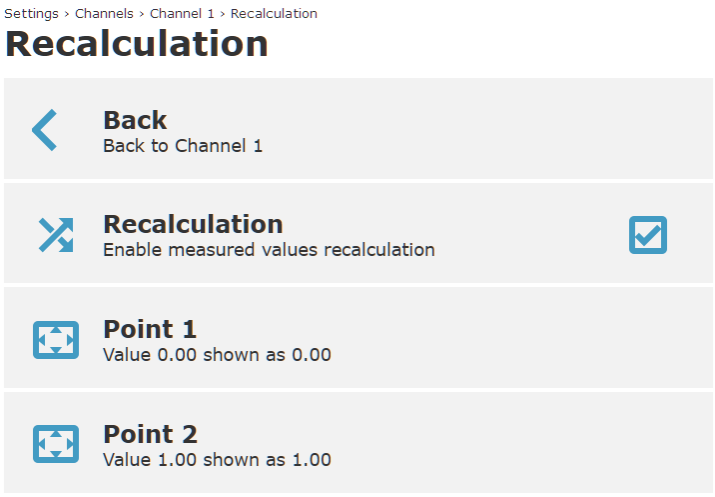


Image above illustrates how settings of alarms works. There is set alarm limit 50 % with delay 10 sec and hysteresis 2 %. At the beginning is alarm not activated because measured value does not exceed limit value for whole delay time. After that is alarm activated because measured value was above limit for longer time than is set delay. Alarm state persists till measured value goes under limit with hysteresis (50 % - 2 % = 48 %).

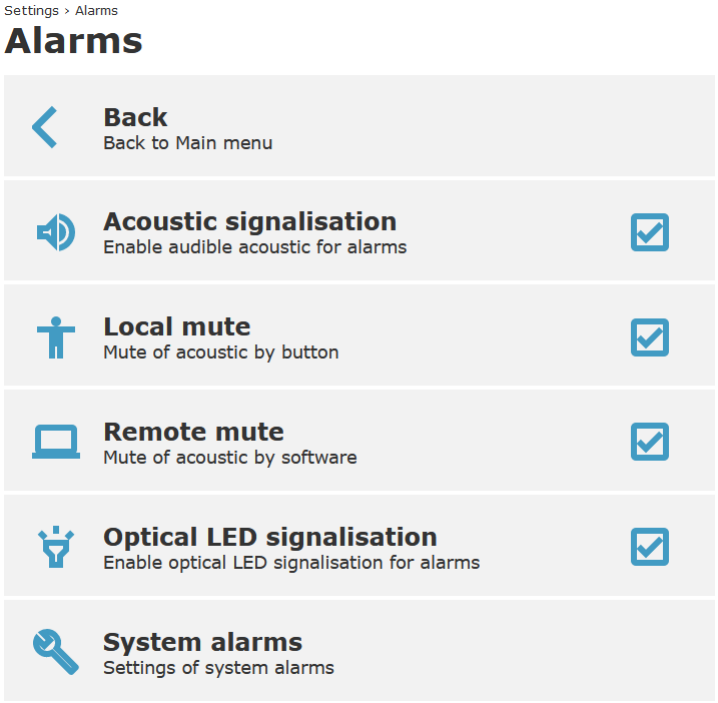
Recalculation of measured values

Measured values can be re-calculated using linear equation. This option can be enabled when some correction of measured values is needed. Enabling this option does not affect calibration of Digi probes or device itself.



Alarm settings

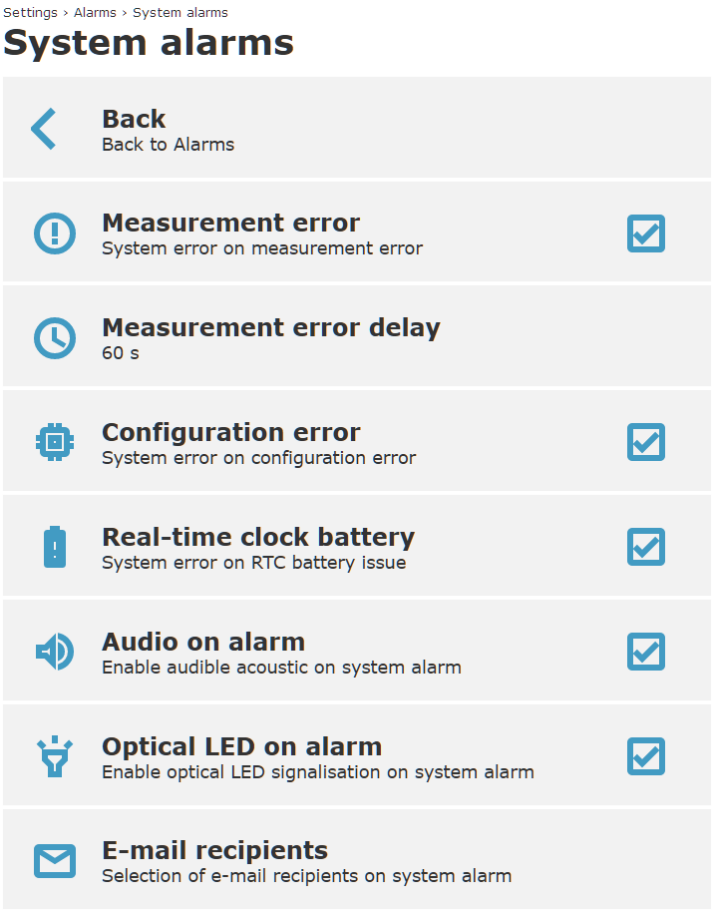
Alarm setting page allows for globally enable or disable audible and optical LED signalisation. There is option to enable local or remote mute of as well.



System alarms

System alarms are used to diagnose functionality of measurement chain including device or connected probes. A system alarm notifies about failure of the device including connected probes. On the other hand, alarms on measurement values indicate an issue with technology monitored by the device. System alarms may to be intended for different person than is responsible for alarms from measured values.

There are three system alarms. System alarm from measurement error on channel, system alarm from configuration error, and error from RTC battery. System alarm from measurement error is activated in case error state on any of channels occurs and this error persists for selected delay. Acoustic and LED signalisation can be used in case of system alarm if needed. Device has capability to send alarm email in case system alarm.



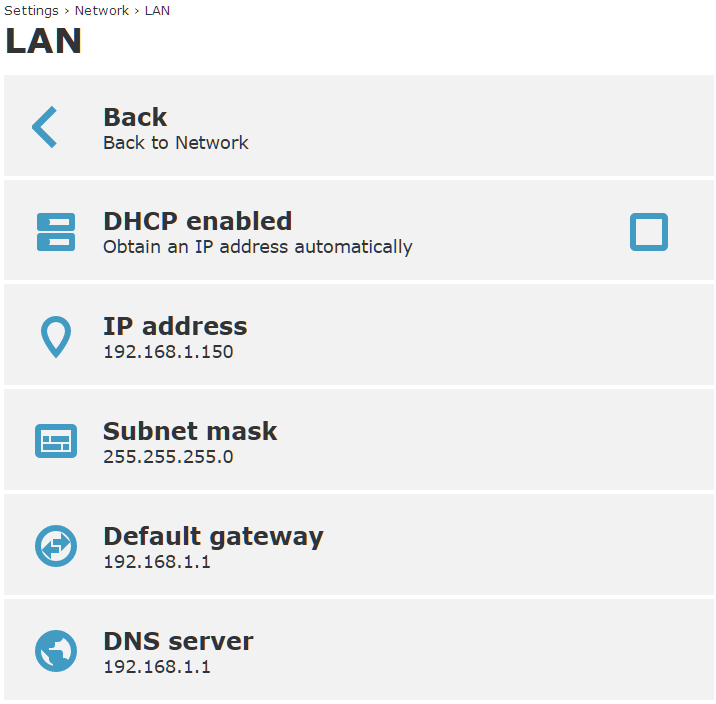
Network settings

Wi-Fi Client

For usage of Wi-Fi sensors at final deployment it needs to be device connected into infrastructure access point. Setup of connection parameters (SSID and password) is done at the Wi-Fi client menu. Scan item shows Wi-Fi networks at range. Wi-Fi network scan interval is set to 20 sec. In case of Wi-Fi network is not show at list, SSID can be inserted manually. When SSID field is blank device is automatically switched into AP mode and stay at this mode. At newly purchased device is SSID filed blank. Supported security modes are Open, WEP, WPA/WPA2-PSK, WPA2-PMF, WPA3 and WPA2-EAP. When WPA2-EAP security is used, it is mandatory set additional parameters at *EAP security* menu.

LAN

Setup of LAN parameters for Client mode. It can be used static IP address or IP address can be obtained from DHCP server automatically. By default, is DHCP option enabled. In case of static IP address need to be used, please contact your network administrator. Unproper IP address, subnet mask, gateway IP or DNS server IP settings can cause conflicts at network and communication troubles of other network devices.



Local IP address of the Wi-Fi sensors can be discovered by ways described at chapter *Troubleshooting*.

AP mode

AP mode is intended for device provisioning and for a first setup. Wi-Fi sensor comes into AP mode when SSID for Wi-Fi client mode is blank. Device can be switched into AP mode by the device buttons manually if needed. When device is switched into AP mode by buttons and there is no other communication with Wi-Fi sensor, device is switched back to client mode automatically after 10 minutes.

SSID, security and channel number can be changed according needs. By the default, SSID contains device serial number and Wi-Fi network security is not used. It is recommended to enable security for AP mode to prevent unauthorised access to the device. Wi-Fi channel number can be changed to prevent interferences with other Wi-Fi networks if needed.

At the AP mode Wi-Fi sensor have own DHCP and DNS server. Network parameters are stated below (parameters are not configurable from web). When Wi-Fi sensor at AP mode is configured from cell phone, it is recommended to deactivate mobile data.

AP mode network parameter	Value
Wi-Fi sensor IP address	192.168.3.1
Domain	wifisensor.net
Gateway IP address	192.168.3.1
DNS server IP address	192.168.3.1
Subnet mask	255.255.255.0
DHCP pool range	192.168.3.2 – 192.168.3.128
DHCP lease time	4096 sec

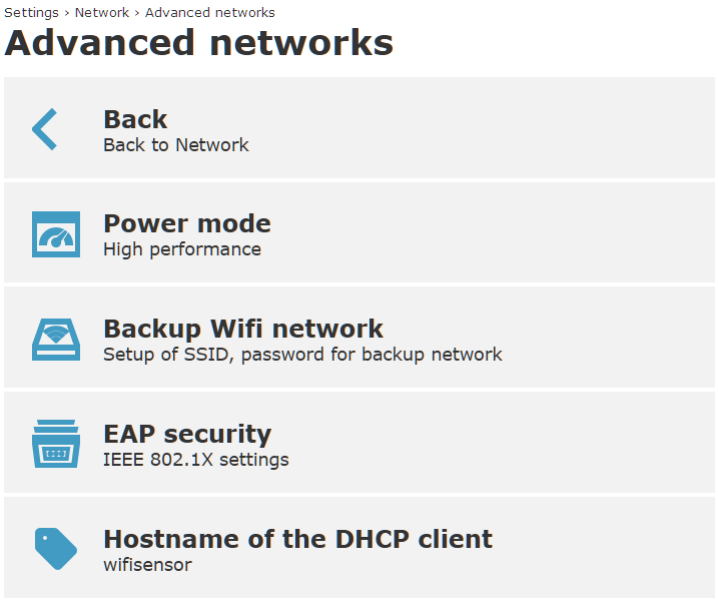
Advanced networks

Advanced networks menu allows to setup of additional wireless features. Power mode feature allow to adjust power consumption and latency at Wi-Fi client mode. At high performance mode have device higher power consumption and latency of network communication is lower. Normal performance mode decreases power consumption. Normal performance mode is recommended at devices stated below and when device is powered from external battery. Devices may not meet specified accuracy when power mode is changed to high performance at device which have set normal performance mode as default.

Backup Wi-Fi network option allows to set another SSID and password. These backup parameters are used in case of outage of primary Wi-Fi network (parameters set at Wi-Fi client option). Backup Wi-Fi parameters are used in case of device is not able to connect by the primary parameters for 2 minutes. In case of even backup Wi-Fi network is not available, device will alternate between primary and backup Wi-Fi with period 2 minutes.

EAP security option allows to setup parameters for WPA2 Enterprise security (IEEE 802.1X) including upload of required certificates.

Device identification for DHCP server at client mode is configurable via Hostname for DHCP client option. This option set name for mDNS as well.

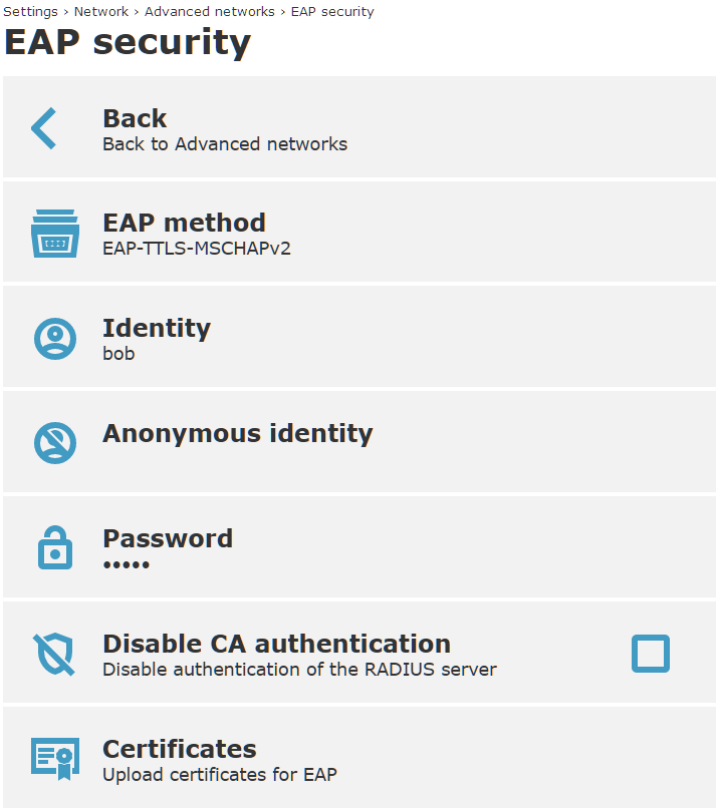


Default power mode	Device model(s)
High performance	AWP-T1P, AWP-T4P, AWP-TR1D, AWP-TR2D, AWP-TR1D-T3P, AWP-C
Normal performance	AWP-T, AWP-TR, AWP-TRCP, AWP-TRP

EAP security

WPA2-EAP security requires additional settings including uploading Certificate, Private key, and CA file. These information and files should be obtained from network administrator.

