



BE WAVE Hybrid system control panel

HYBRID 128 Plus

HYBRID 128

Firmware version 1.4

EN



hybrid_en 05/26

IMPORTANT

The security alarm system should be installed by qualified personnel.

Prior to installation, please read carefully this manual in order to avoid mistakes that can lead to malfunction or even damage to the equipment.

Disconnect power before making any electrical connections.

Changes, modifications or repairs not authorized by the manufacturer shall void your rights under the warranty.

The symbols on the rating plate of the device indicate:

 The device meets the requirements of the applicable EU directives.

 The device must not be disposed of with other municipal waste. It should be disposed of in accordance with the existing rules for environment protection (the device was placed on the market after 13 August 2005).

 Alternating current (AC).

 Direct current (DC).

SATEL aims to continually improve the quality of its products, which may result in changes in their technical specifications and software. Current information about the changes being introduced is available on our website.

Please visit us at:
<https://support.satel.pl>

**Hereby, SATEL sp. z o.o. declares that the radio equipment type HYBRID 128 Plus / HYBRID 128 is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address:
www.satel.pl/ce**

Signs in this manual

 Caution – information on the safety of users, devices, etc.

 Note – suggestion or additional information.

CONTENTS

1. Introduction	4
2. Features	4
Devices in the system	4
System division	4
Hardwired zones	4
Hardwired outputs	5
Communication bus	5
Users	5
Be Wave app	5
BE WAVE Soft program	5
Arming	5
Scenes and routines	5
Schedules	5
Event log	6
Messaging	6
Reporting	6
Firmware update	6
Mainboard	6
3. Supported devices	6
3.1 Bus devices	7
3.1.1 Detectors	7
3.1.2 Expanders	8
3.1.3 LCD keypads	8
3.1.4 Keypads	8
3.1.5 Proximity card readers	8
3.2 Wireless devices	8
3.2.1 Detectors	8
3.2.2 Actuators	9
3.2.3 Sirens	10
3.2.4 Keypad	10
3.2.5 Keyfobs and buttons	10
3.2.6 Expanders	10
3.2.7 Repeater	10
3.3 Virtual IP devices	10
4. Installation	11
4.1 Installation plan	11
4.2 Estimation of the system current consumption	11
4.3 Cabling	11
4.4 Mounting the control panel	11
4.4.1 Tips for installation	11
4.4.2 Description of the mainboard	12
Description of terminals	13
4.5 Connecting the bus devices	13
4.6 Connecting the detectors	14
4.6.1 End-of-line resistors	15
4.7 Connecting the LAN	15
4.8 Installing the SIM cards [HYBRID 128 Plus]	15
4.9 Connecting the power and starting the control panel	16

4.10	Connecting the sirens.....	16
4.11	Installing wireless devices	16
5.	Managing, programming and controlling the system	16
5.1	Be Wave app.....	16
5.1.1	Description of the Be Wave app home screen	17
5.1.2	Changing the app language	17
5.1.3	Changing the app theme	18
5.2	BE WAVE Soft program	18
5.2.1	Description of the BE WAVE Soft program home screen	18
5.2.2	Changing the program language	19
5.2.3	Changing the program theme.....	19
5.3	Adding the control panel (site).....	19
5.3.1	Adding the control panel in the Be Wave app.....	19
	Adding the first control panel (site)	19
	Adding another control panel (site).....	24
5.3.2	Adding the control panel in the BE WAVE Soft program	25
	Adding the first control panel (site)	25
	Adding another control panel (site).....	29
5.4	Adding mainboard zones and outputs to the system.....	30
5.4.1	Adding mainboard zones and outputs in the Be Wave app.....	31
5.4.2	Adding the mainboard zones and outputs in the BE WAVE Soft app.....	34
5.5	Adding a bus device to the system.....	39
5.5.1	Adding a bus device in the Be Wave app.....	39
5.5.2	Adding a bus device in the BE WAVE Soft program	42
5.6	Adding a wireless device to the system.....	47
5.6.1	Adding a wireless device in the Be Wave app.....	48
5.6.2	Adding a wireless device in the BE WAVE Soft program	51
5.7	Adding a virtual IP device to the system.....	56
5.7.1	Adding a virtual IP device in the Be Wave app.....	56
5.7.2	Adding a virtual IP device in the BE WAVE Soft program	58
5.8	Removing the device from the system	61
5.8.1	Deleting a device in the Be Wave app.....	61
5.8.2	Deleting a device in the BE WAVE Soft program	61
5.9	Description of settings	62
5.9.1	Device settings	62
5.9.2	Additional device settings	64
	Settings of devices with built-in temperature sensor	64
	Hardwired detectors and zones settings	64
	Hardwired zones settings	65
	<i>Alarm</i> output settings.....	65
	<i>BI switch</i> output settings.....	65
	<i>MONO switch</i> output settings.....	65
	Thermostat settings.....	66
	Detector with lighting feature settings.....	66
	ADC-200 dimmer settings	66
	ARC-200 controller settings	66
	ARSC-200 controller settings	66
	ASW-200 smart plug settings.....	67
5.9.3	Alarm source	67
5.9.4	IP device settings	67

5.9.5	Communication settings	68
	SIM1 / SIM2	68
	LAN	68
	Wi-Fi	68
5.9.6	Advanced settings	69
5.9.7	Reporting	69
	Station 1 / Station 2	70
5.9.8	Email settings	72
5.9.9	Encryption settings for the MIFARE cards	72
5.10	Adding a user	73
	5.10.1 Adding a user in the Be Wave app	73
	5.10.2 Adding a user in the BE WAVE Soft program	76
	5.10.3 User with access to the entire site	78
	User privileges	78
	5.10.4 User with access to a part of the site	79
5.11	Enabling SMS / CLIP notifications [HYBRID 128 Plus]	79
	5.11.1 Enabling SMS / CLIP notifications in the Be Wave app	79
	5.11.2 Enabling SMS / CLIP notifications in the BE WAVE Soft program	79
5.12	Enabling email notifications	79
	5.12.1 Enabling email notifications in the Be Wave app	79
	5.12.2 Enabling email notifications in the BE WAVE Soft program	80
6.	Testing	80
	6.1 Enabling the diagnostic mode	80
	6.1.1 Enabling the diagnostic mode in the Be Wave app	80
	6.1.2 Enabling the diagnostic mode in the BE WAVE Soft program	81
	6.2 Disabling the diagnostic mode	81
	6.2.1 Disabling the diagnostic mode in the Be Wave app	81
	6.2.2 Disabling the diagnostic mode in the BE WAVE Soft program	81
7.	Maintenance	81
	7.1 Firmware update	81
	7.1.1 Starting the update in the Be Wave app	81
	7.1.2 Starting the update in the BE WAVE Soft program	81
	7.2 Importing system settings from SD card	81
	7.2.1 Importing system settings in the Be Wave app	81
	7.2.2 Importing system settings in the BE WAVE Soft program	82
	7.3 Exporting system settings to SD card	82
	7.3.1 Exporting system settings in the Be Wave app	82
	7.3.2 Exporting system settings in the BE WAVE Soft program	82
	7.4 Restoring the control panel factory settings	82
	7.4.1 Restoring the factory settings from the Be Wave app	82
	7.4.2 Restoring the factory settings from the BE WAVE Soft program	82
	7.4.3 Hardware factory restore	82
8.	Specifications	83

1. Introduction

This manual will help you install the HYBRID 128 Plus / HYBRID 128 control panel. The BE WAVE Hybrid system combines burglary, fire, and other random event protection functions with home automation functions. You can manage and control it from the Be Wave mobile app or the BE WAVE Soft program.

The manual applies to the control panel with electronics version 1.5.

The HYBRID 128 Plus / HYBRID 128 control panel complies with the following standards: EN 50131-1 Grade 2, EN 50131-3 Grade 2, EN 50131-6 Grade 2, EN 50130-4, EN 50130-5 Class II.



The performance of extra features such as SMS, CLIP, push or email notifications depends on external networks and third-party services – including telecommunications providers – which are beyond our control. These services may occasionally experience disruptions that affect the delivery of notifications. The proper functioning of these features may also depend on the settings of your devices. While we do our best to minimize the risk of such issues, we cannot accept responsibility for the uninterrupted and error-free operation of features that rely on third-party services, particularly telecommunications networks or from the actions of device manufacturers.

The alarm system cannot prevent burglary, hold-up or fire from happening, but in emergency situation it will allow you to take steps to minimize the potential damage (it will signal an alarm using visual or audible signaling, notify the system users or the appropriate authorities of the alarm etc.). As a result, it may deter potential intruders.

2. Features

Devices in the system

- Support for up to 128 hardwired, wireless, and virtual IP devices.
- Hardwired devices:
 - devices connected to the system's zones and outputs,
 - bus devices connected to the RS communication bus (up to 32 physical devices).
- Wireless devices:
 - operation in the 868 MHz frequency band,
 - AES encrypted two-way radio communication,
 - transmission channel diversity – 4 channels for automatic selection of the one that will enable transmission without interference with other signals,
 - additional transmission channel to receive pictures from the APCAM-200 (Motion Detector Cam) and AOCAM-210 (Outdoor Motion Detector Cam) detectors.
- Virtual IP devices:
 - IP zones (receiving HTTP notifications),
 - IP outputs (sending HTTP notifications).

System division

- Capability to assign devices to 50 rooms.

Hardwired zones

- 4 zones on the control panel mainboard.
- Capability to increase the number of hardwired zones using expanders.

- Support for NO and NC detectors, as well as roller shutter and shock detectors.
- Support for Single EOL, Double EOL and Triple EOL configuration.
- Programmable value of end-of-line resistors.

Hardwired outputs

- 4 outputs on the control panel mainboard.
- Capability to increase the number of hardwired outputs using expanders.

Communication bus

- RS communication bus for connecting up to 32 devices.

Users

- Up to 50 users.
- Capability to assign to the user:
 - code,
 - up to 4 MIFARE proximity cards (passive transponder in the form of a card, tag, etc.).

Be Wave app

- Mobile app to manage the system:
 - communication via the local network or establishing connection through the Internet using the SATEL server,
 - system programming,
 - system control,
 - system diagnostics,
 - valid for installation on up to 5 different mobile devices of the user.

BE WAVE Soft program

- Program to manage the system:
 - communication via the local network or establishing connection through the Internet using the SATEL server,
 - system programming,
 - system control,
 - system diagnostics,
 - valid for installation on a computer with the Windows 10 / Windows 11 system (or newer).

Arming

- Capability to arm the system fully or partially.

Scenes and routines

- Up to 100 scenes and routines.
- Scenes for easier control.
- Routines for automated system operation.

Schedules

- Up to 50 schedules.
- Capability to use schedules for routines.

Event log

- 8000 event log entries.

Messaging

- Event notification types:
 - push,
 - email messages,
 - SMS [HYBRID 128 Plus],
 - CLIP [HYBRID 128 Plus].

Reporting

- Reporting events to two monitoring stations.
- Support for Contact ID, SIA and Bold Manitou communication formats.
- Data transmission via Ethernet or cellular network [HYBRID 128 Plus].
- Dual Path Reporting compliant with EN 50136 [HYBRID 128 Plus].

Firmware update

- Capability to update firmware of the control panel and the devices in the system.

Mainboard

- 4 programmable hardwired zones.
- 4 programmable high-current hardwired outputs.
- Removable terminal blocks.
- RS communication bus (RS-485).
- Built-in Ethernet (LAN) port.
- Built-in Wi-Fi:
 - operating in the 2.4 and 5 GHz bands,
 - IEEE 80.11 b/g/n (2,4 GHz) / IEEE 802.11 a/n (5 GHz) standards.
- Built-in cellular telephone [HYBRID 128 Plus]:
 - operating in the 2G and 4G networks,
 - dual SIM support.
- LED indicator.
- Powered by 12 VDC.
- Connector for SATEL power supply (e.g. APS-412).

3. Supported devices

You can install up to 128 devices in the system:

- hardwired devices – connected to:
 - zones (e.g. detectors),
 - outputs (e.g. sirens),
 - RS bus (bus devices),
- wireless devices,
- virtual IP devices.

3.1 Bus devices

You can connect up to 32 physical devices to the RS communication bus.

3.1.1 Detectors

SLIM-PIR-PRO BUS (PIR motion detector with anti-mask) – detector that uses infrared to detect motion.

SLIM-PIR-LUNA BUS (PIR motion detector with lighting feature) – detector that uses infrared to detect motion. Equipped with LEDs for lighting.

SLIM-PIR-LUNA-PET BUS (PIR motion detector with lighting feature and pet immunity) – detector that uses infrared to detect motion. Equipped with LEDs for lighting. It ignores moving pets up to 20 kilos.

SLIM-R-PIR-PRO BUS (Ceiling PIR motion detector with anti-mask (recessed)) – ceiling detector that uses infrared to detect motion. For mounting in a suspended ceiling.

SLIM-S-PIR-PRO BUS (Ceiling PIR motion detector with anti-mask (surface mount)) – ceiling detector that uses infrared to detect motion. For mounting on the surface of the ceiling.

SLIM-R-PIR-LUNA BUS (Ceiling PIR motion detector with lighting feature (recessed)) – ceiling detector that uses infrared to detect motion. Equipped with LEDs for lighting. For mounting in a suspended ceiling.

SLIM-S-PIR-LUNA BUS (Ceiling PIR motion detector with lighting feature (surface mount)) – ceiling detector that uses infrared to detect motion. Equipped with LEDs for lighting. For mounting on the surface of the ceiling.

SLIM-DUAL-PRO BUS (Dual technology motion detector with anti-mask) – detector that uses infrared and microwaves to detect motion.

SLIM-DUAL-LUNA BUS (Dual technology motion detector with lighting feature) – detector that uses infrared and microwaves to detect motion. Equipped with LEDs for lighting.

SLIM-DUAL-LUNA-PET BUS (Dual technology motion detector with lighting feature and pet immunity) – detector that uses infrared and microwaves to detect motion. Equipped with LEDs for lighting. It ignores moving pets up to 20 kilos.

SLIM-R-DUAL-PRO BUS (Ceiling dual technology motion detector with anti-mask (recessed)) – ceiling detector that uses infrared and microwaves to detect motion. For mounting in a suspended ceiling.

SLIM-S-DUAL-PRO BUS (Ceiling dual technology motion detector with anti-mask (surface mount)) – ceiling detector that uses infrared and microwaves to detect motion. For mounting on the surface of the ceiling.

SLIM-R-DUAL-LUNA BUS (Ceiling dual technology motion detector with lighting feature (recessed)) – ceiling detector that uses infrared and microwaves to detect motion. Equipped with LEDs for lighting. For mounting in a suspended ceiling.

SLIM-S-DUAL-LUNA BUS (Ceiling dual technology motion detector with lighting feature (surface mount)) – ceiling detector that uses infrared and microwaves to detect motion. Equipped with LEDs for lighting. For mounting on the surface of the ceiling.

TPH-2 (Temperature, pressure and humidity sensor) – sensor for measuring temperature, pressure and air humidity.

3.1.2 Expanders



Required firmware version of expanders: 6.02 (or newer).

INT-E (Zone expander) – expander used to expand the system by 8 programmable hardwired zones.

INT-O (Output expander) – expander used to expand the system by 8 programmable hardwired outputs.

INT-ORS (DIN-rail output expander) – expander used to expand the system by 8 programmable relay outputs. It can control 230 VAC electrical devices. For mounting on a 35 mm DIN-rail.

INT-PP (Zone and output expander) – expander used to expand the system by 8 programmable hardwired zones and 8 programmable hardwired outputs.

INT-IORS (DIN-rail zone and output expander) – expander used to expand the system by 8 programmable hardwired zones and 8 programmable relay outputs. It can control 230 VAC electrical devices. For mounting on a 35 mm DIN-rail.

3.1.3 LCD keypads



Required firmware version of LCD keypads: 2.02 (or newer).

INT-TSG2R (Touchscreen keypad) – LCD keypad with 4.3" touchscreen. Equipped with 13.56 MHz MIFARE proximity card reader.

INT-TSH2R (Touchscreen keypad) – LCD keypad with 7" touchscreen. Equipped with 13.56 MHz MIFARE proximity card reader.

INT-TSH210 (Touchscreen keypad) – LCD keypad with 10" touchscreen.

3.1.4 Keypads



Required firmware version of the keypad: 1.03 (or newer).

SO-MF5 (Keypad with MIFARE proximity card reader) – touch keypad. Equipped with 13.56 MHz MIFARE proximity card reader.

3.1.5 Proximity card readers



Required firmware version of the reader: 1.03 (or newer).

SO-MF3 (MIFARE proximity card reader) – 13.56 MHz MIFARE proximity card reader.

3.2 Wireless devices

3.2.1 Detectors

APD-200 (Motion Detector) – detector that uses infrared to detect motion.

APD-200 Pet (Motion Detector Pet) – detector that uses infrared to detect motion. It ignores moving pets up to 20 kilos.

APCAM-200 (Motion Detector Cam) – detector that uses infrared to detect motion. It has a camera that sends photos in case of alarm or on user's request.

APMD-250 (Motion Detector Plus) – detector that uses infrared and microwaves to detect motion.

AOD-210 (Outdoor Motion Detector) – detector that uses infrared and microwaves to detect motion. It ignores moving pets up to 20 kilos. It is designed for outdoor installation.

AOCAM-210 (Outdoor Motion Detector Cam) – detector that uses infrared and microwaves to detect motion. It has a camera that sends photos in case of alarm or on user's request. It ignores moving pets up to 20 kilos. It is designed for outdoor installation.

ACD-220 (Curtain Detector) – detector that uses infrared to detect motion in an area shaped like a curtain.

AOCD-260 (Outdoor Curtain Detector) – detector that uses infrared and microwaves to detect motion in an area shaped like a curtain. It is designed for outdoor installation.

APC-200 (Ceiling Motion Detector) – ceiling detector that uses infrared to detect motion. Available in two variants:

APC-200 R – for mounting in a suspended ceiling.

APC-200 S – for mounting on the surface of the ceiling.

APMC-250 (Ceiling Motion Detector Plus) – ceiling detector that uses infrared and microwaves to detect motion. Available in two variants:

APMC-250 R – for mounting in a suspended ceiling.

APMC-250 S – for mounting on the surface of the ceiling.

AGD-200 (Glass Break Detector) – detector that detects a glass break.

AXD-200 (Multipurpose Detector) – multipurpose detector that can be used as:

Shock detector – detects shocks accompanying attempts to force open a door or window.

Opening detector – detects the opening of a door or window. You can connect a wired NC detector to it (e.g. a wired opening detector). The built-in opening sensor can be disabled.

Shock and opening detector – detects shocks accompanying attempts to force open a door or window. It also detects the opening of a door or window. You can connect a wired NC detector to it (e.g. a wired opening detector). The built-in opening sensor can be disabled.

Flood detector – detects indoor water flooding. The FPX-1 probe by SATEL is required.

Temperature sensor – measures the air temperature.

Roller shutter detector – detects the opening of a door or window. You can connect to it a wired roller shutter detector and a wired NC detector (e.g. a wired opening detector).

AXD-200 Lite (Opening Detector) – detector that detects the opening of a door or window. You can connect a wired NC detector to it (e.g. a wired opening detector). The built-in opening sensor can be disabled.

AFD-200 (Flood Detector) – detector that detects indoor water flooding.

ASD-200 (Fire Detector Plus) – detector that detects the presence of smoke or a rapid temperature rise (early signs of fire).

ASD-250 (Fire Detector Pro) – detector that detects the presence of smoke (early sign of fire). It meets the EN 14604 requirements.

ACMD-200 (Carbon Monoxide Detector) – detector that detects hazardous concentration of carbon monoxide.

ADD-200 (Outdoor Dusk Detector) – detector that detects dusk and dawn based on the measurement of light intensity. It is designed for outdoor installation.

ATPH-200 (Multi Sensor) – sensor for measuring temperature, pressure and air humidity.

3.2.2 Actuators

ADC-200 (Smart Dimmer) – dimmer used to adjust the brightness of 230 VAC lighting. It can be used to turn on / turn off / dim down / dim up the lights.

ARC-200 (Smart RGBW LED Driver) – controller used to control the light color and adjust the brightness of 12...48 VDC LED lighting. It can be used to turn on / turn off / dim down / dim up the lights / change the light color.

ARSC-200 (Smart Blinds) – controller used to open and close roller blinds / shutters / electric windows. It controls devices driven by a 230 VAC motor with limit switches.

ART-210 (Smart Thermostat) – radiator thermostat used to maintain the set room temperature by regulating the flow of warm water to the radiator.

ASW-200 (Smart Plug) – plug used to turn ON / OFF any 230 VAC electrical appliance connected to its outlet.

ASW-210 (Smart 2-CH Relay) – controller used to turn ON / OFF up to two 230 VAC electrical appliances.

ASW-220 (Smart 2-CH Relay PM) – controller used to turn ON / OFF up to two 230 VAC electrical appliances. It measures the power consumed by appliances connected to the controller outputs.

3.2.3 Sirens

ASP-200 (Outdoor Siren) – siren that emits sound and light. It is designed for outdoor installation.

ASP-215 (Indoor Siren) – siren that emits sound and light.

3.2.4 Keypad

AKP-200 (Smart Keypad) – keypad used to control the BE WAVE system.

3.2.5 Keyfobs and buttons

APT-200 (Smart Keyfob) – keyfob used to control the BE WAVE system remotely.

APT-210 (Smart Keyfob) – keyfob used to control the BE WAVE system remotely.

APB-200 (Panic Button) – panic button.

APB-210 (Smart Button) – control button.

3.2.6 Expanders

ACX-210 (Mini Multi Extender) – expander that allows you to use wired detectors in a wireless system and to control wired devices. Due to its small size, it can be installed inside another device enclosure.

ACX-220 (Multi Extender) – expander that allows you to use wired detectors in a wireless system and to control wired devices.

AUT-200 (Wireless Universal Transmitter) – module that allows you to use wired detectors in a wireless system.

ATX-200 (Smart Switch Controller) – module that enables electrical switches to be used to control the BE WAVE system.

3.2.7 Repeater

ARU-200 (Smart Repeater) – radio signal repeater that extends the range of radio communication in the BE WAVE system. This allows you to install wireless devices further away from the control panel.



Required firmware version of the repeater: 2.00 (or newer).

3.3 Virtual IP devices

An IP device can receive and send HTTP notifications. When an HTTP notification is received (e.g. from an IP camera), the IP zone is violated. When the IP output is activated / deactivated, an HTTP notification is sent.



For security reasons, it is not recommended to use HTTP requests outside of the local network. These requests are not encrypted.

4. Installation



Disconnect power before making any electrical connections.

For installation, you will need the following tools:

- 2.5 mm flathead screwdriver,
- Philips screwdriver,
- precision pliers,
- flat-nose pliers,
- drill with a set of drill bits.

4.1 Installation plan

Before you start the installation, draw up a plan of the premises and mark on it all the devices that are to be included in the system: control panel, keypads, detectors, sirens, expanders, etc. The control panel and other alarm system components should be installed within the protected area.

4.2 Estimation of the system current consumption

Sum up the current consumption of the wired devices to be installed in the system (control panel, keypads, expanders, detectors, sirens, etc.). Based on this, select the appropriate SATEL power supply for your system. With more devices, it may be necessary to use several power supplies in the system.

If you plan to connect devices to particular power outputs, remember that the sum of currents consumed by the connected devices must not exceed the maximum current carrying capacity of those outputs.

4.3 Cabling

Prepare the cables for connecting hardwired devices and run them to the place of control panel installation. To connect devices to screw terminals, use flexible wires with a cross section of 0.5-0.75 mm². For the RS communication bus, use a UTP cable (unshielded twisted pair).

4.4 Mounting the control panel



The control panel mainboard incorporates components sensitive to electrostatic discharges.

4.4.1 Tips for installation

- The control panel should be installed indoors, in spaces with normal air humidity.
- Do not install the control panel outdoors.
- When selecting a place of installation, consider the radio communication range.
- Thick walls, metal partitions, etc. reduce the range of the radio signal.
- The control panel must be protected against unauthorized access.
- It is recommended to install the control panel in a plastic enclosure.
- Do not install the control panel in a metal enclosure.
- The control panel requires 12 VDC power. Connect a SATEL power supply to the APS connector (e.g. APS-412).

- Run the cables inside the control panel enclosure and secure the enclosure to the wall with screws and anchors.
- Remember to connect the enclosure tamper switch to the control panel tamper input. If the enclosure tamper switch is not to be connected to the control panel tamper input, connect the TMP terminal to the COM terminal.

4.4.2 Description of the mainboard

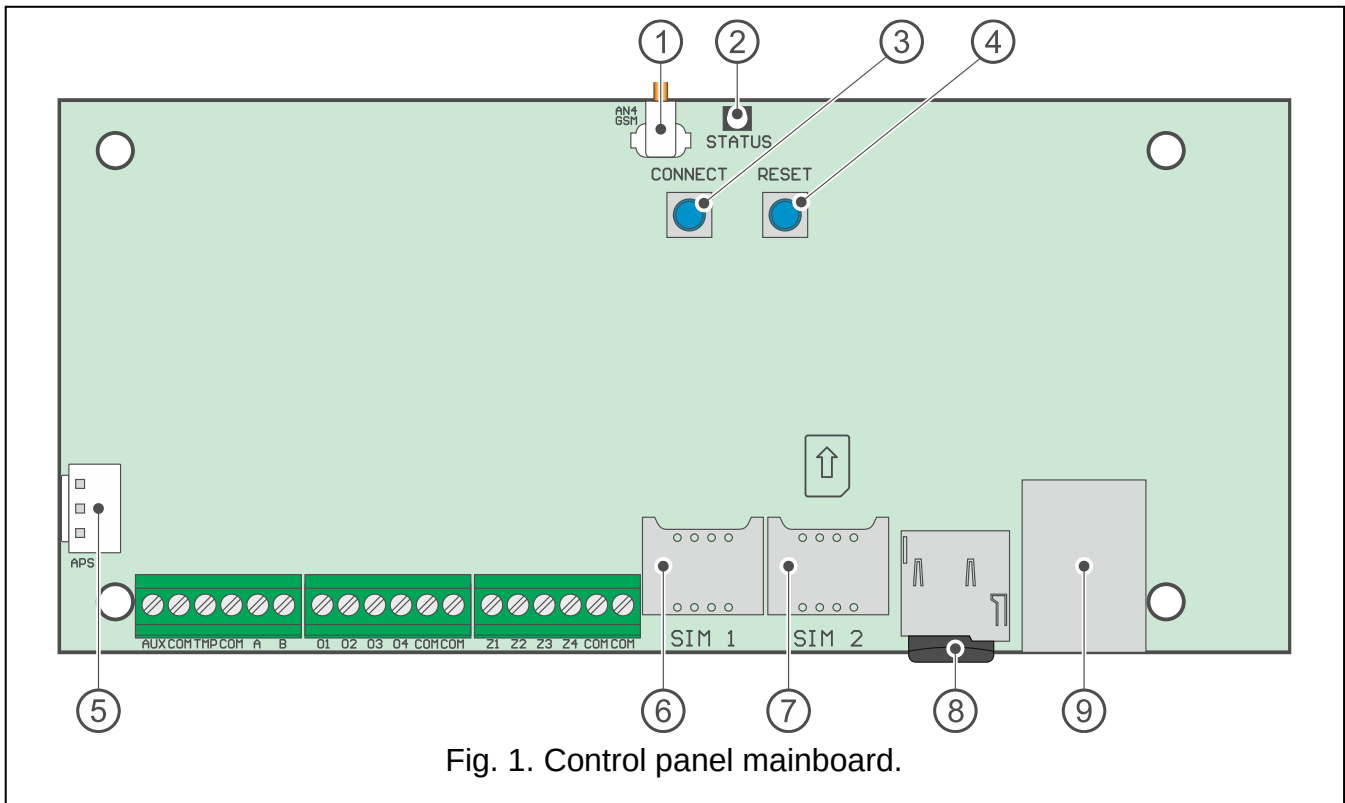


Fig. 1. Control panel mainboard.

- ① antenna cable.
- ② STATUS LED indicator:
 - flashing in pink – control panel startup in progress,
 - ON in pink – control panel operates in the Wi-Fi access point mode (you can connect to the control panel in the BEWAVE_AP network),
 - ON in blue – control panel is connected to a local network but has no access to the Internet or no connection to the SATEL server,
 - ON in green – control panel is connected to the Internet,
 - additionally flashing in yellow – trouble,
 - additionally flashing in red – alarm,
 - colors changing smoothly – control panel's firmware update in progress,
 - ON in white – control panel's factory reset in progress.
- ③ CONNECT button – press and hold for 5 seconds to enable / disable the Wi-Fi access point mode.
- ④ RESET button – press and hold for 5 seconds to restore factory settings (see “Hardware factory restore” p. 82.).
- ⑤ APS connector to connect a SATEL power supply (e.g. APS-412).



The control panel reports the following information about the power supply connected to the APS connector:

- supply voltage,
- current consumption from the power supply,
- power supply troubles (loss of 230 VAC, battery trouble, power supply overload).

- ⑥ SIM1 slot for installing the first SIM card [HYBRID 128 Plus].
- ⑦ SIM2 slot for installing a second SIM card [HYBRID 128 Plus].
- ⑧ SD memory card (factory-installed). Stored on the SD card are:
 - backup settings (in order to restore settings in case of trouble or copy settings to another control panel),
 - photos sent by detectors equipped with a camera,
 - photos used in the Be Wave app / BE WAVE Soft program (for personalized room views),
 - data from devices measuring temperature, pressure, humidity, power consumption, etc.,
 - file of system items names (it can be created if the file is to be forwarded to the monitoring station).
- ⑨ LAN cable port.

Description of terminals

AUX - +12 VDC power output.

COM - common ground.

TMP - tamper input (NC). If the enclosure tamper switch is not to be connected to the input, connect the TMP terminal to the COM terminal.

