BE WAVE Wire system control panel

WIRE 128

Firmware version 1.4

EN

wire_en 05/26

SATEL sp. z o.o. • ul. Budowlanych 66 • 80-298 Gdańsk • POLAND
tel. +48 58 320 94 00
www.satel.pl

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:

CE 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

The declaration of conformity may be consulted at 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 4
Communication bus 5
Users 5
Be Wave app 5
BE WAVE Soft program 5
Arming 5
Scenes and routines 5
Schedules 5
Event log 5
Messaging 5
Reporting 6
Firmware update 6
Mainboard 6
3. Supported devices 6
3.1 Bus devices 6
3.1.1 Detectors 6
3.1.2 Expanders 7
3.1.3 LCD keypads 7
3.1.4 Keypads 8
3.1.5 Proximity card readers 8
3.2 Virtual IP devices 8
4. Installation 8
4.1 Installation plan 8
4.2 Estimation of the system current consumption 8
4.3 Cabling 9
4.4 Mounting the control panel 9
4.4.1 Tips for installation 9
4.4.2 Description of the mainboard 10
Description of terminals 11
4.5 Connecting the bus devices 11
4.6 Connecting the detectors 12
4.6.1 End-of-line resistors 13
4.7 Connecting the LAN 13
4.8 Connecting the power and starting the control panel 13
4.9 Connecting the sirens 14
5. Managing, programming and controlling the system 14
5.1 Be Wave app 14
5.1.1 Description of the Be Wave app home screen 15
5.1.2 Changing the app language 15
5.1.3 Changing the app theme 16
5.2 BE WAVE Soft program 16
5.2.1 Description of the BE WAVE Soft program home screen 16
5.2.2 Changing the program language 17

5.2.3 Changing the program theme 17
5.3 Adding the control panel (site) 17
5.3.1 Adding the control panel in the Be Wave app 18
Adding the first control panel (site) 18
Adding another control panel (site) 21
5.3.2 Adding the control panel in the BE WAVE Soft program 23
Adding the first control panel (site) 23
Adding another control panel (site) 26
5.4 Adding mainboard zones and outputs to the system 27
5.4.1 Adding mainboard zones and outputs in the Be Wave app 28
5.4.2 Adding the mainboard zones and outputs in the BE WAVE Soft app 31
5.5 Adding a bus device to the system 36
5.5.1 Adding a bus device in the Be Wave app 36
5.5.2 Adding a bus device in the BE WAVE Soft program 39
5.6 Adding a virtual IP device to the system 45
5.6.1 Adding a virtual IP device in the Be Wave app 45
5.6.2 Adding a virtual IP device in the BE WAVE Soft program 47
5.7 Removing the device from the system 50
5.7.1 Deleting a device in the Be Wave app 50
5.7.2 Deleting a device in the BE WAVE Soft program 50
5.8 Description of settings 51
5.8.1 Device settings 51
5.8.2 Additional device settings 52
Settings of devices with built-in temperature sensor 52
Hardwired detectors and zones settings 52
Hardwired zones settings 52
Alarm output settings 53
BI switch output settings 53
MONO switch output settings 53
Thermostat settings 53
Detector with lighting feature settings 54
5.8.3 Alarm source 54
5.8.4 IP device settings 54
5.8.5 Communication settings 55
LAN 55
Wi-Fi 55
5.8.6 Advanced settings 55
5.8.7 Reporting 56
Station 1 / Station 2 56
5.8.8 Email settings 58
5.8.9 Encryption settings for the MIFARE cards 59
5.9 Adding a user 60
5.9.1 Adding a user in the Be Wave app 60
5.9.2 Adding a user in the BE WAVE Soft program 63
5.9.3 User with access to the entire site 65
User privileges 65
5.9.4 User with access to a part of the site 66
5.10 Enabling email notifications 66
5.10.1 Enabling email notifications in the Be Wave app 66
5.10.2 Enabling email notifications in the BE WAVE Soft program 66

6. Testing 66
6.1 Enabling the diagnostic mode 66
6.1.1 Enabling the diagnostic mode in the Be Wave app 66
6.1.2 Enabling the diagnostic mode in the BE WAVE Soft program 67
6.2 Disabling the diagnostic mode 67
6.2.1 Disabling the diagnostic mode in the Be Wave app 67
6.2.2 Disabling the diagnostic mode in the BE WAVE Soft program 67
7. Maintenance 67
7.1 Firmware update 67
7.1.1 Starting the update in the Be Wave app 67
7.1.2 Starting the update in the BE WAVE Soft program 67
7.2 Importing system settings from SD card 67
7.2.1 Importing system settings in the Be Wave app 67
7.2.2 Importing system settings in the BE WAVE Soft program 68
7.3 Exporting system settings to SD card 68
7.3.1 Exporting system settings in the Be Wave app 68
7.3.2 Exporting system settings in the BE WAVE Soft program 68
7.4 Restoring the control panel factory settings 68
7.4.1 Restoring the factory settings from the Be Wave app 68
7.4.2 Restoring the factory settings from the BE WAVE Soft program 68
7.4.3 Hardware factory restore 68
8. Specifications 68

1. Introduction

This manual will help you install the WIRE 128 control panel. The BE WAVE Wire 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 WIRE 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 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 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).
- 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.

Reporting

- Reporting events to two monitoring stations.
- Support for Contact ID, SIA and Bold Manitou communication formats.
- Data transmission via Ethernet.

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).
- USB-C socket for connecting to a mobile device with the Be Wave app or to a computer with the BE WAVE Soft program.
- Built-in Ethernet (LAN) port.
- LED indicator.
- Powered by 18 VAC (±15%).
- Built-in power supply:
  – switching-mode power supply 12 V / 2 A,
  – short-circuit protection,
  – battery charging circuit,
  – battery status supervision and low battery disconnect system.

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),
- 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 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.). The calculation should take into account the battery charging current. If the sum of currents exceeds the maximum output current of the control panel power supply an additional power supply should be used.

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 mm^2. 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.
- The control panel must be protected against unauthorized access.
- The control panel requires 18 VAC (±15%) power. It is recommended that a transformer with at least 40 VA rating be used.

Do not connect two devices with power supply to one-section transformer.

Before connecting transformer to a circuit from which it will be powered, make sure the circuit is de-energized.

- The transformer should be permanently connected to the 230 VAC mains power.
- The electrical circuit to which the transformer is to be connected must have suitable protection (2-pole switch disconnector and/or 16 A slow-blow fuse).
- Instruct the owner or user of the system on how to disconnect the transformer from the mains supply (e.g. indicate the fuse or circuit breaker protecting the transformer supply circuit).
- For a backup power source, use a 12 V sealed lead-acid battery or other 12 V battery with similar charging characteristics.

Do not connect deeply discharged battery to the control panel (with voltage across unloaded terminals below 11 V). The battery should be precharged.

The used batteries must not be discarded, but should be disposed of in accordance with the existing rules for environment protection.

- The battery capacity must be selected to match current consumption in the system. According to EN 50131 Grade 2, the battery must ensure operation of the system without mains power for 12 hours.
- 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

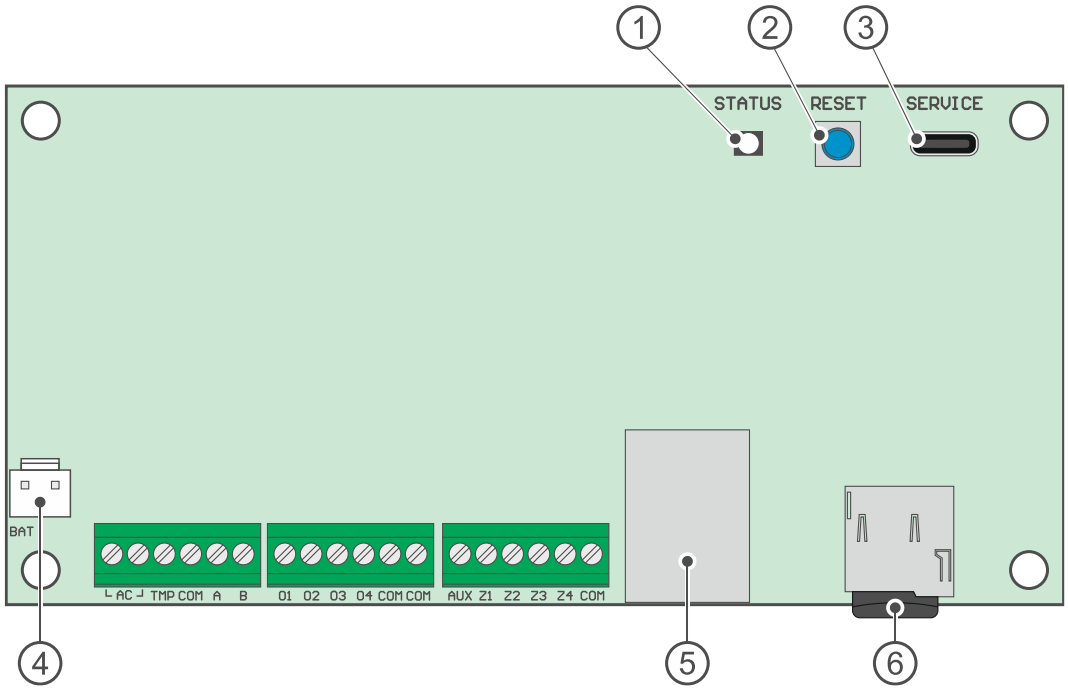


Fig. 1. Control panel mainboard.

(1) STATUS LED indicator:

flashing in pink – control panel startup in progress / communication setting not yet configured,

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.

(2) RESET button – press and hold for 5 seconds to restore factory settings (see "Hardware factory restore" p. 68).

(3) USB-C socket for connecting to a mobile device with the Be Wave app or to a computer with the BE WAVE Soft program.

(4) connector for battery connection wires. The wires are included in the set (Fig. 2).

(5) LAN cable port.

(6) 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 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).

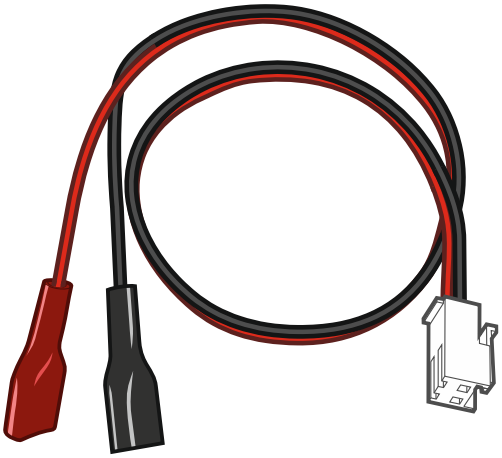


Fig. 2. Battery connection wires (red +, black -).

Description of terminals

AC - 18 VAC power input.

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.

COM - common ground.

A, B - RS communication bus.

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

AUX - +12 VDC power output.

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 Ω ± 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.

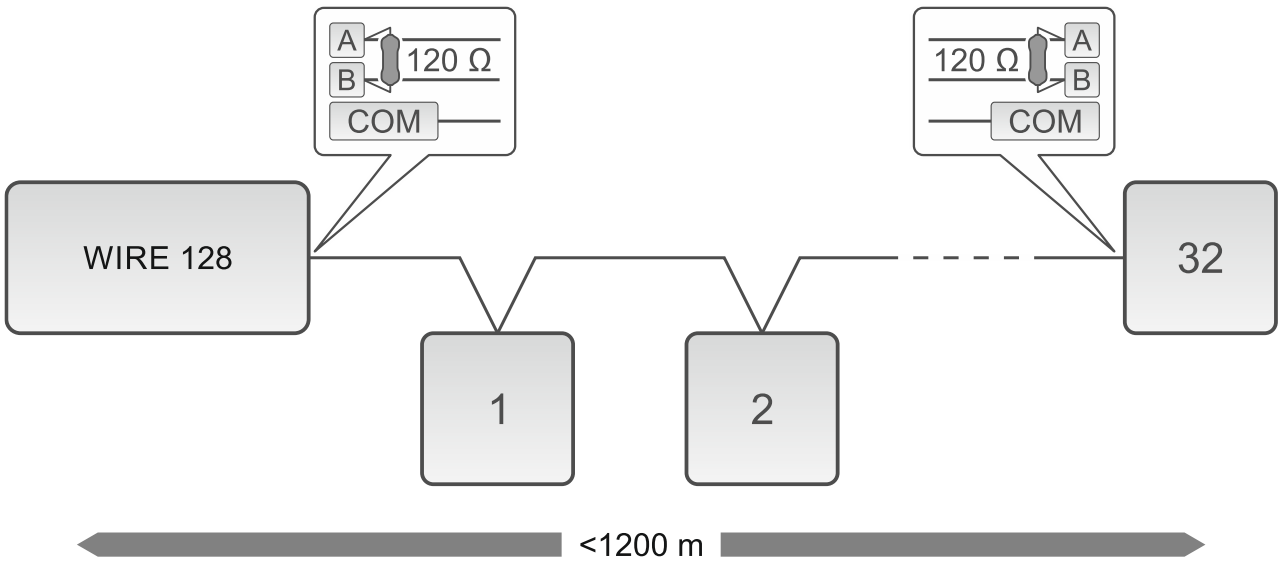


Fig. 3. Diagram of connecting devices to the RS bus.

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.

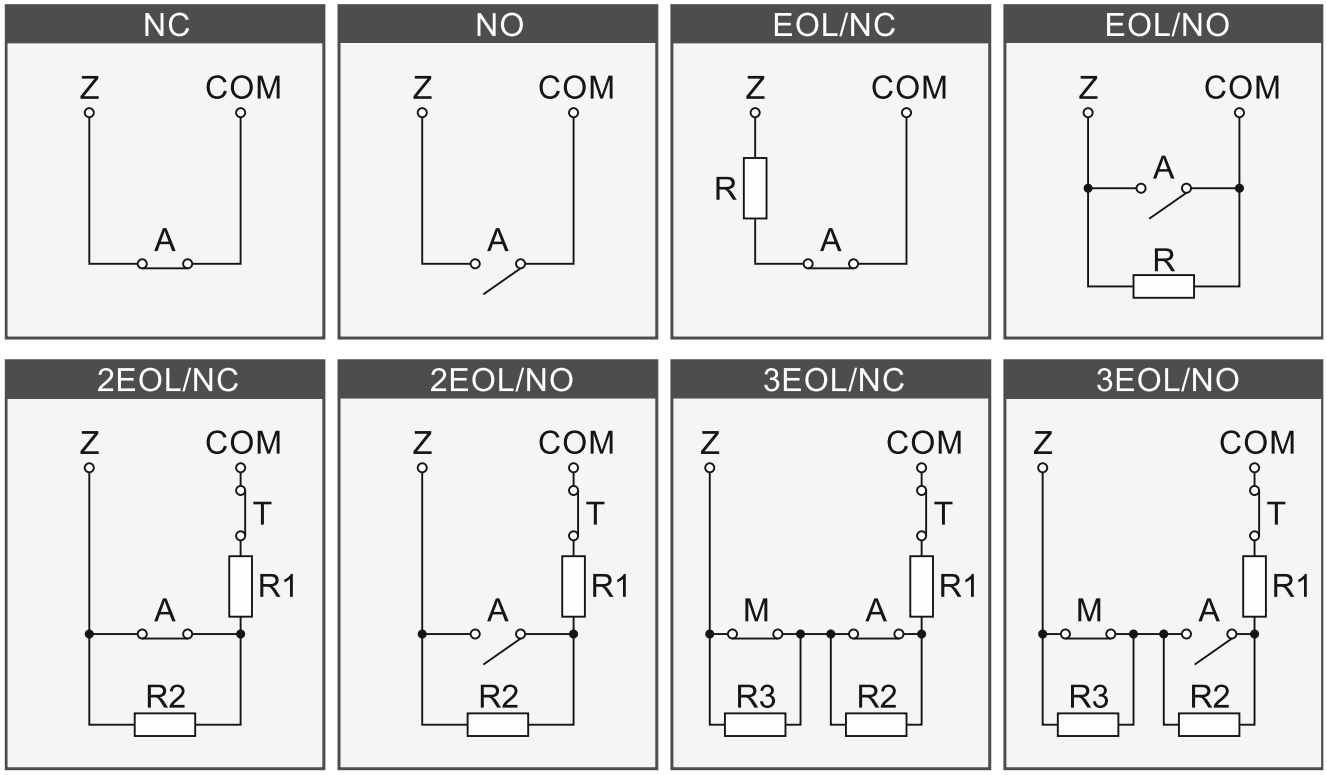


Fig. 4. The ways to connect detectors to zones. The detector outputs are marked with letters: A - alarm, T – tamper, M – anti-masking. R=R1+R2.

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. 55). By default, the following values are programmed:

R1 = 1.1 kΩ;

R2 = 1.1 kΩ;

R3 = 2.2 kΩ.

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

- EOL – use one 2.2 kΩ resistor,
- 2EOL – use two 1.1 kΩ 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 Connecting the power and starting the control panel

1. De-energize the 230 VAC circuit to which the transformer is to be connected.
2. Connect the 230 VAC wires to the terminals of transformer primary winding.
3. Connect the terminals of transformer secondary winding to the control panel AC terminals.

4. Connect the battery wires (Fig. 2) to the control panel connector.
5. Connect the battery: positive terminal to RED wire, negative terminal to BLACK wire. If the battery has screw-type cable lugs, use adapters delivered with the control panel (do not cut off the battery cable lugs). **The control panel will not start after connecting the battery alone.**
6. Turn on 230 VAC power in the circuit to which the transformer is connected. The control panel will start up (the STATUS LED indicator will start flashing).

The above mentioned power-up sequence (first the battery, then the AC power source) will ensure proper operation of the power supply and the electronic protection circuits, thus preventing damage caused by installation mistakes, if any.

If it is necessary to de-energize the control panel, first turn off the AC power (main power source), and then the battery (backup power source). Observe the above described procedure when reconnecting the power.

If the battery voltage drops below 11 V for longer than 1 minute, the control panel will indicate battery failure. When the voltage goes down to approx. 10.5 V, the battery will be disconnected.

4.9 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).

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.

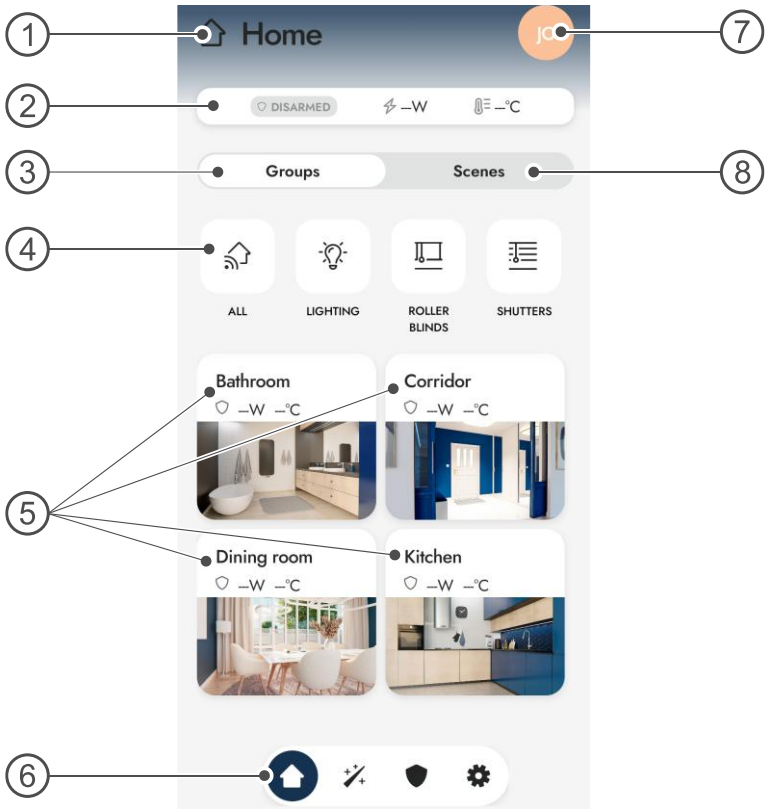
5.1 Be Wave app

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*.

