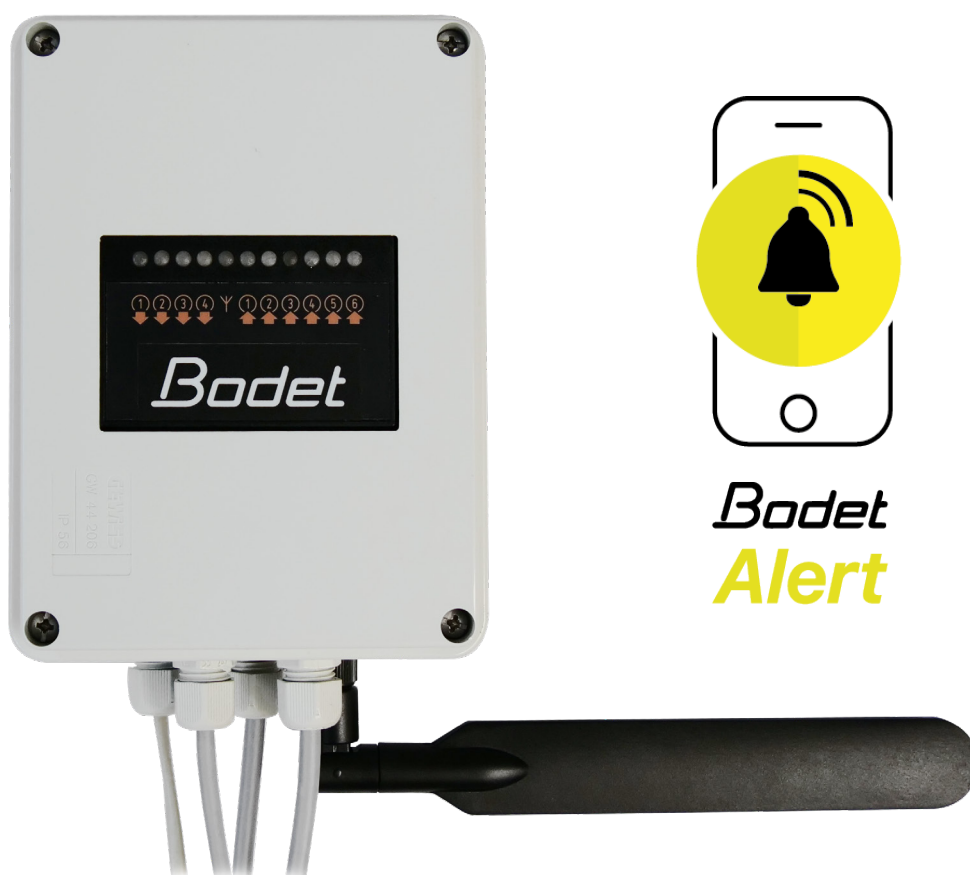


Alert interface box
Bodet Alert safety solution

EN



BODET TIME & SPORT

1 rue du Général de Gaulle

49340 Trémentines | FRANCE

Technical support - EXPORT: +33 2 41 71 72 33



Ref. 608915

Rev. A

On receipt, make sure that the product has not been damaged during transport so that you can make a reservation with the carrier.

TABLE OF CONTENTS

1. GENERAL SAFETY INFORMATION	3
1.1. Symbols used.....	3
1.2. Installing the product	3
1.3. Product troubleshooting.....	4
2. GENERAL INFORMATION	5
2.1. Presentation of the solution	5
2.2. Operating diagram	6
2.3. Unpacking and cleaning the product.....	7
2.4. Prerequisites.....	7
3. INSTALLATION	8
3.1. Product and interface presentation.....	8
3.2. Manipulation(s) to be carried out prior to installation	9
3.3. Mounting and connection(s)	9
4. COMPUTER CONFIGURATION	13
4.1. Sigma software.....	13
4.2. WaryMe administration portal.....	16
5. ADVANCED CONFIGURATION AND EVENT REPORT - PC	22
5.1. Dashboard	22
5.2. Users	22
5.3. Configuration.....	23
5.4. History	27
6. USE - SMARTPHONE	28
6.1. First connection.....	28
6.2. Triggering of an individual alert (SOS)	30
6.3. Activation of a security plan	31
6.4. Reporting an incident	32
7. TECHNICAL FEATURES	33
8. SELF-TROUBLESHOOTING	34

1. GENERAL SAFETY INFORMATION

Please read the safety instructions carefully before installing the product.

Observe the safety tips at all times while installing, using and maintaining the product.

1.1. Symbols used

The following icons are used to indicate risks or sources of danger when installing, using and maintaining this product.

Symbol		Description
	IEC60417 - 1641 Operating instructions	indicates advice, a recommendation or other practical information.
	IEC60417 - 0434b Caution	indicates that special attention needs to be paid.
	IEC60417 - 5031 Direct current	indicates that the product is suitable for direct current.
	IEC60417 - 6414 Separate collection of Waste Electrical and Electronic Equipment (WEEE)	indicates a specific process to be observed for managing waste from electronic equipment.

1.2. Installing the product



Installation and maintenance of this product must be carried out by qualified personnel.

There are some precautions to be taken as for the power supply (12-24V $\overline{=}$) of the transmitter module present in the alert interface box.



The power supply must not be shared with other devices.
The distance between the Sigma master clock (supplying power) and the alert interface box should preferably be less than 3 metres.

Please make sure to choose an appropriate installation location for the equipment.



In order to ensure optimum operation of the alert interface box, please choose an installation location for the GSM/4G reception antenna where there are no major obstacles to reception from the outside (reinforced concrete walls, metal screens, sheet metal shelves,...).
No device with a strong electromagnetic field (radio equipment, electric motors,...) should be located near the antenna connected to the alert interface box.
The antenna is located under the box.



This product has been designed for domestic and industrial use and should be installed indoors, fixed to a wall in a safe and stable location (no vibrations, impacts, humidity, wide variations in temperature). Access should be restricted to authorised personnel.
This product is not waterproof and is not suitable for outdoor use.

1.3. Product troubleshooting

In case of problems when installing or using the product, we recommend that you read chapters **2.4 Prerequisites** and **8. Self-troubleshooting** of this manual before reaching out to BODET technical support.

Some transmitter modules include a Li-Poly battery as backup in the event of a power cut. The battery life is estimated at between 2 and 3 years.



When replacing the battery, please make sure to always use the right type of battery to power the product.

Dispose of used batteries according to the regulations and laws in force in your country.

There are no user-serviceable components in this product.

If necessary, please contact BODET technical support if the product needs troubleshooting.

2. GENERAL INFORMATION

Thank you for choosing a Bodet product.

This product has been carefully designed for your satisfaction according to the rules of our ISO9001 and ISO14001 quality system.

We recommend that you read this manual carefully before installing the product.

Retain this manual throughout the lifespan of your product so that you can refer to it when necessary.

Failure to follow these instructions may cause irreversible damage and invalidate the warranty. In that case, BODET cannot be held liable.

Non-contractual data. BODET reserves the right to make some functional, technical or aesthetic changes to devices without prior notice.

This manual is subject to change without notice. To obtain the latest version of this documentation, please refer to our website: www.bodet-time.com.

2.1. Presentation of the solution

Bodet Alert is a comprehensive safety solution which allows for control and management of safety alerts on the Harmonys IP ecosystem from a smartphone app (WaryMe).

Information on the triggering and stopping of alerts is transmitted via text message between the WaryMe-Bodet Cloud and the Harmonys IP ecosystem through the use of an alert interface box connected to the Sigma master clock.



Bodet Alert is a safety solution app offered as an annual licence to be renewed to ensure continuity of service.



This device cannot be the only means of triggering a safety alert.
A wired control solution shall be imperatively implemented on site.

The Bodet Alert solution can be used to:

- trigger 3 types of alerts (we recommend the following 3 alerts: Intrusion, Lockdown, Evacuation) on the Harmonys IP ecosystem or to stop the current alert,
- be informed when an alert has been triggered,
- to follow the stages of a security plan in case of threats,
- to mobilise, communicate with employees and send mass messages,
- keep a precise history of crisis situations based on reports generated automatically at the end of the event.

The app is configured via a PC interface (Cloud) which allows for:

- management of different profile types,
- management of security plans and alert rules,
- management of groups for mass messaging,
- use of statistics and history reports.

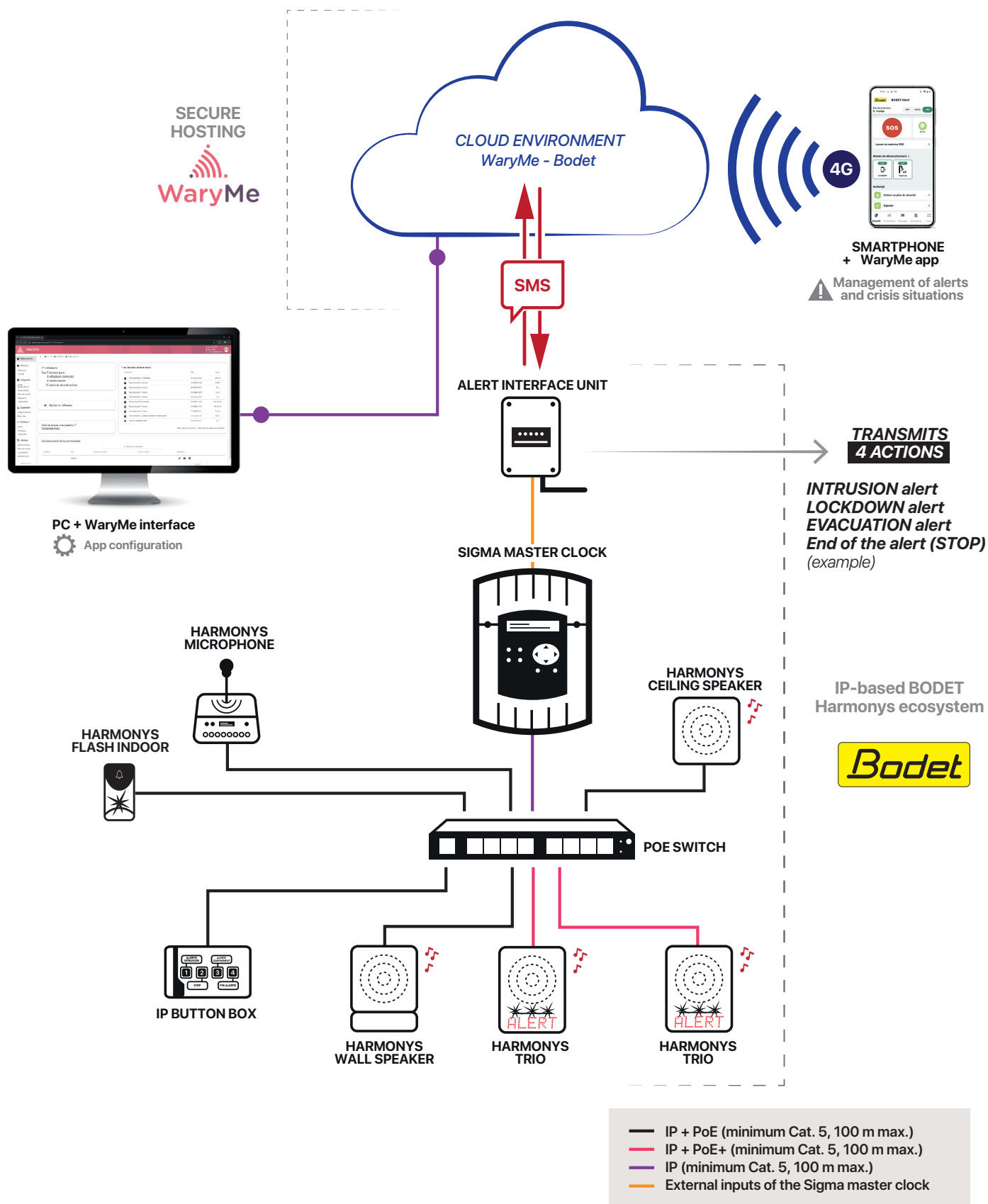
The Bodet Alert app works with an operating licence available in 2 versions: Crisis management or Crisis management + individual alert ("SOS" button from the smartphone app).



Depending on your licence type, the SOS individual alert feature may not be available.

2.2. Operating diagram

This diagram summarises the global solution with the equipment used:



2.3. Unpacking and cleaning the product

Carefully unpack the product and check the content of the package. This must include:

- A pre-wired alert interface box,
- A GSM/4G antenna,
- The installation and operation manual.

Use an antistatic product to clean the product.



Never use alcohol, acetone or other solvents which may damage the products.

2.4. Prerequisites

2.4.1. SIM card and network coverage

Text message communication via the mobile network requires a SIM card to be installed inside the alert interface box. We recommend a SIM card with a package that includes at least unlimited text messages. We recommend the French operator "Orange". It is necessary that you carry out a network compatibility and coverage test before commissioning.



SIM card not supplied with the alert interface box, at your expense.

Micro SIM 3FF format required.

Package with 12-digit SIM M2M card required. (International format).

2.4.2. Hardware installation

The commissioning of the Bodet Alert solution requires an updated Harmonys IP ecosystem.

To ensure installation compatibility, please make sure to have the following minimum versions on the BODET devices installed on all sites to be supervised:

Equipment	Version
Sigma Master Clock	V1.1
Harmonys	V1.1B06
Harmonys Trio	V1.1A16
Harmonys Flash	V1.1B08
Harmonys button box	V1.1A05
Harmonys Line Rack	V1.1B06

Please reach out to our customer support to update your equipment, by e-mail at the following address: export@bodet-timesport.com.



In order to check equipment compatibility and the version of the SIGMA software to be installed with our customer support, please have the master clock software version ready.

2.4.3. Button box configuration

Some rules must be observed when configuring button boxes to ensure proper operation.