EAP method allows to setup mode used to authentication with RADIUS server. List of supported modes is available at *Wi-Fi radio* parameters. Identity and Anonymous identity are used for identification of the user with RADIUS server. Settings of Identity is required even for EAP-TLS methods. Password field is used as the "secret" for authentication of the user. It can be disabled validation of the authentication server against CA file if needed. Certificate, Private key, and CA file may to be uploaded by menu Certificates.

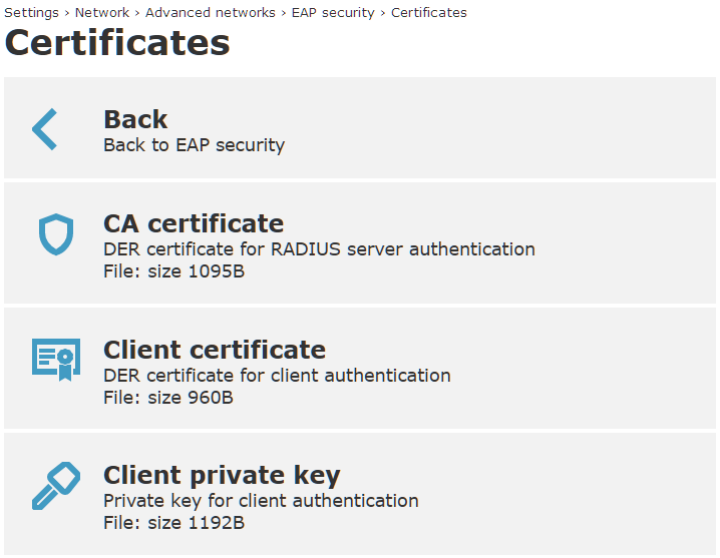


Certificates

At this menu Certificates is possible to upload Certificate, Private key, and CA file for WPA2-EAP security. Supported are files at binary DER format only. Files at PEM format or p12 format are not supported. When files are available at different format them DER, it needs to be converted before uploading into device.

CA certificate allows to upload CA file used for validation of authentication server. CA file needs to be uploaded at all EAP modes with exception EAP-FAST modes. Expiration of CA file is tested against current device time. CA authentication may to be disabled at settings. In this case is uploading of CA file not necessary. Disabling of CA authentication is not recommended from security standpoint.

Client certificate and Private key are mandatory for EAP-TLS modes. Be aware that Wi-Fi sensors supports EAP security with TLS 1.0 only.



Protocols settings

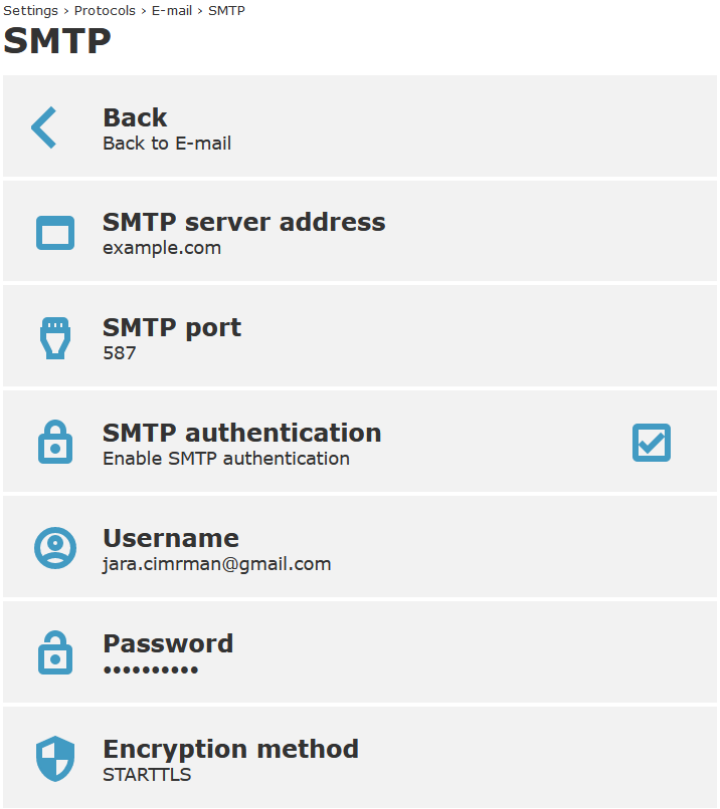
Email

Wi-Fi sensor can send alarm emails directly via SMTP server. Device can send warning email when alarm on channel occurs, or alarm is cleared. Email on system alarm can inform about measurement error or other hardware related issues. Device can send keep alive emails and repeat warning emails when alarm on channels persists.

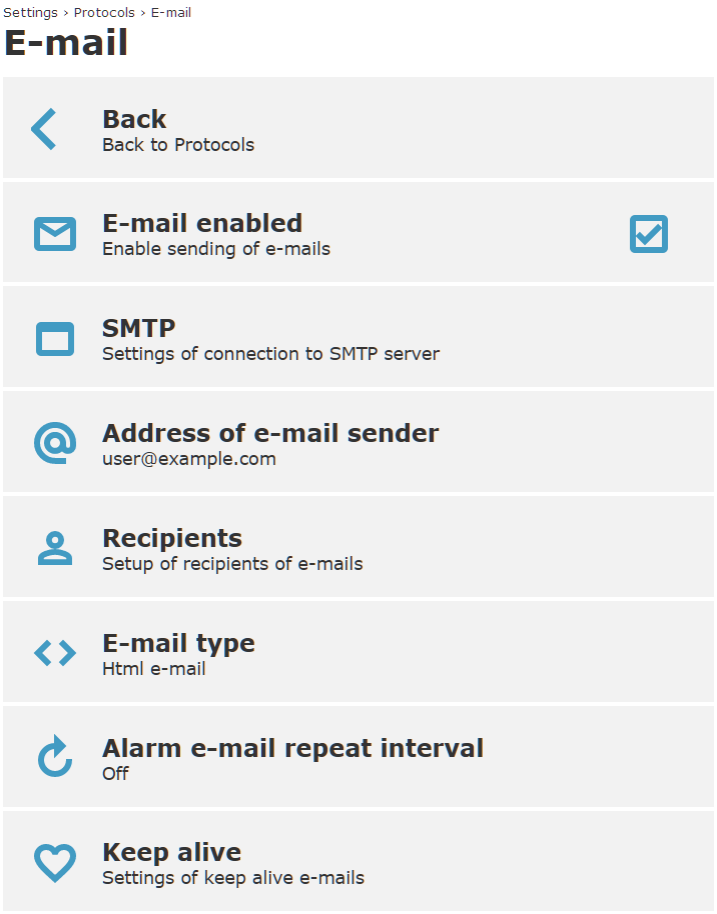
In case of ATAL Cloud or ATAL Database is used, it is not mandatory set sending emails from device itself. ATAL Cloud and ATAL Database have independent way how to send warning emails.

To be able send emails from the Wi-Fi sensors, connection to SMTP server need to be properly set. Information how to set SMTP parameters can provide network administrator. SMTP server address and port need to be set according to used server. When SMTP authentication is used, it needs to be set Username and Password. Username is commonly same as address of email sender. When encrypted communication with server is used, it can be enabled TLS or STARTTLS feature. Common combinations of SMTP port, encryption and authentication are stated at table below.

<table>
<tr><th colspan="2">SMTP server mode</th><th>SMTP port</th><th>Set username and password</th><th>Encryption method</th></tr>
<tr><td colspan="2">No auth. with no encryption</td><td>25</td><td>No</td><td>No</td></tr>
<tr><td colspan="2">Auth. with no encryption</td><td>25</td><td>Yes</td><td>No</td></tr>
<tr><td>Auth. with encryption</td><td>TLS</td><td>465</td><td>Yes</td><td>TLS</td></tr>
<tr><td>Auth. with encryption</td><td>Start TLS</td><td>587</td><td>Yes</td><td>STARTTLS</td></tr>
<tr><td>Auth. with encryption</td><td>OAuth</td><td>465</td><td colspan="2" rowspan="2">Not supported mode</td></tr>
<tr><td>Auth. with encryption</td><td>OAuth</td><td>587</td></tr>
</table>



In addition to the correct setup of SMTP server connection, the address of email sender and addresses of recipients needs to be set. Wi-Fi sensors support up to four recipients which can be for each type of email enabled independently. It can be set email at text or html format according needs. Alarm repeat interval can be selected at range 10 min to 12 hours. In case of this option is enabled, emails are sent repeatedly to recipients if alarm state at channel persists. Keep alive emails can be sent to selected recipients at interval 1 hour to 12 hours if needed.



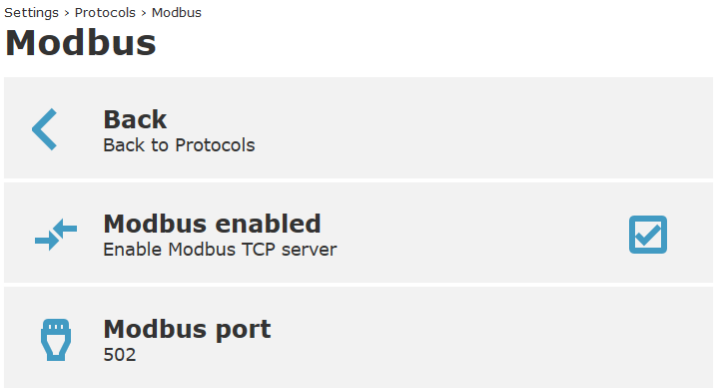
Proper settings of SMTP parameters can be tested at Advanced options menu accessible from main page. At first step need to be email and SMTP connection properly set at settings. After that email can be tested. Return codes are described at table below.

Last state	Description
Unknown	State of test email is unknow. It is likely that request for testing email was not required yet.
Waiting	Sending of testing email is under progress. Please wait.
Successfully sent	Testing email was successfully sent via SMTP server. Please check your inbox.
Error 1	DNS resolve error. Please make sure that is set proper address for SMTP server and IP address of DNS server is correct.
Error 2	Unable to create socket. Please contact support.
Error 3	Unable to open TCP/TLS connection to SMTP server. Please make sure that is set proper address of SMTP server and ISP connectivity is available. Another reason can be not properly set network parameters like a subnet mask, gateway IP or blocked communication at firewall.
Error 4	Connection was instantly closed by server. Please make sure that set proper address of SMTP server and make sure that TLS option is not required.
Error 5	Wrong response to welcome HELO or EHLO command. It seems stat opposite server is not a SMTP server or server requires TLS

	connection which is not enabled at the device. Please check SMTP server address and make sure that TLS option is not required.
Error 6	Authentication error. Error during sending AUTH LOGIN command. Please make sure that authentication at server is enabled and AUTH LOGIN command is supported by server.
Error 7	Authentication error. Error during sending username. Please make sure that is set proper username.
Error 8	Authentication error. Error during sending password. Please make sure that is set proper password.
Error 9	Error during sending MAIL FROM command.
Error 10	Error during sending RCPT TO commands.
Error 11	Error during sending DATA command.
Error 12	Error during sending data of the email message.
Error 13	Error during sending end of the data (dot command).
Error 14	Error during sending QUIT command.
Error 15	Authentication error. It likely that was set wrong username or password. Please make sure that is set proper e-mail sender address. Sender email address is commonly same as username for authentication. Another option can be that user is refused by SMTP server from other reason (e.g. connection is not allowed from that subnet).
Error 16	Other error during communication with SMTP server. It is likely that email was not sent. Device diagnostic log can provide more details about reason of issue.
Error 17	Unable to send test email. Emails are globally disabled, or email parameters are not properly set (e.g. SMTP server address is wrong, is set wrong email sender or no email recipients are set).
Error 18	Error during sending STARTTLS command.
Error 19	Unable to switch socket to secured. Please make sure that STARTTLS feature is supported by SMTP server.

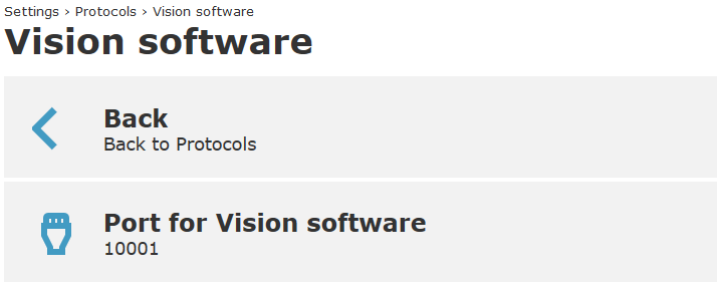
Modbus

Device has integrated Modbus TCP server which allows readings of current values by the 3rd party software (SCADA system). Server inside device can serve two Modbus TCP connections simultaneously. Modbus port is set to 502 by default and Modbus protocol is enabled. Protocol may be disabled if is not used. Modbus TCP registers are described at chapter *Modbus TCP*.