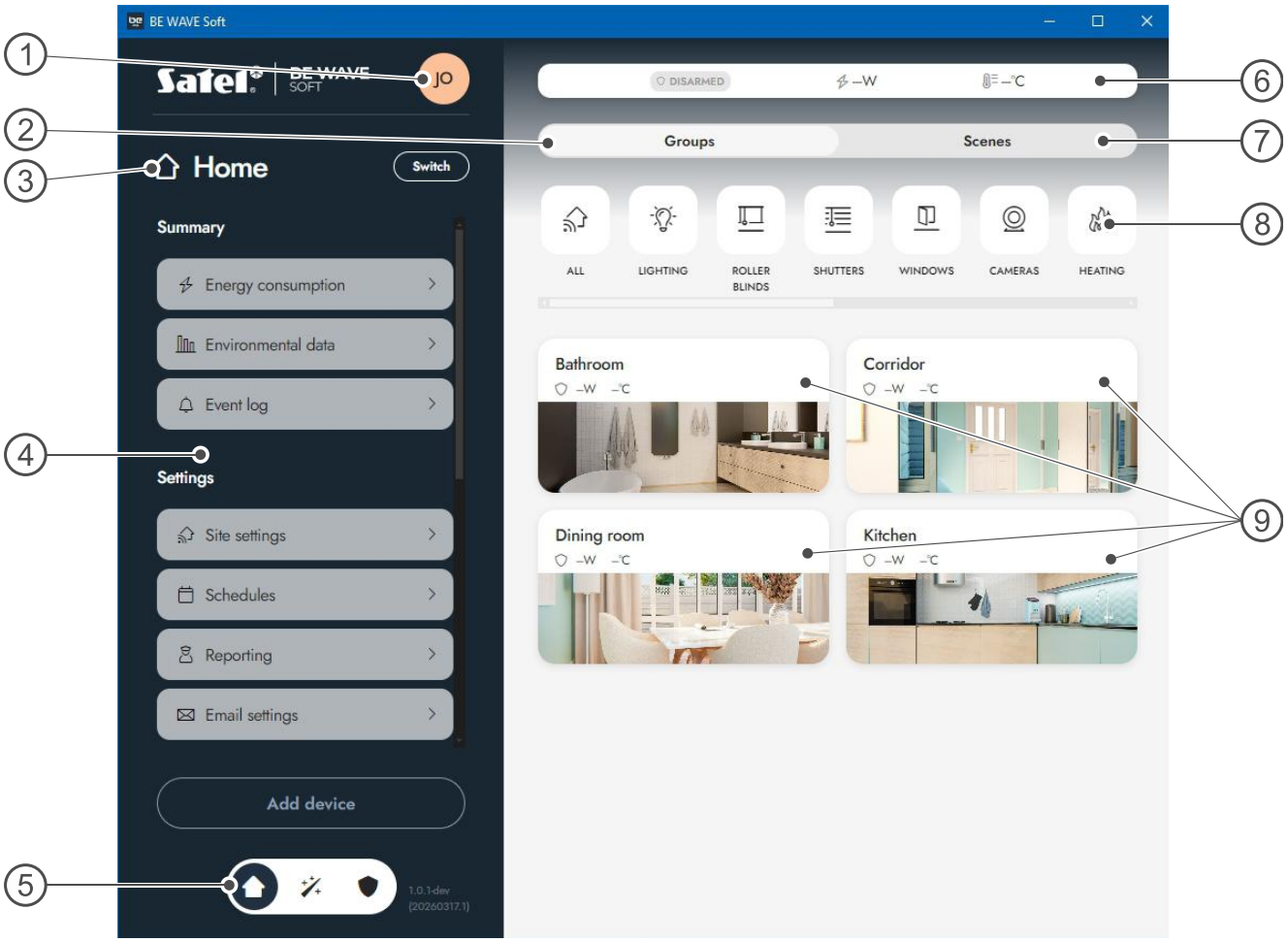
5.2 BE WAVE Soft program

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)

The phone / computer must be connected to the control panel's USB-C socket or to the same local network as the control panel.

5.3.1 Adding the control panel in the Be Wave app

Adding the first control panel (site)

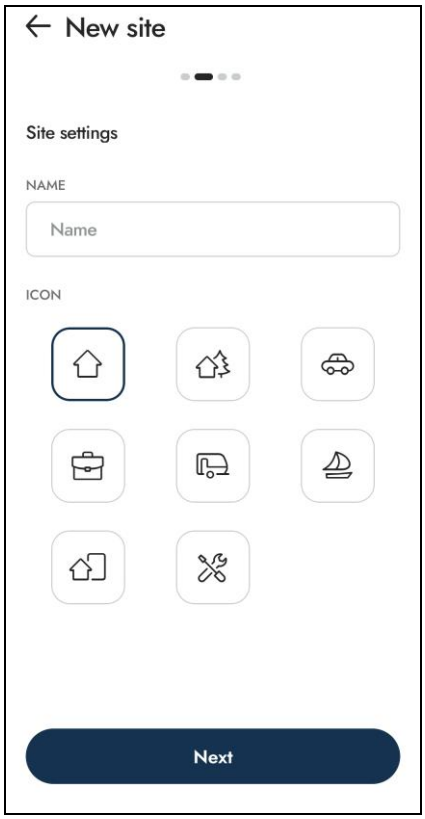
1. Start the Be Wave app. The *Add new site* screen will be displayed.



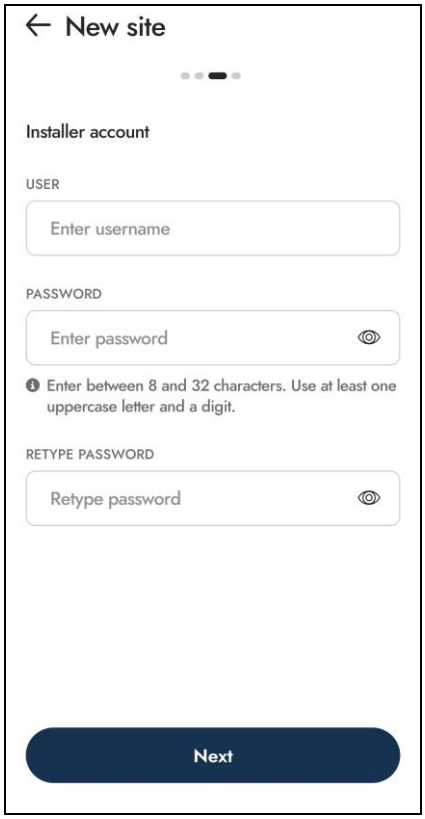
2. Tap the control panel (site) you want to add. Different buttons will appear at the bottom of the screen.



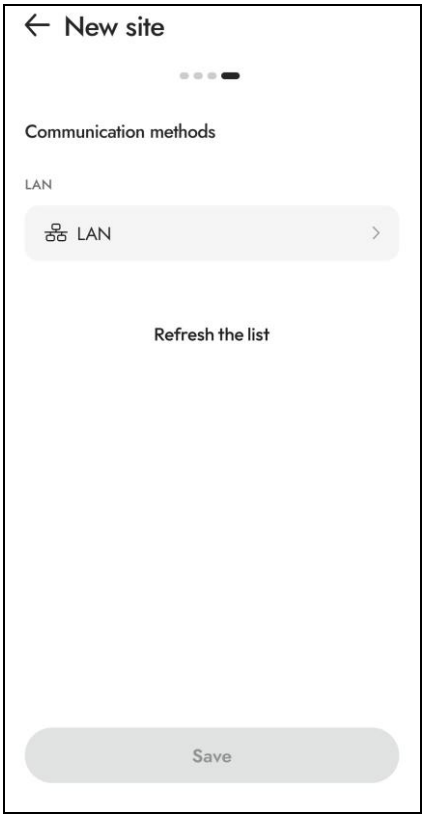
3. Tap *Connect*. The *New site – Site settings* screen will be displayed.



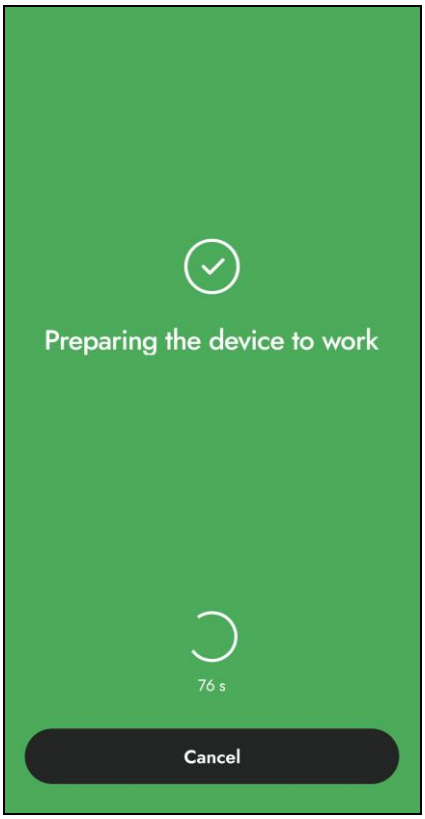
4. Enter the name of the site and select one of the icons to represent the site, then tap *Next*. The *New site – Installer account* screen will be displayed.



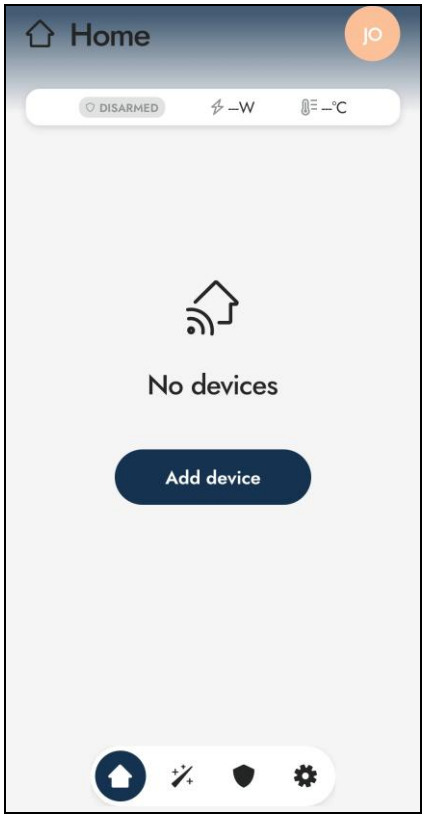
5. Enter the username and password for the installer, then tap *Save*. The *New site – Communication methods* screen will be displayed.



6. Tap *LAN*. A screen for configuring network settings will be displayed (see “Communication settings” p. 55). 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.

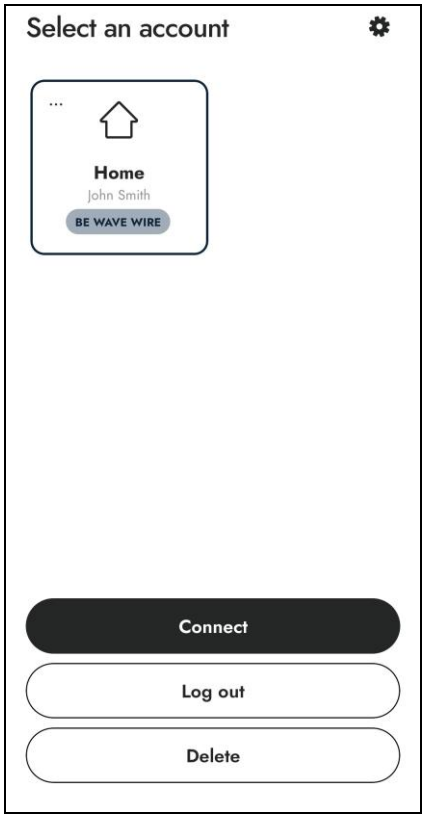


7. When the app connects to the control panel, the app's home screen will be displayed. You can add the first device to the system.

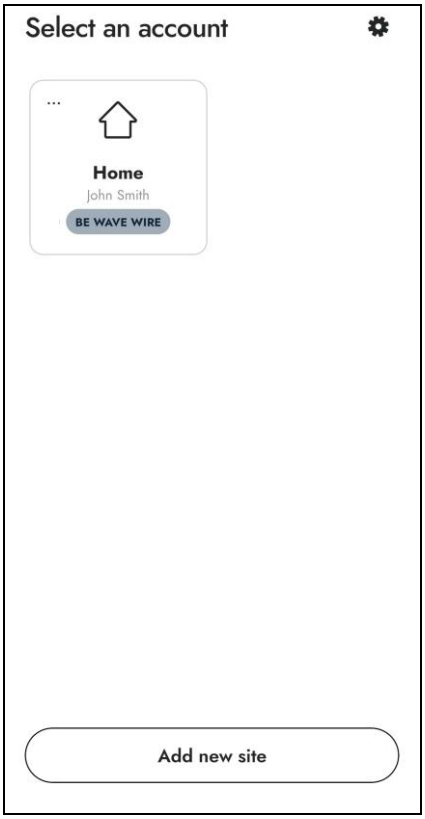


Adding another control panel (site)

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

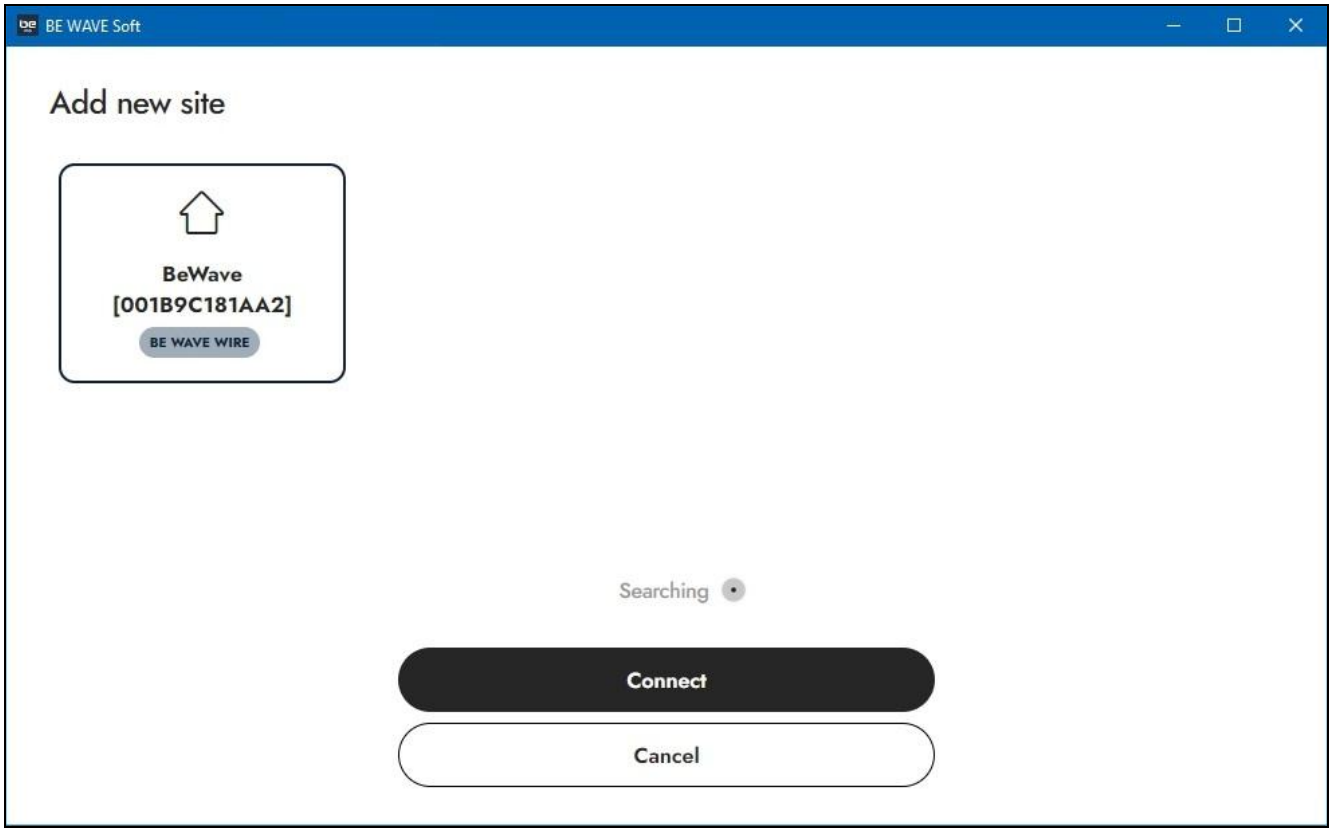
5.3.2 Adding the control panel in the BE WAVE Soft program

Adding the first control panel (site)

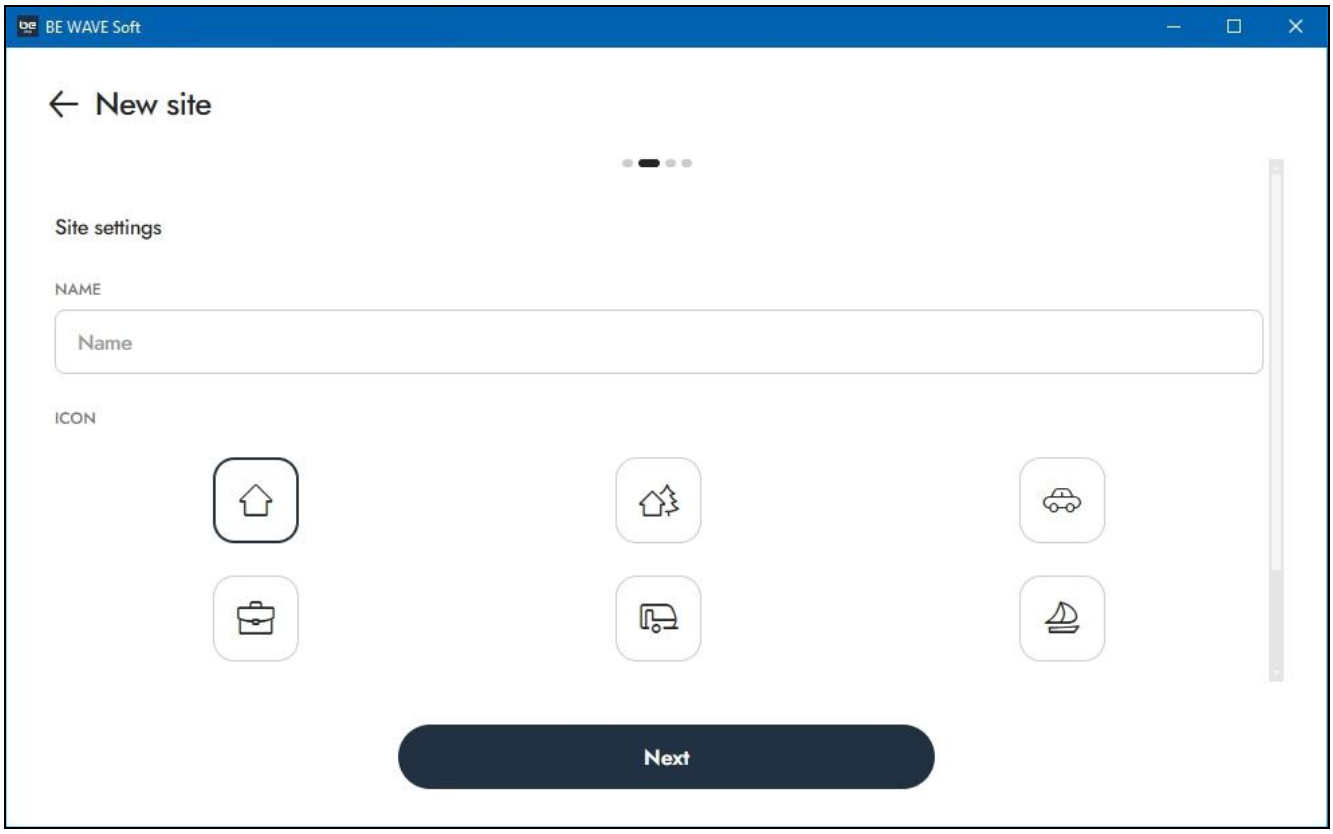
1. Start the BE WAVE Soft program. The *Add new site* window will be displayed.