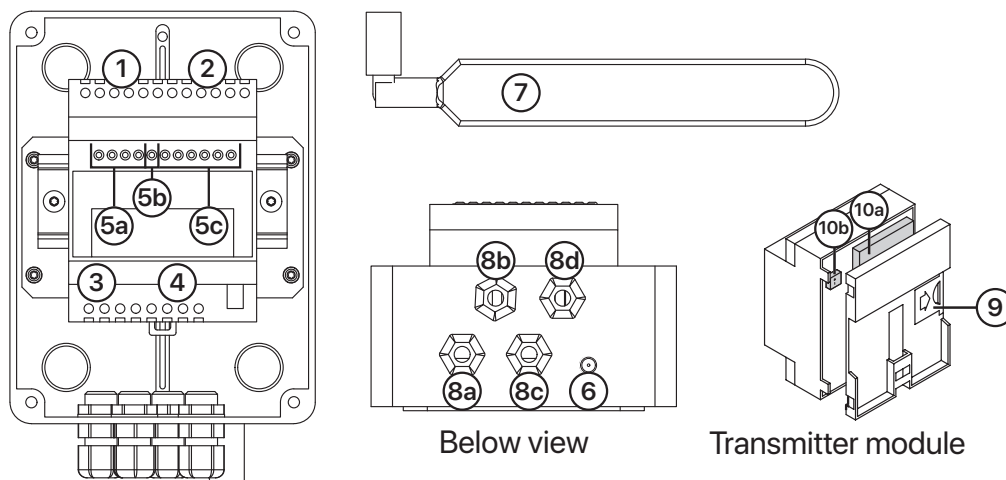
The configuration of button boxes connected to the Sigma master clock installed in each site must be the same as the one that will be entered in the WaryMe app (alert triggering scenarios on equipment). The configuration of the STOP button must correspond to the "OFF global" function in the Sigma configuration.

3. INSTALLATION

3.1. Product and interface presentation

The alert interface box includes a transmitter module connected to a GSM/4G antenna.

fig. 1



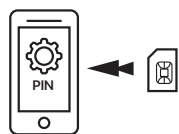
Id.	Designation	Description												
1	Analogue inputs	Not used.												
2	Digital inputs	Connection to the dry contacts of the master clock to send alert triggering information from Sigma to the Cloud.												
3	12-24V $\equiv$ power supply	12V $\equiv$ power supply from the Sigma master clock.												
4	Relay outputs	Connection to the external inputs of the Sigma master clock for triggering/stopping the alerts sent by the Cloud.												
<table> <tr> <th></th><th>Colour</th><th>Status</th></tr> <tr> <td>5a: Status LEDs of relay outputs</td><td>Green</td><td>Switches on (5s) when an output is activated.</td></tr> <tr> <td>5b: GSM status LED"ψ"</td><td>Blue</td><td>Flashing (2s): APN not configured. Flashing (2s) + 3 flashes: Wrong APN. Flashing (5s): connected to the 4G network.</td></tr> <tr> <td>5c: Input status LEDs</td><td>Orange</td><td>Switches on (5s) when an input is activated.</td></tr> </table>				Colour	Status	5a: Status LEDs of relay outputs	Green	Switches on (5s) when an output is activated.	5b: GSM status LED"ψ"	Blue	Flashing (2s): APN not configured. Flashing (2s) + 3 flashes: Wrong APN. Flashing (5s): connected to the 4G network.	5c: Input status LEDs	Orange	Switches on (5s) when an input is activated.
	Colour	Status												
5a: Status LEDs of relay outputs	Green	Switches on (5s) when an output is activated.												
5b: GSM status LED"ψ"	Blue	Flashing (2s): APN not configured. Flashing (2s) + 3 flashes: Wrong APN. Flashing (5s): connected to the 4G network.												
5c: Input status LEDs	Orange	Switches on (5s) when an input is activated.												
6	Remote connector for the GSM/4G antenna	SMA female connector.												
7	GSM/4G antenna	Connected to the interface box.												
8	8a: PG7 cable gland	1-pair cable routing (to master clock power supply).												
	8b: PG7 cable gland	1-pair cable routing (to master clock external input).												
	8c: PG7 cable gland	3-pair cable routing (to the 3 option card external inputs).												
	8d: PG7 cable gland	3-pair cable routing (to the 3 dry contacts of the master clock).												
9	SIM card slot	Micro SIM 3FF format.												
10	10a: Li-Polybattery 10b: Battery connector	The battery autonomy varies from 15 minutes to 6 hours depending on the charge level and operating conditions.												

3.2. Manipulation(s) to be carried out prior to installation



Before proceeding with the installation and commissioning of the alert interface box on site, it is mandatory to follow these steps.

fig. 2



- 1** Insert the SIM card for the alert interface box into a smartphone.
- 2** Access the settings of the SIM card from the smartphone and deactivate the PIN code.

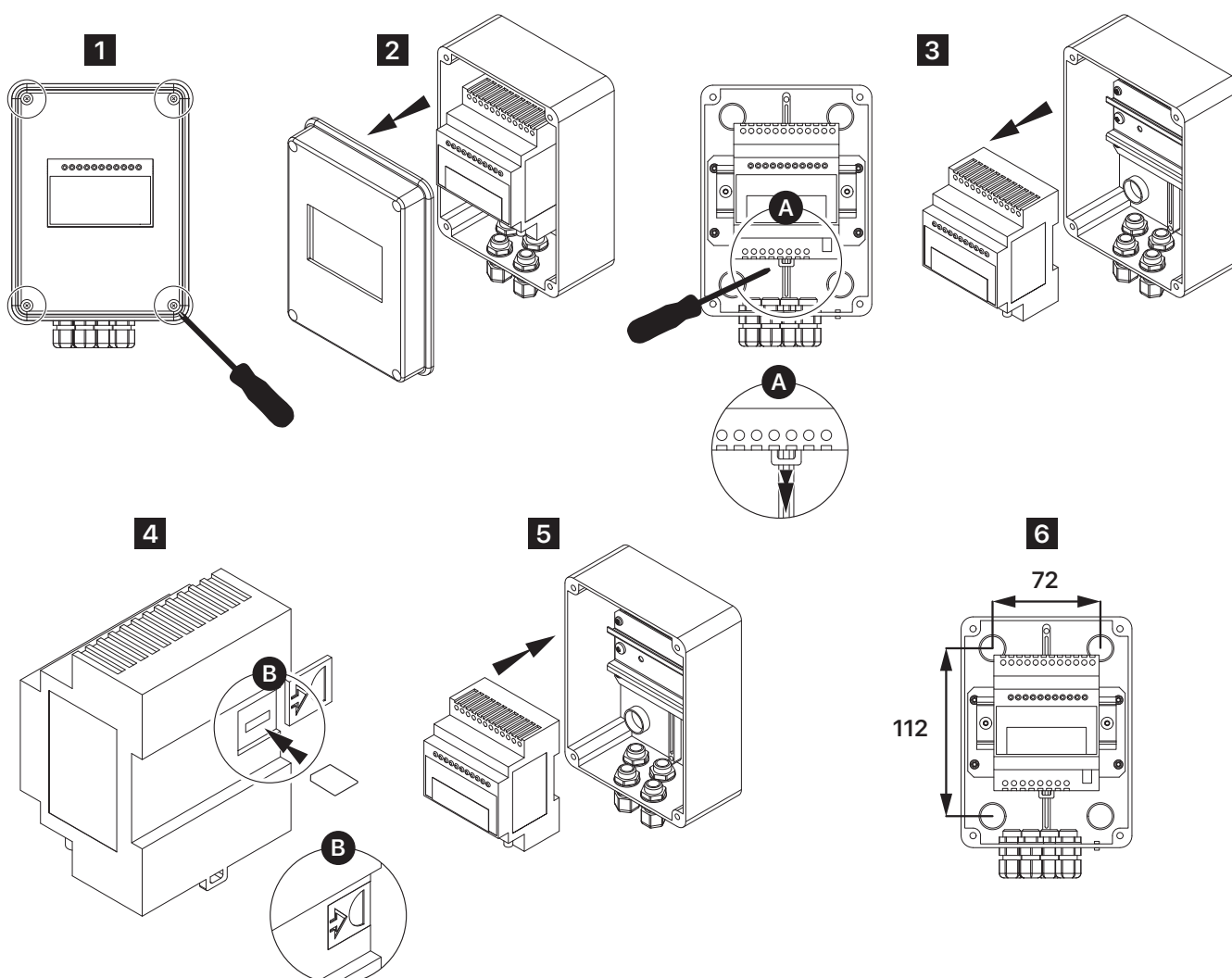
3.3. Mounting and connection(s)



Place the alert interface box near the Sigma master clock, by observing installation recommendations specified in chapter 1.2 *Installing the product*.

Proceed with the commissioning of the product by following the steps below:

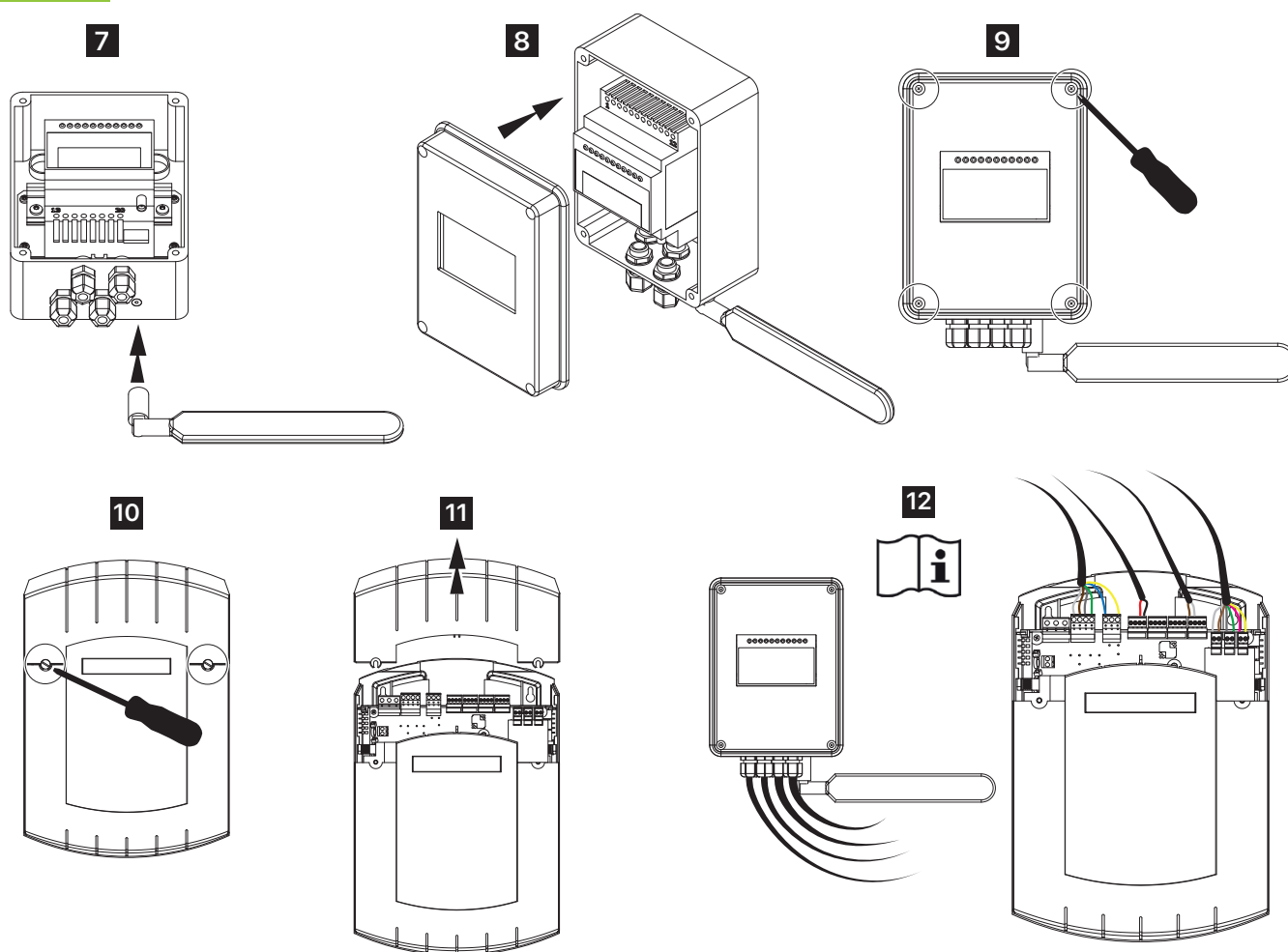
fig. 3



- 1** Open the alert interface unit by unscrewing the 4 locking screws with a cross-headed screwdriver.
- 2** Remove the cover of the alert interface box to insert the SIM card inside the transmitter module before mounting the box.
- 3** Remove the transmitter module from the DIN rail. To carry out this operation, use a flat screwdriver to move the notch on the underside of the module downwards. See fig.3 - zoom A.

- 4** Insert the Micro SIM 3FF card inside the module (SIM slot situated on the rear panel).
A small plastic protection needs to be removed and replaced after insertion. See fig. 3 - zoom B.
The SIM card is to be installed with the chip facing downwards and the diagonal edge towards the transmitter module.
The PIN code of the SIM card must be previously deactivated.
It is mandatory to carry out this manipulation using a smartphone before inserting the SIM card into the transmitter module.
- 5** Replace the transmitter module on the DIN rail using the notch located under the module with a flat screwdriver. See fig.3 - zoom A.
- 6** Fix the alert interface box to the wall using 4 fixing screws, at less than 1.5m from the Sigma master clock (cable length).