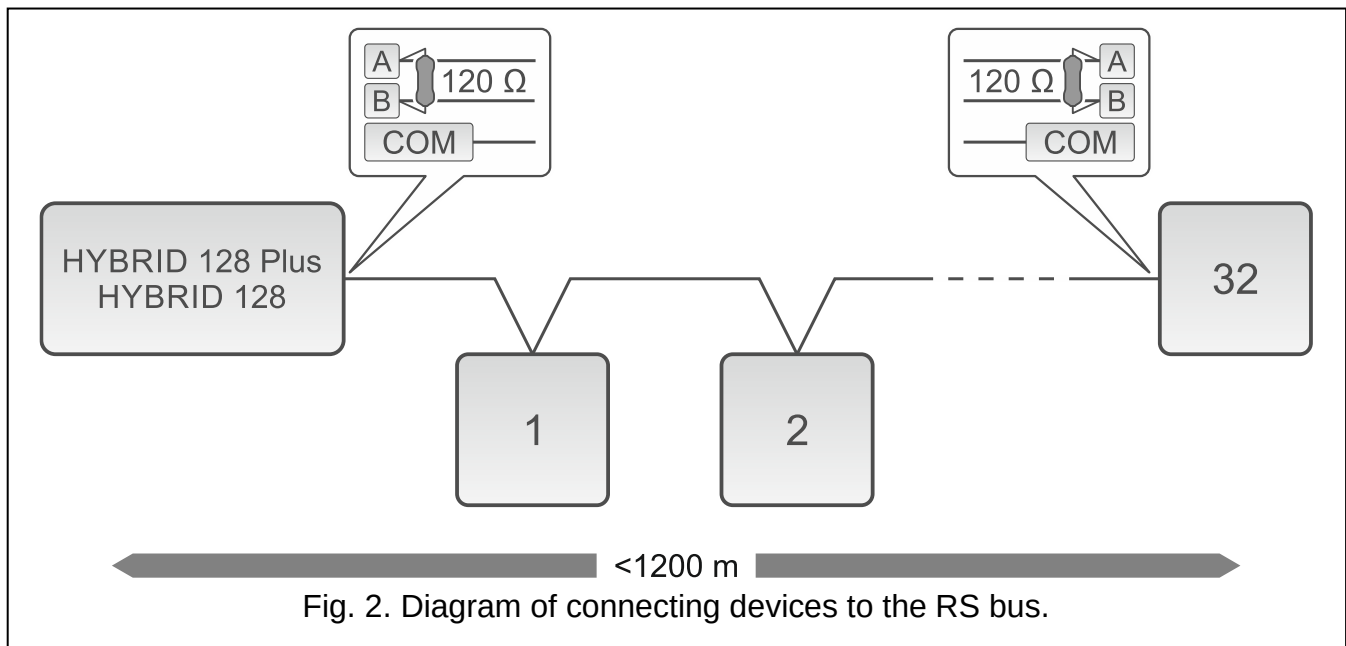
A, B - RS communication bus.

O1...O4 - programmable high-current outputs (+12 VDC).

Z1...Z4 - programmable zones.

4.5 Connecting the bus devices

- You can connect up to 32 devices to the RS bus.
- The devices must be connected in series, one after the other.
- Branch connections are not allowed.
- Use a UTP cable (unshielded twisted pair).
- The length of the bus must not exceed 1200 meters.
- At both ends of the bus, place $120\ \Omega \pm 20\%$ resistors between the A and B terminals.
- Connect the COM terminals of all devices on the bus with an additional wire.
- If you want to extend the bus or create a branch, use the ISO-RS485 isolator by SATEL.



4.6 Connecting the detectors

The zones support the following wiring configurations:

NC – for connecting a detector with NC (normally closed) alarm output. Opening the circuit will generate an alarm.

NO – for connecting a detector with NO (normally open) alarm output. Closing the circuit will generate an alarm.

EOL – for connecting a detector with NC or NO alarm output. An EOL resistor must be used in the circuit. Closing or opening the circuit will generate an alarm.

2EOL/NC – for connecting a detector with NC alarm output and tamper output. Two EOL resistors must be used in the circuit. The zone can recognize 3 states: normal, alarm and tamper.

2EOL/NO – like 2EOL/NC, but for a detector with NO alarm output.

Roller shutter – for connecting a roller shutter detector.

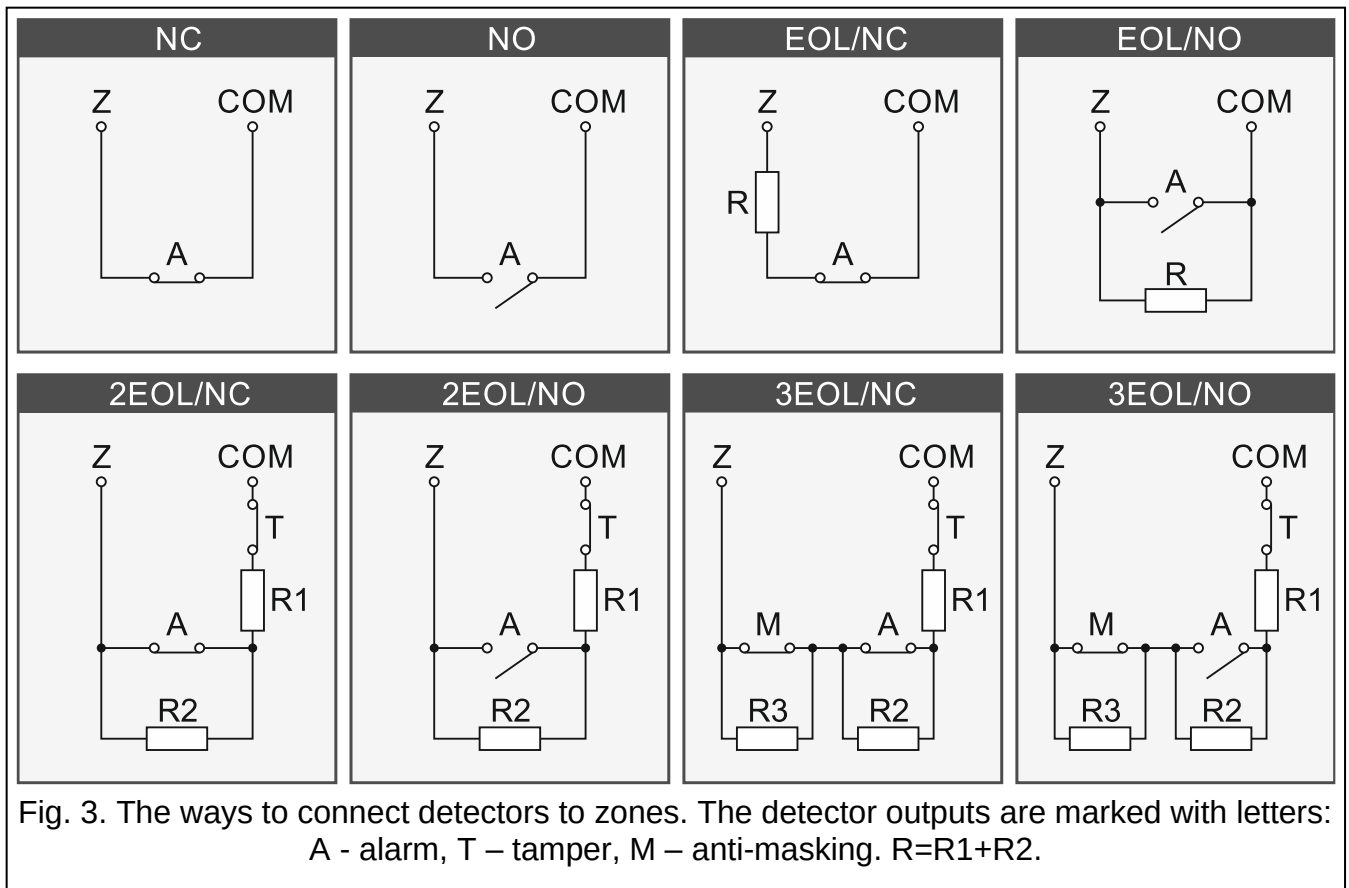
Shock – for connecting a shock detector. You can also connect a detector with NC alarm output to the zone (e.g. you can connect a shock detector and a magnetic contact in series).

Roller shutter 2EOL/NC – for connecting a roller shutter detector with a tamper output. Two EOL resistors must be used in the circuit. The zone can recognize 3 states: normal, alarm and tamper.

Shock 2EOL/NC – for connecting a shock detector with a tamper output. Two EOL resistors must be used in the circuit. The zone can recognize 3 states: normal, alarm and tamper.

3EOL/NC – for connecting a detector with NC alarm output, tamper output and anti-masking output. Three EOL resistors must be used in the circuit. The zone can recognize 4 states: normal, alarm, tamper and detector masking.

3EOL/NO – like 3EOL/NC, but for a detector with NO alarm output.



4.6.1 End-of-line resistors

You can program the value of end-of-line resistors to be used in the system (see “Advanced settings” p. 69). By default, the following values are programmed:

$R_1 = 1.1 \text{ k}\Omega$;

$R_2 = 1.1 \text{ k}\Omega$;

$R_3 = 2.2 \text{ k}\Omega$.

According to the factory settings, depending on the wiring type:

- EOL – use one $2.2 \text{ k}\Omega$ resistor,
- 2EOL – use two $1.1 \text{ k}\Omega$ resistors.

4.7 Connecting the LAN



The control panel can only operate in the local area networks (LAN). It must not be connected directly to the public computer network (MAN, WAN). To establish connection with a public network, use a router or xDSL modem.

If the control panel is to be connected to the wired LAN network, connect the cable to the LAN port. Use a cable compliant with the 100Base-TX standard with the RJ-45 plug (the same as for connecting the computer to the network).

4.8 Installing the SIM cards [HYBRID 128 Plus]

Insert a mini SIM card into the SIM1 slot. If you want to use two cards, insert the second mini SIM card into the SIM2 slot.



If the SIM card requires a PIN code, you can program it using the Be Wave app or the BE WAVE Soft program after starting the control panel.

4.9 Connecting the power and starting the control panel



To power the control panel, use a 12 VDC power supply by SATEL (e.g. APS-412).

The cable connecting the power supply to the control panel APS connector must not be routed over the control panel antenna circuits.

1. Connect a power supply to the APS connector.
2. Power on the power supply (turn on 230 V AC power in the circuit to which the power supply is connected). The control panel will start up (the STATUS LED indicator will start flashing).

4.10 Connecting the sirens



It is recommended that the control panel be started without connected sirens. This will prevent accidental triggering of the signaling after the control panel is started.

The O1...O4 outputs are 1 A / 12 VDC high-current outputs. You can connect directly to those outputs the sirens in which signaling is activated after applying +12 VDC.

Please refer to the manual of the siren for details on how to connect it and configure its settings (if required).

4.11 Installing wireless devices

For details on how to install wireless devices in the BE WAVE Hybrid system, please refer to the manuals of these devices.

5. Managing, programming and controlling the system

You can manage, program and control the system, using the:

- Be Wave app,
- BE WAVE Soft program.



All settings of the INT-TSG2R / INT-TSH2R / INT-TSH210 LCD keypad can only be programmed in the BE WAVE Soft program.

5.1 Be Wave app

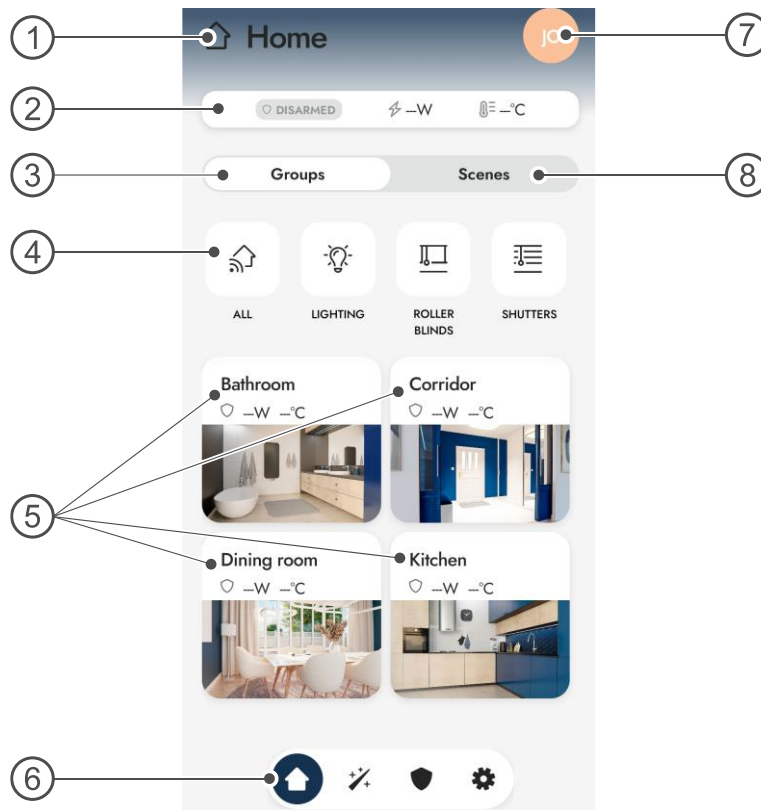
The Be Wave app is designed for mobile devices. You can download it from these online stores: “Google Play” (for Android devices) and “App Store” (for iOS devices). Required Android version: 11 (or newer). Required iOS version: 11 (or newer).

Required Be Wave app version: 1.3.

5.1.1 Description of the Be Wave app home screen



The screenshot is an example. It shows the home screen after the control panel (site) and devices have been added to the app.



Explanation:

- ① icon and name of the site (control panel). Tap to open the *Select an account* screen.
- ② status bar.
- ③ *Groups* tab. Tap to show groups.
- ④ groups. Tap a group to open the group screen.
- ⑤ rooms: Tap a room to open the room screen.
- ⑥ menu bar:
 - tap to open the home screen.
 - tap to open the *Automation* screen.
 - tap to open the *Alarm system* screen.
 - tap to open the *Settings* screen.
- ⑦ profile icon. Tap to open the *My profile* screen.
- ⑧ *Scenes* tab. Tap to show the scenes created in the system.

5.1.2 Changing the app language

1. Tap the icon or name of the site. The *Select an account* screen will be displayed.
2. Tap in the top right corner. The *Common settings* screen will be displayed.
3. Tap *Application language*. The *Language* screen will be displayed.
4. Select the language to be used in the app.
5. Tap *Save*.

5.1.3 Changing the app theme

1. Tap the icon or name of the site. The *Select an account* screen will be displayed.
2. Tap  in the top right corner. The *Common settings* screen will be displayed.
3. Tap *Theme*. The *Theme* screen will be displayed.
4. Select the theme to be used in the app.
5. Tap Save.

5.2 BE WAVE Soft program

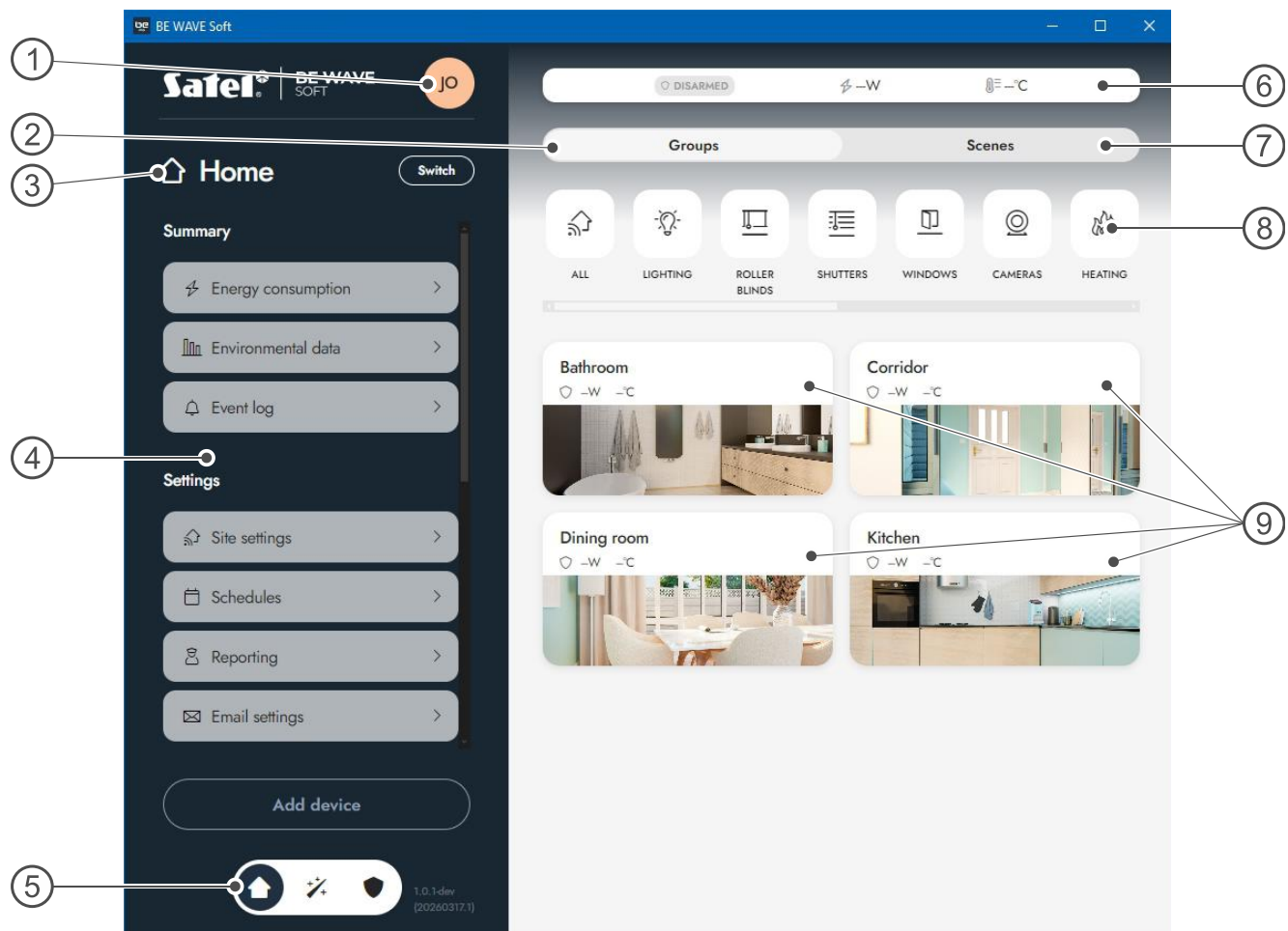
The BE WAVE Soft program is designed for Windows computers. You can download it from www.satel.pl. Required operating system version: Windows 10 / Windows 11 (or newer).

Required BE WAVE Soft program version: 1.00

5.2.1 Description of the BE WAVE Soft program home screen



The screenshot is an example. It shows the home screen after the control panel (site) and devices have been added to the program.



Explanation:

- ① profile icon. Click to open the *My profile* window.
- ② *Groups* tab. Click to show groups.
- ③ icon and name of the site (control panel). Click the *Switch* button to open the *Select an account* window.
- ④ side menu (contains the same elements as the *Settings* screen in the Be Wave app).

⑤ menu bar:

-  - click to open the home screen.
-  - click to open the *Automation* window.
-  - click to open the *Alarm system* window.

⑥ status bar.

⑦ *Scenes* tab. Click to show the scenes created in the system.

⑧ groups. Click a group to open the group window.

⑨ rooms: Click a room to open the room window.

5.2.2 Changing the program language

1. Click the *Switch* button next to the site name. The *Select an account* window will be displayed.
2. Click  in the top right corner. The *Common settings* window will be displayed.
3. Click *Application language*. The *Language* screen will be displayed.
4. Select the language to be used in the app.
5. Click *Save*.

5.2.3 Changing the program theme

1. Click the *Switch* button next to the site name. The *Select an account* window will be displayed.
2. Click  in the top right corner. The *Common settings* window will be displayed.
3. Click *Theme*. The *Theme* screen will be displayed.
4. Select the theme to be used in the program.
5. Click *Save*.

5.3 Adding the control panel (site)



After start-up, the control panel with factory settings operates in the Wi-Fi access point mode (the STATUS LED indicator is ON in pink). It allows the app / program to connect to the control panel.

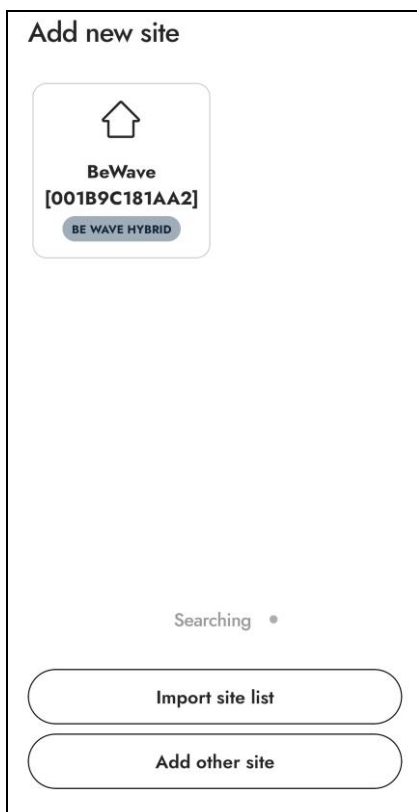
5.3.1 Adding the control panel in the Be Wave app

Adding the first control panel (site)

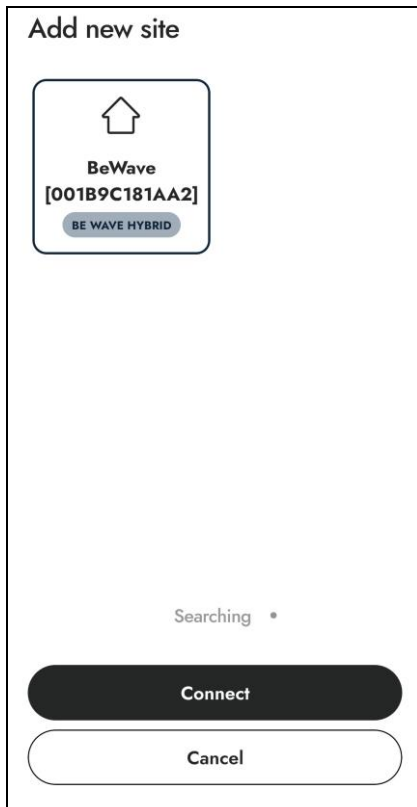


Before you start the Be Wave app, connect your phone to the BEWAVE_AP network. The network's full name contains the MAC address of the control panel. Make sure it is the MAC address of your control panel.

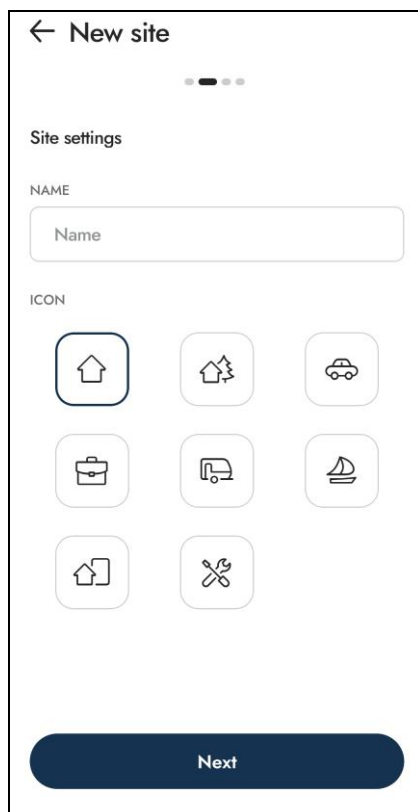
1. Start the Be Wave app. The *Add new site* screen will be displayed.



2. Tap the control panel (site) you want to add. Different buttons will appear at the bottom of the screen.

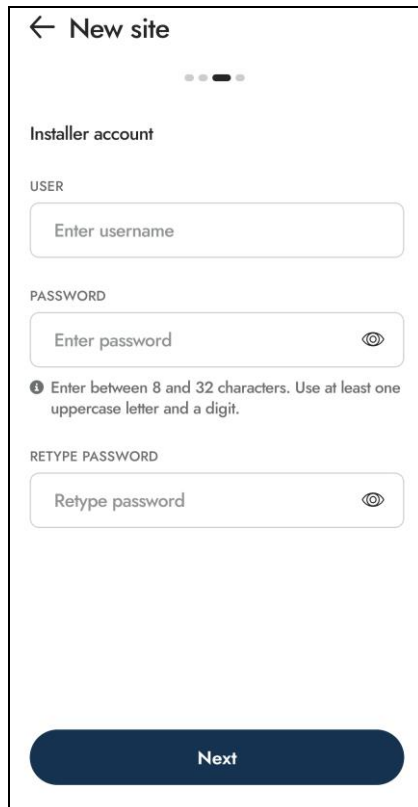


3. Tap *Connect*. The *New site – Site settings* screen will be displayed.



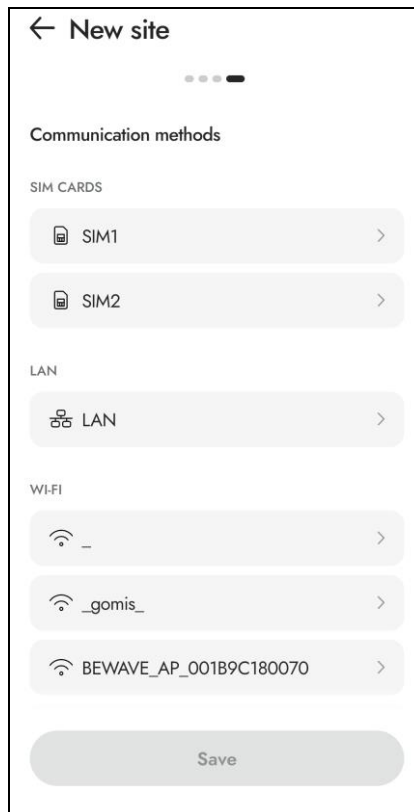
The screenshot shows the 'New site' screen with a back arrow and the title 'New site'. Below the title is a progress indicator with three dots, the second of which is filled. The section is titled 'Site settings'. Under 'NAME', there is a text input field with the placeholder 'Name'. Under 'ICON', there is a grid of eight icons: a house, a house with a tree, a car, a briefcase, a truck, a sailboat, a house with a square, and a wrench. At the bottom is a dark blue button labeled 'Next'.

4. Enter the name of the site and select one of the icons to represent the site, then tap *Next*. The *New site – Installer account* screen will be displayed.



The screenshot shows the 'New site' screen with a back arrow and the title 'New site'. Below the title is a progress indicator with three dots, the second of which is filled. The section is titled 'Installer account'. Under 'USER', there is a text input field with the placeholder 'Enter username'. Under 'PASSWORD', there is a text input field with the placeholder 'Enter password' and an eye icon. Below the password field is a note: 'Enter between 8 and 32 characters. Use at least one uppercase letter and a digit.' Under 'RETYPE PASSWORD', there is a text input field with the placeholder 'Retype password' and an eye icon. At the bottom is a dark blue button labeled 'Next'.

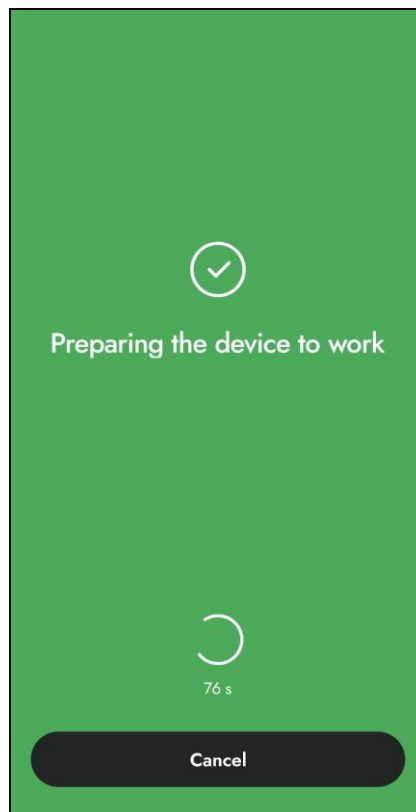
5. Enter the username and password for the installer, then tap **Save**. The *New site – Communication methods* screen will be displayed.



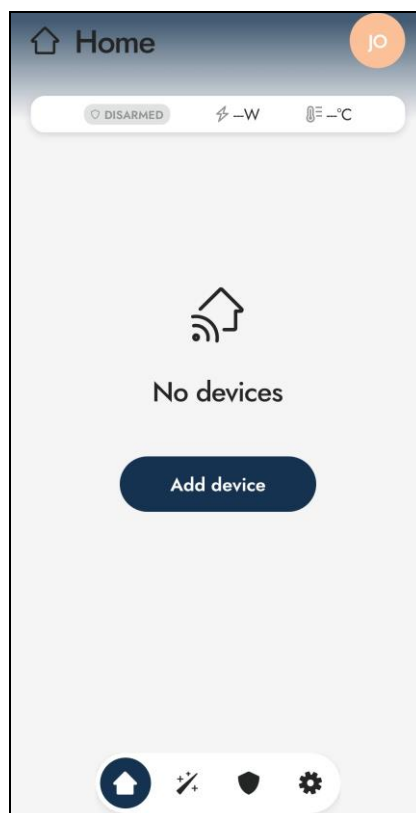
6. Select the communication method to be used with the control panel. A new screen will be displayed. Configure the settings for the selected communication method (see “Communication settings” p. 68). Once the settings are configured and saved, you will return to the *New site – Communication methods* screen. Tap **Save**. A screen will be displayed saying that the control panel is being prepared to work.



While the control panel is being prepared to work, the Wi-Fi access point mode will be disabled. The control panel will switch to the selected communication method.

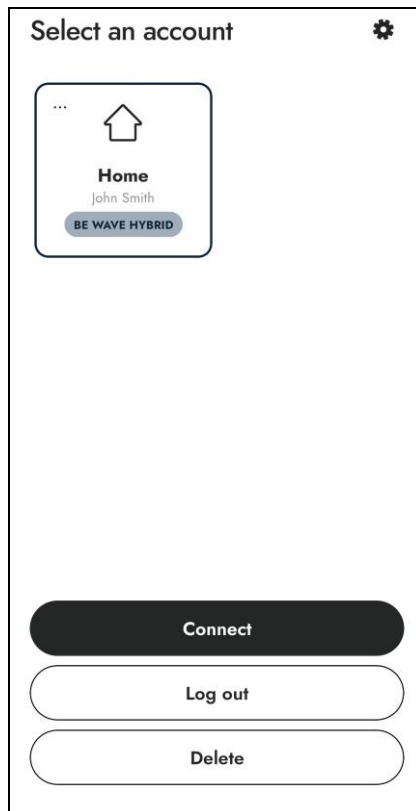


7. When the app connects to the control panel by means of the selected communication method, the app's home screen will be displayed. You can add the first device to the system.