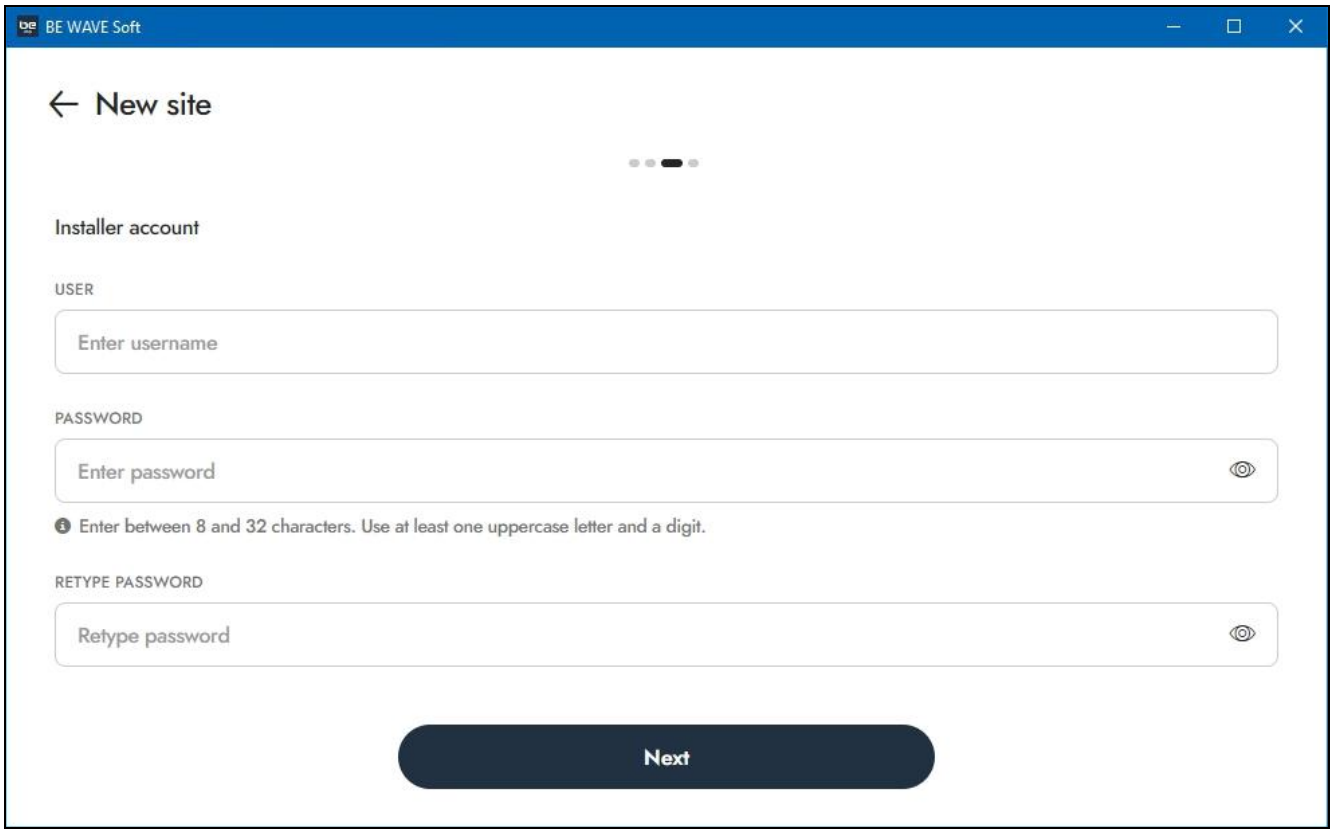
2. Click the control panel (site) you want to add. Different buttons will appear at the bottom of the window.



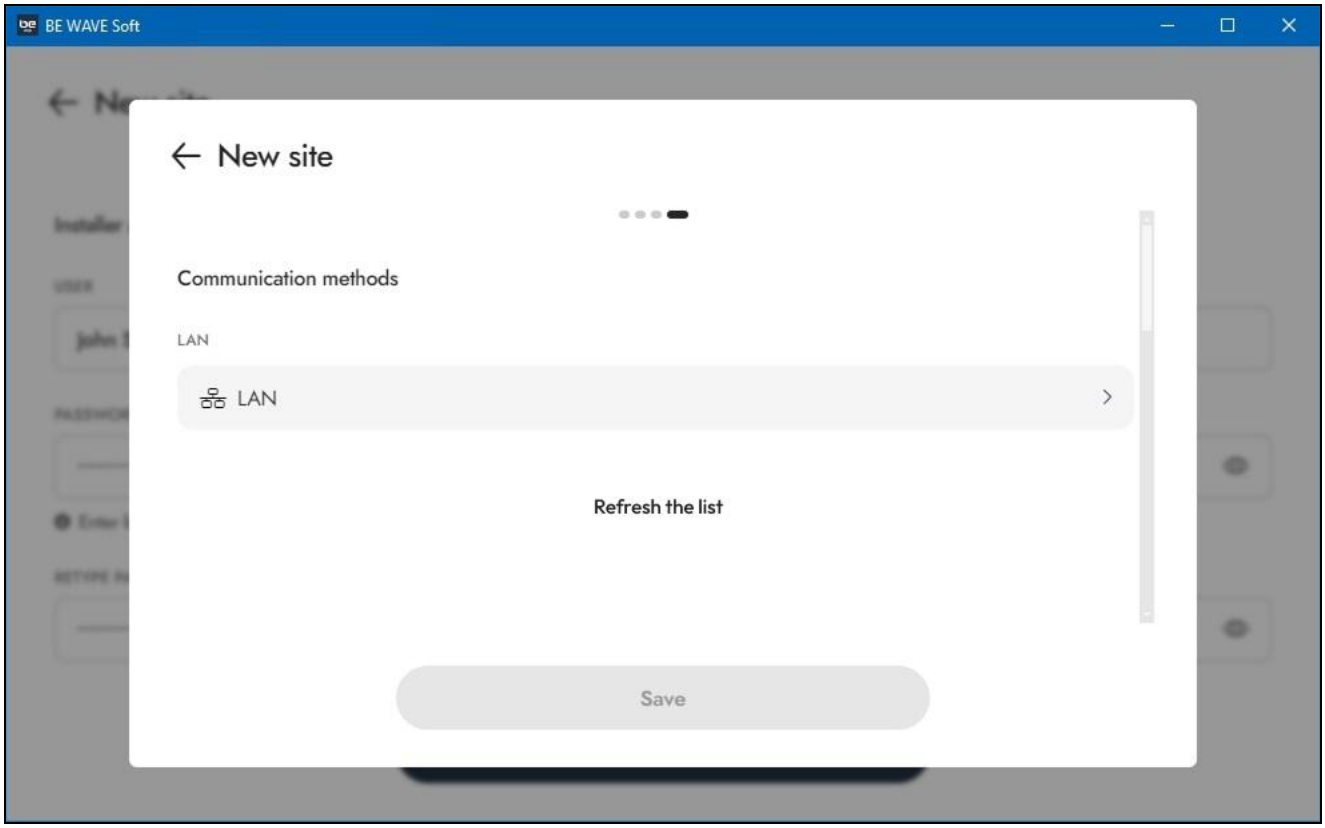
3. Click *Connect*. The *New site – Site settings* window will be displayed.



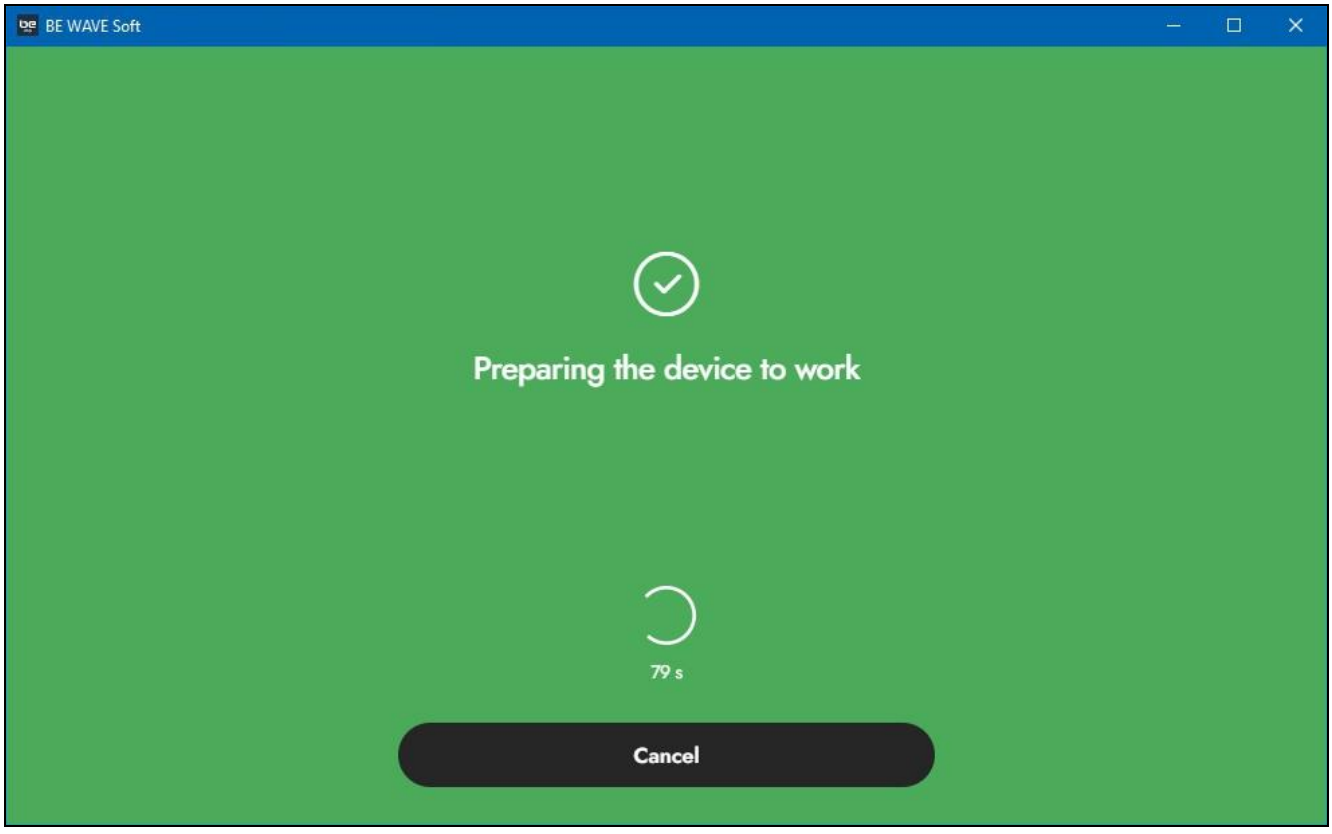
4. Enter the name of the site and select one of the icons to represent the site, then click *Next*. The *New site – Installer account* window will be displayed.



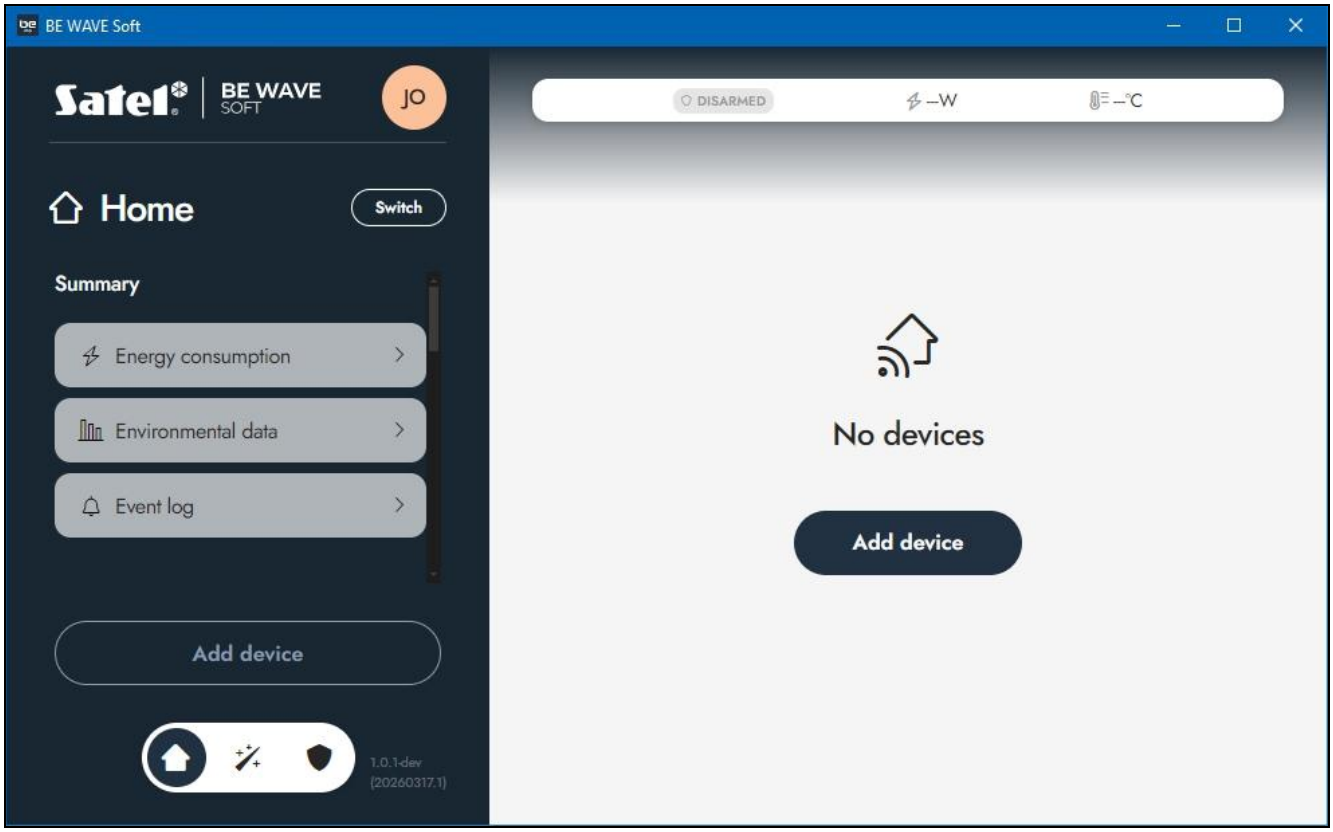
5. Enter the username and password for the installer, then click *Save*. The *New site – Communication methods* window will be displayed.



6. Click *LAN*. A window for configuring network settings will be displayed (see "Communication settings" p. 55). 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.

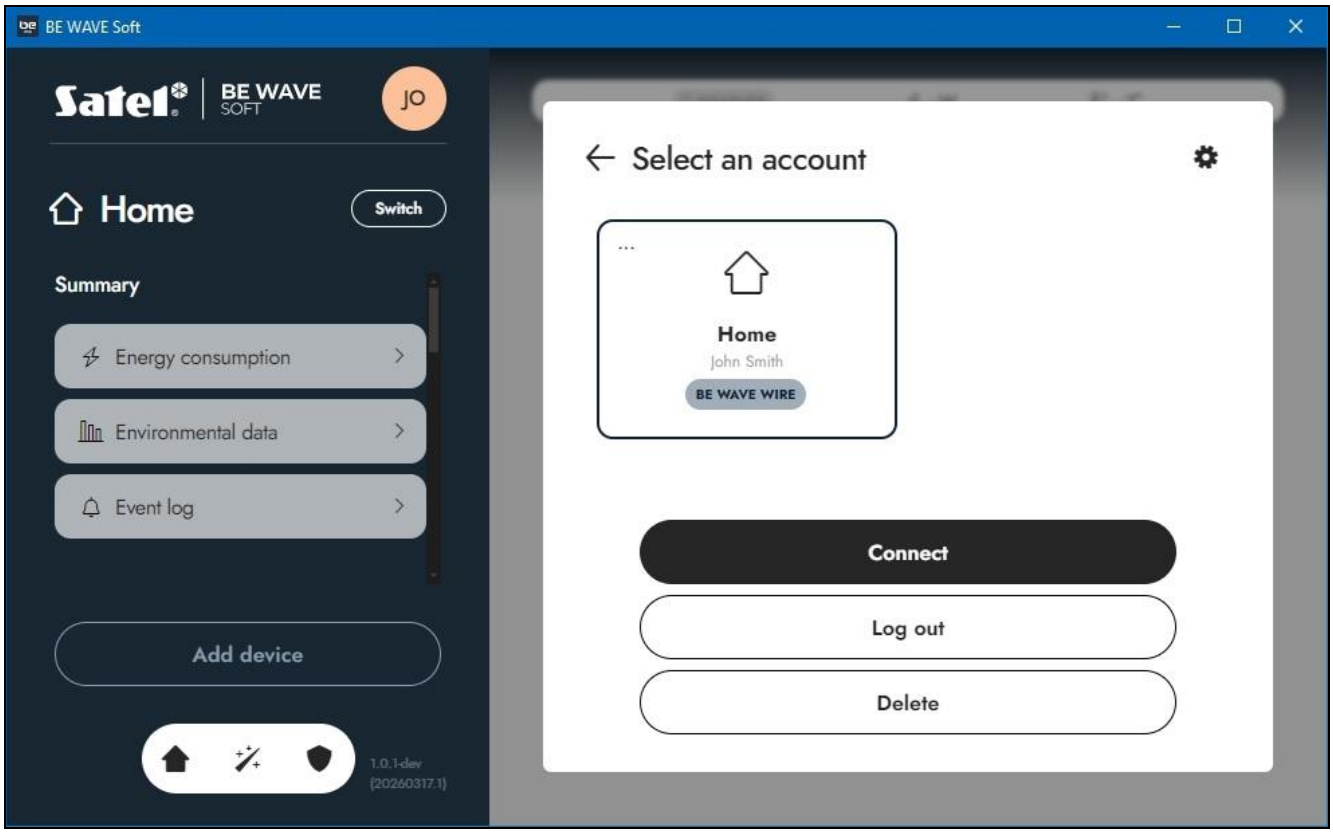


7. When the program connects to the control panel, the program's home screen will be displayed. You can add the first device to the system.