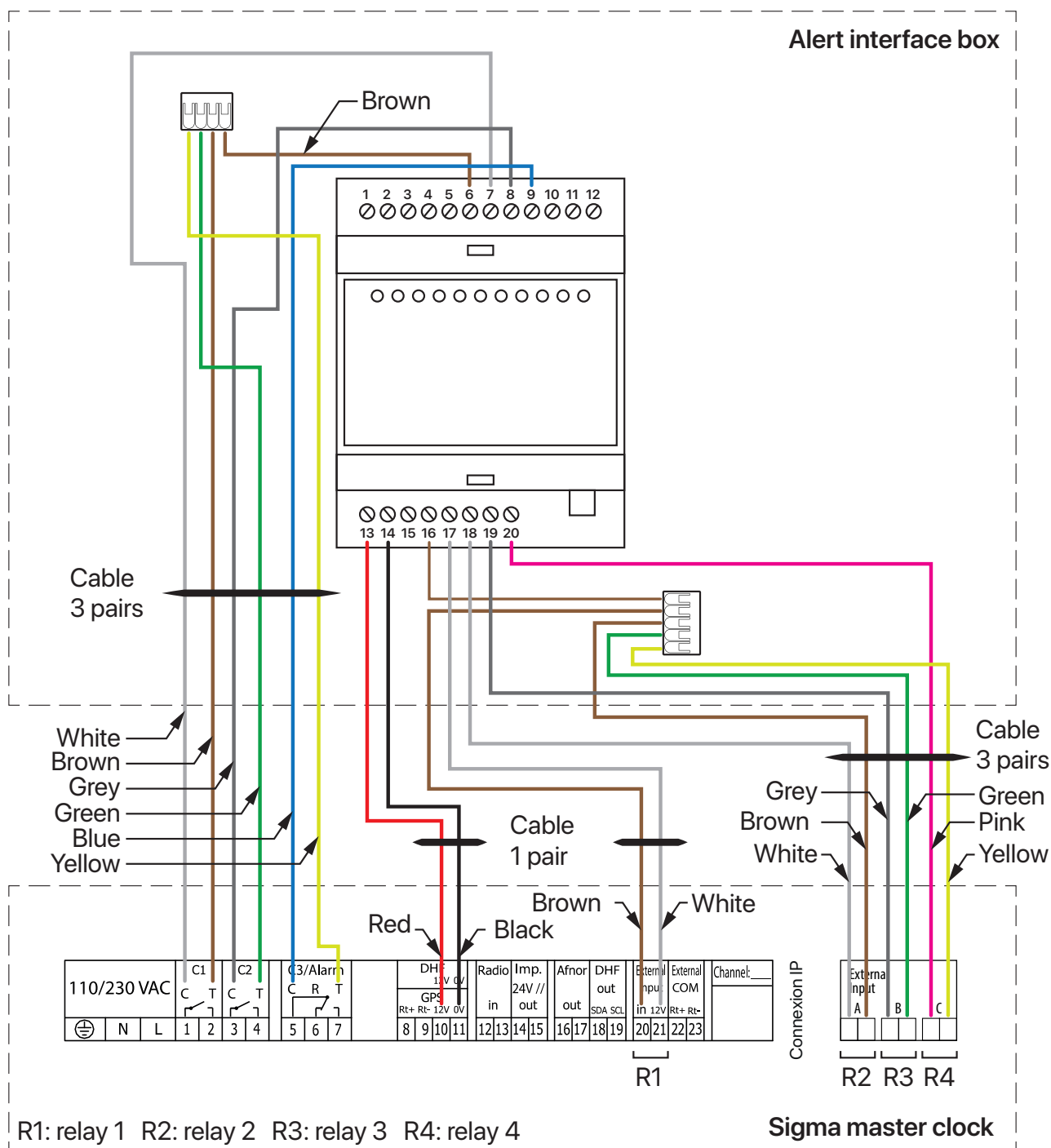
fig. 4



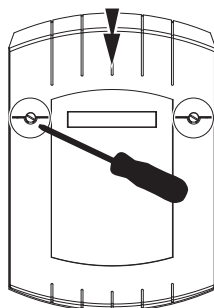
- 7** Screw the GSM/4G antenna to the alert interface box via the SMA female connector located under the box. Preferably orient the antenna horizontally when fixed.
- 8** Replace the alert interface box cover.
- 9** Retighten the cover of the alert interface box using a cross-headed screwdriver.
- 10** Unscrew the top cover of the Sigma master clock using a flat screwdriver.
- 11** Remove the top cover of the Sigma master clock to access connections.
- 12** Proceed with the cabling between the alert interface box and the Sigma master clock by reading the user manual carefully.

fig. 5

13



14



13 Proceed with the cabling. See figure 5.**Observe the cabling described to ensure proper operation.**

All connections have already been made inside the alert interface box.

The wires are already connected to the terminal blocks. You just have to connect them to the master clock.

1-pair cable: connected to the 12V power supply of the master clock.

Red wire: terminal 10 (GPS - 12V).

Black wire: terminal 11 (GPS - 0V).

1-pair cable: external input of the master clock.

Brown wire: terminal 20 (External input - in).

White wire: terminal 21 (External input - 12V).

3-pair cable: external inputs of the 3-input option card.

White wire: external input A (left).

Brown wire: external input A (right).

Grey wire: external input B (left)

Green wire: external input B (right).

Pink wire: external input C (left).

Yellow wire: external input C (right).

3-pair cable: connected to the dry contacts of the master clock.

White wire: terminal 1 (C1 - Common).

Brown wire: terminal 2 (C1 - Work).

Grey wire: terminal 3 (C2 - Common).

Green wire: terminal 4 (C2 - Work).

Blue wire: terminal 5 (C3/Alarm - Common)

Yellow wire: terminal 7 (C3/Alarm - Work).

Please refer to the next chapter and the user manual of the Sigma master clock for configuring the 3-input option card as well as the relay contacts of the Sigma master clock.

Example of standard lockdown configuration:

Input 20/21 - Relay 1 - Button 1 - Intrusion Alert

External input A - Relay 2 - Button 2 - Lockdown Alert

External input B - Relay 3 - Button 3 - Evacuation Alert

External input C - Relay 4 - Button 4 - STOP

Depending on the configuration on site, it is possible:

-to send 4 actions from the Cloud to the Sigma master clock,

-to send 6 actions from the Sigma master clock to the Cloud (with a 3-relay option card).

14 Replace and retighten the top cover of the Sigma master clock using a flat screwdriver.

In the case of a Sigma master clock in rack format, all connections are directly made on the product rear panel.

4.COMPUTER CONFIGURATION

4.1. Sigma software

To ensure proper interfacing between the alert interface box and the Sigma master clock and ensure consistent configuration, follow the steps below from the configuration PC on site, with the Sigma software installed.



Please refer to the Sigma software user manual for more details on the menus.

The configuration below describes a standard lockdown configuration:

Input 20/21 - Relay 1 - Button 1 - Intrusion Alert

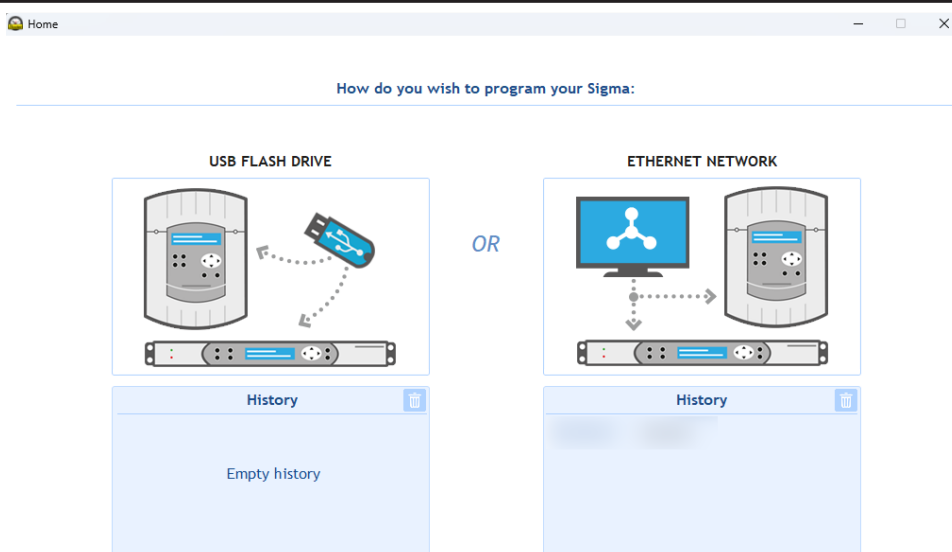
External input A - Relay 2 - Button 2 - Lockdown Alert

External input B - Relay 3 - Button 3 - Evacuation Alert

External input C - Relay 4 - Button 4 - STOP

Launching the SIGMA software

- 1 Launch the Sigma software from the configuration PC and select the Sigma master clock available on site.

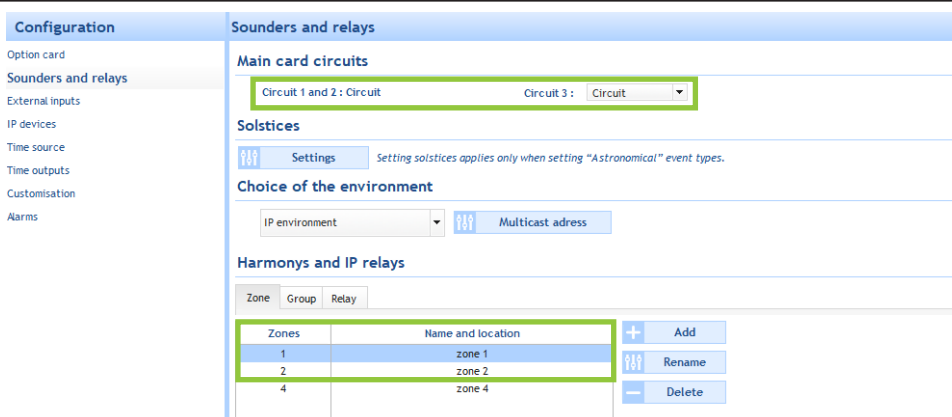


Relay and zone configuration

- 2 Access the "Configuration" menu, then the "Sounders and relays" tab.

Configure relays 1, 2 and 3 in "circuit" mode.

Add zones if required.



Button box configuration

- 3** Access the "Use" menu, then the "Button box" tab, and click on "Configuration A".

Then, successively select each button (1/2/3/4) by selecting the following settings:

Button 1:

- Mode: ON.
- Select the zones and circuit 01.
- Alert mode: activated.
- Duration: 5s.

Button 2:

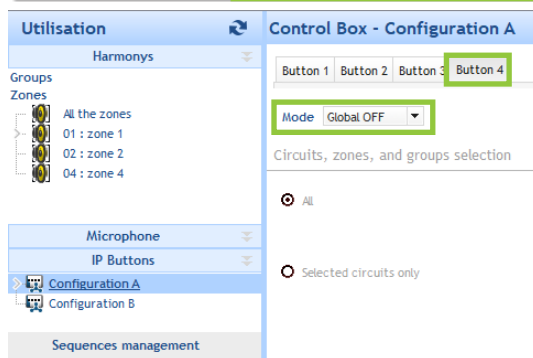
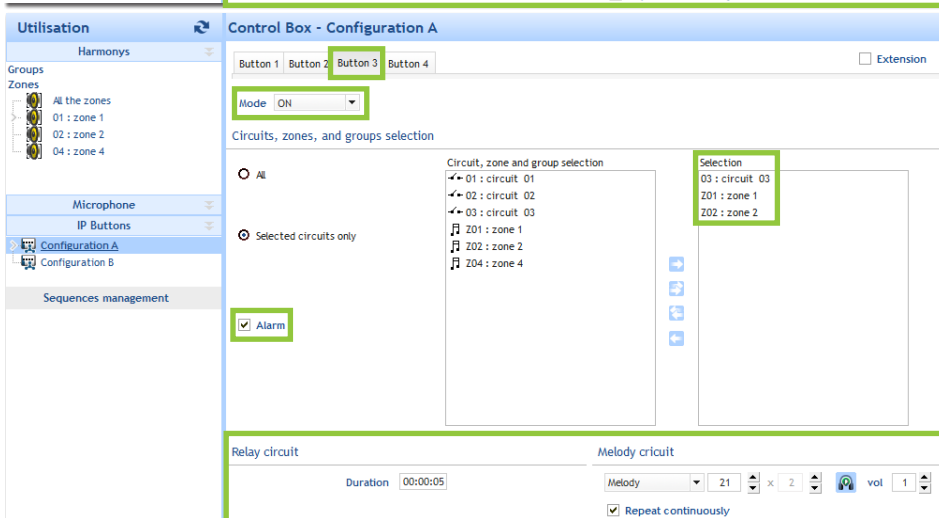
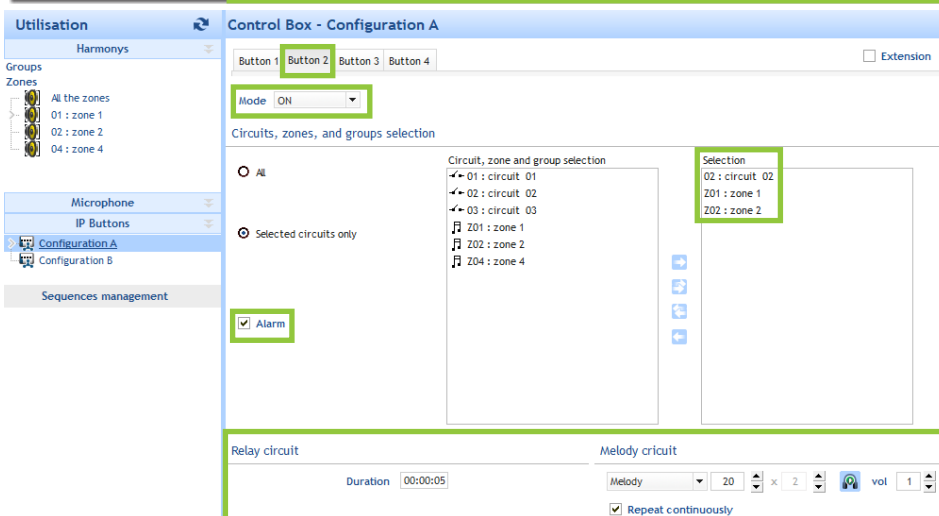
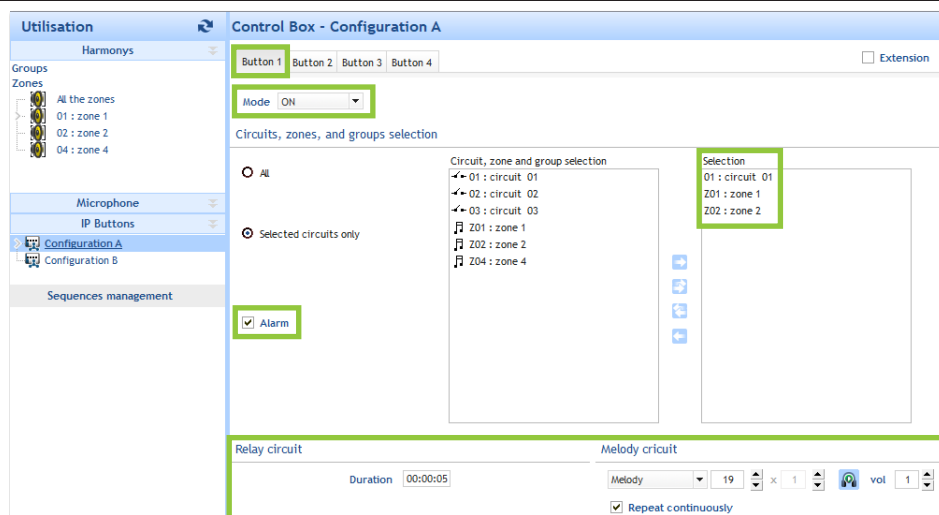
- Mode: ON.
- Select the zones and circuit 02.
- Alert mode: activated.
- Duration: 5s.

