Hub User Manual

Updated December 20, 2019

Hub is a central device of the Ajax security system, coordinating the connected devices, and interacting with the user and security company.

How to install the Ajax StarterKit, if you’ve never done this before. A masterclass from the undisputed cruiserweight champion Oleksandr Usyk.

Hub requires Internet access to communicate with the cloud server Ajax Cloud—for configuring and controlling from any point of the world, transferring event notifications, and updating the software. Ajax Cloud locates on the Amazon Web Services capacities. The personal data and system operation logs are stored under multilevel protection, and information exchange with Hub is carried out via an encrypted channel on a 24-hour basis.

Communicating with Ajax Cloud, the system can use the Ethernet connection and GSM network.

Please use both communication channels to ensure more reliable communication between the hub and Ajax Cloud.

Hub can be controlled via the app for iOS, Android, macOS, or Windows. The app allows responding promptly to any notifications of the security system.

Follow the link to download the app for your OS:

Android

iOS

The user can customize notifications in the hub settings. Choose what is more convenient for you: push notifications, SMS, or calls. If the Ajax system is connected to the central monitoring station, the alarm signal will be sent directly to it, bypassing Ajax Cloud.

Buy intelligent security control panel Hub

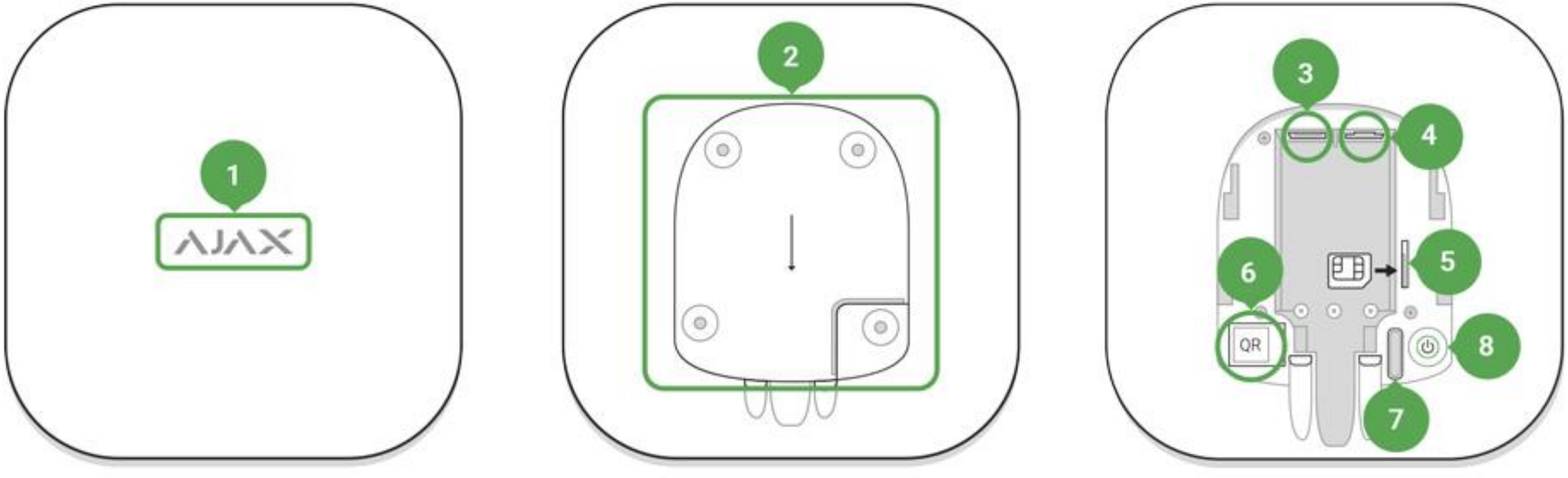
Up to 100 Ajax devices can be connected to the hub. The protected Jeweller radio protocol ensures reliable communication between the devices at a distance of up to 2 km in the line of sight.

List of Ajax devices

Use scenarios to automate the security system and decrease the number of routine actions. Adjust the security schedule, program actions of automation devices (Relay, WallSwitch or Socket) in response to an alarm, Button press or by schedule. A scenario can be created remotely in the Ajax app.

How to create and configure a scenario in the Ajax security system

Sockets and Indication



1. LED logo indicating the hub status
2. SmartBracket attachment panel (perforated part is required for actuating the tamper in case of any attempt to dismantle the hub)
3. Socket for the power supply cable
4. Socket for the Ethernet cable

5. Slot for the micro SIM
6. QR code
7. Tamper button
8. On/Off button

Logo Indication

When clicking the power button, the Ajax logo lights up green for a second. Right after that, the logo changes its color to red, indicating that the hub is loading. When loading is complete, the color of the logo depends on the connection with Ajax Cloud.

If the hub is not connected to the power supply, the logo lights up for 3 minutes, then flashes every 20 seconds.