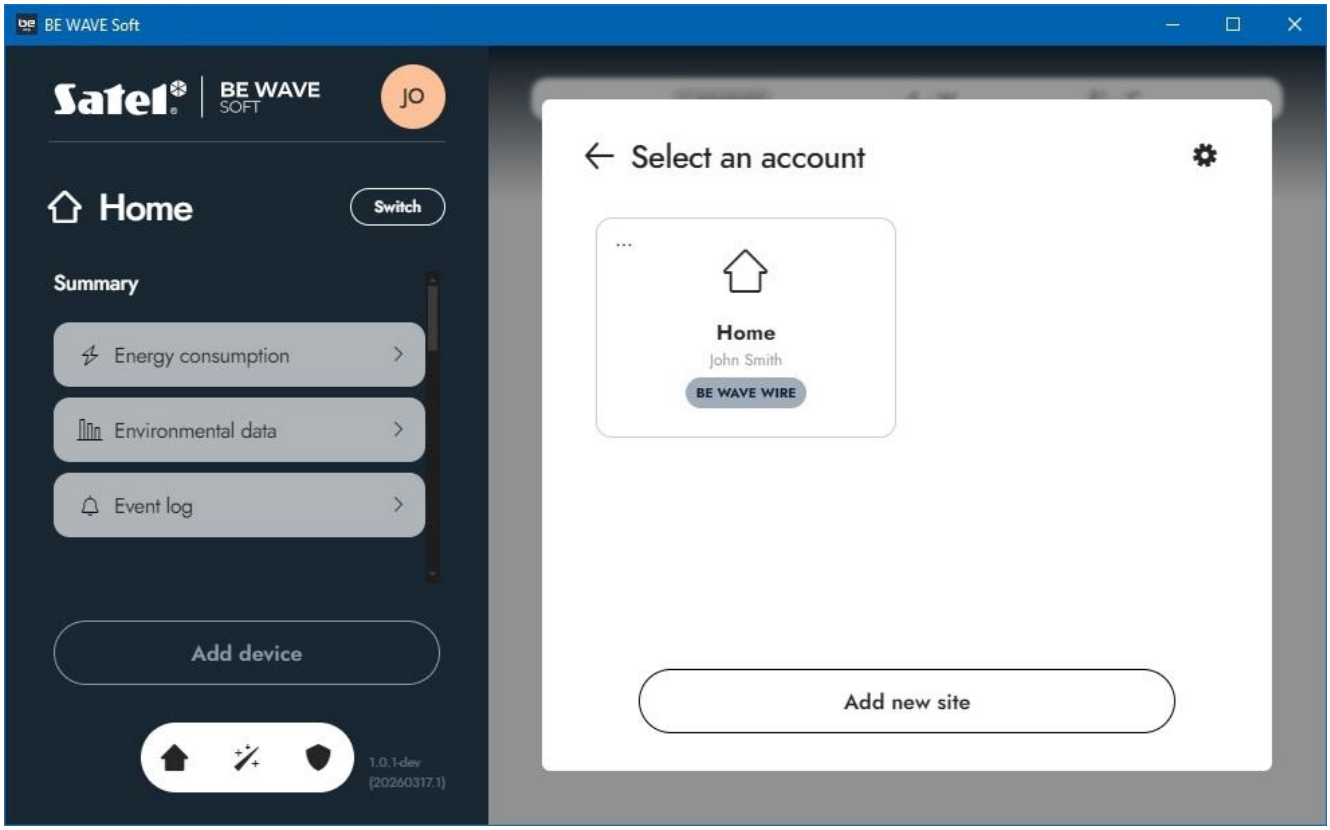


Adding another control panel (site)

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



2. 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.



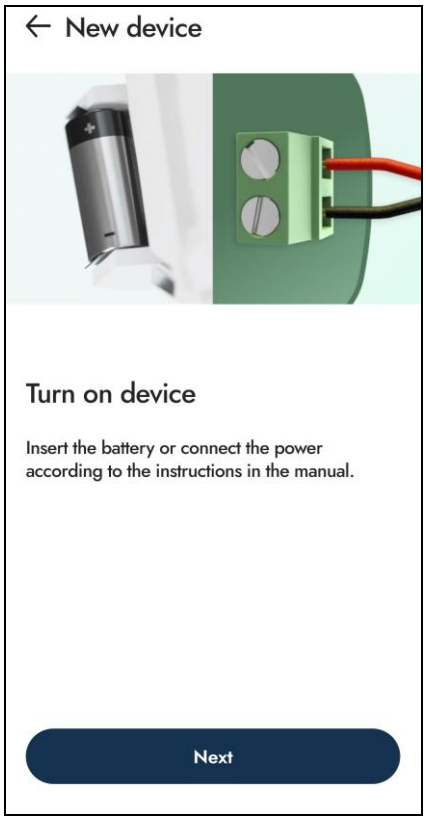
3. Click *Add new site*. The *Add new site* window will be displayed.
4. In the next steps, the procedure is the same as for adding the first control panel.

5.4 Adding mainboard zones and outputs to the system

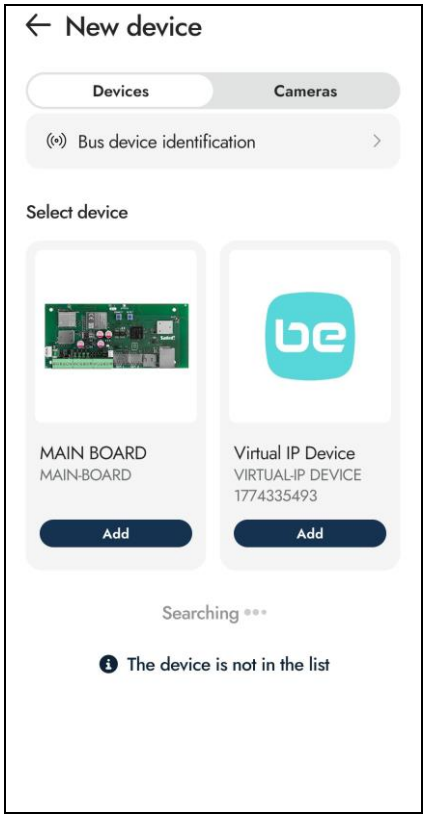
The mainboard zones / outputs must be added to the system so that the system can support the devices connected to them.

5.4.1 Adding mainboard zones and outputs in the Be Wave app

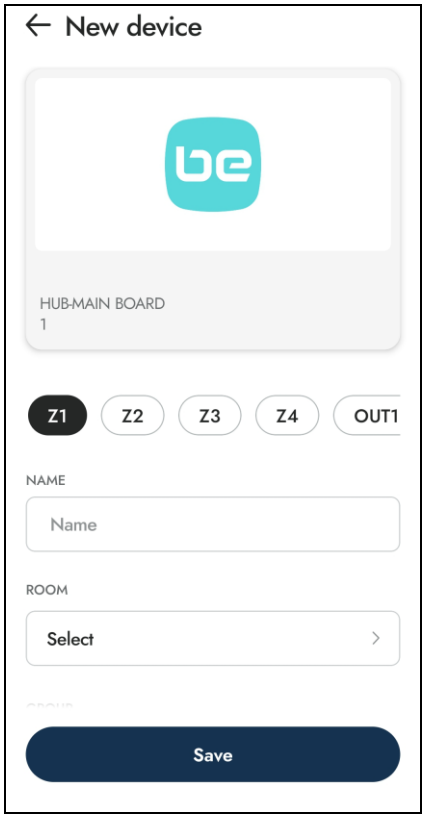
1. Tap the *Add device* button on the home screen. On a new screen you will be asked to turn on the device.



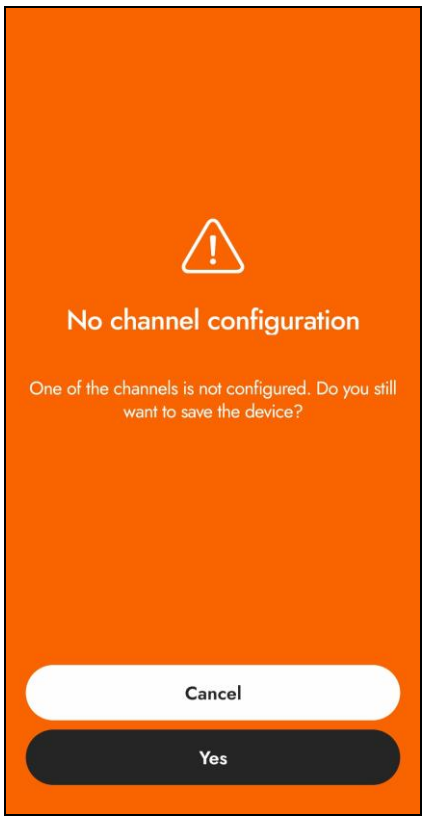
2. Tap *Next*. The list of devices you can add will be displayed



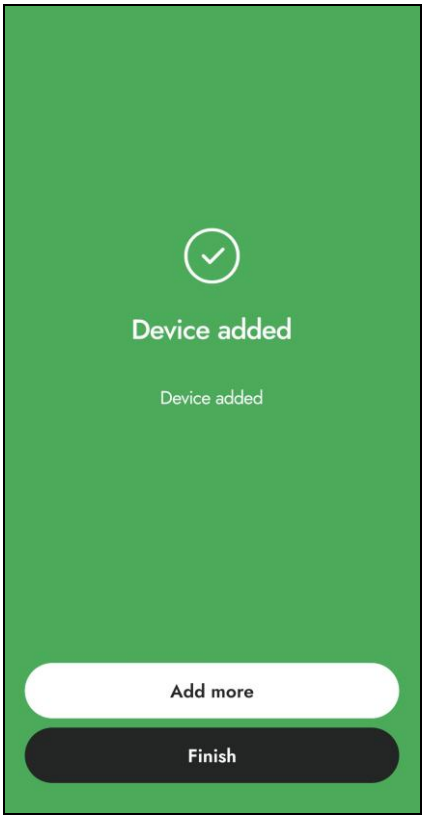
3. Tap *MAIN BOARD*. The screen with mainboard zone / output settings will be displayed.



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. 51), 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.



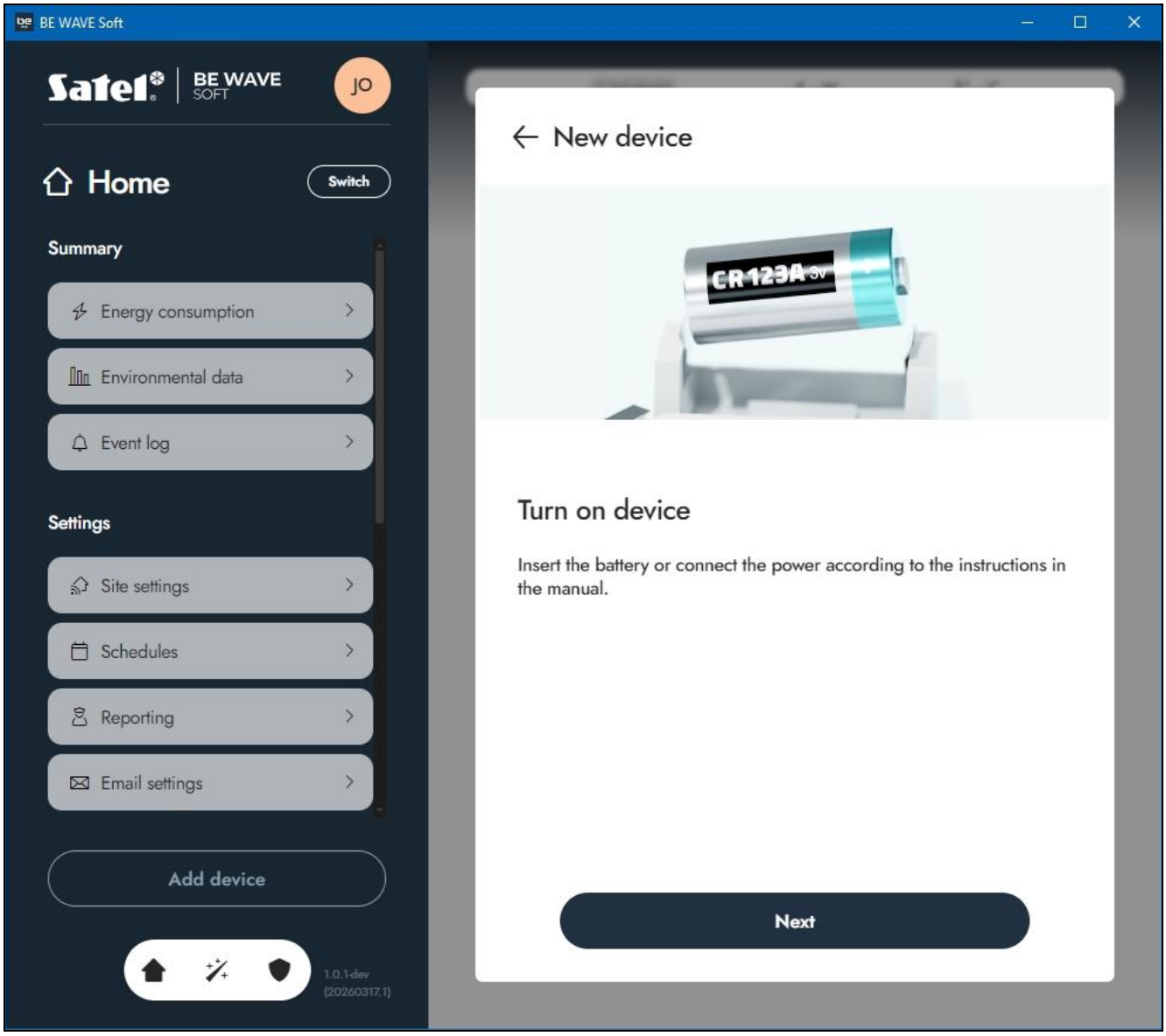
6. If you configured all zones / outputs (channels) or you tapped *Yes* on the warning screen, a screen will be displayed saying that the device has been added.



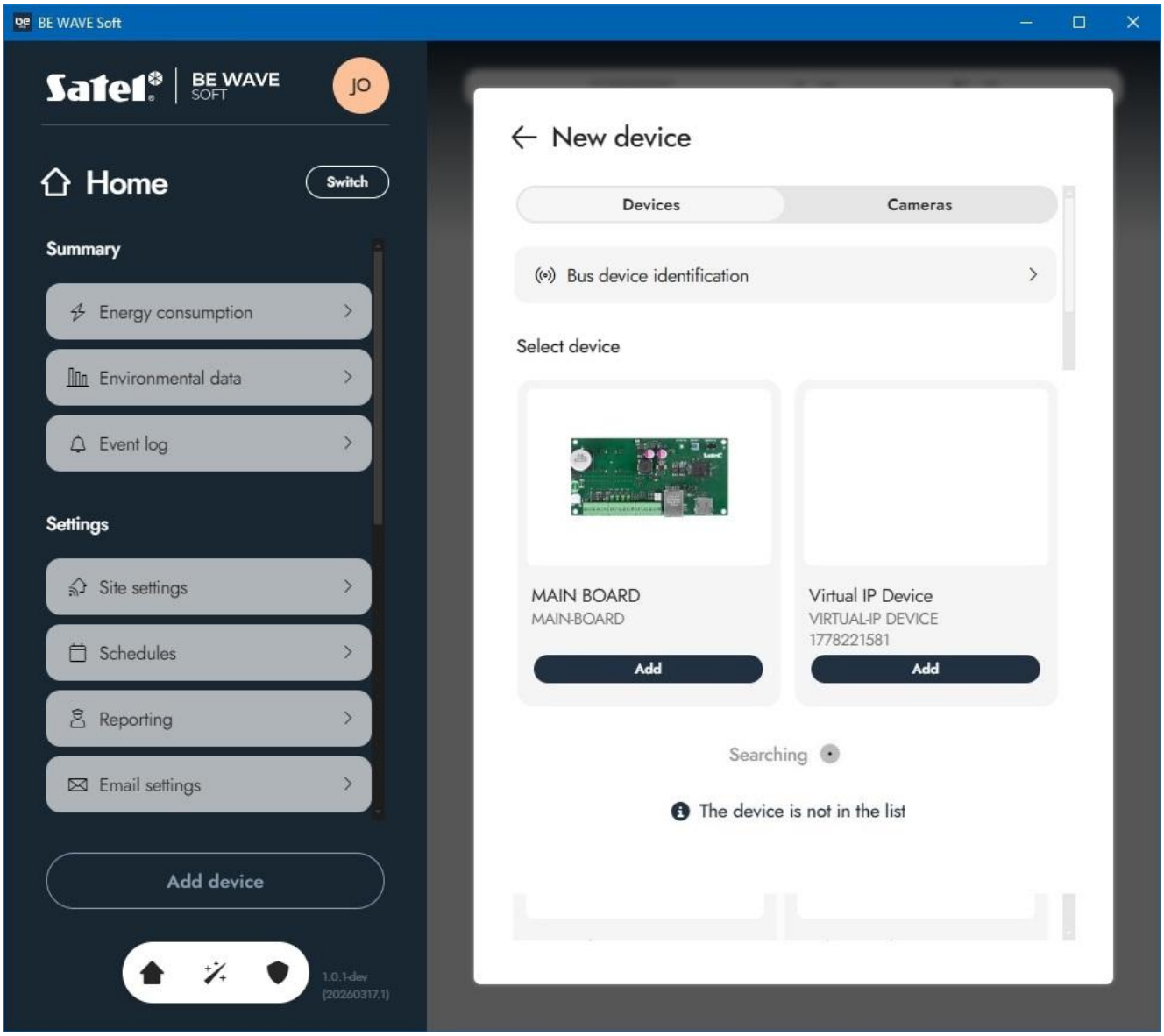
7. Tap *Add more* if you want to add another device or *Finish* if you do not want add any more devices.
8. Configure additional settings if it is required for the zone / output (e.g. output for which the *Alarm* operation mode has been selected require programming the alarm sources – see “Alarm source” p. 54).

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

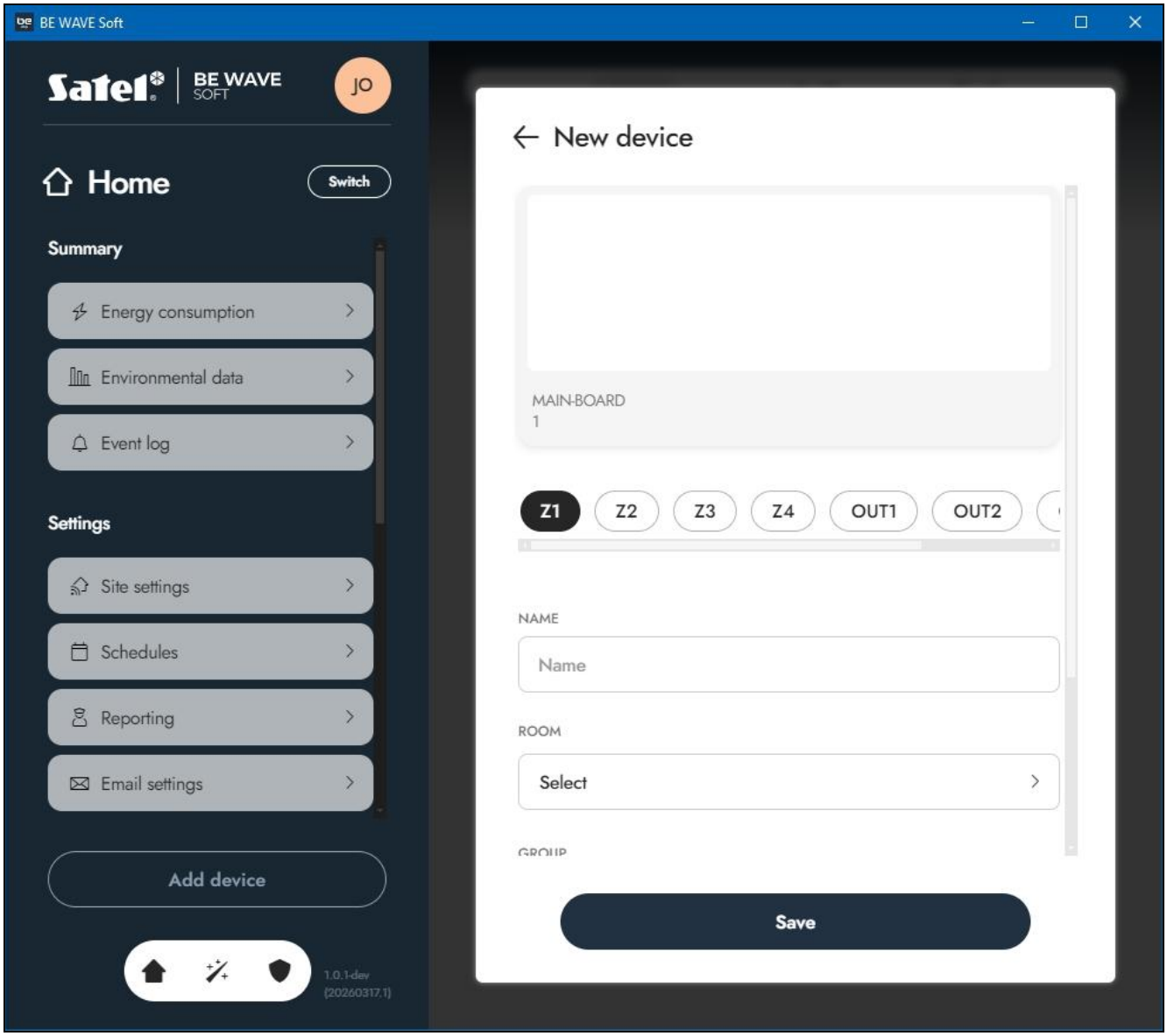
1. Click the *Add device* button. In the new window you will be asked to turn on the device.