Button 3:

- Mode: ON.
- Select the zones and circuit 03.
- Alert mode: activated.
- Duration: 5s.

Button 4:

- Mode: OFF Global.



Configuration of external inputs

- 4 Access the "Configuration" menu, then click on the "External inputs" tab.

Activate each external input and imperatively use the same settings as for the button boxes:

- Mode,
- Alert mode,
- Select the zones and circuits,
- Melodies (No.,...).

Configuration

Option card

Sounders and relays

External inputs

IP devices

Time source

Time outputs

Customisation

Alarms

External input

Sigma Option card No.04 Option card No.06

Mode : ON

Circuits, zones, and groups selection

☐ All

☒ Selected circuits only

☒ Alarm

Relay Circuit

Duration : 00:00:05

Melody

Melody 19 x 3 vol 1

☒ Repeat continuously

Selection

01 : circuit 01
Z01 : zone 1
Z02 : zone 2

Configuration

Option card

Sounders and relays

External inputs

IP devices

Time source

Time outputs

Customisation

Alarms

External inputs

Sigma Option card No.04 Option card No.06

Input A Input B Input C

Mode : ON

Circuits, zones, and groups selection

☐ All

☒ Selected circuits only

☒ Alarm

Relay circuit

Duration 00:00:05

Melody circuit

Melody 20 x 1 vol 1

☒ Repeat continuously

Selection

02 : circuit 02
Z01 : zone 1
Z02 : zone 2

Configuration

Option card

Sounders and relays

External inputs

IP devices

Time source

Time outputs

Customisation

Alarms

External inputs

Sigma Option card No.04 Option card No.06

Input A Input B Input C

Mode : ON

Circuits, zones, and groups selection

☐ All

☒ Selected circuits only

☒ Alarm

Relay circuit

Duration 00:00:05

Melody circuit

Melody 21 x 1 vol 1

☒ Repeat continuously

Selection

03 : circuit 03
Z01 : zone 1
Z02 : zone 2

Configuration

Option card

Sounders and relays

External inputs

IP devices

Time source

Time outputs

Customisation

Alarms

External inputs

Sigma Option card No.04 Option card No.06

Input A Input B Input C

Mode : Global OFF

Circuits, zones, and groups selection

☐ All

☒ Selected circuits only

Relay circuit

Duration 00:00:05

Melody circuit

Deactivation of manually programmed relay circuits

Manually programmed melodies are stopped

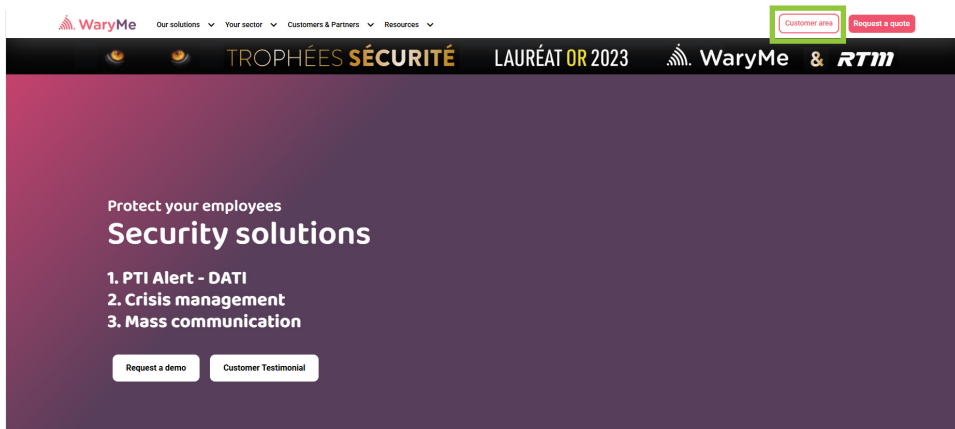
Selection

4.2. WaryMe administration portal

To configure the alert interface box, please follow the steps below from a PC by connecting to the WaryMe administration portal.

Connection to the WaryMe administration portal

- 1 Access the WaryMe portal from the "www.waryme.com" website, and click on the "Customer area" tab.

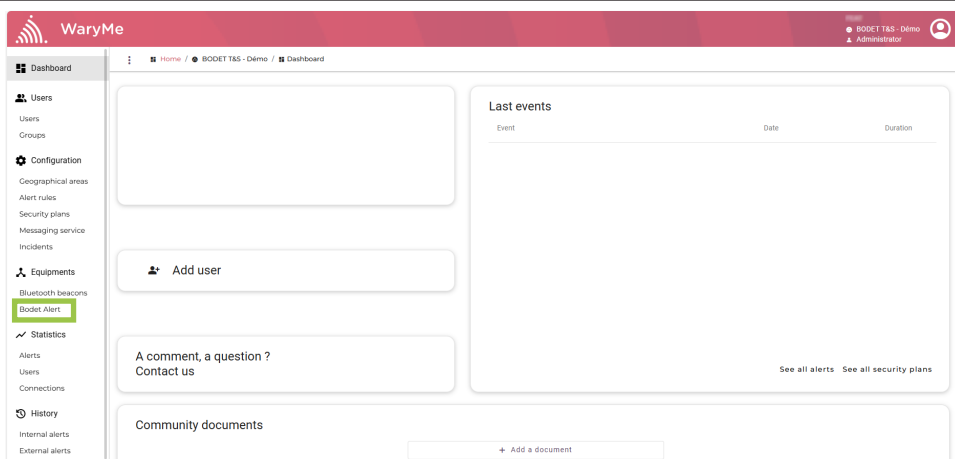


- 2 Connect to the administration portal by using the credentials of the organisation's administrator account to be able to modify the configuration.

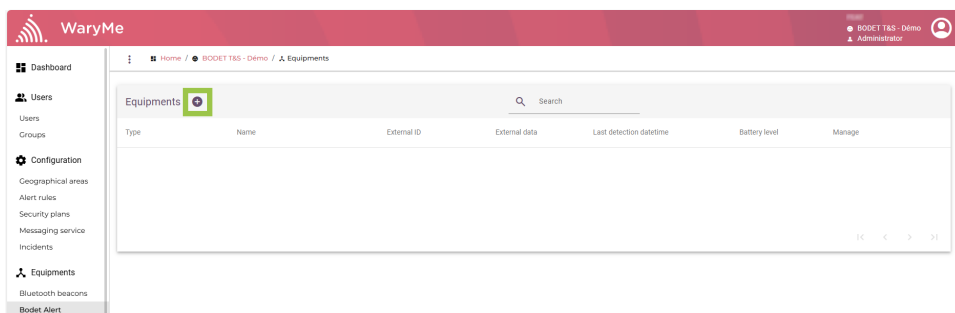


Adding the alert interface box as external equipment

- 3 In the side menu, click on the "Bodet Alert" tab to add and configure the alert interface box as external equipment.



- 4 Click on + to add the alert interface box as new equipment. This opens the "Add a device" window.



- 5** Select the type of equipment:
- Type:
Bodet Alert interface.

Fill in the fields:

- Name:
Bodet Alert interface.
- External ID: telephone number associated with the SIM card inserted into the transmitter module of the alert interface box.

Click on "Create".

Adding alert feedback actions (Sigma to Cloud)

- 6** Once the equipment has been added, click on it to select it. This opens the "Update a device" window.

- 7** Click on the "Actions" tab. This tab enables to configure actions (alert triggering) from the Sigma master clock to the Cloud.

Click on **+** to add an action. This opens the "Configure action" window.

8 Configure the first "Intrusion" alert feedback action by selecting:

- Source event:
Alert 1.
- Action type:
Activate a security plan.
- Security rule:
Intrusion.

Click on "Create".

Configure action

Source event*

Alert 1

Action type*

Activate a security plan

Security rule*

Intruder

Cancel

Create

9 Repeat the previous step twice for the 2 other actions aiming at sending the "Lockdown" and "Evacuation" alert feedbacks from the Sigma master clock to the Cloud. Follow the settings below:

Lockdown

- Source event:
Alert 2.
- Action type:
Activate a security plan.
- Security rule:
Lockdown.

Evacuation

- Source event:
Alert 3.
- Action type:
Activate a security plan.
- Security rule:
Evacuation.

Click on "Close" once the configuration is completed.

Update a device

Informations

Actions

Actions +

Search

Source event	Action type	Security rule	Manage
Alert 1	Activate a security plan	Intruder	
Alert 2	Activate a security plan	Lockdown	
Alert 3	Activate a security plan	Evacuation	

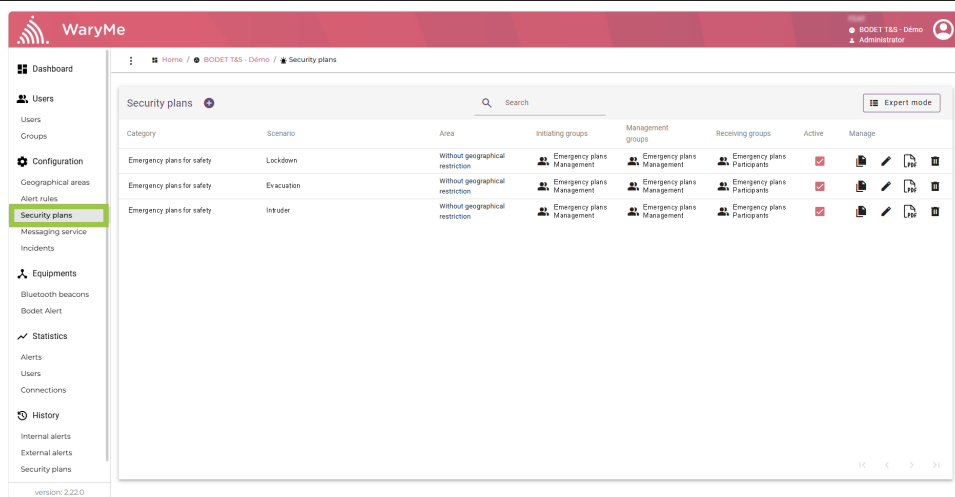
1 - 3 of 3

Close

Adding alert triggering/stopping actions (Cloud to Sigma)

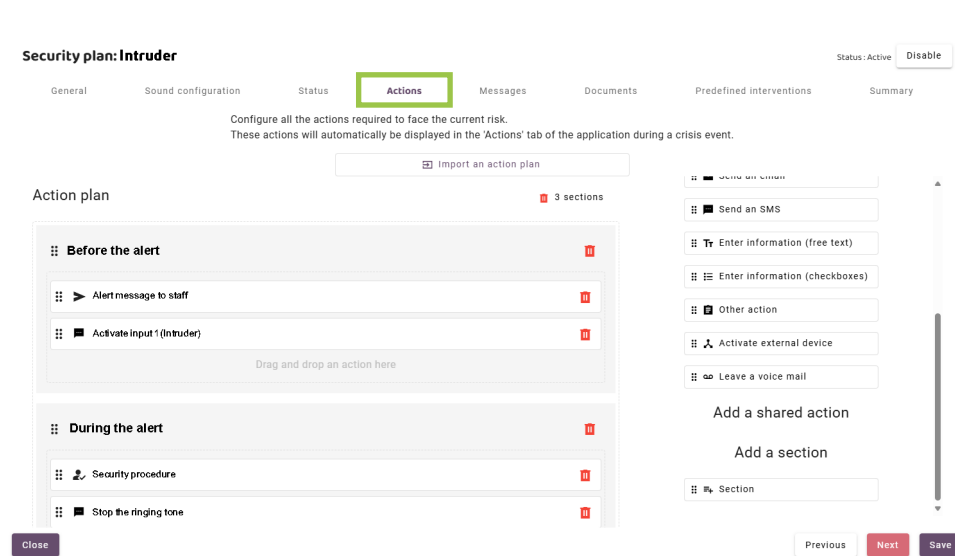
- 10** From the side menu, click on the "Security plans" menu to add alert triggering and stopping actions from the Cloud to the Sigma master clock.