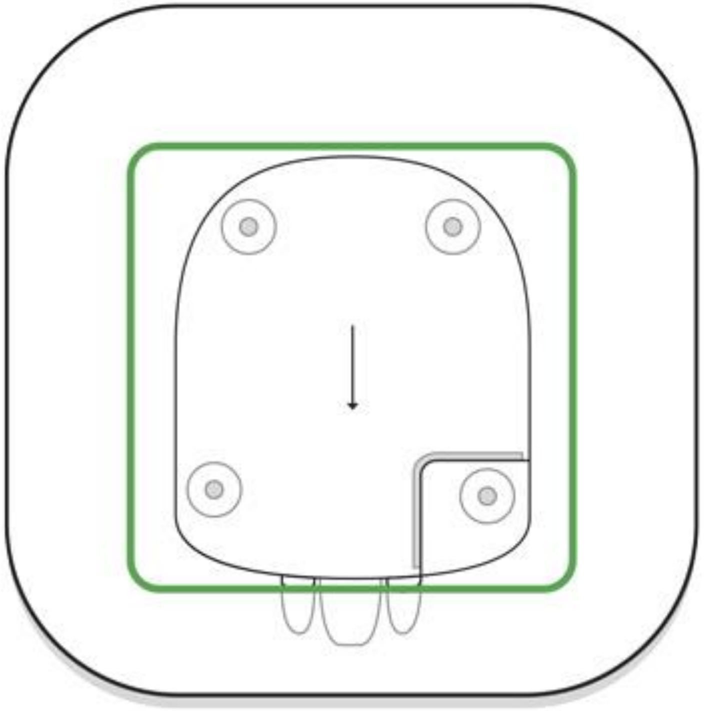
Communication with Ajax Cloud

Highlight colour notifies of the communication with the Ajax Cloud

Indication	Event
Lights white	Both communication channels are connected (Ethernet and GSM)
Lights bright green	One communication channel is connected
Lights red	The hub is not connected to the Internet or there is no communication with the server

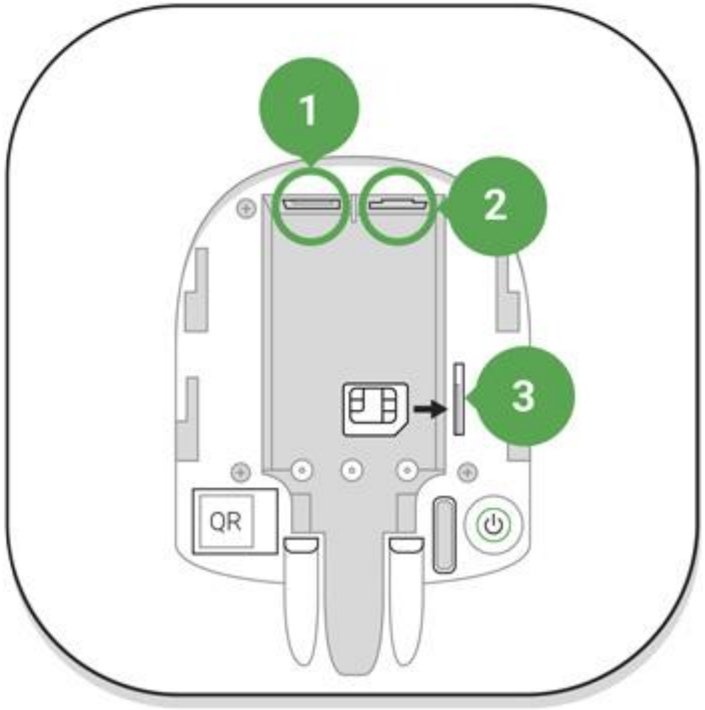
Connecting to the Network

1. Open the hub lid by shifting it down with force.



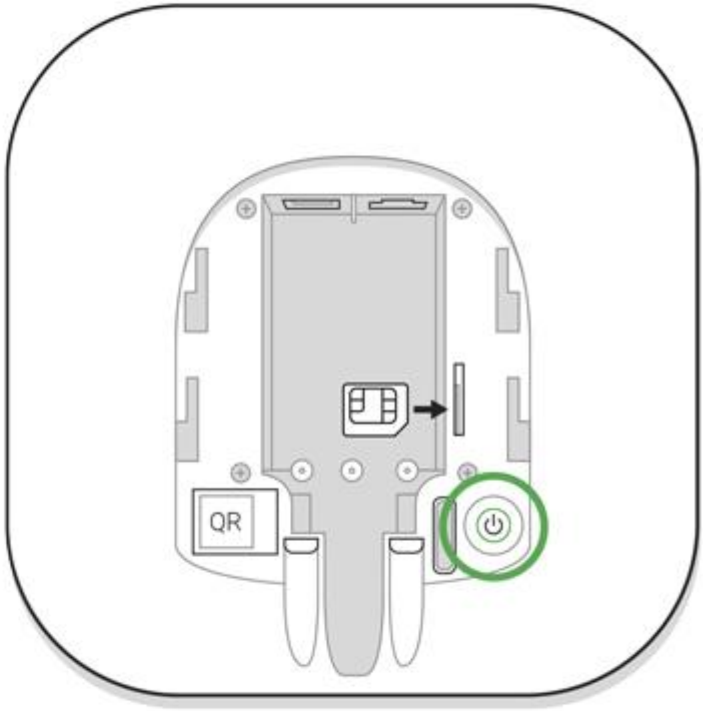
Be careful and do not damage the tamper protecting the hub from dismantling!

2. Connect the power supply and Ethernet cables to the sockets.



1 — Power Socket
2 — Ethernet socket
3 — SIM-card slot

3. Press and hold the power button for 2 seconds until the logo lights up. The hub needs approximately 2 minutes to identify the available communication channels.



The bright green or white logo color indicates that the hub is connected to Ajax Cloud.

If the Ethernet connection does not occur automatically, disable proxy, filtration by MAC addresses and activate the DHCP in the router settings: the hub will receive an IP address. During the next setup in the web or mobile app, you will be able to set a static IP address.

To connect the hub to the GSM network, you need a micro-SIM card with a disabled PIN code request (you can disable it using the mobile phone) and a sufficient amount on the account to pay for the GPRS, SMS services and calls.

In some regions, Hub is sold with a SIM card along

If the hub does not connect to Ajax Cloud via GSM, use Ethernet to set up the network parameters in the app. For the proper setting of the access point, username, and password, please contact the support service of the operator.

Ajax Account

The user with administrator rights can configure the Ajax security system via the app. The administrator account with the information about the added hubs is encrypted and placed on Ajax Cloud.

All the parameters of the Ajax security system and connected devices set by the user are stored locally on the hub. These parameters are inextricably linked with the hub: changing the hub administrator does not affect the settings of the connected devices.

One phone number may be used to create only one Ajax account.