2. Click *Next*. The list of devices you can add will be displayed.

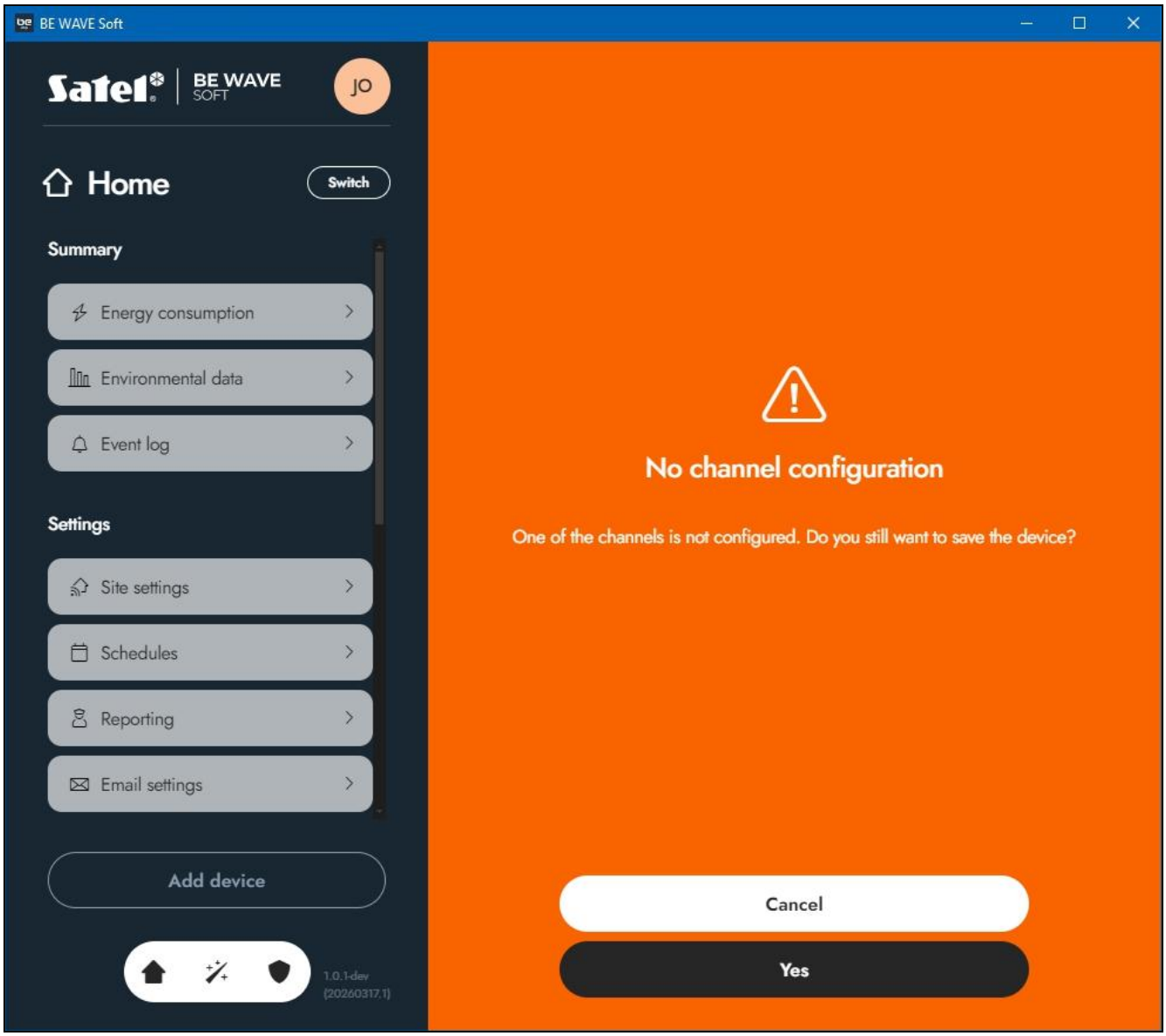


3. Click *MAIN BOARD*. The window with mainboard zones / outputs will be displayed.

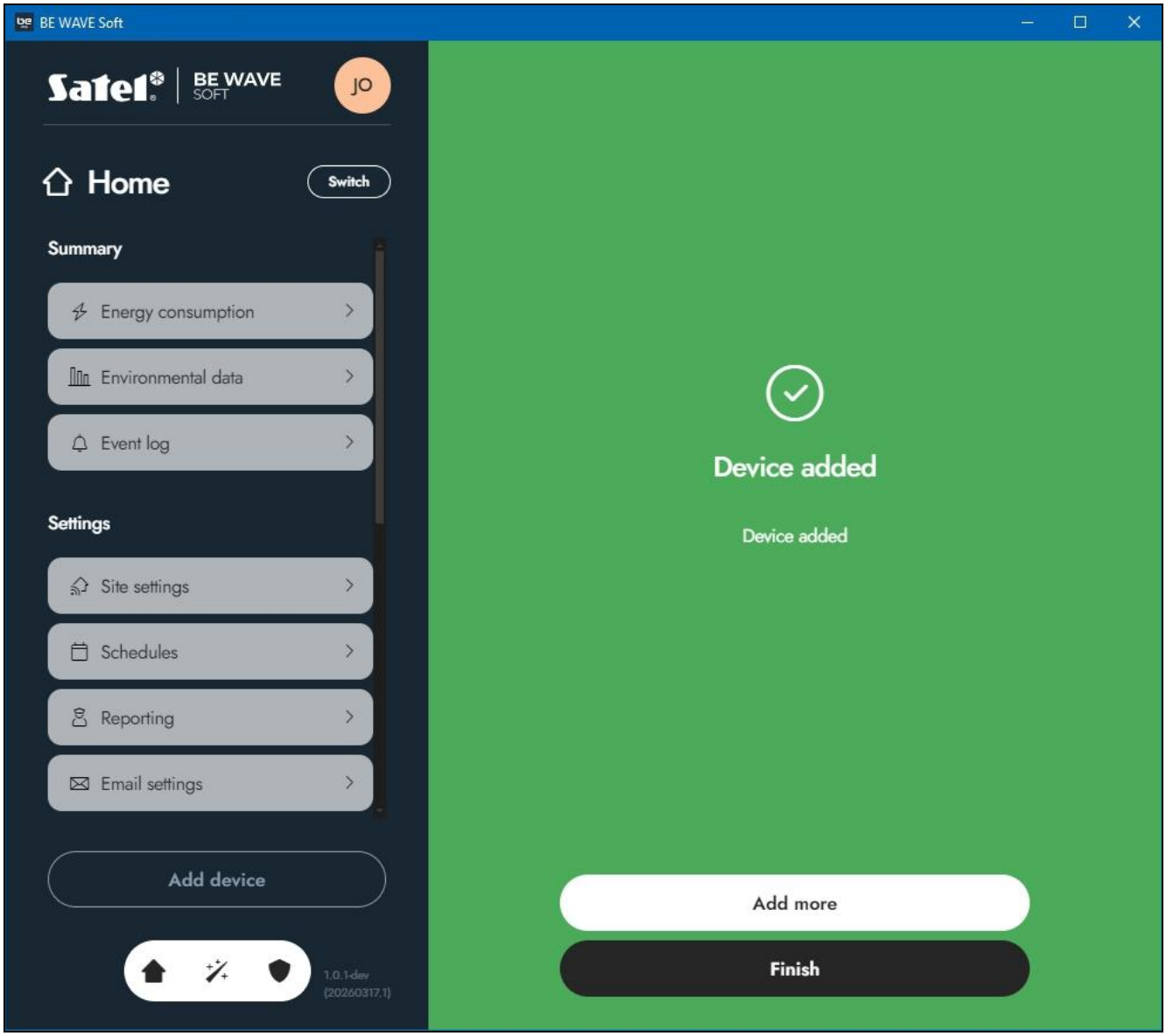


4. Configure the settings of zones / outputs you want to add to the system (enter the name, assign the zone / output to a room and a group, select the zone type / output operation mode – see “Device settings” p. 51), then click *Save*.

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.

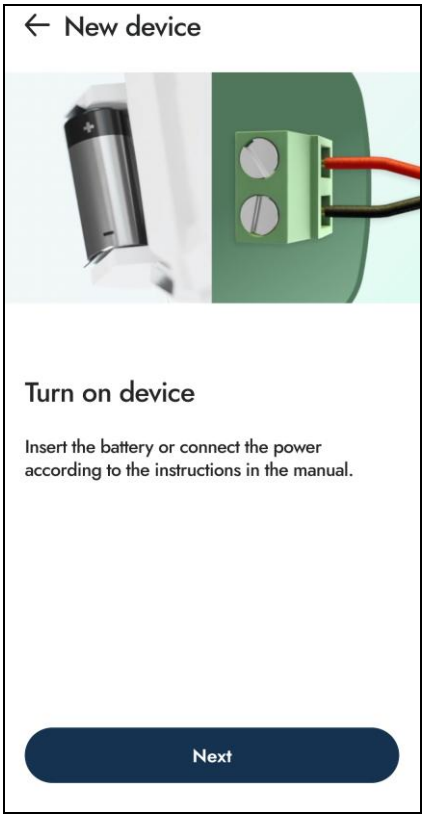


7. Click *Add more* if you want to add another device or *Finish* if you do not want to add any more devices.
8. Configure additional settings if it is required for the zone / output (e.g. output for which the *Alarm* operation mode has been selected require programming the alarm sources – see “Alarm source” p. 54).

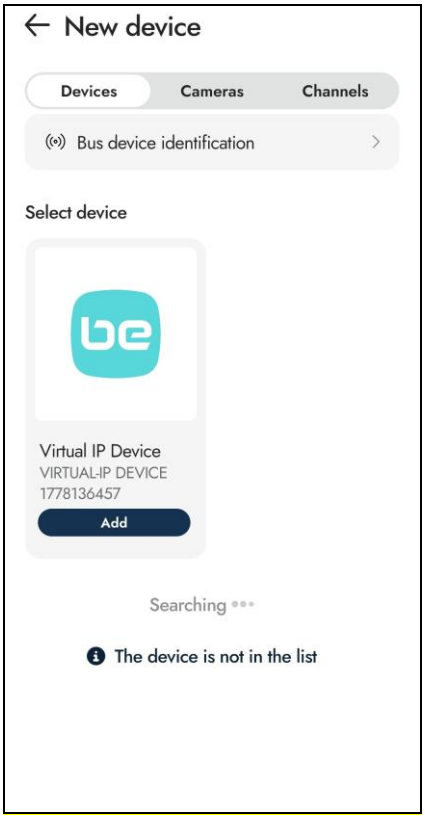
5.5 Adding a bus device to the system

5.5.1 Adding a bus device in the Be Wave app

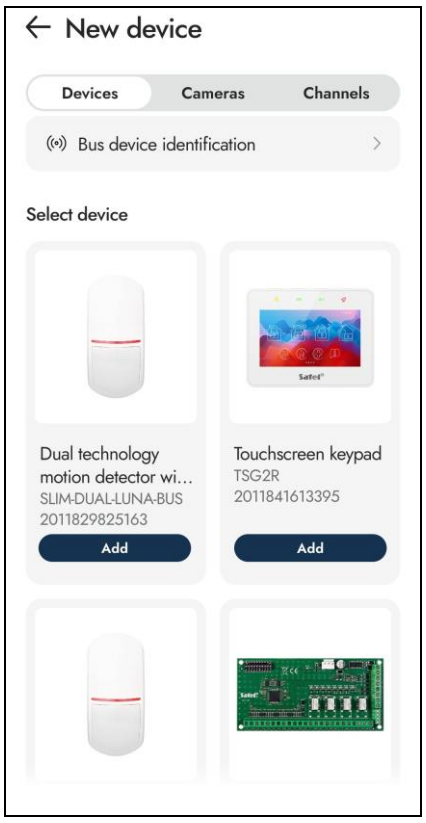
1. Tap the *Add device* button on the room screen, group screen or *Settings* screen. On a new screen you will be asked to turn on the device.



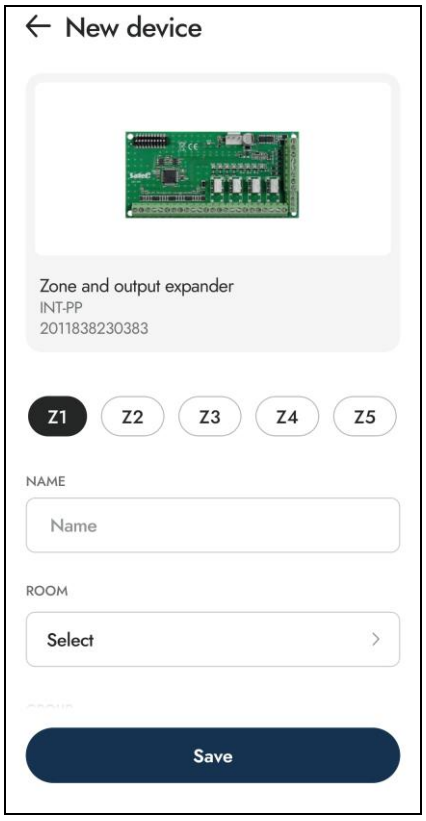
2. Tap *Next*. The list of devices you can add will be displayed.



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).

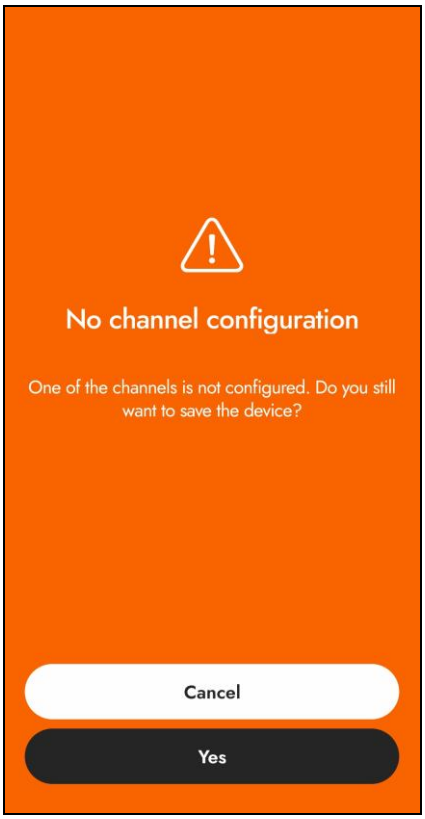


4. Tap the bus device you want to add. A screen with device settings will be displayed (the screenshot is an example).

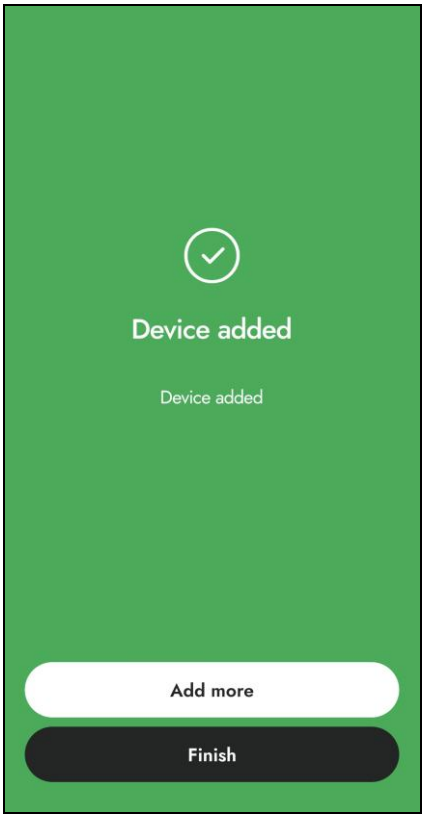


5. Configure the device settings (enter the name, assign the device to a room and to a group, etc. – see “Device settings” p. 51), then tap *Save*.

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.