There is a pre-configured standard security plan for each "Intrusion", "Lockdown" and "Evacuation" alerts. These plans can be customised.



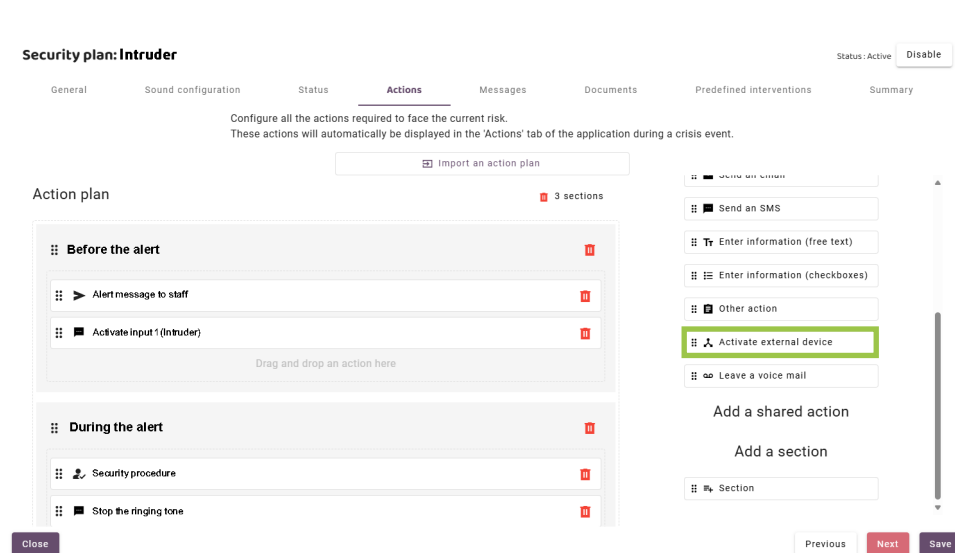
- 11** Select the "Intrusion" security plan. The "Intrusion security plan" window opens.

Click on the "Actions" tab. This tab enables to add alert triggering and stopping actions from the security plan (Cloud) to the Sigma master clock.



- 12** Add actions to send to the Sigma master clock via the alert interface box by dragging and dropping the "Activate external device" action from the list "Add a shared action" to a block in the security plan.

This opens the "Add an action type: Activate external device" window.



- 13** Configure the action to be sent to the Sigma master clock.

In each security plan (Intrusion, Lockdown, Evacuation) it is possible to add an action at the beginning of the event to trigger the alert to the Sigma master clock and a second one at the end of the event to stop the alert.

For example:

For the "Intrusion" security plan, please configure the triggering action as follows:

- Title: Activating the alert on the audio system.
- Action type: Required.
- Device: Bodet Alert interface
- Action: Relay 1 (standard lockdown configuration).

Click on "Add" then on "Save".

Start again from step 12 and configure the alert stopping action at the end of the event as follows:

- Title: Stopping the alert on the audio system.
- Action type: Required.
- Device: Bodet Alert interface.
- Action: Relay 4 (standard lockdown configuration).

This screenshot shows the 'Add an action type' form for 'Activate external device'. The 'Title' field is 'Activating the alert on the audio system', marked as 'Required'. The 'Device' dropdown is set to 'Bodet Alert interface'. The 'Action' dropdown is set to 'Relay 1'. There is a checkbox for 'Automatically engage at event start'. Buttons for 'Cancel' and 'Add' are at the bottom.

This screenshot shows the 'Security plan: Intruder' configuration page. The 'Actions' tab is selected. The 'Action plan' section shows a sequence of actions: 'Before the alert' (Alert message to staff, Activating the alert on the audio system, Activate input 1 (Intruder)), 'During the alert' (Security procedure). The right sidebar lists predefined interventions like 'Send an SMS', 'Enter information (free text)', 'Enter information (checkboxes)', 'Other action', 'Activate external device', and 'Leave a voice mail'. Buttons for 'Close', 'Previous', 'Next', and 'Save' are at the bottom.

This screenshot shows the 'Add an action type' form for 'Activate external device'. The 'Title' field is 'Stopping the alert on the audio system', marked as 'Required'. The 'Device' dropdown is set to 'Bodet Alert interface'. The 'Action' dropdown is set to 'Relay 4'. There is a checkbox for 'Automatically engage at event start'. Buttons for 'Cancel' and 'Add' are at the bottom.

- 14** Repeat steps 11, 12 and 13 for the "Lockdown" and "Evacuation" security plans in order to add alert triggering and stopping actions depending on the desired scenario. Please note that the standard lockdown configuration requires the following settings:
- Triggering actions of the corresponding alert:**
- "Intrusion" security plan: Action > Relay 1
 - "Lockdown" security plan: Action > Relay 2
 - "Evacuation" security plan: Action > Relay 3
- Stopping action (whatever the type of alert: Intrusion, Lockdown,...)**
- "Intrusion", "Lockdown" security plans,... : Action > Relay 4.



These different steps enable to carry out the commissioning of the Bodet Alert solution easily. Every security plan can be customised depending on the scenarios prepared by the organisation in which the solution has been rolled out. Group management can also be customised.



A comprehensive alert launching and stopping test should be carried out from the security plans (WaryMe smartphone app) and from control solutions on site (IP button box) in order to check the proper communication between the Bodet audio ecosystem and the WaryMe app (Cloud).

5. ADVANCED CONFIGURATION AND EVENT REPORT - PC

This chapter summarises the main configuration features available from the WaryMe administration portal as well as the event report feature.



Please refer to the WaryMe technical support for the full management of all the features available from the administration portal.

5.1. Dashboard

The dashboard is the homepage of the administration portal.

WaryMe Dashboard

27 users
This last 7 days:
0 user connected
3 alerts emitted
38 security plans triggered

Last events

Event	Date	Duration
Security plan - Evacuation	05/03/2025 09:56	8s
Security plan - Intruder	05/03/2025 09:56	13s
Security plan - Intruder	05/03/2025 09:55	23s
Security plan - Intruder	03/03/2025 16:41	1m 13s
Individual alert	03/03/2025 16:39	5s
Individual alert	03/03/2025 16:39	8s
Individual alert	03/03/2025 16:39	11s
Security plan - Intruder	03/03/2025 15:20	1h 18m 30s
Security plan - Intruder	03/03/2025 15:15	2m 42s
Security plan - Intruder	03/03/2025 13:56	25s

A comment, a question ?
Contact us

Community documents

+ Add a document

version: 2.22.0

This page displays the latest user connections and events (triggering of security plans,...). It is also possible to upload documents on the portal.

5.2. Users

5.2.1. Users

The "Users" menu allows for management of all users of the Bodet Alert solution.

WaryMe Users

Users View All Members Guests

Search

Import Export Welcome message

Name	Login	Email address	Phone number	Role	Version	State	External data	Manage
Superadmin 10.0.0.100	superadmin@waryme.com	superadmin@waryme.com		Superadmin	Android Superadmin 2.22.0 (2025-03-05)	OK		
Admin 10.0.0.100	admin@waryme.com	admin@waryme.com		Administrator	Web Admin 2.22.0	OK		
User 10.0.0.100	user@waryme.com	user@waryme.com		User	Web User 2.22.0	Unknown		
Superadmin 10.0.0.100	superadmin@waryme.com	superadmin@waryme.com		Superadmin	Web Admin 2.22.0	OK		
User 10.0.0.100	user@waryme.com	user@waryme.com		User	Web User 2.22.0	Unknown		
Admin 10.0.0.100	admin@waryme.com	admin@waryme.com		Administrator	Web Admin 2.22.0	Unknown		
User 10.0.0.100	user@waryme.com	user@waryme.com		User	Web User 2.22.0	Unknown		
Superadmin 10.0.0.100	superadmin@waryme.com	superadmin@waryme.com		Superadmin	Web Admin 2.22.0	Unknown		
User 10.0.0.100	user@waryme.com	user@waryme.com		User	Web User 2.22.0	Unknown		
Admin 10.0.0.100	admin@waryme.com	admin@waryme.com		Administrator	Web Admin 2.22.0	Unknown		
User 10.0.0.100	user@waryme.com	user@waryme.com		User	Web User 2.22.0	Unknown		
Superadmin 10.0.0.100	superadmin@waryme.com	superadmin@waryme.com		Superadmin	Web Admin 2.22.0	Unknown		
User 10.0.0.100	user@waryme.com	user@waryme.com		User	Web User 2.22.0	Unknown		
Admin 10.0.0.100	admin@waryme.com	admin@waryme.com		Administrator	Web Admin 2.22.0	Unknown		
User 10.0.0.100	user@waryme.com	user@waryme.com		User	Web User 2.22.0	Unknown		

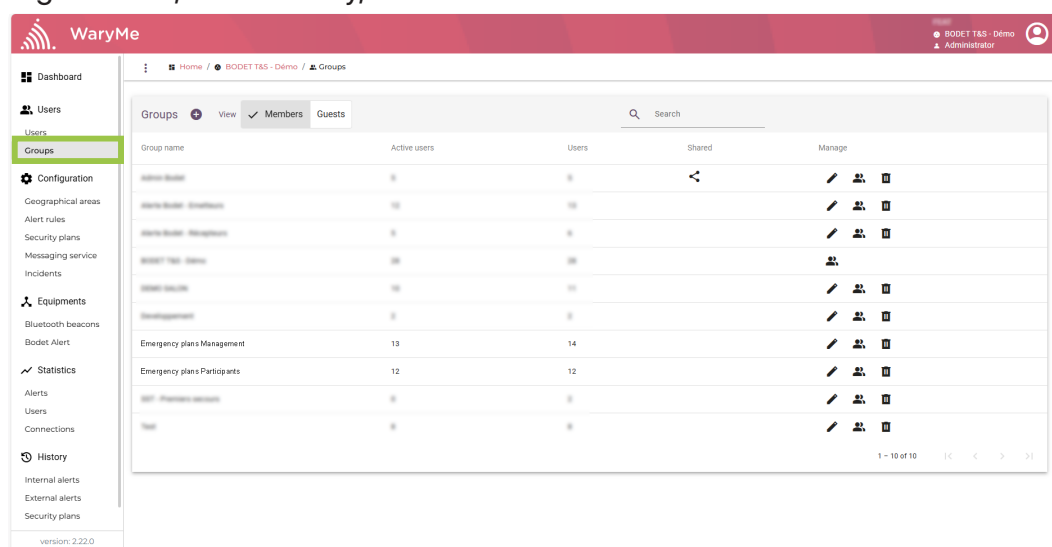
1 - 28 of 28

version: 2.22.0

This page enables to add, modify and import users. Each user can be assigned a role (administrator or user) and a group to be granted rights (triggering of security plans,...).

5.2.1. Groups

The “Groups” menu enables users to be grouped into communities depending on the structure of the organisation, the hierarchy,...



This page allows for creation and management of groups. It is possible to add users to a group from a group page.



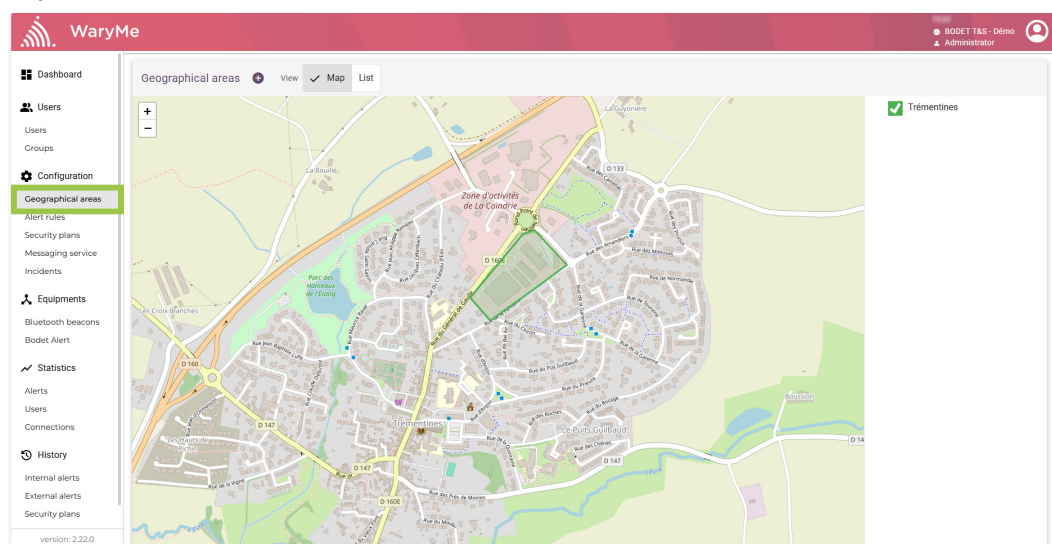
Access to these features is granted to groups and not to individual users. In the case of a lockdown alert, there are usually at least 2 groups:

- Lockdown Supervisors: triggering of alerts and sequence of security plan stages,
- Lockdown Participants: interactions via text messages in the security plans and triggering of individual protection alerts (SOS).

5.3. Configuration

5.3.1. Geographical areas

The “Geographical areas” menu allows for access restriction to some features depending on whether the user is present or not in the defined area.

