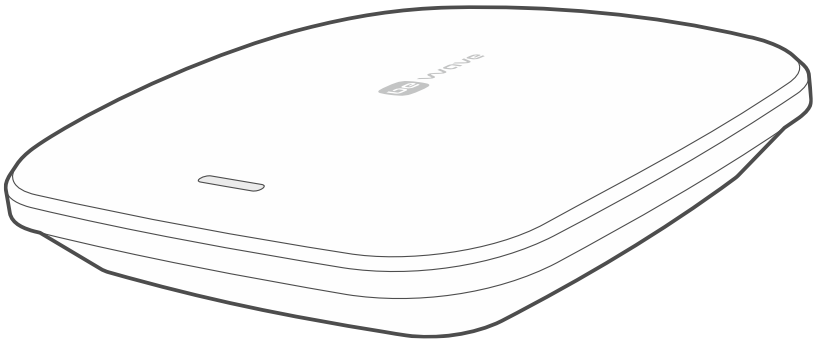
BE WAVE system controller

Smart HUB Plus
Smart HUB
Smart HUB Plus LV

EN

Firmware version 1.3



CE

smart_hub_en 12/25

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

IMPORTANT

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).

 Protection class II (protective insulation).

 The device is designed for indoor installation.

 Alternating current (AC).

 Direct current (DC).

 Prior to installation, please read carefully the manual.

Hereby, SATEL sp. z o.o. declares that the radio equipment type Smart HUB Plus / Smart HUB / Smart HUB Plus LV 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 3
2. Features 3
3. Supported devices 4
3.1 Wireless devices 4
3.1.1 Detectors 4
3.1.2 Actuators 5
3.1.3 Sirens 6
3.1.4 Keypad 6
3.1.5 Keyfobs and buttons 6
3.1.6 Ekspanders 6
3.1.7 Repeater 6
3.2 Virtual IP devices 6
4. Installation 7
4.1 Installing the Smart HUB Plus / Smart HUB controller 7
4.1.1 Description of the Smart HUB Plus / Smart HUB controller 8
4.1.2 Installation tips for the Smart HUB Plus / Smart HUB controller 9
4.1.3 Mounting the Smart HUB Plus / Smart HUB controller 10
4.2 Installing the Smart HUB Plus LV controller 15
4.2.1 Description of the Smart HUB Plus LV controller 15
4.2.2 Installation tips for the Smart HUB Plus LV controller 16
4.2.3 Mounting the Smart HUB Plus LV controller 17
4.3 Installing wireless devices 21
5. Managing, programming and controlling the BE WAVE system 21
5.1 Be Wave app 21
5.1.1 Description of the Be Wave app home screen 21
5.2 BE WAVE Soft program 22
5.2.1 Description of the BE WAVE Soft program home screen 22
5.3 Adding the controller (site) 23
5.3.1 Adding the controller in the Be Wave app 23
Adding the first controller (site) 23
Adding another controller (site) 27
5.3.2 Adding the controller in the BE WAVE Soft program 28
Adding the first controller (site) 28
Adding another controller (site) 34
5.4 Adding a wireless device to the system 35
5.4.1 Adding a wireless device in the Be Wave app 36
Adding the first wireless device 36
Adding another wireless device 38
5.4.2 Adding a wireless device in the BE WAVE Soft program 39
Adding the first wireless device 39
Adding another wireless device 42
5.5 Adding a virtual IP device 43
5.5.1 Adding a virtual IP device in the Be Wave app 43
5.5.2 Adding a virtual IP device in the BE WAVE Soft program 46
5.6 Deleting a device 49
5.6.1 Deleting a device in the Be Wave app 49
5.6.2 Deleting a device in the BE WAVE Soft 50
5.7 Description of settings 50

5.7.1 Device settings....50
5.7.2 Alarm source....52
5.7.3 IP device settings....52
5.7.4 Reporting....53
Station 1 / Station 2....53
5.8 Adding a user....56
5.8.1 Adding a user in the Be Wave app....56
5.8.2 Adding a user in the BE WAVE Soft program....59
5.8.3 User with access to the entire site....61
User privileges....61
5.8.4 User with access to a part of the site....62
6. Testing....62
6.1 Enabling the diagnostic mode....62
6.1.1 Enabling the diagnostic mode in the Be Wave app....62
6.1.2 Enabling the diagnostic mode in the BE WAVE Soft program....63
6.2 Disabling the diagnostic mode....63
6.2.1 Disabling the diagnostic mode in the Be Wave app....63
6.2.2 Disabling the diagnostic mode in the BE WAVE Soft program....63
7. Maintenance....63
7.1 Firmware update....63
7.1.1 Starting the update in the Be Wave app....63
7.1.2 Starting the update in the BE WAVE Soft program....63
7.2 Replacing the battery in the controller....63
7.3 Restoring the controller factory settings....64
7.3.1 Restoring the factory settings from the Be Wave app....64
7.3.2 Restoring the factory settings from the BE WAVE Soft program....65
7.3.3 Hardware factory restore....65
7.4 Turning off the Smart HUB Plus / Smart HUB controller....65
7.5 Turning off the Smart HUB Plus LV controller....65
8. Specifications....65
8.1 Smart HUB Plus / Smart HUB....65
8.2 Smart HUB Plus LV....66

1. Introduction

This manual will help you install the Smart HUB Plus / Smart HUB / Smart HUB Plus LV controller. The BE WAVE system combines building automation functions and security functions which protect against burglary, fire or other emergencies. You can manage and control it from the Be Wave mobile app or the BE WAVE Soft program.

The manual applies to the controller with electronics version:

Smart HUB / Smart HUB Plus: 1.5,

Smart HUB Plus LV: 1.2.

The performance of extra features such as SMS, CLIP or push 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.

2. Features

- Support for up to 128 wireless devices and virtual IP 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 images 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),
- Capability to assign devices to 50 rooms.
- Up to 50 users.
- Be Wave 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 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).
- Capability to arm the system fully or partially.
- Up to 100 scenes and routines:
  - scenes for easier control.
  - routines for automated system operation.
- 8000 event log entries.
- Event notification types:
  - push,
  - SMS [Smart HUB Plus / Smart HUB Plus LV],
  - CLIP [Smart HUB Plus / Smart HUB Plus LV].
- Reporting:
  - reporting events to two monitoring stations,
  - support for Contact ID, SIA and Bold Manitou communication formats,
  - data transmission via Ethernet or cellular network [Smart HUB Plus / Smart HUB Plus LV],
  - Dual Path Reporting compliant with EN 50136 [Smart HUB Plus / Smart HUB Plus LV].
- Capability to update firmware of the controller and the devices in the system.
- 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 [Smart HUB Plus / Smart HUB Plus LV]:
  - operating in the 2G and 4G networks,
  - dual SIM support.
- LED indicator.
- Powered by:
  - 230 VAC [Smart HUB Plus / Smart HUB],
  - 9...28 VDC [Smart HUB Plus LV].
- Backup battery.
- Battery charging circuit.
- Battery status control and low battery disconnect system.
- Tamper protection against enclosure opening and removal from mounting surface.

3. Supported devices

You can install up to 128 wireless devices and virtual IP devices in the system.

3.1 Wireless devices

3.1.1 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.

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

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 (e.g. a wired opening detector) to the 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) – detector that measures temperature, pressure and humidity.

3.1.2 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.

3.1.3 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.

3.1.4 Keypad

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

3.1.5 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.

3.1.6 Ekspanders

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.

3.1.7 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 controller.

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 (e.g. to an IP camera).

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

4. Installation

If the device is mounted higher than 2 m above the ground, it can become a danger when it falls off the wall.

There is a danger of battery explosion when using a different battery than recommended by the manufacturer, or handling the battery improperly.

Do not crush the battery, cut it or expose it to high temperatures (throw it into the fire, put it in the oven, etc.).

Do not expose the battery to very low pressure due to the risk of battery explosion or leakage of flammable liquid or gas.

4.1 Installing the Smart HUB Plus / Smart HUB controller

The controller can be connected to a power outlet whose voltage is the same as the voltage indicated on the controller's rating plate.

Do not connect the controller to a power outlet if the controller power cable or enclosure are damaged.

Do not touch the power cable plug with wet hands.

Do not pull the cable to disconnect it from the outlet. Pull the plug instead.

If smoke is coming out of the device, disconnect the power cable from the outlet.

Do not place heavy objects on the controller.

Do not install the controller at locations above 2000 m above sea level.

4.1.1 Description of the Smart HUB Plus / Smart HUB controller

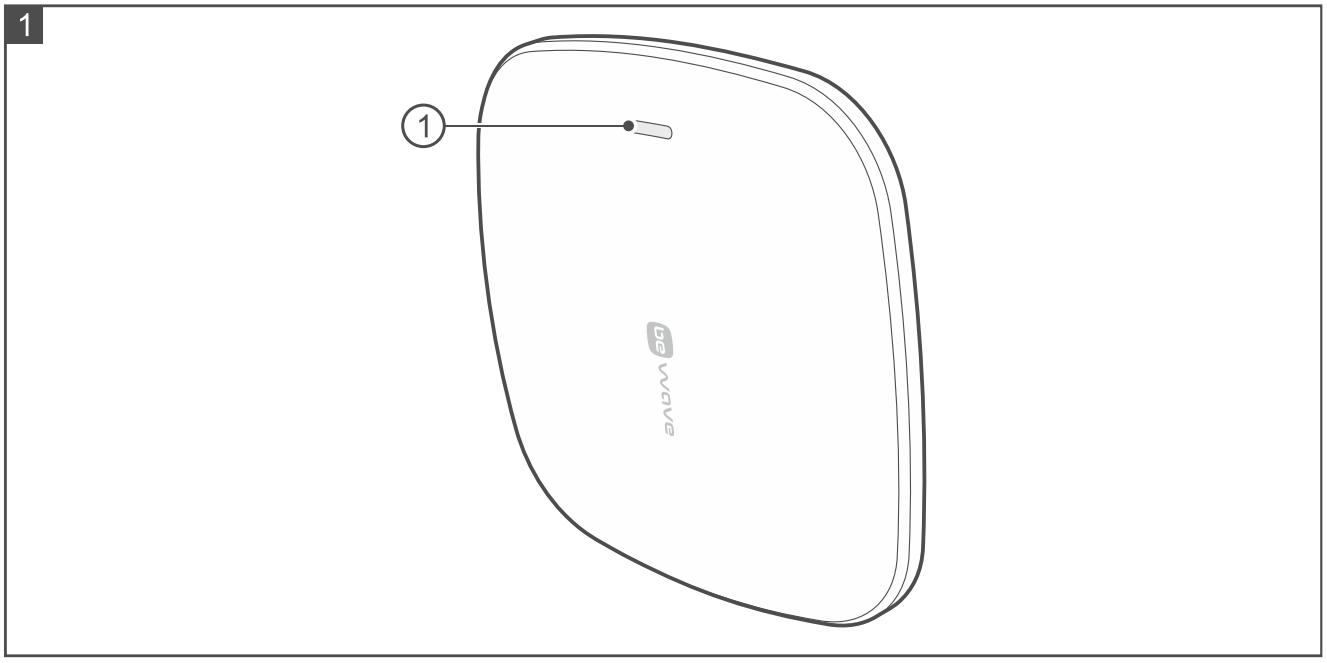


Figure 1 shows the controller's front side:

① LED indicator:

flashing in pink – controller startup in progress,

ON in pink – controller operates in the Wi-Fi access point mode (you can connect to the controller in the BEWAVE_AP network),

ON in blue – controller is connected to a local network but has no access to the Internet or no connection to the SATEL server,

ON in green – controller is connected to the Internet,

additionally flashing in yellow – trouble,

additionally flashing in red – alarm,

colors changing smoothly – controller's firmware update in progress,

ON in white – controller's factory reset in progress.

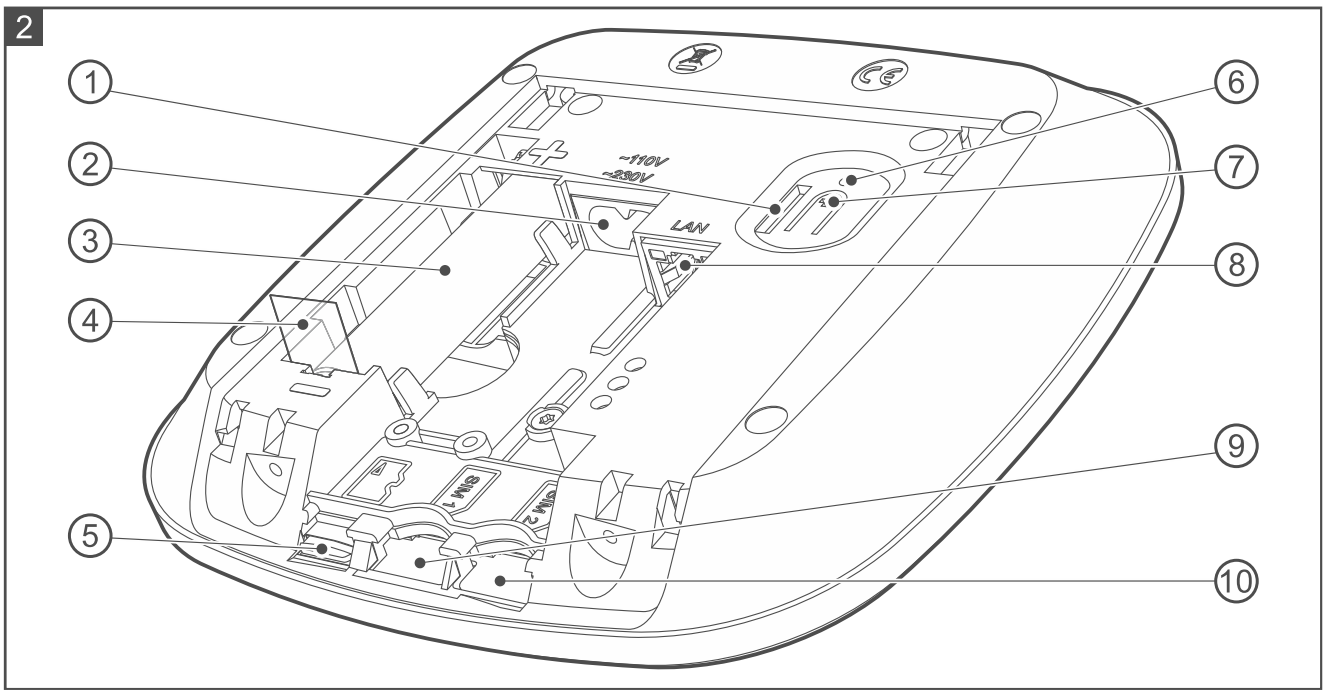


Figure 2 shows the inside of the Smart HUB Plus / Smart HUB controller after opening the enclosure.

① tamper protection.

② power cable port.

③ lithium-ion rechargeable battery (3.6 V / 3200 mAh).

④ battery insulator pull tag.

⑤ 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 controller),
- photos sent by the Motion Detector Cam,
- photos used in the Be Wave app (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).

⑥ factory reset pinhole – see “Hardware factory restore” p. 65.

⑦ button to enable / disable the Wi-Fi access point mode (press and hold for 5 seconds).

⑧ LAN cable port.

⑨ SIM1 slot for first SIM card [Smart HUB Plus].

⑩ SIM2 slot for second SIM card [Smart HUB Plus].

4.1.2 Installation tips for the Smart HUB Plus / Smart HUB controller

- The controller should be installed indoors, in spaces with normal air humidity.
- You can mount the controller on the wall or place it on a tabletop.
- The place of installation should be close to a 230 VAC power outlet. The outlet must be readily available.
- The electrical circuit to which the controller is to be connected must have suitable protection.

- The BE WAVE wireless devices you are planning to install must be within the range of the controller's radio communication. Keep this in mind when selecting a place of installation for the controller. Please note that thick walls, metal partitions, etc. will reduce the range of the radio signal.

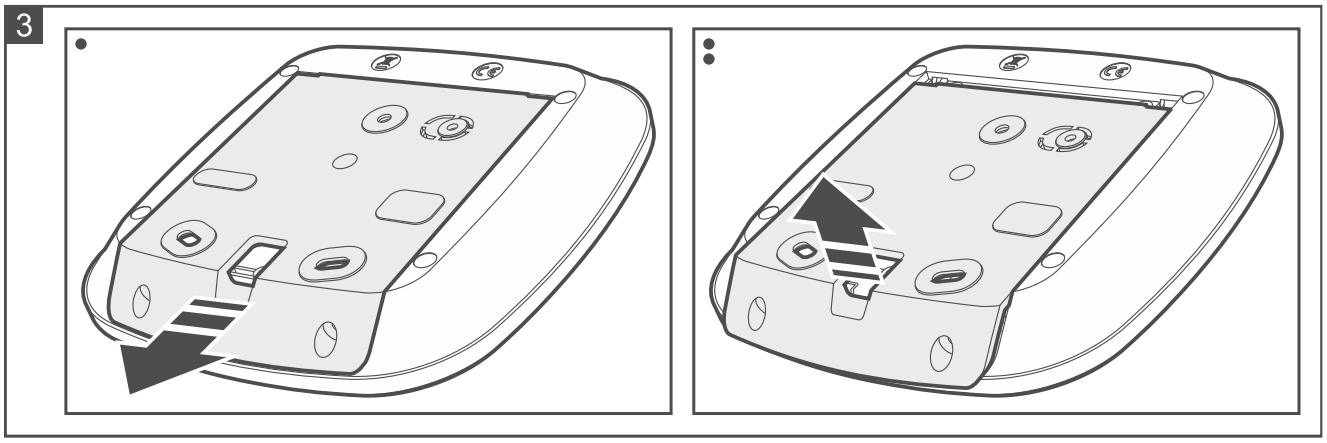
4.1.3 Mounting the Smart HUB Plus / Smart HUB controller

If the controller is to meet the requirements of Standard EN 50131 for Grade 2, mount the controller on the wall.

Do not mount the controller on the wall with cables pointing upwards.

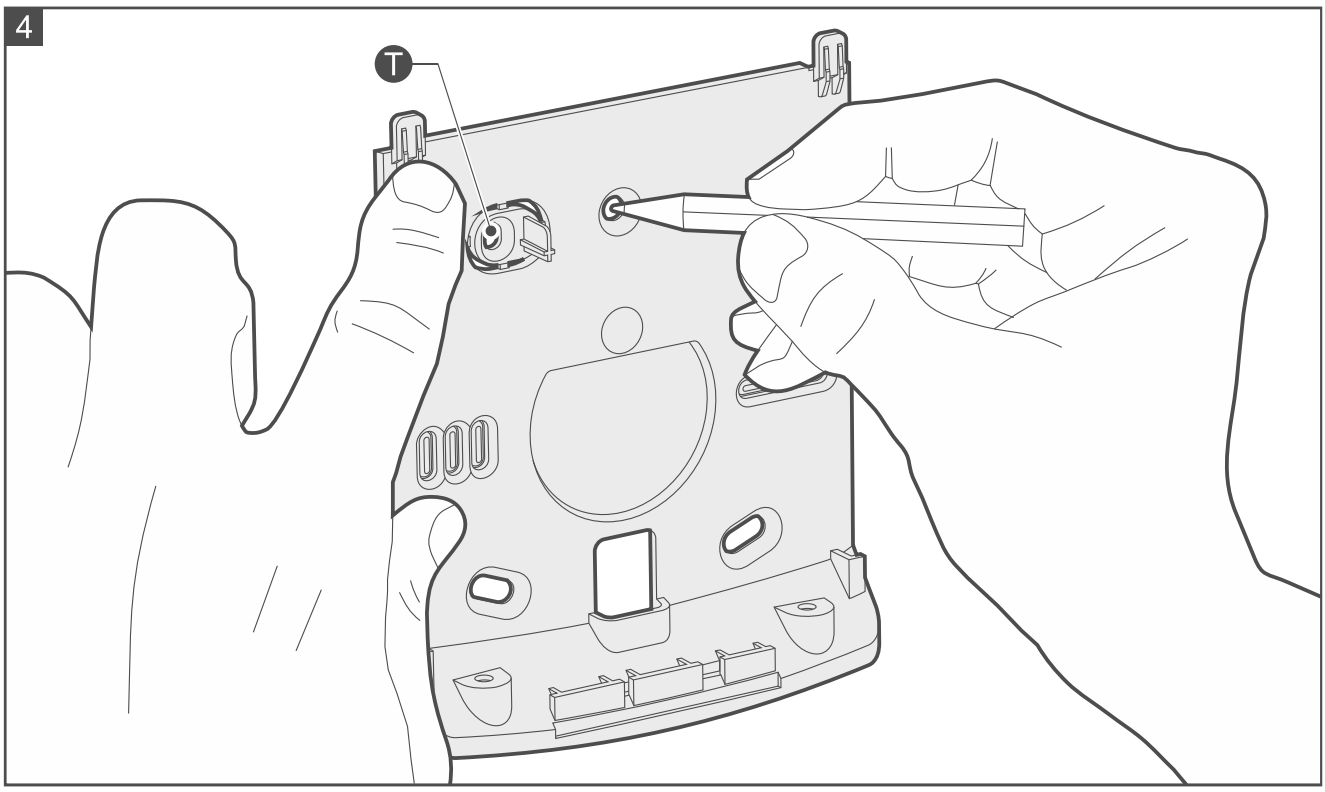
If the controller is to remain placed on the tabletop, skip steps 2, 3 and 5 and apply adhesive anti-slip pads on the bottom of the enclosure (Fig. 14). The pads are supplied with the controller.

1. Open the controller enclosure (Fig. 3).

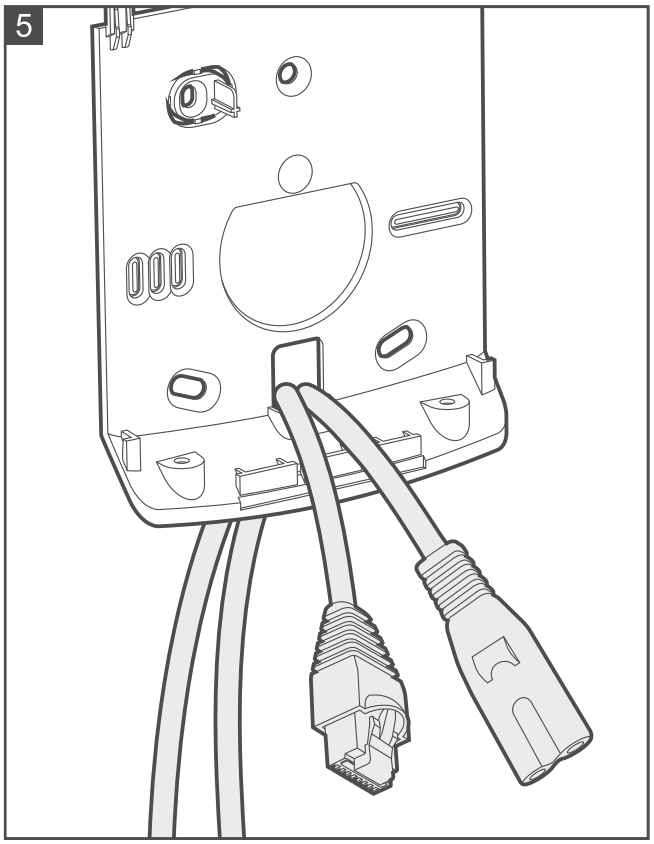


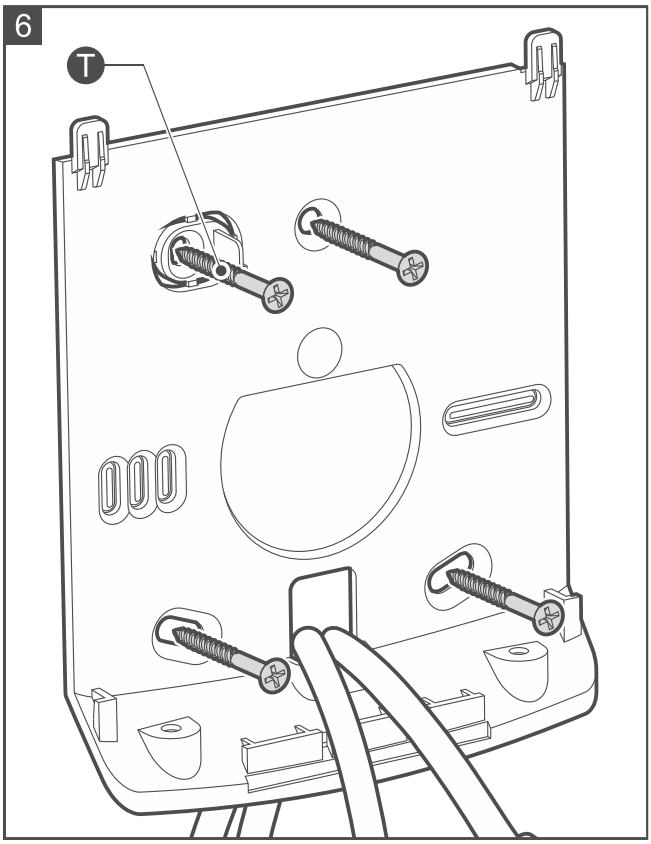
2. Place the enclosure base against the wall and mark the location of the mounting holes (Fig. 4). If the controller is to detect removal from the surface, mark the location of the hole in the tamper protection element (marked with the T symbol in the figure).