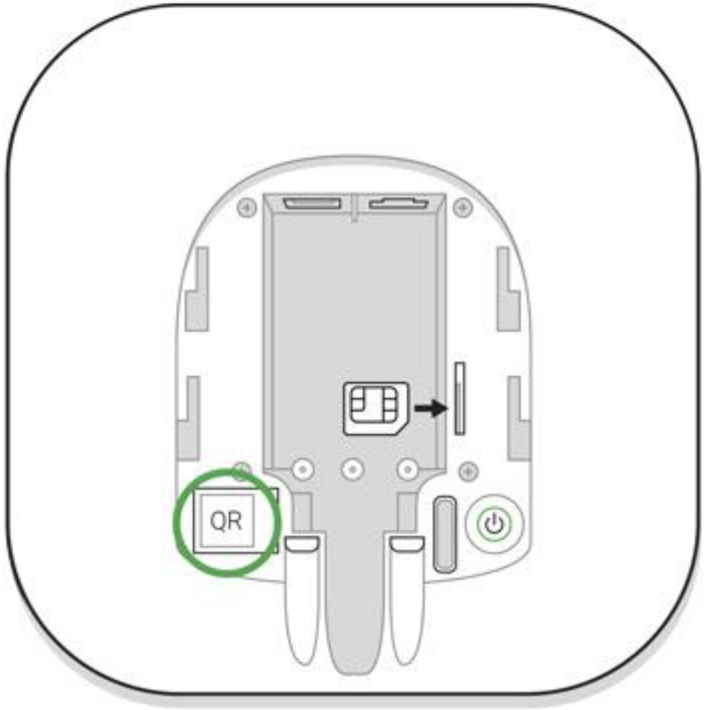
Create the Ajax account in the app following the step-by-step guide. As part of the process, you need to confirm your email and phone number.

Ajax account allows to combine the roles: you can be the administrator of one hub, as well as the user of another hub.

Adding the hub to the Ajax app

Granting access to all system functions (to display notifications in particular) is a mandatory condition for controlling the Ajax security system via the smartphone/tablet.

1. Login into your account.
2. Open the **Add Hub** menu and select the way of registering: manually or step-by-step guidance.
3. At the registration stage, type the name of the hub and scan the QR code located under the lid (or enter a registration key manually).



4. Wait until the hub is registered and displayed on the application desktop.

Installation

Prior to installing the hub, make sure that you have selected the optimal location: the SIM card demonstrates consistent reception, all the devices have been tested for radio communication, and the hub is hidden from direct view.

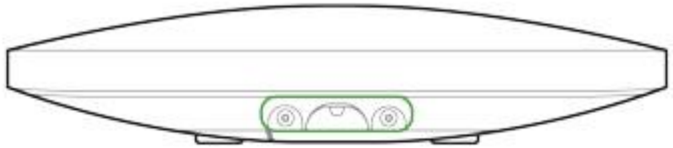
The hub should be reliably attached to the surface (vertical or horizontal). We do not recommend using double-sided adhesive tape: it cannot guarantee secure attachment and simplifies the removal of the device.

Do not place the hub:

- outside the premises (outdoors);
- nearby or inside any metal objects or mirrors causing attenuation and screening of the signal;
- in places with low GSM signal and high radio interference level;
- inside any premises with the temperature and humidity beyond the range of permissible limits.

Installation of the hub:

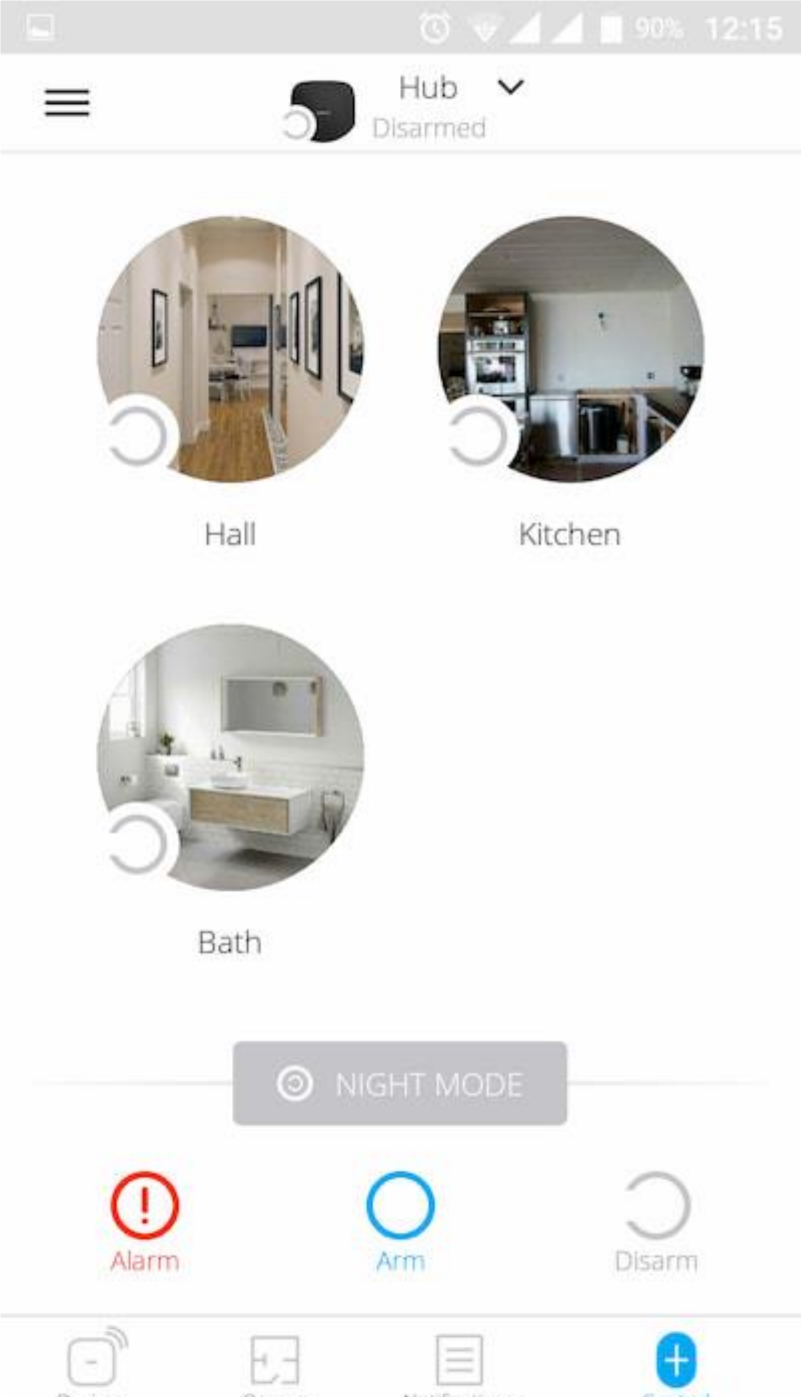
1. Fix the hub lid on the surface using bundled screws. When using any other fixing accessories, make sure that they do not damage or deform the hub lid.
2. Put the hub on the lid and fix it with bundled screws.