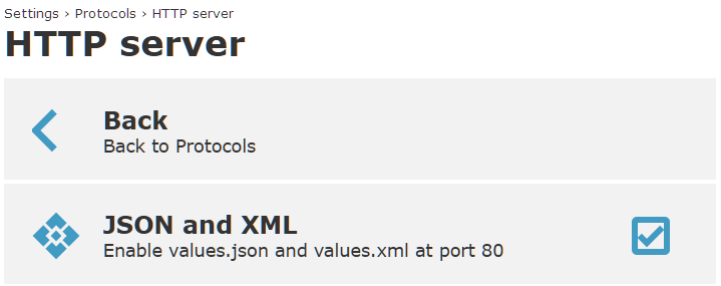
Vision software

Settings of TCP communication port for PC software – WifiSensorUtility, etc. Port is set to 10001 by default and may to be changed according to requirements. Wi-Fi sensor here act as a TCP server. Communication port is secured by TLS connection and verified against certificate by software.



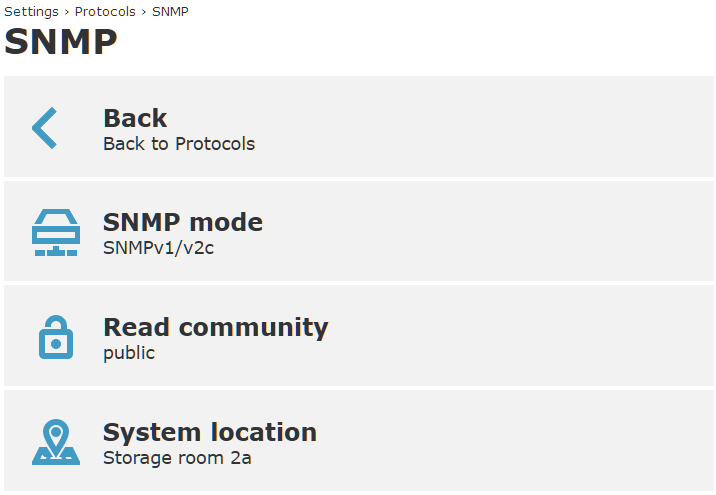
HTTP server

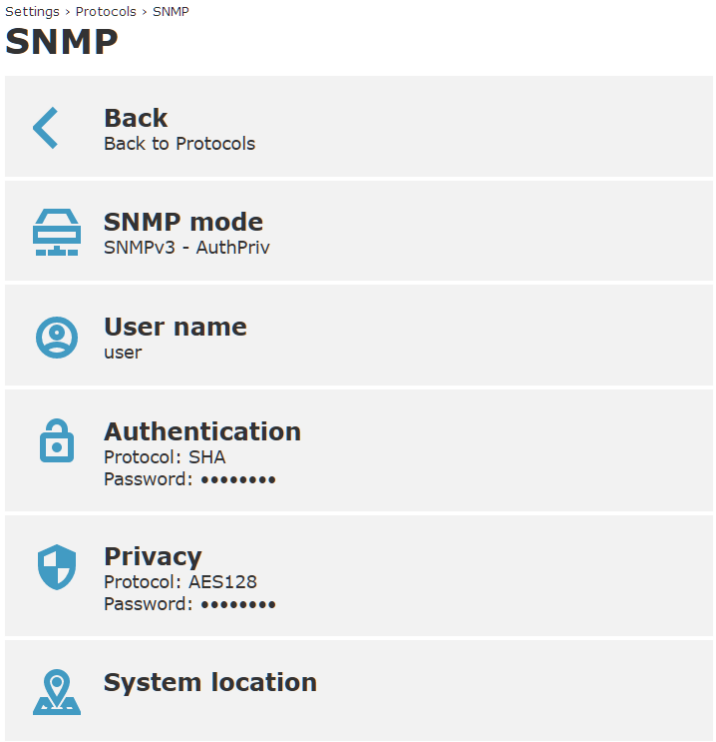
Measured values can be obtained by HTTP GET requests sent to http server running at Wi-Fi sensor at TCP port 80. Values can be provided in XML or JSON format via files values.xml and values.json. Feature is independent on device security and can be enabled according needs. Detail information are at chapter *JSON and XML via http server*.



SNMP

Wi-Fi sensors can provide measured values via SNMP protocol. Supported versions of protocol are SNMPv1, SNMPv2c and SNMPv3. Default SNMP mode is SNMPv1/v2c. SNMP read community (password) is set to public as default. SNMPv3 have three types of operation (NoAuthNoPriv, AuthNoPriv and AuthPriv). Depending on used mode it needs to be set username, password for authentication and privacy password. System location allow to set description of position where is device located. Writing via SNMP protocol is not supported. Detail description of SNMP protocol and OID keys you find at chapter *SNMP protocol*.





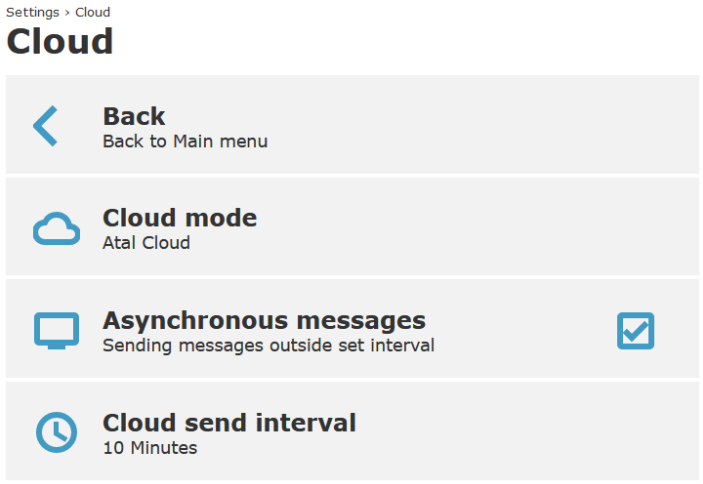
Cloud protocol settings

Wi-Fi sensors have capability to send current readings to remote server by http(s) POST with JSON data structure. This feature is used for data transmission into ATAL Cloud, ATAL Database or 3rd party server. Detail description of protocol is available at chapter *Cloud protocol - JSON*. Values are stored into internal non-volatile memory in case of data transfer to server is not successful. Size of this memory is 2240 sets of values. Thanks to this feature, current readings are not lost in case of Wi-Fi or connectivity outage. There are two modes of Cloud protocol – ATAL Cloud and ATAL Database / User server.

ATAL Cloud mode

By enabling this mode device sends current readings directly into ATAL Cloud. ATAL Cloud is a paid service. Each Wi-Fi sensor comes with 3 moths free trial period for ATAL Cloud. It allows to test features of ATAL Cloud without any additional costs. To be device visible at ATAL Cloud, it needs to be registered into Cloud. This can be done by the procedure described at registration card. Registration card is part of original package.

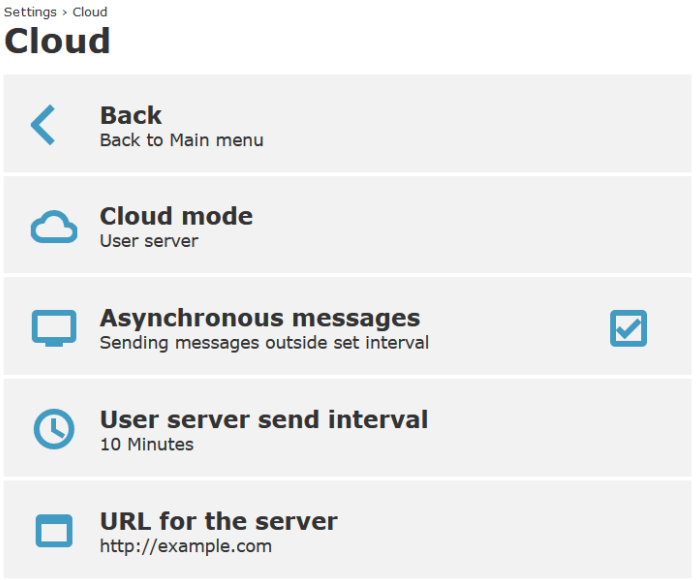
Sending interval into ATAL Cloud is adjustable at range 5 min to 12 hours. Shortest recommended interval is 10 min. Enabled feature of Asynchronous messages allows to send messages when alarm event occurs or is cleared. Asynchronous message is sent after connection into Wi-Fi networks as well. Asynchronous messages are enabled by default.



ATAL Database / User server

This mode allows to send messages to ATAL Database software or to the 3rd party system. ATAL Database is a SQL based system which allow to acquire measured values from ATAL devices and analyse them. ATAL Database can be used as alternative to ATAL Cloud at highly secure environment where is usage of Cloud services not allowed. 30-days trial version of ATAL Database is available. Device settings required to proper connection into ATAL Database is described at manual for ATAL Database.

Sending interval can be adjusted at range 10 sec to 12 hours. Enabled feature of Asynchronous messages allows to send messages when alarm occurred or is cleared. Memory for unsent readings can be deactivated if needed. By disabling this feature will be values lost in case of Wi-Fi or connectivity outage. URL need to contain proper address of entry point for ATAL Database or 3rd party http server.



Testing Cloud message

Connection to Cloud server can be tested at Advanced options menu accessible from main page. The first step is to enable and saving Cloud settings. After that, the Cloud connection can be tested. Return and error code at Cloud message test:

Last state	Description
Unknown	State of test message is unknow. It is likely that request for testing message was not required yet.
Waiting	Sending of testing message is under progress. Please wait.
Successfully sent	Message was successfully delivered and confirmed by the server.
Error 1	Request was not sent because device is not at connected Client mode. In case of device is at AP mode, testing message cannot be sent.
Error 2	DNS resolve error. Please make sure that is set proper URL for Cloud server and IP address of DNS server is correct.
Error 3	Unable to create Cloud socket. Please contact support.
Error 4	Unable to open TCP/TLS connection to Cloud server. Please make sure that is set proper URL, server is running, and ISP connectivity is available. Another reason can be not properly set network parameters like a subnet mask, gateway IP or blocked communication at firewall.
Error 5	Transfer error to the server. Device can open TCP/TLS connection, but data transfer was not successful. Please make sure that at opposite side is running http(s) server.
Error 6	Missing parameter <Result> at response. It seems that at opposite side is running http(s) server but is not able to process communication from device.
Error 7	Missing confirmation (“True”) at <Result> parameter.
Error 8	Unable to send message. Cloud protocol is not enabled or wrong URL for Cloud server.

Communication protocols

Modbus TCP

Modbus TCP protocol allows to read measured values from the device by the 3rd party SCADA software. Modbus TCP server supports two connections (sockets) simultaneously. Default TCP port is 502. Modbus device address (Unit Identifier) can be arbitrary. Modbus write command is not supported. Brief description and example in Python language is available at About / Library section of webpages. Detail description of the Modbus protocol is free to download at *www.modbus.org*.

Supported Modbus commands (functions):

Command	Code	Description
Read Holding Register(s)	0x03	Reads 16-bit register(s)
Read Input Register(s)	0x04	Reads 16-bit register(s)

Table with Modbus registers. Depending on used communication library it may to be required insert register number(s). Number of the register is an address of register plus one (e.g. register with number 0x9C41 have the Modbus address 0x9C40). Inside Modbus TCP frames are physically send address.

Variable	Address [HEX]	Address [DEC]	Type
Device identification			
Serial number (Device serial number have 8 digits which are split into four Modbus registers)	0x9C22	39970	BCD
	0x9C23	39971	BCD
	0x9C24	39972	BCD
	0x9C25	39973	BCD
Device type	0x9C26	39974	HEX
Device states			
Internal acoustic signalisation	0x9C27	39975	INT
Optical LED signalisation	0x9C28	39976	INT
RSSI value	0x9C29	39977	INT
Configuration error	0x9C2A	39978	INT
System alarm - measurement error	0x9C2B	39979	INT
Low voltage of RTC battery	0x9C2C	39980	INT
Measured values			
Measured value at channel 1 … Measured value at channel 8	0x9C40 … 0x9C47	40000 … 40007	INT*X
State of alarm 1 at channel 1 …	0x9C48 …	40008 …	INT

State of alarm 1 at channel 8	0x9C4F	40015	
State of alarm 2 at channel 1 … State of alarm 2 at channel 8	0x9C50 … 0x9C57	40016 … 40023	INT
Unit for channel 1 … Unit for channel 8	0x9C58 … 0x9C5F	40024 … 40031	STR
Number of decimal places for ch1 … Number of decimal places for ch8	0x9C60 … 0x9C67	40032 … 40039	INT
Measured value at channel 1 … Measured value at channel 2	0x9C68 … 0x9C77	40040 … 40055	32b INT * (X+2)
Measured value at channel 1 … Measured value at channel 2	0x9C78 … 0x9C87	40056 … 40071	IEEE 754 FLOAT
Min. value for channel 1 … Min. value for channel 8	0x9C88 … 0x9C8F	40072 … 40079	INT*X
Max. value for channel 1 … Max. value for channel 8	0x9C90 … 0x9C97	40080 … 40087	INT*X

Type of variables:

Type	**Description**
BCD	Register is at BCD format (16bit)
HEX	Number at HEX format (16bit)
INT	Register is a signed 16bit integer with range -32768 to 32767
INT*X	Register is a signed 16bit integer. From the reason to increase resolution of transferred value, is measured value multiplied by value X. Number of decimal places can be obtained from registers 40032 - 40039 or from the table below. Example: number of decimal places is 1 then temperature value 238 from register can be translated to 23.8°C. Error values are transmitted as number lower than -32000 (e.g. -32005 = Error 5).
STR	Two bytes text via one 16bit Modbus register
INT*(X+2)	32bit measured value with increased resolution by 2. Value is transmitted via two 16bit Modbus registers. Most significant part of number is transmitted first (e.g. value 22.825 = reg1: 0, reg2: 22825). Error values are transmitted as numbers lower then -320000000 (e.g -320000011 = Error 11).
IEEE 754	Value is a 32bit IEEE 754 float value transmitted via two Modbus registers. Value 22.704 is transmitted like a 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	80 = 80.1 %RH
Dew point	1 (= *10)	°C or °F	93 = 9.3 °C
Absolute humidity		g/m^3	85 = 8.5 g/m^3
Specific humidity		g/kg	76 = 7.6 g/kg
Mixing ratio		g/kg	78 = 7.8 g/kg
Specific enthalpy		kJ/kg	445 = 44.5 kJ/kg
Humidex (at °C)			258 = 25.8
Barometric pressure	1 (= *10)	hPa	10117 = 1011.7 hPa
	2 (= *100)	kPa	10117 = 101.17 kPa
	1 (= *10)	mBar	10118 = 1011.8 mBar
	1 (= *10)	mmHg	7588 = 758.8 mmHg
	2 (= *100)	inHg	2988 = 29.88 inHg
	1 (= *10)	inH_2O	4062 = 406.2 inH_2O
	3 (= *1000)	PSI	14675 = 14.675 PSI
	1 (= *10)	oz/in^2	2348 = 234.8 oz/in^2
CO_2 concentration	0 (= *1)	ppm	890 = 890 ppm

Cloud protocol – JSON

Wi-Fi sensors have capability to send current readings to remote server by http(s) POST with JSON data structure. JSON protocol is described at this chapter. Python example of http server is available at About / Library section of webpages. There are two modes of Cloud protocol - ATAL Cloud mode and ATAL Database / User server. This chapter is described User server mode only.