The controller must detect removal from the surface if it is to meet the requirements of Standard EN 50131 for Grade 2.



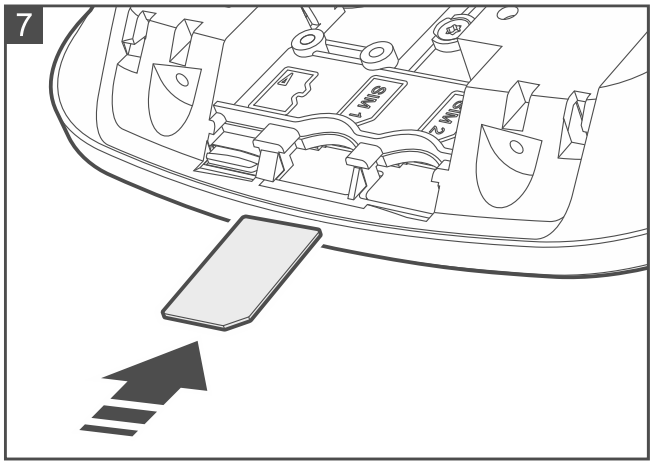
3. Drill the holes in the wall for wall plugs (anchors). Use wall plugs specifically intended for the mounting surface (different for concrete or brick wall, different for plaster wall, etc.).
4. Run the cable(s) through the opening in the enclosure base (Fig. 5).
5. the enclosure base to the wall with screws (Fig. 6).

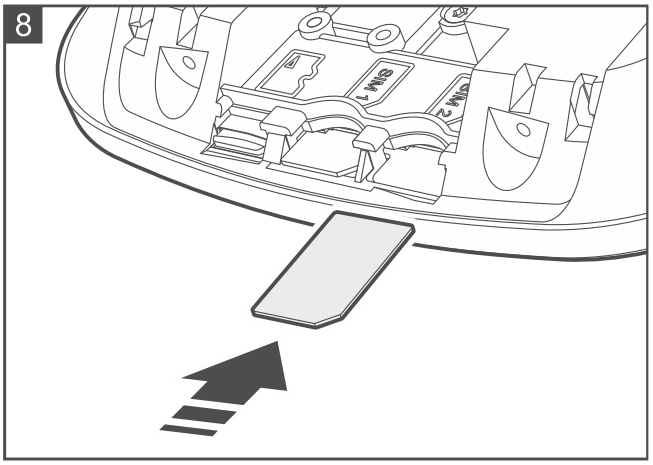




6. Insert a mini SIM card into the SIM1 slot (Fig. 7) [Smart HUB Plus].

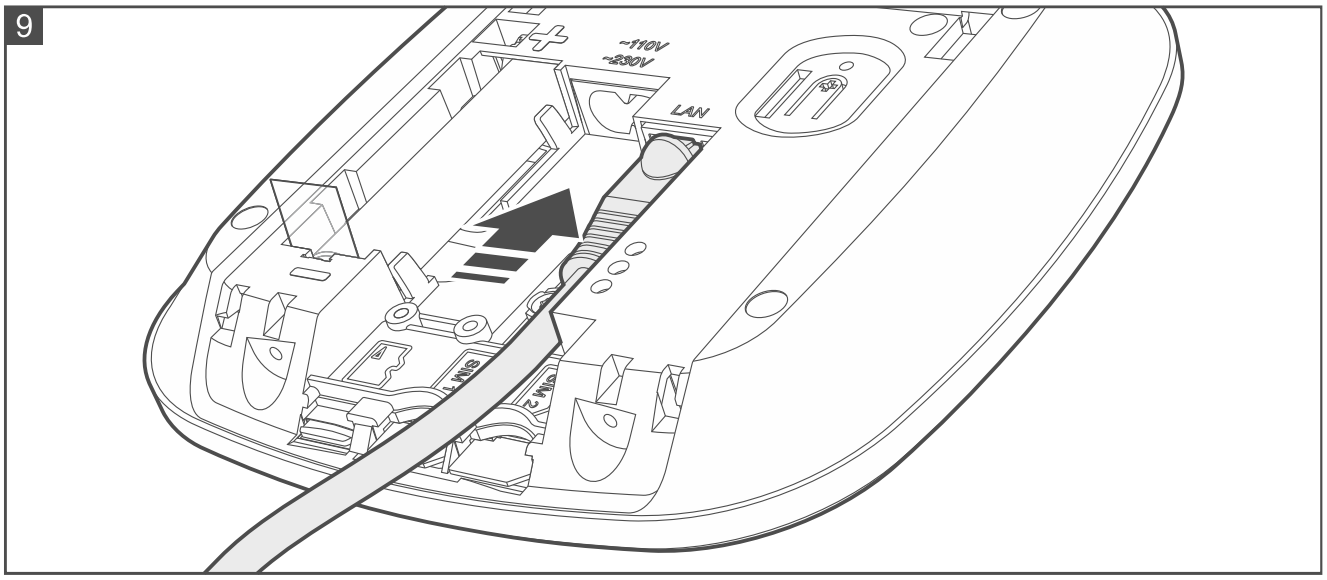
7. If you want to use two cards, insert the second mini SIM card into the SIM2 slot (Fig. 8) [Smart HUB Plus].





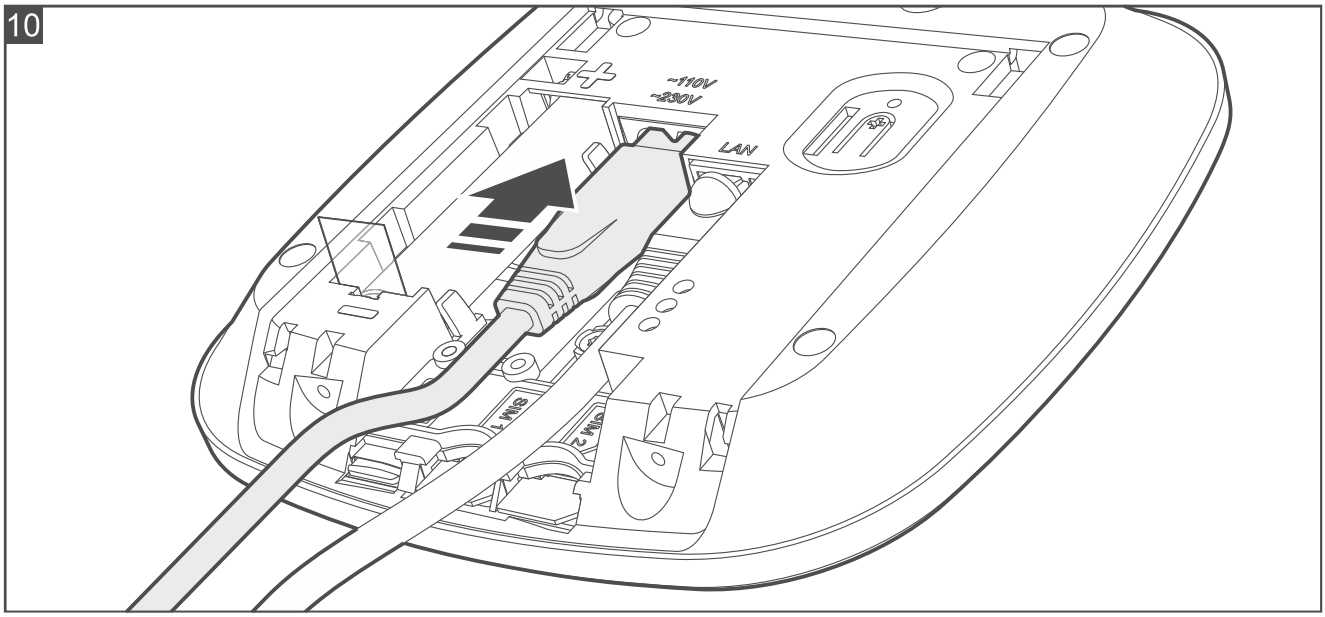
8. If the controller is to be connected to the wired LAN network, connect the cable to the LAN port (Fig. 9). Use a cable compliant with the 100Base-TX standard with the RJ-45 plug (the same as for connecting the computer to the network).

The controller 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.

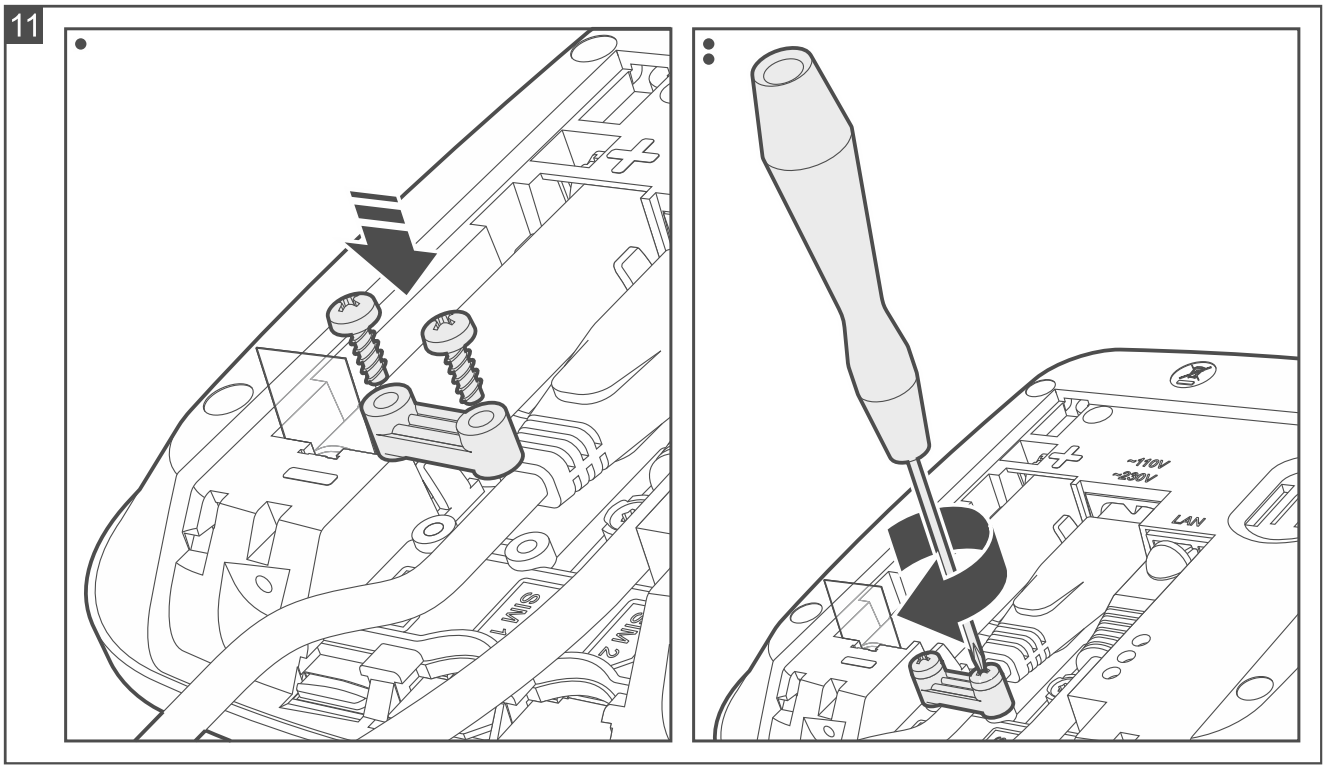


9. Connect the power cable to the power cable port in the controller (Fig. 10) and secure the cable fastener with screws (Fig. 11).

10

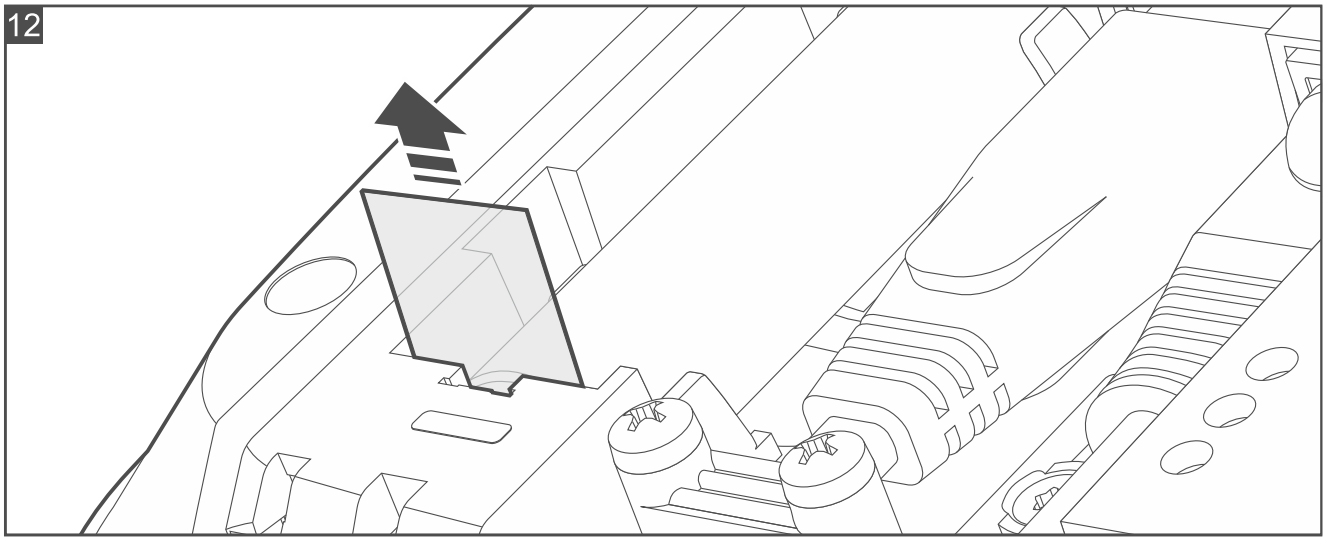


11



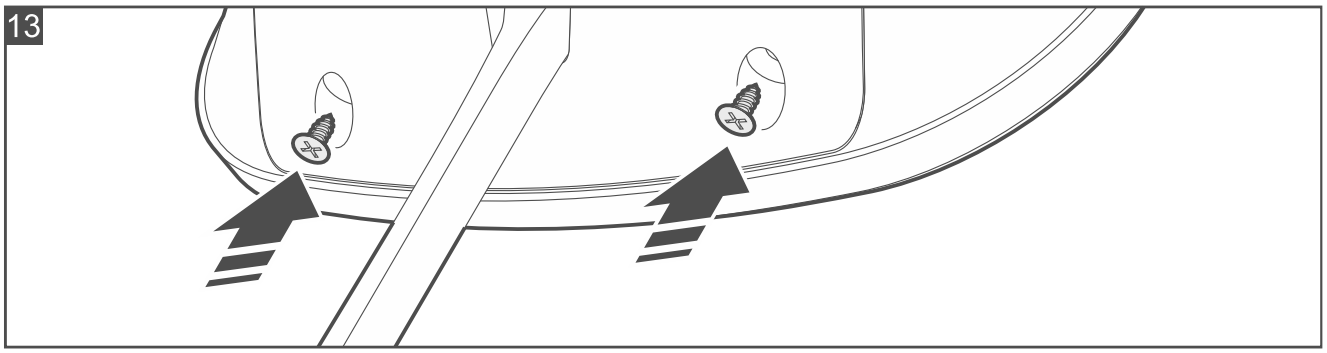
10. Remove the battery insulator tag (Fig. 12). The controller will power on (the controller LED indicator will start flashing).

12



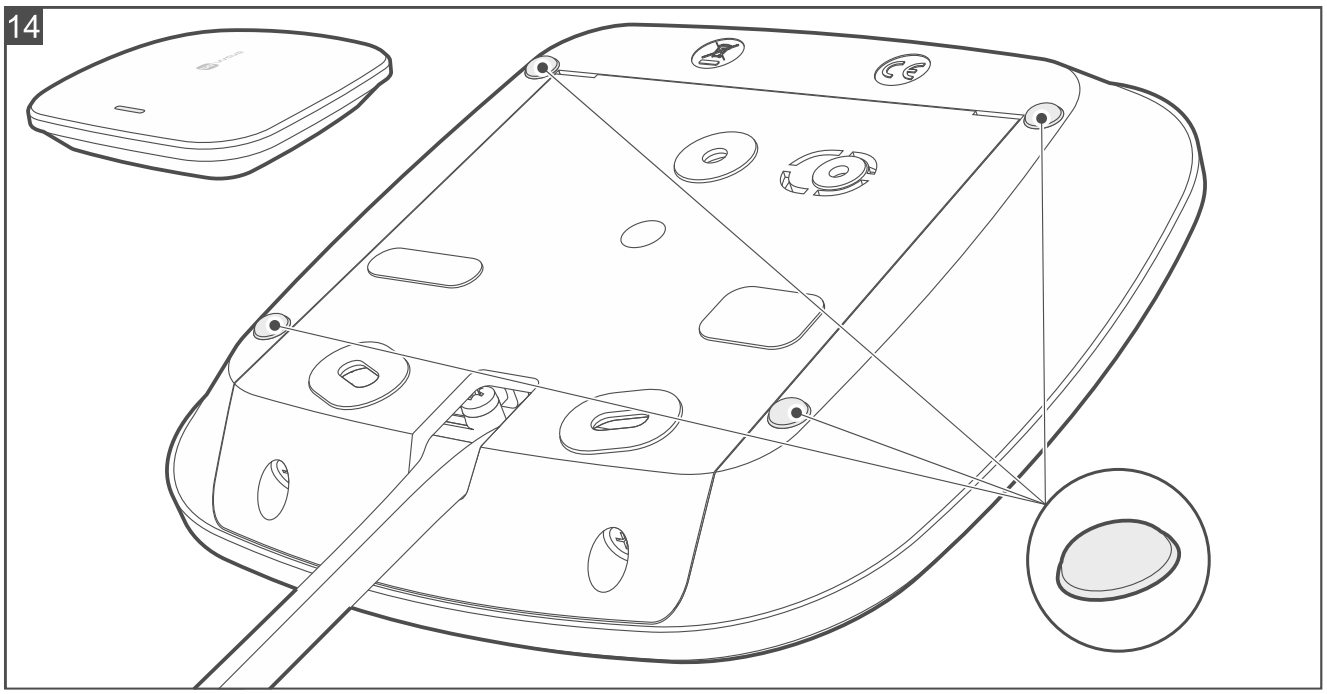
11. Close the enclosure and secure it with screws (Fig. 13).

13



12. Plug the power cable to the power outlet.
13. Start the Be Wave app to configure the controller settings and add BE WAVE devices.

14



4.2 Installing the Smart HUB Plus LV controller

Disconnect power before making any electrical connections.

Do not place heavy objects on the controller.

4.2.1 Description of the Smart HUB Plus LV controller

15

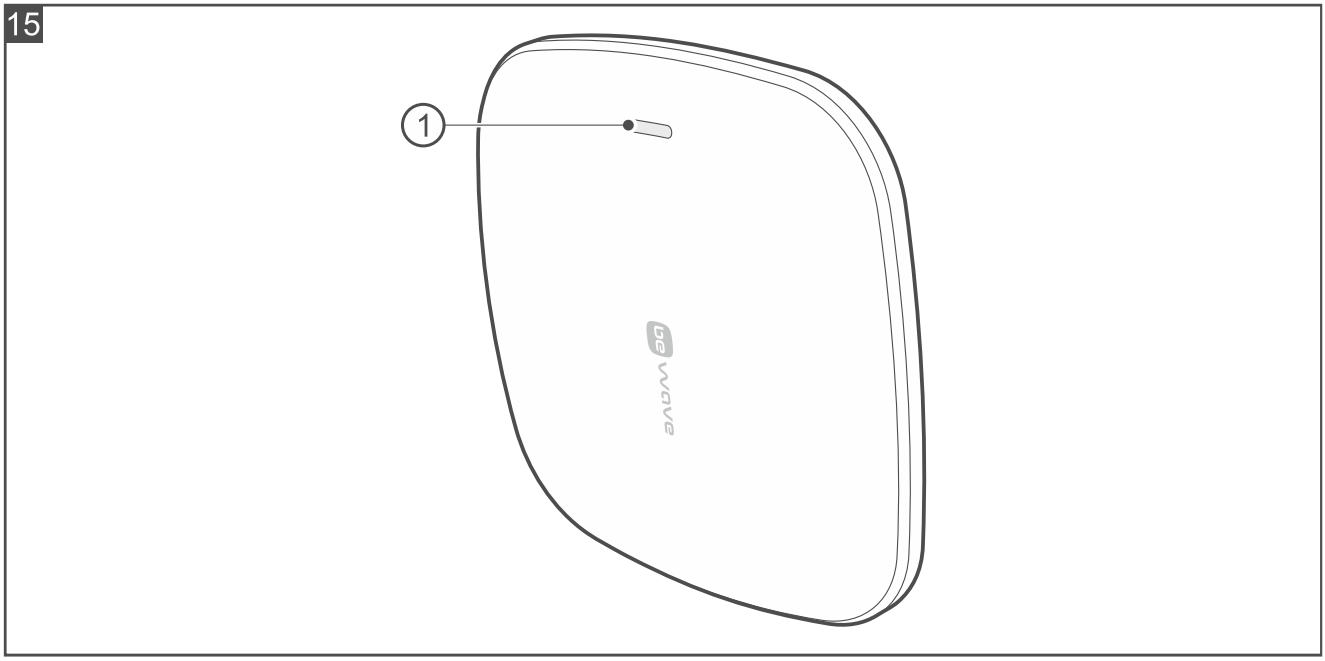


Figure 15 shows the controller's front side:

(1) LED indicator:

flashing in pink – controller startup in progress,

ON in pink – controller operates in the Wi-Fi access point mode (you can connect to the controller in the BEWAVE_AP network),

ON in blue – controller is connected to a local network but has no access to the Internet or no connection to the SATEL server,

ON in green – controller is connected to the Internet,

additionally flashing in yellow – trouble,

additionally flashing in red – alarm,

colors changing smoothly – controller's firmware update in progress,

ON in white – controller's factory reset in progress.

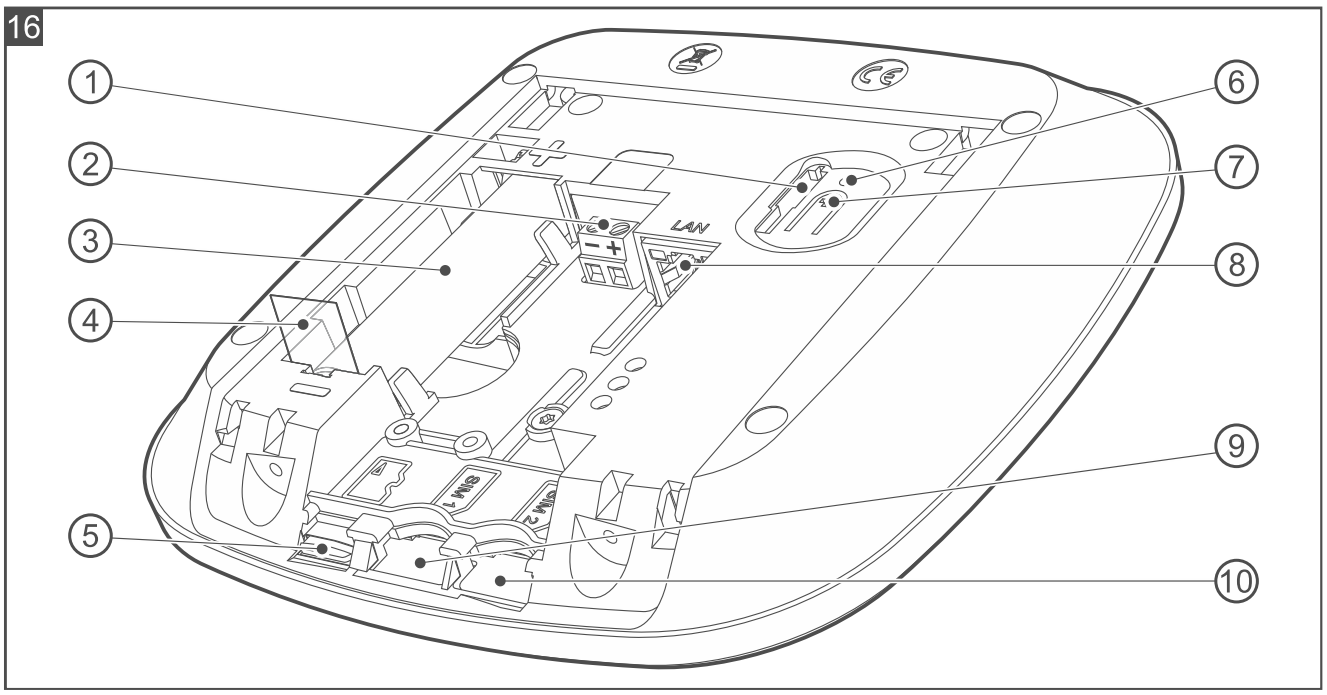


Figure 16 shows the inside of the Smart HUB Plus LV controller after opening the enclosure.