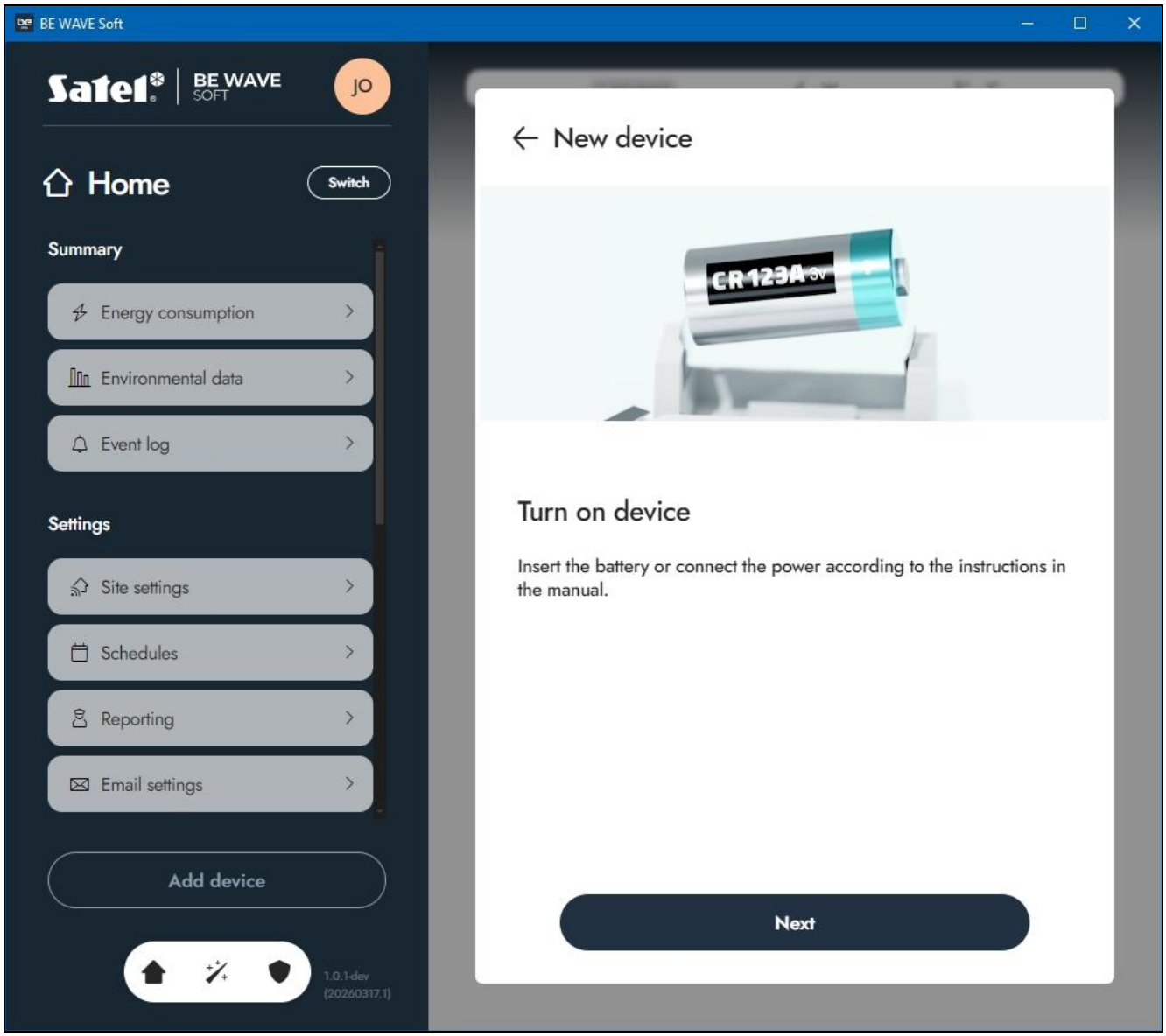


8. Tap *Add more* if you want to add another device or *Finish* if you do not want add any more devices.

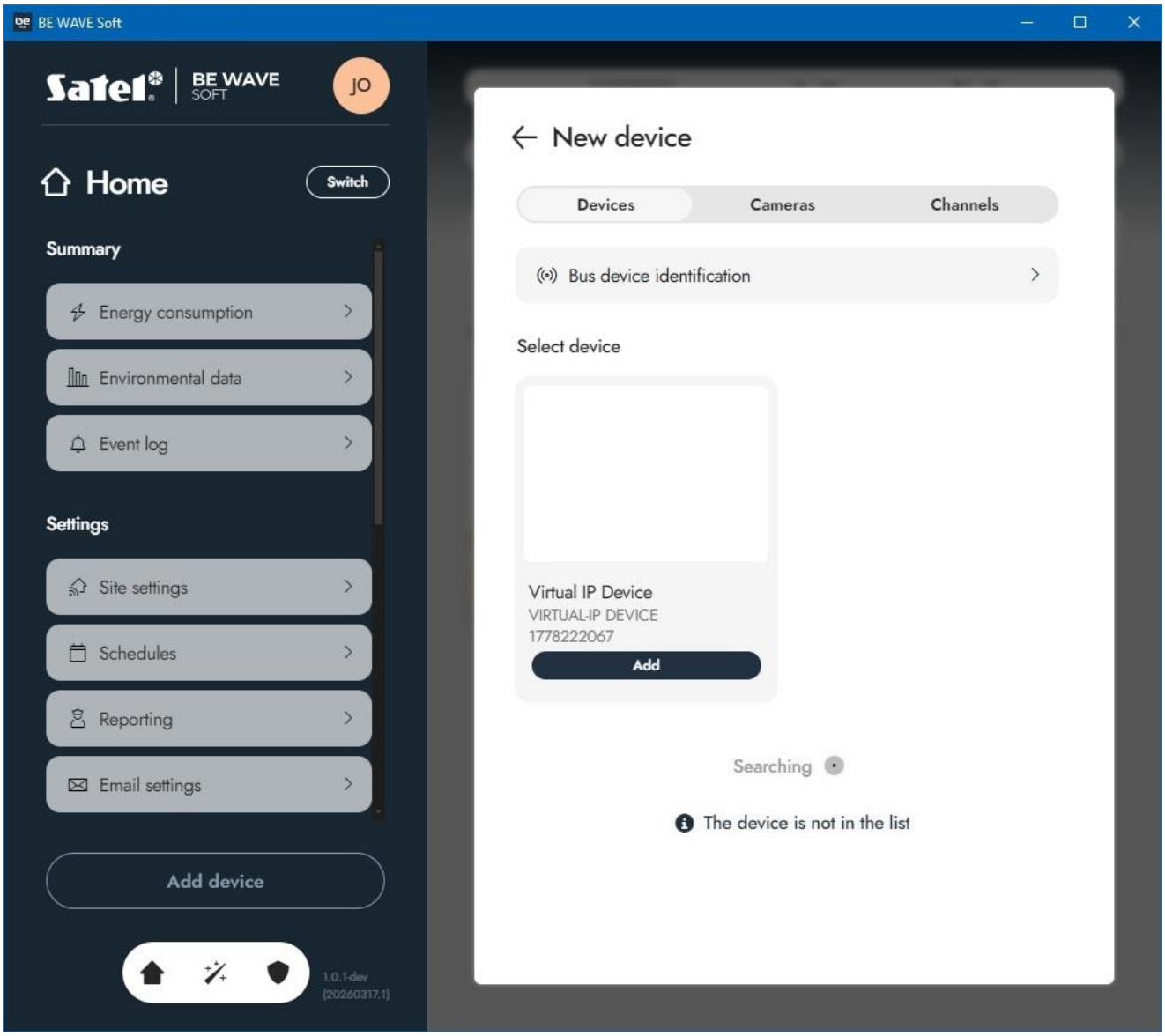
9. Configure additional settings if it is required for the device (e.g. output for which the *Alarm* operation mode has been selected require programming the alarm sources – see “Alarm source” p. 54).

5.5.2 Adding a bus device in the BE WAVE Soft program

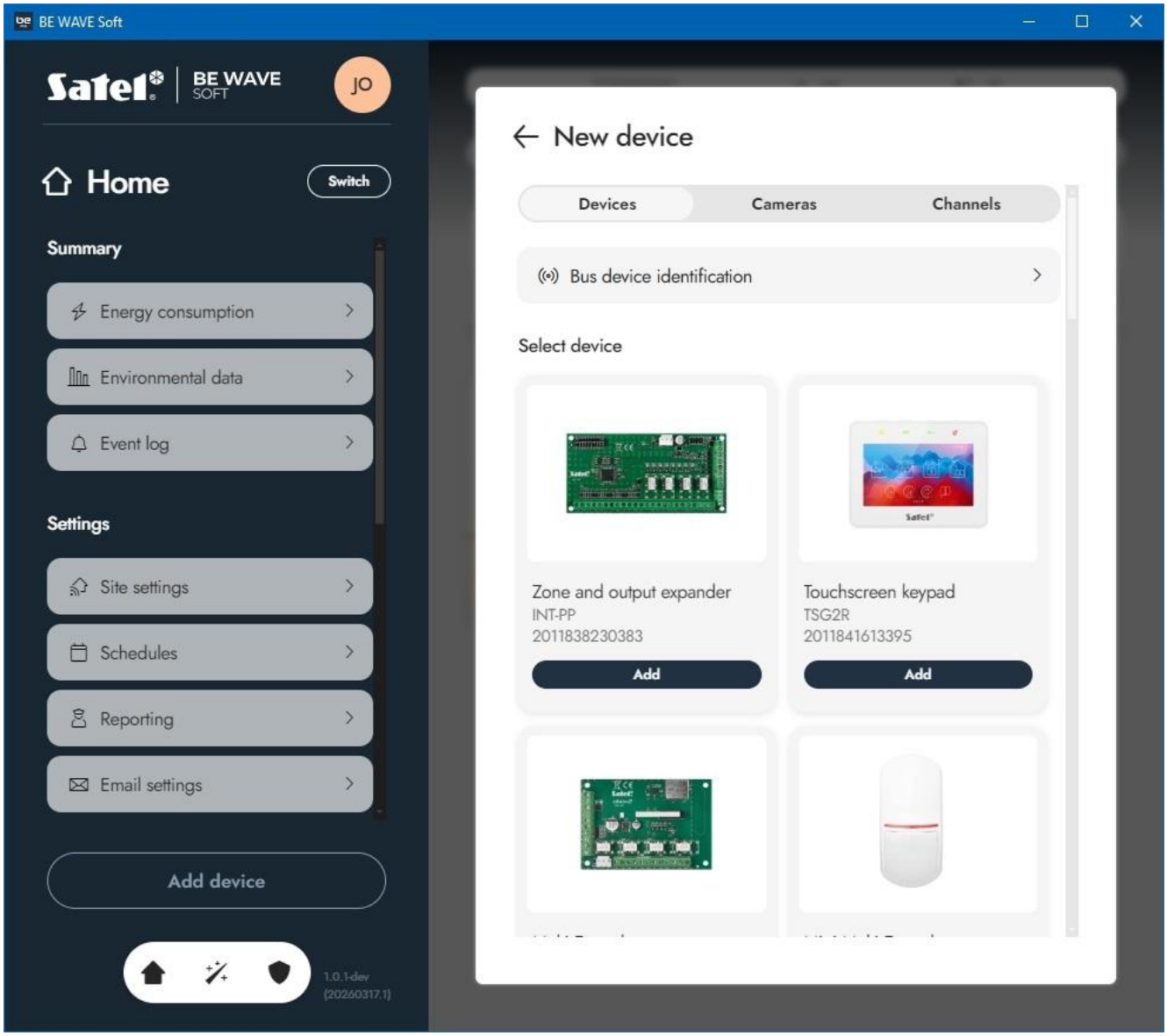
1. Click the *Add device* button on the side menu, in the room window or group window. In the new window you will be asked to turn on the device.



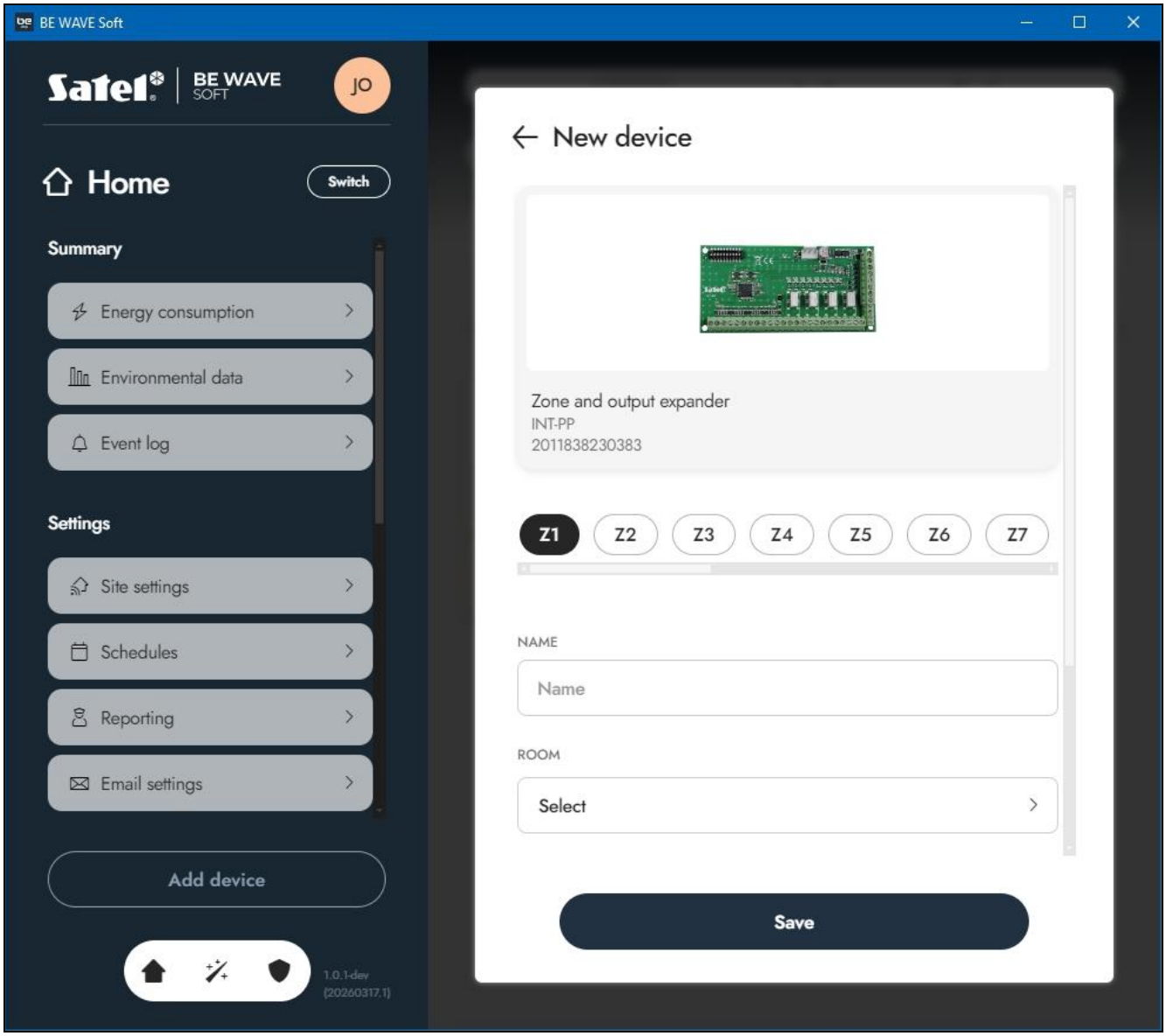
2. Click *Next*. The list of devices you can add will be displayed.



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).

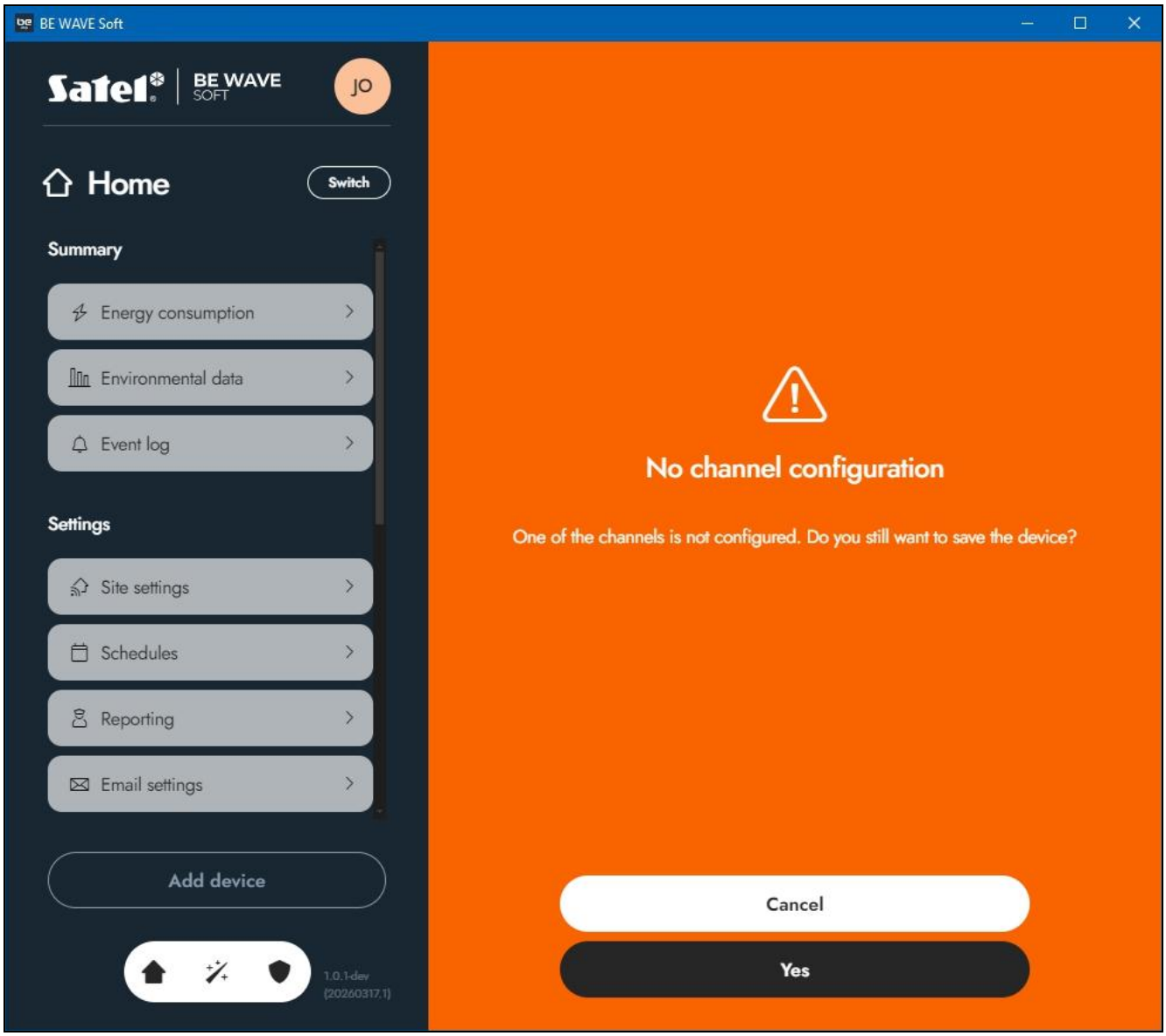


4. Click the bus device you want to add. A window with device settings will be displayed (the screenshot is an example).

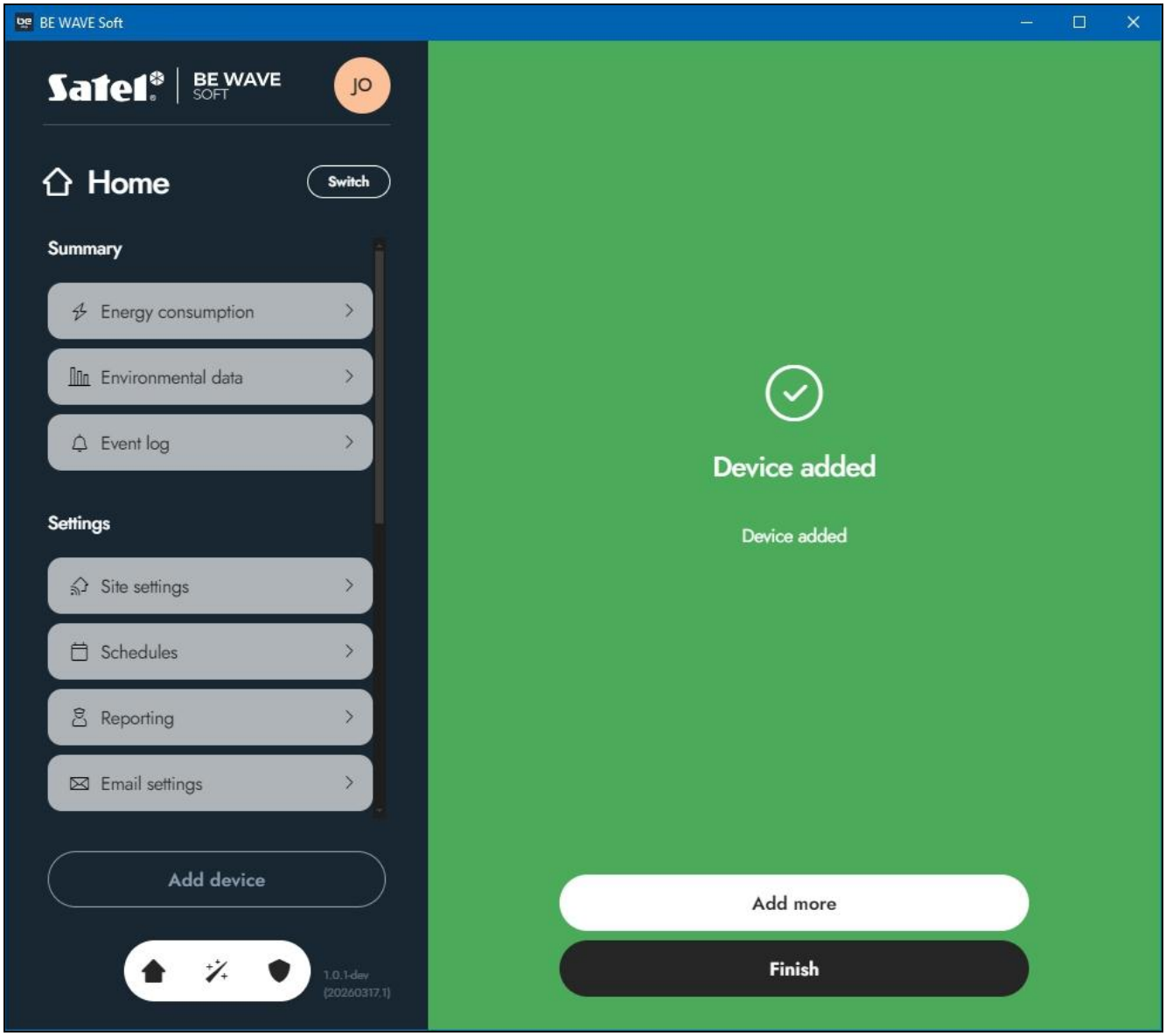


5. Configure the device settings (enter the name, assign the device to a room and to a group, etc. – see “Device settings” p. 51), then click *Save*.