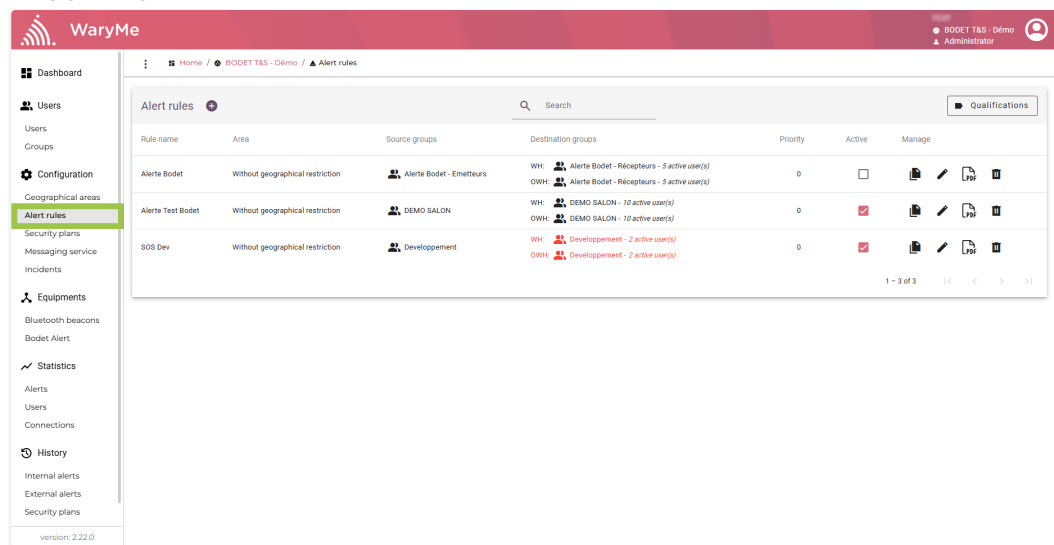


Only individual protection alerts (SOS) are concerned by the geographical restriction. The mobilisation chain and the intervention protocol can be customised for each area.

This page allows for creation of geographical areas in which the individual protection system will be effective.

5.3.1. Alert rules

The "Alert rule" menu allows for configuration of the individual alert feature (SOS). If a user has enabled an alert rule, the "SOS" button appears on the home screen of the WaryMe smartphone app. See chapter 6.2 *Triggering an individual alert (SOS)*.



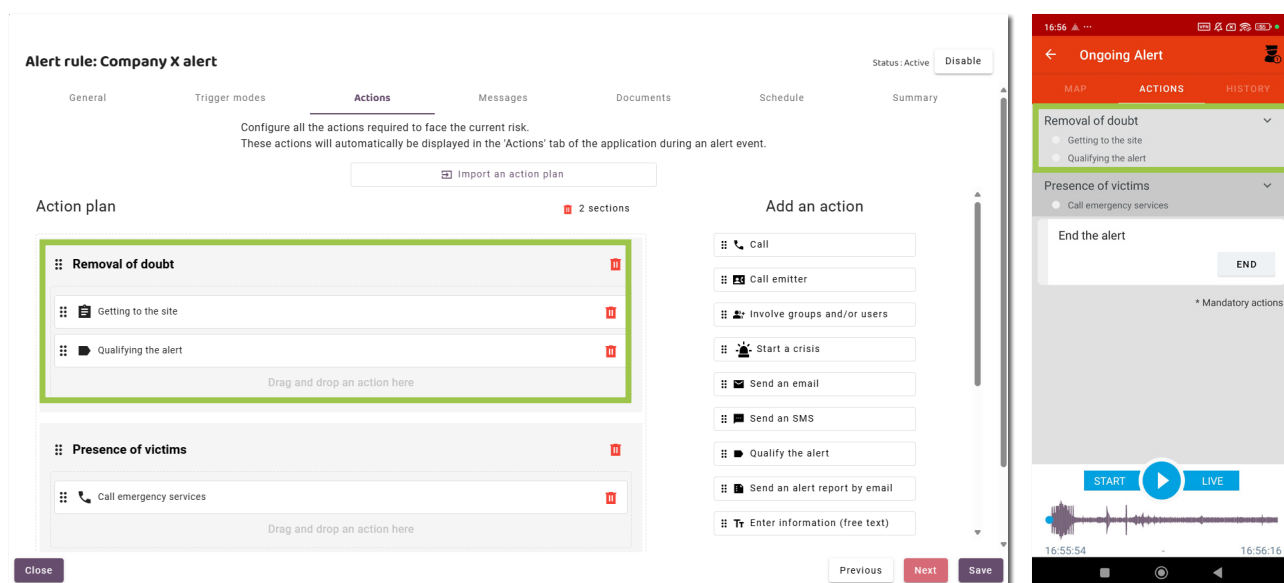
This page enables to add and modify alert rules. The alert rule defines:

- the groups authorised to trigger an individual alert,
- the triggering geographical scope,
- the groups receiving the information relating to the triggering of an individual alert.

It is also possible to define:

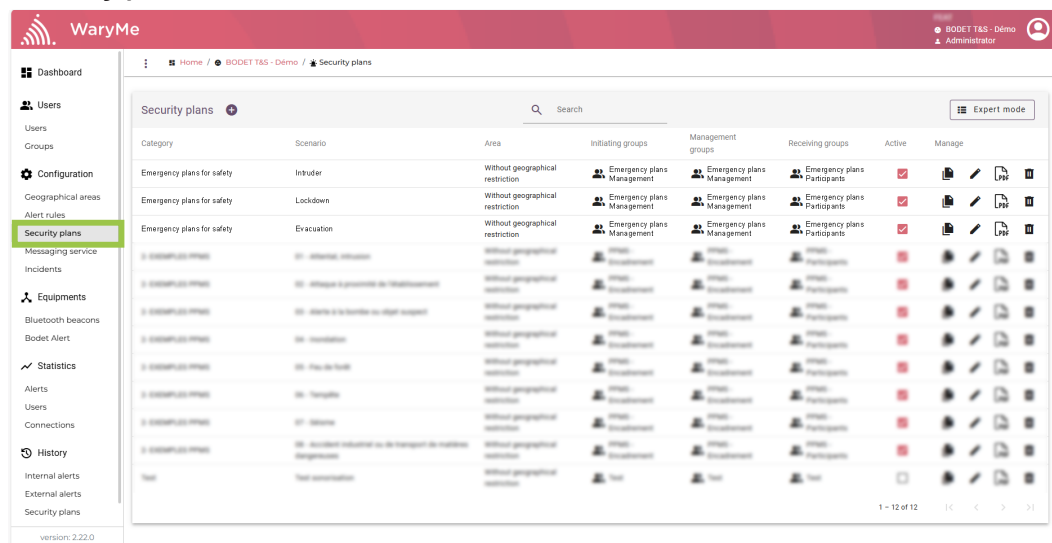
- triggering modes,
- alert qualifications (assault, accident,...),
- the action protocol to be implemented in case of triggering of an individual alert,
- predefined messages and available documents.

Action protocol example (created from the administration portal) and available from the WaryMe smartphone app when activating an individual alert (SOS):



5.3.1. Security plans

The “Security plans” menu enables to establish and prepare the action protocol to be initiated in case of major events, to facilitate management. If a user manages one or several security plans, the “Triggering a security plan” button appears on the home screen of the WaryMe smartphone app. See chapter 6.3 *Triggering a security plan*.



This page enables to add and modify security plans.

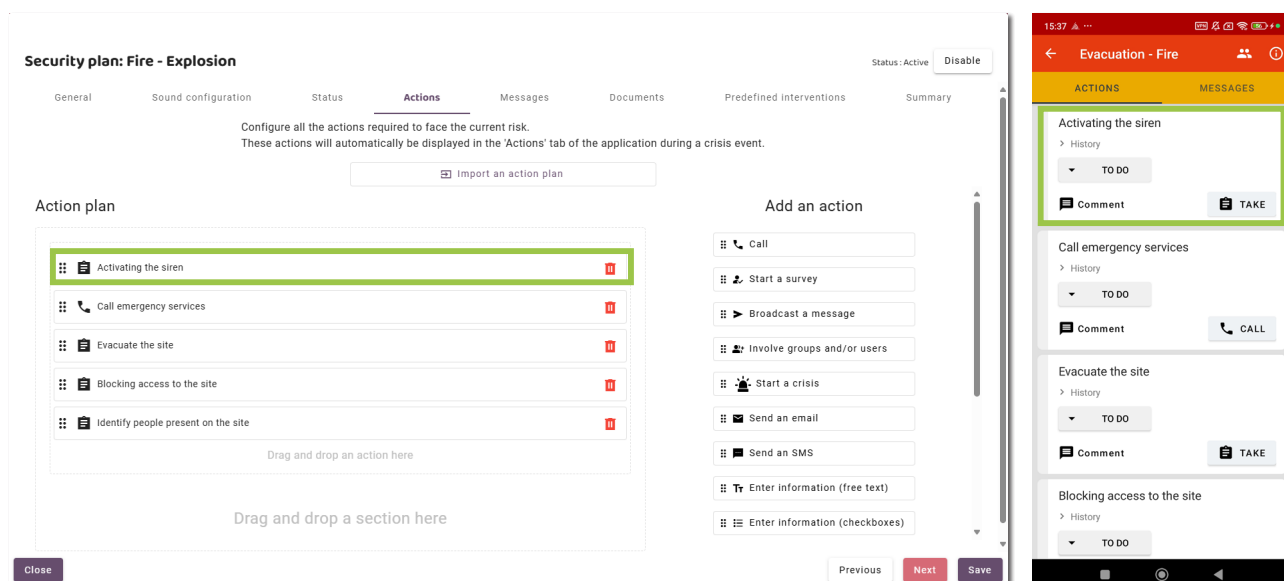
For user management, a security plan is defined by:

- groups authorised to trigger security plans,
- groups authorised to manage security plans,
- groups authorised to receive security plan information.

The main feature is the creation of the action protocol to follow, following the triggering of a security plan. Besides, it is possible to define:

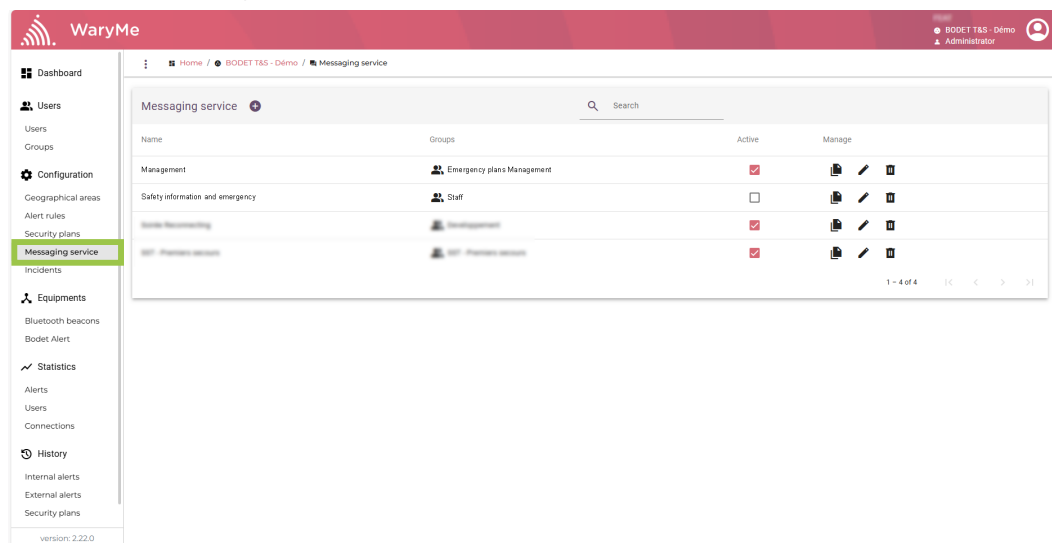
- security plan monitoring indicators,
- the way in which recipient smartphones will respond in case of an alert triggering and actions to be followed on the security plan (ringtone or on vibrate, sound volume,...),
- the messaging service and predefined messages to be broadcast while the event is being processed,
- available documents and an intervention model.

Action protocol example (created from the administration portal) and available from the WaryMe smartphone app when activating a security plan:



5.3.1. Messaging service

The “Messaging service” menu enables to configure communication threads to use apart from crisis situations. If a user is a member of one or several communication threads, the “Messages” button appears on the home screen of the WaryMe smartphone app.



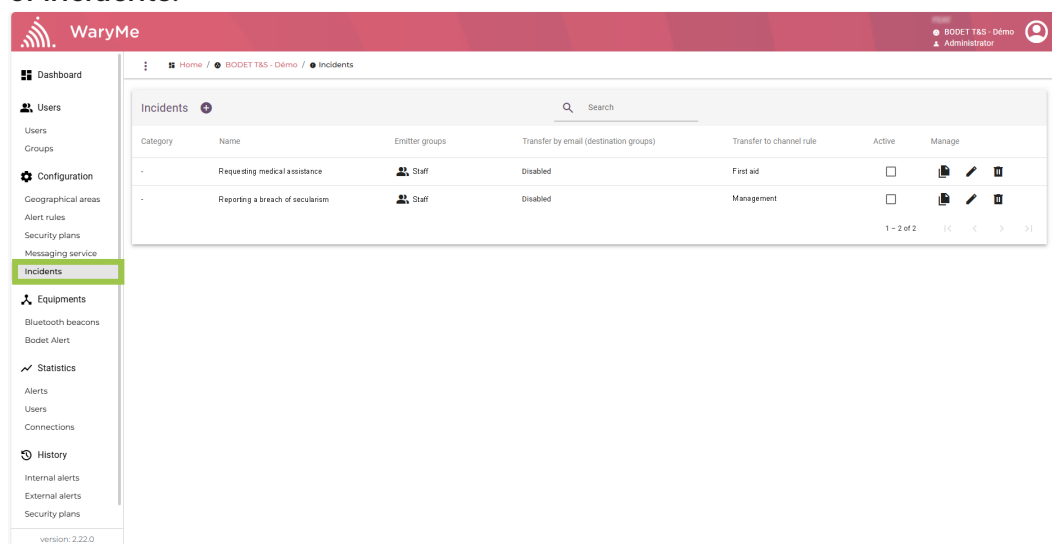
This page enables to add and modify communication threads.

For each thread, it is possible to define:

- the communication mode,
- member groups,
- predefined messages,
- available documents.