Measured values are sent via HTTP POST with JSON data content. Structure of JSON message is described in chapter *JSON Structure*. Each message needs to be confirmed by response described in chapter *Message response*. In case the message is not confirmed from the server side, then message is not marked as successfully sent. And when memory (cache) feature is not deactivated, message is re-sent again at next connection. Messages from memory (cache) are send first. Size of memory (cache) is 2240 messages and is cleared after changing device setup. Device uses HTTP 1.1 transfer. That means via one TCP connection can be sent multiple POST requests (multiple JSON messages). In case of server is not capable to properly serve this behaviour, memory (cache) feature needs to be deactivated. Responses without chunked transfer encoding are expected (that means messages with proper header Content-Length are expected). Device supports HTTP and HTTPs JSON message.

JSON structure

Structure of JSON wrapper is following:

```
{
  <JsonType>,
  <JsonVersion>,
  <OrderId>,
  <MsgType>,
  <MsgCache>,
  <Sn>,
  <Desc>,
  <Kind>,
  <AState>,
  <NConf>,
  <ConfID>,
  <Interval>,
  <Time>,
  <Rssi>,
  <LocalIP>,
  <Channels>
}
```

AState filed structure:

```
<AState>: { <Reg>, <Mask> }
```

Time field structure:

```
<Time>: { <Now>, <Sample>, <IsValid> }
```

RSSI values structure:

```
<Rssi>: { <Now>, <Sample> }
```

Structure for channels:

```
<Channels>:
[
```

```
  {
    <Nr>,
    <En>,
    <Quant>,
    <Val>,
    <ValStr>,
    <Unit>,
    <Dec>,
    <Alarm>: [ <_Al1>, <_Al2> ],
    <AlarmLim>: [ <_AlLim1>, <_AlLim2> ],
    <AlarmMode>: [ <_AlMode1>, <_AlMode2> ]
  },
  {
    <Nr>,
    <En>,
    <Quant>,
    <Val>,
    <ValStr>,
    <Unit>,
    <Dec>,
    <Alarm>: [ <_Al1>, <_Al2> ],
    <AlarmLim>: [ <_AlLim1>, <_AlLim2> ],
    <AlarmMode>: [ <_AlMode1>, <_AlMode2> ]
  },

  ...
  ...

]
```

Description of parameters inside JSON message:

Parameter	Type	Range	Description
<JsonType>	INT		Type of the JSON message. For a Wi-Fi sensor is set to 2.
<JsonVersion>	INT		Version of JSON message. At present time is set to 1.
<OrderId>	INT	0 – 32bit unsigned	Order number of messages from device restart. First message is set to 0.
<MsgType>	INT	0 – 4	Message type: 0 first message after restart 1 first message after changing config 2 synchronous message 3 asynchronous message 4 testing message
<MsgCache>	INT	0 – 7	Reason code in conjunction with JSON cache/non-volatile memory: 0 direct message without using cache 1 sent from cache (NO_WLAN) 2 sent from cache (DNS_ERR) 3 sent from cache (SOCK_ERR) 4 sent from cache (CONNECTION_ERR) 5 sent from cache (TRANSFER_ERR) 6 sent from cache (RESULT_NO) 7 sent from cache (RESULT_CONFIRM)
<Sn>	STR	8B length	Serial number of the device (e.g. 20286614)
<Desc>	STR	64B length	Device name at UTF-8
<Kind>	INT	1 – 11	Identification of device type: 1 AWP-T T 2 AWP-T4P T

				3	AWP-TR	T+RH
				4	AWP-TR1D	T+RH
				5	AWP-TR2D	T+RH
				6	AWP-TR1D-T3P	T+RH
				7	AWP-TRP	T+RH+P
				8	AWP-TRCP	T+RH+P+CO2
				9	AWP-C	CO2
				11	AWP-T1P	T
<AState>				AState status register. Description of the AState register is described at table below.		
	<Reg>	INT	0 – 65535	Value of the AState register at the moment when request was created.		
	<Mask>	INT	0 – 65535	Mask of active bites at AState register		
<NConf>		INT	0 – 255	Configuration number		
<ConfID>		STR	15B length	Configuration unique ID (X-YYYYYYYY-ZZZZ)		
<Interval>		INT	0 – 65535	Sending interval in [sec]		
<Time>				Date and time		
	<Now>	STR	RFC3339	Time when message was transmitted to server		
	<Sample>	STR	RFC3339	Time when message was sampled (it can be older then <Now> due to sending message from cache)		
	<IsValid>	INT	0, 1	Indication if time is valid (1 = RTC time is valid)		
<Rssi>				RSSI (Received signal strength indication at [dBm]). In case of value is not available is returned -99. Expected range for Wi-Fi is at range -30 to -99dBm.		
	<Now>	INT	< 0	RSSI value at the time when message is transmitted to server		
	<Sample>	INT	< 0	RSSI value at the time when message was sampled		
<LocalIP>		STR	64B length	IP address of the device at local network		
<Channels>				Measured values at channels. In case of channel is not available at the device, channel is not shown.		
	<Nr>	INT		Channel number		
	<En>	INT	0, 1	Channel is enabled at settings (1 = enabled)		
	<Quant>	STR	32B len	Name of the channel at UTF-8		
	<Val>	STR	32B length	Measured value at float format transmitted via HEX characters (FF8100NN = error number NN)		
	<ValStr>	STR	32B length	Measured value at string format (e.g. 12.8, n/a, Error X)		
	<Unit>	STR	16B length	Unit of the channel at UTF-8		
	<Dec>	INT	0 - 10	Number of decimal places		
	<Alarm>			State of alarm at the channel (1 = alarm)		
		<_Al1>	INT	0, 1	Alarm 1 at channel	
		<_Al2>	INT	0, 1	Alarm 2 at channel	
	<AlarmLim>			Alarm limit at float format transmitted via HEX characters. IEEE 754 Float number 72.0442 is transmitted as hexadecimal string 429016A0.		
		<_AlLim1>	STR	32B len	Alarm 1 limit for channel	
		<_AlLim2>	STR	32B len	Alarm 2 limit for channel	

	<AlarmMode>				Alarm mode:	
					0	alarm disabled
					1	lower than limit
					2	higher than limit
		<_AlMode1>	INT	0 – 2	Alarm 1 mode	
		<_AlMode2>	INT	0 – 2	Alarm 2 mode	

JSON field <AState>-<Reg> is a status of the device at moment when values were sampled. Description of the status bits:

Bit	Description
bit0 – bit1	RSSI level indicator (0 = poor signal, 1 = sufficient, 2 = good, 3 = excellent)
bit2 – bit4	Unused
bit5	WLAN co-processor error (=1)
bit6	Internal hardware error (1 = Internal hardware error - RTC, EEPROM, LCD)
bit7	Device properly connected into Wi-Fi (=1)
bit8	Optical LED active (=1)
bit9	Acoustic active (=1)
bit10	Unused
bit11	RTC time may not be valid - low voltage detected at RTC (=1)
bit12	Measurement error at one of channels (=1)
bit13	Configuration is not valid - configuration error (=1)
bit14 – bit15	Unused

Some bits at AState register can be deactivated at the configuration. Table below shows these bits. Other bits are unused.

Bit	Description
bit8	Optical signalisation is enabled inside the configuration (=1)
bit9	Acoustic is enabled inside the configuration (=1)
bit12	Enabled feature alarm on measurement error (=1)

Message response

Delivered messages to http(s) server needs to be confirmed by following response:

```
{
  <Result>,
  <Message>
}
```

Parameter	Type	Range	Description
<Result>	BOOL		Response whether incoming message was successfully processed by the server. In case of server response is true, message is marked as successfully sent and message is removed from cache (if cache feature is not deactivated).
<Message>	STR	100B length	Optional text message from server. This text message can be shown at diagnostic log (text message cannot contain character ").

Example the proper response:

```
HTTP/1.1 200 OK
Date: Thu, 02 Jul 2020 08:04:30 GMT
Content-length: 75
{
  "Result":true,
  "Message":"All is OK. Message was successfully processed."
}
```

JSON and XML via http server

Measured values can be obtained by HTTP GET requests sent to http server running at Wi-Fi sensor at TCP port 80. Values can be provided in XML or JSON format via files values.xml and values.json. Feature is independent on device security. From this reason is feature disabled by default. To be able utilize this feature, it needs to be intentionally enabled at device setup. When feature is disabled http error code 403 is returned. Python examples how to get values via XML and JSON file are available at About / Library section of webpages.

Responses to GET requests to files values.xml and values.json at port 80 are served by the http 1.0 server with single TCP socket capability. Response time depends on Wi-Fi signal strength and load of http server. Average response time at high performance mode is 25 ms. In case of communication issues or server overloading it can be response time up to 10 sec.

XML structure

XML file structure can be validated against XSD schema available at About / Library section of webpages. At same place are available examples of XML files as well.

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. 20280001)
<time>	STR	RFC3339	Current device time
<timeunix>	INT	32bit unsigned	Current device time as Unix timestamp (seconds since 01/01/1970)
<synch>	INT	0, 1	Indication if device time is valid (1 = time is valid)
<rssi>	INT	< 0	Received signal strength indication at [dBm]
<acc>	INT	0, 1	Acoustic active (=1)
<ch1> … **<ch8>**			Element with information about each channel with current measured values.

Description of tags for channels:

Parameter	Type	Range	Description
<name>	STR	32B length	Name of the channel (at English language)
<unit>	STR	16B length	Unit of the channel
<value>	STR	32B length	Measured value at 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

Structure of JSON file values.json is following:

```
{
  <devname>,
  <devsn>,
  <time>,
  <timeunix>,
  <synch>,
  <rssi>,
  <acc>,
  <ch> [
    {
      <name>,
      <unit>,
      <value>,
      <alarm1>,
      <alarm2>
    },
    ...
    ...
    {
      <name>,
      <unit>,
      <value>,
      <alarm1>,
      <alarm2>
    }
  ]
}
```

where:

Parameter		Type	Range	Description
<devname>		STR	64B length	Device name
<devsn>		STR	8B length	Serial number of the device (e.g. 20280001)
<time>		STR	RFC3339	Current device time
<timeunix>		INT	32bit unsigned	Current device time as Unix timestamp (seconds since 01/01/1970)
<synch>		INT	0, 1	Indication if device time is valid (1 = time is valid)
<rssi>		INT	< 0	Received signal strength indication at [dBm]
<acc>		INT	0, 1	Acoustic active (=1)
<ch>	**<name>**	STR	32B length	Name of the channel (at English language)
	<unit>	STR	16B length	Unit of the channel
	<value>	STR	32B length	Measured value at 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)

SNMP protocol

Measured values, alarms, and device state can be read by SNMP protocol. Supported are SNMPv1, SNMPv2c and SNMPv3. As default mode is used mixed mode SNMPv1/v2c. SNMP uses UDP port 161. Default SNMP read community is set to public. Writing via SNMP protocol is not supported. SNMP Traps are not supported. MIB table is available at About / Library section of webpages.

Supported operation modes with SNMPv3 are following - NoAutNoPriv (authentication and encryption is not used), AuthNoPriv (authentication without encryption) and AuthPriv (authentication with encryption). When AuthNoPriv and AuthPriv modes are used, key(s) need to be calculated from password(s). This calculation requires extensive computing resources. From this reason startup of SNMP protocol is delayed by 30 sec after device boot or changing SNMP settings. Supported authentication types are MD5 and SHA. Supported privacy protocols are DES and AES128 (commonly called as AES only).

Recommended is usage of SNMPv3 at AuthPriv mode with SHA and AES128. Passwords for authentication and privacy should not be same. Passwords should have at least 8 characters without repetitive characters.