① tamper protection.

② 9...28 VDC terminals.

③ lithium-ion rechargeable battery (3.6 V / 3200 mAh).

④ battery insulator pull tag.

⑤ 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 controller),
- photos sent by the Motion Detector Cam,
- photos used in the Be Wave app (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).

⑥ factory reset pinhole – see “Hardware factory restore” p. 65.

⑦ button to enable / disable the Wi-Fi access point mode (press and hold for 5 seconds).

⑧ LAN cable port.

⑨ SIM1 slot for first SIM card.

⑩ SIM2 slot for second SIM card.

4.2.2 Installation tips for the Smart HUB Plus LV controller

- The controller should be installed indoors, in spaces with normal air humidity.
- You can mount the controller on the wall or place it on a tabletop.
- The BE WAVE wireless devices you are planning to install must be within the range of the controller’s radio communication. Keep this in mind when selecting a place of installation for the controller. Please note that thick walls, metal partitions, etc. will reduce the range of the radio signal.

4.2.3 Mounting the Smart HUB Plus LV controller

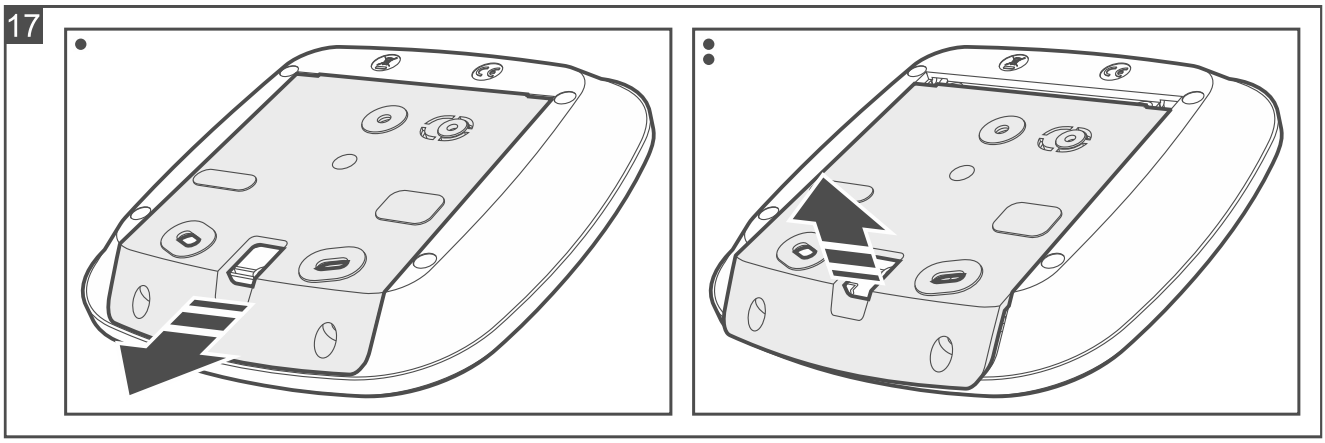
If the controller is to meet the requirements of Standard EN 50131 for Grade 2, mount the controller on the wall.

Do not mount the controller on the wall with cables pointing upwards.

If the controller is to remain placed on the tabletop, skip steps 2, 3 and 5 and apply adhesive anti-slip pads on the bottom of the enclosure (Fig. 14). The pads are supplied with the controller.

1. Open the controller enclosure (Fig. 17).

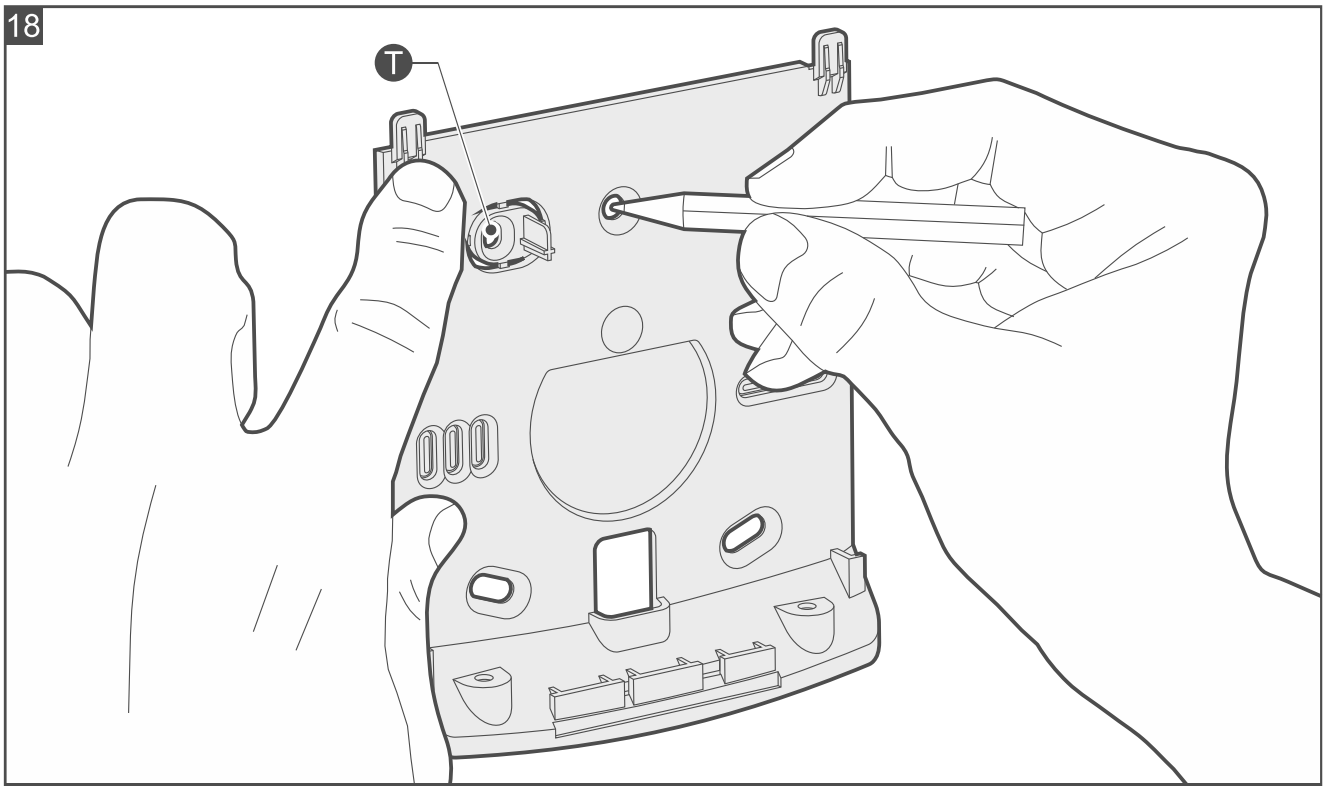
17



2. Place the enclosure base against the wall and mark the location of mounting holes (Fig. 18). If the controller is to detect removal from the surface, mark the location of the hole in the tamper protection element (marked with the T symbol in the figure).

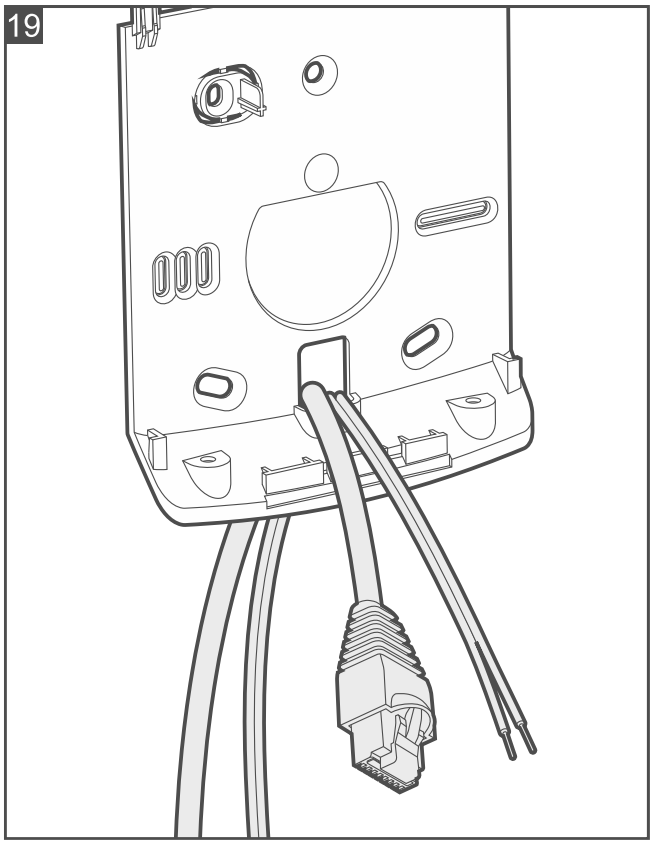
The controller must detect removal from the surface if it is to meet the requirements of Standard EN 50131 for Grade 2.

18

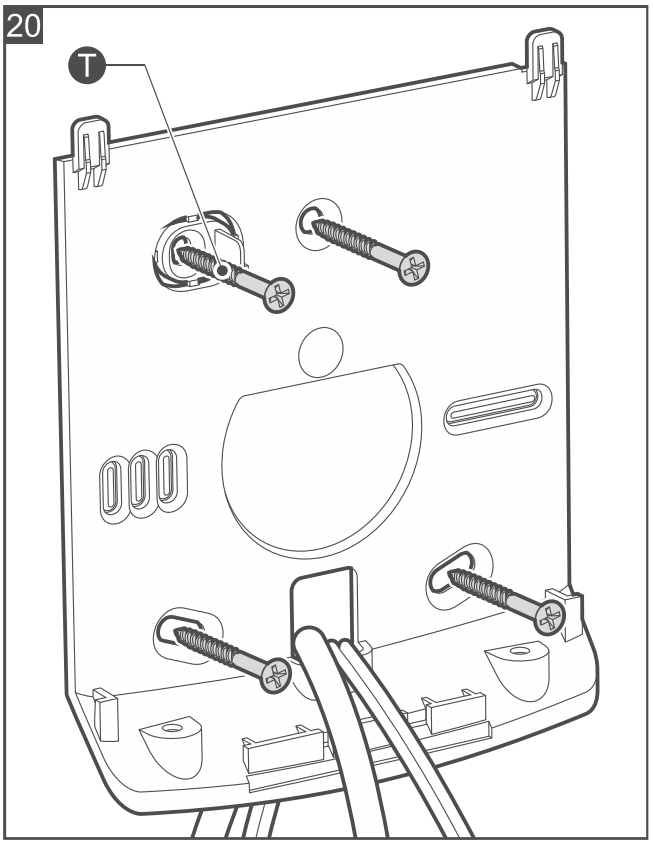


3. Drill the holes in the wall for wall plugs (anchors). Use wall plugs specifically intended for the mounting surface (different for concrete or brick wall, different for plaster wall, etc.).
4. Run the cable(s) through the opening in the enclosure base (Fig. 19).
5. Secure the enclosure base to the wall with screws (Fig. 20).

19

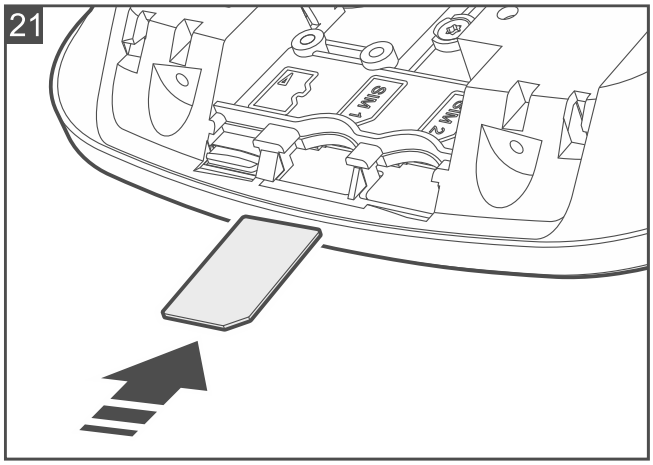


20

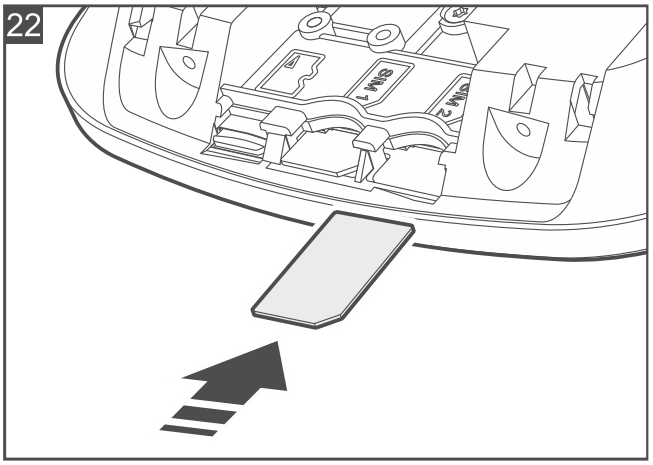


6. Insert a mini SIM card into the SIM1 slot (Fig. 21).
7. If you want to use two cards, insert the second mini SIM card into the SIM2 slot (Fig. 22).

21



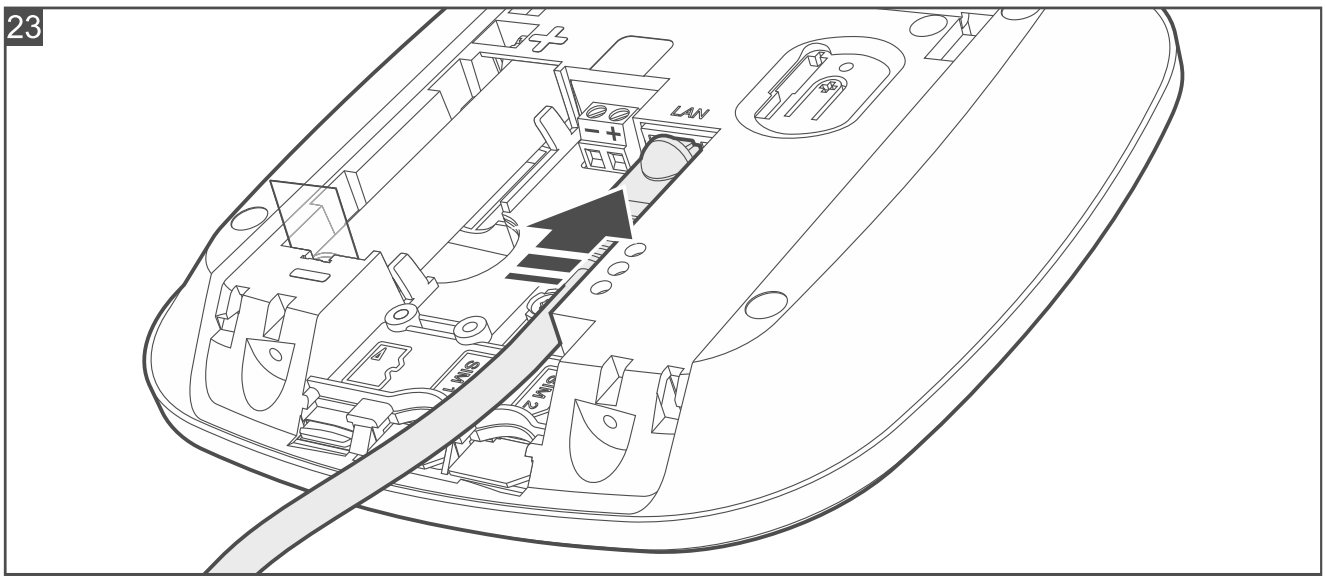
22



8. If the controller is to be connected to the wired LAN network, connect the cable to the LAN port (Fig. 23). Use a cable compliant with the 100Base-TX standard with the RJ-45 plug (the same as for connecting the computer to the network).

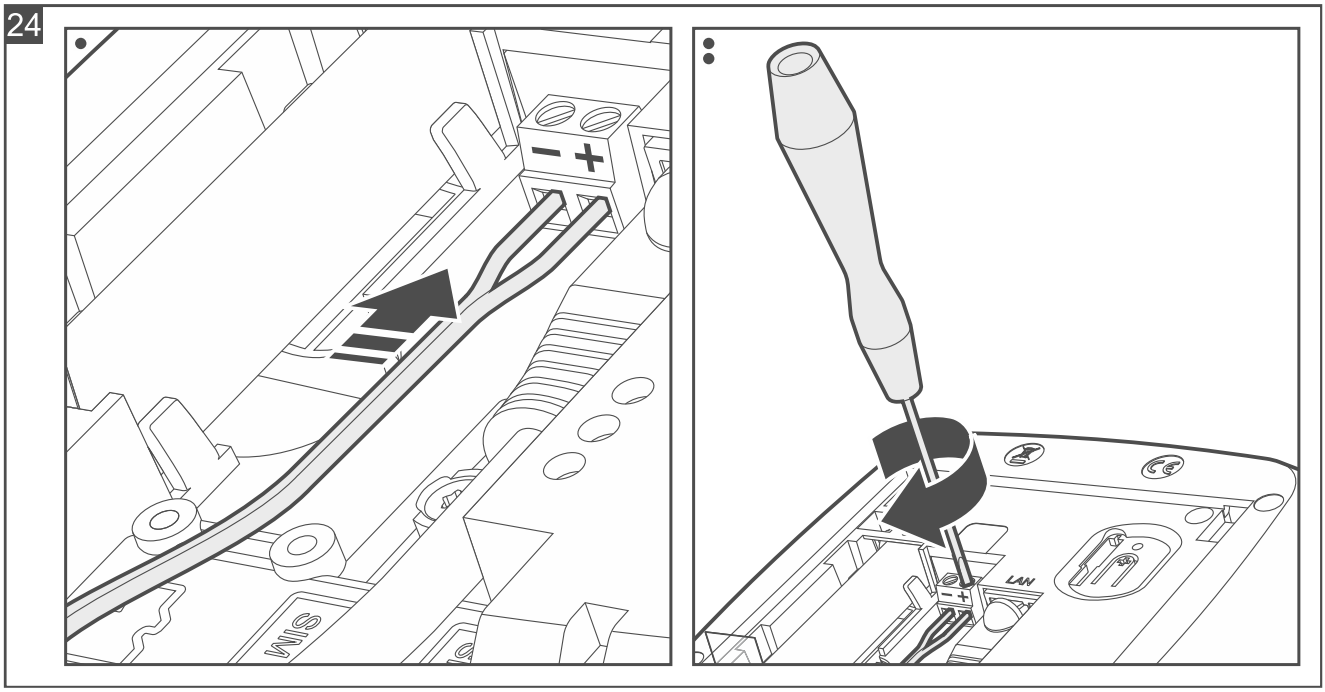
The controller can only operate in the local area networks (LAN). It must not be connected directly to the public computer network (MAN, WAN). To establish connection with a public network, use a router or xDSL modem.

23

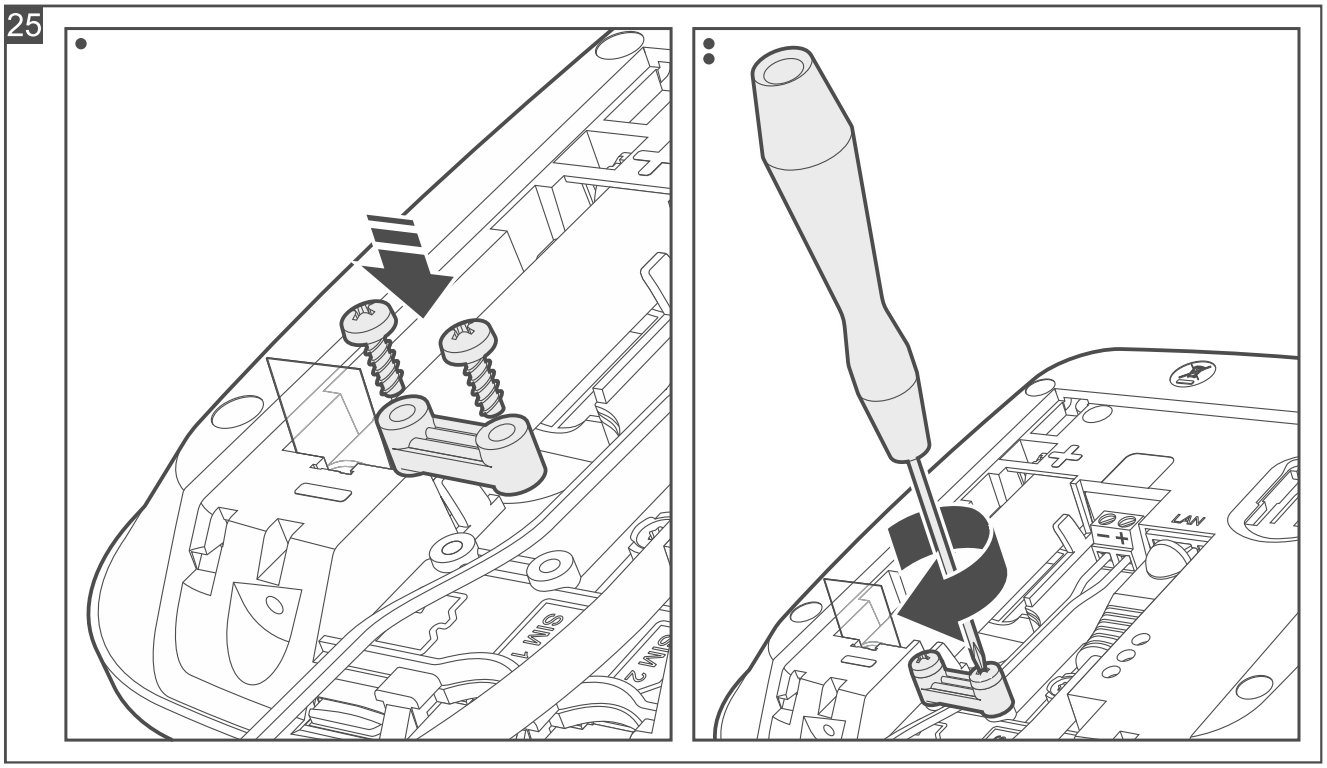


9. Screw the power wires to the terminals (Fig. 24) and secure the power wires fastener with screws (Fig. 25).

24

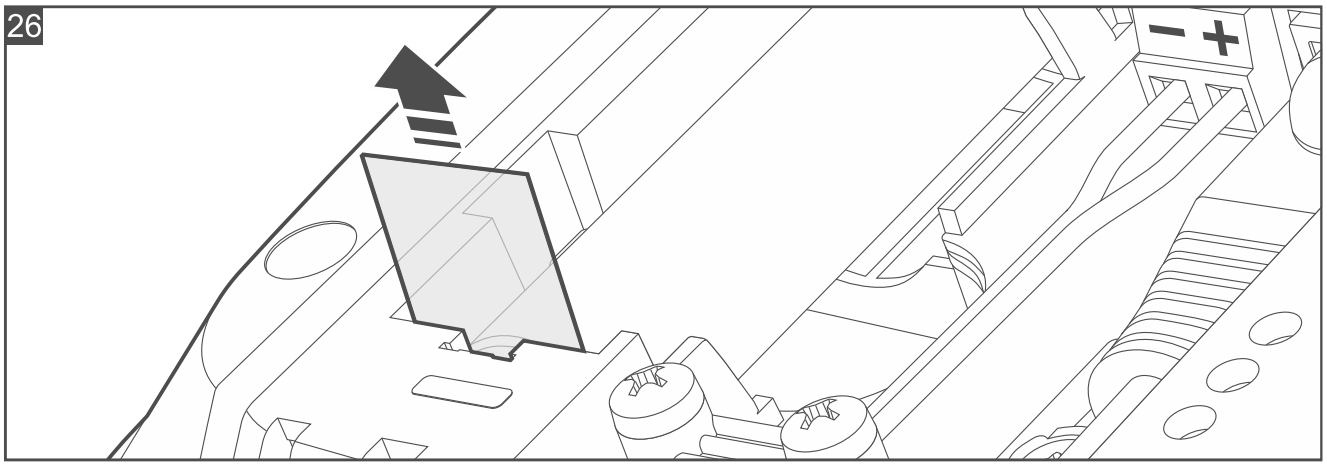


25



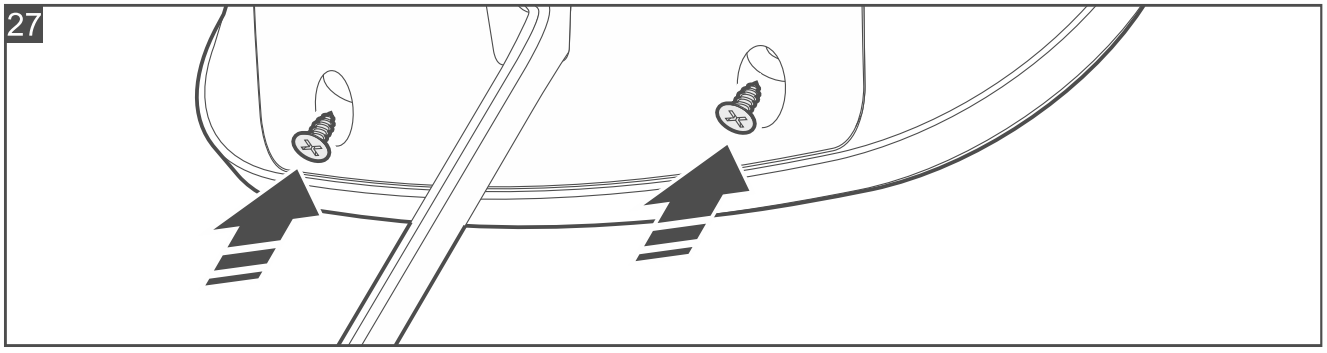
10. Remove the battery insulator tag (Fig. 26). The controller will turn on (the controller LED indicator will start flashing).