5.3.1. Incidents

The “Incidents” menu allows for configuration of forms for reporting a non-critical event (incident, breach of secularism...) that needs to be dealt with. If a user is authorised to report one or several incidents, the “Report” button will appear on the home screen of the WaryMe smartphone app. See chapter **6.4 Reporting of incidents**.



This page enables to add and modify incident types.

For each incident type, it is possible to define:

- the groups authorised to report an incident,
- the recipient groups and the notification mode (messaging service, e-mail).
- the incident qualification form,
- available documents.

5.4. History

5.4.1. Security plans

The "Security plans" menu of the "History" section enables to consult the past sequence of stages of a security plan activated as part of a drill or a real event in order to check that the actions defined in the plan at the time of the event have been carried out correctly.

Last security plan						
Date	Scenario	Type	Duration	Triggered by	Ended by	Export
05/03/2025 16:36	Intruder	Exercise	21s	WaryMe	WaryMe	PDF CSV
05/03/2025 09:56	Intruder	Real event	8s	WaryMe - Odette Boudet T&S	WaryMe - WaryMe	PDF CSV
05/03/2025 09:56	Intruder	Real event	13s	WaryMe - Odette Boudet T&S	WaryMe - WaryMe	PDF CSV
05/03/2025 09:55	Evacuation	Exercise	23s	WaryMe - WaryMe	WaryMe - WaryMe	PDF CSV
03/03/2025 16:41	Lockdown	Exercise	1m 13s	WaryMe - WaryMe	WaryMe - WaryMe	PDF CSV
03/03/2025 15:20	Intruder	Real event	1h 18m 30s	WaryMe - Odette Boudet T&S	WaryMe - WaryMe	PDF CSV
03/03/2025 15:15	Intruder	Exercise	2m 42s	WaryMe - WaryMe	WaryMe - WaryMe	PDF CSV
03/03/2025 13:56	Intruder	Exercise	25s	WaryMe - WaryMe	WaryMe - WaryMe	PDF CSV
03/03/2025 13:54	Intruder	Exercise	1m 45s	WaryMe - WaryMe	WaryMe - WaryMe	PDF CSV
03/03/2025 13:53	Intruder	Real event	12s	WaryMe - Odette Boudet T&S	WaryMe - WaryMe	PDF CSV
03/03/2025 13:53	Intruder	Real event	16s	WaryMe - Odette Boudet T&S	WaryMe - WaryMe	PDF CSV
03/03/2025 13:52	Intruder	Exercise	16s	WaryMe - WaryMe	WaryMe - WaryMe	PDF CSV
03/03/2025 10:02	Intruder	Exercise	14s	WaryMe - WaryMe	WaryMe - WaryMe	PDF CSV



It is possible to export this history report in PDF format.

Example of the history report of a security plan activated as part of a drill in PDF format:

Bodet T&S Execution report of a security plan Intruder alert Type EXERCISE Triggered by XXXXXXXXXX Ended by XXXXXXXXXX Start 03/03/2025 - 13h04 (local hour Europe/Paris) End 03/03/2025 - 13h06 (local hour Europe/Paris) ID 4122859003 Document generated by WaryMe the 06/03/2025 13:49, local hour Europe/Paris 1/3	Summary Action plan ALERT Alert message to staff Activate audio alert 13:54:47 COMMUNICATE Personal safety procedures Broadcasting a situation message Stop the audio alert 13:54:55 COMPLETE Return to normal situation Document generated by WaryMe the 06/03/2025 13:49, local hour Europe/Paris 2/3	Events description <table> <tr> <td>03/03/2025 13:54:43 XXXXXXXX</td> <td>START OF SECURITY PLAN</td> <td>Initiating group: Developpement Management group: Developpement Receiving group: Developpement</td> </tr> <tr> <td>03/03/2025 13:54:47 XXXXXXXX</td> <td>ACTION State change To do: On going</td> <td>ACTIVATE AUDIO ALERT A Activate external device Device: undefined Action: undefined</td> </tr> <tr> <td>03/03/2025 13:54:47 XXXXXXXX</td> <td>ACTION State change To do: On going</td> <td>ACTIVATE AUDIO ALERT A Activate external device Device: undefined Action: undefined</td> </tr> <tr> <td>03/03/2025 13:54:55 XXXXXXXX</td> <td>ACTION State change To do: On going</td> <td>STOP AUDIO ALERT A Activate external device Device: undefined Action: undefined</td> </tr> <tr> <td>03/03/2025 13:54:55 XXXXXXXX</td> <td>ACTION State change To do: On going</td> <td>STOP AUDIO ALERT A Activate external device Device: undefined Action: undefined</td> </tr> <tr> <td>03/03/2025 13:56:29 XXXXXXXX</td> <td>END OF SECURITY PLAN</td> <td></td> </tr> </table> Document generated by WaryMe the 06/03/2025 13:49, local hour Europe/Paris 3/3	03/03/2025 13:54:43 XXXXXXXX	START OF SECURITY PLAN	Initiating group: Developpement Management group: Developpement Receiving group: Developpement	03/03/2025 13:54:47 XXXXXXXX	ACTION State change To do: On going	ACTIVATE AUDIO ALERT A Activate external device Device: undefined Action: undefined	03/03/2025 13:54:47 XXXXXXXX	ACTION State change To do: On going	ACTIVATE AUDIO ALERT A Activate external device Device: undefined Action: undefined	03/03/2025 13:54:55 XXXXXXXX	ACTION State change To do: On going	STOP AUDIO ALERT A Activate external device Device: undefined Action: undefined	03/03/2025 13:54:55 XXXXXXXX	ACTION State change To do: On going	STOP AUDIO ALERT A Activate external device Device: undefined Action: undefined	03/03/2025 13:56:29 XXXXXXXX	END OF SECURITY PLAN	
03/03/2025 13:54:43 XXXXXXXX	START OF SECURITY PLAN	Initiating group: Developpement Management group: Developpement Receiving group: Developpement																		
03/03/2025 13:54:47 XXXXXXXX	ACTION State change To do: On going	ACTIVATE AUDIO ALERT A Activate external device Device: undefined Action: undefined																		
03/03/2025 13:54:47 XXXXXXXX	ACTION State change To do: On going	ACTIVATE AUDIO ALERT A Activate external device Device: undefined Action: undefined																		
03/03/2025 13:54:55 XXXXXXXX	ACTION State change To do: On going	STOP AUDIO ALERT A Activate external device Device: undefined Action: undefined																		
03/03/2025 13:54:55 XXXXXXXX	ACTION State change To do: On going	STOP AUDIO ALERT A Activate external device Device: undefined Action: undefined																		
03/03/2025 13:56:29 XXXXXXXX	END OF SECURITY PLAN																			

6. USE - SMARTPHONE

This chapter summarises the main features available from the mobile interface of the WaryMe smartphone app.

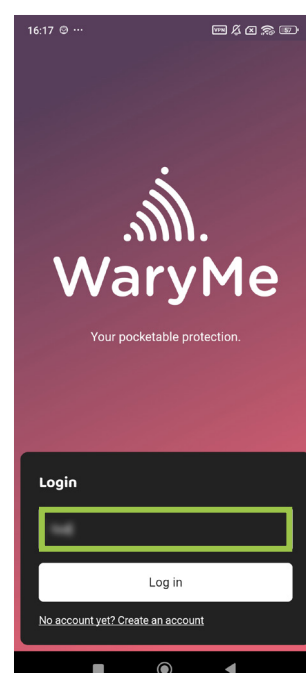
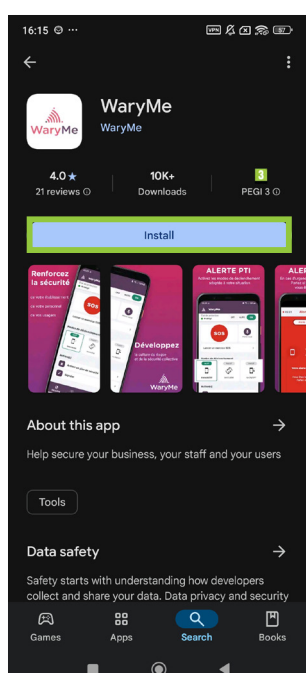
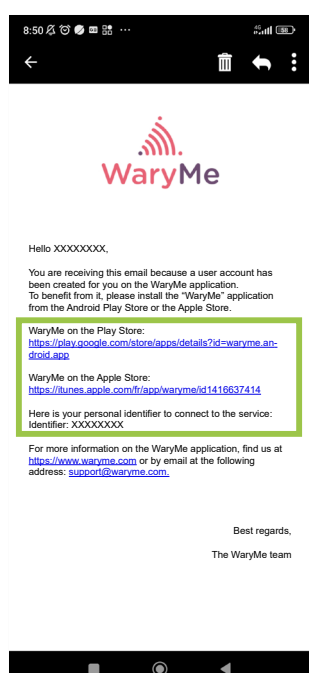


Please refer to the WaryMe technical support for the full description of all the features available from the smartphone app.

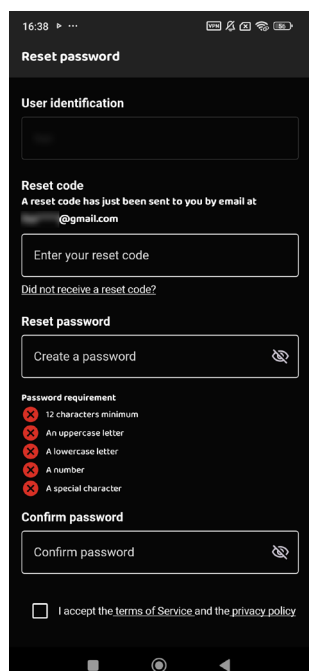
6.1. First connection

When implementing the Bodet Alert solution within your organisation, it is likely that all login credentials will be created and added beforehand from the administration portal.

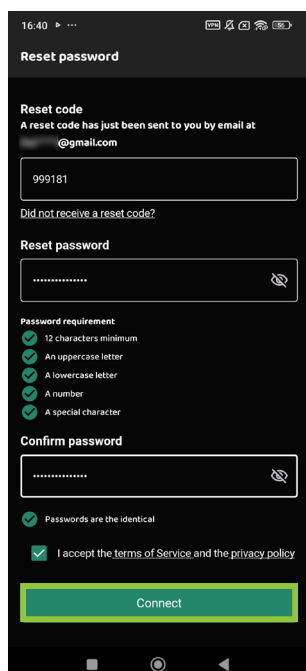
To do so, follow these steps:



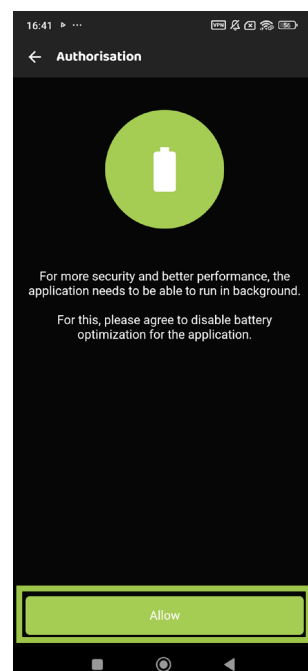
- 1** Connect to your professional mailbox. WaryMe will send you an e-mail following the creation of your user profile by the technical team of your organisation, via the administration portal. **This mail contains your user ID.**
- 2** Download the WaryMe app on your smartphone via the Play Store or AppStore. The mail contains the download link to these 2 platforms.
- 3** Enter the user ID given in the e-mail when opening the app.



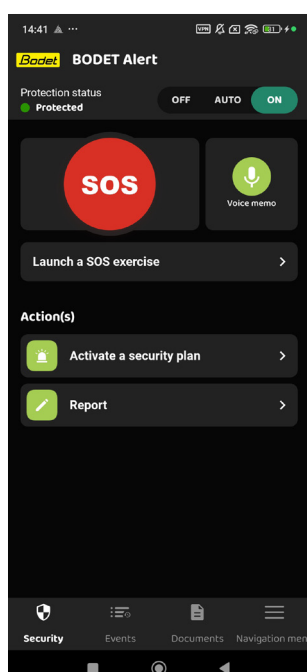
- 4** Fill in the account activation form.
Go back to your mailbox to retrieve the activation code. This code is valid for 10 minutes.



- 5** Click on "Connect" once all the information has been entered.



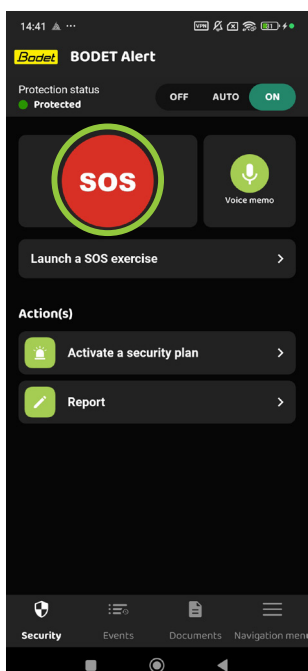
- 6** Grant all authorisations required by the app for full protection.



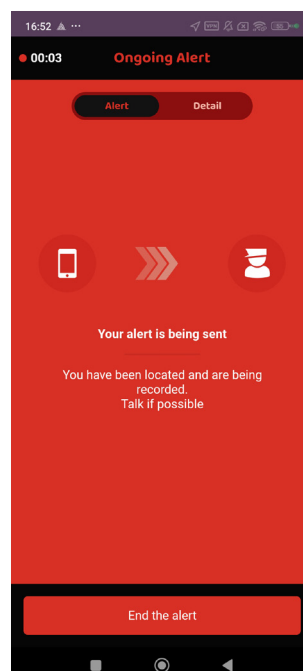
- 7** The app home screen only displays the features that the user has been granted.