List of SNMP OID keys:

OID	Type	Description
Device identification		
.1.3.6.1.4.1.22626.1.8.1.1.0	STRING	Device name
.1.3.6.1.4.1.22626.1.8.1.2.0	STRING	Device serial number
.1.3.6.1.4.1.22626.1.8.1.3.0	INTEGER	Device type
.1.3.6.1.4.1.22626.1.8.1.4.0	STRING	Device model as string
Measured values (ch = 1 to 8)		
.1.3.6.1.4.1.22626.1.8.2.1.1.1.ch	INTEGER	Channel number
.1.3.6.1.4.1.22626.1.8.2.1.1.2.ch	STRING	Channel name
.1.3.6.1.4.1.22626.1.8.2.1.1.3.ch	STRING	Measured value
.1.3.6.1.4.1.22626.1.8.2.1.1.4.ch	INT*X	Measured value at format INT*X
.1.3.6.1.4.1.22626.1.8.2.1.1.5.ch	INTEGER	Number of decimal points for value INT*X
.1.3.6.1.4.1.22626.1.8.2.1.1.6.ch	STRING	Channel unit
.1.3.6.1.4.1.22626.1.8.2.1.1.7.ch	INTEGER	State of alarm 1 at channel
.1.3.6.1.4.1.22626.1.8.2.1.1.8.ch	INTEGER	State of alarm 2 at channel
.1.3.6.1.4.1.22626.1.8.2.1.1.9.ch	STRING	Minimal value for channel
.1.3.6.1.4.1.22626.1.8.2.1.1.10.ch	STRING	Maximum value for channel
Device state		
.1.3.6.1.4.1.22626.1.8.3.1.0	INTEGER	Acoustic signalisation active
.1.3.6.1.4.1.22626.1.8.3.2.0	INTEGER	Optical LED signalisation active
.1.3.6.1.4.1.22626.1.8.3.3.0	INTEGER	RSSI (signal strength)
.1.3.6.1.4.1.22626.1.8.3.4.0	STRING	Time according RFC3339
.1.3.6.1.4.1.22626.1.8.3.5.0	STRING	Time at Unix timestamp
.1.3.6.1.4.1.22626.1.8.3.6.0	INTEGER	Time is valid
.1.3.6.1.4.1.22626.1.8.3.7.0	INTEGER	Device configuration error

.1.3.6.1.4.1.22626.1.8.3.8.0	INTEGER	Measurement error
.1.3.6.1.4.1.22626.1.8.3.9.0	INTEGER	Real-time clock battery error

List of supported OID keys for MIB-II 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 start-up)
.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 device setup)
.1.3.6.1.2.1.1.6.0	STRING	sysLocation (system location from device setup)
.1.3.6.1.2.1.1.7.0	INTEGER	sysServices (72=application services)

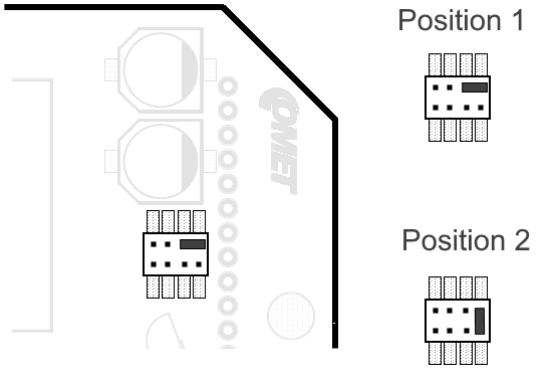
Troubleshooting

Factory defaults

By the factory defaults procedure, the device is restored into same state as was newly purchased. Current device settings are lost including passwords and Wi-Fi connection parameter. Provisioning procedure for connecting into Wi-Fi network needs to be done again. Uploaded certificates for WPA2-EAP security are not deleted during factory defaults procedure. Factory default procedure can be done locally only. Lid of device needs to be disassembled using screwdriver Torx T10. This screwdriver is not a part of shipment.

Factory defaults procedure:

1. Remove device power supply by disconnecting USB-C connector.
2. Unscrew four Torx screw and open device lid.
3. Change jumper position from Position 1 to Position 2 as shown at image below. For changing jumper position may to be used tweezers.



4. Connect power supply by the USB-C connector.
5. Wait till be shown text DEF1 DONE at LCD display.
6. Disconnect power supply.
7. Move jumper back to Position 1.
8. Close device lid and put back all four screws.
9. Power on device. Factory defaults restore procedure was accomplished.

Factory defaults procedure restore configuration of device itself. Calibration constants inside Digi probes and device are not changed. Device calibration can be restored by modified factory default procedure. Before you power on device (point 4), you need to press and hold button SET. Button can be released while text DEF2 DONE is shown. Other steps are same as at procedure above.

Forgotten administrator password

When administrator password is forgotten and there is no access to the device, *Factory defaults procedure* should be done. Procedure is described in chapter above.

How to determine device IP address

IP address of device in Client mode can be obtained from DHCP server or can be set manually static IP. IP address at Access point mode is not configurable by end-user and is set to 192.168.3.1. IP address of device regardless selected mode can be determined by multiple ways.

- IP address is shown on the device LCD display after short press of MODE button. When IP address is show as 0.0.0.0 it means IP address is not assigned. Either device is not connected into Wi-Fi network or Wi-Fi sensor was not able obtain IP address from DHCP server.
- IP address can be discovered by search option at software ATAL Vision or software TSensor. This software is free for download at manufacturer webpages.
- Local IP address of Wi-Fi sensor can be shown at ATAL Cloud or ATAL Database. To be able to utilize this feature, Wi-Fi sensor needs to be connected to that platform.
- Web interface of the infrastructure access point / router can show IP address when device is at Client mode and DHCP is used. This may to vary according to model of access point / router.

How to use newly connected Digi probe

When Error 30, Error 40 or text n/a is shown at channel after connection new Digi probe, it means that Digi probe need to be detected. Probes are detected after device restart of can be detected manually at menu Advanced options / Service.

Error codes at channels

This chapter contains list of error codes which may to be shown at channel(s). Please follow recommendation below before you contact technical support. Error codes at LCD display are shown with prefix character „E". Error codes are reported via Modbus TCP registers as numbers lower than -32000 (e.g. -32005 = Error 5).

Error code	Description
Error 1	A/D converter for measurement from Pt1000 probes is under lower limit. It is likely that temperature probe is shorted. Please inspect probe for a damage and replace damaged probe.
Error 2	A/D converter for measurement from Pt1000 probes is above high limit. It is likely that temperature probe is not connected, or cable is damaged. Please inspect probe for a damage or connect probe.
Error 3	Measured value is outside expected range. Please contact technical support.
Error 4	The source value for computed value (dew point) is not available. Please check relevant Digi probe if is properly connected and is not damaged.
Error 10	Communication error with internal CO_2 sensor. Please contact technical support.
Error 11	Measurement error from internal CO_2 sensor. One of reasons for this error is an insufficient voltage from power source. Please make sure that is used proper power supply adapter, USB cable is not too long or damaged. In case of issue will not be resolved by using another adapter and cable, contact technical support.
Error 15	Communication error with relative humidity sensor inside Digi probe. It is likely that relative humidity sensor is damaged. Please restart device by disconnecting from power source. If error state persists, replace Digi probe.
Error 16	Measurement error from relative humidity sensor. Please restart device by disconnecting from power source. If error state persists, replace Digi probe.
Error 20	Unable to read calibration constants from internal barometric pressure sensor. Please contact technical support.
Error 21	Measurement error at internal barometric pressure sensor. Please contact technical support.
Error 30	Communication error with internal A/D converter. Please contact technical support.

Error 35 or n/a	Measured value from Digi probe is not available. It is likely that Digi probe is not connected. Please connect Digi probe and detect Digi probe(s).
Error 36	During Digi probe detection procedure was returned CRC error of memory for calibration data. Please contact technical support. They will provide software WifiSensorUtility which will allow to restore content of memory for calibration data from backup.
Error 37	Unknow type of Digi probe. Please update firmware version and after that detect Digi probe(s) again.
Error 38	Communication error with memory for calibration data inside Digi probe. It is likely that Digi probe is not connected properly, or probe is damaged. Please connect properly Digi probe or replace damaged probe.
Error 39	Memory for calibration data inside Digi probe have wrong CRC. Please follow procedure for Error 36.
Error 40	Connected type of Digi probe is not same as was detected probe. Please detect connected Digi probe(s) again.
Error 50	Device configuration for channel is damaged. Damaged configuration can be fixed by the Factory defaults procedure or using WifiSensorUtility which can be obtained from technical support.
Error 52	Measured value cannot be shown due to overflow during conversion.
Error 53 or n/a	Value is not available. This error is shown at disabled channels or when value was not measured yet. CO_2 concentration is available 15 sec after device start-up.
Error 55	This error is related to values transferred via Modbus TCP. It signalises overflow of Modbus register.

Warning exclamation mark on LCD

Warning exclamation mark shown on left bottom corner of LCD display signalise issue with device itself. Main reasons for this warning are:

- Hardware issue with one of these components – Wi-Fi coprocessor, internal memory chip, RTC chip or LCD driver chip.
- Damaged content of configuration memory.

Damaged content of configuration memory can be identified by warning message in case of attempt to device setup. Damaged content can be fixed by the *Factory defaults procedure* or using WifiSensorUtility. This software can be obtained from technical support.

In case of issue with hardware, please contact technical support directly.

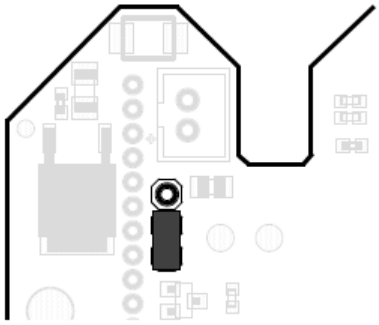
Battery symbol at LCD or wrong device time

Device time is maintained by internal RTC (real-time clock) circuit with coin-cell backup battery. Battery lifetime is designed for a whole device lifespan and is not exchangeable by the end-user.

In case of battery sign at LCD display and red exclamation mark at the web pages are shown, it means that current time may not be correct. Correct time at device setup should be set and saved. After that can be device powered off for 5 minutes to validate that coin-cell backup battery works properly. If battery symbol is shown after power-on again, please contact technical support.

Unable to power on device

When device is not showing any signs of function when power supply is connected, it generally means issue with power adapter or USB cable. At first step please make sure that mains socket is functional and is used compatible power adapter. If so, exchange power adapter and USB cable to another one. Specification of USB cable and power adapter you find at chapter *Power supply*. If issue will not be resolved, please open device lid and visually inspect device board for any damage. Please make sure that jumper header inside device is connected according to image below. For other help please contact technical support.



Device is restarting continuously

During device restart are all segments of LCD display light up. When device is continuously restarting it commonly means that power adapter or USB cable is damaged. Please exchange cable and power adapter. Specification of USB cable and power adapter you find at chapter *Power supply*. If issue will not be resolved by another USB cable and power adapter, please contact technical support.

Measurement accuracy issue

Measurement accuracy issue of temperature and relative humidity are commonly caused by wrong position of probes or wrong measurement methodology. Please follow recommendations described at chapter *Operation in application areas*. In case of error is shown at measurement channel, please see recommendations at *Error codes at channels*.

Another group of issues are the random spikes at the measurement values. Common reason for such issues is a source of the electromagnetic interferences next to cable or device itself. Do not install device to the closer proximity than is 1 m from access point. Other reasons can be damaged insulation of cables. Please make sure that shielding of probes is properly connected as well.

Wi-Fi network connection problems

In case of troubles with connection into Wi-Fi network these steps may to be followed:

1. At first step please makes sure that are inserted proper Wi-Fi connection credentials like SSID, password and encryption type. Credentials can be tested with another Wi-Fi devices if needed. Personal security types WEP, WPA / WPA2, WPA2-PMF and WPA3 are supported. WPA2 Enterprise security is supported beginning firmware version 10.0.6.0.
2. Make sure that signal strength is sufficient. Move Wi-Fi sensor near to the used access point / router and repeat connection attempt.
3. Check setup of infrastructure access point or router. Wi-Fi sensors uses 2.4 GHz communication. Make sure that 2.4 GHz radio at access point is not disabled or access point is not at 5 GHz mode only. Access point used at Europe countries can use channels 1 – 13. Access point configured for usage in USA can use 1 – 11 channels only. Access points / routers can have configured restriction according to MAC addresses of the clients. Make sure that these restrictions are properly configured.

Connection problems to Wi-Fi with WPA2-EAP

For WPA2-EAP connection needs to be properly configured network and Wi-Fi sensor itself. From this reason contact your network administrator and ask for help with connectivity issue at first step.

For diagnose of issues with WPA2-EAP connections are logs from the authentication (RADIUS) server and diagnostic log from Wi-Fi sensor essential. Be aware that log from Wi-Fi sensor is deleted after device restart. From this reason is recommended to set backup Wi-Fi network with PSK password, for downloading diagnostic log, after unsuccessful connection into primary Wi-Fi (with EAP security). EAP connection troubleshooting checklist:

EAP mode	Checklist
EAP-TLS EAP-TTLS-TLS EAP-PEAP0-TLS EAP-PEAP1-TLS	1. Make sure that is selected SSID of proper network and WPA2-EAP security is selected. 2. Check that proper parameters are inserted at EAP security menu (e.g. EAP mode). Identity parameter needs to be set. 3. Make sure that proper CA file, Client certificate and Private key are uploaded. Files need to be uploaded at DER format. Client certificate and Private key are mandatory for these EAP modes. 4. Make sure that device have set proper time for testing expiration of CA file. Validation of CA file may to be deactivated at settings. 5. Make sure that proper EAP mode is enabled at RADIUS server. Make sure that TLS 1.0 is allowed at server.
EAP-TTLS-MSCHAPv2 EAP-TTLS-PSK EAP-PEAP0-MSCHAPv2 EAP-PEAP0-PSK EAP-PEAP1-PSK	1. Make sure that is selected SSID of proper network and WPA2-EAP security is selected. 2. Check that proper parameters are inserted at EAP security menu (e.g. EAP mode). Identity parameter and Password are mandatory. 3. Make sure that proper CA file is uploaded. CA file needs to be uploaded at DER format. 4. Make sure that device have set proper time for testing expiration of CA file. Validation of CA file may to be deactivated at settings. 5. Make sure that proper EAP mode is enabled at RADIUS server. Make sure that TLS 1.0 is allowed at server.