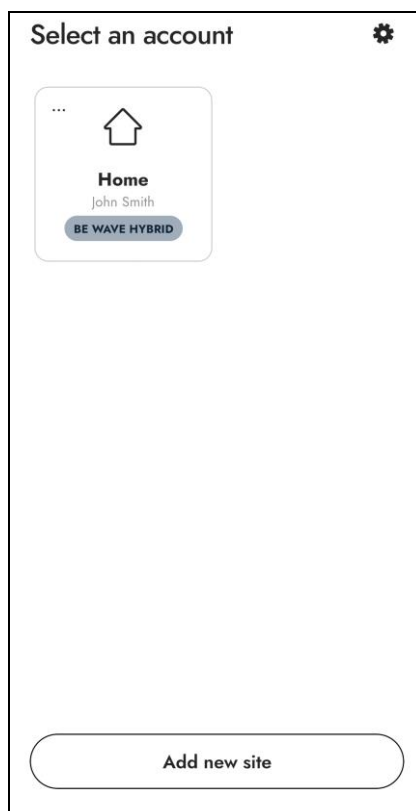


Adding another control panel (site)

1. Tap the icon or name of the site. The *Select an account* screen will be displayed.



2. Tap a blank space on the screen to deselect the site. The *Add new site* button will be displayed at the bottom of the screen.



3. Connect your phone to the BEWAVE_AP network. The network's full name contains the MAC address of the control panel. Make sure it is the MAC address of the new control panel.

4. Tap the *Add new site* button. The *Add new site* screen will be displayed.
5. In the next steps, the procedure is the same as for adding the first control panel.

5.3.2 Adding the control panel in the BE WAVE Soft program



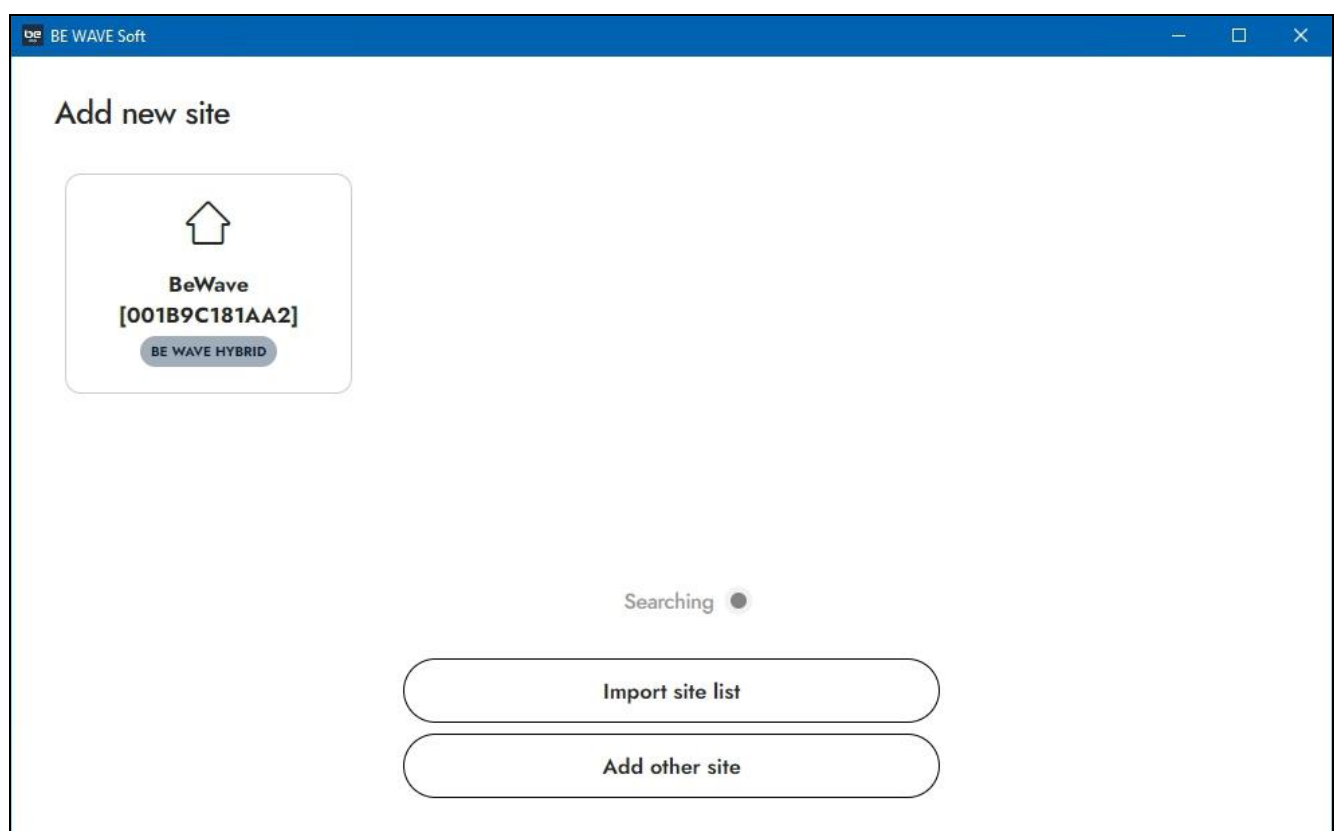
The computer must be connected to the same local network as the control panel or must be equipped with a Wi-Fi network card.

Adding the first control panel (site)

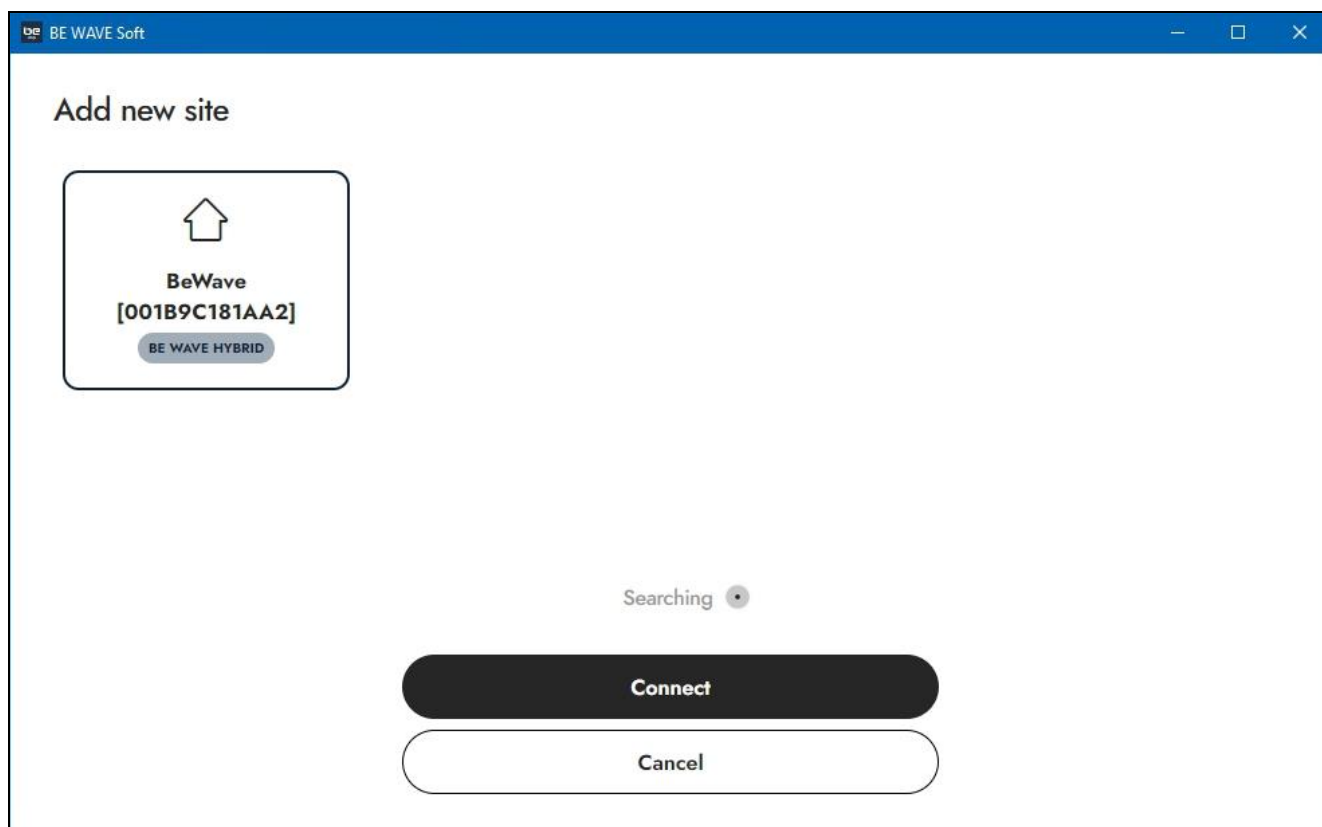


If the control panel is not connected to the local network, before you start the BE WAVE Soft program, connect your computer to the BEWAVE_AP network. The network's full name contains the MAC address of the control panel. Make sure it is the MAC address of your control panel.

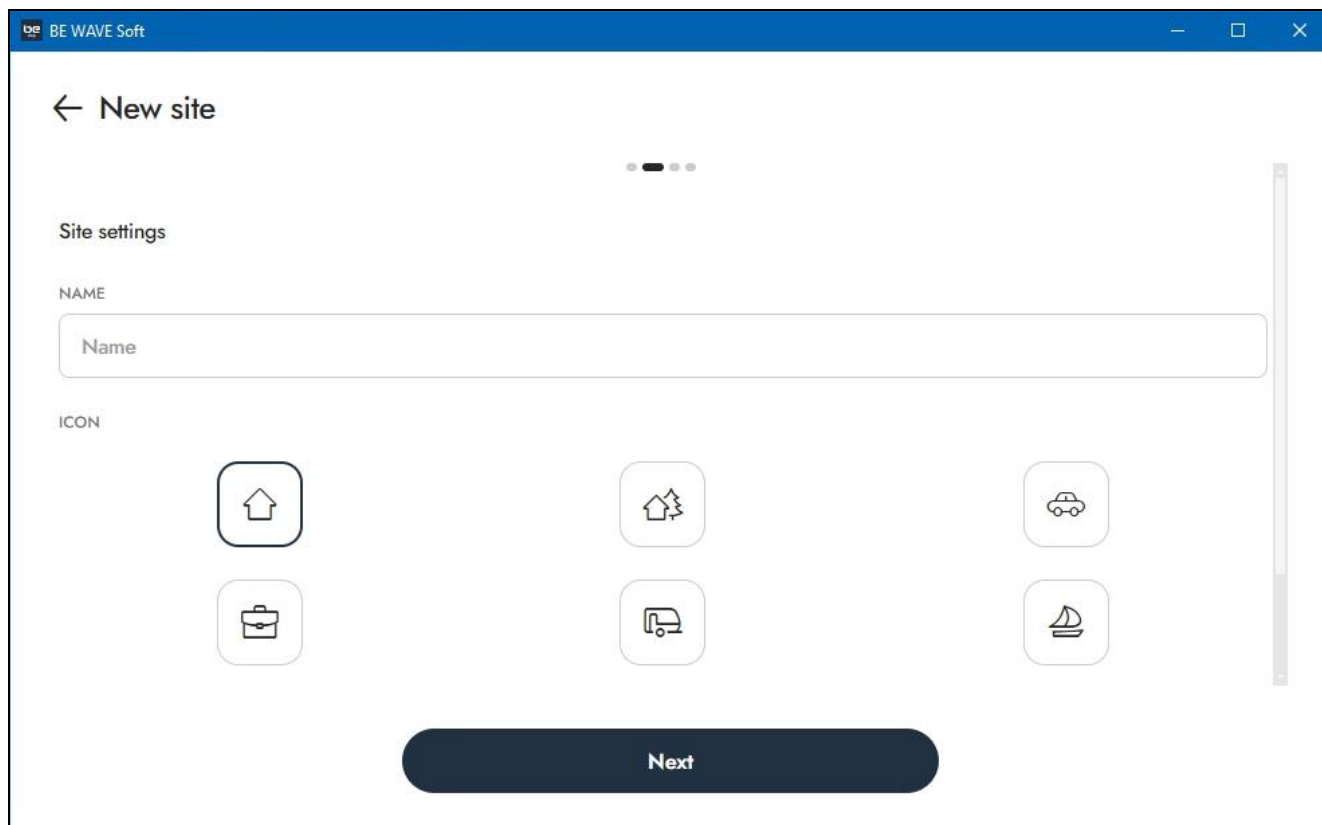
1. Start the BE WAVE Soft program. The *Add new site* window will be displayed.



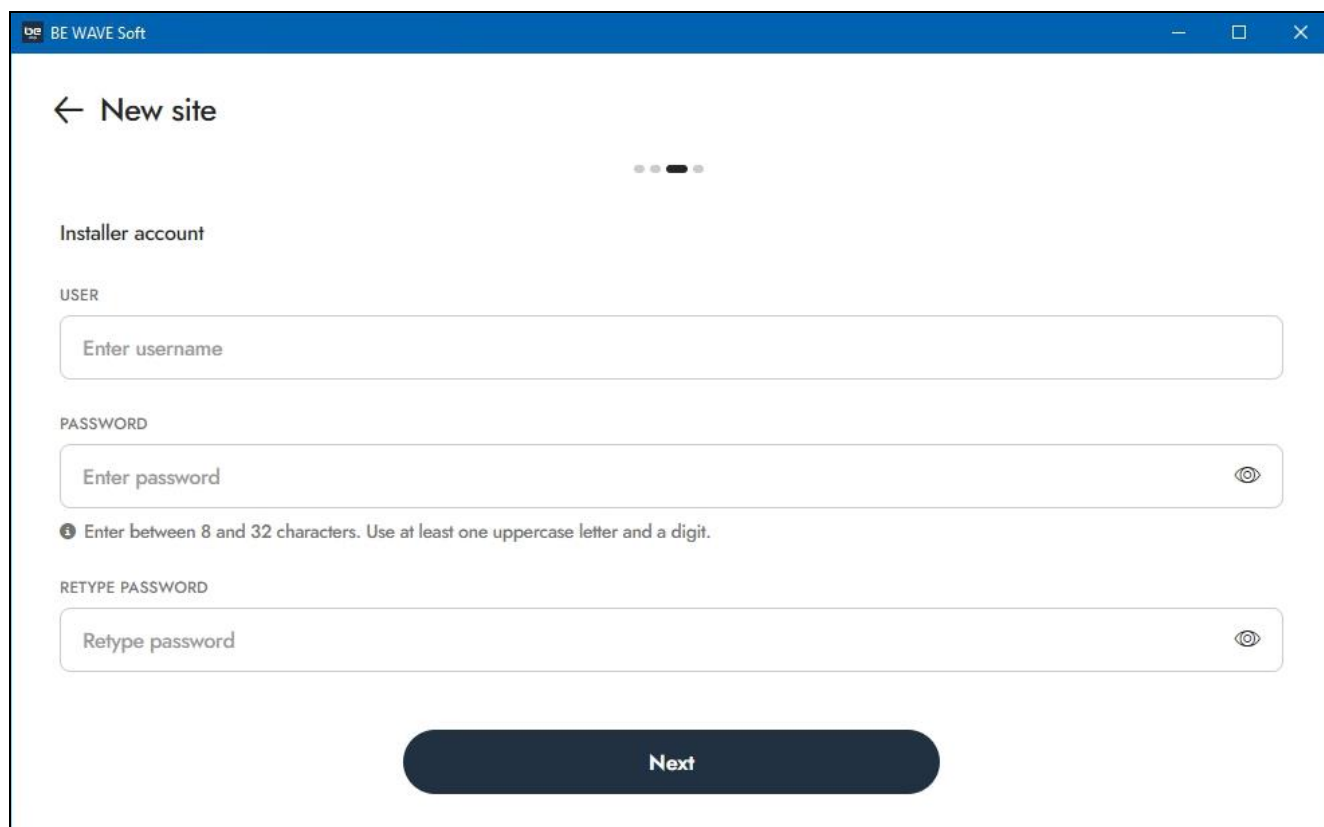
- Click the control panel (site) you want to add. Different buttons will appear at the bottom of the window.



- Click *Connect*. The *New site – Site settings* window will be displayed.

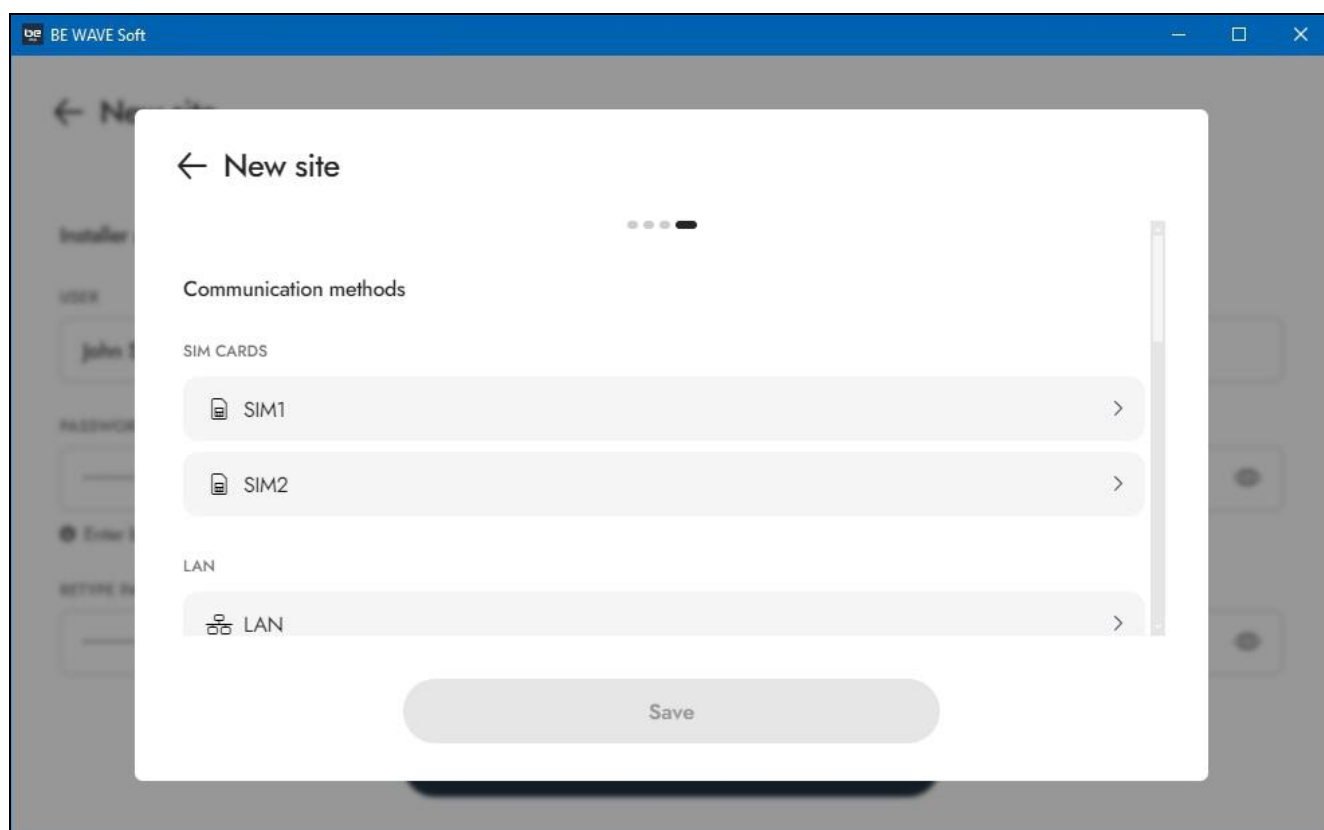


4. Enter the name of the site and select one of the icons to represent the site, then click *Next*. The *New site – Installer account* window will be displayed.



The screenshot shows a window titled "BE WAVE Soft" with a "New site" header and a back arrow. Below the header is a progress indicator with four dots, the second of which is filled. The "Installer account" section contains three input fields: "USER" with a placeholder "Enter username", "PASSWORD" with a placeholder "Enter password" and an eye icon, and "RETYPE PASSWORD" with a placeholder "Retype password" and an eye icon. A note below the password fields states: "Enter between 8 and 32 characters. Use at least one uppercase letter and a digit." At the bottom is a large "Next" button.

5. Enter the username and password for the installer, then click *Save*. The *New site – Communication methods* window will be displayed.



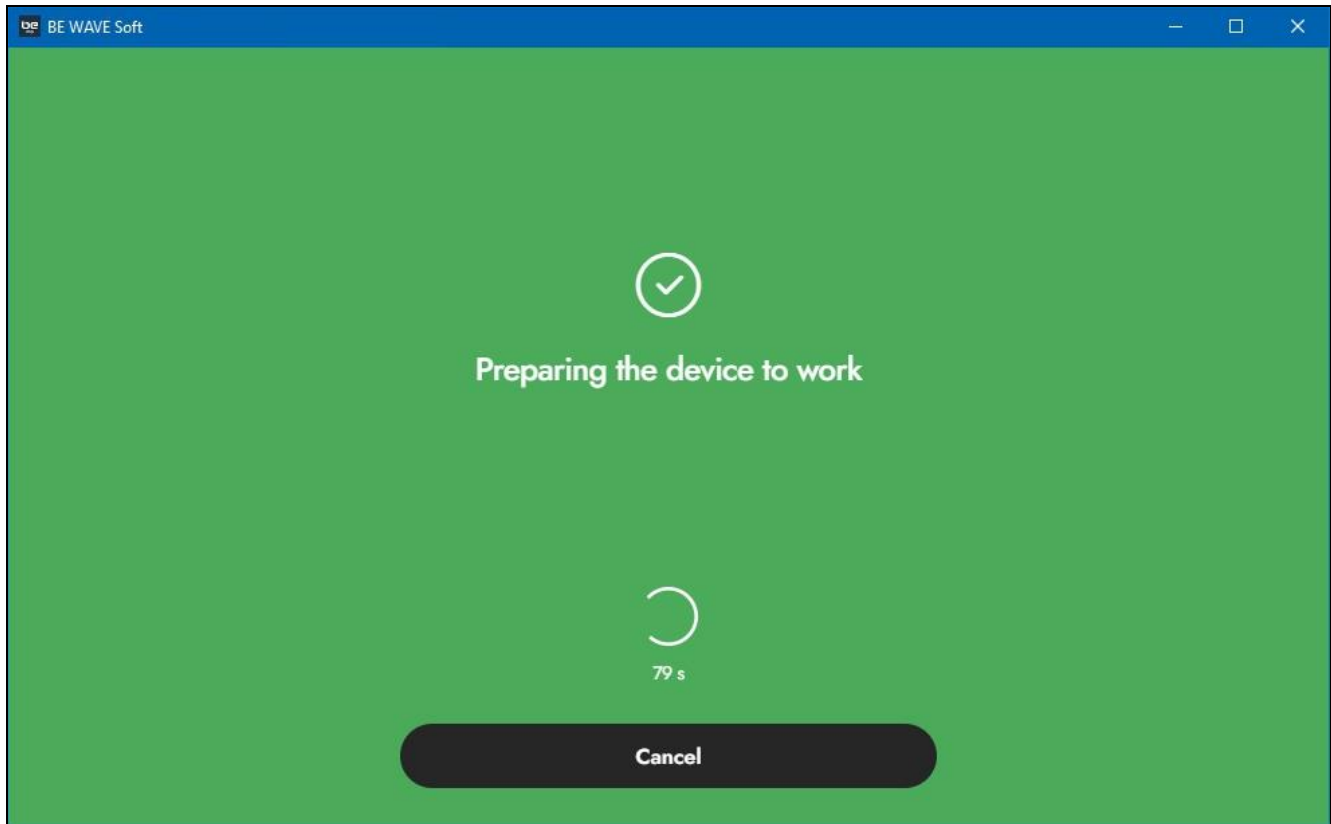
The screenshot shows the same "New site" window, but now displaying the "Communication methods" section. The "SIM CARDS" section has two entries: "SIM1" and "SIM2", each with a SIM card icon and a right arrow. The "LAN" section has one entry: "LAN" with a LAN icon and a right arrow. At the bottom is a large "Save" button.

6. Select the communication method to be used with the control panel. A new window will be displayed. Configure the settings for the selected communication method (see "Communication settings" p. 68). Once the settings are configured and saved, you will

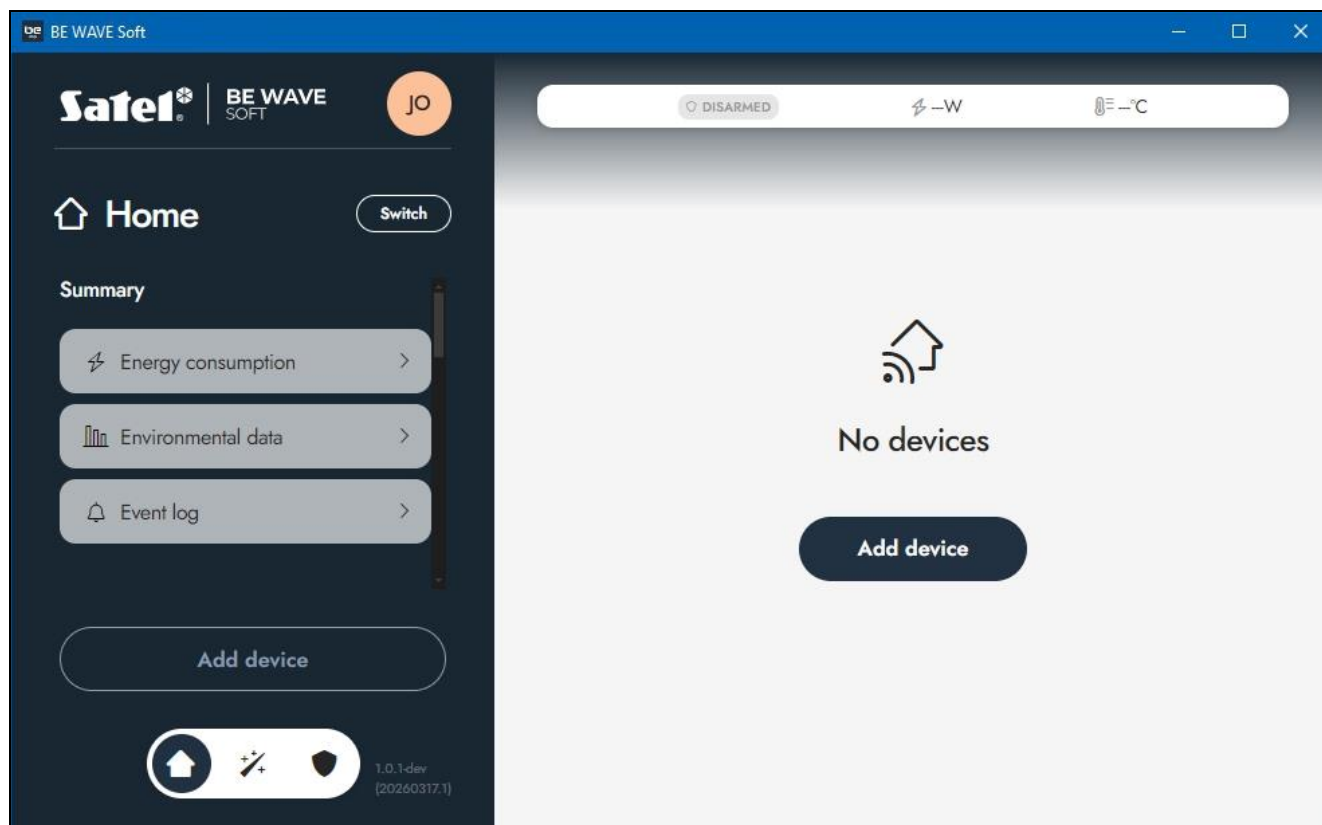
return to the *New site – Communication methods* window. Click *Save*. A window will be displayed saying that the control panel is being prepared to work.



While the control panel is being prepared to work, the Wi-Fi access point mode will be disabled. The control panel will switch to the selected communication method.

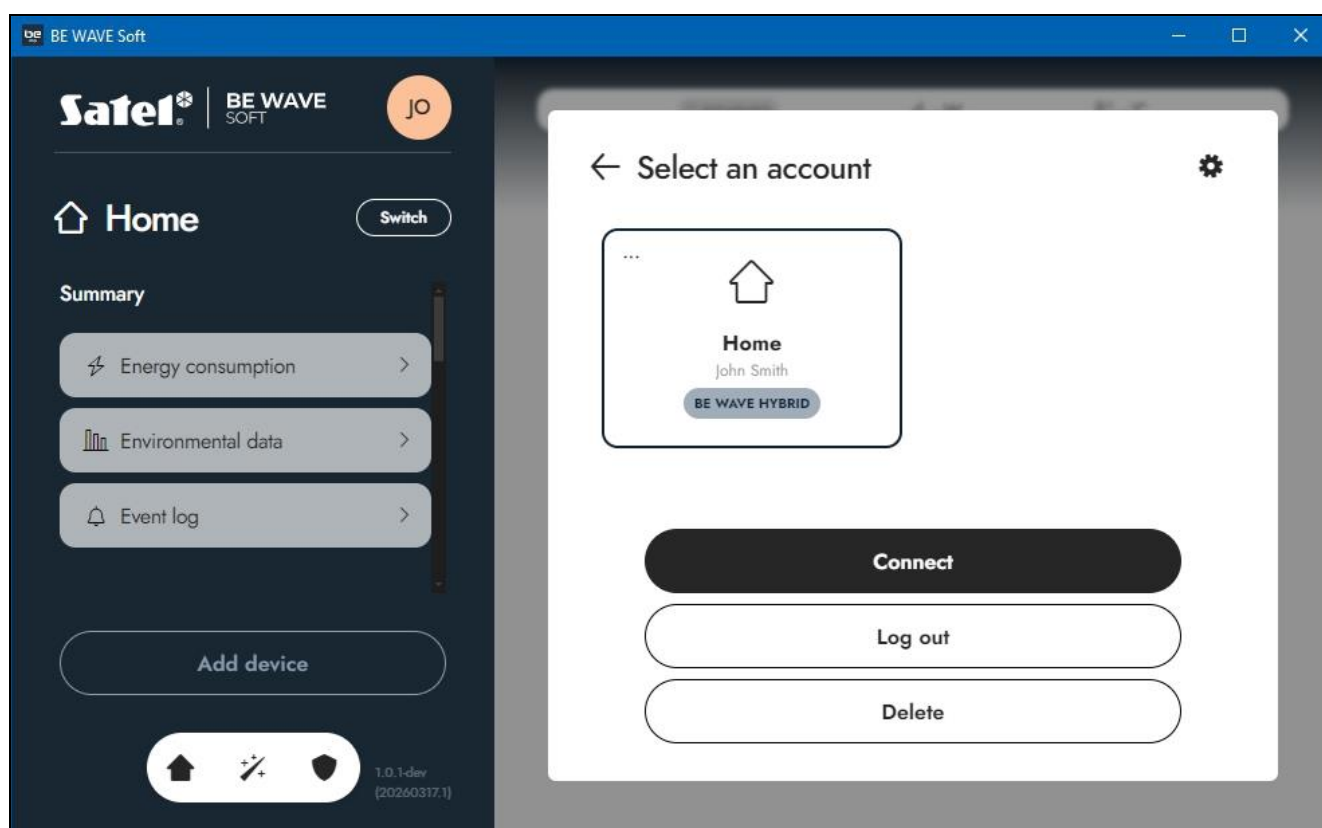


- When the program connects to the control panel by means of the selected communication method, the program's home screen will be displayed. You can add the first device to the system.