26



11. Close the enclosure and secure it with screws (Fig. 27).

27



12. Power on the controller.
13. Start the Be Wave app to configure the controller settings and add BE WAVE devices.

4.3 Installing wireless devices

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

5. Managing, programming and controlling the BE WAVE system

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

- Be Wave app,
- BE WAVE Soft program.

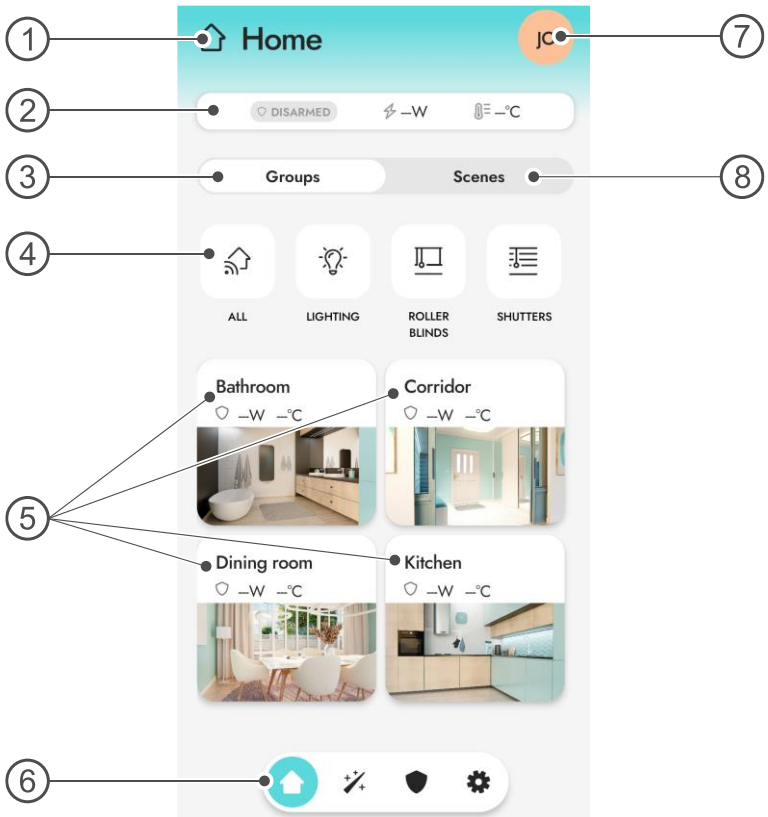
5.1 Be Wave app

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 system version: 11 (or newer). Required iOS system version: 11 (or newer).

Required Be Wave app version: 1.2.

5.1.1 Description of the Be Wave app home screen

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



Explanation:

① icon and name of the site (controller). 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.

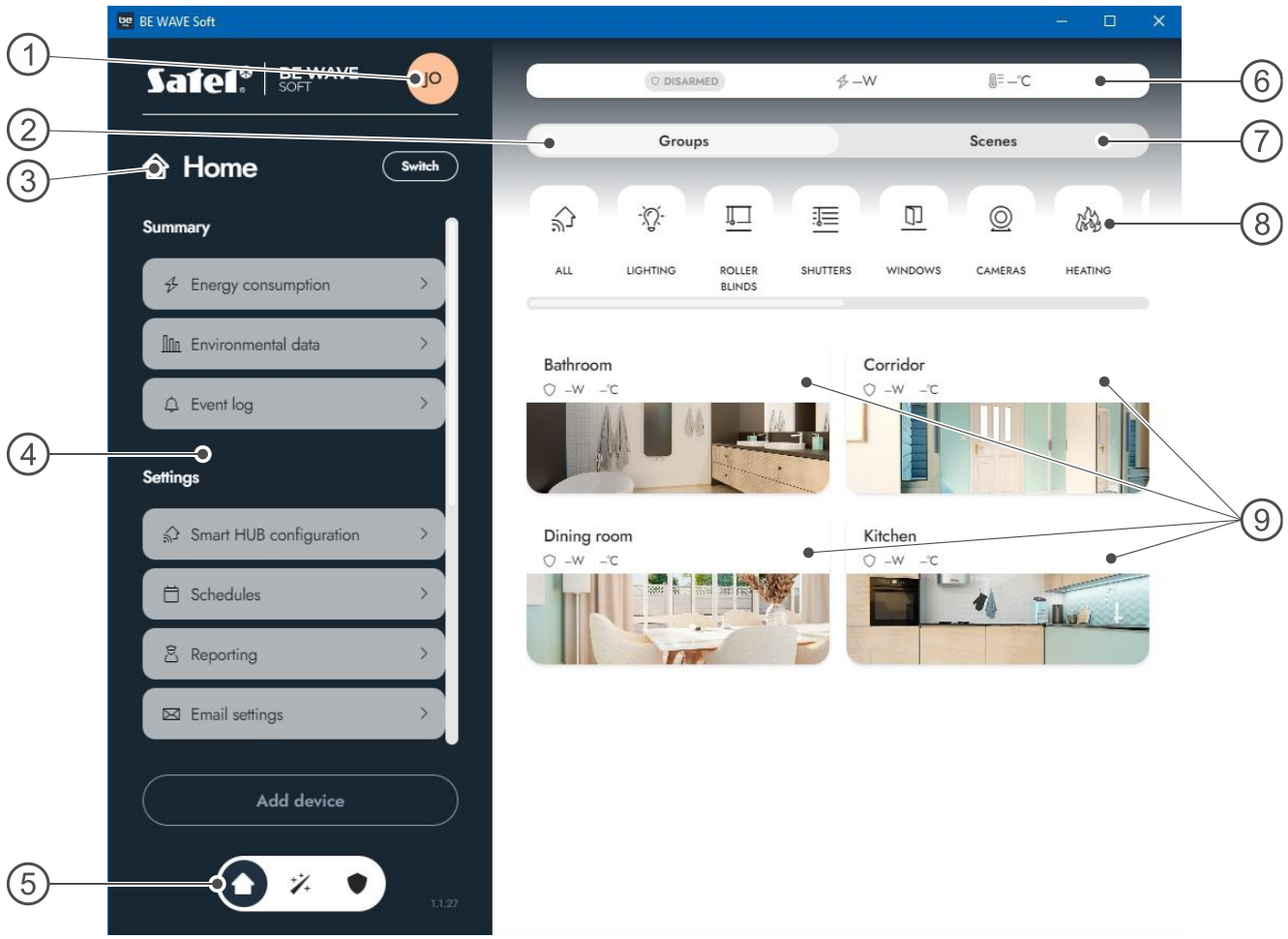
5.2 BE WAVE Soft program

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 controller (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 (controller). 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.

5.3 Adding the controller (site)

After start-up, the controller with factory settings operates in the Wi-Fi access point mode (the controller's LED indicator is ON in pink). It allows the app to connect to the controller.

5.3.1 Adding the controller in the Be Wave app

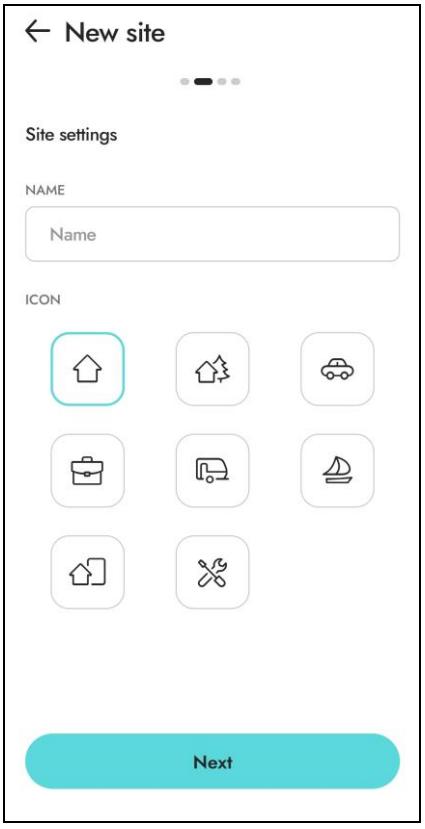
Adding the first controller (site)

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 controller. Make sure it is the MAC address of your controller.

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

2. Tap the controller (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.



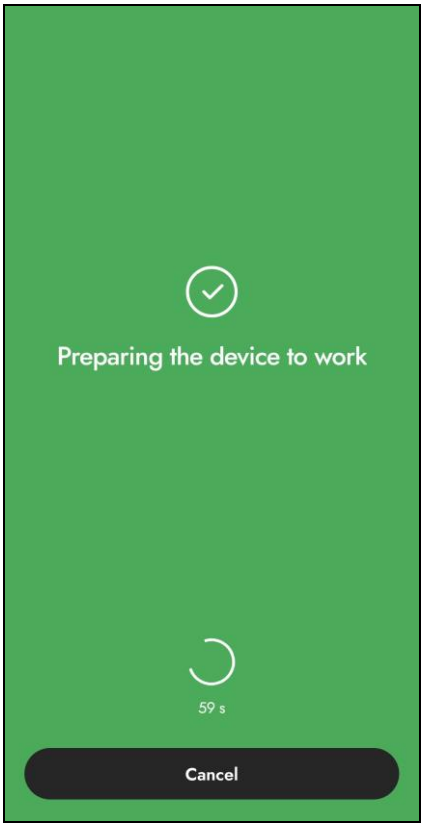
4. Enter the name of the site and select one of the icons to represent the site, then tap *Next*. The *New site – Installer account* screen will be displayed.

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

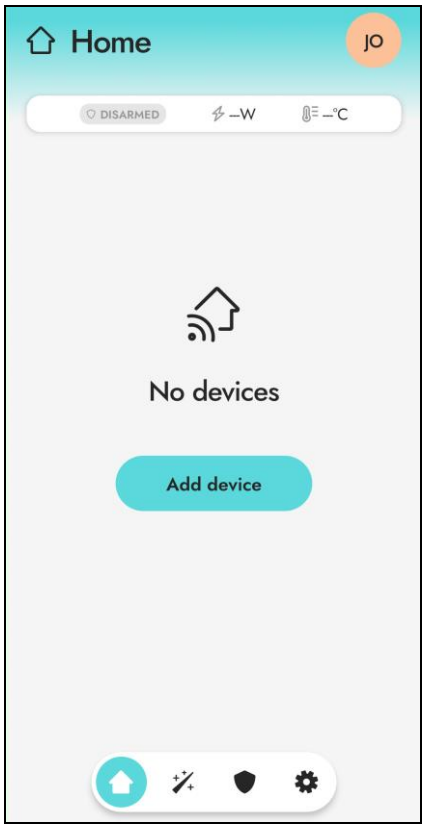
6. Select the communication method to be used with the controller. A new screen will be displayed. Configure the settings for the selected communication method, then save the

settings. You will return to the *New site – Communication methods* screen. Tap *Save*. A screen will be displayed saying that the controller is being prepared to work.

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

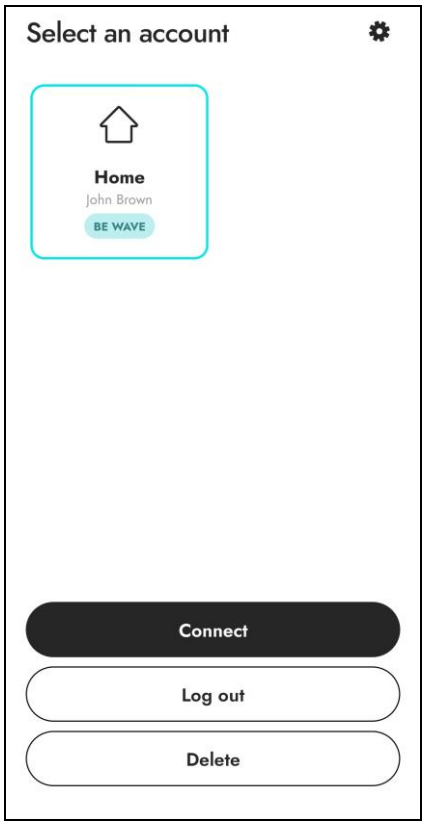


7. When the app connects to the controller by means of the selected communication method, the app's home screen will be displayed. You can add the first device to the system.

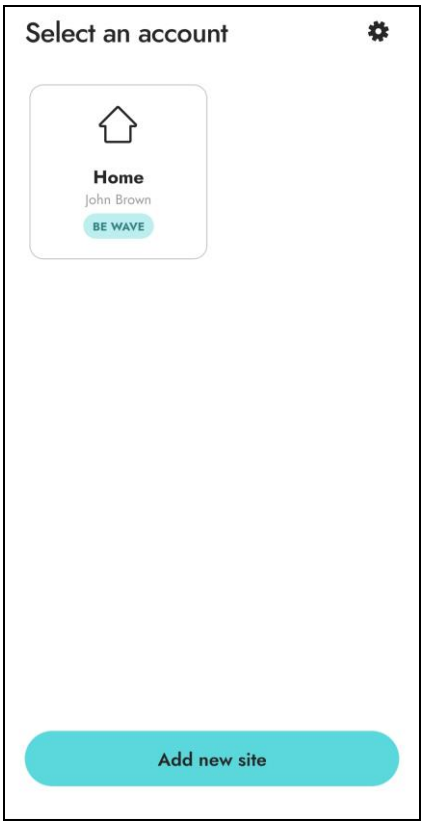


Adding another controller (site)

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 controller. Make sure it is the MAC address of the new controller.
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 controller.

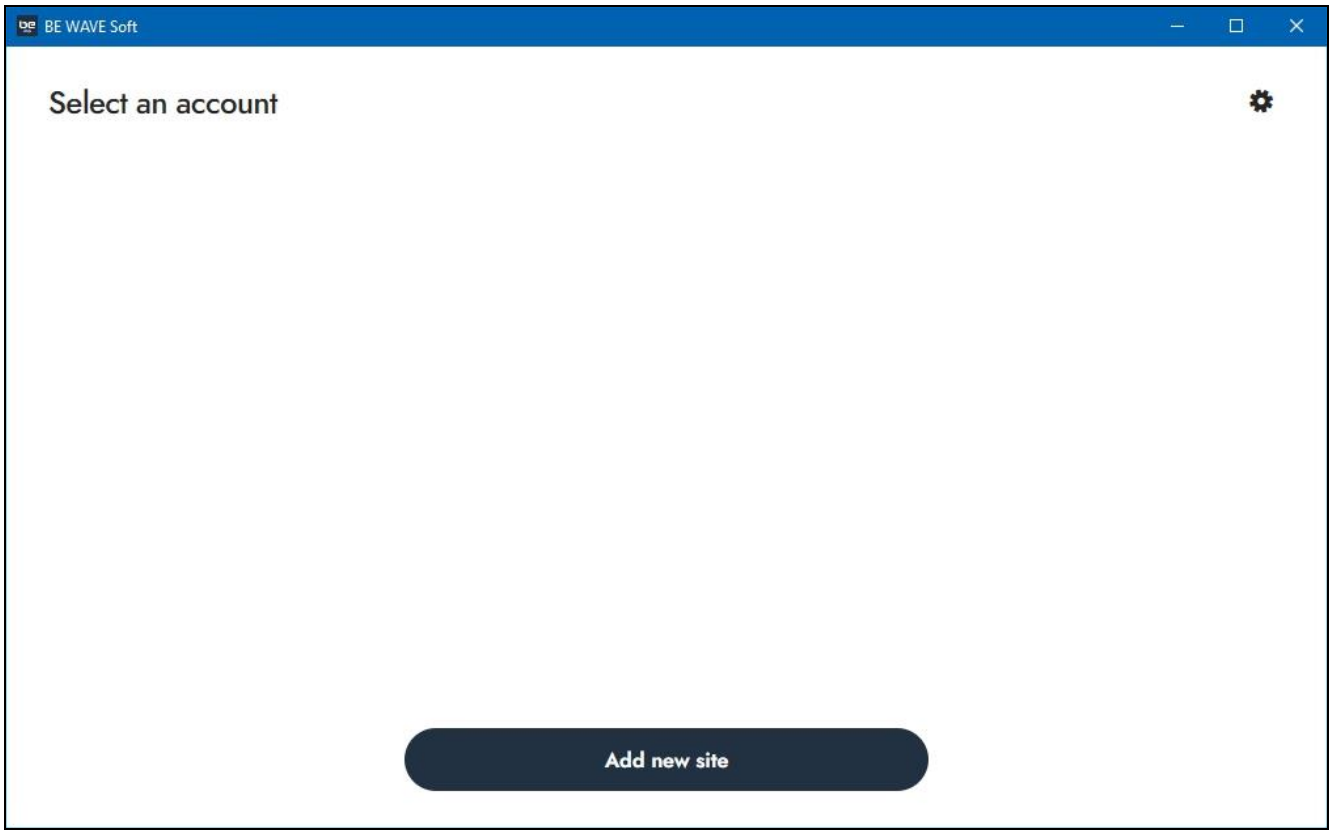
5.3.2 Adding the controller in the BE WAVE Soft program

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

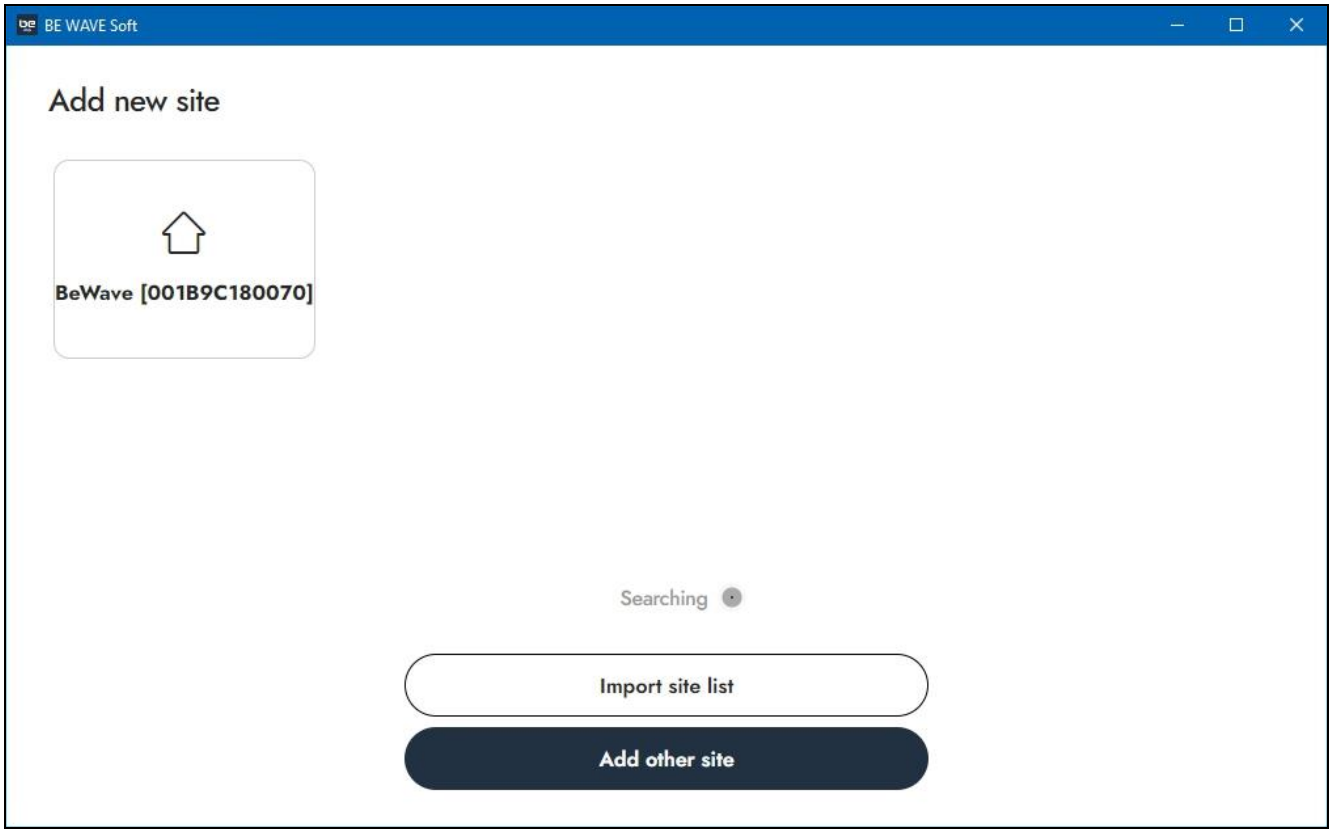
Adding the first controller (site)

If the controller 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 controller. Make sure it is the MAC address of your controller.