Wi-Fi signal strength issues

Proper function of Wi-Fi sensors depends on wireless connection into infrastructure access point or Wi-Fi router. In case of signal strength is not sufficient, device may not work properly, and there can be an issue with data transfers into acquisition system or sending warning emails. Signal strength depends on distance between device and access point and type of obstacles between device and access point. Attenuation depends on type of the material of obstacles and for 2.4 GHz is approximately following:

Material	**Signal lost**
Ceiling	20-30 dB
Concrete wall	10-15 dB
Brick wall	8 dB
Dry wall	4 dB

In case of connection issues, it should be check whether signal strength is sufficient. When signal strength is not sufficient, position of the device or position of infrastructure access point should be changed. Adding additional access point near to device may to be solution to coverage issues as well. Usage of Wi-Fi devices at places where is installed many access points with overlapping channels may to be problematic. In this case you should use least occupied Wi-Fi channel. Usage of such channel will minimise potential interferences.

Recommended signal strength (RSSI) is higher than -70 dBm (e.g. -55 dBm). Signal strength can be examined by following steps:

1. Connect device at client mode into infrastructure access point.
2. Place device to the location in which should be RSSI measured.
3. Press three times SET button.
4. Move away from proximity of the device. After 30 sec read RSSI value from the device LCD. In case RSSI value -99 is showing please wait longer. When value -99 is persistent, make sure that device is properly connected into Wi-Fi network.

Recommendations for operation and maintenance

Operation in application areas

Before putting the device into operation, it should be considered, if device is suitable for the intended purpose. Device settings should be determined together with intended use case. In case that 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 such applications in which the device malfunction could directly endanger life and health of humans and animals or affect function of the other equipment with life-sustaining functions. In the applications where device failure or malfunction could cause severe property damage it is recommended to provide the system with suitable and independent signalling equipment. This independent system will be able to evaluate such failure and prevent the above-mentioned material damage.

Device positioning. Follow the rules and principles mentioned in this manual. You should choose a place for the device position, where the negative influence caused by environment is as lowest as possible. When measurements in refrigerators, metal boxes, metal chambers are performed, it is recommended to place the device outside and leaving only the sensors and probes inside the measured environment. Such device position will improve operation reliability, improve Wi-Fi signal strength, and allow to use LCD display outside chamber.

Positioning of temperature sensors. These sensors should be placed in locations where sufficient air circulation is ensured and where the most critical location is supposed (according to the application requirements). To prevent heat conduction through the sensor cables from undesirable influencing the measurement value, the sensor must be properly inserted into the measured environment. If you follow the temperature distribution in an air-conditioned storehouse, do not place the sensor into the direct air stream generated by the air-conditioning unit. As a matter of fact, the temperature distribution in large-chamber refrigerators may be quite inhomogeneous, the temperature differences may to be up to 10 °C. Similar dispersion can be found inside deep-freezing boxes (e.g. in those used for blood preservation by deep freezing).

Positioning of humidity sensors. The positioning of humidity sensors depends on the application requirements as well. Humidity measurements in refrigerators without additional humidity stabilization can be very questionable. When the cooling is switched on/off, there may be significant changes in humidity in the range of tens of percent, even if the mean value is correct. Moisture condensation on the freezer walls is common.

Recommendations for calibration

Metrological verification is carried out according to the requirements of the application with intervals fixed by the user. Recommended calibration interval is stated at *Technical specification* for each device type. According to legal requirements at some applications, it may to be required, to be calibration performed by an independent accredited laboratory.

Recommendations for regular checks

It is recommended to check the measurement chain to which the instrument is incorporated at the regular base. Checking interval and inspection scope depend on the application and the user's internal regulations. Results of each regular check should be recorded. Found problems should be addressed accordingly according to their severity. In fixed installations following checks are recommended to be performed:

- Overall visual check of the device including cover integrity a condition of connectors.
- Check of the cabling and probes. It should be inspected cable connections, cable surface integrity and proper cable routing (e.g. installation of new high voltage or high current cables parallel to the device cabling).
- Check of all probes and sensing elements. Visual inspection for a water ingress into probes. Check location where are probes placed with respect to correct measurement conditions.
- Functionality check of whole measurement chain (checking of features utilized by the application):

  a) Check whether measured values are as expected. Measured values can be observed at device LCD display or device webpages.

  b) Check whether measured values are properly transferred into data acquisition platform like is ATAL Cloud or ATAL Database. Data are transmitted according to selected sensing interval.

  c) Check history data inside data acquisition platform for any unexpected data outage or alarm states.

  d) Functionality check of alarming feature(s). This should be done by changing the input quantity to give rise to an alarm. This alarm state should be signalised at device LCD display and alarm email should be delivered (if feature is used).

IT security advisories

IT security is an important aspect of deployment of any device connected into wired or wireless networks. It is not important from application and measurement device standpoint only, but overall integrity of network infrastructure itself. Any not adequately secured network device or IoT device may to compromise security of network. Following chapter contains list of the recommendation how to securely use Wi-Fi sensors.

Wi-Fi sensor security. Wi-Fi sensors have integrated advanced security features. There are three types of user accounts with predefined rules for each user type. These rules are described at chapter *Security*. Wi-Fi sensors are shipped without enabled security. It is strongly recommended to enable device security when device is used at the final deployment. It should be used as strongest password as possible. It should be at least 10 characters long together including numbers and multiple special characters. Never use same password for multiple devices or accounts.

Wi-Fi sensors can be switched from Wi-Fi client mode into AP mode using physical buttons at device. After switching into AP mode Wi-Fi sensor acts as an access point with capability connection up to four clients. By default, this AP mode is not protected, that means open Wi-Fi network. It is strongly recommended to enable WPA2 security with strong password as possible for AP mode.

Device does not use UPnP feature by any kind. List of ingress ports at device you find at *Appendix 6*. Firmware of Wi-Fi sensors is not written in Java language. No issues related to Java libraries are related to Wi-Fi sensor firmware.

Infrastructure security. At final deployment are Wi-Fi sensors connected to infrastructure access point or router with Wi-Fi capability. It is recommended to connect Wi-Fi sensors into separate Wi-Fi network with own SSID. This Wi-Fi network should have own separate VLAN tag as well. Please make sure that VLAN network is properly isolated at firewall settings. It is recommend using strong password together with WPA2 PMF or WPA3 security. Do not use WEP security.

Wi-Fi sensors have capability to connection into network with Enterprise security (WPA2-EAP). List of all supported EAP modes is available at chapter *Wi-Fi radio*. For some EAP modes is mandatory to upload Client certificate, Private Key and CA file into device. CA file is used for validation of authentication (RADIUS) server. Validation of RADIUS server may to be disabled at device settings. This approach is not recommended from the security standpoint.

Access from another location. In case of access from another location (outside local network) to Wi-Fi sensor is required, it is recommended to use VPN. Do not expose device directly into internet by direct port forwarding at the gateway or NAT. This approach can prevent potential direct attack to the device.

Firmware update. It is recommended to use latest firmware inside device. Firmware file should be obtained from official sources like a manufacturer webpages or direct contact with technical support only. Never use firmware from unofficial sources. Such firmware may to affect proper function of device or compromise security.

Decommission. In case of device decommission, sold or moving to another location, be aware, that device may to contain confidential information. *Factory defaults procedure* is a recommended approach to avoid such leak. If WPA2-EAP security with uploaded certificates is used, these certificates should be deleted. This can be done using WifiSensorUtility. Alternative way can be uploading dummy certificates via webpages.

Device backup configuration file. Device setup can be saved into file for future restore. Be aware that backup file contains confidential data like a password for WLAN. Backup files are not encrypted.

Device security support. Technical support may to be contacted in can any concerns or questions related to device security.

Firmware update

Device firmware can be updated via web pages – Advanced options / Service menu. In case of security is enabled, administrator permissions are required. Firmware downgrade is not supported via web pages.

Latest firmware version can be obtained from manufacturer webpages or from technical support. Before starting update, please read update instruction carefully.

Technical support and service

Technical support is provided by the distributor of device. Contact for distributor is stated at warranty card included with product. It is recommended to send diagnostic file downloaded from device when you send support request. Diagnostic file can be downloaded at menu Advanced options / Service. Diagnostic file contains important technical information about function of device. If may to contain confidential information like an IP address or SSID. It does not contain passwords.

Warning. Do not try to repair the device by yourself. Any repairs may be carried out by suitably instructed service personnel only. Improper installation, operation, or intervention into the device itself may lead to loss of warranty. Manufacturer reserves rights to deny the free of charge repairs of such damaged devices during warranty period.

Technical specification

Power supply

Supply voltage:

5.0 V to 5.4 V DC

Consumption:

Typ. 150 mA at high performance mode (max. 500 mA)

Recommended power supply adapter:

ATRU-AC04 (Sunny SYS 1561-1105)

Recommended cable:

ATRU-AC01U (USB A to USB-C length 1 m)

Connector:

USB-C

General parameters

Measurement interval:

1 sec (15 sec for a CO_2 concentration measurement)

LCD display switching interval:

4 sec

Realtime clock:

With internal backup battery, with deviation max. 200 ppm ±5 ppm/year at temperature 23 °C ±10 °C

Wi-Fi radio

Frequency:

2.4 GHz

Standard:

IEEE 802.11 b/g/n

Max. transmit power:

18 dBm

Channel with:

20 MHz

Contains FCC ID:

Z64-CC3220MOD

Wi-Fi security:

Open, WEP, WPA / WPA2, WPA2-PMF, WPA3

WPA2 Enterprise (IEEE 802.1X)

Supported WPA2 enterprise methods:

EAP-TLS *

EAP-TTLS-TLS *

EAP-TTLS-MSCHAPv2 *

EAP-TTLS-PSK *

EAP-PEAP0-TLS *

EAP-PEAP0-MSCHAPv2 *

EAP-PEAP0-PSK *

EAP-PEAP1-TLS *

EAP-PEAP1-PSK *

EAP-FAST-AUTH-PROVISIONING *

EAP-FAST-UNAUTH-PROVISIONING *

EAP-FAST-NO-PROVISIONING *

* TLS 1.0 is supported only (TLS 1.1, TLS 1.2 is not supported)

Wi-Fi modes:

Client mode

Access point mode (up to four clients connected simultaneously)

Antenna:

Standard device:

- External antenna not detachable

Communication protocols

Supported protocols:

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

HTTP(S), SMTP, Modbus TCP, SNMP

Webserver:

HTTP(S) 1.1 server, HTTPS with TLS version 1.2

Up to three connected clients to webserver simultaneously

Port forwarding from 80 to TCP port 81 (HTTP) or 443 (HTTPS)

Supported browsers: Mozilla Firefox, Google Chrome, Microsoft Edge. Internet Explorer is not supported.

SMTP – Email:

Supported authentication – AUTH LOGIN

Supported encryption – TLS, STARTTLS

OAuth 1.0 or 2.0 is not supported

Cloud protocol:

HTTP(S) POST with JSON data

HTTP(S) 1.1 client, HTTPS with TLS version 1.2

Non-volatile memory for up to 2240 sets of values

Modbus TCP protocol:

Up to two connected clients to server simultaneously

JSON and XML via http server:

Current readings via HTTP GET at port 80

SNMP protocol:

Supported versions - SNMPv1, SNMPv2c, SNMPv3

Partial support for MIB-II table (RFC1213) – System node

SNMPv3 authentication - MD5, SHA

SNMPv3 privacy - DES, AES128

SNMPv3 is operable after 30 sec from device start-up

SNMP Traps are not supported

Parameters of inputs

AWP-T

Measured values:

Temperature from a probe which is part of shipment

Range:

-30 °C to +60 °C

Accuracy:

±0.4 °C

Response time:

t90 < 1 min (temperature step 20 °C, air flow 1 m/s)

Resolution:

0.1 °C (ADC resolution 16 bit)

Recommended calibration interval:

2 years

AWP-T1P

Measured values:

Temperature from external probe Pt1000

Range:

-90 °C to +260 °C (sensor Pt1000/3850 ppm)
Measurement current ~250 uA

Input accuracy (without probes):

±0.2 °C the at range below +100 °C
±0.2 % from measured value at range above +100 °C

Overall measurement accuracy of device with connected probe is composed from accuracy of input and accuracy of used probe.

Probe connection:

Two wire connection with capability for deviation compensation due to resistance of uses cable. Connection is done via CINCH (RCA) connector. Connection is described at *Appendix 2*.

Recommended length of probe Pt1000 is up to 15 m. Length of probe cannot exceed 30 m. It is strongly recommended to use shielded cable of probe only.

Response time:

According to used probe

Resolution:

0.1 °C (ADC resolution 16 bit)

Recommended calibration interval:

2 years

AWP-T4P

Measured values:

4x Temperature from external probes Pt1000

Range:

-90 °C to +260 °C (sensor Pt1000/3850 ppm)

Measurement current ~250uA

Input accuracy (without probes):

±0.2 °C the at range below +100 °C

±0.2 % from measured value at range above +100 °C

Overall measurement accuracy of device with connected probe is composed from accuracy of input and accuracy of used probe.

Probe connection:

Two wire connection with capability for deviation compensation due to resistance of uses cable. Connection is done via CINCH (RCA) connector. Connection is described at *Appendix 2*.

Recommended length of probe Pt1000 is up to 15 m. Length of probe cannot exceed 30 m. It is strongly recommended to use shielded cable of probe.

Response time:

According to used probe

Resolution:

0.1 °C (ADC resolution 16 bit)

Recommended calibration interval:

2 years

AWP-TR

Measured values:

Temperature and relative humidity from a probe, which is part of shipment. Other humidity quantities are calculated from the measured temperature and humidity.