6.2. Triggering of an individual alert (SOS)

6.2.1. Triggering an individual alert (SOS)

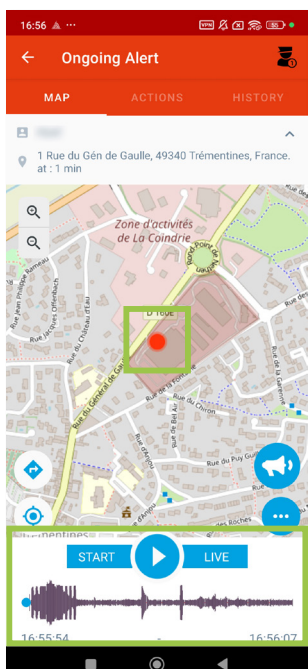


1 Press the "SOS" button displayed on the app home screen in case of accident, assault or emergency situation.

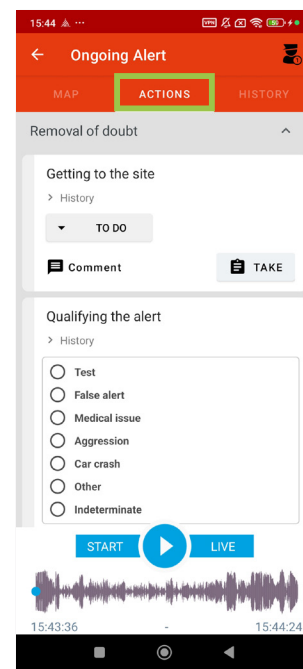


2 Speak if you are able to, your smartphone will record the ambient sound and will broadcast it in real time to the programmed recipients (security teams,...). Your location will also be recorded and sent in real time to recipients.

6.2.1. Receiving an individual alert (SOS)



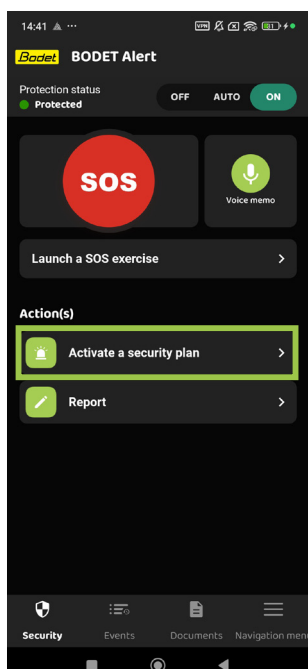
1 **Analysing the alert.** The SOS individual alert is sent to all programmed recipients (security team,...) depending on established security rules (geographical area,...). **Each user receives the alert directly on their smartphone.** On most smartphones, the app manages to bypass any active silent mode to alert recipients.



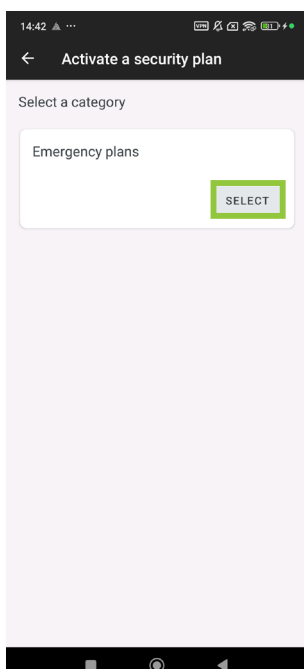
2 **Qualifying the alert.** The real-time ambient listening and location allows to remove any doubt and qualify the event. **It is possible to implement an action plan** in order to guide the intervention to provide assistance.

6.3. Activation of a security plan

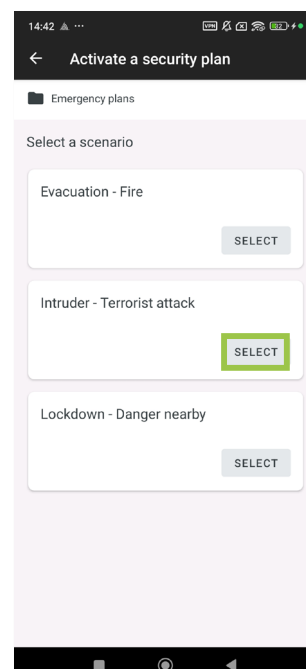
6.3.1. Activating a security plan



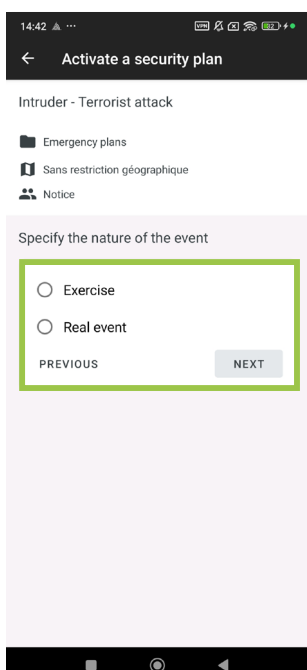
1 Click on "Activate a security plan" from the app home screen in case of major event.



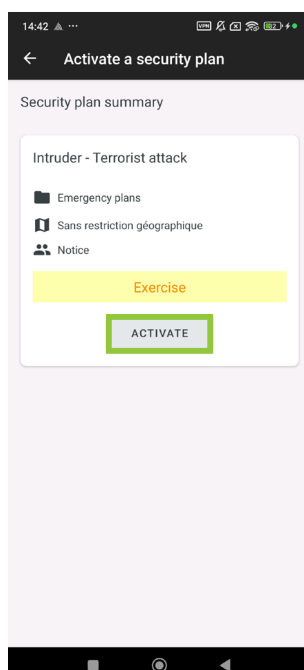
2 Select the category of the security plan depending on the event.



3 Select the scenario of the security plan most suitable to the event.

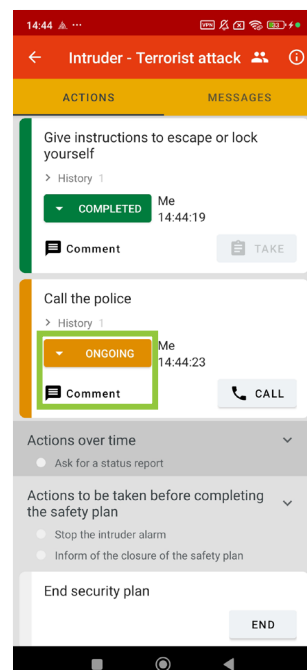
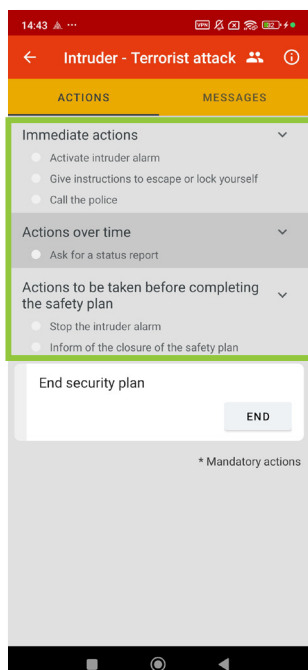


4 Select the type of event: exercise or real event.



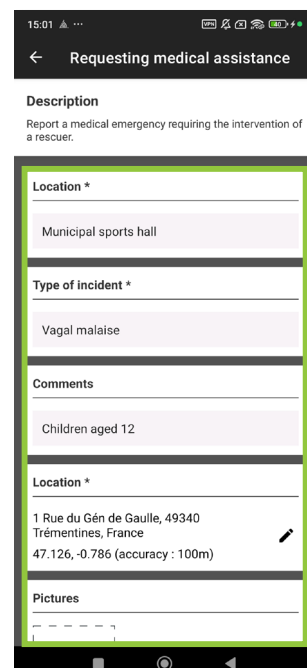
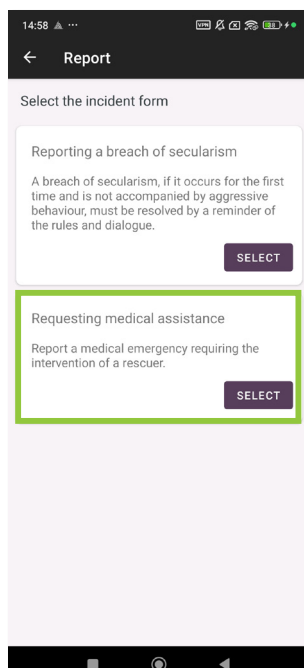
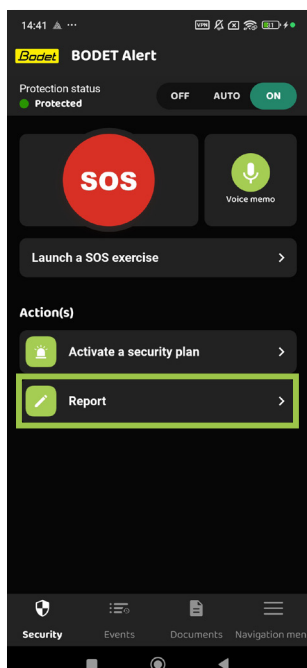
5 Click on "Activate" to display the security plan stages and start managing the event.

6.3.2. Managing and collaborating to a security plan



- 1 Follow and carry out the actions provided in the plan.** The users authorised to manage the security plan are able to access all the plan stages previously prepared to start managing the event. The step-by-step structuring of the security plan enables to start managing the crisis situation with a previously defined methodology and process.
- 2 Filling in, commenting and following the plan.** Each authorised user can fill in and comment a plan stage. Each action stage mentions a status (pending, in progress, completed, cancelled, failed) to simplify follow-up. Any change in status is shared with other users that can be informed in real time of the evolution of the security plan. All actions are recorded and timestamped.

6.4. Reporting an incident



- 1 Click on "Report" from the app home screen if you have any incident to report.**
- 2 Select the type of incident depending on the nature of the information to be reported (medical assistance, breach of secularism,...).**
- 3 Fill in and send the incident form.**

7. TECHNICAL FEATURES

Compliance

- Directives..... RED 2014/53/EU,
RoHS 2011/65/EU.

Mechanical features

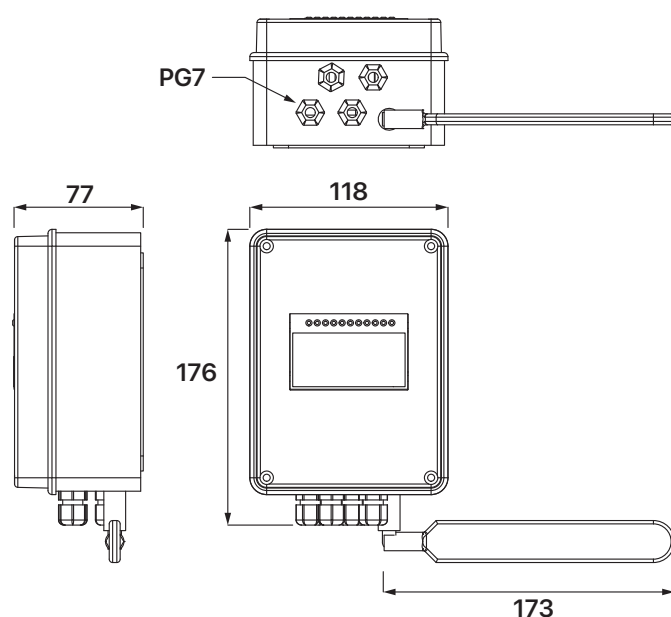
- Construction..... Plastic casing.
- Mounting options..... Wall mounting.
- Protection index..... IP40.
- Weight..... 700 g.
- Operating temperature..... -20°C to 60°C.
- Humidity level..... 5 to 95% (non-condensing).
- Cable routing..... 4 PG7 cable glands.
- Dimensions..... See below.

Electrical features

- Power supply..... 12-24V $\overline{=}$ - 690 mA max.
- Electrical insulation..... Class II.
- Overvoltage category..... Category II.
- Digital inputs..... Input voltage: 3-12V $\overline{=}$
Input current: 2mA.
- Relay outputs..... Maximum voltage: 250V $\sim$.
Max breaking capacity: 750 VA.
- Battery..... Li-poly technology.
Voltage: 3.7V.
Capacity: > 320 mAh.
- Antenna (supplied)..... 4G network. Connection to SMA female coaxial jack.

Dimensions (mm)

fig. 6



8. SELF-TROUBLESHOOTING

What to do if...	Action(s) to be carried out
No action is sent, whether between the Cloud (mobile app) and the Bodet audio ecosystem or vice versa.	1 Check that the alert interface box is correctly powered and switched on. 2 Check that the GSM 4G antenna is connected to the alert interface box. 3 Check that the SIM card inserted into the transmitter module has been correctly configured (PIN code deactivated). 4 Check all connections between the alert interface box and the Sigma master clock. 5 Check the configuration of the alert interface box from the WaryMe administration portal.
Triggering an alert from the Cloud (mobile app) activates the triggering of another alert on site.	1 Check all connections between the alert interface box and the Sigma master clock. 2 Check the configuration of the alert interface box from the WaryMe administration portal in the security plans (activation of the right relay). See chapter <i>4.2 WaryMe administration portal</i>, section "Adding alert triggering/stopping actions (Cloud to Sigma)". 3 Check the consistency of the configuration between the IP button boxes (Sigma) and the configuration established for the Bodet Alert solution. See chapter <i>4.1 Sigma software</i>.
Triggering an alert on site (IP button box) activates the triggering of another cloud-based security plan.	1 Check all connections between the alert interface box and the Sigma master clock. 2 Check the configuration of the alert interface box from the WaryMe administration portal in the "Equipment" section. See chapter <i>4.2 WaryMe administration portal</i>, section "Adding alert feedback actions (Sigma to Cloud)". 3 Check the consistency of the configuration between the IP button boxes (Sigma) and the configuration established for the Bodet Alert solution. See chapter <i>4.1 Sigma software</i>.



bodet-time.com



EXPORT

Technical support

+33 2 41 71 72 33

export@bodet-timesport.com

Documentary base available at:

www.bodet-time.com

MADE IN FRANCE