Fixing the hub on lid with screws prevents any accidental shifting of the hub and minimizes the risk of device theft.

If the hub is securely attached, dismantling its body from the surface triggers the tamper alarm, and the system notifies you about this.

Rooms in the Ajax app


90%
12:15
Hub
Disarmed
Hall
Kitchen
Bath
NIGHT MODE
Alarm
Arm
Disarm

The virtual rooms are used to group the connected devices. The user can create up to 50 rooms, with each device located only in one room.

Without creating the room, you are not able to add devices in the Ajax app!

Creating and Setting Up a Room

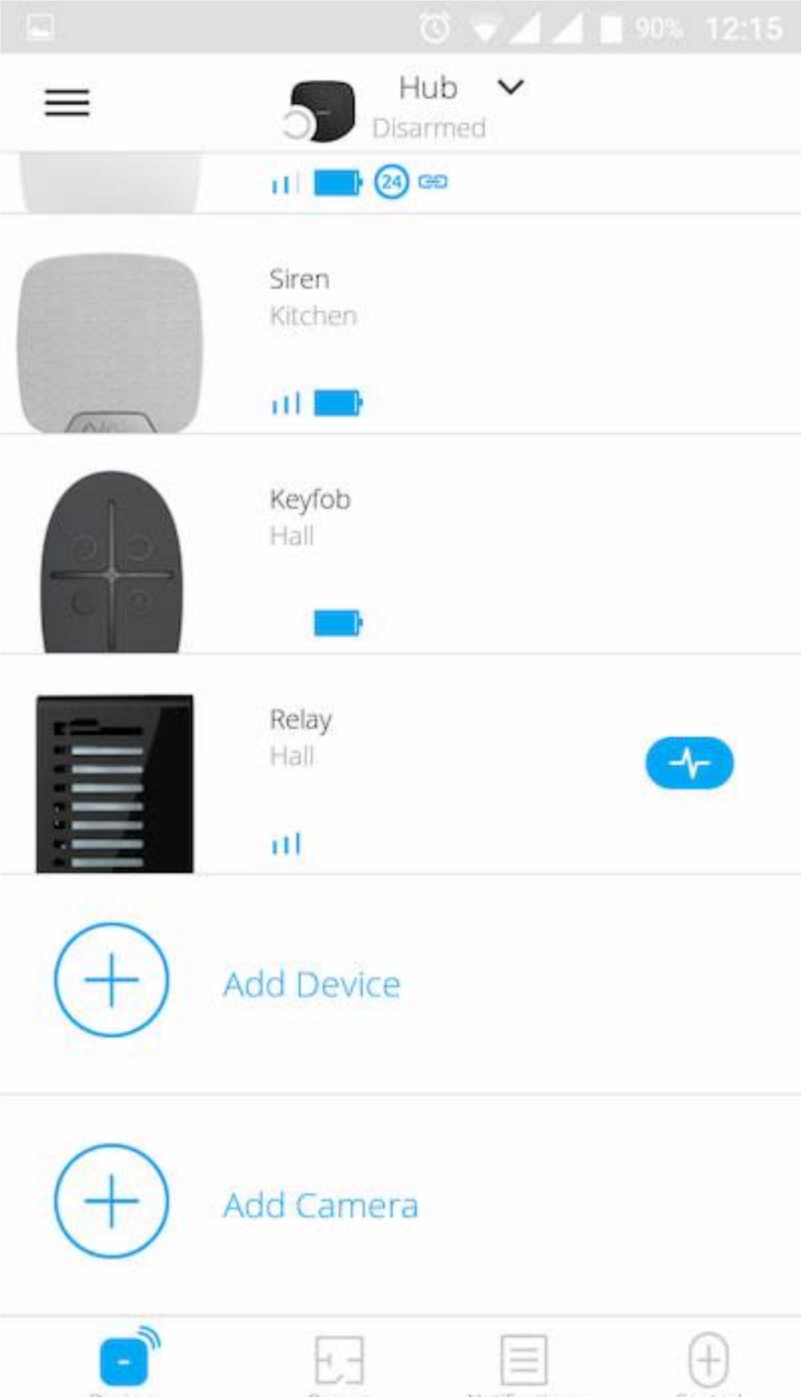
The room is created in the app using the **Add Room** menu.

Please assign a name for the room, and optionally, attach (or make) a photo: it helps to find the needed room in the list quickly.

By pressing on the gear button go to the room settings menu.

To delete the room, move all the devices to other rooms using the device setup menu. Deleting the room erases all its settings.

Connecting Devices


90% 12:15
Hub
Disarmed
24
Siren
Kitchen
Keyfob
Hall
Relay
Hall
Add Device
Add Camera

During the first hub registration in the app, you will be prompted to add devices to guard the room. However, you can refuse and return to this step later.