Range:

Temperature: -30 °C to +60 °C

Relative humidity: 0 %RH to 95 %RH without condensation

Dew point temperature: -60 °C to +60 °C

Accuracy:

Temperature: ±0.4 °C

Relative humidity:

- sensor accuracy: ±1.8 %RH at temperature 23 °C and humidity range 0 %RH to 90 %RH

- hysteresis: < ±1.0 %RH
- non-linearity: < ±1.0 %RH

Dew point temperature:

±1.5 °C at ambient temperature T < 25 °C and RH > 30 %RH. Please see chart at *Appendix 1* for detail information. Detail accuracy of other humidity quantities is stated there as well.

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

Temperature: t90 < 1 min for temperature step 20 °C

Relative humidity: t90 < 6 sec for a 60 %RH step at constant T

Resolution:

Temperature including dew point temperature: 0.1 °C

Relative humidity: 0.1 %RH

Recommended calibration interval:

1 year

AWP-TR1D

Measured values:

Temperature and relative humidity from an external probe TRHD-xxxE. Other humidity quantities are calculated from the measured temperature and humidity.

Range, accuracy, and response time:

See manual for a particular TRHD-xxxE probe

Probe connection:

TRHD-xxxE probe is connected by 4-pin M8 ELKA 4008V connector. Connection of pins is described at *Appendix 3*.

Maximum length of cable for TRHD-xxxE probe cannot exceed 15 m.

Resolution:

Temperature including dew point temperature: 0.1 °C

Relative humidity: 0.1 %RH

Recommended calibration interval:

1 year (according to used probe)

AWP-TR2D

Measured values:

2x Temperature and relative humidity from external probes TRHD-xxxE. Other humidity quantities are calculated from the measured temperature and humidity.

Range, accuracy, and response time:

See manual for a particular TRHD-xxxE probe(s)

Probe connection:

TRHD-xxxE probe is connected by 4-pin M8 ELKA 4008V connector. Connection of pins is described at *Appendix 3*.

Maximum length of cable for TRHD-xxxE probe cannot exceed 15 m.

Resolution:

Temperature including dew point temperature: 0.1 °C

Relative humidity: 0.1 %RH

Recommended calibration interval:

1 year (according to used probe)

AWP-TR1D-T3P

Measured values:

Temperature and relative humidity from an external probe TRHD-xxxE and up to three temperatures from external probes Pt1000. Other humidity quantities are calculated from the temperature and humidity measured by the TRHD-xxxE probe.

TRHD-xxxE probe range, accuracy, and response time:

See manual for a particular TRHD-xxxE probe

TRHD-xxxE probe connection:

TRHD-xxxE probe is connected by 4-pin M8 ELKA 4008V connector. Connection of pins is described at *Appendix 3*.

Maximum length of cable for TRHD-xxxE probe cannot exceed 15 m.

Pt1000 probe(s) range:

-90 °C to +260 °C (sensor Pt1000/3850 ppm)

Measurement current ~250uA

Pt1000 input accuracy (without probes):

±0.2 °C the at range below +100 °C

±0.2 % from measured value at range above +100 °C

Overall measurement accuracy of device with connected probe is composed from accuracy of input and accuracy of used probe.

Pt1000 probe(s) response time:

According used probe

Pt1000 probe connection:

Two wire connection with capability for deviation compensation due to resistance of uses cable. Connection is done via CINCH (RCA) connector. Connection is described at *Appendix 2*.

Recommended length of probe Pt1000 is up to 15 m. Length of probe cannot exceed 30 m. It is strongly recommended to use shielded cable of probe.

Resolution:

Temperature including dew point temperature: 0.1 °C

Relative humidity: 0.1 %RH

Recommended calibration interval:

1 year (according to used probe)

AWP-TRCP

Measured values:

Temperature and relative humidity from a probe, which is part of shipment. CO_2 concentration and barometric pressure from internal sensors. Other humidity quantities are calculated from the measured temperature and humidity.

Range:

Temperature: -30 °C to +60 °C

Relative humidity: 0 %RH to 95 %RH without condensation

Barometric pressure: 700 hPa to 1100 hPa

CO_2 concentration: 0 to 5000 ppm (optionally 0 to 10000 ppm)

Dew point temperature: -60 °C to +60 °C

Accuracy:

Temperature: ±0.4 °C

Relative humidity:

- sensor accuracy: ±1.8 %RH at temperature 23 °C and humidity range 0 %RH to 90 %RH
- hysteresis: < ±1.0 %RH
- non-linearity: < ±1.0 %RH

Barometric pressure: ±1.3 hPa at temperature 23 °C

CO_2 concentration in the air:

- 50 + 0.03 * measured value [ppm CO_2 at 23 °C and 1013 hPa]
- temperature dependency in range -20 to 45 °C is typ. ± (1 + measured value / 1000) [ppm CO_2/°C]

Dew point temperature:

±1.5 °C at ambient temperature T < 25 °C and RH > 30 %RH. Please see chart at *Appendix 1* for detail information. Detail accuracy of other humidity quantities is stated there as well.

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

Temperature: t90 < 1 min for temperature step 20 °C

Relative humidity: t90 < 6 sec for a 60 %RH step at constant T

Barometric pressure: t90 < 44 sec

CO_2 concentration: t90 < 2 min

Resolution:

Temperature including dew point temperature: 0.1 °C

Relative humidity: 0.1 %RH

Barometric pressure: 1 hPa

CO_2 concentration: 1 ppm

Recommended calibration interval:

1 year

AWP-C

Measured values:

CO_2 concentration of air

Range:

0 ppm to 5000 ppm (range 0 ppm to 10000 ppm as option)

Accuracy:

- 50 + 0.03 * measured value [ppm CO_2 at 23 °C and 1013 hPa]
- temperature dependency in range -20 to 45 °C is typ. ± (1 + measured value / 1000) [ppm CO_2/°C]

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

t90 < 2 min

Resolution:

1 ppm

Recommended calibration interval:

5 years

Measured values:

Temperature and relative humidity from a probe, which is part of shipment. Barometric pressure from internal sensor. Other humidity quantities are calculated from the measured temperature and humidity.

Range:

Temperature: -30 °C to +60 °C

Relative humidity: 0 %RH to 95 %RH without condensation

Barometric pressure: 600 hPa to 1100 hPa

Dew point temperature: -60 °C to +60 °C

Accuracy:

Temperature: ±0.4 °C

Relative humidity:

- sensor accuracy: ±1.8 %RH at temperature 23 °C and humidity range 0 %RH to 90 %RH
- hysteresis: < ±1.0 %RH
- non-linearity: < ±1.0 %RH

Barometric pressure: ±1.3 hPa at temperature 23 °C

Dew point temperature:

±1.5 °C at ambient temperature T < 25 °C and RH > 30 %RH. Please see chart at *Appendix 1* for detail information. Detail accuracy of other humidity quantities is stated there as well.

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

Temperature: t90 < 1 min for temperature step 20 °C

Relative humidity: t90 < 6 sec for a 60 %RH step at constant T

Barometric pressure: t90 < 44 sec

Resolution:

Temperature including dew point temperature: 0.1 °C

Relative humidity: 0.1 %RH

Barometric pressure: 1 hPa

Recommended calibration interval:

1 year

Operating and storage conditions

Operating temperature:

-30 to +60 °C (LCD display visibility -10 to +60 °C)

Operating humidity:

0 %RH to 95 %RH without condensation

Operating pressure:

600 to 1100 hPa (for AWP-TRCP, AWP-C range is 700 to 1000 hPa)

Operating environment:

chemically non-aggressive

Storage temperature:

-30 to +60 °C

Storage humidity:

5 to 90 %RH

Mechanical properties

Dimensions (h x w x d):

93 x 81 x 32 mm without connected probes and cables

Mass:

~ 120 g

Case material:

Polycarbonate LEXAN™ EXL1434T resin

Ingress protection:

IP30

End of operation

In case of device decommission be aware that device may to contain confidential information (e.g. passwords). From this reason is recommended *do Factory defaults procedure* before putting device into electronic waste. If WPA2-EAP security with uploaded certificates is used, these certificates should be deleted. This can be done by the WifiSensorUtility software.

Disconnect power supply from the device and dispose device as an electronic waste. The device contains integrated primary lithium battery with capacity 48 mAh.

Declaration of Conformity

The device is in accordance with directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address www.atal.nl

Appendix

Appendix 1: Accuracy of dew point and other humidity quantities

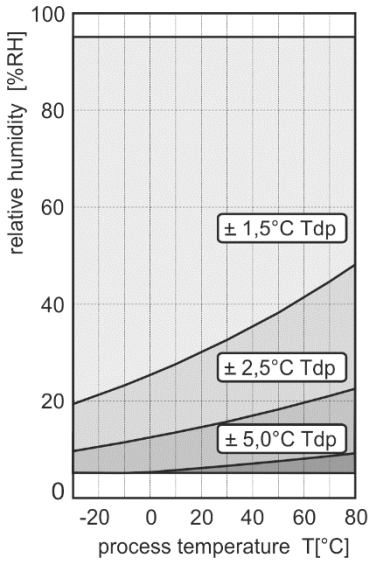
Dew point temperature:

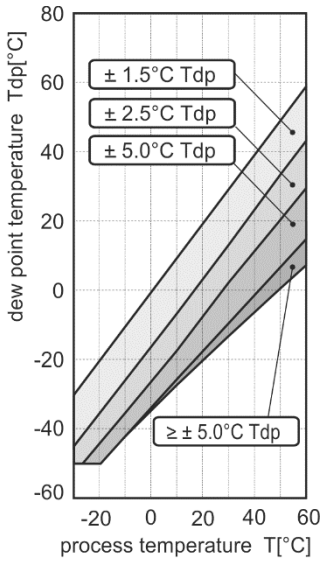
Accuracy:

±1.5 °C at ambient temperature T < 25 °C and RH > 30 %RH

Range:

-50 °C to +60 °C





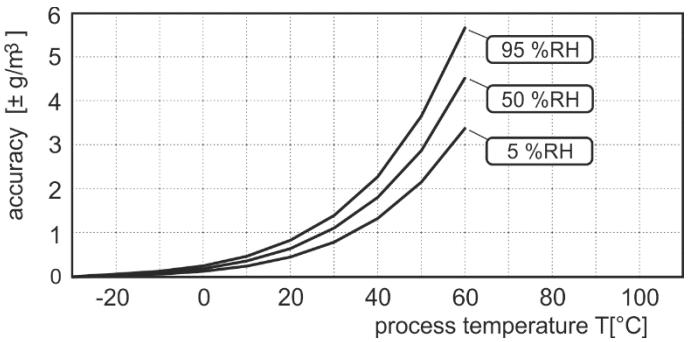
Absolute humidity

Accuracy:

±1.5 g/m^3 at ambient temperature T < 25 °C

Range:

0 g/m^3 to 130 g/m^3



Specific humidity *

Accuracy:

± 2 g/kg at ambient temperature T < 35 °C

Range:

0 g/kg to 130 g/kg

Mixing ratio *

Accuracy:

± 2 g/kg at ambient temperature T < 35°C

Range:

0 g/kg to 150 g/kg

Specific enthalpy *

Accuracy:

± 3 kJ/kg at ambient temperature T < 25°C

Range:

0 kJ/kg to 450 kJ/kg

Humidex

Accuracy:

± 2.0 ºC

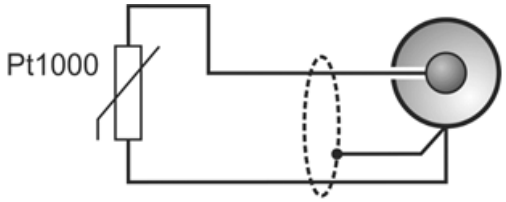
Range:

Index is relevant when temperature is in the range of 21°C to 43°C and outdoor humidity is 20 %RH or above

** Computed value of the humidity quantity depends on barometric pressure. At devices which are not equipped by the internal atmospheric pressure sensor is constant value of the barometric pressure configured at the settings. Default value is 1013 hPa.*

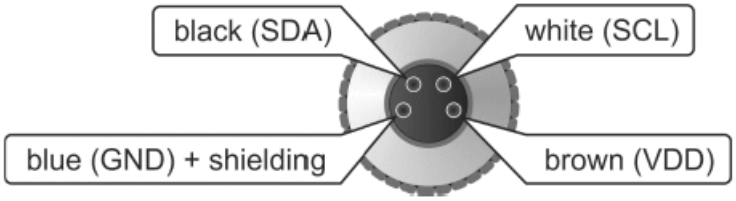
Appendix 2: Connection of Pt1000 probe(s) connector

Connectors for Pt1000 probes uses CINCH (RCA) connector. Connection of for AWP-T1P, AWP-T4P, AWP-TR1D-T3P Pt1000 probe is shown below.



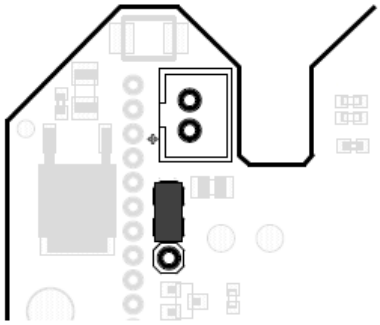
Appendix 3: Connection of the TRHD-xxxE probe(s) connector

TRHD-xxxE probe is connected by 4-pin M8 ELKA 4008V connector. Colour coding of wire connection for AWP-TR1D, AWP-TR2D, AWP-TR1D-T3P is shown at image below.



Appendix 4: Optional power 5V via connector

Wi-Fi sensors have capability to be powered via internal connector by +5V DC instead from USB C connector. For more details, how can be device connected, please contact technical support.