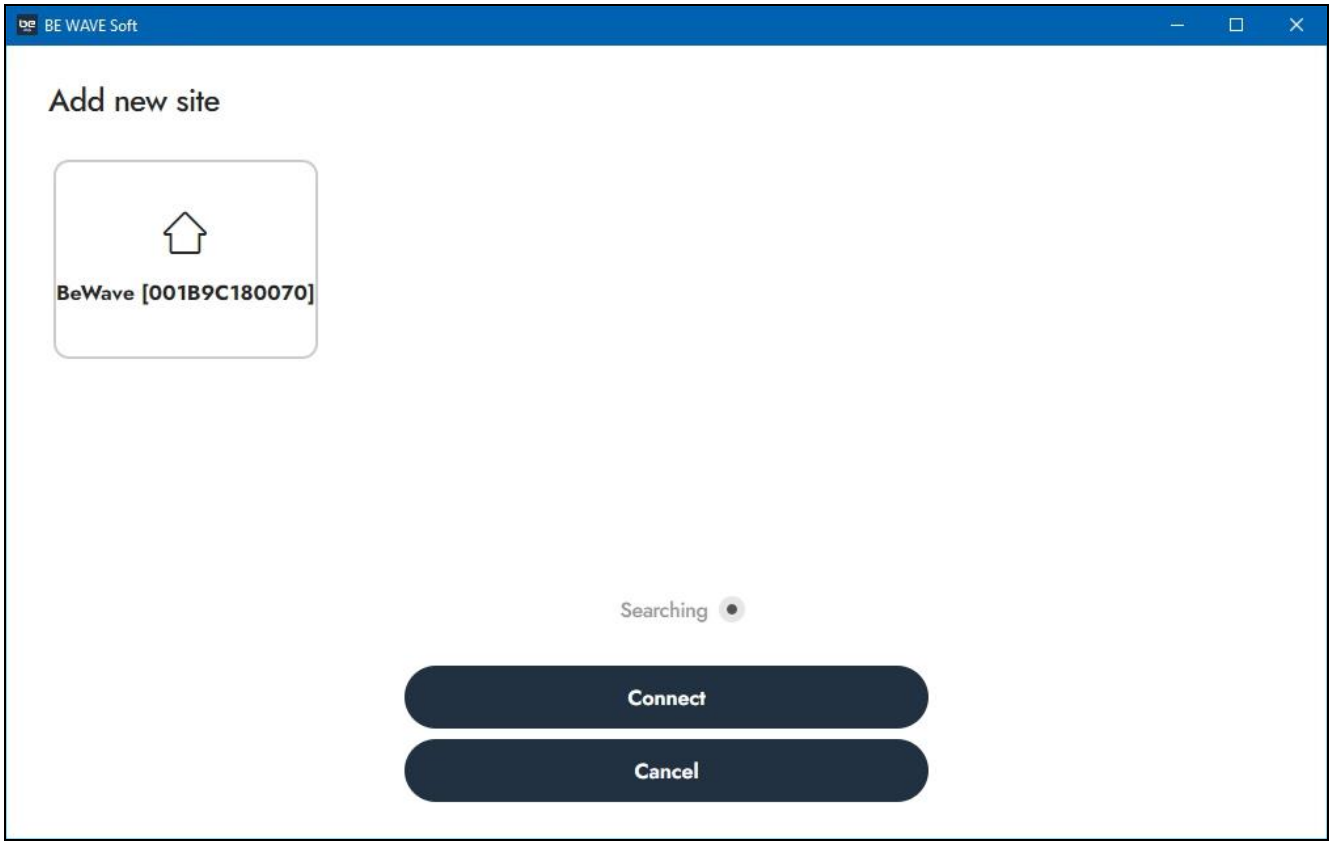
1. Start the BE WAVE Soft program. The *Select an account* window will be displayed.



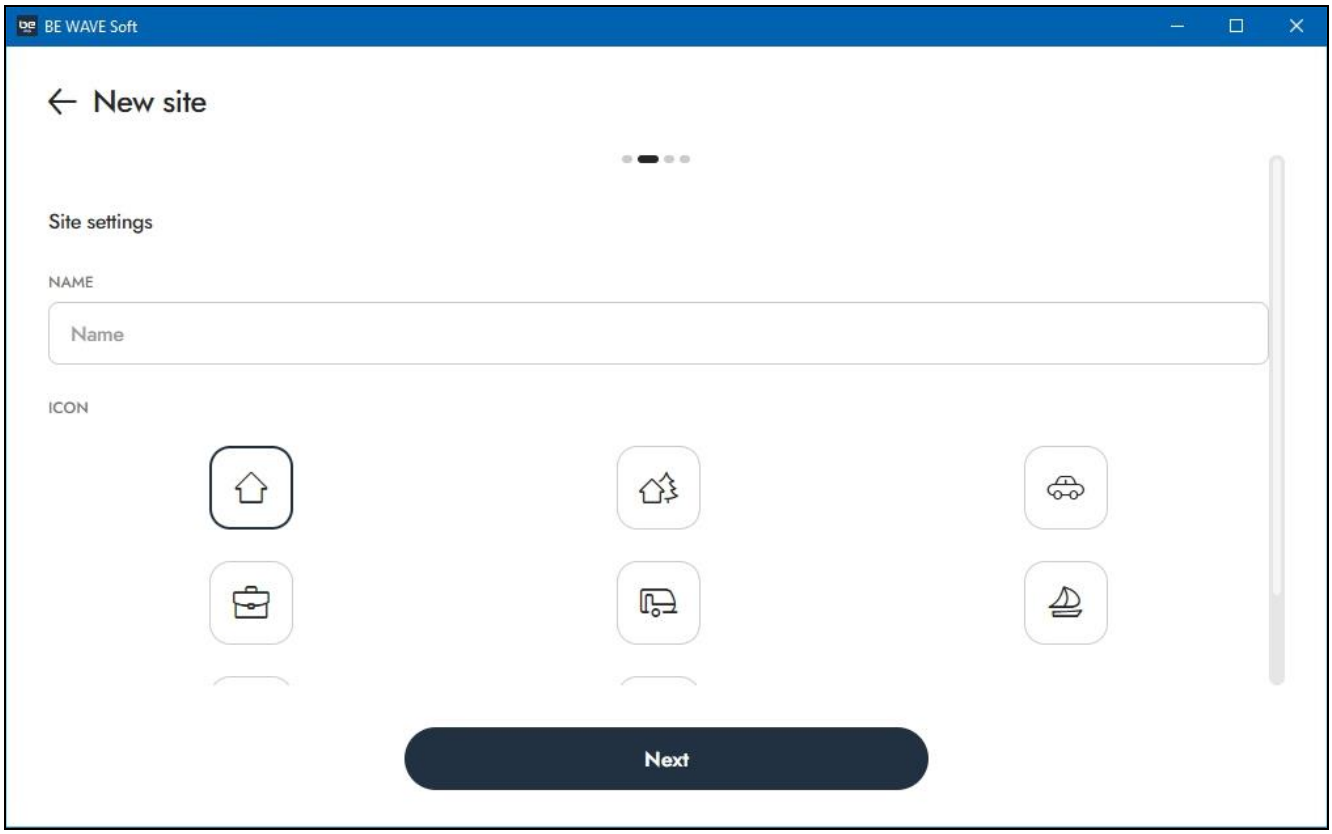
2. Click *Add new site*. The *Add new site* window will be displayed.



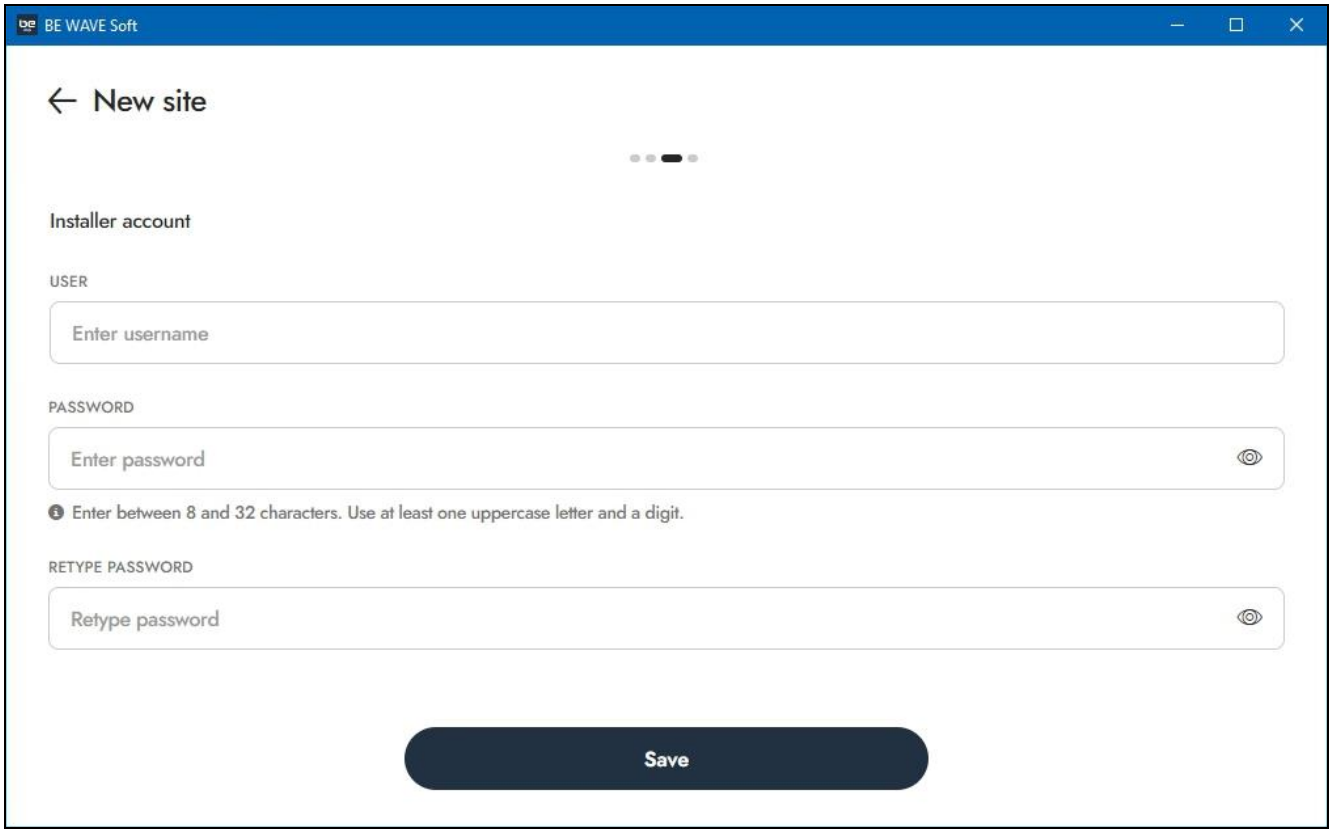
3. Click the controller (site) you want to add. Different buttons will appear at the bottom of the window.



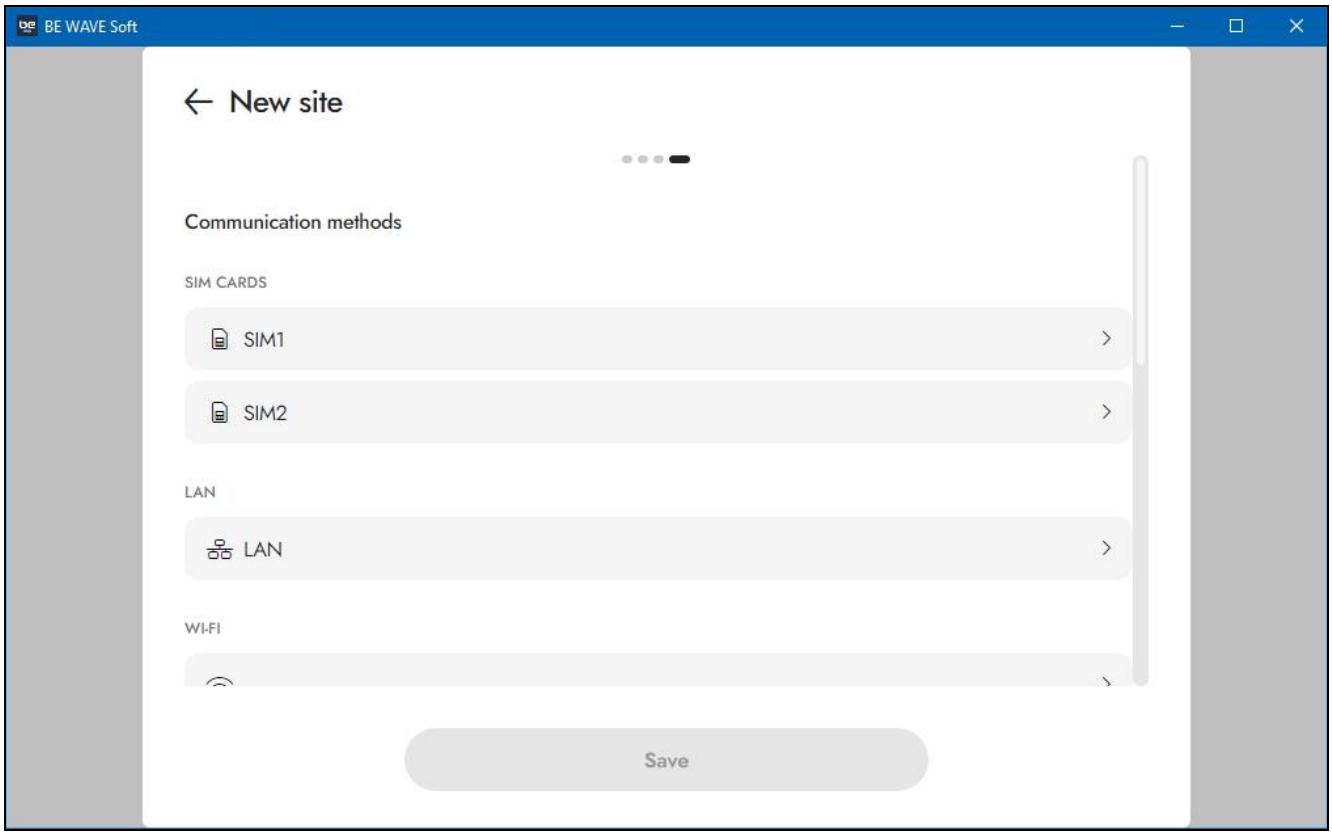
4. Click the *Connect* button. The *New site – Site settings* window will be displayed.



5. 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.



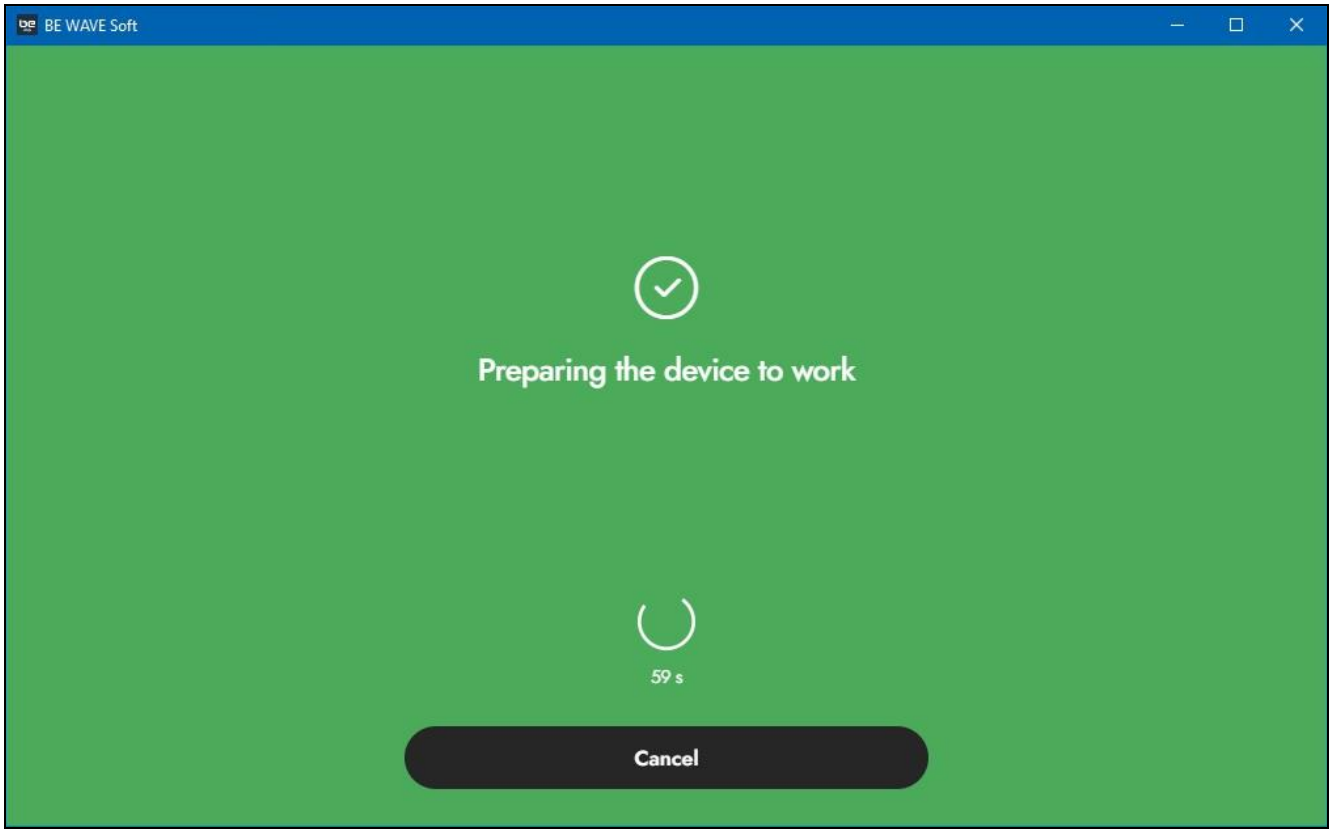
6. Enter the username and password for the installer, then click *Save*. The *New site – Communication methods* window will be displayed.



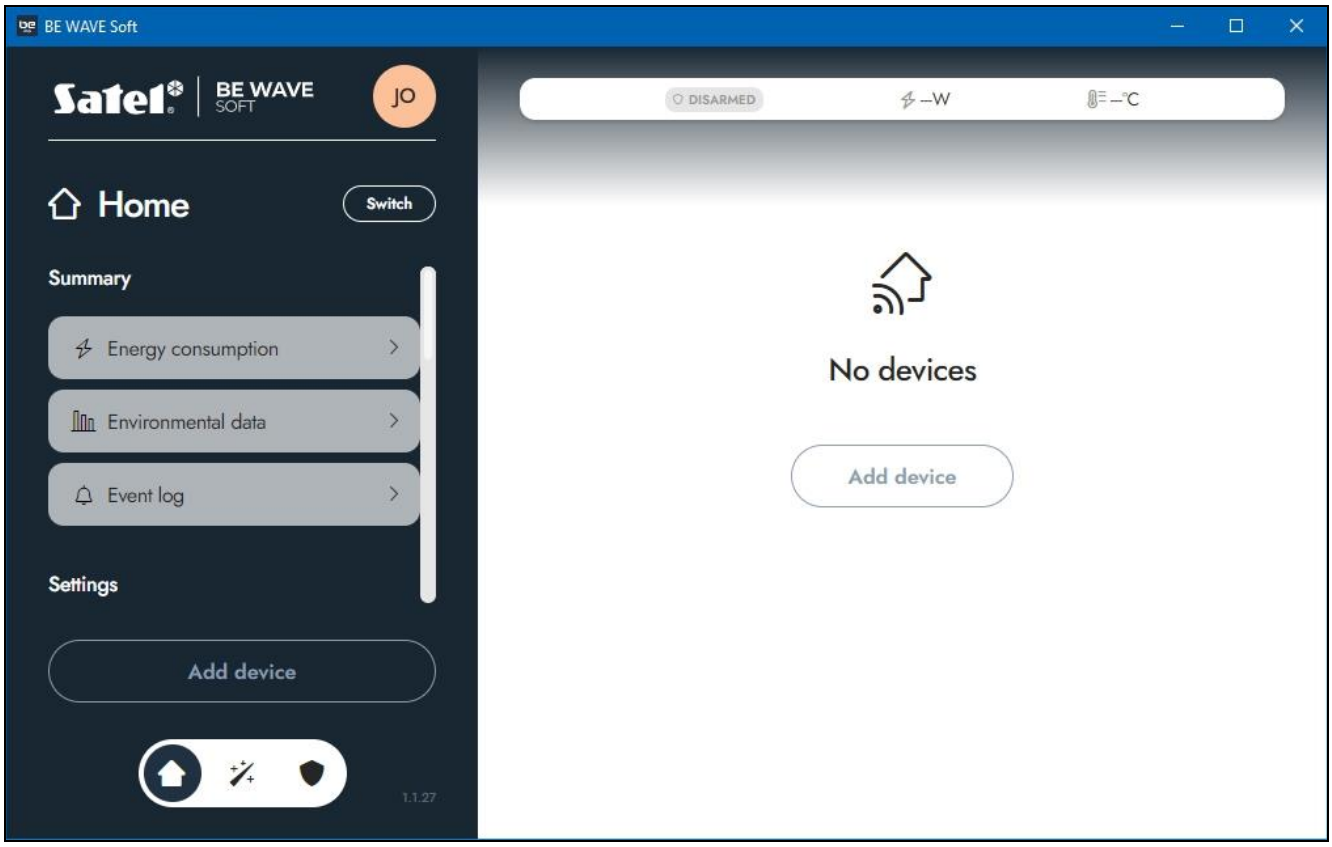
7. Select the communication method to be used with the controller. A new window will be displayed. Configure the settings for the selected communication method, then save the

settings. You will return to the *New site – Communication methods* screen. Click *Save*. A window will be displayed saying that the controller is being prepared to work.

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

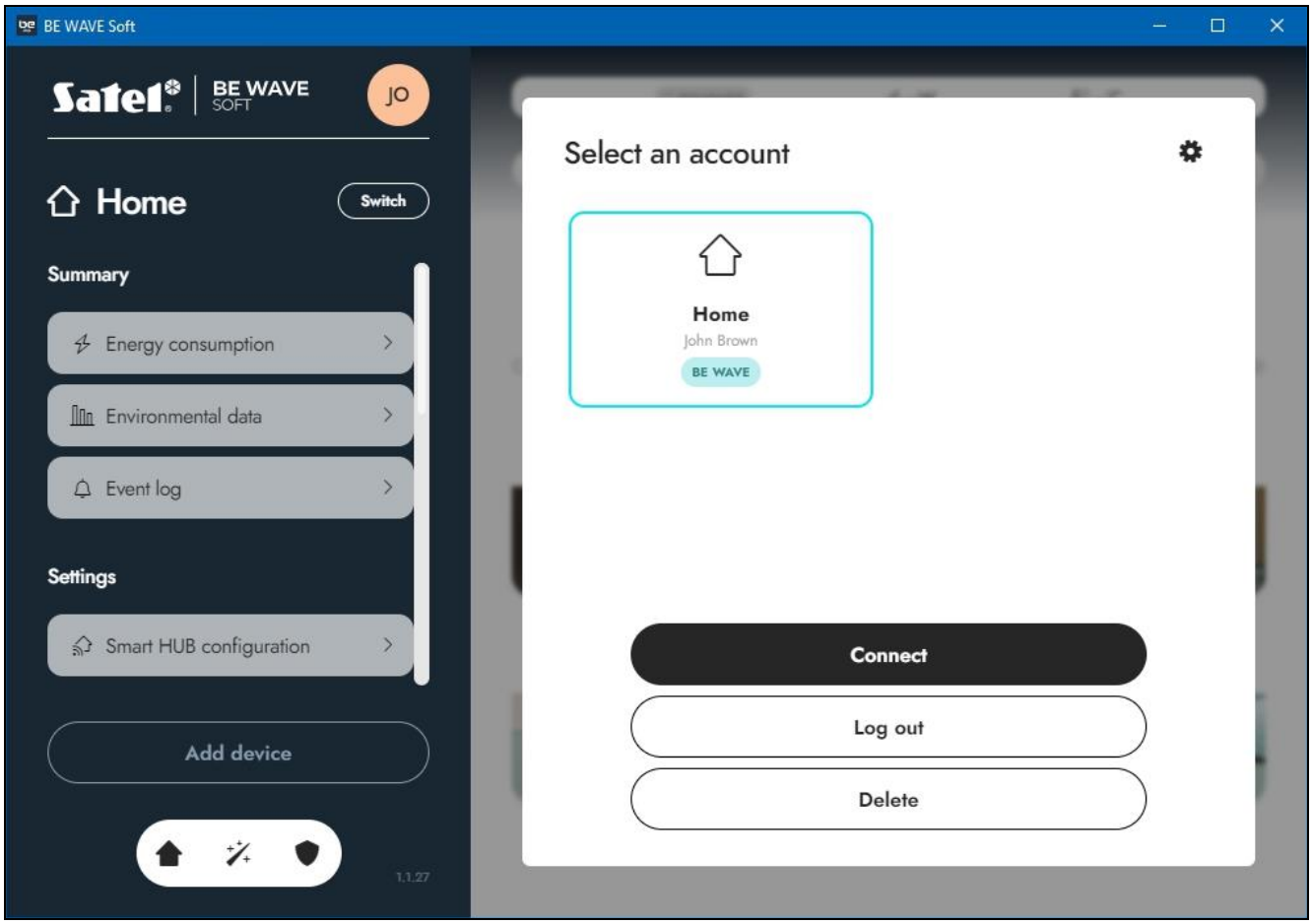


8. When the program connects to the controller by means of the selected communication method, the program's home screen will be displayed. You can add the first device to the system.