Adding another control panel (site)

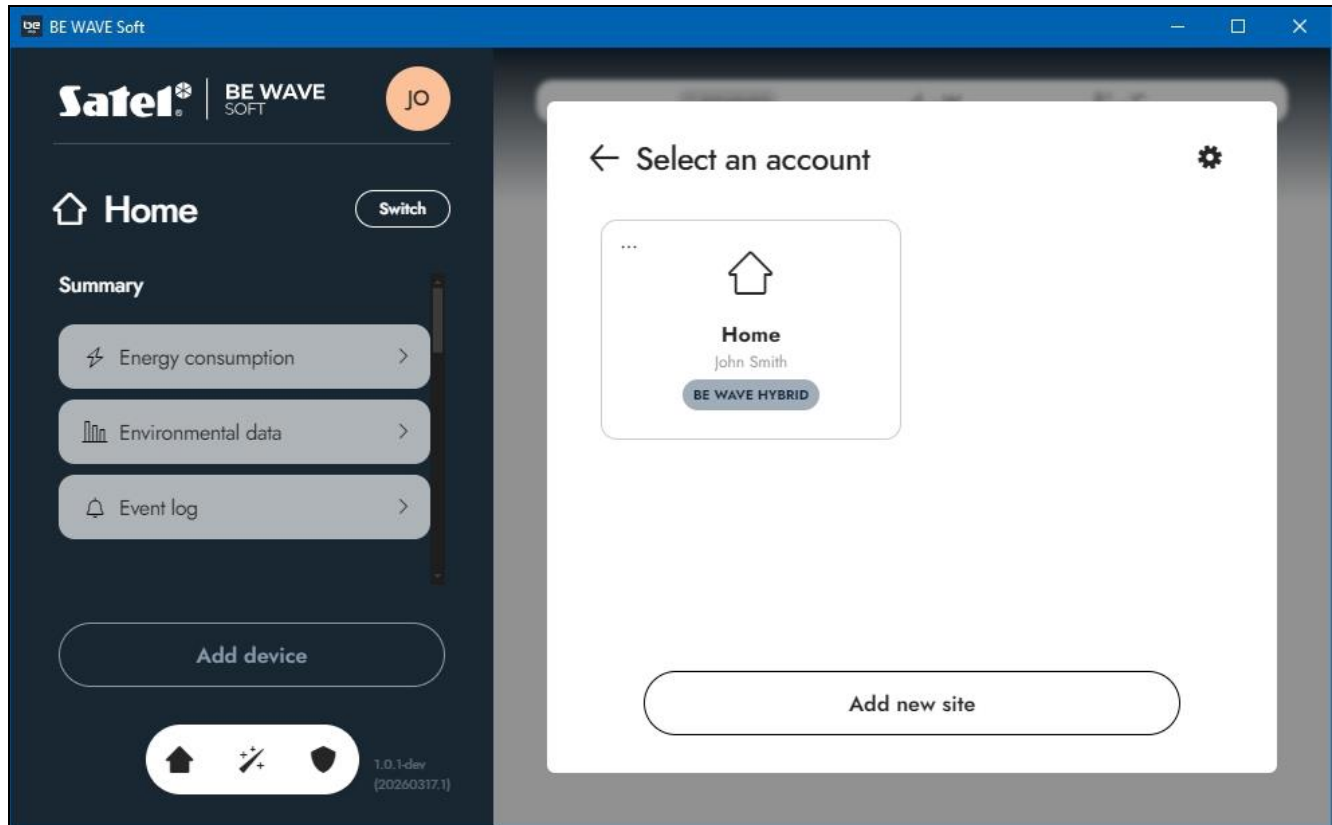
- Click the *Switch* button next to the site name. The *Select an account* window will be displayed.



- Click a blank space inside the window to deselect the site. The *Add new site* button will be displayed at the bottom of the window.



If the control panel is not connected to the local network, connect your computer to the BEWAVE_AP network. The network's full name contains the MAC address of the control panel. Make sure it is the MAC address of the new control panel.



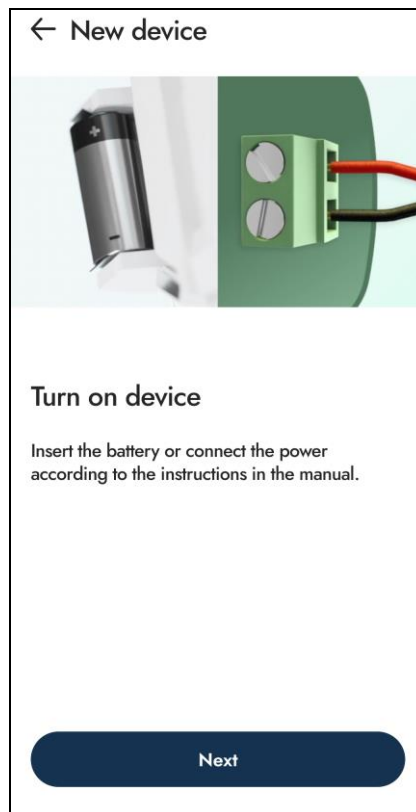
- Click *Add new site*. The *Add new site* window will be displayed.
- In the next steps, the procedure is the same as for adding the first control panel.

5.4 Adding mainboard zones and outputs to the system

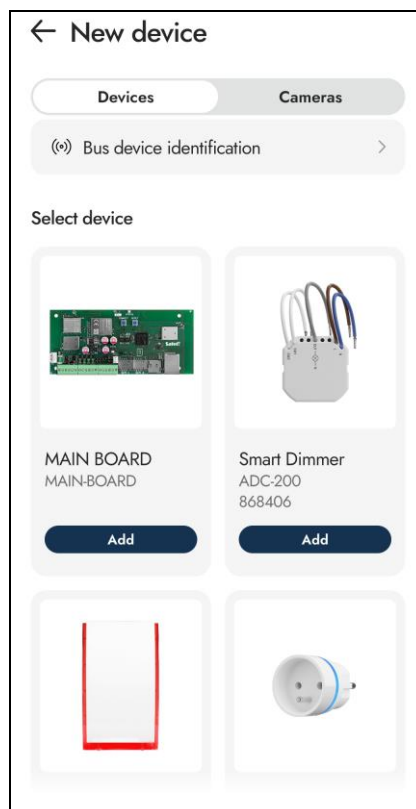
The mainboard zones / outputs must be added to the system so that the system can support the devices connected to them.

5.4.1 Adding mainboard zones and outputs in the Be Wave app

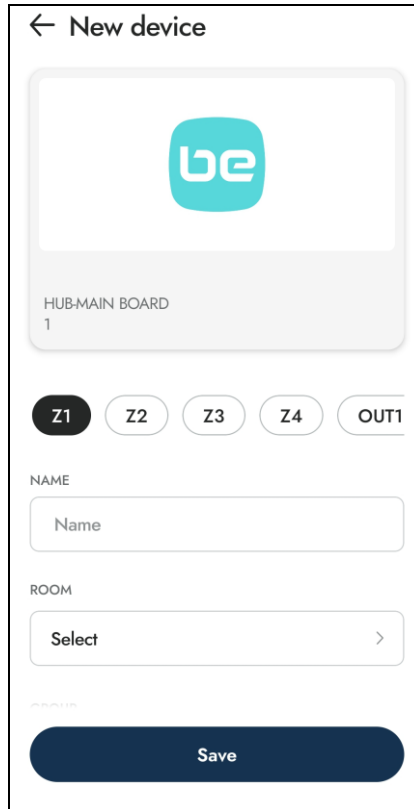
1. Tap the *Add device* button on the home screen. On a new screen you will be asked to turn on the device.



2. Tap *Next*. The list of devices you can add will be displayed (the screenshot is an example).



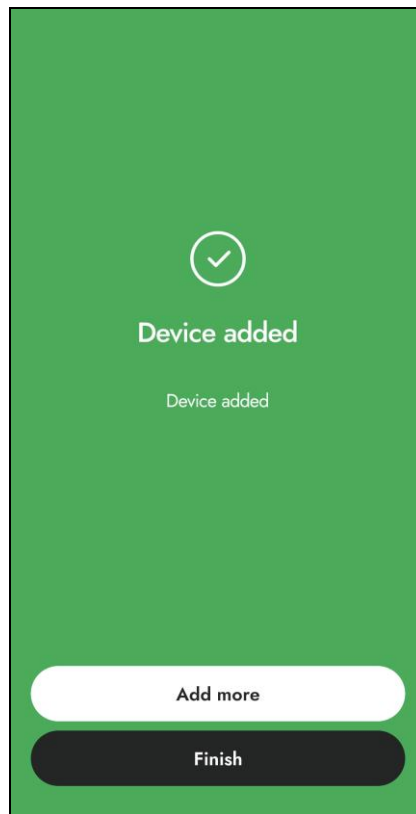
3. Tap *MAIN BOARD*. The screen with mainboard zone / output settings will be displayed.



4. Configure the settings of zones / outputs you want to add to the system (enter the name, assign the zone / output to a room and a group, select the zone type / output operation mode – see “Device settings” p. 62), then tap *Save*.
5. If you have not configured all zones / outputs (channels), a warning will be displayed. You can tap *Cancel* to return to configuring zones / outputs, or tap *Yes* to add the configured zones / outputs to the system.



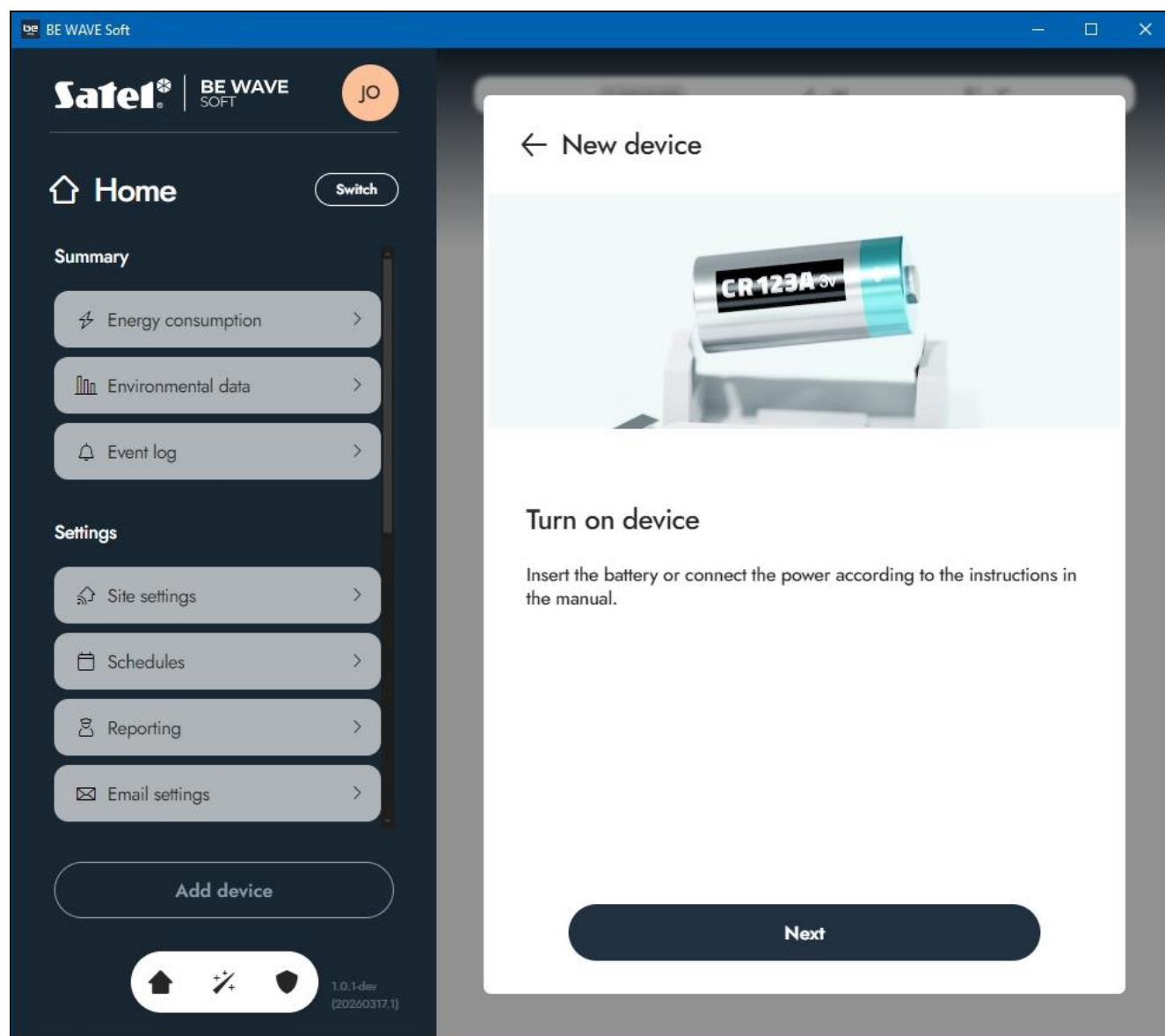
6. If you configured all zones / outputs (channels) or you tapped Yes on the warning screen, a screen will be displayed saying that the device has been added.



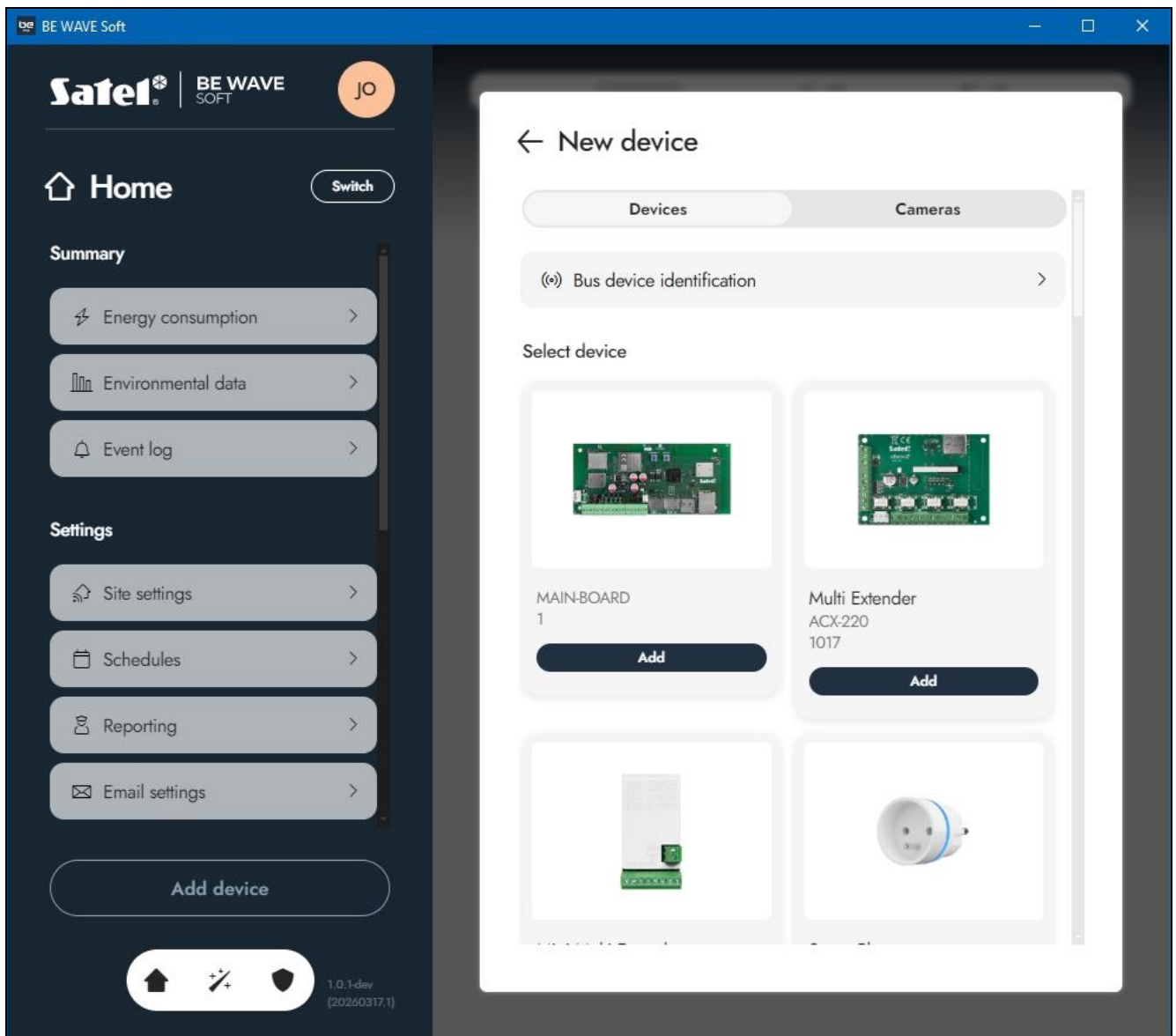
7. Tap *Add more* if you want to add another device or *Finish* if you do not want add any more devices.
8. Configure additional settings if it is required for the zone / output (e.g. output for which the *Alarm* operation mode has been selected require programming the alarm sources – see “Alarm source” p. 67).

5.4.2 Adding the mainboard zones and outputs in the BE WAVE Soft app

1. Click the *Add device* button. In the new window you will be asked to turn on the device.



2. Click *Next*. The list of devices you can add will be displayed (the screenshot is an example).

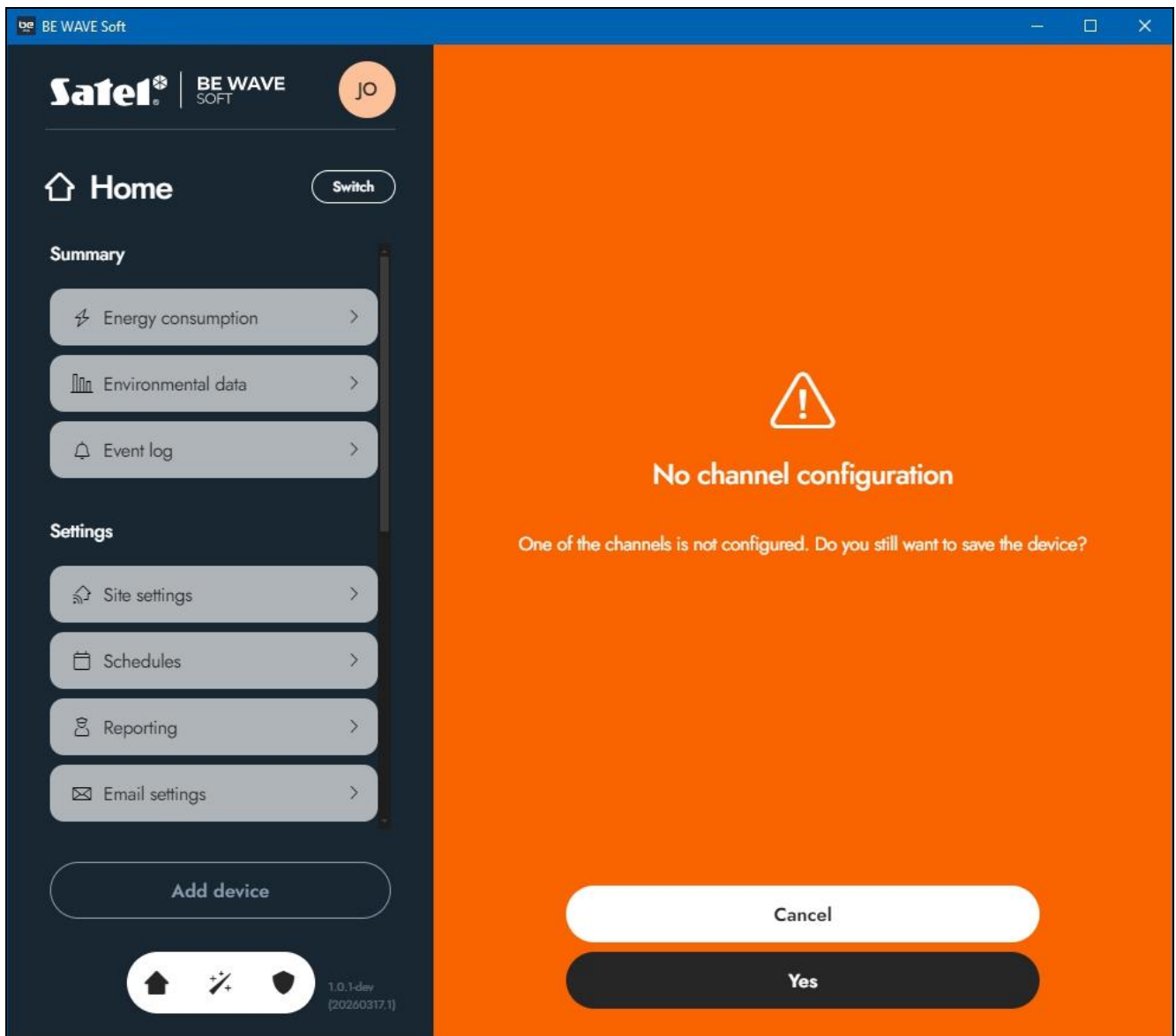


3. Click **MAIN BOARD**. The window with mainboard zones / outputs will be displayed.

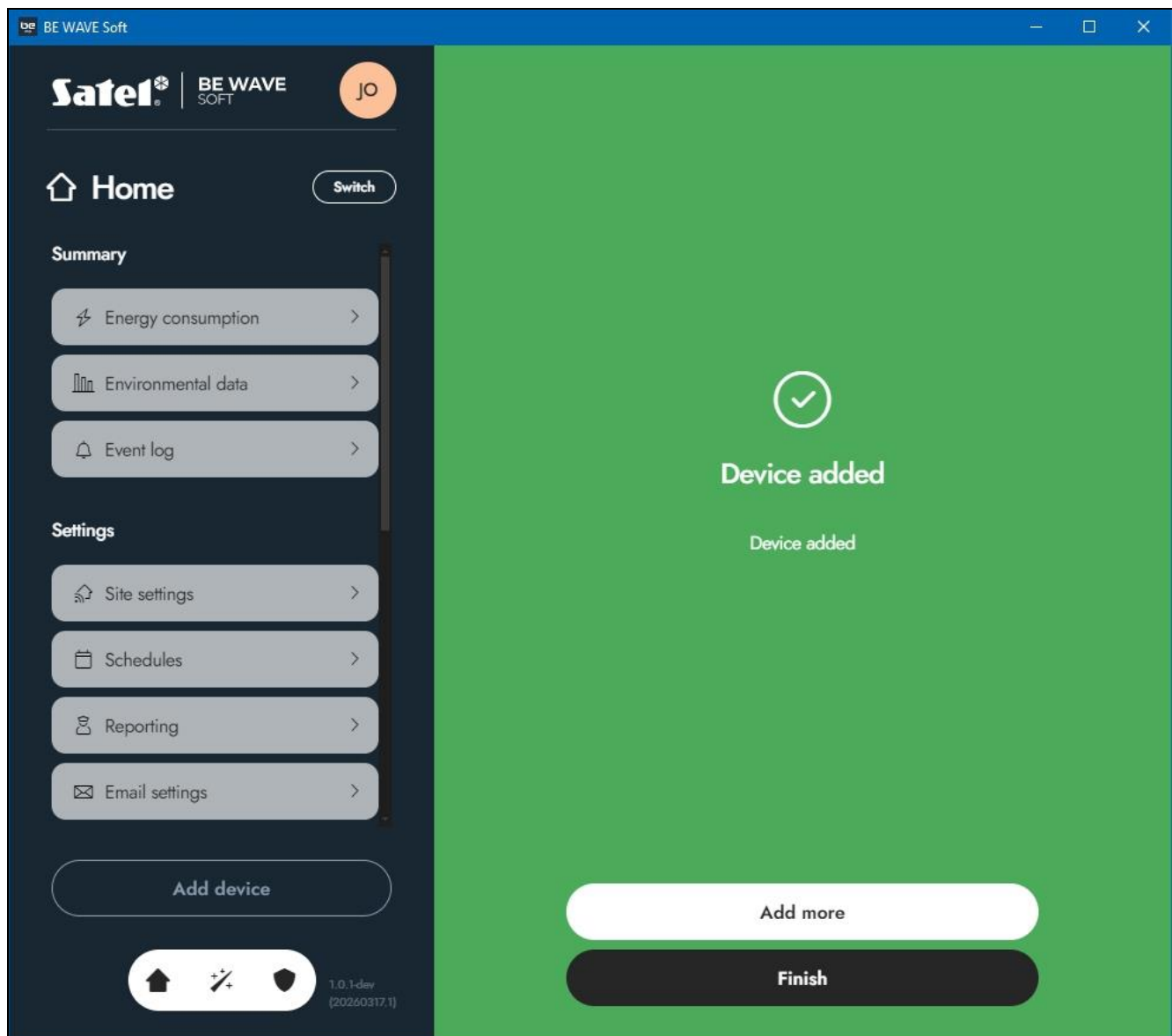
The screenshot displays the SATEL BE WAVE Soft web interface. On the left is a dark sidebar with navigation options: Home, Summary (Energy consumption, Environmental data, Event log), and Settings (Site settings, Schedules, Reporting, Email settings). An 'Add device' button is at the bottom of the sidebar. The main content area is titled 'New device' and shows a configuration form for a 'MAIN-BOARD 1'. It features a row of buttons for selecting a zone or output: Z1 (selected), Z2, Z3, Z4, OUT1, and OUT2. Below these are input fields for 'NAME' (with a placeholder 'Name'), 'ROOM' (with a 'Select' dropdown), and 'GROUP'. A large 'Save' button is at the bottom of the form. The top of the interface shows the SATEL logo, BE WAVE SOFT, and a user profile icon labeled 'JO'.

4. Configure the settings of zones / outputs you want to add to the system (enter the name, assign the zone / output to a room and a group, select the zone type / output operation mode – see “Device settings” p. 62), then click **Save**.

5. If you have not configured all zones / outputs (channels), a warning will be displayed. You can click *Cancel* to return to configuring zones / outputs, or click *Yes* to add the configured zones / outputs to the system.



6. If you configured all zones / outputs (channels) or you clicked Yes in the warning window, a window will be displayed saying that the device has been added.

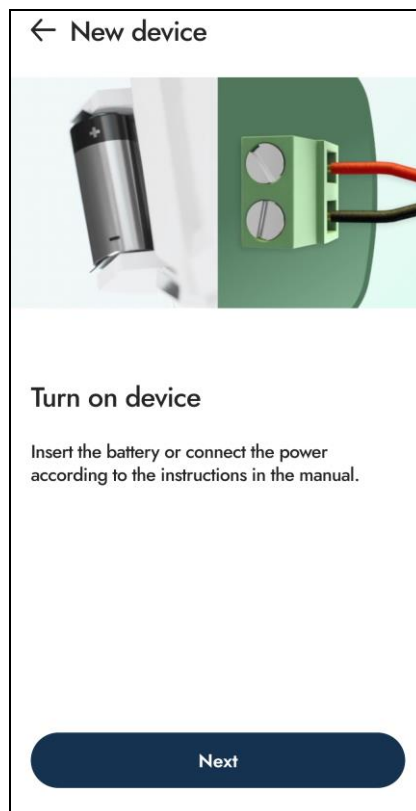


7. Click *Add more* if you want to add another device or *Finish* if you do not want to add any more devices.
8. Configure additional settings if it is required for the zone / output (e.g. output for which the *Alarm* operation mode has been selected require programming the alarm sources – see “Alarm source” p. 67).

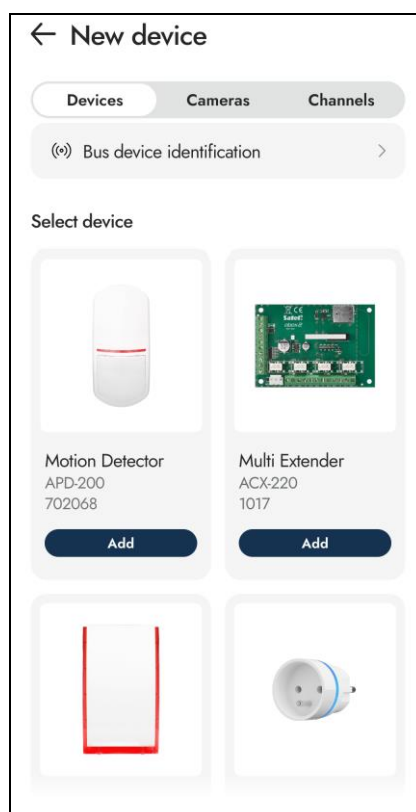
5.5 Adding a bus device to the system

5.5.1 Adding a bus device in the Be Wave app

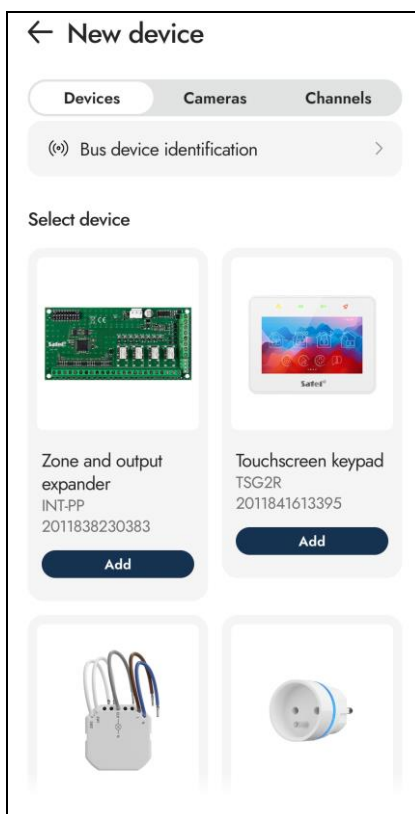
1. Tap the *Add device* button on the room screen, group screen or *Settings* screen. On a new screen you will be asked to turn on the device.