The user can add the device only when the security system is disarmed!

1. Open the room in the app and select the **Add Device** option.
2. Name the device, scan the **QR code** (or insert the ID manually), select the room and go to the next step.
3. When the app starts searching and launches countdown, switch on the device: its LED will blink once. For detection and pairing to occur, the device should be located within the coverage area of the wireless network of the hub (at a single protected object).

Connection request is transmitted for a short time at the moment of switching on the device.

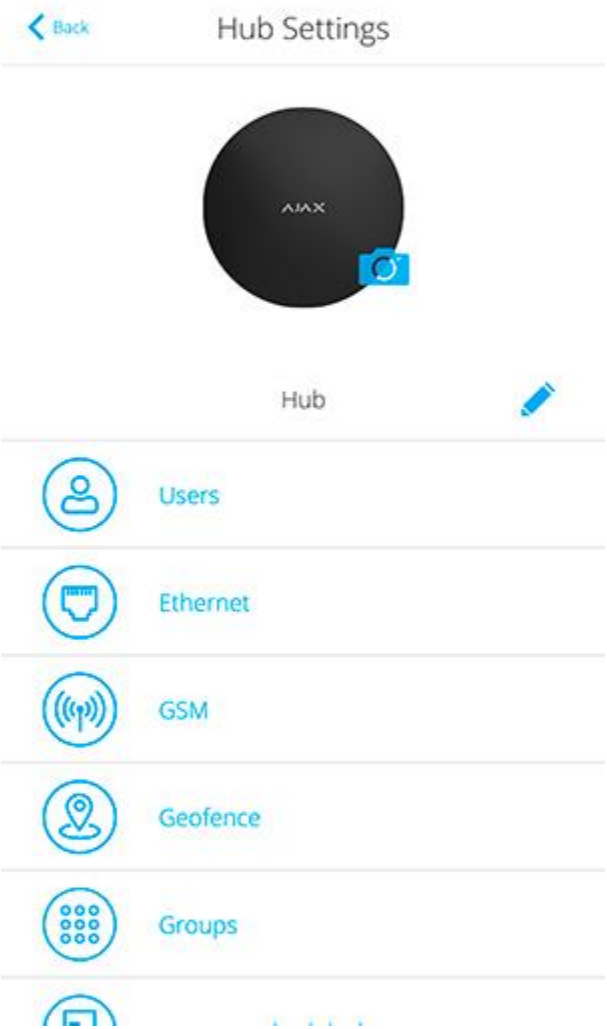
If the connection fails on the first try, switch off the device for 5 seconds and retry.

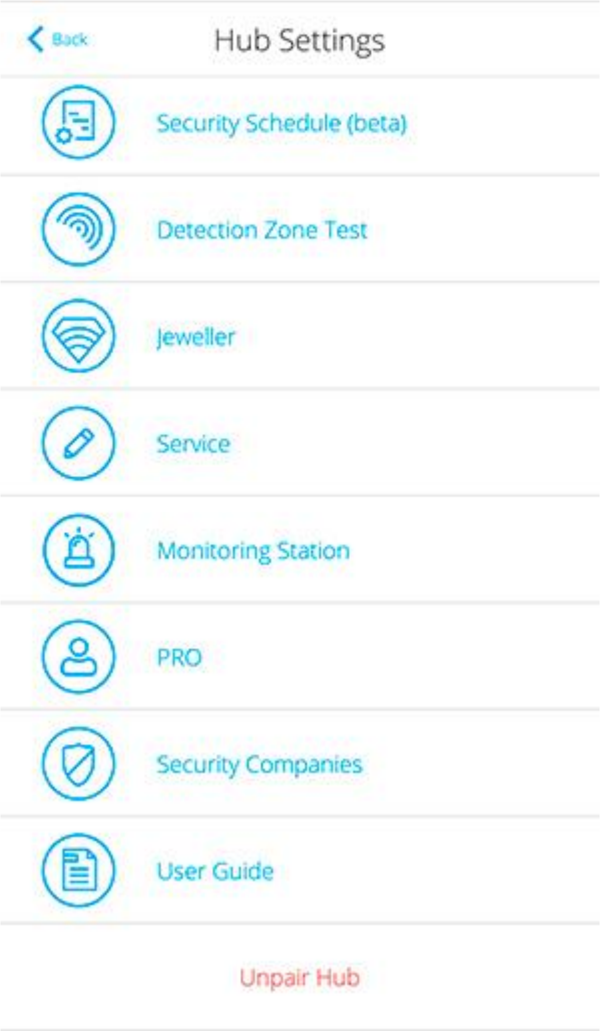
Up to 10 cameras or DVRs that support RTSP protocol can be connected to Hub.

How to configure and connect an IP camera to the Ajax security system

Settings

The hub and connected devices settings are in the **Hub Settings** menu .





Adjustable parameters:

- **Users** — define who has access to your security system, what rights are granted to them, how the hub notifies of events.
- **Ethernet** — configure the Ethernet connection.
- **GSM** — switch on/off cellular communication, configure the connection and check the balance.
- **Geofence** — set the reminder of arming/disarming the security system, when entering the specified area.

The user location is determined based on the data from the GPS antenna or iBeacon (only for Apple devices).

- **Groups** — open group mode settings.
- **Security Schedule** — set a schedule to arm/disarm the security system automatically.
- **Detection Zone Test** — run the detection zone test for the connected devices.
- **Jeweller** — configure the hub-detector ping interval and number of undelivered packets that determines connection failure.

The ping interval determines how frequently the devices communicate. The shorter interval (in seconds) means faster delivery of the events between the hub and the connected devices. The number of undelivered packets determines how quickly the hub identifies the connection loss with the device.