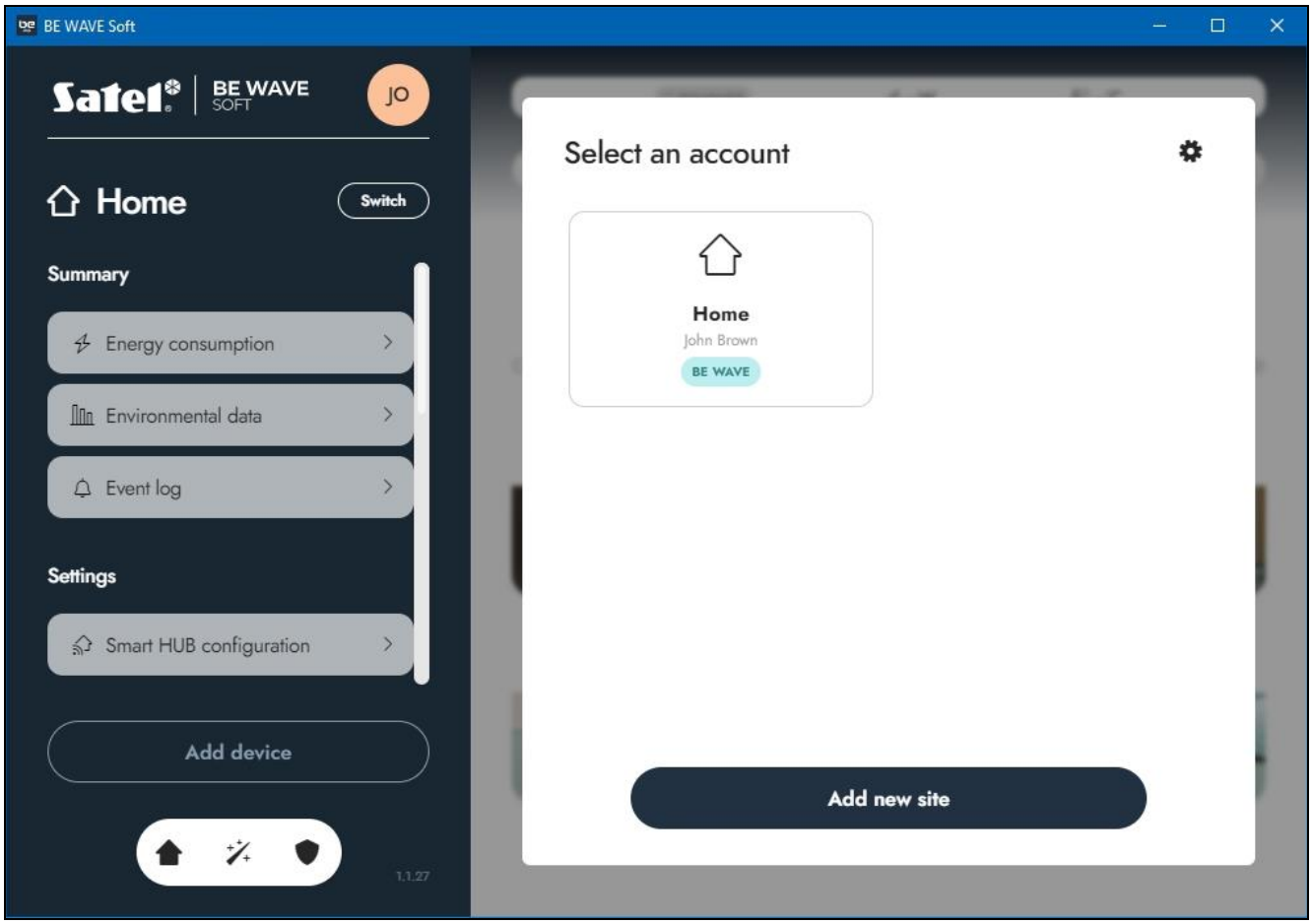
Adding another controller (site)

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.

If the controller 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 controller. Make sure it is the MAC address of the new controller.



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

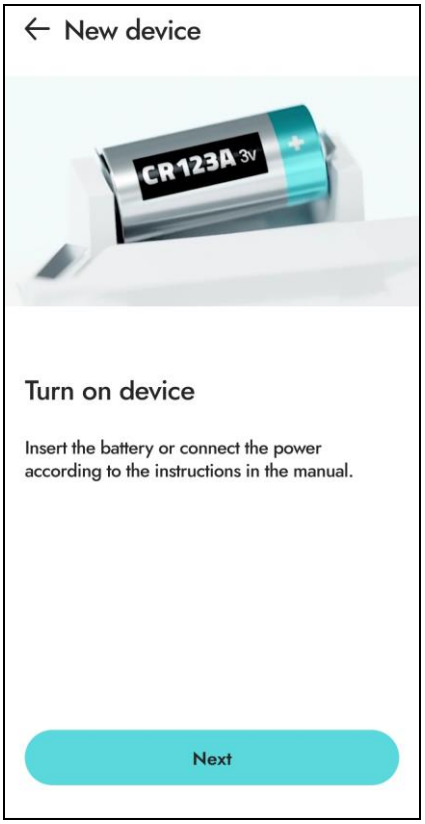
5.4 Adding a wireless device to the system

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).

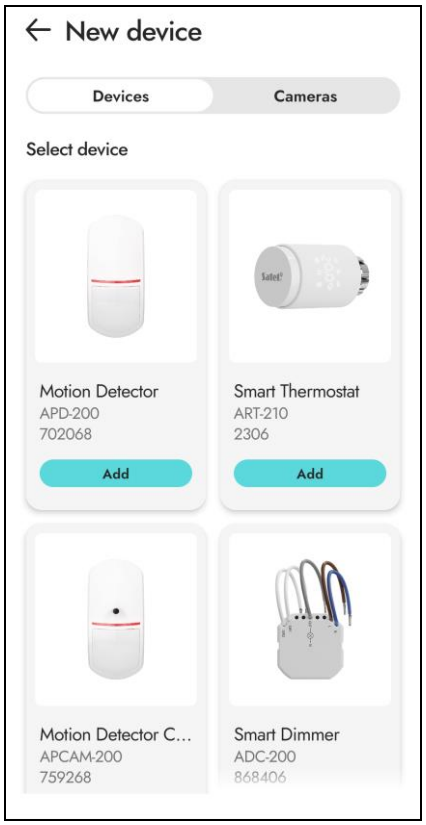
5.4.1 Adding a wireless device in the Be Wave app

Adding the first wireless device

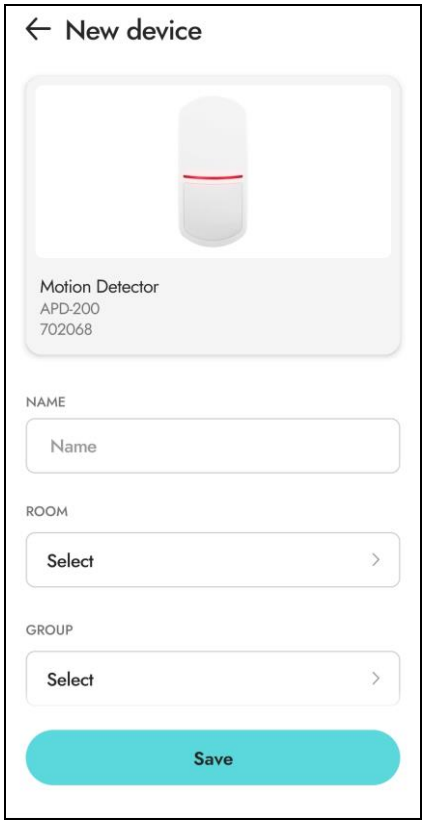
1. Tap the *Add device* button on the home screen. On a new screen you will be asked to turn on the device.



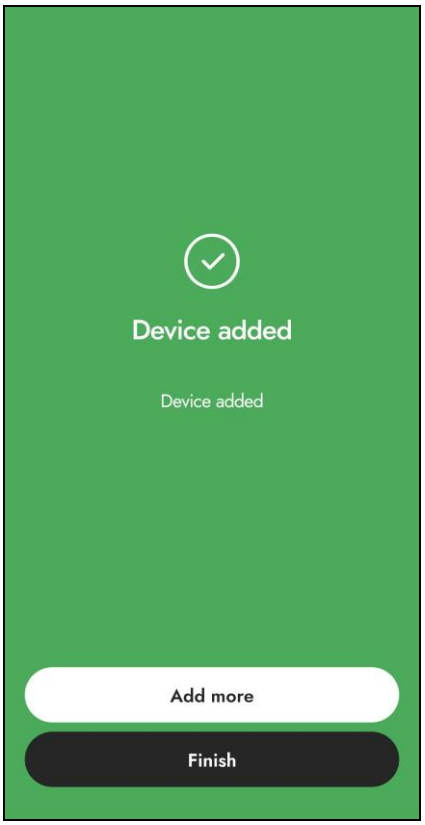
2. Insert the battery, connect the power, etc. (for detailed information, please refer to the manuals of particular devices), then tap *Next*. The list of wireless devices detected by the controller will be displayed (the screenshot is an example).



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. 50), 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 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. 52).

Adding another wireless device

If you want to add another BE WAVE device, tap on the home screen and tap:

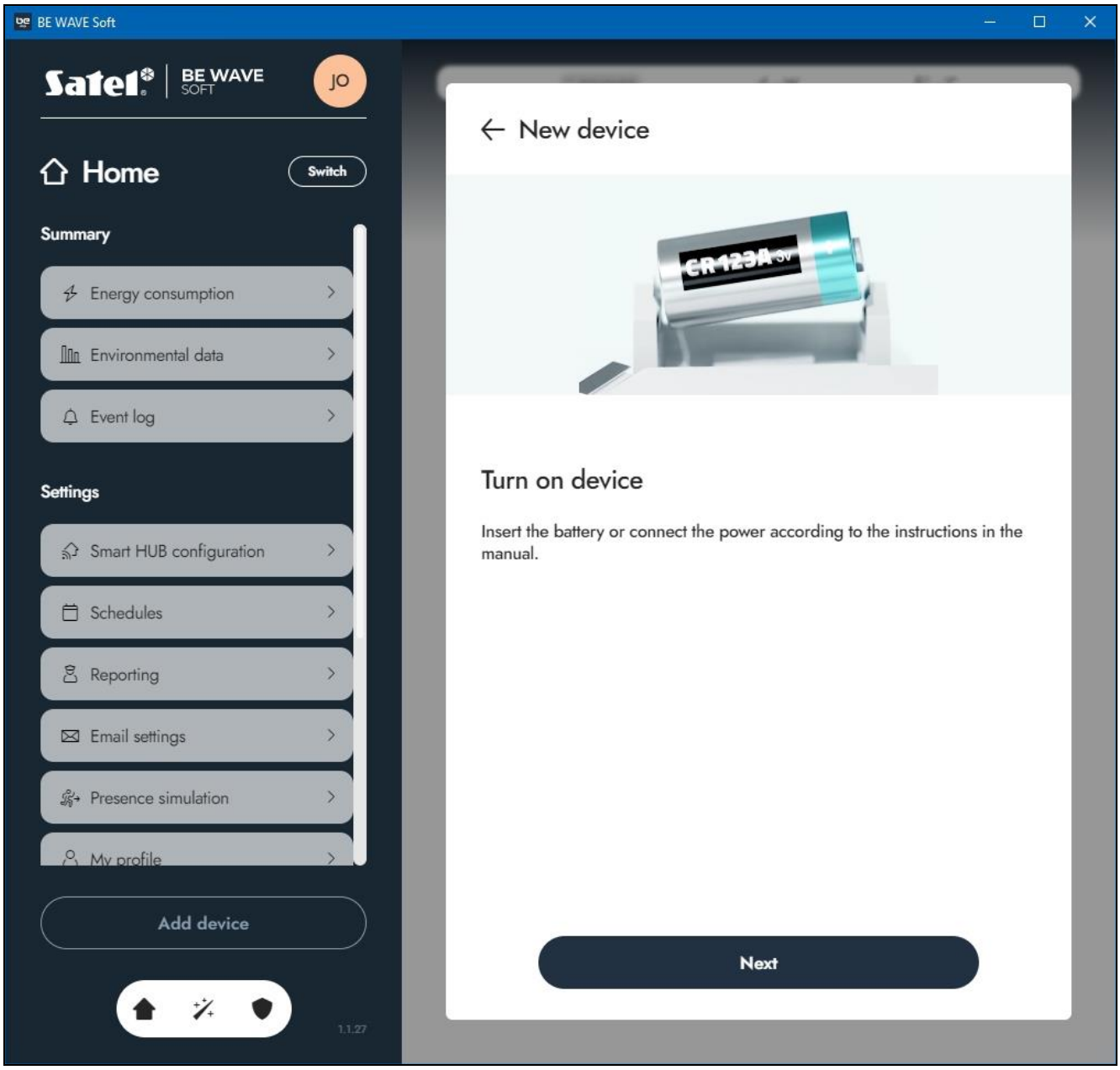
- group – at the bottom of the screen that will be displayed, the *Add device* button will be available.
- room – at the bottom of the screen that will be displayed, the *Add device* button will be available.
- icon – at the bottom of the screen that will be displayed, the *Add device* button will be available.

When you tap the *Add device* button, the process of adding the device is the same as for the first device.

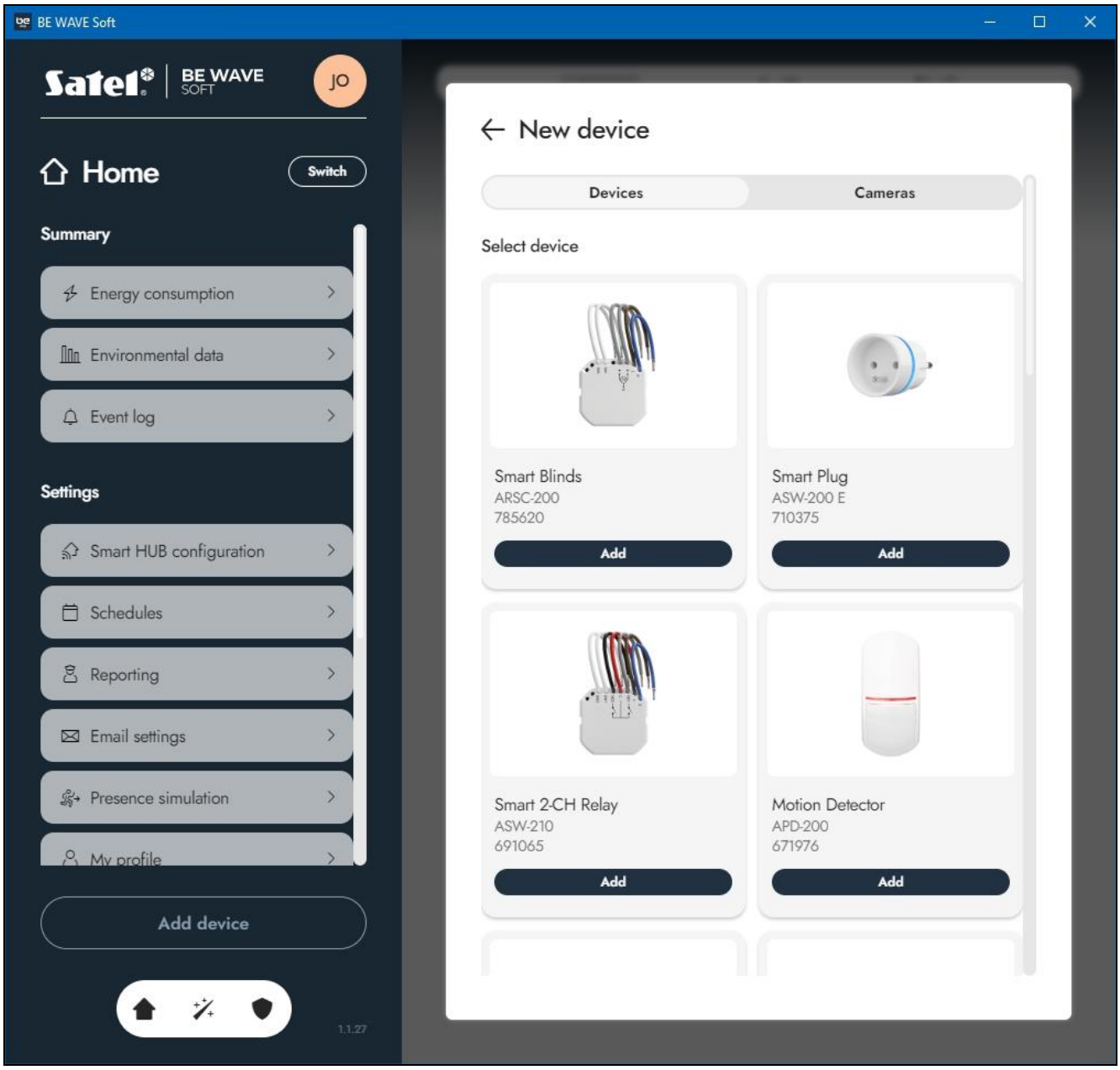
5.4.2 Adding a wireless device in the BE WAVE Soft program

Adding the first wireless device

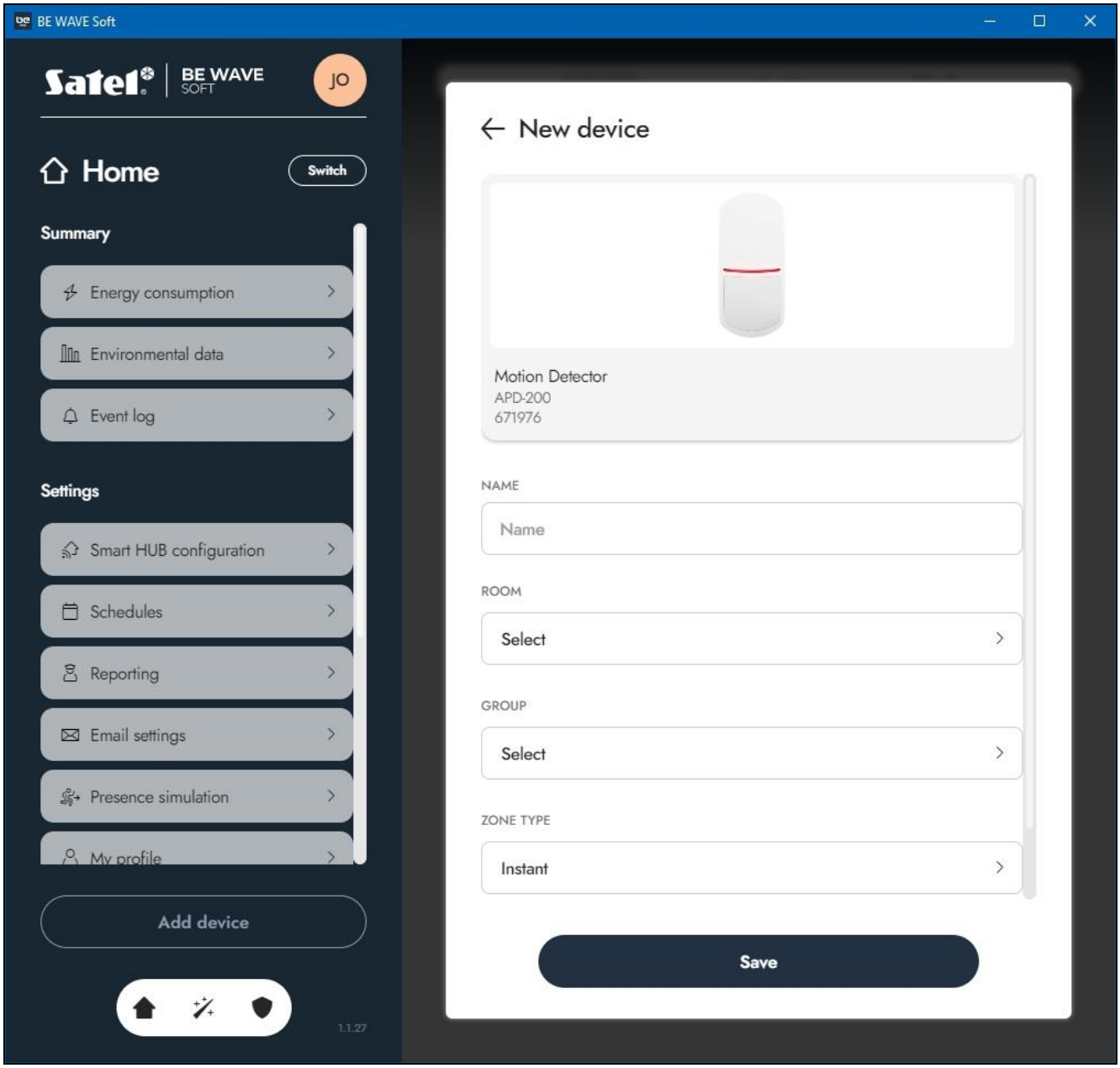
1. Click the *Add device* button. In the new window you will be asked to turn on the device.



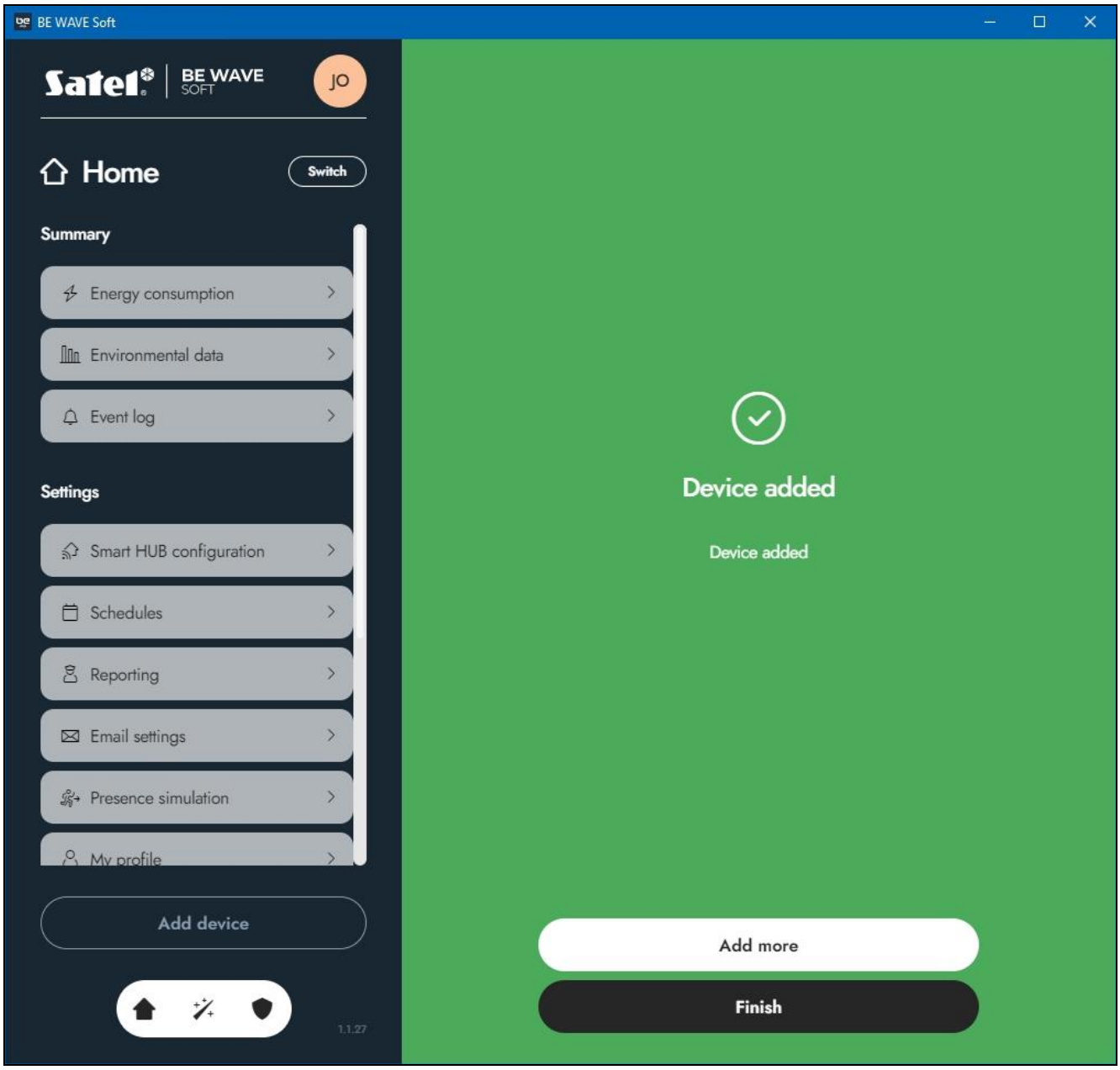
2. Insert the battery, connect the power, etc. (for detailed information, please refer to the manuals of particular devices), then click *Next*. The list of wireless devices detected by the controller will be displayed (the screenshot is an example).