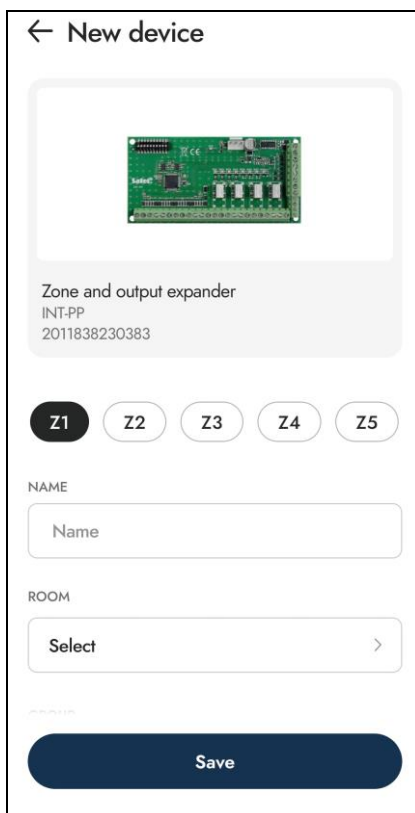
2. Tap *Next*. The list of devices you can add will be displayed (the screenshot is an example).



3. Tap *Bus device identification*. When the identification is completed, the bus devices will appear on the list of devices (the screenshot is an example).

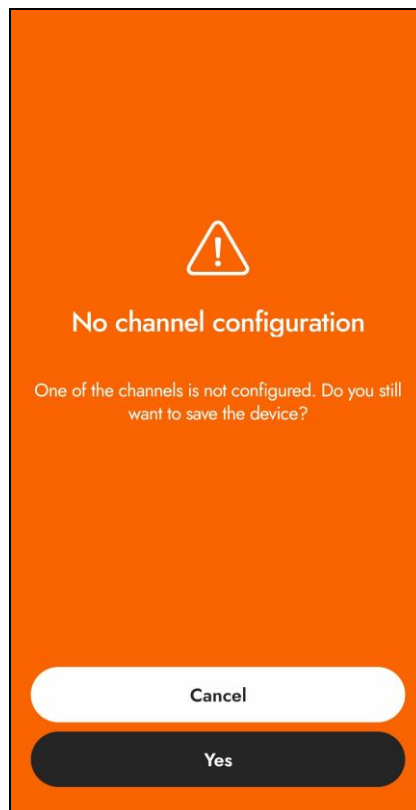


4. Tap the bus device you want to add. A screen with device settings will be displayed (the screenshot is an example).

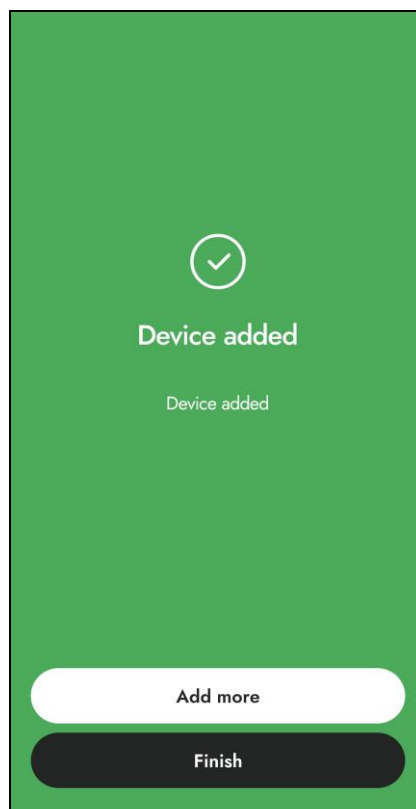


5. Configure the device settings (enter the name, assign the device to a room and to a group, etc. – see “Device settings” p. 62), then tap Save.

6. If the device offers several channels and you have not configured all of them, a warning will be displayed. You can tap *Cancel* to return to configuring the device, or tap *Yes* to add the configured channels.



7. If you configured all channels or you tapped *Yes* on the warning screen, a screen will be displayed saying that the device has been added.

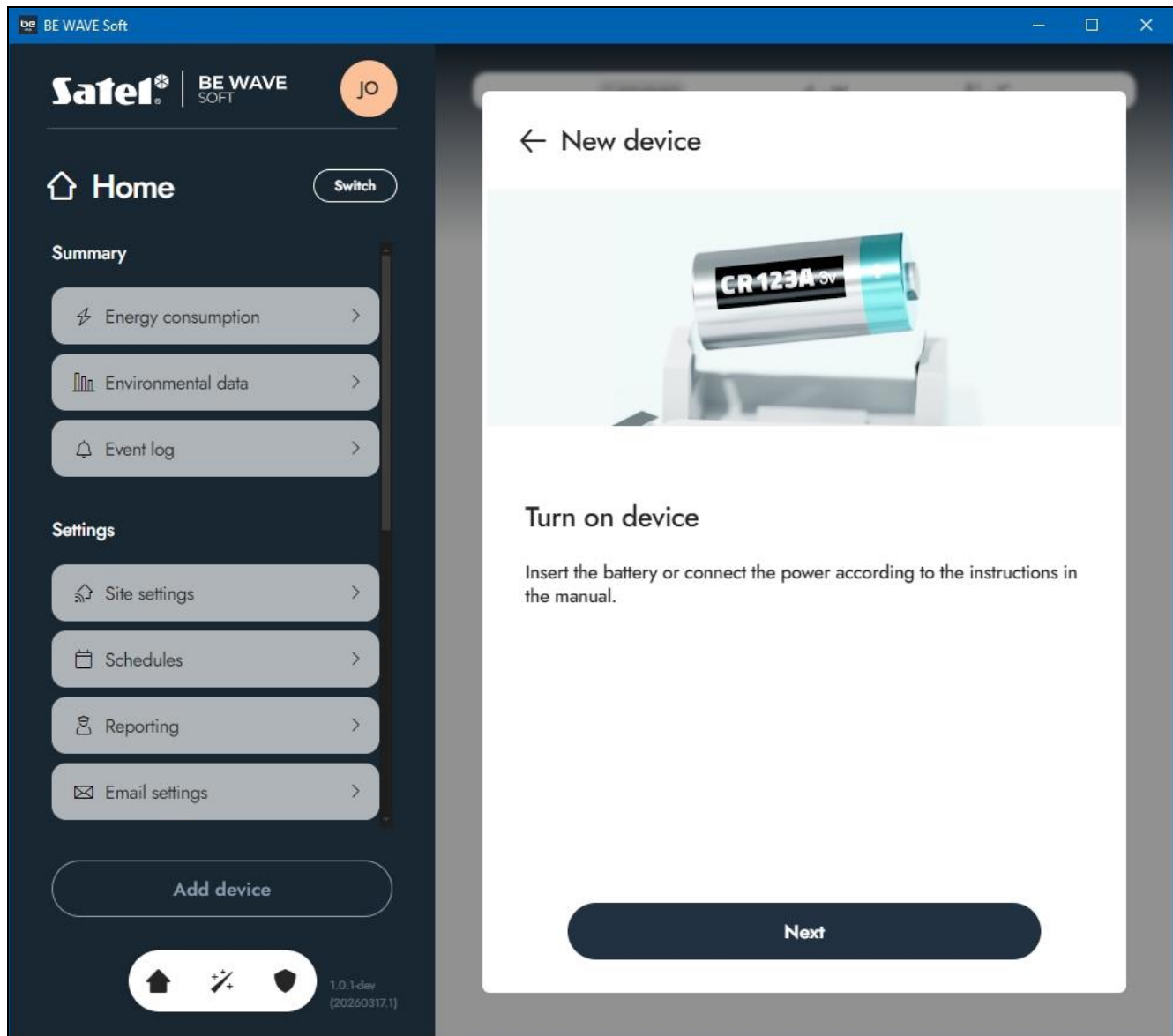


8. Tap *Add more* if you want to add another device or *Finish* if you do not want add any more devices.

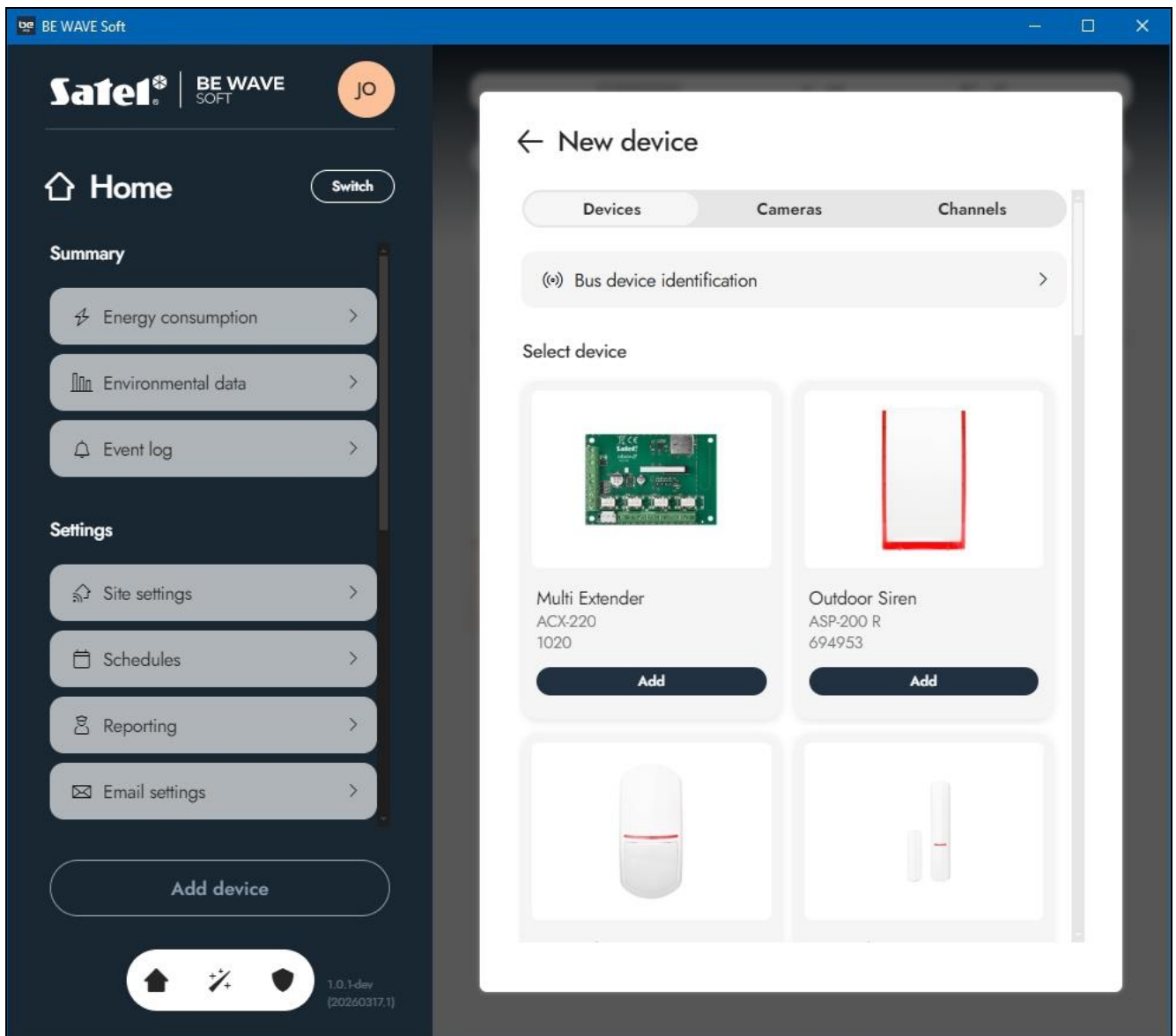
9. Configure additional settings if it is required for the device (e.g. output for which the *Alarm* operation mode has been selected require programming the alarm sources – see “Alarm source” p. 67).

5.5.2 Adding a bus device in the BE WAVE Soft program

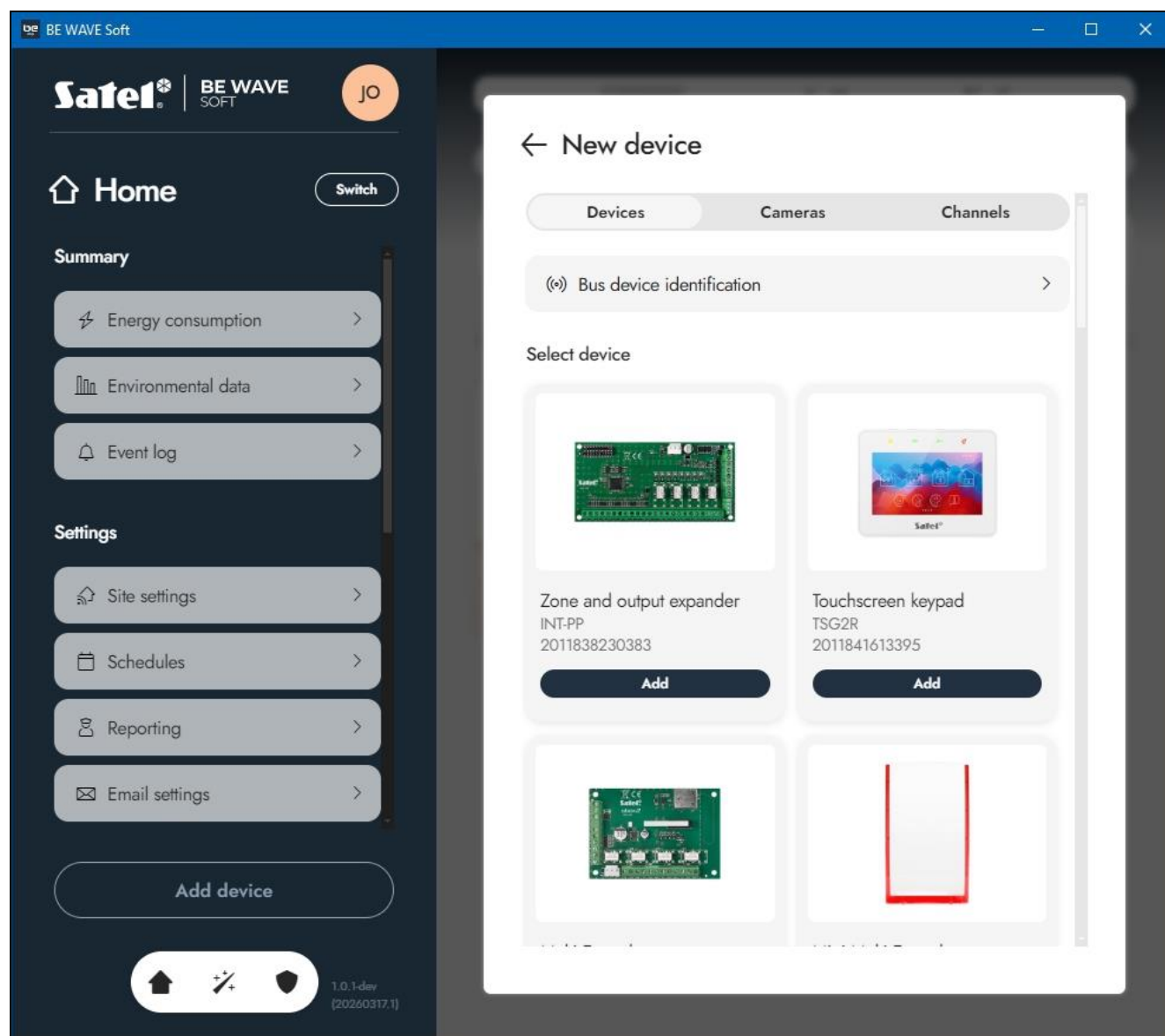
1. Click the *Add device* button on the side menu, in the room window or group window. In the new window you will be asked to turn on the device.



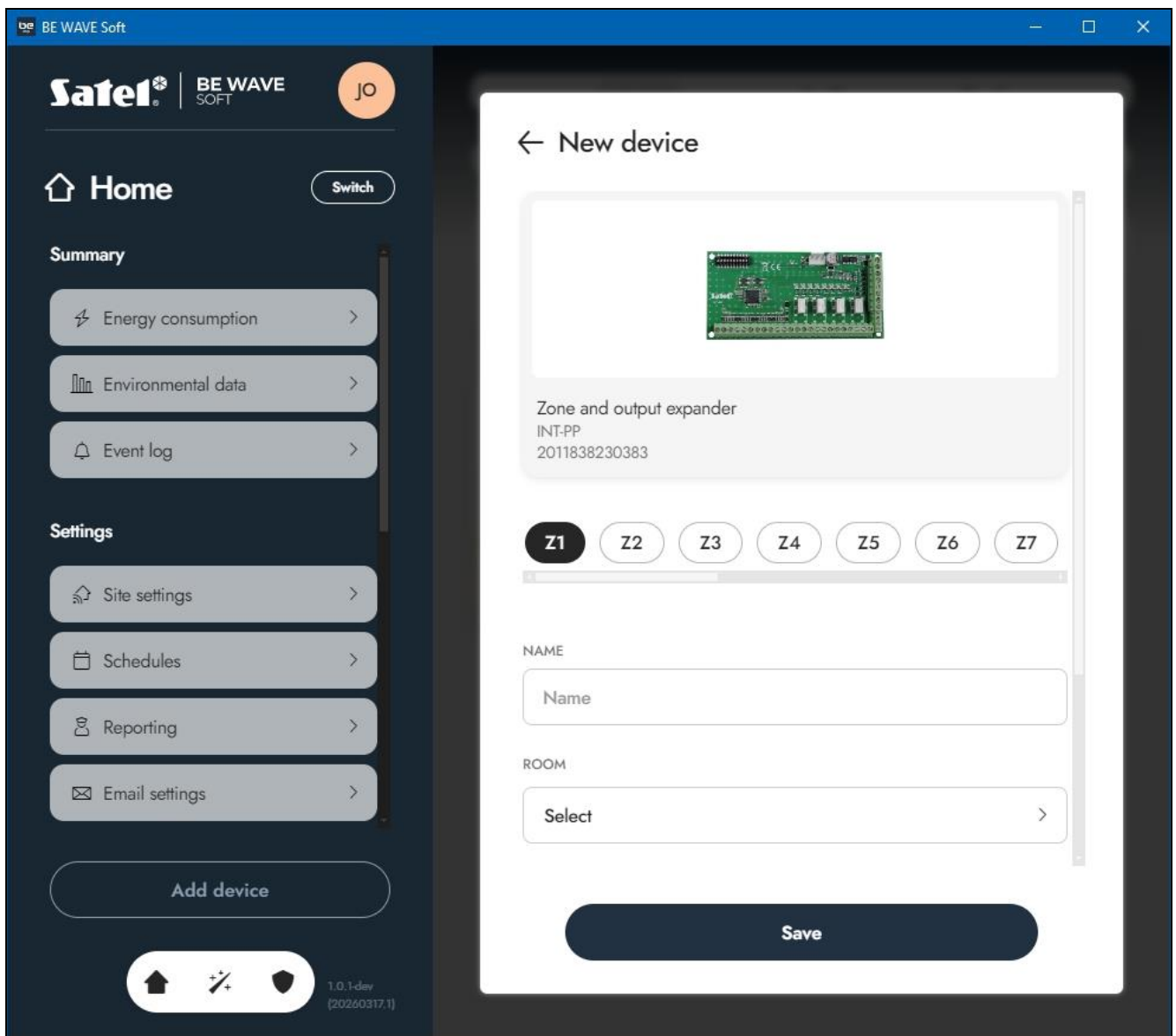
2. Click *Next*. The list of devices you can add will be displayed (the screenshot is an example).



3. Click *Bus device identification*. When the identification is completed, the bus devices will appear on the list of devices (the screenshot is an example).

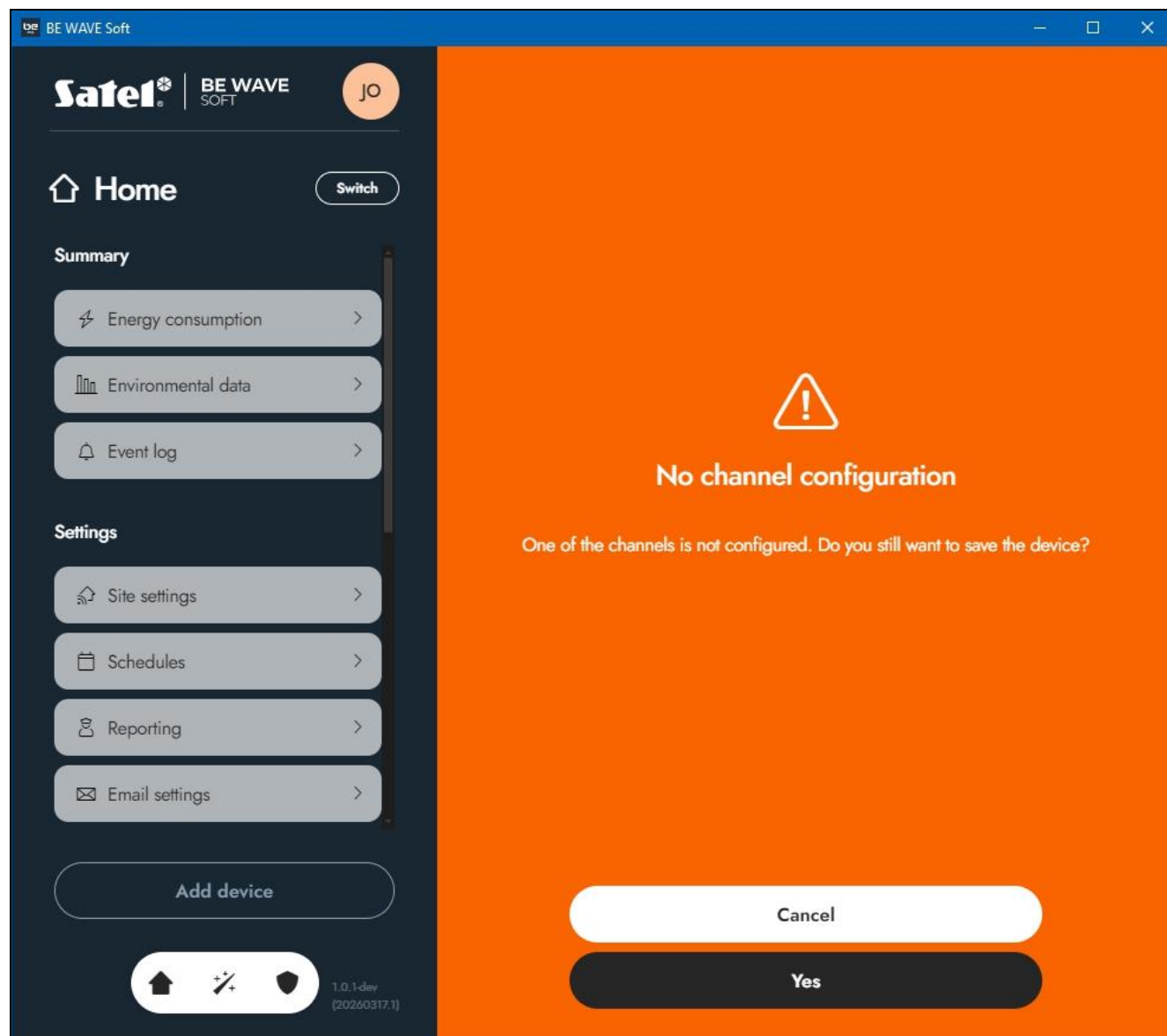


- Click the bus device you want to add. A window with device settings will be displayed (the screenshot is an example).

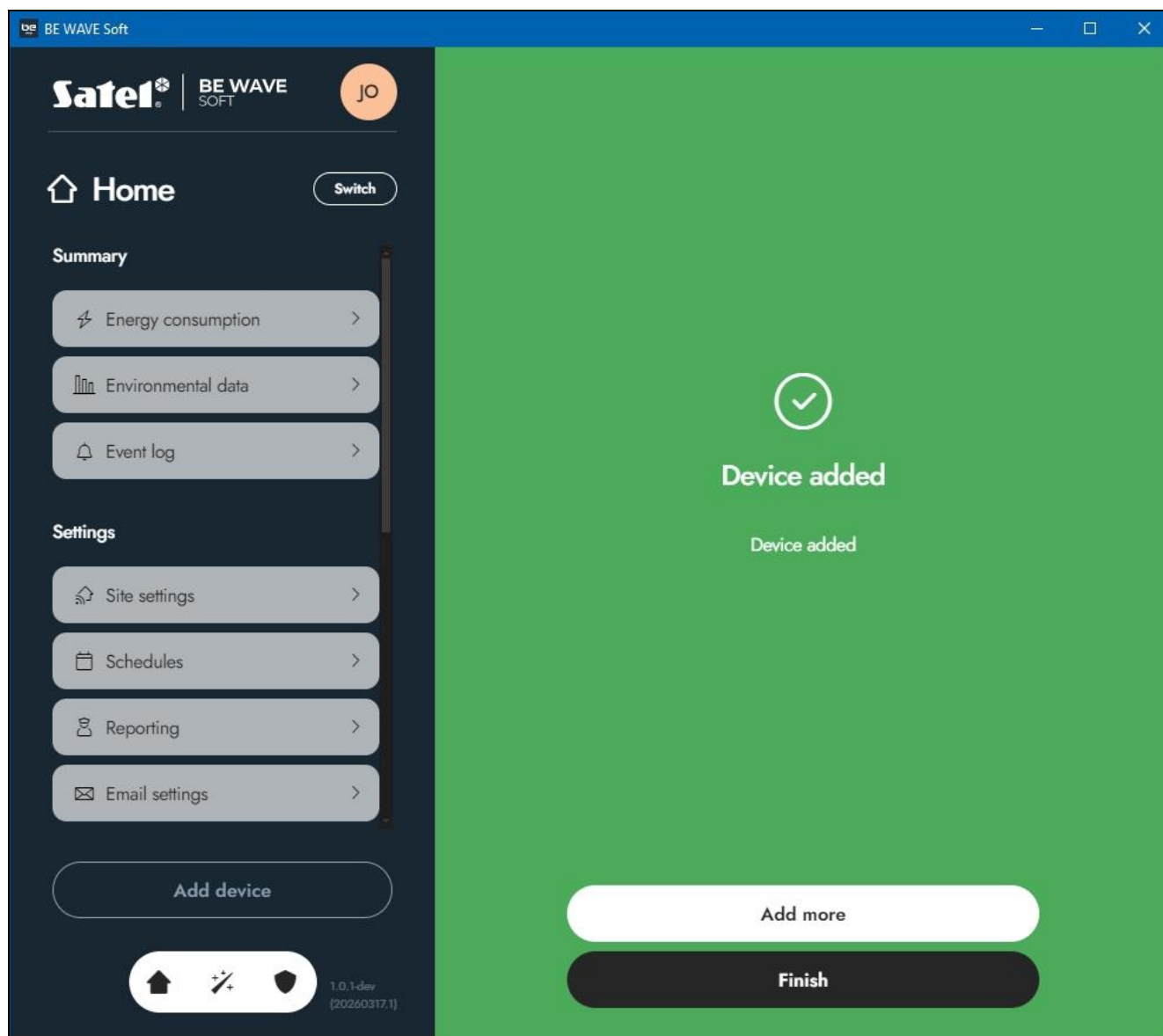


- Configure the device settings (enter the name, assign the device to a room and to a group, etc. – see “Device settings” p. 62), then click Save.

6. If the device offers several channels and you have not configured all of them, a warning will be displayed. You can click *Cancel* to return to configuring the device, or click *Yes* to add the configured channels.



7. If you configured all channels or you clicked Yes in the warning window, a window will be displayed saying that the device has been added.



8. Click *Add more* if you want to add another device or *Finish* if you do not want to add any more devices.
9. Configure additional settings if it is required for the device (e.g. output for which the *Alarm* operation mode has been selected require programming the alarm sources – see “Alarm source” p. 67).

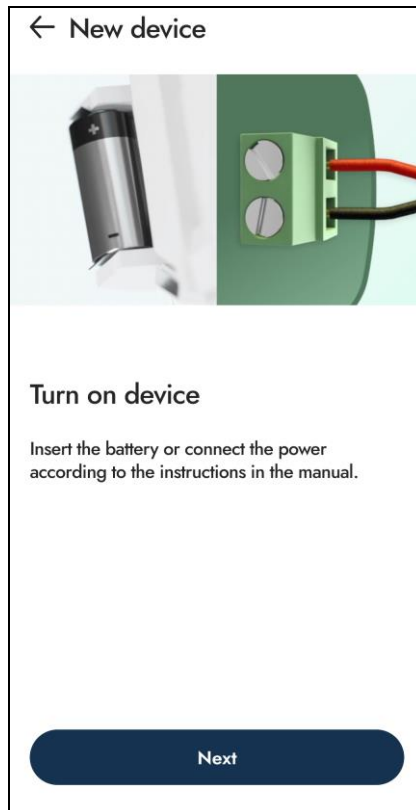
5.6 Adding a wireless device to the system



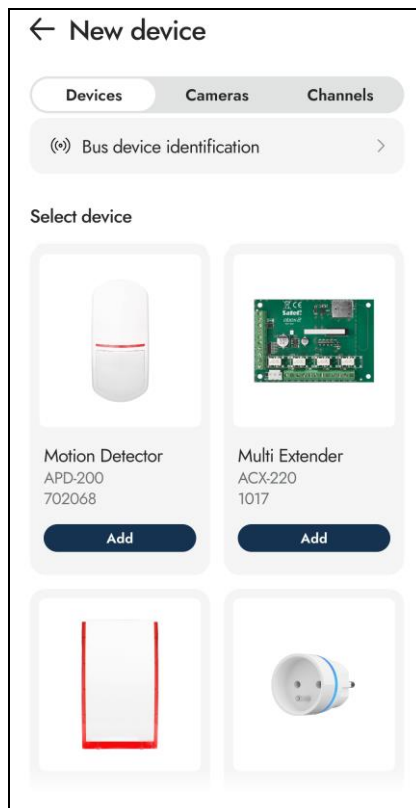
Before adding a device that was previously registered to the BE WAVE / ABAX 2 / ABAX system, you must restart it (remove the battery / power the device off for 30 seconds).