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.

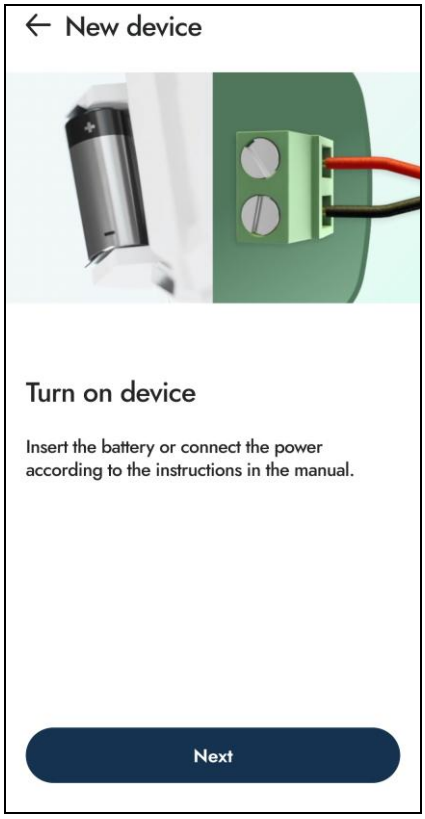


8. Click *Add more* if you want to add another device or *Finish* if you do not want to add any more devices.
9. Configure additional settings if it is required for the device (e.g. output for which the *Alarm* operation mode has been selected require programming the alarm sources – see “Alarm source” p. 54).

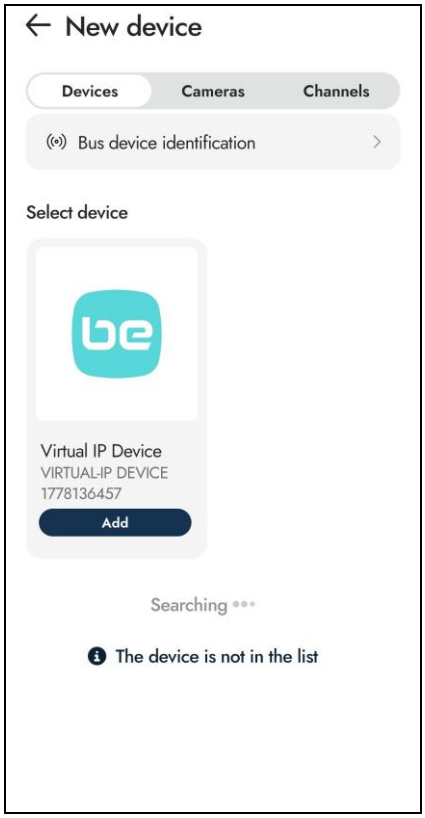
5.6 Adding a virtual IP device to the system

5.6.1 Adding a virtual IP device in the Be Wave app

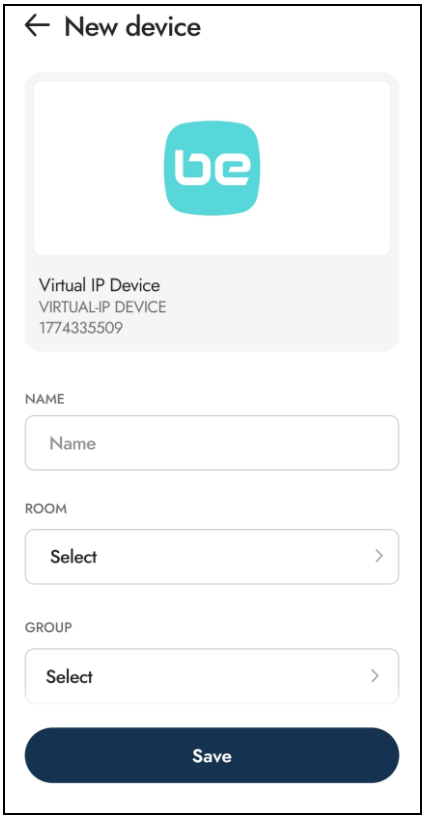
1. Tap the *Add device* button on the room screen, group screen or *Settings* screen. On a new screen you will be asked to turn on the device.



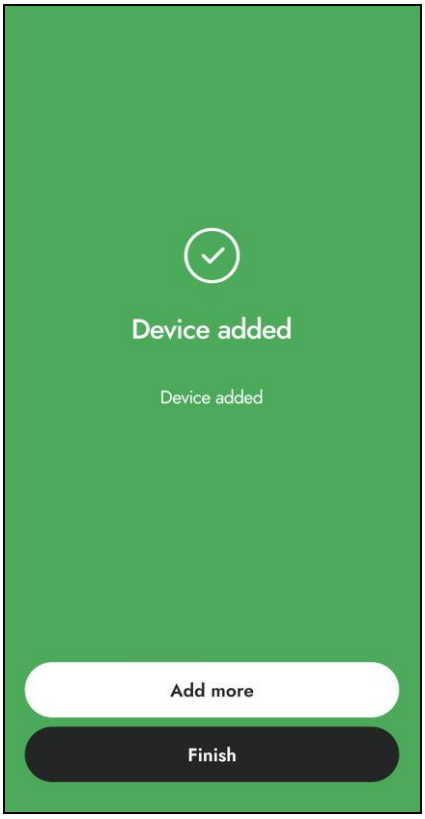
2. Tap *Next*. The list of devices you can add will be displayed (the screenshot is an example).



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. 51), then tap *Save*. A screen will be displayed saying that the device has been added.

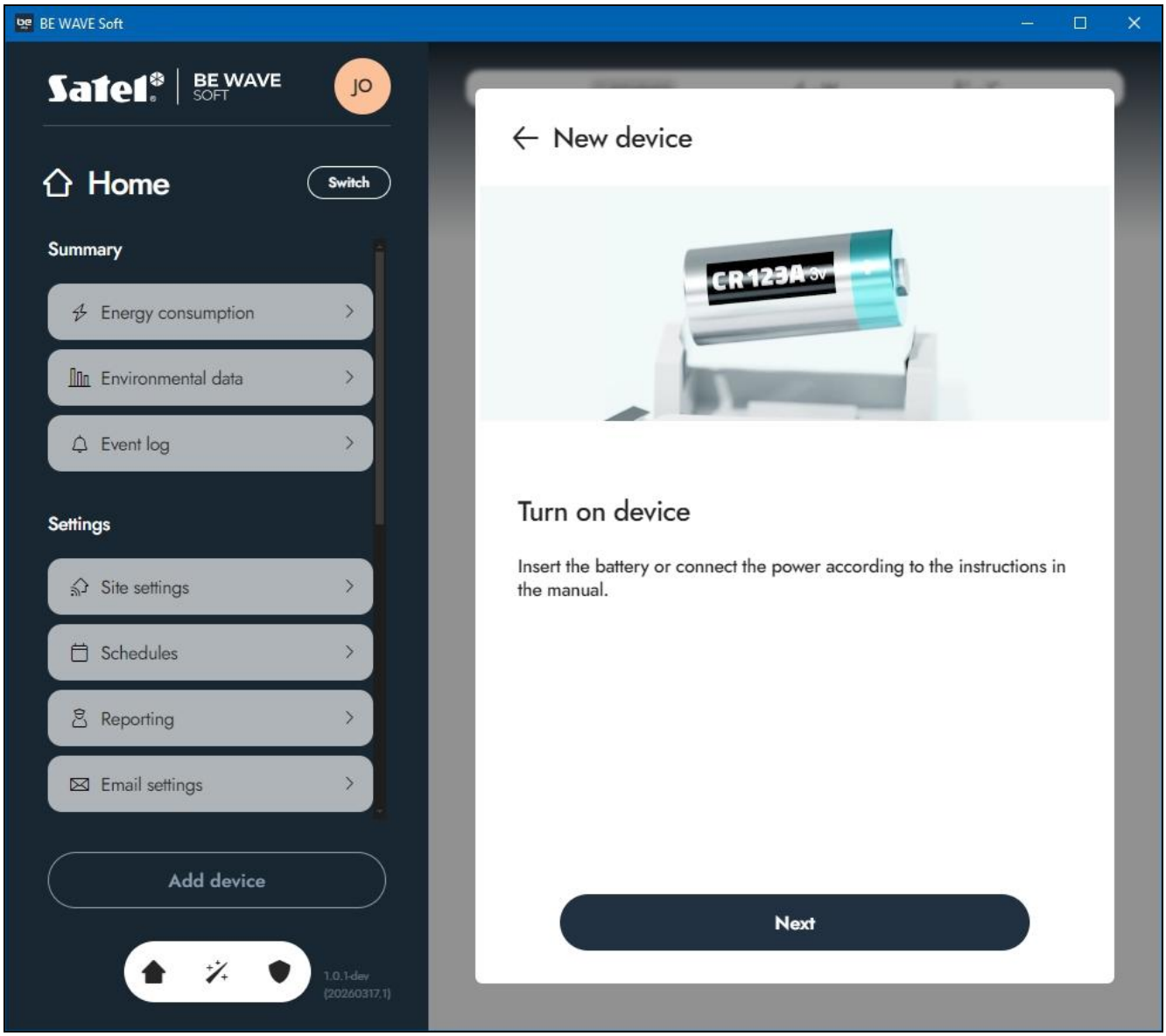


5. Tap *Add more* if you want to add another device or *Finish* if you do not want add any more devices.

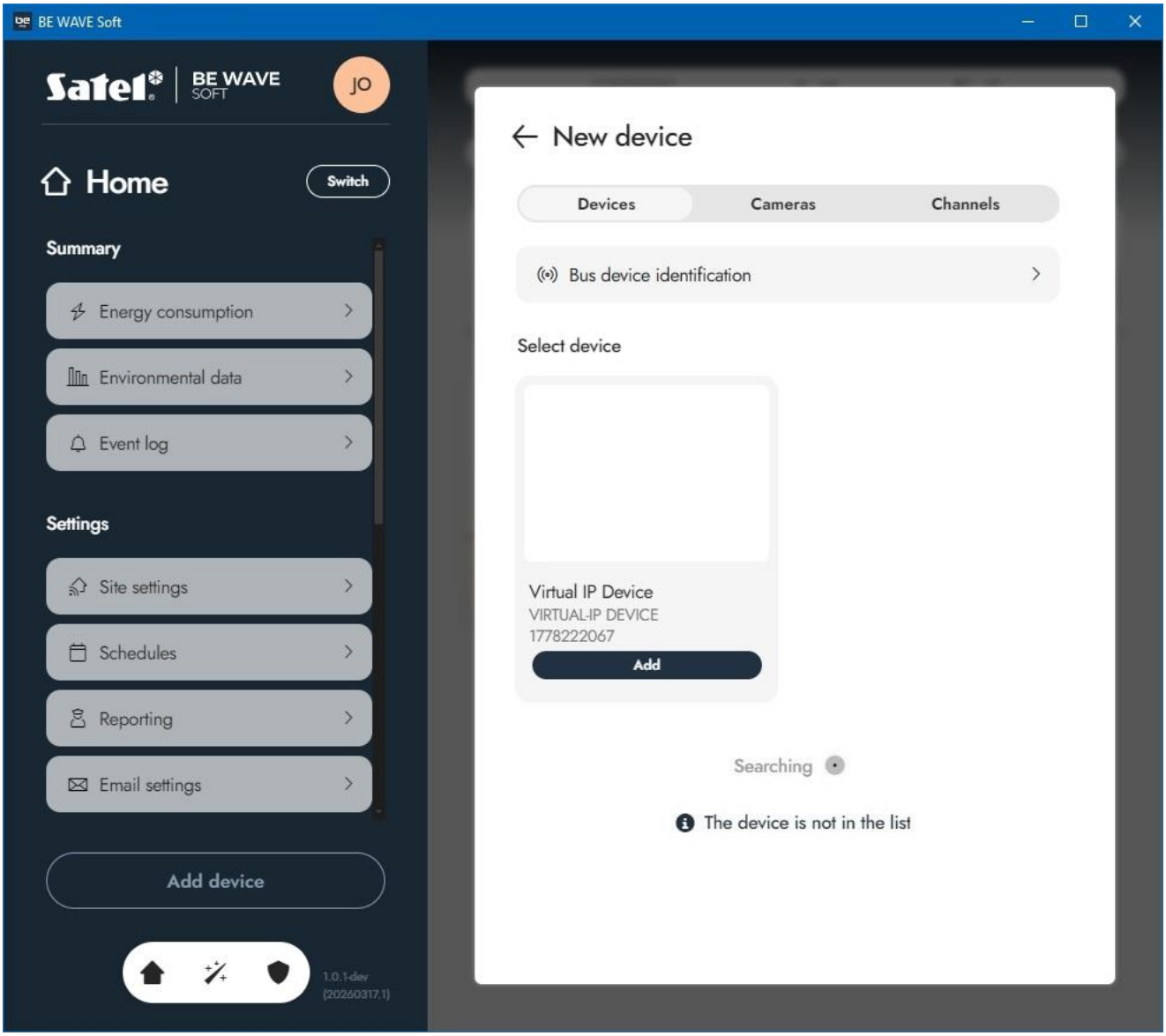
6. Configure additional settings of the IP device (see “IP device settings” p. 54).

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

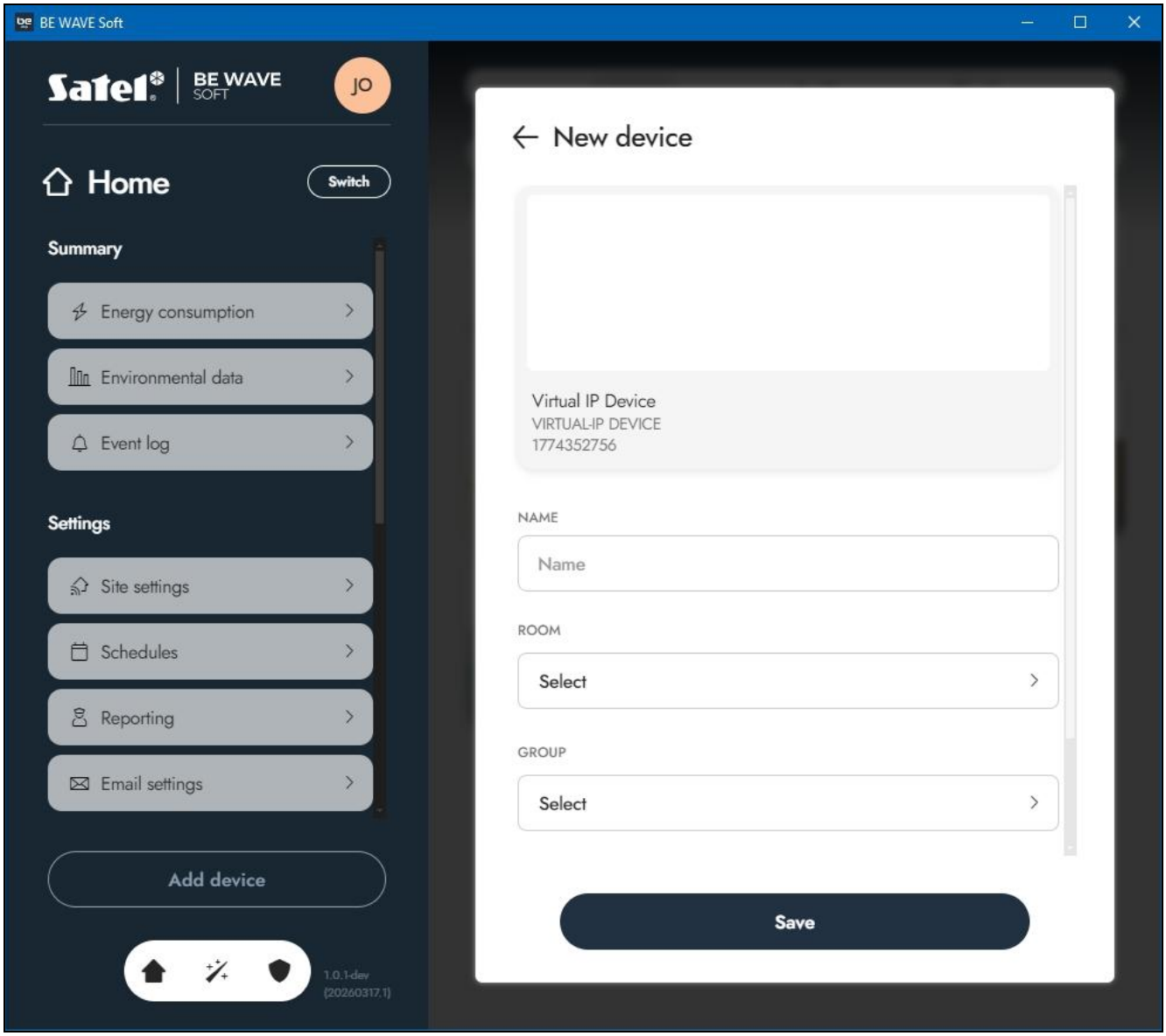
1. Click the *Add device* button on the side menu, in the room window or group window. In the new window you will be asked to turn on the device.



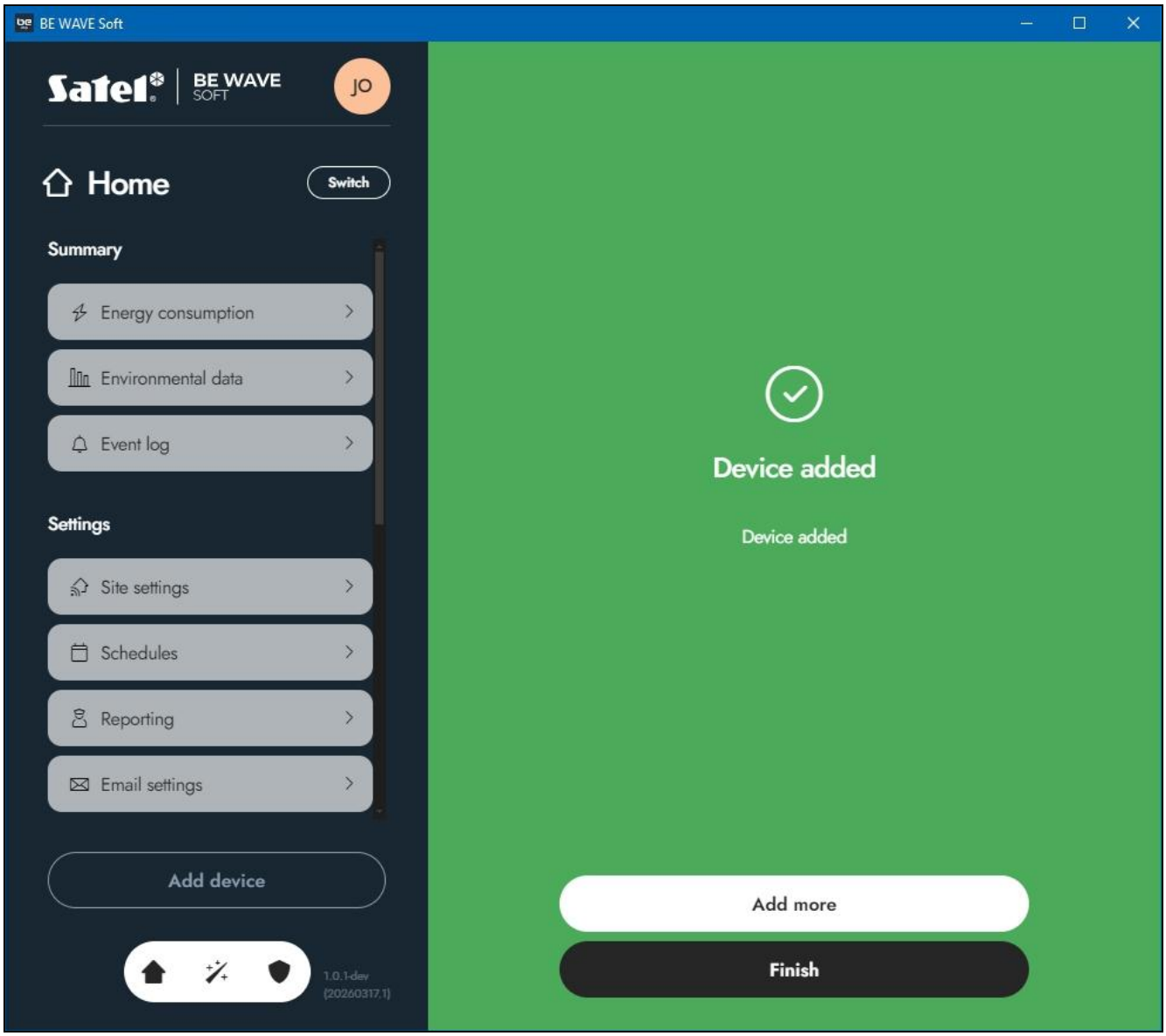
2. Click *Next*. The list of devices you can add will be displayed (the screenshot is an example).