Calculation of the time for raising the alarm (with the default parameters):

(8 packets + 1 corrective) × 36 seconds inquiry interval = 5 minutes 24 seconds

In any case, alarms are transmitted immediately. Keep in mind that the ping interval can reduce the maximum number of connected devices:

Interval	Connection limit
12 seconds	39 devices
24 seconds	79 devices
36 and more seconds	100 devices

- **Service —** opens service settings of the hub.

Connection Failure Alarm Delay — regulates the alarm notification delay of the server connection loss.

Server Ping Interval — regulates the interval of sending pings from the hub to the server.

Time for generation of the message of the connection loss between the server and the hub is calculated as follows (with the default parameters):

(3 pings + 1 corrective) × 60 seconds inquiry interval + 300 seconds time filter = 9 minutes.

You can disable hub firmware auto-update (enabled by default).

How to turn off hub firmware auto-update

- **Monitoring Station —** configure CMS connection settings.
- **PRO —** configure PRO-accounts connected to the hub.

- **Security Companies** — choose and connect a security company in your region.

Settings Reset

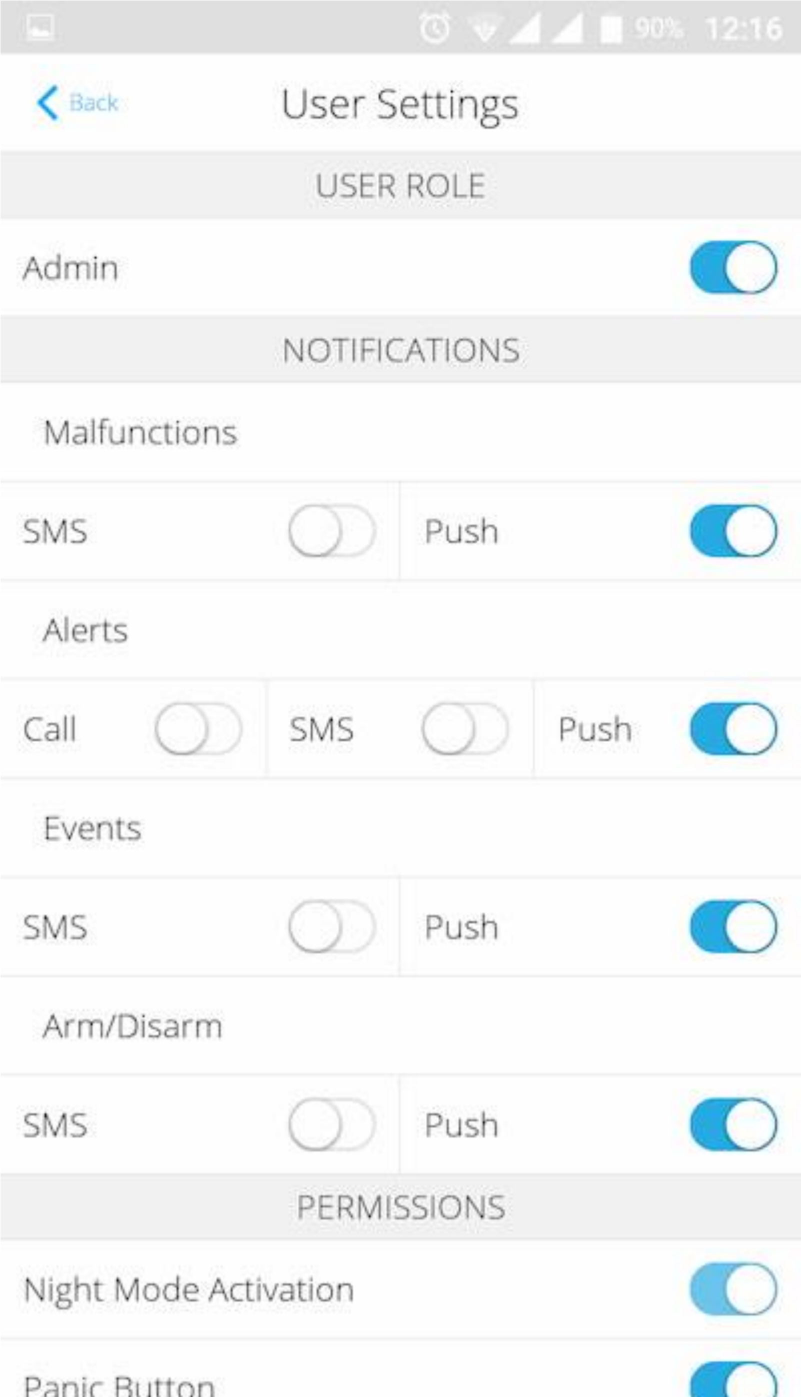
To return the hub to the factory default settings, switch it on, then hold the power button for 30 seconds (logo will start blinking red).

At the same time, all the connected detectors, room settings and user settings will be deleted. User profiles will remain connected to the system.

Users

After adding the hub to the account, you become the administrator of this device. One hub can have up to 50 users/administrators. The administrator can invite users to the security system and determine their rights.