5.6.1 Adding a wireless device in the Be Wave app

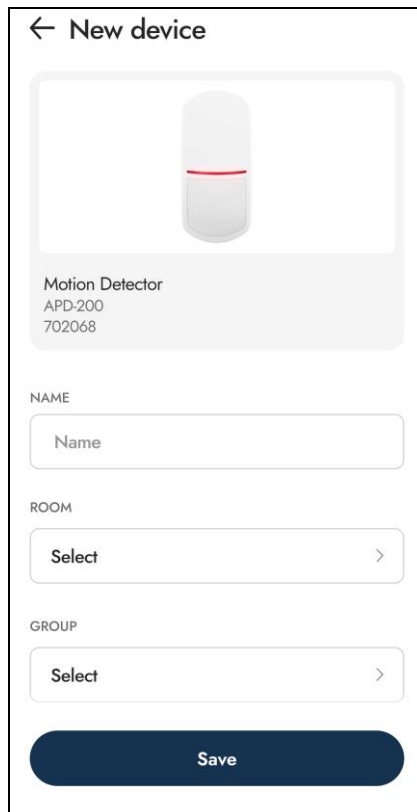
1. Tap the *Add device* button on the room screen, group screen or *Settings* screen. On a new screen you will be asked to turn on the device.



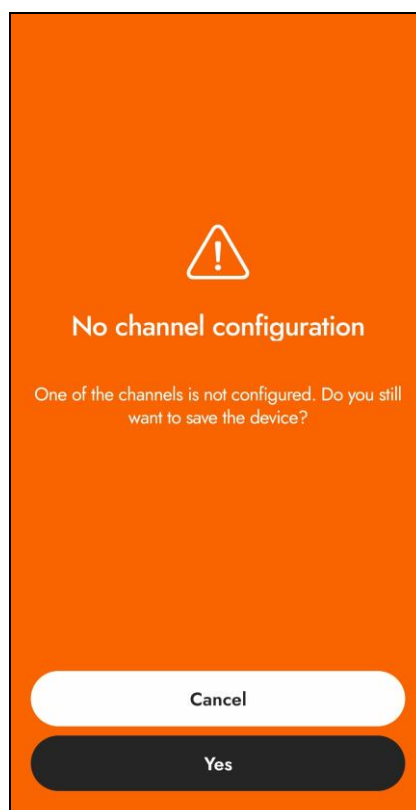
2. Insert the battery, connect the power, etc. (for detailed information, please refer to the manuals of particular devices), then tap *Next*. The list of devices you can add will be displayed (the screenshot is an example).



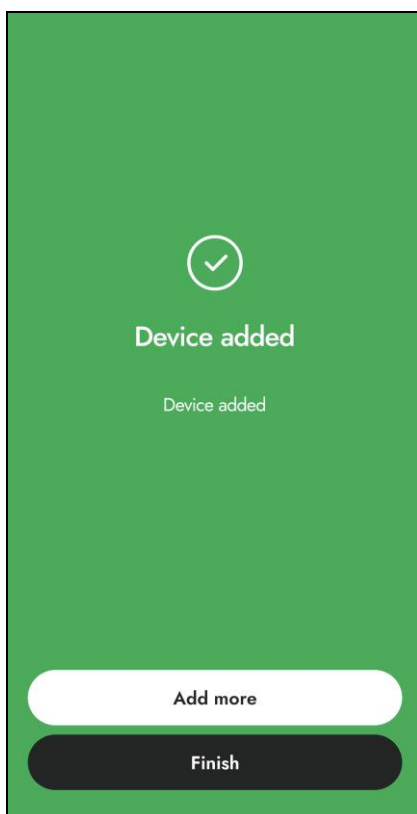
3. Tap the device you want to add. A screen with device settings will be displayed (the screenshot is an example).



4. Configure the device settings (enter the name, assign the device to a room and to a group, etc. – see “Device settings” p. 62), then tap **Save**.
5. If the device offers several channels and you have not configured all of them, a warning will be displayed. You can tap *Cancel* to return to configuring the device, or tap *Yes* to add the configured channels.



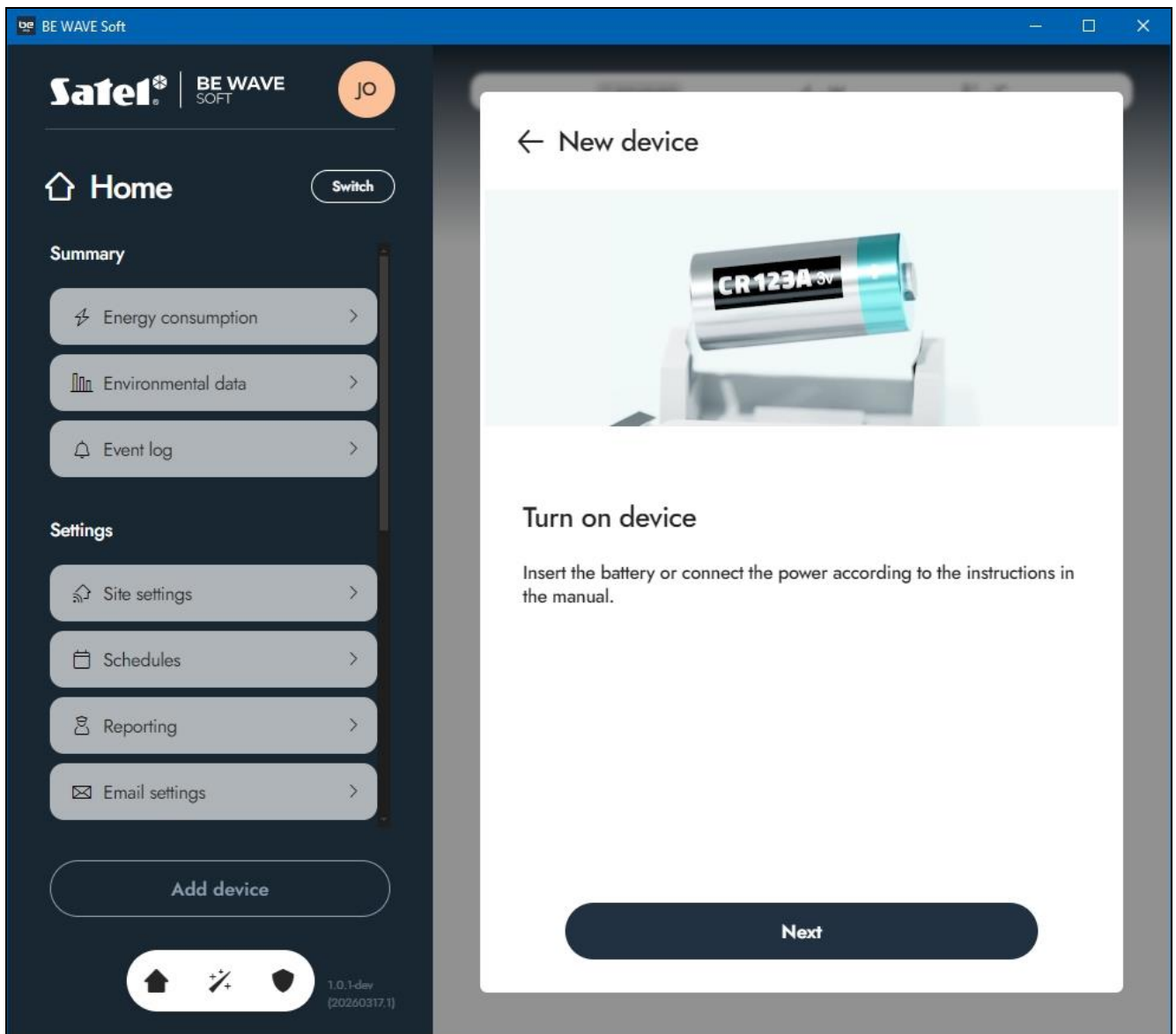
6. If you configured all channels or you tapped Yes on the warning screen, a screen will be displayed saying that the device has been added.



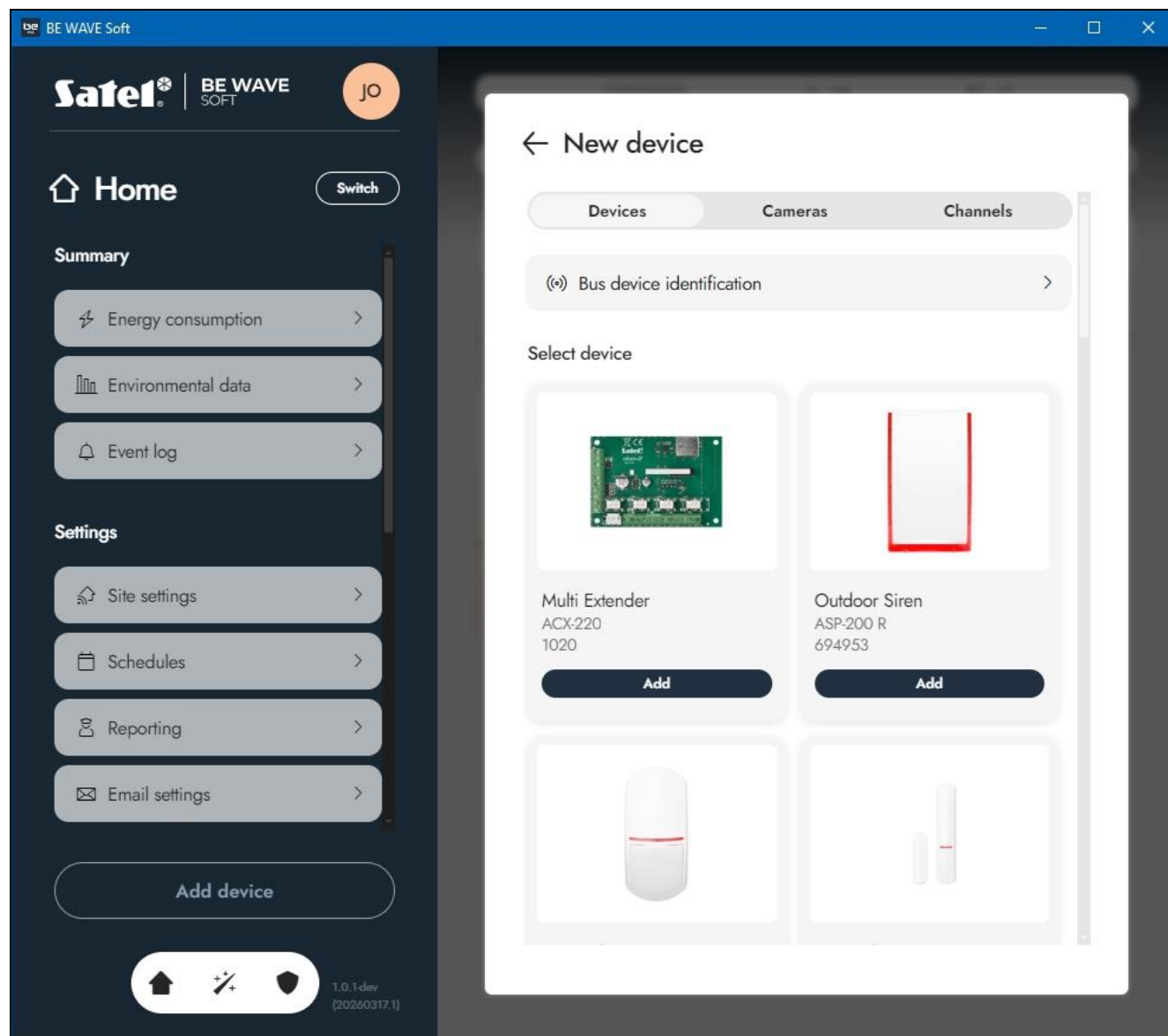
7. Tap *Add more* if you want to add another device or *Finish* if you do not want add any more devices.
8. Configure additional settings if it is required for the device (e.g. sirens and other devices for which the *Alarm* operation mode has been selected require programming the alarm sources – see “Alarm source” p. 67).

5.6.2 Adding a wireless device in the BE WAVE Soft program

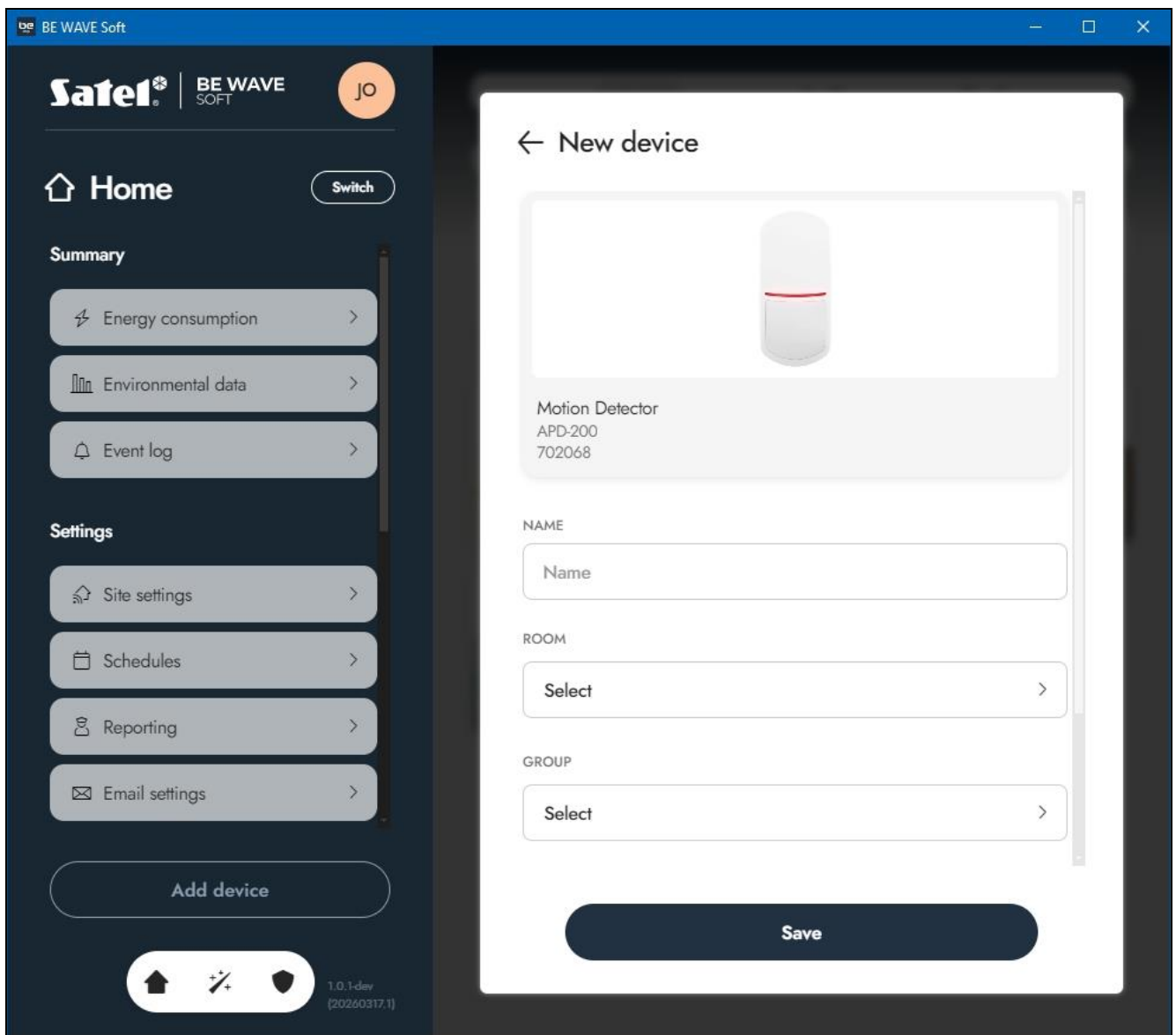
1. Click the *Add device* button on the side menu, in the room window or group window. In the new window you will be asked to turn on the device.



2. Insert the battery, connect the power, etc. (for detailed information, please refer to the manuals of particular devices), then click *Next*. The list of devices you can add will be displayed (the screenshot is an example).

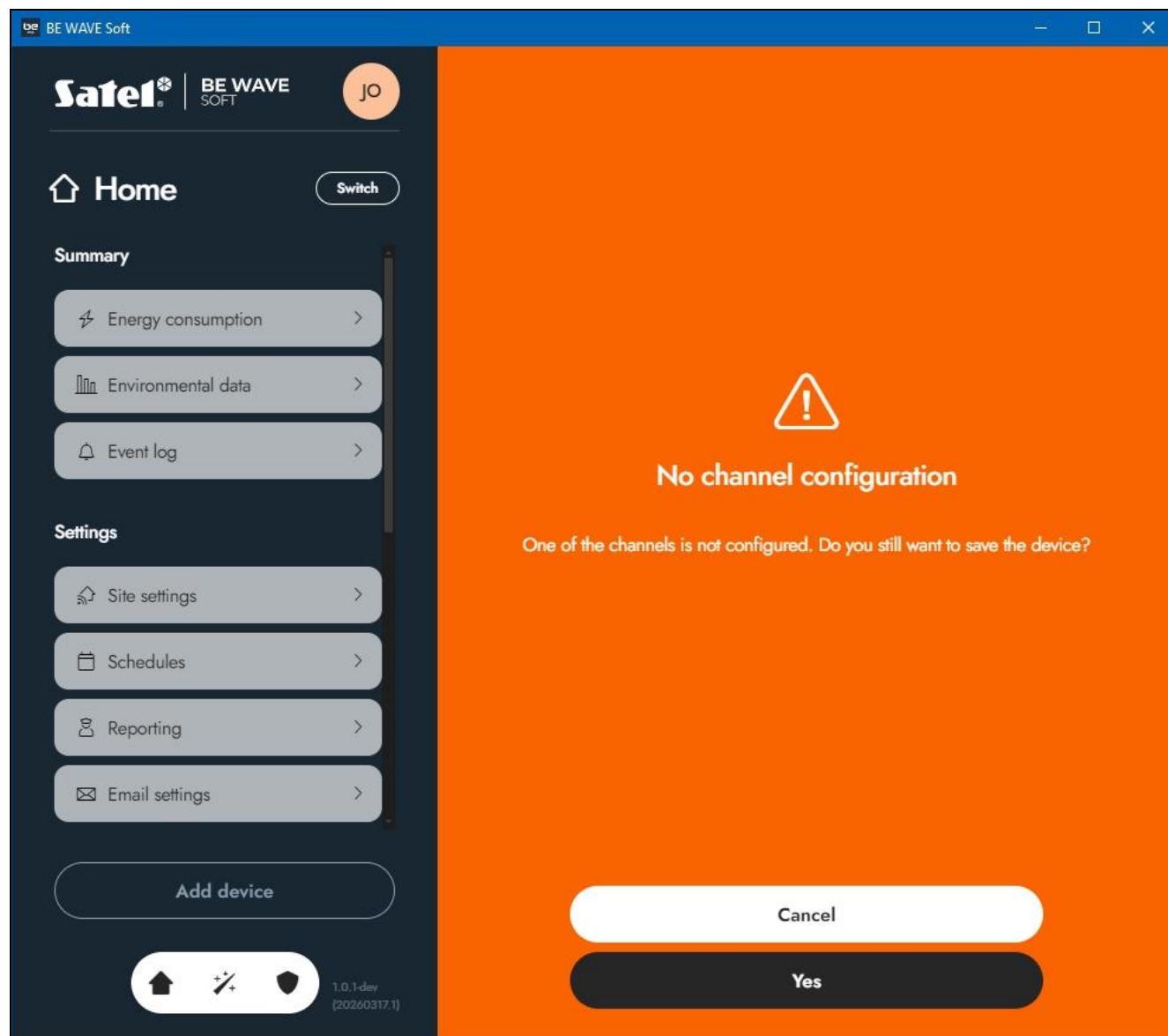


3. Click the device you want to add. A window with device settings will be displayed (the screenshot is an example).

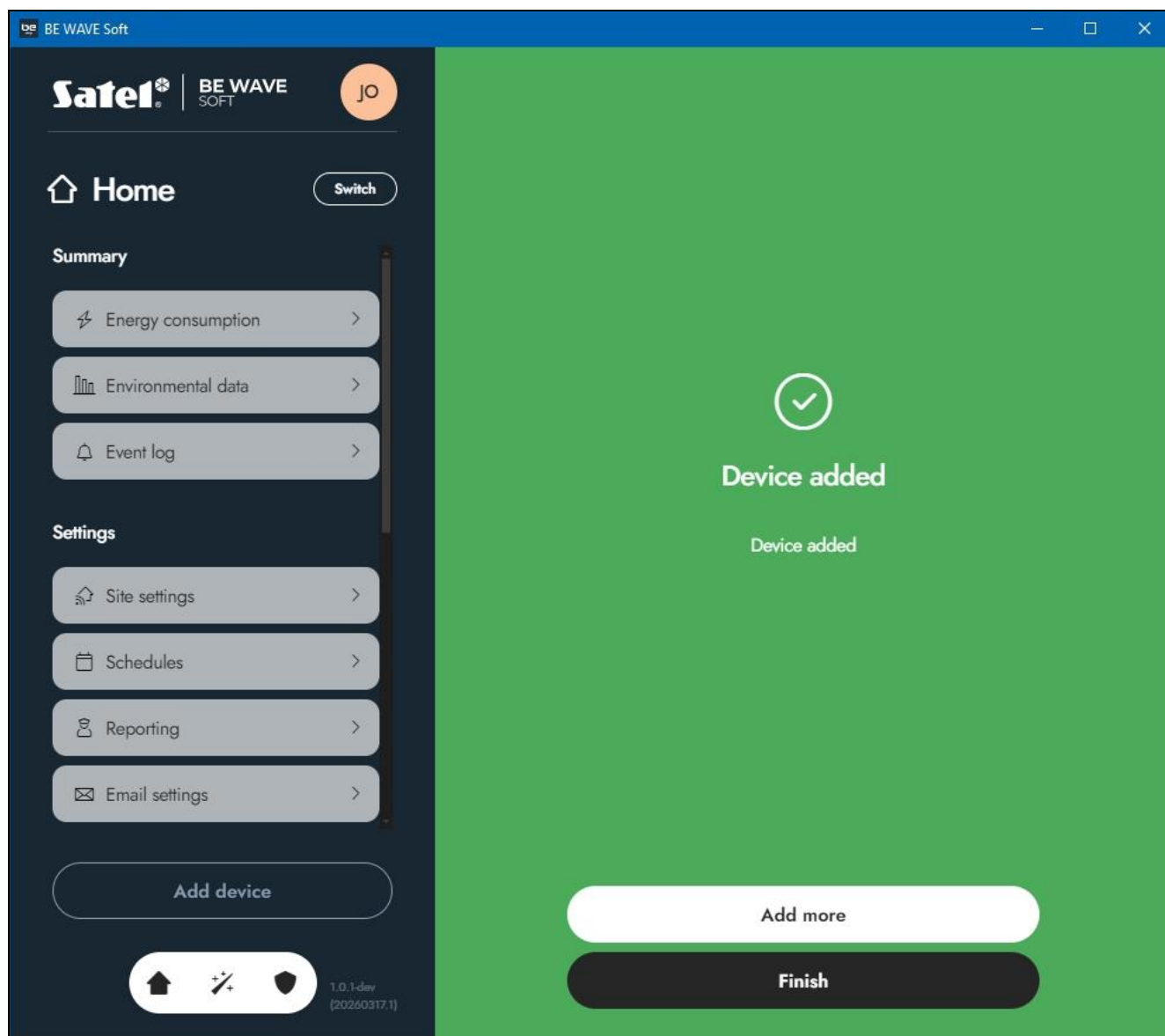


4. Configure the device settings (enter the name, assign the device to a room and to a group, etc. – see “Device settings” p. 62), then click Save.

5. If the device offers several channels and you have not configured all of them, a warning will be displayed. You can click *Cancel* to return to configuring the device, or click *Yes* to add the configured channels.



6. If you configured all channels or you clicked Yes in the warning window, a window will be displayed saying that the device has been added.

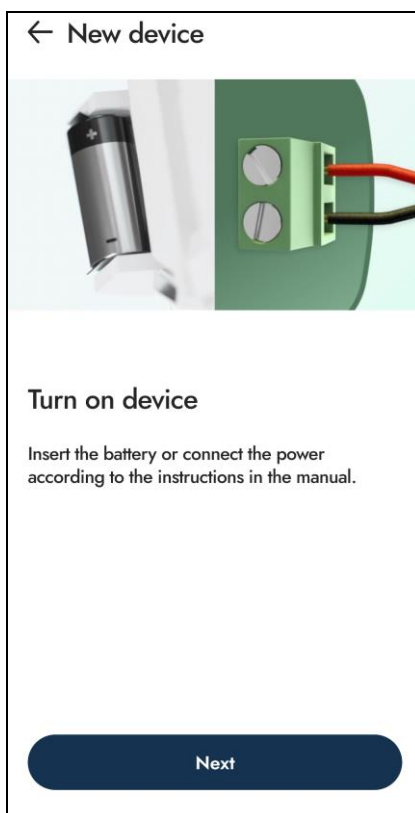


7. Click *Add more* if you want to add another device or *Finish* if you do not want to add any more devices.
8. Configure additional settings if it is required for the device (e.g. sirens and other devices for which the *Alarm* operation mode has been selected require programming the alarm sources – see “Alarm source” p. 67).

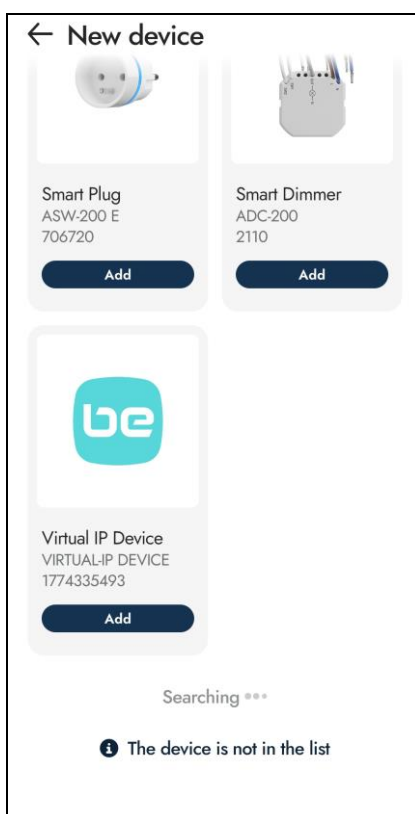
5.7 Adding a virtual IP device to the system

5.7.1 Adding a virtual IP device in the Be Wave app

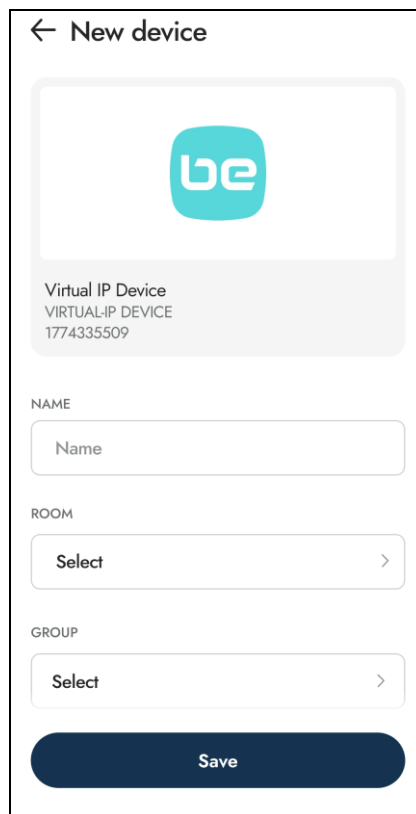
1. Tap the *Add device* button on the room screen, group screen or *Settings* screen. On a new screen you will be asked to turn on the device.



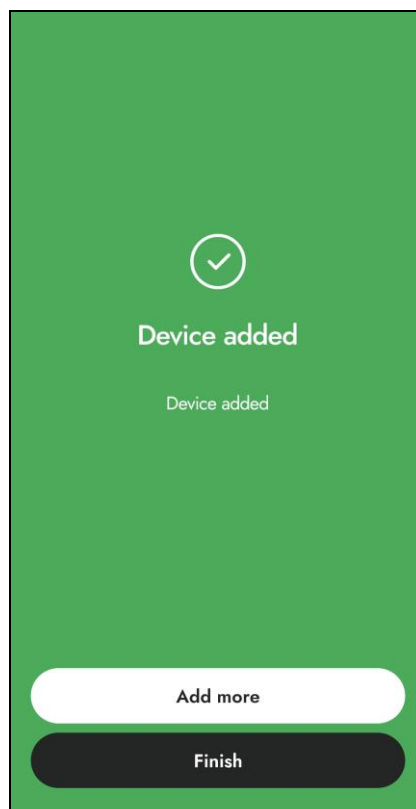
2. Tap *Next*. The list of devices you can add will be displayed (the screenshot is an example).



3. Tap *Virtual IP Device*. A screen with IP device settings will be displayed (the screenshot is an example).



4. Configure the IP device settings (enter the name, assign the device to a room and to a group and select the zone type – see “Device settings” p. 62), then tap *Save*. A screen will be displayed saying that the device has been added.