Appendix 5: Acoustic and optical LED operation diagram

Image below described operation diagram of acoustic system at Wi-Fi sensors. Device acoustic can be activated from two different sources. It can be activated from alarms on channel and from system alarms. To be device acoustic functional it needs to be globally enabled and enabled alarm source as well. Mute for device acoustic can be done locally via button SET at device or from web pages (software). Both ways for mute are independently configurable.

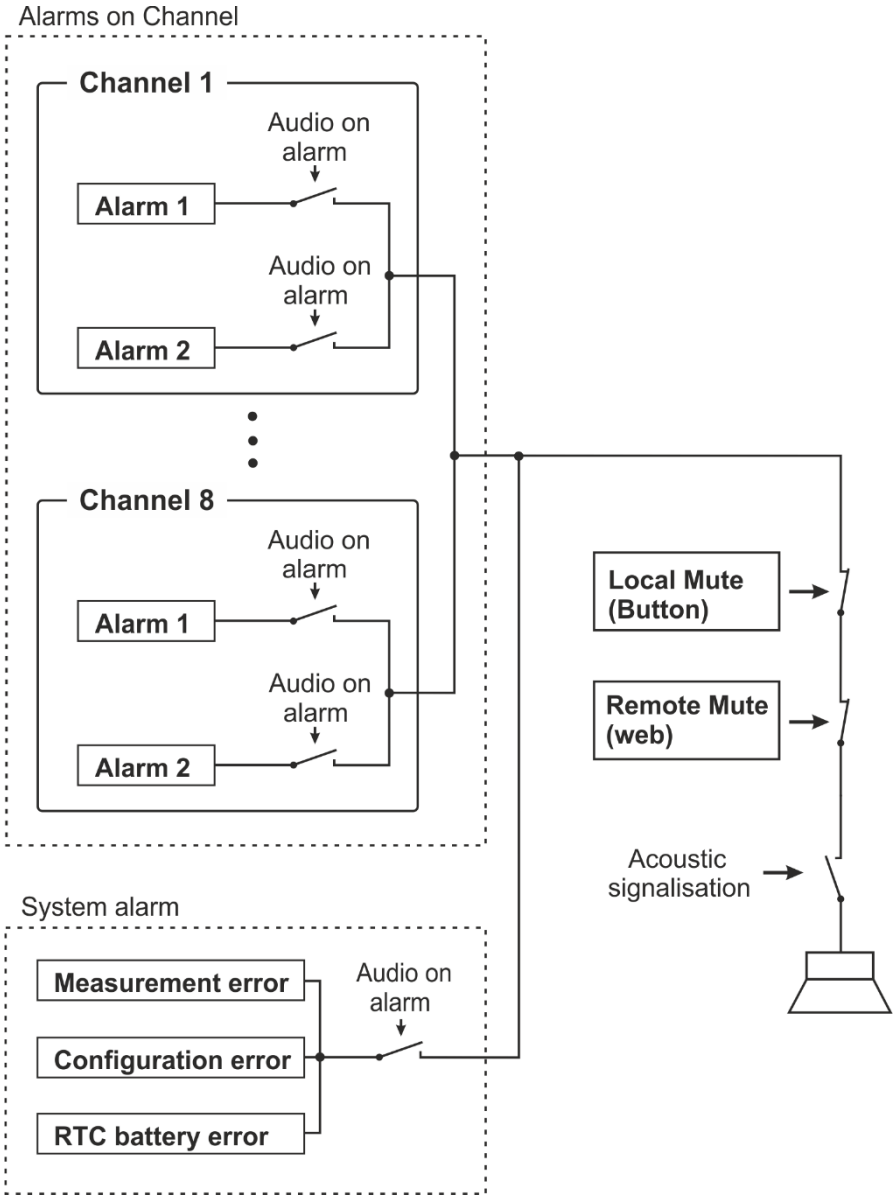
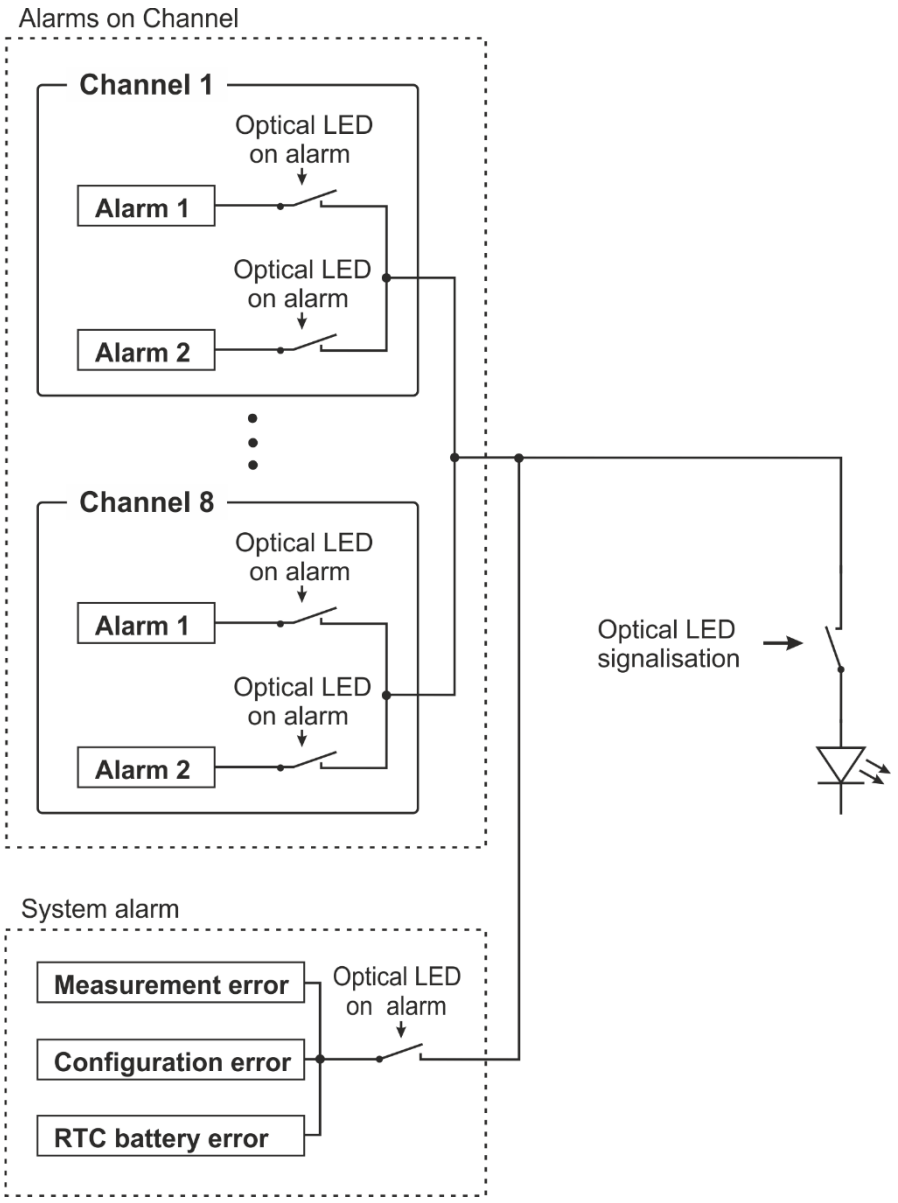


Image below described operation diagram of optical LED signalisation subsystem at Wi-Fi sensors. LED signalisation can be activated from two different sources. It can be activated from alarms on channel and from system alarms. To be device LED signalisation functional it needs to be globally enabled and enabled alarm source as well. Mute feature for LED signalisation is not available.



Appendix 6: List of used ports

This table show list of used ingress ports of Wi-Fi sensors.

Protocol	Port number	Usage
TCP	80	HTTP webserver redirection port. Used for get current values via values.xml and values.json as well.
TCP	81	HTTP webserver
TCP	443	HTTPS webserver when device security is enabled
TCP	502	Modbus TCP port (default port)
TCP	10001	Communication with software WifiSensorUtility (default port)
UDP	5353	mDNS discovery protocol
UDP	30718	Discovery protocol
UDP	161	SNMP protocol

Note: ICMP Echo (ping) is enabled at Wi-Fi sensors.

Appendix 7: Tests with 3rd party SMTP services

Wi-Fi sensors with firmware version 10.0.6.0 were successfully validated with following 3rd party email services. This list is valid at date of creation 2022-06-27. Not all services may to be available at all countries. Because these email services are from 3rd party, we do not guarantee proper function with Wi-Fi sensors or compatibility by any kind.

Service	SMTP server address	Port	Encryption	Note
Gmail	smtp.gmail.com	465	TLS	Note 1
		587	STARTTLS	
Outlook.com	smtp-mail.outlook.com	587	STARTTLS	Note 2
AOL Mail	smtp.aol.com	465	TLS	Note 3
		587	STARTTLS	
Yahoo! Mail	smtp.mail.yahoo.com	465	TLS	Note 4
		587	STARTTLS	
GMX.com	mail.gmx.com	465	TLS	Note 5
		587	STARTTLS	
Seznam.cz	smtp.seznam.cz	25	No	
		465	TLS	
		587	STARTTLS	
Centrum.cz	smtp.centrum.cz	25	No	
		465	TLS	
		587	STARTTLS	

Note 1: For support of TLS of STARTTLS encryption with Gmail SMTP server, is mandatory to enable 2-Step Verification. When this verification is enabled, it can be set App password used for the SMTP authentication.

Note 2: In case of Outlook.com is used as part of the corporate Office 365, this feature can be disabled by administrator.

Note 3: For sending emails via AOL SMTP server, it needs to be enabled App Password (Options / Account Info / Account Security / Other ways to sign in / Generate and manage app passwords).

Note 4: For sending emails via Yahoo SMTP server, it needs to be enabled App Password (Account Info / Account Security / Other ways to sign in / Generate and manage app passwords).

Note 5: For sending emails via GMX SMTP server, feature need to be enabled at E-mail settings (E-mail / Settings / POP&IMAP / Enable access to this account via POP3 and IMAP).

Appendix 8: List of available device options

Following options for Wi-Fi sensors are available and can be ordered with new devices.

Option	Order code
CO_2 concentration range 0 to 10000 ppm instead standard range 0 to 5000 ppm	AWP-C / 10000 ppm, AWP-TRCP / 10000 ppm

Appendix 9: Enterprise security tested with FreeRADIUS

Table below contains list of EAP methods validated with FreeRADIUS server version 3.0.21.

EAP Method	CA file	Client certificate	Note
EAP-TLS	yes	yes	Note 1, Note 2, Note 3
EAP-TTLS-TLS	yes	yes	
EAP-TTLS-MSCHAPv2	yes	no	Note 1, Note 3, Note 4
EAP-PEAP0-MSCHAPv2	yes	no	
EAP-PEAP0-PSK	yes	no	
EAP-FAST-AUTH-PROVISIONING	no	no	Note 1, Note 5

Note 1: Support for TLS 1.0 need to be enabled at FreeRADIUS server (by default is enabled TLS 1.1 and TLS 1.2). TLS 1.0 can be enabled via EAP configuration file (/mods-enabled/eap) and option tls_min_version = "1.0".

Note 2: Client is authenticated at server using the Client certificate and Private key. Client certificate and Private key need to be uploaded into Wi-Fi sensor at DER format. Files at PEM format or p12 are not supported. OpenSSL can be used for conversion between file formats. Identity for EAP-TLS methods needs to be set. In case of Identity string is not provided by network administrator, it can be used any string. Password is not mandatory.

Note 3: Wi-Fi sensors validate authentication server against CA file. This file needs to be uploaded into Wi-Fi sensor at DER format. CA file is expected for all EAP methods with exception EAP-FAST. Expiration of CA file is checked against internal time. Make sure that device have set proper RTC time. CA validation may to be disabled at device settings. This approach is not recommended from the security standpoint.

Note 4: Methods where Certificate and Private key inside device are not used. Identity string and Password need to be set for authentication against RADIUS server.

Note 5: Cisco EAP-FAST methods are used without Certificate, Private key, and CA file. Identity string and Password need to be set.

Revision history

Document version	Date	Note
IE-WFS-AWP-01	February 2021	Initial document version for firmware version 10.0.2.0.
IE-WFS-AWP-02	April 2021	Revision of chapter “Provisioning and first setup” Added new troubleshooting chapter – “Wi-Fi network connection problems” Added new appendix – “Tests with 3rd party SMTP services” Added information about meaning of IP address 0.0.0.0 after press of MODE button Correction of typos
IE-WFS-AWP-03	May 2021	Added new appendix – “List of available device options” Correction of typos
IE-WFS-AWP-04	July 2021	Changes related to firmware version 10.0.2.2: Increased size of memory (cache) from 960 to 2240 records, new asynchronous message when device connect into Wi-Fi, added DHCP hostname at the advanced networks menu. Correction of typos
IE-WFS-AWP-05	October 2021	Changes related to firmware version 10.0.3.0: Added description of “MEMORY” symbol on LCD, description of backup WLAN. New image at troubleshooting section New appendix: Optional power 5V via connector New appendix: Structure of settings menu Graphic improvements of manual Correction of typos
IE-WFS-AWP-06	January 2022	Changes related to firmware version 10.0.4.0: Added support for SNMP protocol Added capability for save device setup into backup file New information added into chapter “IT security advisories”
IE-WFS-AWP-07	February 2022	New support for SNMPv3 at firmware version 10.0.5.0.

IE-WFS-AWP-08	May 2022	New support for EAP security at firmware version 10.0.6.0. Updated Appendix 7, new Appendix 9 Correction of typos
IE-WFS-AWP-09	June 2022	Updated Appendix 7 with the information about Gmail SMTP server. Correction of typos at specification (communication protocols, AWP-TR specification) and declaration of conformity chapter.
IE-WFS-AWP-10	August 2022	Changed description of the TLS 1.0 limitation for WPA2-EAP.

Note: Page numbers may to differ between document versions.