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



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. 51), 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. 54).

5.7 Removing the device from the system

5.7.1 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.

5.7.2 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.

5.8 Description of settings

5.8.1 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.

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.

Type – parameter for the zone. Determines whether a button is connected to the zone:

None – no button is connected to the zone.

Single – a single button is connected to the zone.

Button type – parameter for the zone, if *Single* was selected for the button type. Specifies the type of the connected single button:

Switch

Bell

Remember after power loss – option for a wired output (mainboard, expanders). If enabled, after the power is restored, the output status from before the power loss will be recovered (set values, etc.).

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

5.8.2 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.

5.8.3 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.

5.8.4 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.

5.8.5 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*).

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.

5.8.6 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 kΩ.

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.

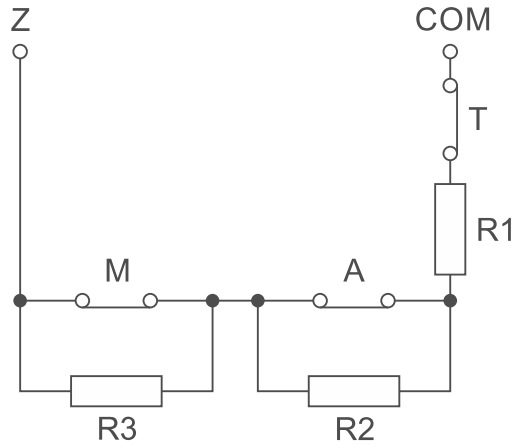


Fig. 5. Numbering of end-of-line resistors. The detector outputs are marked with letters: A - alarm, T – tamper, M – anti-masking.

5.8.7 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.

5.8.8 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.

5.8.9 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.

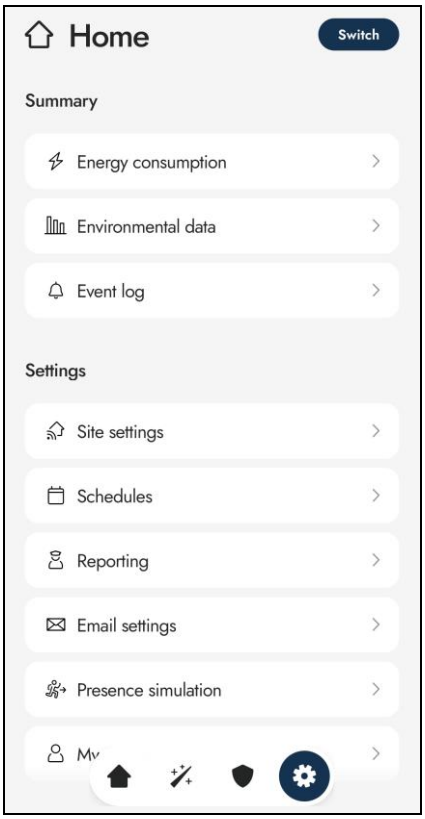
For security reasons, we recommend using DESFire cards with encrypted card numbers.

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

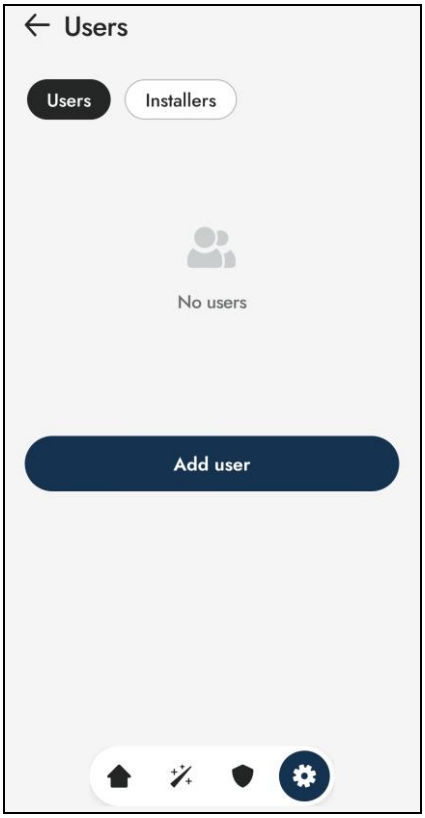
5.9 Adding a user

5.9.1 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.



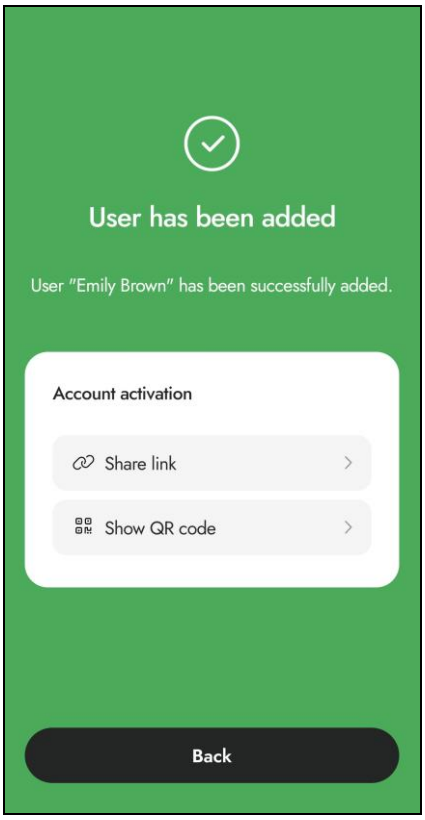
3. Tap the *Add user* button. The *New user* screen will be displayed.



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. 65) or *Part of the site* (see “User with access to a part of the site” p. 66) 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.

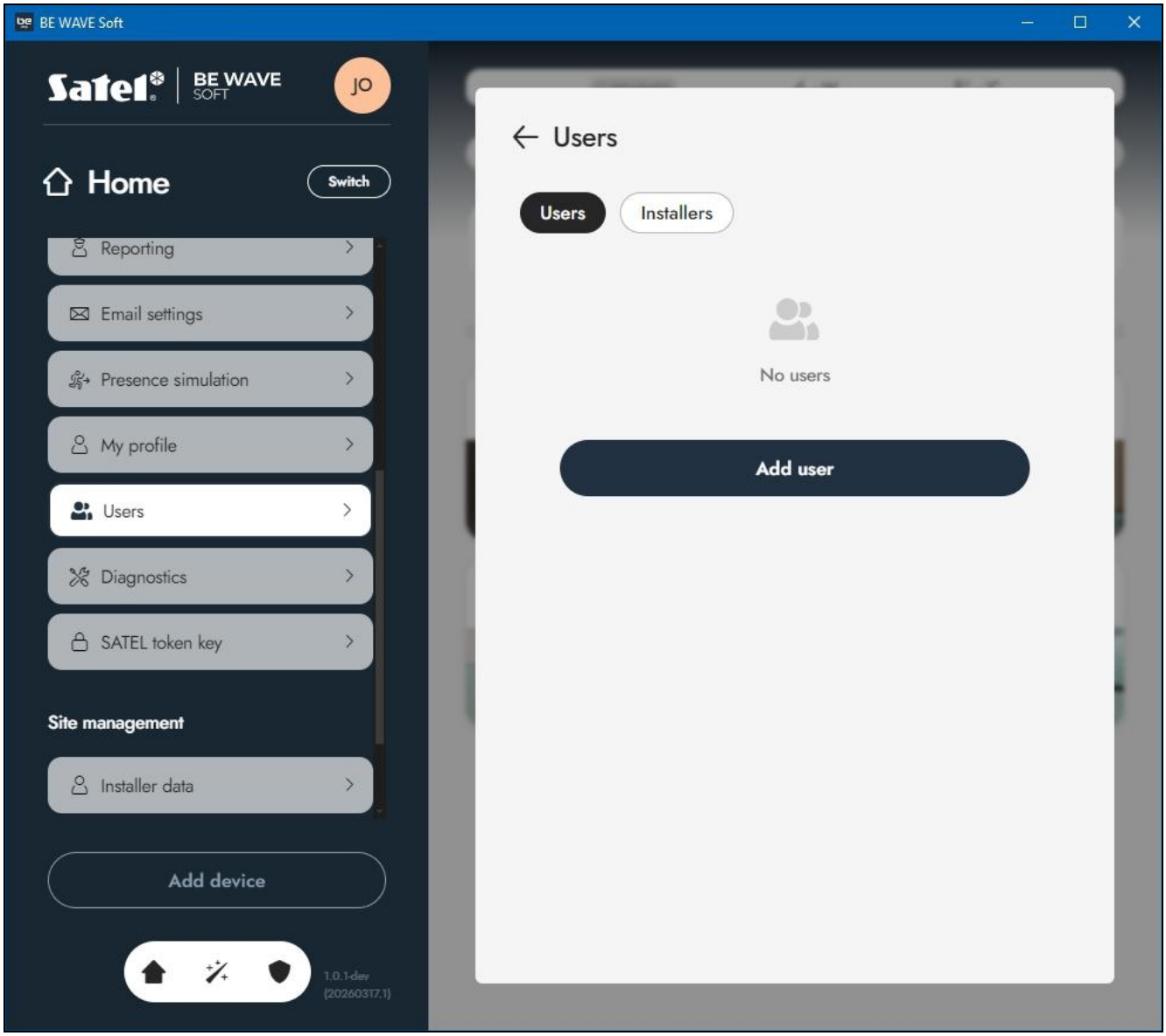
The user must activate the account within 24 hours of generating the link / QR code. Otherwise, the user will have to request a new link / QR code.



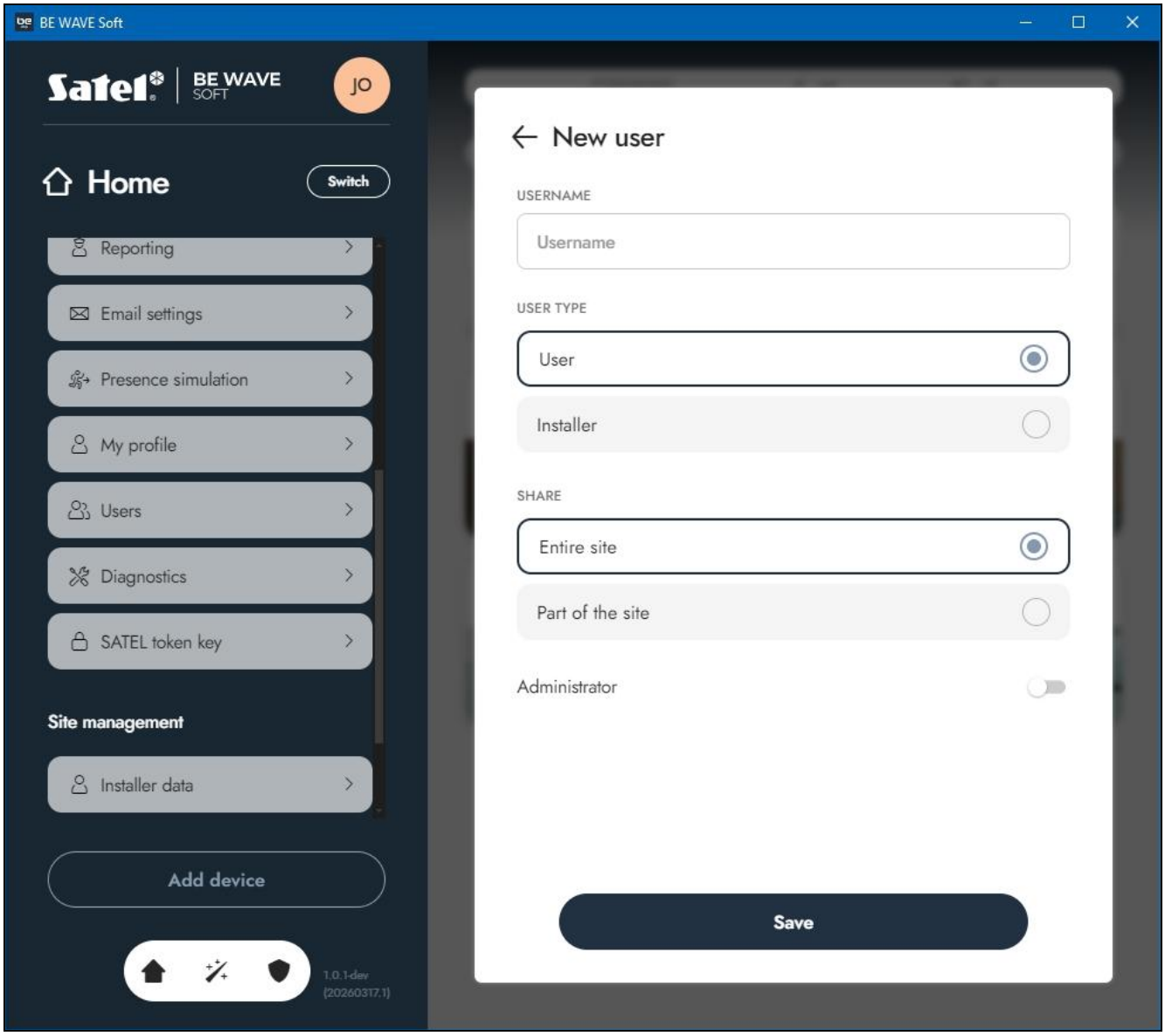
8. Tap *Back*. The *Users* screen will be displayed.

5.9.2 Adding a user in the BE WAVE Soft program

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



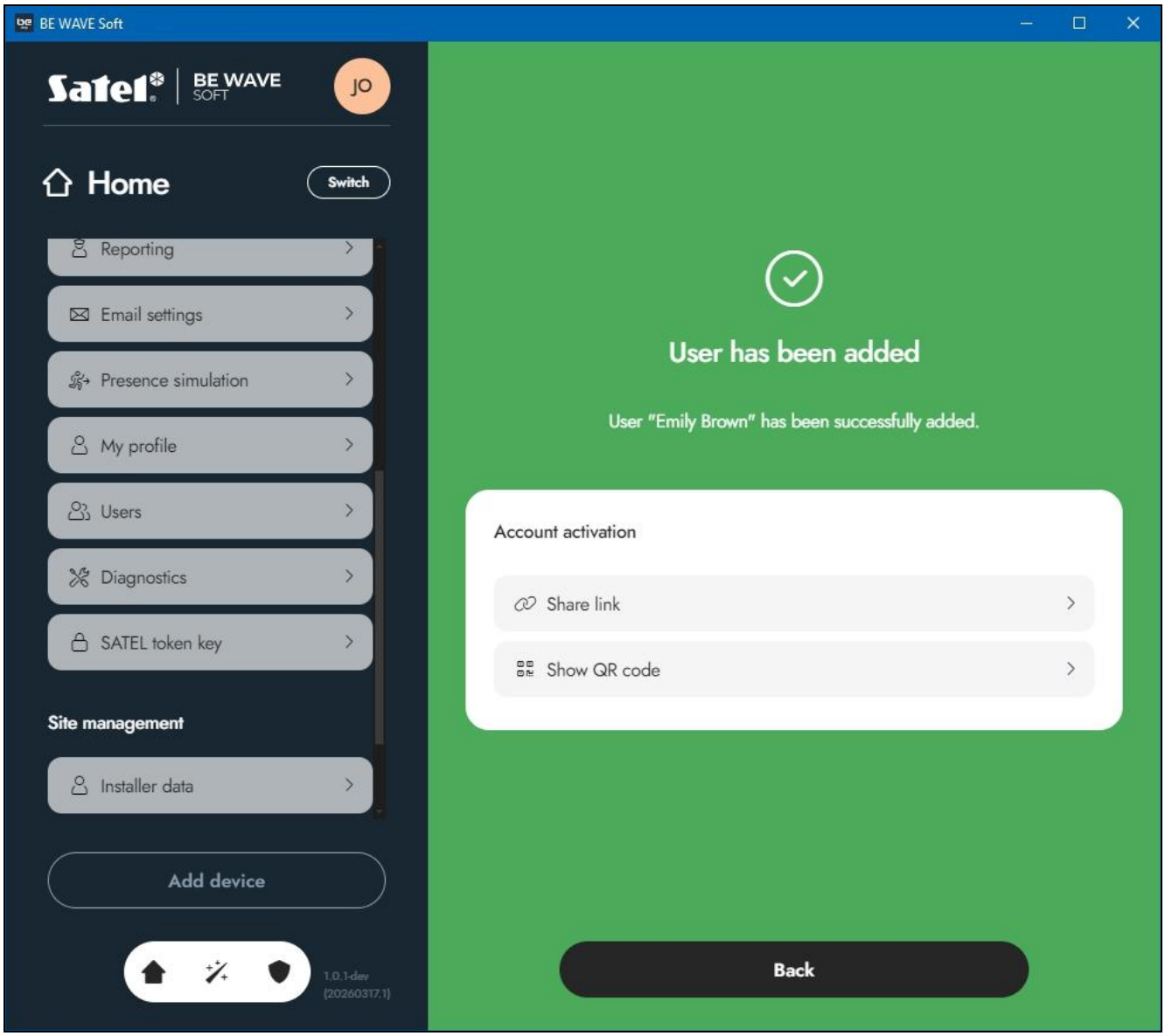
2. Click *Add user* button. The *New user* window will be displayed.



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. 65) or *Part of the site* (see “User with access to a part of the site” p. 66) 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.

5.9.3 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.

5.9.4 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.

5.10 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. 58).

5.10.1 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*.

5.10.2 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. When the diagnostic mode is enabled:

- system cannot be armed,
- tamper alarms are not signaled.

6.1 Enabling the diagnostic mode

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.

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. 66).
2. Open the control panel enclosure.
3. Press and hold the RESET button on the control panel main board for 5 seconds.

8. Specifications

Supply voltage ..... 18 VAC ±15%, 50-60 Hz

Recommended transformer	40 VA
Standby current consumption	120 mA
Maximum current consumption	170 mA
Standby current consumption from battery	100 mA
Maximum current consumption from battery	140 mA
Power supply output voltage	12 VDC ±15%
Power supply output voltage range	10.5 V…14 VDC
Power supply output current	3 A
Battery charging current	400 mA
Battery failure voltage threshold	11 V ±10%
Battery cut-off voltage	10.5 V ±10%
AUX output	1 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	138 x 69 mm
Weight	93 g