Events and Alarms Notifications



User Settings

USER ROLE

Admin ●

NOTIFICATIONS

Malfunctions

SMS ○ | Push ●

Alerts

Call ○ | SMS ○ | Push ●

Events

SMS ○ | Push ●

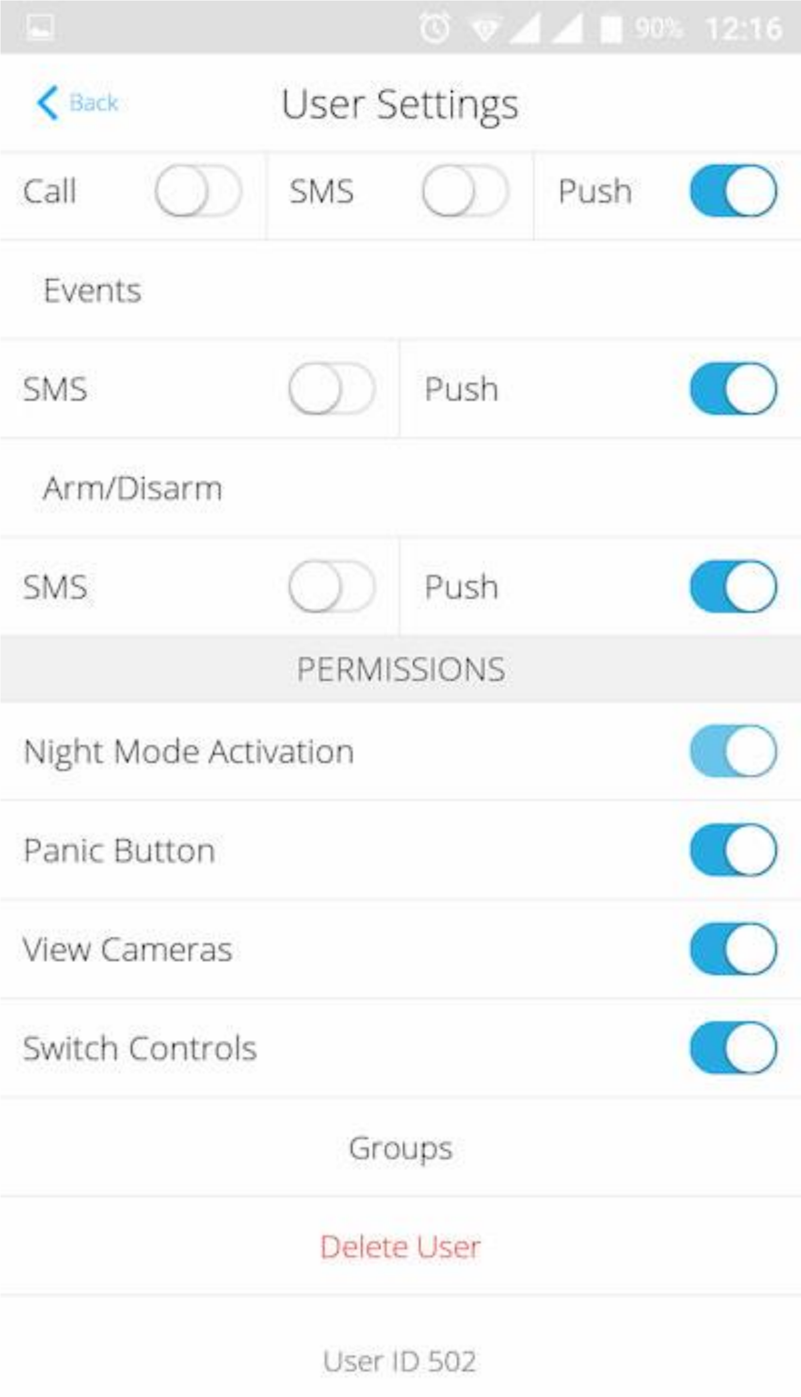
Arm/Disarm

SMS ○ | Push ●

PERMISSIONS

Night Mode Activation ●

Panic Button ●



90% 12:16

Back

User Settings

Call ○ | SMS ○ | Push ●

Events

SMS ○ | Push ●

Arm/Disarm

SMS ○ | Push ●

PERMISSIONS

Night Mode Activation ●

Panic Button ●

View Cameras ●

Switch Controls ●

Groups

Delete User

User ID 502

The hub notifies users of events in three ways: push notifications, SMS and calls.

Notifications are set in the menu **Users**:

Event types	For what it is used	Types of notifications
Arming / Disarming	Notices are received after arming/disarming	SMS Push-notification
Alarm	Notices of intrusion, fire, flood	SMS Push-notification Call
Events	Notices of events related to the Ajax WallSwitch, Relay control	SMS Push-notification
Malfunctions	Notices of the lost communication, jamming, low battery charge or opening of the detector body	SMS Push-notification

- **Push notification** is sent by Ajax Cloud to the Ajax Security system app, if an Internet connection is available.
- **SMS** is sent to the phone number indicated by the user when registering the Ajax account.