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. 50), 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 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. 52).

Adding another wireless device

If you want to add another wireless device, click the *Add device* button on the side menu or click:

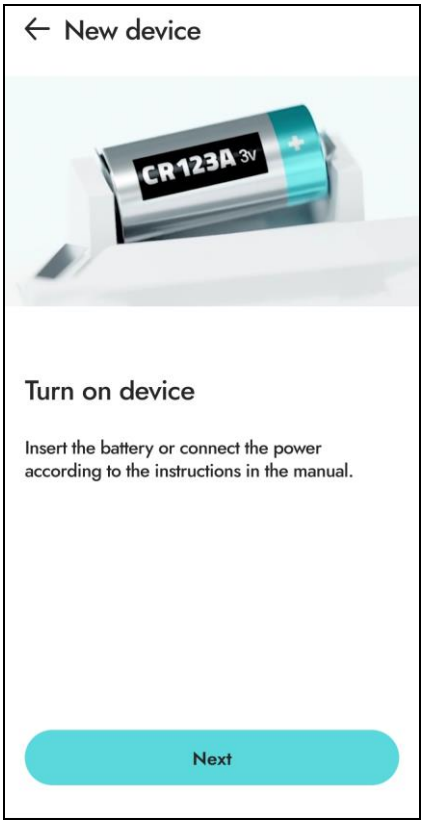
- group – at the bottom of the window that will be displayed, the *Add device* button will be available,
- room – at the bottom of the window that will be displayed, the *Add device* button will be available.

After you click the *Add device* button, the process of adding the device is the same as for the first device.

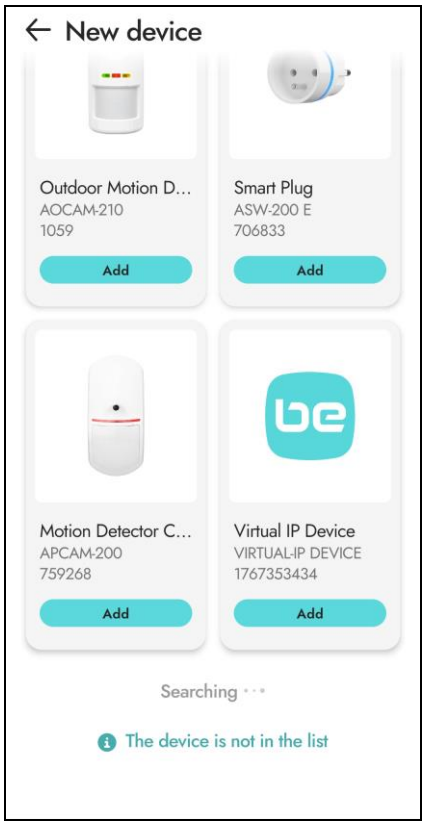
5.5 Adding a virtual IP device

5.5.1 Adding a virtual IP device in the Be Wave app

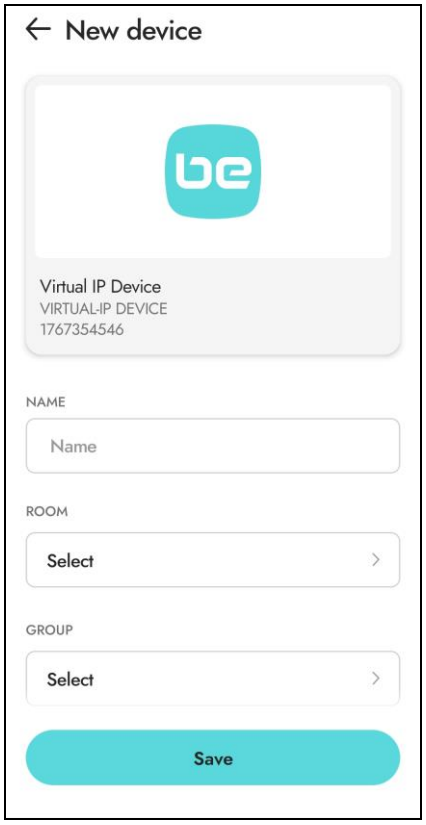
1. Tap the *Add device* button (on the room screen, group screen or settings screen). On a new screen you will be asked to turn on the device.



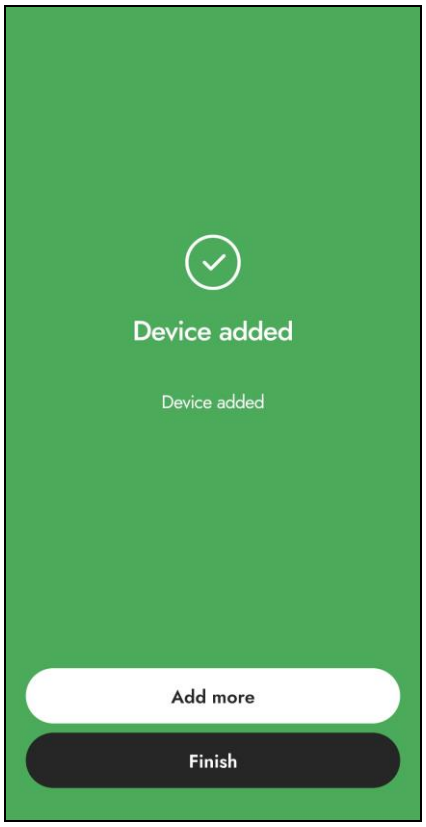
2. Tap *Next*. The list of wireless devices detected by the controller will be displayed (the screenshot is an example).



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



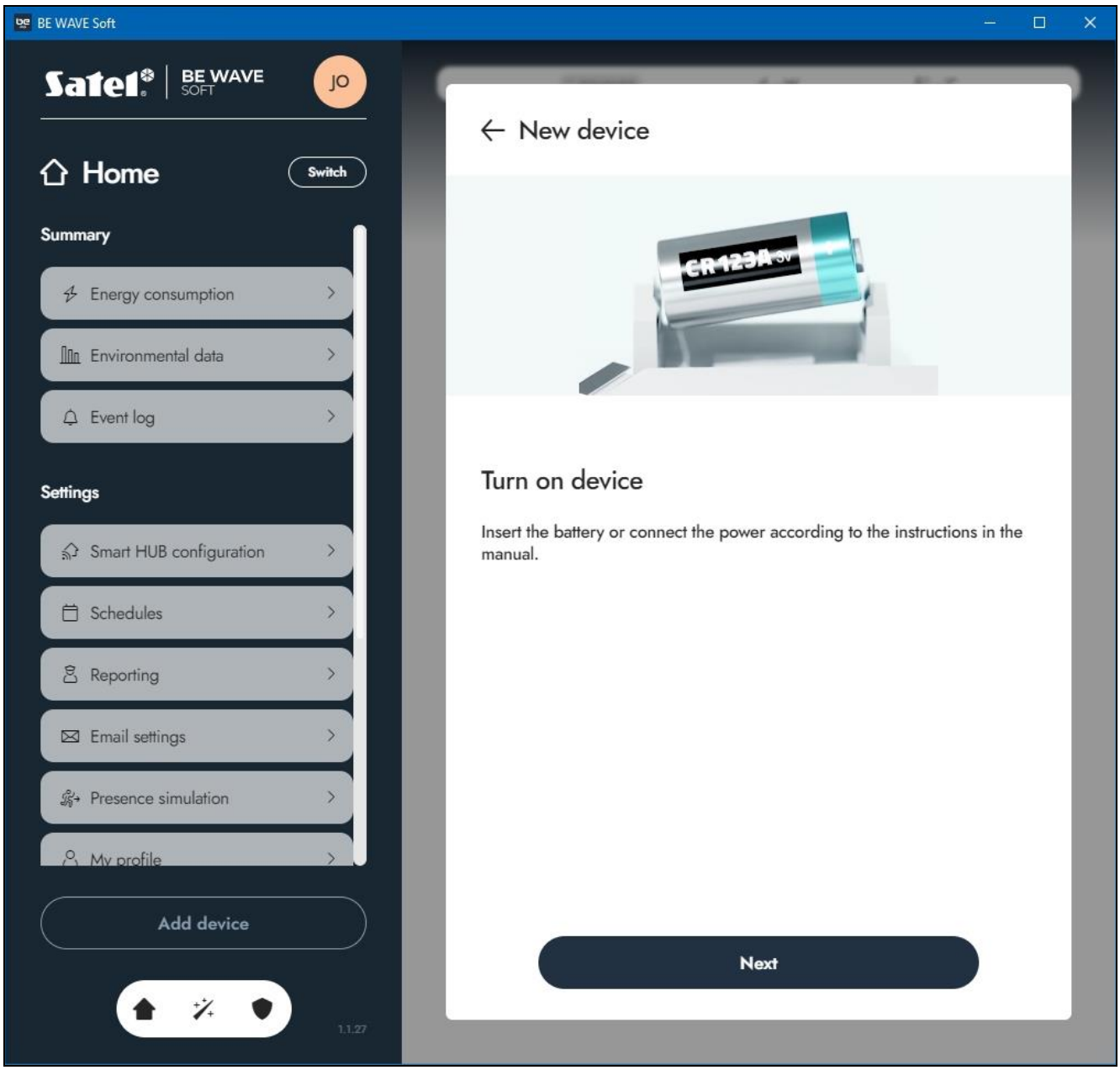
4. Configure the IP device settings (enter the name, assign the device to a room and to a group and select the zone type – see “Device settings” p. 50), then tap *Save*. A screen will be displayed saying that the device has been added.



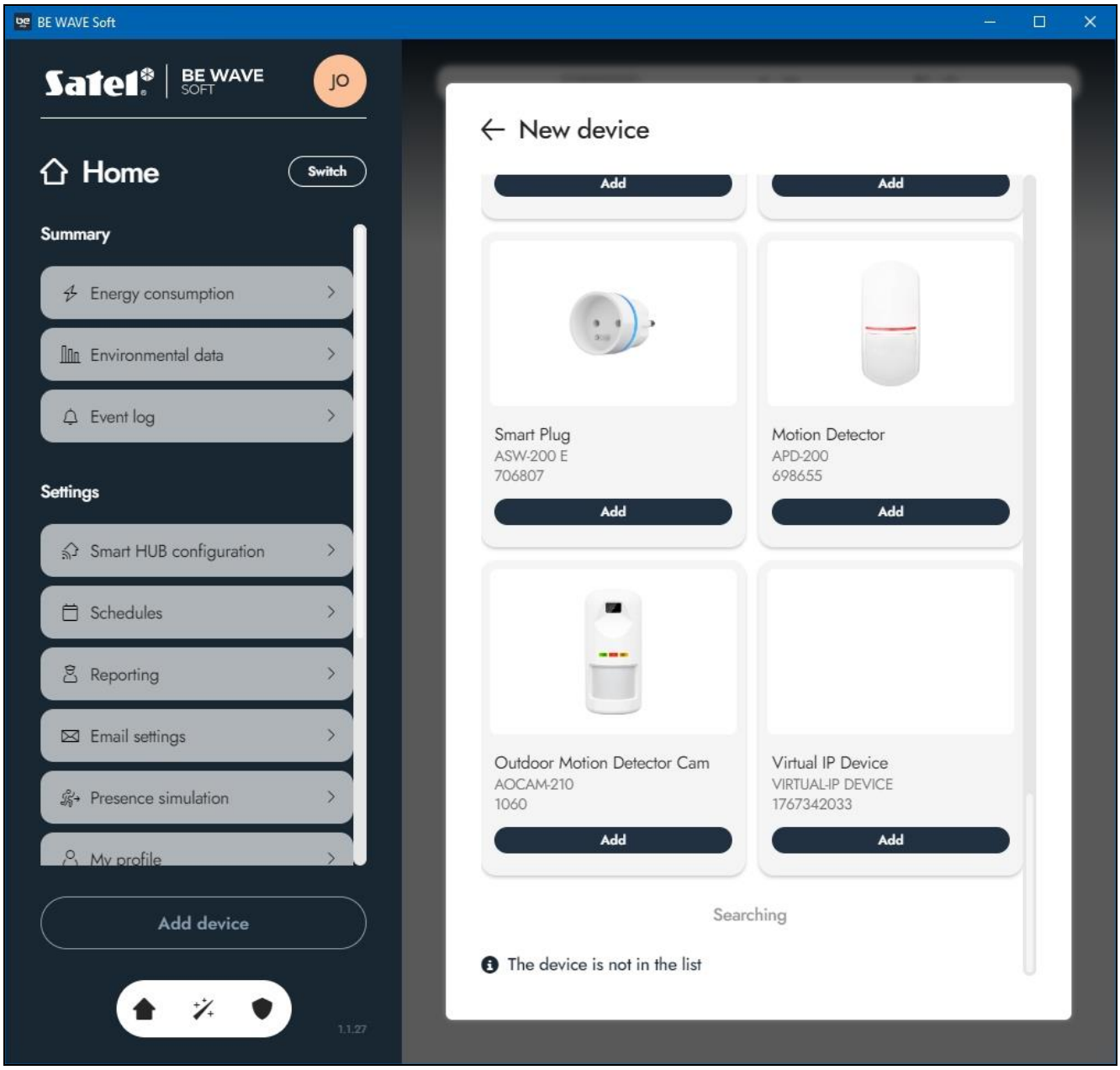
5. Tap *Add more* if you want to add another device or *Finish* if you do not want to add any more devices.
6. Configure additional settings of the IP device (see “IP device settings” p. 52).

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

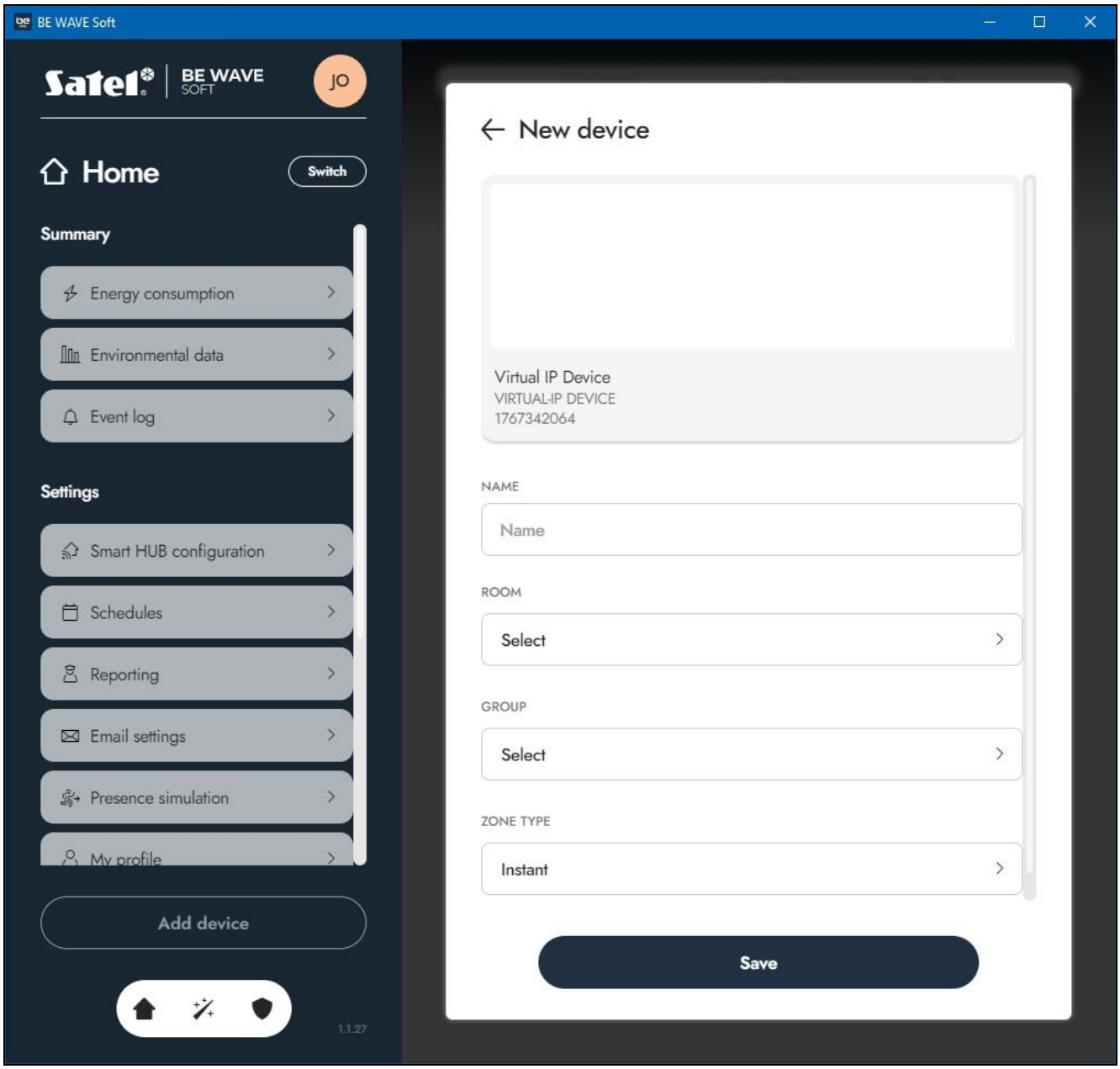
1. Click the *Add device* button (on the side menu, in the room window or group window). In the new window you will be asked to turn on the device.



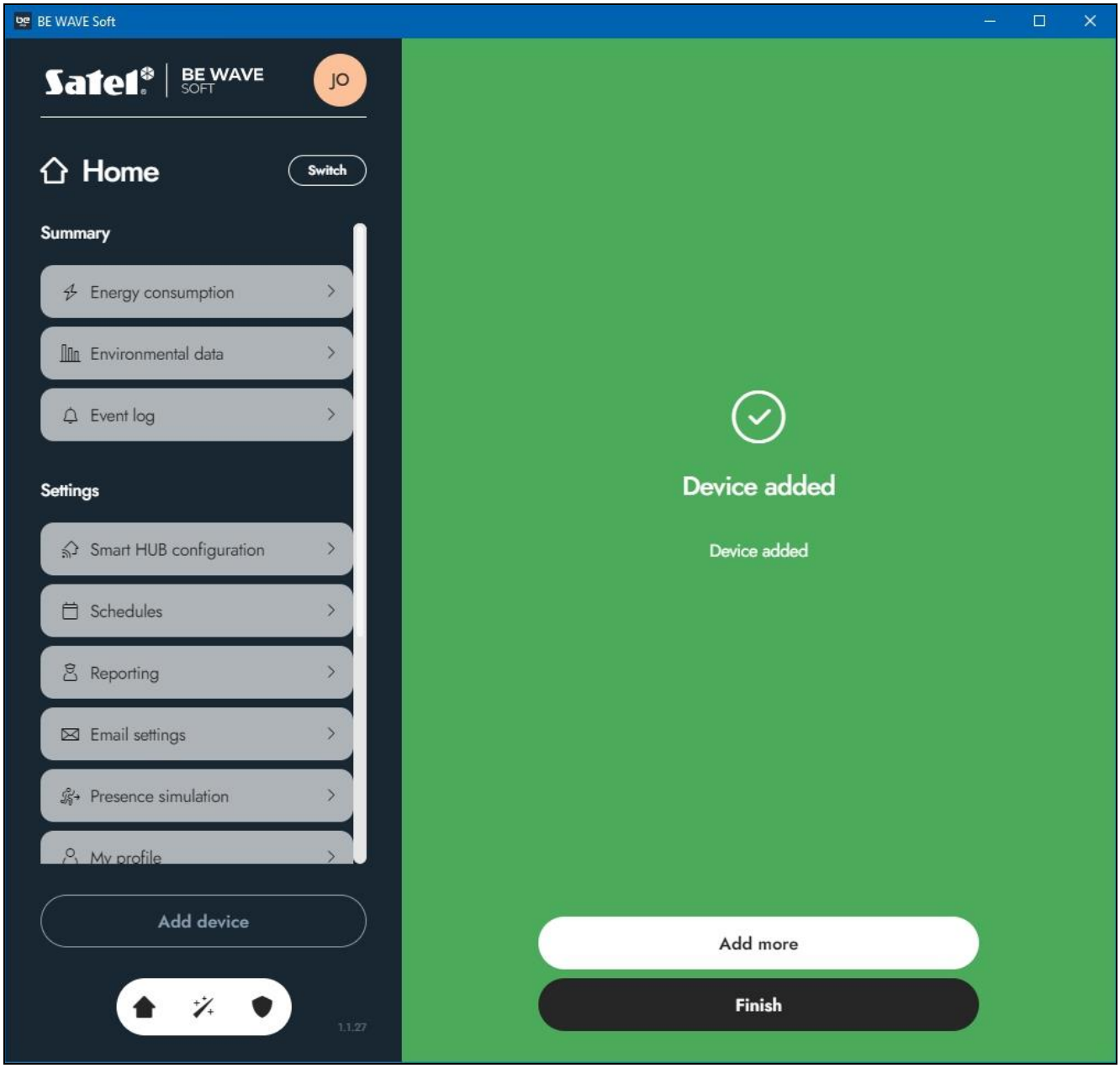
2. Click *Next*. The list of wireless devices detected by the controller will be displayed (the screenshot is an example).



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



4. Configure the device settings (enter the name, assign the device to a room and to a group and select the zone type – see “Device settings” p. 50), 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. 52).

5.6 Deleting a device

5.6.1 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 the *Delete device* button. You will be asked for confirmation.
4. Tap *Yes*. The device will be deleted.

5.6.2 Deleting a device in the BE WAVE Soft

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 the *Delete device* button. You will be asked for confirmation.
4. Click *Yes*. The device will be deleted.

5.7 Description of settings

5.7.1 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 device is to be turned on.

Alarm – 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 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 – device is turned on for a programmed time. Programming of the *Operating time* parameter is required.

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

Thermostat heating – 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.

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.

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

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 panic alarm – zone violation will generate a panic alarm. 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.

Button 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.
- ASW-210 controller (Smart 2-CH Relay):

  None – no button is connected to the input.

  Single – a single button is connected to the input.

Control mode – parameter for the ADC-200 dimmer (Smart Dimmer) / ARC-200 controller (Smart RGBW LED Driver) / ASW-210 controller (Smart 2-CH Relay), if *Single* was selected for the button type, and the ATX-200 module (Smart Switch Controller). Select 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). 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 the ACX-210 expander output (Mini Multi Extender) / ACX-220 expander output (Multi Extender) / 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). 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.

5.7.2 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.

5.7.3 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 an IP address or 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.

5.7.4 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 controller 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 controller fails to connect to station 1 during the link test, the controller 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 controller 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 – controller 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 an IP address or domain name.

Port [server 1] – number of the port used for communication between the controller 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 an IP address or domain name.

Port [server 2] – number of the port used for communication between the controller 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 controller 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 controller 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 controller for the purpose of *SIA-IP* reporting. The parameter allows you to expand the list of attributes used to identify the controller. 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 controller for the purpose of *SIA-IP* reporting. The parameter allows you to expand the list of attributes used to identify the controller. 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 controller).

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 controller).

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 controller 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 controller 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 controller 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 controller fails to connect to the monitoring station's server 1 during the link test, the controller 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 an IP address or domain name.

Port [server 1] – number of the port used for communication between the controller 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 an IP address or domain name.

Port [server 2] – number of the port used for communication between the controller 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 – controller 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 controller 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.

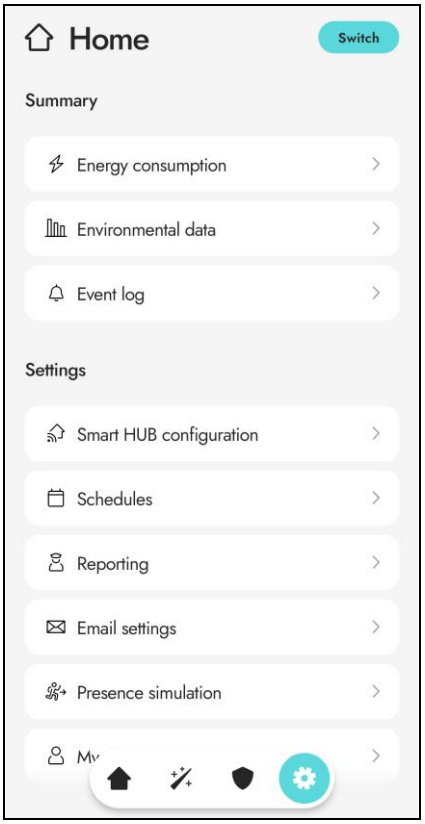
On time – if the test transmission is to be sent every day at a specified time, enter the hour and minutes.