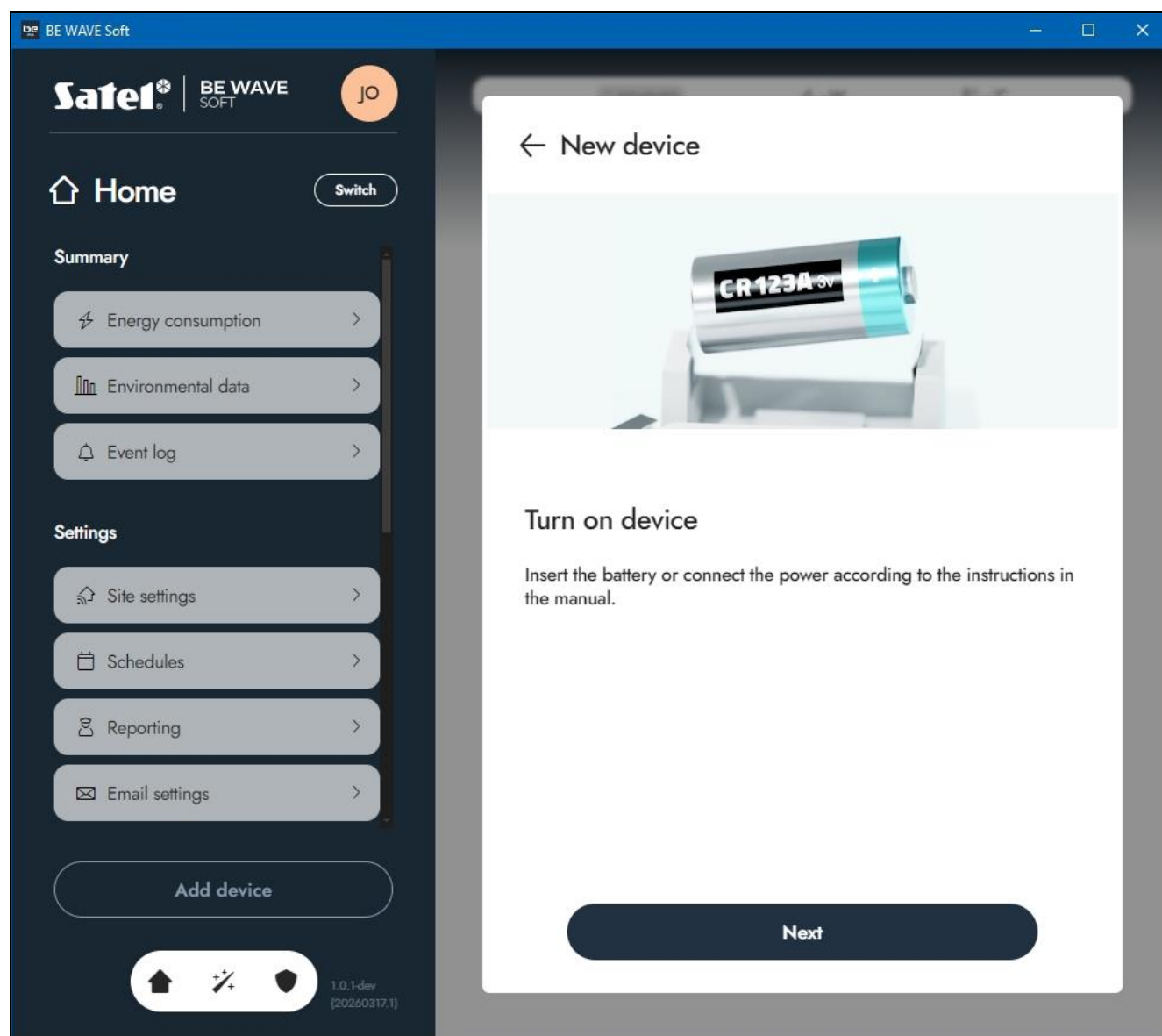


5. Tap *Add more* if you want to add another device or *Finish* if you do not want add any more devices.

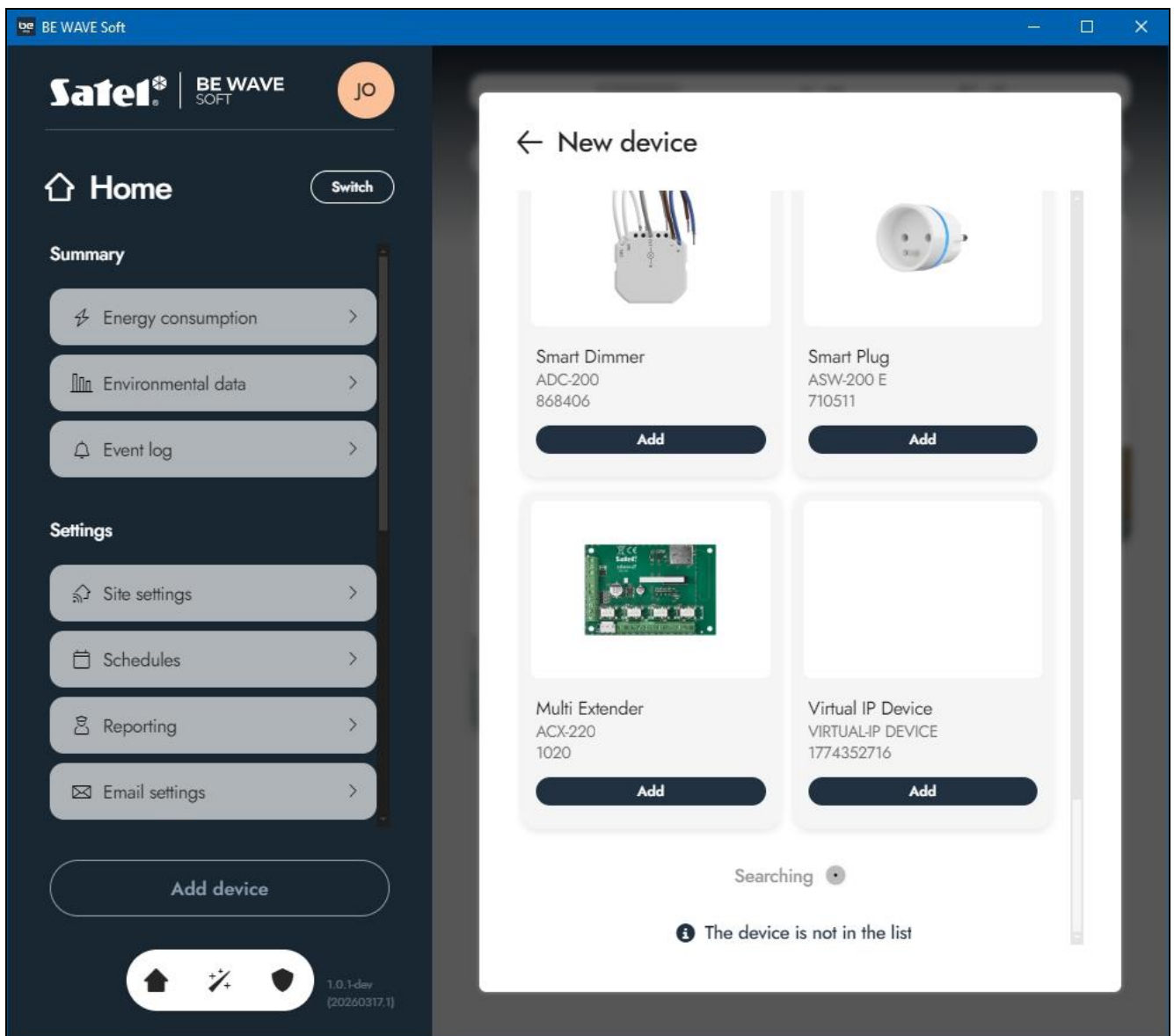
6. Configure additional settings of the IP device (see “IP device settings” p. 67).

5.7.2 Adding a virtual IP device in the BE WAVE Soft program

1. Click the *Add device* button on the side menu, in the room window or group window. In the new window you will be asked to turn on the device.



2. Click *Next*. The list of devices you can add will be displayed (the screenshot is an example).



3. Click *Virtual IP Device*. A window with IP device settings will be displayed (the screenshot is an example).

The screenshot displays the SATEL BE WAVE Soft web interface. On the left is a dark sidebar with the SATEL logo, user 'JO', and navigation links: Home, Summary (Energy consumption, Environmental data, Event log), and Settings (Site settings, Schedules, Reporting, Email settings). An 'Add device' button is at the bottom of the sidebar. The main area shows a 'New device' modal window. Inside this window, there is a preview of a 'Virtual IP Device' with ID '1774352756'. Below the preview are three form fields: 'NAME' (with a 'Name' placeholder), 'ROOM' (a dropdown menu), and 'GROUP' (another dropdown menu). A large 'Save' button is positioned at the bottom of the modal.

BE WAVE Soft

SATEL® | BE WAVE SOFT

JO

Home

Switch

Summary

- Energy consumption
- Environmental data
- Event log

Settings

- Site settings
- Schedules
- Reporting
- Email settings

Add device

1.0.1-dev (20260317.1)

← New device

Virtual IP Device
VIRTUAL-IP DEVICE
1774352756

NAME

Name

ROOM

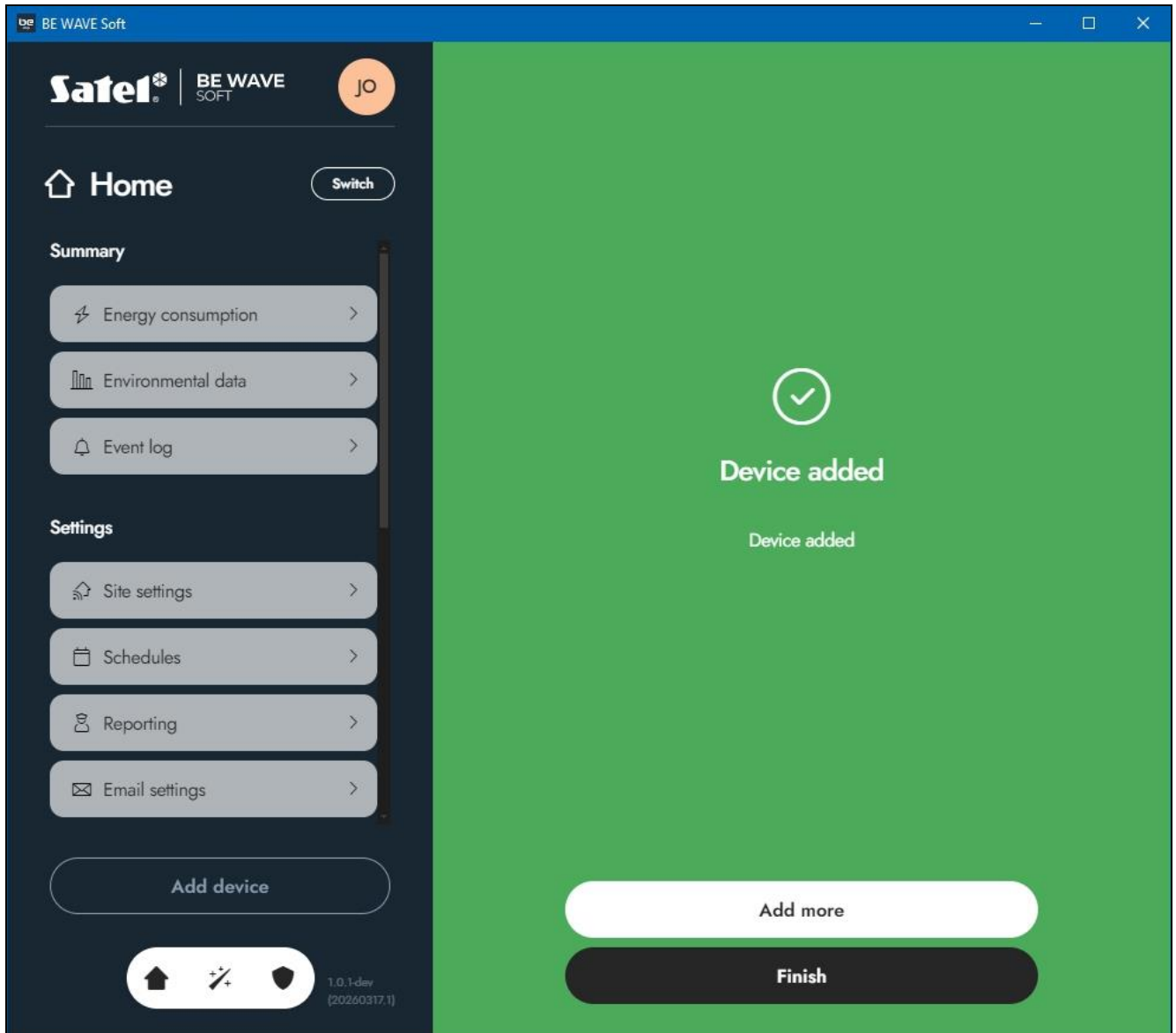
Select

GROUP

Select

Save

4. Configure the IP device settings (enter the name, assign the device to a room and to a group and select the zone type – see “Device settings” p. 62), then click **Save**. A window will be displayed saying that the device has been added.



5. Click *Add more* if you want to add another device or *Finish* if you do not want to add any more devices.
6. Configure additional settings of the IP device (see “IP device settings” p. 67).

5.8 Removing the device from the system

5.8.1 Deleting a device in the Be Wave app

1. Tap the room or group in which you want to delete a device. The room / group screen will be displayed.
2. Tap the device you want to delete. The device screen will be displayed.
3. Tap *Delete device*. You will be asked for confirmation.
4. Tap *Yes*. The device will be deleted.

5.8.2 Deleting a device in the BE WAVE Soft program

1. Click the room or group in which you want to delete a device. The room / group window will be displayed.

2. Click the device you want to delete. The device window will be displayed.
3. Click *Delete device*. You will be asked for confirmation.
4. Click Yes. The device will be deleted.

5.9 Description of settings

5.9.1 Device settings

The settings described in this section are available when adding a device or after tapping / clicking the *Edit device* button ([room] / [group] >[device] >*Edit device*).

Name – individual device name.

Room – room in which the device is installed.

Working mode – parameter for:

- AXD-200 detector (Multipurpose Detector). Select the purpose of the detector:

Shock detector – to detect shocks.

Opening detector – to detect the opening of a door or window. You can also connect a wired NC detector to it (e.g. a wired opening detector).

Shock and opening detector – to detect shocks and the opening of a door or window. You can also connect a wired NC detector to it (e.g. a wired opening detector).

Flood detector – to detect indoor water flooding.

Temperature sensor – to measure air temperature.

Roller shutter detector – to detect the opening of a door or window. You can also connect a wired roller shutter detector and a wired NC detector to it (e.g. a wired opening detector).

- ARC-200 controller (Smart RGBW LED Driver). Select the purpose of the controller:

RGB – to control an RGB LED strip.

RGBW – to control an RGBW LED strip.

COLD/WARM – to control a CCT LED strip.

MONO – to control a single color LED strip / LED bulb / halogen bulb.

- ARSC-200 controller (Smart Blinds). Select the purpose of the controller:

Blind – to open / close venetian blinds.

Shutter – to open / close roller shutters.

Window actuator – to open / close electric windows.

Group – group of devices to which the device belongs.

Operation mode – this parameter defines when the output / device is to be turned on.

Alarm – output / device is turned on after alarm is generated in the system. Programming of these settings is required: *Operating time* and *Alarm source*.

BI switch – after activation, the output / device changes its status to the opposite:

- if it was turned off, it will be turned on,
- if it was turned on, it will be turned off.

MONO switch – output / device is turned on for a programmed time. Programming of the *Operating time* parameter is required.

Thermostat cooling – output / device is turned on when the temperature rises above the set temperature. Programming of temperature is required.

Thermostat heating – output / device is turned on when the temperature drops below the set temperature. Programming of temperature is required.



If programming of additional parameters is required, they are available in the app / program after tapping / clicking the device.

Zone type – parameter for detectors, buttons and zones. In the description below, the general term “zone” is used. Select the zone type to define the reaction to detector violation, button pressing, zone violation, etc.:

Instant – when the zone is armed, zone violation will generate an alarm. Typically, this zone type is used for outdoor motion detectors and detectors protecting windows.

Entry/Exit – when the *Exit delay* countdown is running, zone violation will not generate an alarm. When the zone is armed, zone violation will start the *Entry delay* countdown. The system must be disarmed before the *Entry delay* is over. Otherwise, an alarm will be generated. Typically, this zone type is used for detectors protecting entrances/exits (e.g. front doors).

Interior delayed – when *Entry delay* is running, zone violation will start the *Delay time* countdown. The system must be disarmed before the *Delay time* is over. Otherwise, an alarm will be generated. When the zone is armed but the *Entry delay* countdown is not running, zone violation will generate an alarm. Typically, this zone type is used for indoor motion detectors and detectors protecting internal doors.

No alarm actions – zone violation will trigger no direct reaction. This zone can be used to run routines.

24h audible alarm – zone violation will generate an audible alarm. This zone type is intended for detectors that are to be always armed and generate loud alarms.

24h tamper alarm – zone violation will generate a tamper alarm and trouble. This zone type is intended for tamper circuits control.

24h panic alarm – zone violation will generate a panic alarm. This zone type is intended for panic buttons.

24h silent alarm – zone violation will generate a silent panic alarm. Loud signaling will not be triggered but the event code can be sent to the monitoring station. This zone type is intended for panic buttons.

24h medical alarm – zone violation will generate a medical alarm. This zone type is intended for emergency call buttons.

24h fire alarm – zone violation will generate a fire alarm. This zone type is intended for fire detectors.

24h flood alarm – zone violation will generate a flood alarm. This zone type is intended for flood detectors.

Trouble – zone violation will generate a trouble. Zone restore means trouble restore.

Tamper – system reaction to device tamper:

Trouble only – device tamper only generates a trouble.

Loud alarm only when armed – device tamper generates a loud alarm only when the device is armed.

Always loud alarm – device tamper always generates a loud alarm.

Lighting type – parameter for the ADC-200 dimmer (Smart Dimmer). Select the light source connected to the dimmer:

Conventional / LED bulb – conventional filament bulb, halogen bulb or LED bulb.

With transformer – light source powered by an electronic or magnetic transformer.

Autodetection – dimmer will automatically recognize the type of connected load.

Type – parameter for:

– ADC-200 dimmer (Smart Dimmer) / ARC-200 controller (Smart RGBW LED Driver):

None – no button is connected to the input.

Single – a single button is connected to the input.

Double – a double button is connected to the input.

- zone / ASW-210 controller (Smart 2-CH Relay) / ASW-220 controller (Smart 2-CH Relay PM):

None – no button is connected to the input.

Single – a single button is connected to the input.

Button type – parameter for the zone / ADC-200 dimmer (Smart Dimmer) / ARC-200 controller (Smart RGBW LED Driver) / ASW-210 controller (Smart 2-CH Relay) / ASW-220 controller (Smart 2-CH Relay PM), if *Single* was selected for the button type, and the ATX-200 module (Smart Switch Controller). Specifies the type of the connected single button:

Switch

Bell

Local control – option for the ADC-200 dimmer (Smart Dimmer) / ARC-200 controller (Smart RGBW LED Driver) / ASW-210 controller (Smart 2-CH Relay) / ASW-220 controller (Smart 2-CH Relay PM). If enabled, the buttons connected to the inputs control the device directly. If disabled, the buttons connected to the inputs do not control the devices directly (can be used in routines).

Remember last value – option for the ADC-200 dimmer (Smart Dimmer) / ARC-200 controller (Smart RGBW LED Driver). If enabled, the device remembers the last settings (after turning the lighting off and on again the value set before turning the lighting off will be used).

Remember after power loss – option for a wired output (mainboard, wired and wireless expanders) / ADC-200 dimmer (Smart Dimmer) / ARC-200 controller (Smart RGBW LED Driver) / ARSC-200 controller (Smart Blinds) / ASW-200 plug (Smart Plug) / ASW-210 controller (Smart 2-CH Relay) / ASW-220 controller (Smart 2-CH Relay PM). If enabled, after the power is restored, the device status from before the power loss will be recovered (set values, etc.).

ECO mode – if enabled, periodical communication with the device takes place every 3 minutes. Thanks to this, the device battery life can be extended up to four times. If disabled, periodical communication with the device takes place every 24 seconds.



If you enable the ECO option for a detector, the delay between arming / disarming the system and sending this command to the detector can be up to three minutes.

Disable tamper – if enabled, the device does not report tamper.

5.9.2 Additional device settings

The settings described in this section are available after tapping / clicking the device ([room] / [group] >[device]).

Settings of devices with built-in temperature sensor

Temperature correction – the value by which the temperature information sent by the device is corrected.

Hardwired detectors and zones settings

Violations count – the number of violations after which the control panel will report a violation. If the number of violations is lower, they will be ignored.

Counting time – time in which violations are counted.

Hardwired zones settings

Zone wiring type – type of detector and the way it is connected to the zone:

Not used – the zone is not used (no device is connected to the zone).

NC – the zone supports an NC (normally closed) detector.

NO – the zone supports an NO (normally open) detector.

EOL – the zone supports an NO or NC detector with EOL resistor in the circuit.

2EOL/NC – the zone supports an NC detector with two EOL resistors in the circuit.

2EOL/NO – the zone supports an NO detector with two EOL resistors in the circuit.

Roller shutter – the zone supports a roller shutter detector.

Shock – the zone supports a shock detector (it can also support an NC detector).

Roller shutter 2EOL/NC – the zone supports a roller shutter detector with two EOL resistors in the circuit.

Shock 2EOL/NC – the zone supports a shock detector (it can also support an NC detector) with two EOL resistors in the circuit.

3EOL/NC – the zone supports an NC detector with three EOL resistors in the circuit.

3EOL/NO – the zone supports an NO detector with three EOL resistors in the circuit.



Opening the circuit that supports a shock detector for 200 ms or longer – regardless of the programmed sensitivity and impulses count (see below) – will result in zone violation. This allows you to connect a shock detector and an NC detector (e.g. a magnetic contact) in series to the zone.

Sensitivity – depending on wiring type:

NC / NO / EOL / 2EOL/NC / 2EOL/NO / 3EOL/NC / 3EOL/NO – time for which the zone must remain violated for the control panel to report the violation.

Shock / Shock 2EOL/NC – the shock whose duration is equal to or longer than the defined time will cause violation of the zone.

Impulses count – the number of pulses/shocks after which the zone will be violated. The parameter applies to the *Roller shutter / Roller shutter 2EOL/NC / Shock / Shock 2EOL/NC* wiring type.

Impulses time – the time during which the defined number of pulses must be detected for the zone to be violated. The parameter applies to the *Roller shutter / Roller shutter 2EOL/NC* wiring type.

Alarm output settings

ON/OFF – enable this option to turn on the output for the *Operating time*. Disable this option to turn off the output.

Operating time – period of time during which the output is turned on.

BI switch output settings

ON/OFF – enable this option to turn on the output. Disable this option to turn off the output.

Schedule – schedule that controls the output.

MONO switch output settings

ON/OFF – enable this option to turn on the output for the *Operating time*. Disable this option to turn off the output.

Operating time – period of time during which the output is turned on.

Schedule – schedule that controls the output.

Thermostat settings

Temperature set – currently set temperature threshold.

Day temperature – day temperature threshold. Used when the thermostat operation is controlled by a schedule.

Night temperature – night temperature threshold. Used when the thermostat operation is controlled by a schedule.

ECO mode temperature – ECO mode temperature threshold.

Manual temperature – temperature threshold set manually.

BOOST mode period – operating time of the boost heat function.

Temperature sensor – device with a temperature sensor that provides temperature data.

Temperature correction – the value by which the temperature information sent by the device is corrected.

Schedule – schedule that controls the *Day temperature* and *Night temperature* thresholds. During the hours specified by the schedule, the *Day temperature* threshold is active. Outside those hours, the *Night temperature* threshold is active.

Hysteresis – temperature difference between turning the thermostat on and off. The thermostat will be turned on when temperature drops below the threshold (heating) / rises above the threshold (cooling) by a value higher than the hysteresis.

Detector with lighting feature settings

Lighting – enable this option to turn on the lighting. Disable this option to turn off the lighting.

ADC-200 dimmer settings

ON/OFF – enable this option to turn on the lighting. Disable this option to turn off the lighting.

Maximum level – maximum brightness level that can be set.

Minimum level – minimum brightness level that can be set.

Brightening time – time required to change the brightness from the minimum level to the maximum level.

Schedule – schedule that controls the dimmer.

ARC-200 controller settings

ON/OFF – enable this option to turn on the lighting. Disable this option to turn off the lighting.

Maximum level – maximum brightness level that can be set.

Minimum level – minimum brightness level that can be set.

Brightening time – time required to change the brightness from the minimum level to the maximum level.

Color – LED lighting color.

ARSC-200 controller settings

Upward driving time – time required to raise fully lowered blinds / open fully closed blinds / open fully closed window.

Downward driving time – time required to lower fully raised blinds / close fully open blinds / close fully open window.

Upward slats rotation time – time required to move the slats of horizontal blinds from the lower to the upper end position.

Downward slats rotation time – time required to move the slats of horizontal blinds from the upper to the lower end position.

Switch-on delay when up – motor inertia time during upward movement, i.e. the time from applying voltage to the actual start of the motor.

Switch-on delay when down – motor inertia time during downward movement, i.e. the time from applying voltage to the actual start of the motor.

Schedule – schedule that controls the controller.

ASW-200 smart plug settings

ON/OFF – enable this option to turn on the plug. Disable this option to turn off the plug.

LED indicator – operating mode of the LED indicator:

Disabled – if enabled, the LED indicator is disabled, i.e. it does not indicate when the plug is on but it indicates warm-up and troubles.

By consumption – if enabled, the LED indicator color shows the power consumption of the connected device. The color changes from blue (minimum power consumption) to red (maximum power consumption).

Predefined – color of the LED indicator when the plug is turned on.

Schedule – schedule that controls the plug.

Operating time – period of time during which the plug is turned on. This parameter is available if the *Alarm* or *MONO switch* operating mode has been selected for the plug.

5.9.3 Alarm source

The settings described in this section are available after tapping / clicking the *Alarm source* button ([room] / [group] >[device] >*Alarm source*).

Every alarm – if enabled, every alarm is signaled by the device.

Alarm signaling disabled – indicator shows if alarms are signaled by the device.

System alarm – if enabled, system alarms are signaled (e.g. alarms generated by scenes and routines).

Devices – if enabled, you can select the devices from which alarms are signaled.

Rooms – if enabled, you can select the rooms from which alarms are signaled.

Arming mode – if enabled, you can select the arming modes for which alarms are signaled.

5.9.4 IP device settings

The settings described in this section are available after tapping / clicking the *IP device settings* ([room] / [group] >[device] >*IP device settings*).

IP device – if enabled, the IP device is supported and its settings are available.



For an IP device, you can program the settings of both the IP zone and the IP output, only the IP zone or only the IP output.

Communication loss time – time after which the IP device reports a loss of communication if it does not receive the HTTP Keep-Alive request. If you enter 0, the communication supervision will be disabled.

HTTP Keep-Alive request – string of characters that must be included in the received HTTP notification to confirm that communication is to be maintained.

Return time – time after which the IP zone will return to normal state (zone restore). The countdown is reset after each violation.

HTTP violation request – string of characters that must be included in the received HTTP notification for the IP zone to be violated.



The 5000 port is used for receiving HTTP notifications.

IP output address – address to which HTTP notifications will be sent. You can enter the IP address or the domain name.

Port – number of the port used for sending HTTP notifications. If you enter 0, the service will be disabled. This port cannot be used by another service, device, etc.

HTTP output OFF request – string of characters to be sent in an HTTP notification if the IP output is deactivated.

HTTP output ON request – string of characters to be sent in an HTTP notification if the IP output is activated.

5.9.5 Communication settings

The settings described in this section are available when adding a control panel (site) or after tapping / clicking *Connection methods (Settings >Site settings >Connection methods)*.

SIM1 / SIM2



You can obtain the SIM card settings from the mobile network operator.

PIN – SIM card PIN code.

APN – access point name for Internet connection.

User – username for Internet connection.

Password – password for Internet connection.

DNS 1 – IP address of the DNS 1 server to be used by the control panel.

DNS 2 – IP address of the DNS 2 server to be used by the control panel.

SMS center number – telephone number of the operator's SMS center. If the number has been saved to the SIM card memory by the operator, there is no need to program it. Otherwise, enter the number if the control panel is to send SMS messages.

Force network operator – codes of the operator of cellular network to which the SIM card is to log in. Enter in sequence:

- MCC (Mobile Country Code) – country code,
- MNC (Mobile Network Code) – operator code.

Enter the codes if you want the card to log in only to a specific operator's network. Remember that entering incorrect data may prevent logging in to the cellular network. If you do not enter the code, the card will log in to any available cellular network.

LAN

Configure connection manually – if enabled, you can program the network settings manually. If disabled, the control panel automatically downloads network settings from the DHCP server.

IPv4 – control panel IP address.

Mask – subnet mask in which the control panel operates.

Gateway – IP address of the network device through which devices in the local network can communicate with devices in other networks.

DNS 1 – IP address of the DNS 1 server to be used by the control panel.

DNS 2 – IP address of the DNS 2 server to be used by the control panel.

Wi-Fi

Password – Wi-Fi access password.

Configure connection manually – if enabled, you can program the network settings manually. If disabled, the control panel automatically downloads network settings from the DHCP server.

IPv4 – control panel IP address.

Mask – subnet mask in which the control panel operates.

Gateway – IP address of the network device through which devices in the local network can communicate with devices in other networks.

DNS 1 – IP address of the DNS 1 server to be used by the control panel.

DNS 2 – IP address of the DNS 2 server to be used by the control panel.

5.9.6 Advanced settings

The settings described in this section are available after tapping / clicking the *Advanced settings* button (*Settings > Site settings > Advanced settings*).

Hide arming – if enabled, the arming information in the LCD keypads / keypads is hidden after 180 seconds.

Alarm after 5 incorrect codes – if enabled, using a wrong code / proximity card 5 times will generate an alarm.

Lock keypad after 5 incorrect codes – if enabled, using a wrong code / proximity card 5 times will lock the LCD keypad / keypad / reader for 90 seconds.

R1 resistor – value of the R1 EOL resistor. By default: 1100 Ω .

R2 resistor – value of the R2 EOL resistor. By default: 1100 Ω .

R3 resistor – value of the R3 EOL resistor. By default: 2200 Ω .



The sum of values preset for three resistors may not exceed 15 k Ω .

When programming the R3 resistor value, remember that it must differ from that of the R2 resistor by at least 500 Ω .

The resistor value for Single EOL configuration is the sum of R1 and R2 resistors.

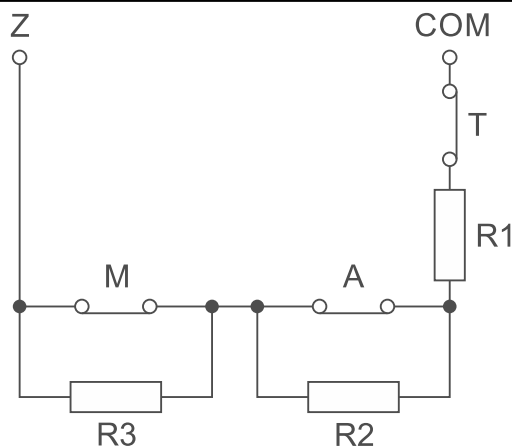


Fig. 4. Numbering of end-of-line resistors. The detector outputs are marked with letters: A - alarm, T – tamper, M – anti-masking.

5.9.7 Reporting

The settings described in this section are available after tapping / clicking the *Reporting* button (*Settings > Reporting*).

Mode – the way of sending event codes to the monitoring stations:

Disabled – no event codes are sent.

Only to station 1 – event codes are only sent to station 1.

Only to station 2 – event codes are only sent to station 2.

To station 1 and 2 – event codes are sent to both monitoring stations.

To station 1 or 2 – the control panel sends an event code to station 1 and, if unsuccessful, to station 2.

Station 1 / Station 2

Station 2 takes over link test – if enabled, when the control panel fails to connect to station 1 during the link test, the control panel will test the link to station 2. This option applies to the *SIA-IP* and *BOLD MANITOU* reporting types.

Type – you can select one of the following types: *SATEL IP*, *SIA IP* or *BOLD MANITOU*.

Channels – the order of using different transmission channels for the purpose of reporting. If an attempt to send an event code to the monitoring station via one channel fails, the control panel will use the next channel in line. A successful attempt to send an event code to the monitoring station will terminate the procedure (with the exception of test transmissions). Select the channels to be used and arrange them in order on the list using drag and drop. If you select *NONE* or select no channel on the list, event codes will not be sent.

Reporting format – the format in which event codes are sent to the monitoring station. You can select *SIA* or *Contact ID*.

Device identifier – control panel identifier for the purpose of reporting. It allows the monitoring station to determine where the events are being sent from. For the *Contact ID* format, enter 4 hexadecimal characters (digits or capital letters from A to F). For the *SIA* format, enter 4 or 6 hexadecimal characters (digits or capital letters from A to F).

Protocol – network protocol used to send event codes. You can select *TCP* or *UDP*.

Server 1 address – address of the monitoring station's server 1. You can enter the IP address or the domain name.

Port [server 1] – number of the port used for communication between the control panel and the monitoring station's server 1. If you enter 0, the service will be disabled. This port cannot be used by another service, device, etc.

Server 2 address – address of the monitoring station's server 2. You can enter the IP address or the domain name.

Port [server 2] – number of the port used for communication between the control panel and the monitoring station's server 2. If you enter 0, the service will be disabled. This port cannot be used by another service, device, etc.

SATEL station key – string of characters used for encrypting data sent to the monitoring station using *SATEL IP*. By default, you can enter up to 12 alphanumeric characters (digits, letters and special characters). If you enable the *HEX* option, you can enter 24 hexadecimal characters (digits or capital letters from A to F).

ETHM/GPRS key – string of characters used for identifying the control panel for the purpose of *SATEL IP* reporting. By default, you can enter up to 5 alphanumeric characters (digits, letters and special characters). If you enable the *HEX* option, you can enter 10 hexadecimal characters (digits or capital letters from A to F).

SIA ID – string of characters used for identifying the control panel for the purpose of *SIA-IP* reporting. You can enter up to 16 hexadecimal characters (digits or capital letters from A to F).

SIA: Account prefix – string of characters used for additional identification of the control panel for the purpose of *SIA-IP* reporting. The parameter allows you to expand the list of attributes used to identify the control panel. You can enter up to 6 hexadecimal characters (digits or capital letters from A to F).

SIA: Receiver number – string of characters used for additional identification of the control panel for the purpose of *SIA-IP* reporting. The parameter allows you to expand the list of attributes used to identify the control panel. You can enter up to 6 hexadecimal characters (digits or capital letters from A to F).

Encryption – option applies to *SIA-IP*. If enabled, data being sent is encrypted, and date and time are sent with the event code (the monitoring station can program date and time in the control panel).

Send date and time – option applies to *SIA-IP*. If enabled, date and time are sent with the event code (the monitoring station can program date and time in the control panel).

Server 1 heartbeat interval – number of seconds between additional tests of link to server 1 for the *BOLD MANITOU* reporting. If you enter 0, the link to server will not be additionally tested.

Server 2 heartbeat interval – number of seconds between additional tests of link to server 2 for the *BOLD MANITOU* reporting. If you enter 0, the link to server will not be additionally tested.

Advanced settings – if enabled, additional reporting settings are available:

Number of attempts – number of attempts to send an event. If all attempts are failed, the control panel will suspend monitoring.

Interval between attempts – time between each subsequent attempt to send an event.

Suspension period – time for which reporting will be suspended if all attempts to send an event through all provided transmission channels are failed. The control panel will make another attempt to send the event after this time elapsed or after a new event occurred.

SIA-IP test period: Server 1 / Server 2 – number of days, hours, minutes and seconds between the tests of link to the server for the *SIA-IP* reporting.

Both server link test – option applies to *SIA-IP*. If enabled, the control panel tests link to both servers of the monitoring station.

Server 2 takes over link test from server 1 – option applies to *SIA-IP*. If enabled, when the control panel fails to connect to the monitoring station's server 1 during the link test, the control panel will test link to server 2.

Send pictures only when the detector is armed – option applies to *BOLD MANITOU*. If enabled, pictures are only sent if the detector with camera is armed.

Send pictures to the station – option applies to *SATEL IP*. If enabled, the settings for sending pictures taken by camera detectors to the monitoring station are available.

Server 1 address – address of server 1 to which pictures are to be sent. You can enter the IP address or the domain name.

Port [server 1] – number of the port used for communication between the control panel and server 1. If you enter 0, the service will be disabled. This port cannot be used by another service, device, etc.

Server 2 address – address of server 2 to which pictures are to be sent. You can enter the IP address or the domain name.

Port [server 2] – number of the port used for communication between the control panel and server 2. If you enter 0, the service will be disabled. This port cannot be used by another service, device, etc.

Device identifier for picture sending – control panel identifier for the purpose of sending pictures to the monitoring station. You can enter up to 8 alphanumeric characters (digits, letters and special characters).

Password – password used to log in the control panel to the monitoring station for the purpose of sending pictures. You can enter up to 16 alphanumeric characters (digits, letters and special characters).

Send pictures only when the detector is armed – if enabled, pictures are only sent if the detector with camera is armed.

Test transmissions settings – if enabled, the test transmissions settings are available.

Every – if the test transmission is to be sent at specified time intervals, enter the interval in days, hours and minutes.

On time – if the test transmission is to be sent every day at a specified time, enter the hour and minutes.

Independent of events – option applies to test transmissions sent at specified time intervals. If enabled, the time is counted from the last test transmission. If disabled, the time is counted from the last transmission, regardless of whether it was a test transmission or another event code was sent.

5.9.8 Email settings

The settings described in this section are available after tapping / clicking the *Email settings* button (*Settings > Email settings*).

Subject – email subject. It is included in every notification email sent by the control panel.

Email – email address to be displayed to email recipients as the sender's address.

SMTP server – address of the outgoing mail server.

SMTP port – number of the outgoing mail port.

TLS – encryption protocol used. You can select: *SSL_TLS*, *SSL_START_TLS* or *SSL_NO_TLS*.

Sender – name to be displayed to email recipients as the sender's name.

Authentication – if enabled, the authentication is enabled.

Username – email address used for authentication (login to mail account).

Password – password used for authentication.

5.9.9 Encryption settings for the MIFARE cards

The settings described in this section are available after tapping / clicking the *SATEL token key* button (*Settings > SATEL token key*).

SATEL token key – card number access key for the MIFARE card. It is used for reading encrypted card numbers. By default: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 (no key – reader only reads the card's unencrypted factory serial number (CSN)).

No encryption – if this option is enabled, the reader only reads the card's unencrypted factory serial number (CSN). There is no need to program the cards but such cards are not secured against copying.



To write encrypted numbers to cards, the SO-PRG programmer and the CR SOFT program by SATEL are required.

The key in the system must be the same as the key used in the CR SOFT program to write the card number.

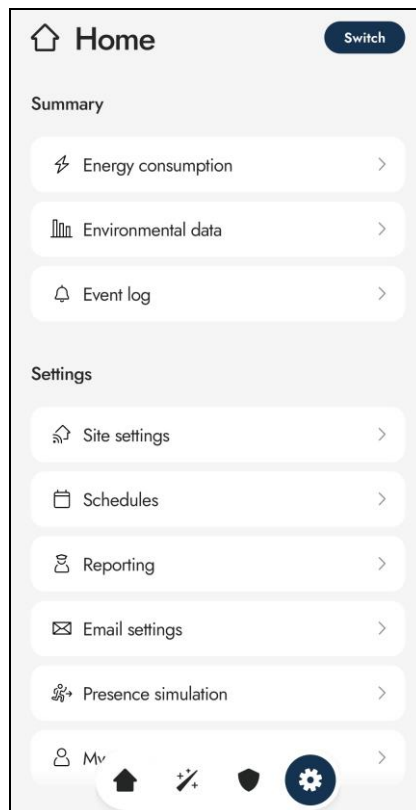
For security reasons, we recommend using DESFire cards with encrypted card numbers.

The card number's 8 bytes are used. If the number is shorter, zeros will be added to complete the number.

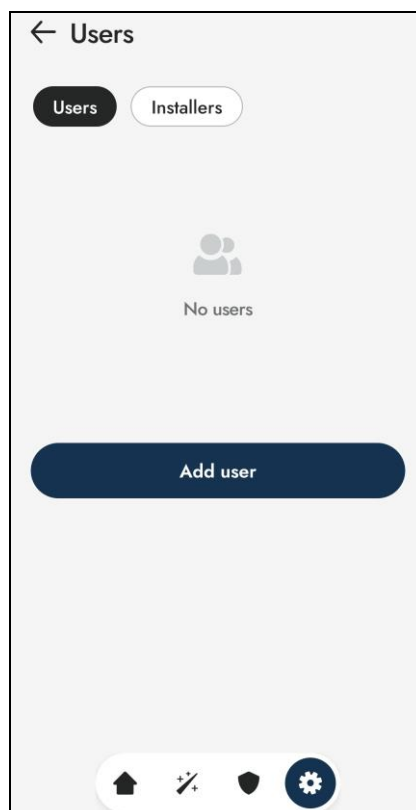
5.10 Adding a user

5.10.1 Adding a user in the Be Wave app

1. Tap  on the menu bar. The *Settings* screen will be displayed.



2. Tap the *Users* button. The *Users* screen will be displayed.



3. Tap the *Add user* button. The *New user* screen will be displayed.

← New user

USERNAME

Username

USER TYPE

User ☒

Installer ☐

SHARE

Entire site ☒

Part of the site ☐

Administrator ☐

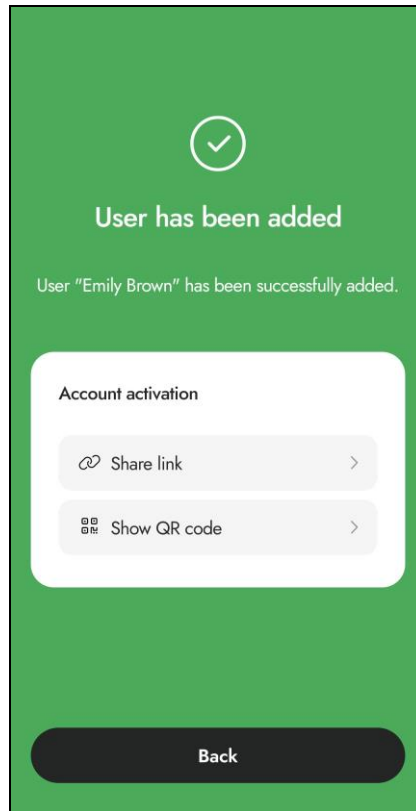
Save

4. Enter the username.
5. Select the user type: *User* or *Installer*.
6. If you selected the *User* type, you can select the *Entire site* (see “User with access to the entire site” p. 78) or *Part of the site* (see “User with access to a part of the site” p. 79) option.

7. Tap *Save*. A screen will be displayed saying that the user has been added. Two options to activate the new user account are available on the screen:
- tap *Share link* if you want to send a link to the user.
 - tap *Show QR code* if you want to share a QR code with the user.



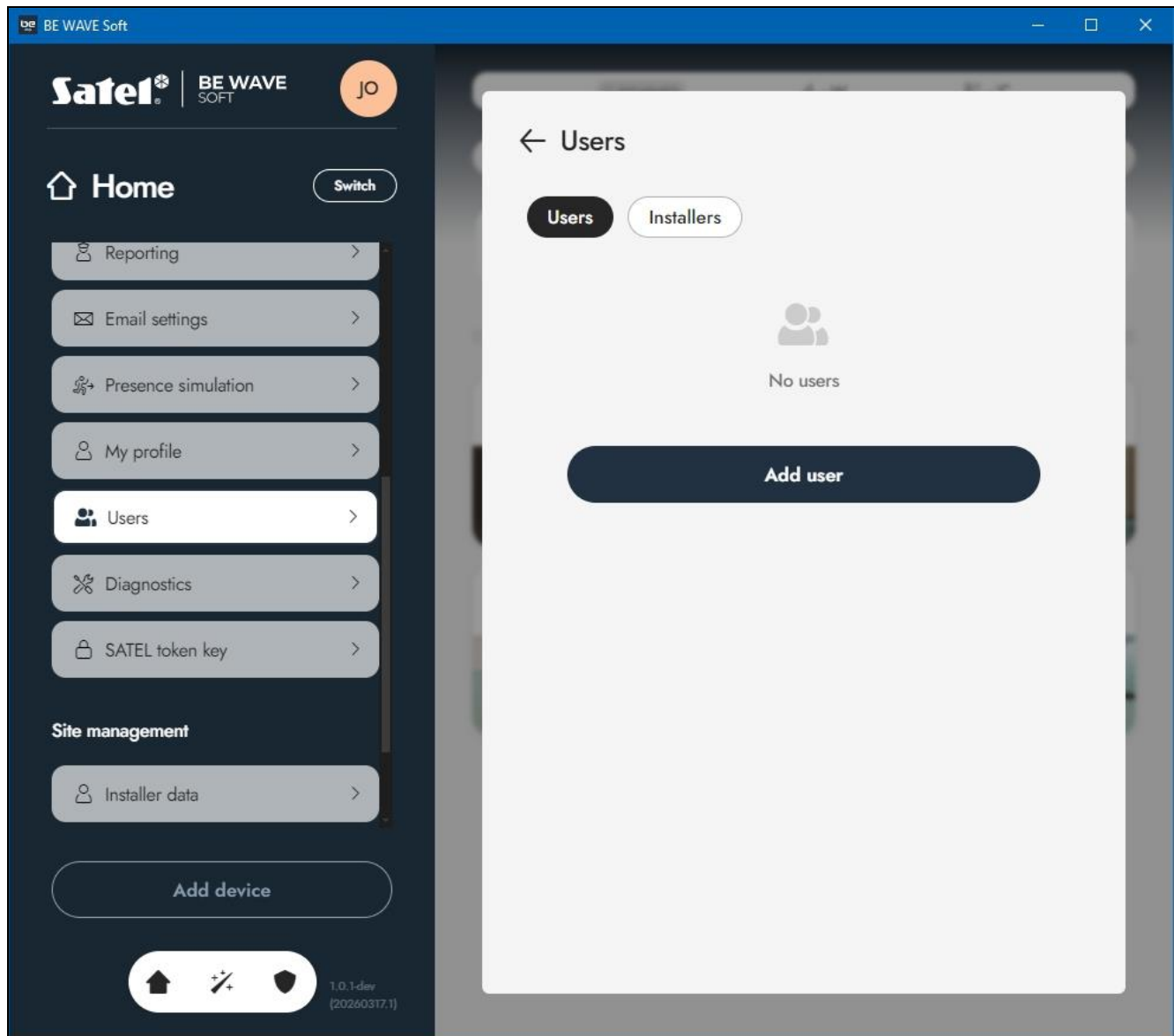
The user must activate the account within 24 hours of generating the link / QR code. Otherwise, the user will have to request a new link / QR code.



8. Tap *Back*. The *Users* screen will be displayed.

5.10.2 Adding a user in the BE WAVE Soft program

1. Click the *Users* button on the side menu. The *Users* window will be displayed.



2. Click *Add user* button. The *New user* window will be displayed.

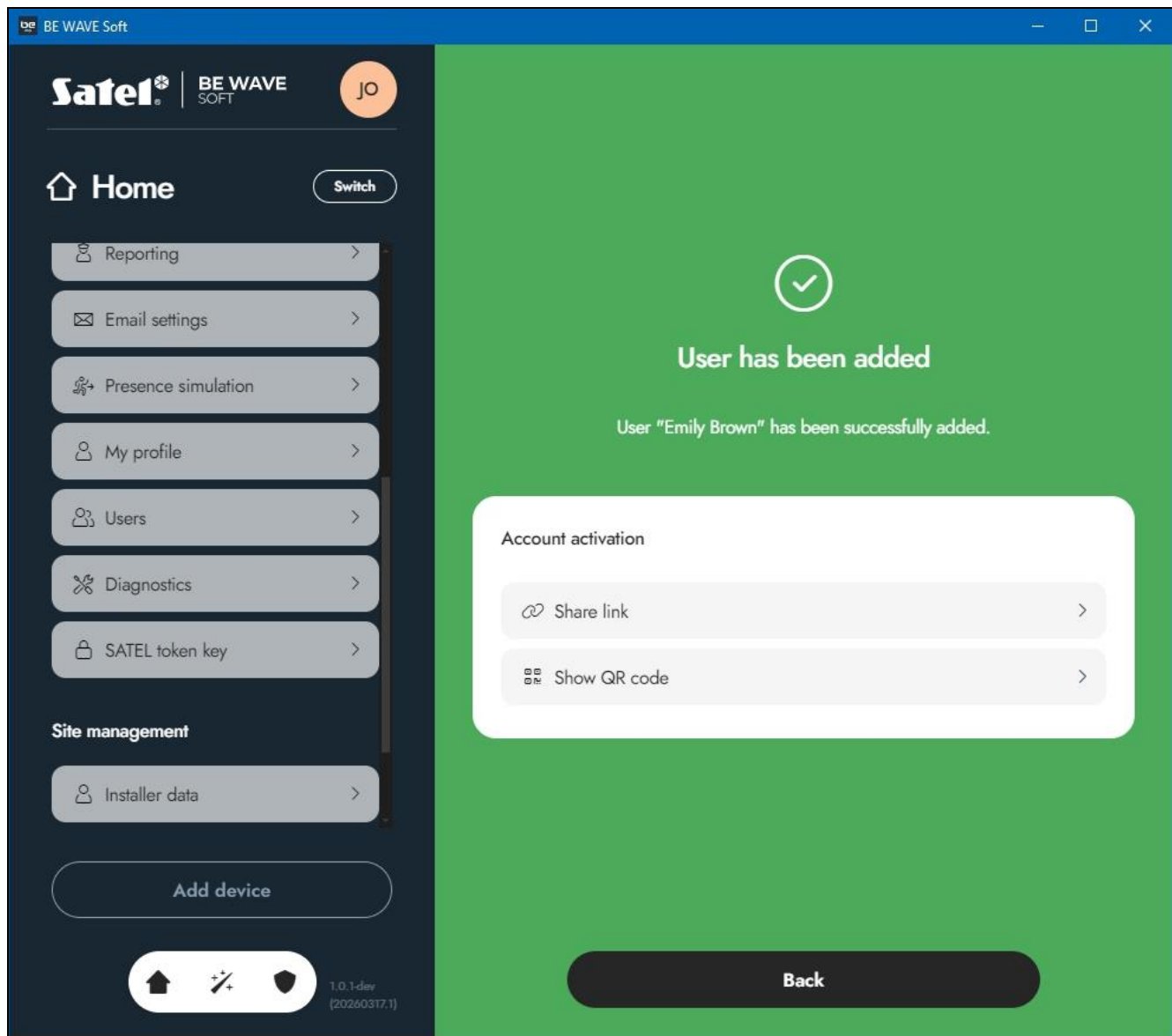
The screenshot displays the SATEL BE WAVE Soft application interface. On the left is a dark sidebar with the SATEL logo, a user profile icon labeled 'JO', and a 'Switch' button. Below these are menu items: Home, Reporting, Email settings, Presence simulation, My profile, Users, Diagnostics, and SATEL token key. A 'Site management' section includes 'Installer data'. At the bottom of the sidebar is an 'Add device' button and a status bar showing '1.0.1-dev (20260317.1)'. The main area on the right shows a 'New user' modal window. This window has a back arrow and the title 'New user'. It contains three sections: 'USERNAME' with a text input field labeled 'Username'; 'USER TYPE' with two radio button options, 'User' (selected) and 'Installer'; and 'SHARE' with two radio button options, 'Entire site' (selected) and 'Part of the site'. There is also an 'Administrator' toggle switch which is currently turned off. At the bottom of the modal is a large dark blue 'Save' button.

3. Enter the username.
4. Select the user type: *User* or *Installer*.
5. If you selected the *User* type, you can select the *Entire site* (see “User with access to the entire site” p. 78) or *Part of the site* (see “User with access to a part of the site” p. 79) option.

6. Click **Save**. A window will be displayed saying that the user has been added. Two options to activate the new user account are available in the window:
 - tap *Share link* if you want to send a link to the user.
 - tap *Show QR code* if you want to share a QR code with the user.



The user must activate the account within 24 hours of generating the link / QR code. Otherwise, the user will have to request a new link / QR code.



7. Click **Back**. The *Users* window will be displayed.

5.10.3 User with access to the entire site

If you selected the *Entire site* option when adding the user, you can enable the *Administrator* option to grant the user additional privileges.

User privileges

Edit users – the user can manage users.

Scenes/routines – the user can manage scenes and routines.

Schedules – the user can manage schedules.

Presence simulation – the user has access to the *Presence simulation* function.

System notifications – the user receives notifications of system events.

5.10.4 User with access to a part of the site

If you selected the *Part of the site* option when adding the user, the button *Next* instead of *Save* will be displayed at the bottom of the screen. In the next steps you will be able to select the system elements to which the user is to have access:

- devices,
- arming modes,
- scenes.

5.11 Enabling SMS / CLIP notifications [HYBRID 128 Plus]

Requirements:

- SIM card must be installed in the control panel,
- SIM card settings must be programmed in the control panel (see “Communication settings” p. 68).

5.11.1 Enabling SMS / CLIP notifications in the Be Wave app

1. Tap  on the menu bar. The *Settings* screen will be displayed.
2. Tap *My profile*. The *My profile* screen will be displayed.
3. Tap *Notifications*. The *Notifications* screen will be displayed.
4. Enable the *Phone notifications* option. Additional settings will be displayed.
5. Enter the phone number to which messages should be sent.
6. Select which events the control panel should notify about using SMS and/or CLIP.
7. Tap *Save*.

5.11.2 Enabling SMS / CLIP notifications in the BE WAVE Soft program

1. Click *My profile* on the side menu. The *My profile* window will be displayed.
2. Click *Notifications*. The *Notifications* window will be displayed.
3. Enable the *Phone notifications* option. Additional settings will be displayed.
4. Enter the phone number to which messages should be sent.
5. Select which events the control panel should notify about using SMS and/or CLIP.
6. Click *Save*.

5.12 Enabling email notifications

Requirements:

- control panel must be connected to the Internet,
- email settings must be programmed in the control panel (see “Email settings” p. 72).

5.12.1 Enabling email notifications in the Be Wave app

1. Tap  on the menu bar. The *Settings* screen will be displayed.
2. Tap *My profile*. The *My profile* screen will be displayed.
3. Tap *Notifications*. The *Notifications* screen will be displayed.
4. Enable the *E-mail notifications* option. Additional settings will be displayed.
5. Enter the email address to which messages should be sent.
6. Select which events the control panel should notify about using email.
7. Tap *Save*.

5.12.2 Enabling email notifications in the BE WAVE Soft program

1. Click *My profile* on the side menu. The *My profile* window will be displayed.
2. Click *Notifications*. The *Notifications* window will be displayed.
3. Enable the *E-mail notifications* option. Additional settings will be displayed.
4. Enter the email address to which messages should be sent.
5. Select which events the control panel should notify about using email.
6. Click *Save*.

6. Testing

It is a good practice to test the devices after they are added to the system. We also recommend to periodically check if the devices work correctly. In the Be Wave app / BE WAVE Soft program you can enable the diagnostic mode when you want to carry out testing or maintenance of devices (battery replacement, cleaning the smoke chamber of the ASD-200 (Fire Detector Plus) / ASD-250 (Fire Detector Pro) detector, etc.). When the diagnostic mode is enabled:

- system cannot be armed,
- tamper alarms are not signaled,
- wireless detector LED indicators are ON (the indicators are normally OFF) – e.g. you can check if motion detectors detect motion,
- the AOD-210 (Outdoor Motion Detector), AOCAM-210 (Outdoor Motion Detector Cam) and ADD-200 (Outdoor Dusk Detector) detectors react quicker to changes in light intensity – you can cover the detector with a cardboard box, a thick, dark fabric, etc. The detector should detect dusk after 3 seconds,
- the AGD-200 (Glass Break Detector) reacts to the sound of breaking glass alone (high-frequency sound),
- tamper signaling in the wireless sirens is blocked – you can open the siren enclosure without starting the signaling.



After the diagnostic test is enabled, automatic calibration of the microwave sensor is carried out in dual-technology motion detectors (APMD-250, AOD-210, AOCD-260, etc.). For 10 seconds after the diagnostic mode is enabled, there should be no moving object in the detection area of the microwave sensor, as this will prevent proper calibration of the sensor.

6.1 Enabling the diagnostic mode



All wireless devices will enter the diagnostic mode after some time (up to 24 seconds).

According to requirements of the EN 50131 standard, the level of radio signals sent by wireless devices is reduced when the diagnostic mode is enabled.

Remember to disable the diagnostic mode when testing and maintenance of the devices in the system is complete.

6.1.1 Enabling the diagnostic mode in the Be Wave app

1. Tap  on the menu bar. The *Settings* screen will be displayed.
2. Tap *Diagnostics*. The *Diagnostics* screen will be displayed.
3. Tap *Enable diagnostic mode*.

6.1.2 Enabling the diagnostic mode in the BE WAVE Soft program

1. Click *Diagnostics* on the side menu. The *Diagnostics* window will be displayed.
2. Click *Enable diagnostic mode*.

6.2 Disabling the diagnostic mode

6.2.1 Disabling the diagnostic mode in the Be Wave app

1. Tap  on the menu bar. The *Settings* screen will be displayed.
2. Tap *Diagnostics*. The *Diagnostics* screen will be displayed.
3. Tap *Disable diagnostic mode*.

6.2.2 Disabling the diagnostic mode in the BE WAVE Soft program

1. Click *Diagnostics* on the side menu. The *Diagnostics* window will be displayed.
2. Click *Disable diagnostic mode*.

7. Maintenance

7.1 Firmware update



The Update the system button is available when new firmware version is available.

When the firmware update is complete, the control panel will be restarted.

Sending out the update file to the wireless devices may take some time. The update itself takes only several seconds. The device does not execute its normal functions then.

7.1.1 Starting the update in the Be Wave app

1. Tap  on the menu bar. The *Settings* screen will be displayed.
2. Tap *Site settings*. The *Site settings* screen will be displayed.
3. Tap the *Update the system* button. You will be asked for confirmation.
4. Tap *Yes* to update firmware of the control panel and the devices in the system.

7.1.2 Starting the update in the BE WAVE Soft program

1. Click the *Site settings* button on the side menu. The *Site settings* window will be displayed.
2. Click the *Update the system* button. You will be asked for confirmation.
3. Click *Yes* to update firmware of the control panel and the devices in the system.

7.2 Importing system settings from SD card

7.2.1 Importing system settings in the Be Wave app

1. Tap  on the menu bar. The *Settings* screen will be displayed.
2. Tap *Site settings*. The *Site settings* screen will be displayed.
3. Tap *Import settings from SD card*. You will be asked for confirmation.
4. Enter the password if access to the file is password-protected.

5. Tap Yes to import the settings from the SD card.

7.2.2 Importing system settings in the BE WAVE Soft program

1. Click the *Site settings* button on the side menu. The *Site settings* window will be displayed.
2. Click *Import settings from SD card*. You will be asked for confirmation.
3. Enter the password if access to the file is password-protected.
4. Click Yes to import the settings from the SD card.

7.3 Exporting system settings to SD card



The user settings are not exported.

7.3.1 Exporting system settings in the Be Wave app

1. Tap  on the menu bar. The *Settings* screen will be displayed.
2. Tap *Site settings*. The *Site settings* screen will be displayed.
3. Tap *Export settings to SD card*. You will be asked for confirmation.
4. Enter the password if access to the file should be password-protected.
5. Tap Yes to save the settings to SD card.

7.3.2 Exporting system settings in the BE WAVE Soft program

1. Click the *Site settings* button on the side menu. The *Site settings* window will be displayed.
2. Click *Export settings to SD card*. You will be asked for confirmation.
3. Enter the password if access to the file should be password-protected.
4. Click Yes to save the settings to SD card.

7.4 Restoring the control panel factory settings

7.4.1 Restoring the factory settings from the Be Wave app

1. Tap  on the menu bar. The *Settings* screen will be displayed.
2. Tap *Site settings*. The *Site settings* screen will be displayed.
3. Tap *Restore factory settings*. You will be asked for confirmation.
4. Tap Yes to restore the factory settings.

7.4.2 Restoring the factory settings from the BE WAVE Soft program

1. Click the *Site settings* button on the side menu. The *Site settings* window will be displayed.
2. Click *Restore factory settings*. You will be asked for confirmation.
3. Click Yes to restore the factory settings.

7.4.3 Hardware factory restore

1. Enable the diagnostic mode (see “Enabling the diagnostic mode” p. 80).
2. Open the control panel enclosure.
3. Press and hold the RESET button on the control panel main board for 5 seconds.

8. Specifications

Operating frequency band	868.0 MHz ÷ 868.6 MHz
Radio communication range (in open area)	up to 2000 m
Supply voltage	12 VDC
Standby current consumption	
HYBRID 128 Plus	170 mA
HYBRID 128	145 mA
Maximum current consumption	
HYBRID 128 Plus	260 mA
HYBRID 128	235 mA
AUX output	2.5 A / 12 VDC
O1...O4 outputs	1 A / 12 VDC
Supported memory cards	microSD, micro SDHC
Security grade according to EN 50131-1	Grade 2
Environmental class according to EN 50130-5	II
Operating temperature range	-10°C...+55°C
Maximum humidity	93±3%
Electronics board dimensions	167 x 75 mm
Weight	
HYBRID 128 Plus	100 g
HYBRID 128	90 g