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.

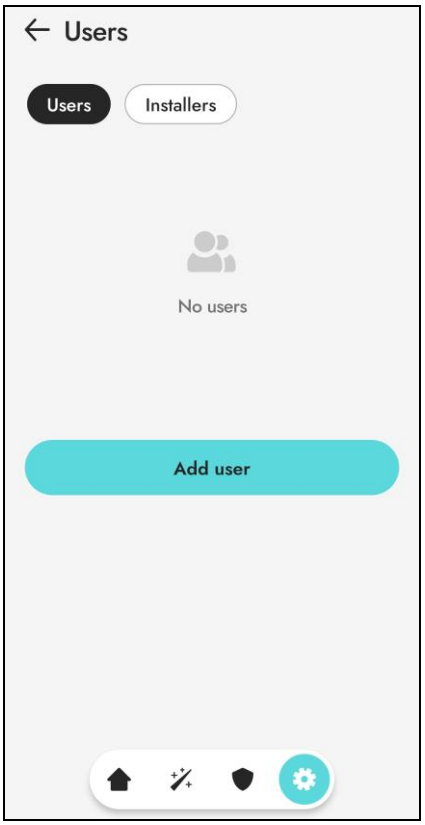
5.8 Adding a user

5.8.1 Adding a user in the Be Wave app

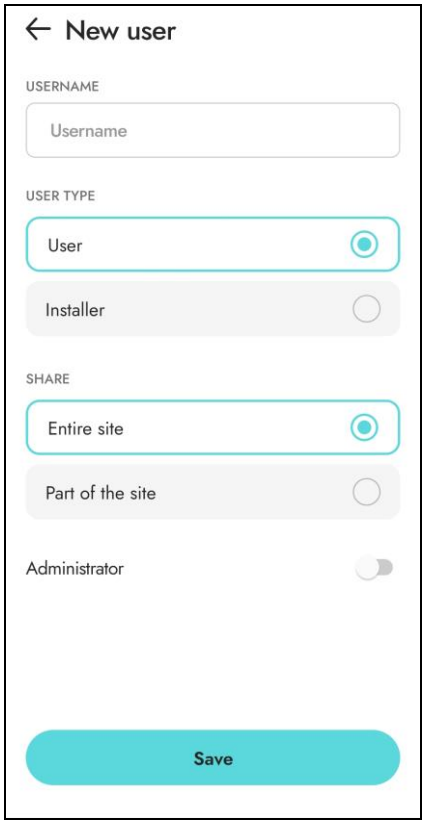
1. Tap on the menu bar. The *Settings* screen will be displayed.



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



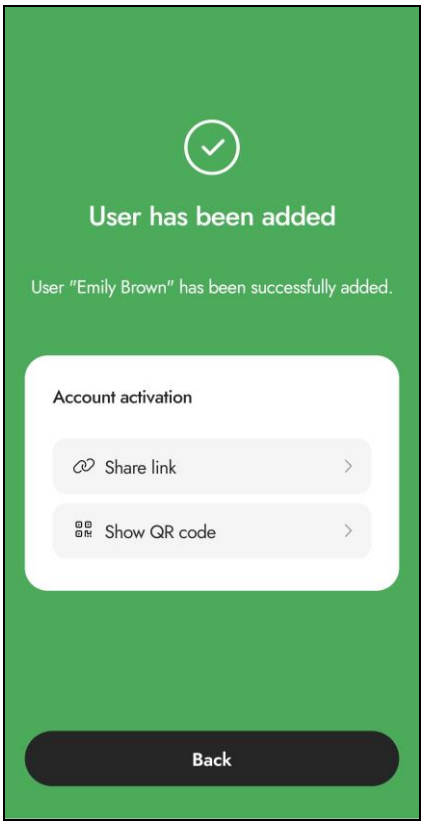
3. Tap the *Add user* button. The *New user* screen will be displayed.



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. 61) or *Part of the site* (see “User with access to a part of the site” p. 62) 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.

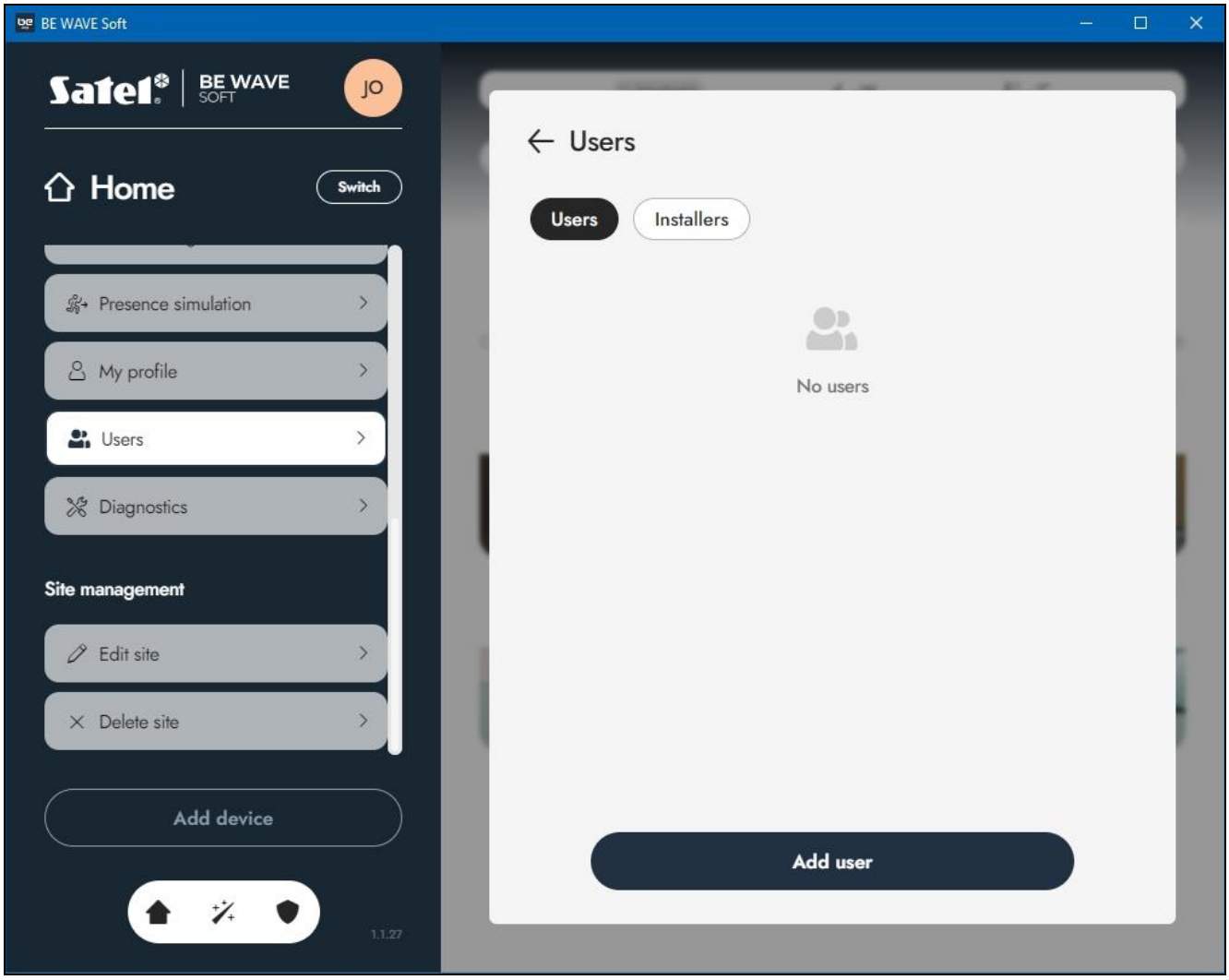
The user must activate the account within 24 hours of generating the link / QR code. Otherwise, the user will have to request a new link / QR code.



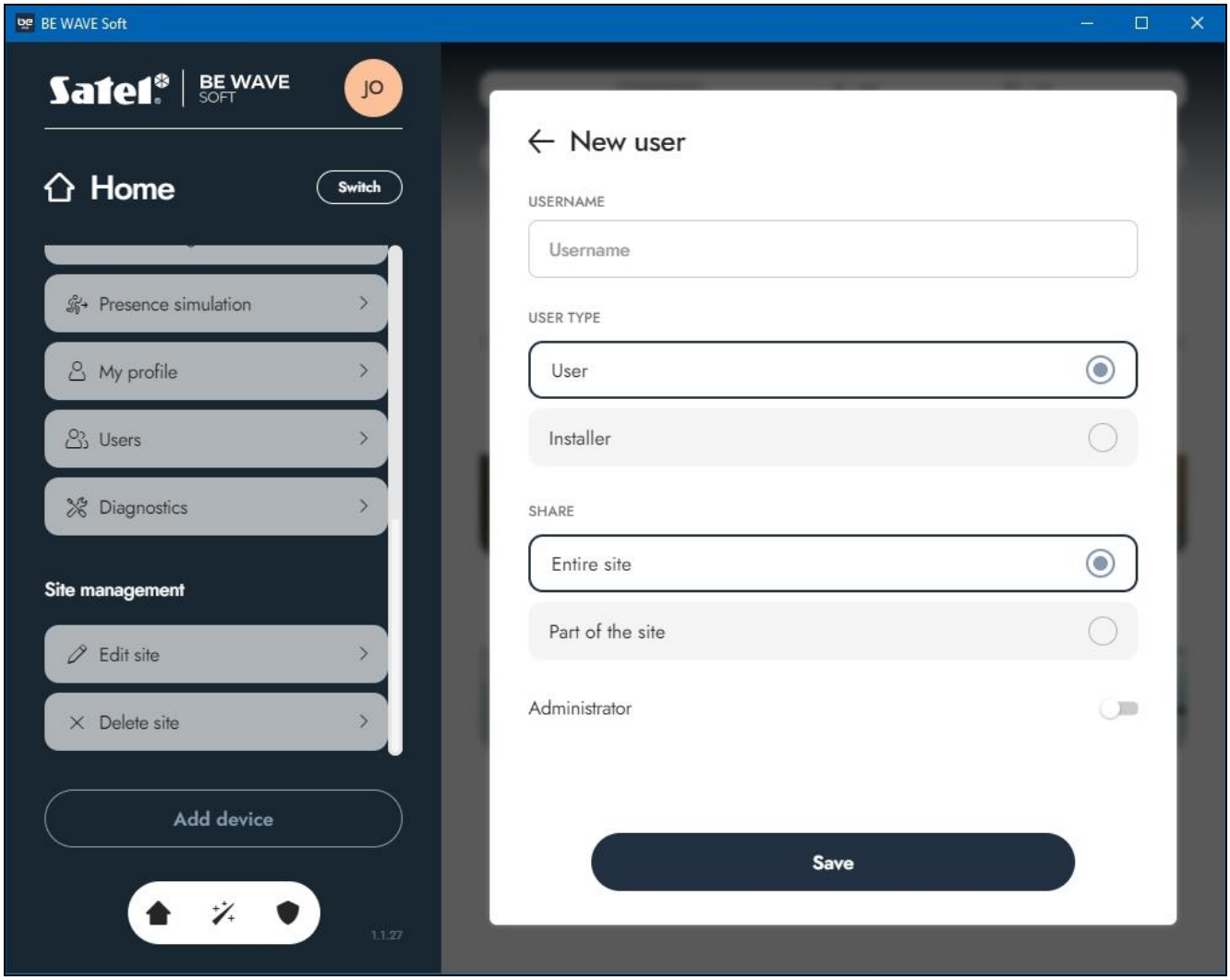
8. Tap *Back*. The *Users* screen will be displayed.

5.8.2 Adding a user in the BE WAVE Soft program

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



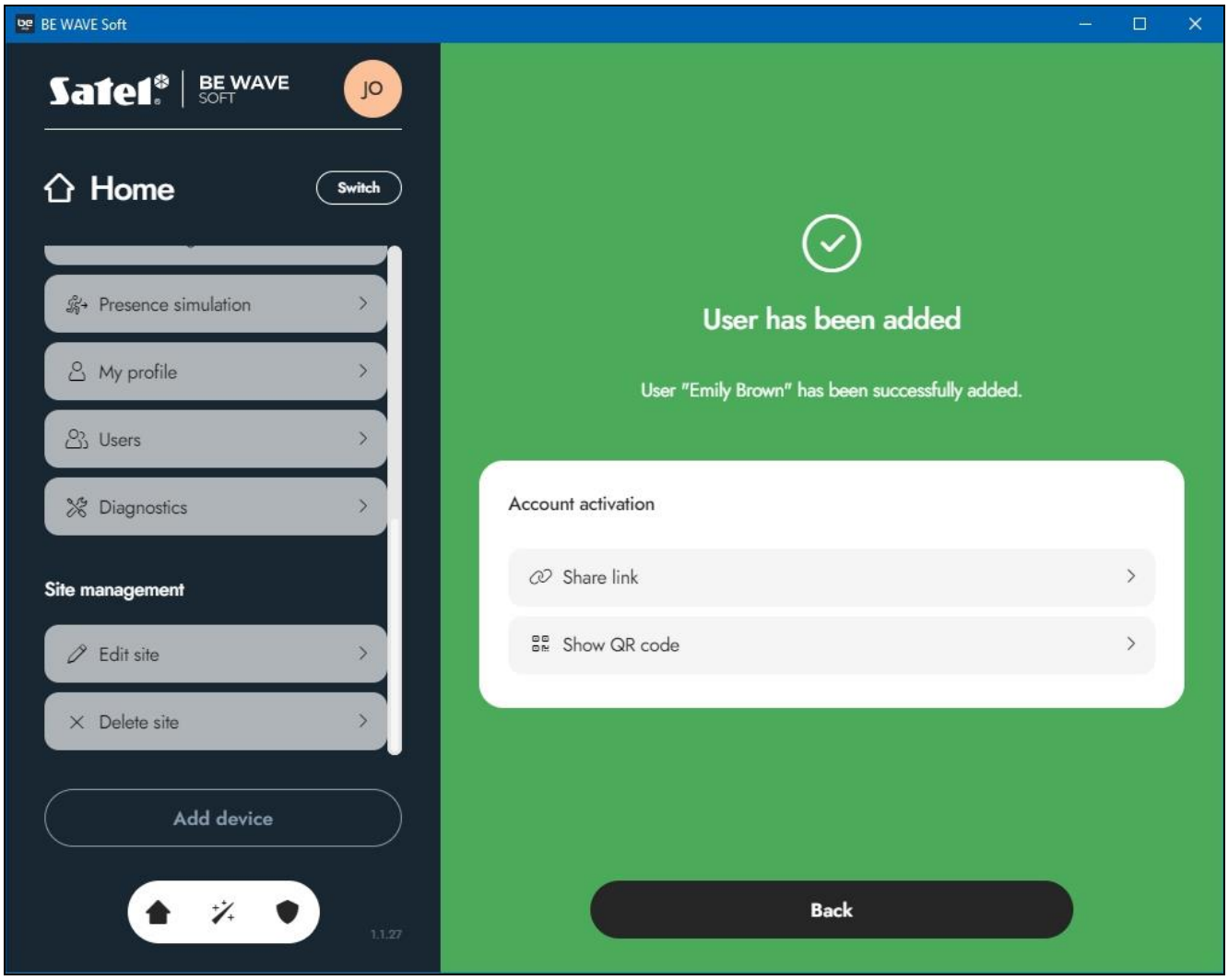
2. Click *Add user* button. The *New user* window will be displayed.



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. 61) or *Part of the site* (see “User with access to a part of the site” p. 62) 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:
   – click *Share link* if you want to send a link to the user.
   – click *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.

5.8.3 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.

5.8.4 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.

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:

- 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 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 the APMD-250 (Motion Detector Plus), AOD-210 (Outdoor Motion Detector), AOCAM-210 (Outdoor Motion Detector Cam) and AOCD-260 (Outdoor Curtain Detector) detectors. 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 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 the *Diagnostics* button. 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 the *Diagnostics* button 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 the *Diagnostics* button. 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 the *Diagnostics* button 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 controller 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 the *Smart HUB configuration* button. The *Smart HUB configuration* 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 controller and the devices in the system.

7.1.2 Starting the update in the BE WAVE Soft program

1. Click the *Smart HUB configuration* button on the side menu. The *Smart HUB configuration* 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 controller and the devices in the system.

7.2 Replacing the battery in the controller

The rechargeable battery in the controller should be replaced by qualified personnel.

Be particularly careful when replacing the battery. The manufacturer is not liable for the consequences of incorrect installation of the battery.

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

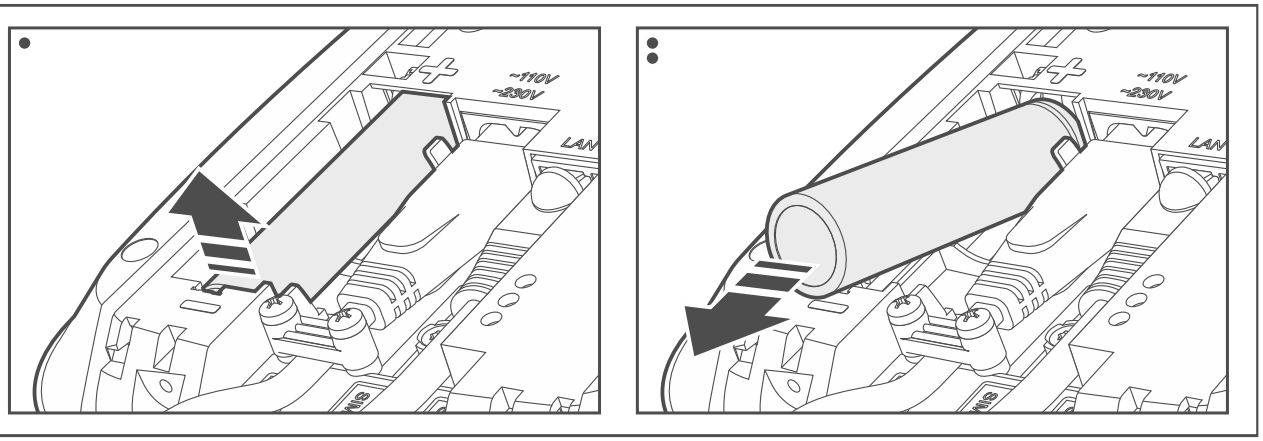
The controller rechargeable battery will not be charged in temperatures below 0°C.

The Be Wave app will notify you that the rechargeable battery is low. The low battery should then be replaced as soon as possible.

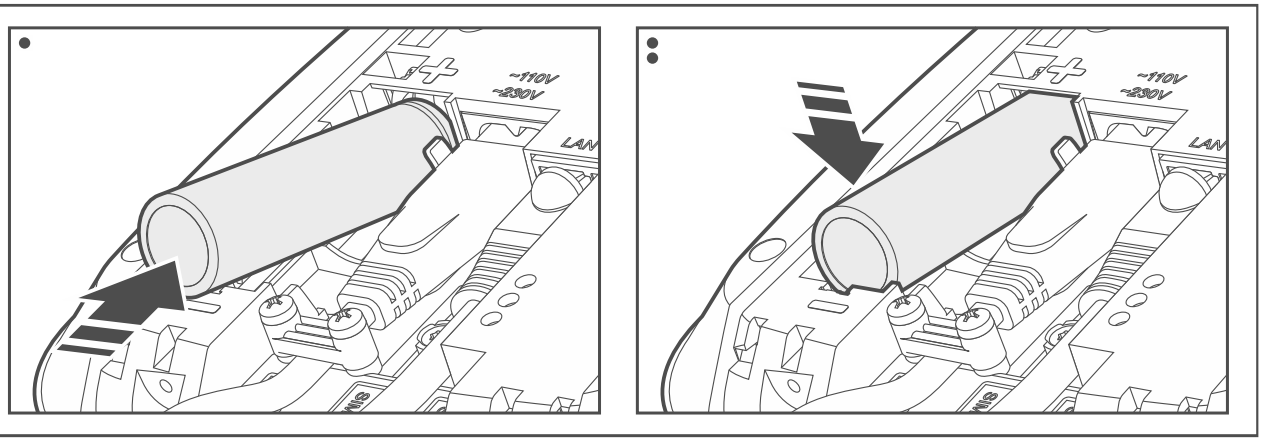
The figures show how to replace the battery in the Smart HUB Plus / Smart HUB controller.

1. Enable the diagnostic mode in the Be Wave app / BE WAVE Soft program.
2. Open the controller enclosure.
3. Remove the old battery (Fig. 28).
4. Install the new battery (Fig. 29).
5. Close the enclosure and secure it with screws.
6. Disable the diagnostic mode in the Be Wave app / BE WAVE Soft program.

28



29



7.3 Restoring the controller factory settings

7.3.1 Restoring the factory settings from the Be Wave app

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

7.3.2 Restoring the factory settings from the BE WAVE Soft program

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

7.3.3 Hardware factory restore

1. Enable the diagnostic mode in the Be Wave app.
2. Open the controller enclosure.
3. Insert a pin in hole marked ⑥ (Fig. 2) and hold for 5 seconds.

7.4 Turning off the Smart HUB Plus / Smart HUB controller

1. Disconnect the power cable from the power outlet.
2. Remove the cover locking screws.
3. Open the controller enclosure.
4. Remove the battery.

7.5 Turning off the Smart HUB Plus LV controller

1. Turn off the controller DC power.
2. Remove the cover locking screws.
3. Open the controller enclosure.
4. Remove the battery.

8. Specifications

8.1 Smart HUB Plus / Smart HUB

Operating frequency band .....868.0 MHz ÷ 868.6 MHz
Radio communication range (in open area) ..... up to 2000 m
Supply voltage ..... 230 VAC, 50 Hz
Rechargeable battery .....18650 3.6 V / 3200 mAh
Standby power consumption
- Smart HUB Plus .....1.85 W
- Smart HUB .....1.82 W

Maximum power consumption
- Smart HUB Plus .....2.8 W
- Smart HUB .....2.65 W

Standby current consumption from battery
- Smart HUB Plus .....272 mA
- Smart HUB .....252 mA

Battery charging current.....185 mA
Low battery voltage threshold .....3.2 V
Battery cut-off voltage .....2.7 V

Battery operating temperature
- discharging ..... -10°C...+60°C
- charging ..... 0°C...+45°C

Supported memory cards ..... microSD, micro SDHC
Security grade according to EN 50131-1 ..... Grade 2
Complied with standards ..... EN 50130-4, EN 50130-5, EN 50131-1, EN 50131-3, EN 50131-5-3
Environmental class according to EN 50130-5 II
Operating temperature range ..... -10°C...+55°C
Maximum humidity ..... 93±3%
Dimensions ..... 158 x 158 x 30 mm
Weight
- Smart HUB Plus ..... 411 g
- Smart HUB ..... 406 g

8.2 Smart HUB Plus LV

Operating frequency band ..... 868.0 MHz ÷ 868.6 MHz
Radio communication range (in open area) ..... up to 2000 m
Supply voltage ..... 9...28 VDC
Rechargeable battery ..... 18650 3.6 V / 3200 mAh
Standby current consumption
- 9 VDC power ..... 113 mA
- 28 VDC power ..... 42 mA

Maximum current consumption
- 9 VDC power ..... 240 mA
- 28 VDC power ..... 60 mA

Standby current consumption from battery ..... 220 mA
Battery charging current ..... 205 mA
Low battery voltage threshold ..... 3.2 V
Battery cut-off voltage ..... 2.7 V
Battery operating temperature
- discharging ..... -10°C...+60°C
- charging ..... 0°C...+45°C

Supported memory cards ..... microSD, micro SDHC
Security grade according to EN 50131-1 ..... Grade 2
Complied with standards ..... EN 50130-4, EN 50130-5, EN 50131-1, EN 50131-3, EN 50131-5-3
Environmental class according to EN 50130-5 II
Operating temperature range ..... -10°C...+55°C
Maximum humidity ..... 93±3%
Dimensions ..... 158 x 158 x 30 mm
Weight ..... 324 g