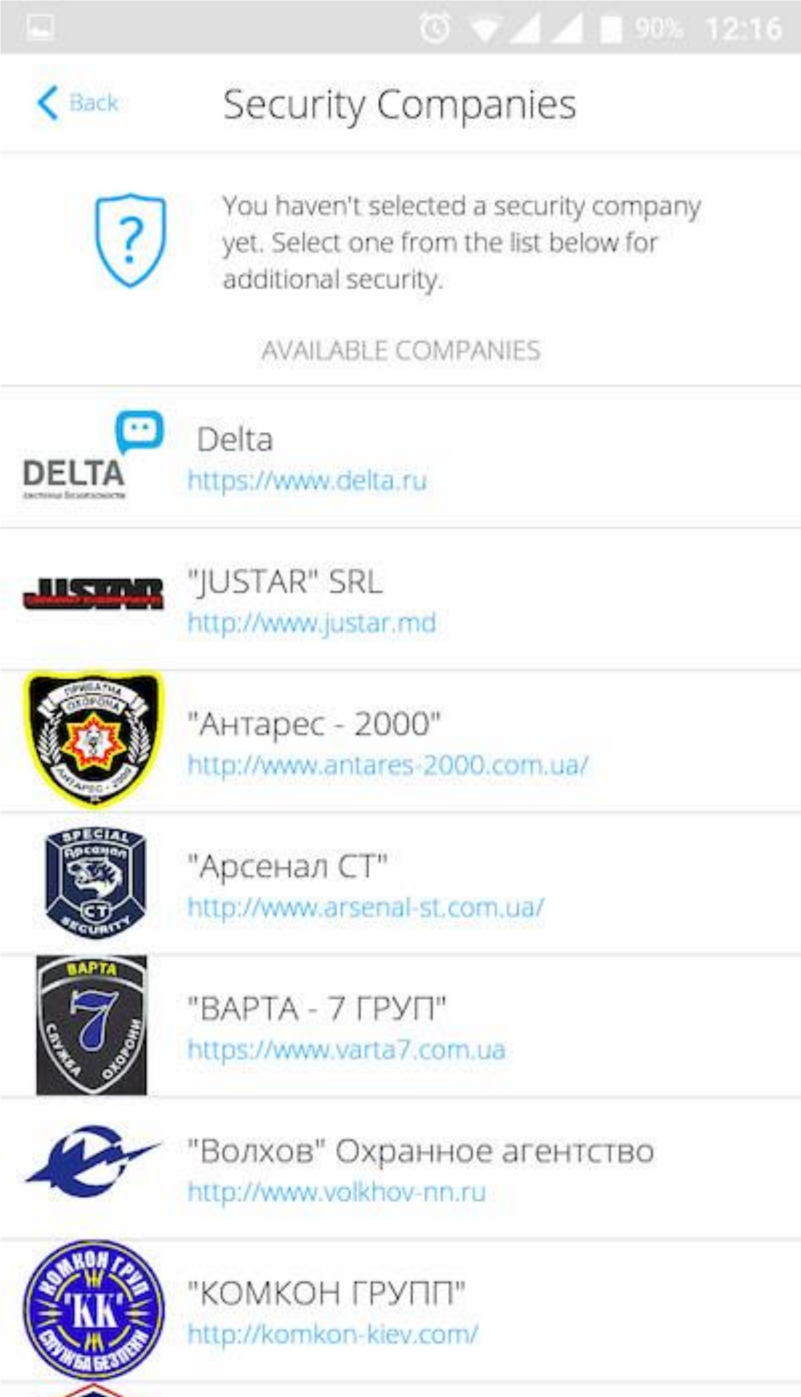
- The **phone call** means that the hub calls the number specified in the Ajax account.

  The hub calls only in case of alarm to get your attention and reduce the feasibility of you missing a critical alert. We recommend to enable this type of notification. The hub consecutively calls all users who have enabled this type of notification in the order specified in the Users Settings. If the second alarm occurs, the hub will make a call again but not more than once in 2 minutes.

  The call is automatically dropped as soon as you answer it. We recommend you to save the phone number associated with the hub SIM card in your contacts list.

  Notification settings may be only changed for registered users.

Connecting a Security Company



Security Companies

You haven't selected a security company yet. Select one from the list below for additional security.

AVAILABLE COMPANIES

Delta
https://www.delta.ru

"JUSTAR" SRL
http://www.justar.md

"Антарес - 2000"
http://www.antares-2000.com.ua/

"Арсенал СТ"
http://www.arsenal-st.com.ua/

"ВАРТА - 7 ГРУП"
https://www.varta7.com.ua

"Волхов" Охранное агентство
http://www.volkhov-nn.ru

"КОМКОН ГРУПП"
http://komkon-kiev.com/

The list of organizations connecting the Ajax system to the central monitoring station is provided in the **Security Companies** menu of the hub settings:

Contact representatives of the company providing services in your city and negotiate on the connection.

Connection to the central monitoring station (CMS) is possible via the Contact ID or SIA protocols.

Maintenance

Check the operational capability of the Ajax security system on a regular basis.

Clean the hub body from dust, spider webs and other contaminants as they appear. Use soft dry napkin suitable for equipment maintenance.

Do not use any substances containing alcohol, acetone, gasoline and other active solvents for cleaning the hub.

How to replace hub battery

Complete Set

1. Ajax Hub

2. SmartBracket mounting panel
3. Power supply cable
4. Ethernet cable
5. Installation kit
6. GSM start package (available not in all countries)
7. Quick Start Guide

Safety Requirements

While installing and using the hub, follow the general electrical safety regulations for using electrical appliances, as well as the requirements of regulatory legal acts on electrical safety.

It is strictly prohibited to disassemble the device under voltage! Do not use the device with a damaged power cable.

Tech Specs

Devices	up to 100

Groups	up to 9
Users	up to 50
Rooms	up to 50
Scenarios	up to 5 (Scenarios by arming/disarming are not included in the general limit of the scenarios)
Connected ReX	1
Power supply	110 – 240 V AC, 50 / 60 Hz
Accumulator unit	Li-Ion 2 A·h (up to 15 hours of autonomous operation in case of inactive Ethernet connection)
Tamper protection	Yes
Frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz depending on the region of sale
Effective radiated power	8.20 dBm / 6.60 mW (limit 25 mW)
Modulation of the radio signal	GFSK
Radio signal range	Up to 2,000 m (any obstacles absent)
Communication channels	GSM 850/900/1800/1900 MHz GPRS, Ethernet
Operating temperature range	From -10°C to + 40°C

Operating humidity	Up to 75%
Overall dimensions	163 x 163 x 36 mm
Weight	350 g
Certification	Security Grade 2, Environmental Class I SP2 (GSM-SMS), SP5 (LAN) DP3 in conformity with the requirements of EN 50131-1, EN 50131-3, EN 50136-2, EN 50131-10, EN 50136-1, EN 50131-6, EN 50131-5-3

Warranty

Warranty for the “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase and does not apply to the pre-installed accumulator.

If the device does not work correctly, you should first contact the support service—in half of the cases, technical issues can be solved remotely!

The full text of the warranty

User Agreement

Technical support: support@ajax.systems

MotionProtect / MotionProtect Plus User Manual

Updated December 21, 2019

MotionProtect is a wireless motion detector designed for indoor use. It can operate for up to 7 years from an in-built battery, and monitors the area within 12-meter radius. MotionProtect ignores animals, while recognizes a human from the first step.

MotionProtect Plus uses radio frequency scanning along with a thermal sensor, filtering interference from thermal radiation. Can operate up to 5 years from an in-builtbattery.

Buy motion detector with microwave sensor MotionProtect Plus

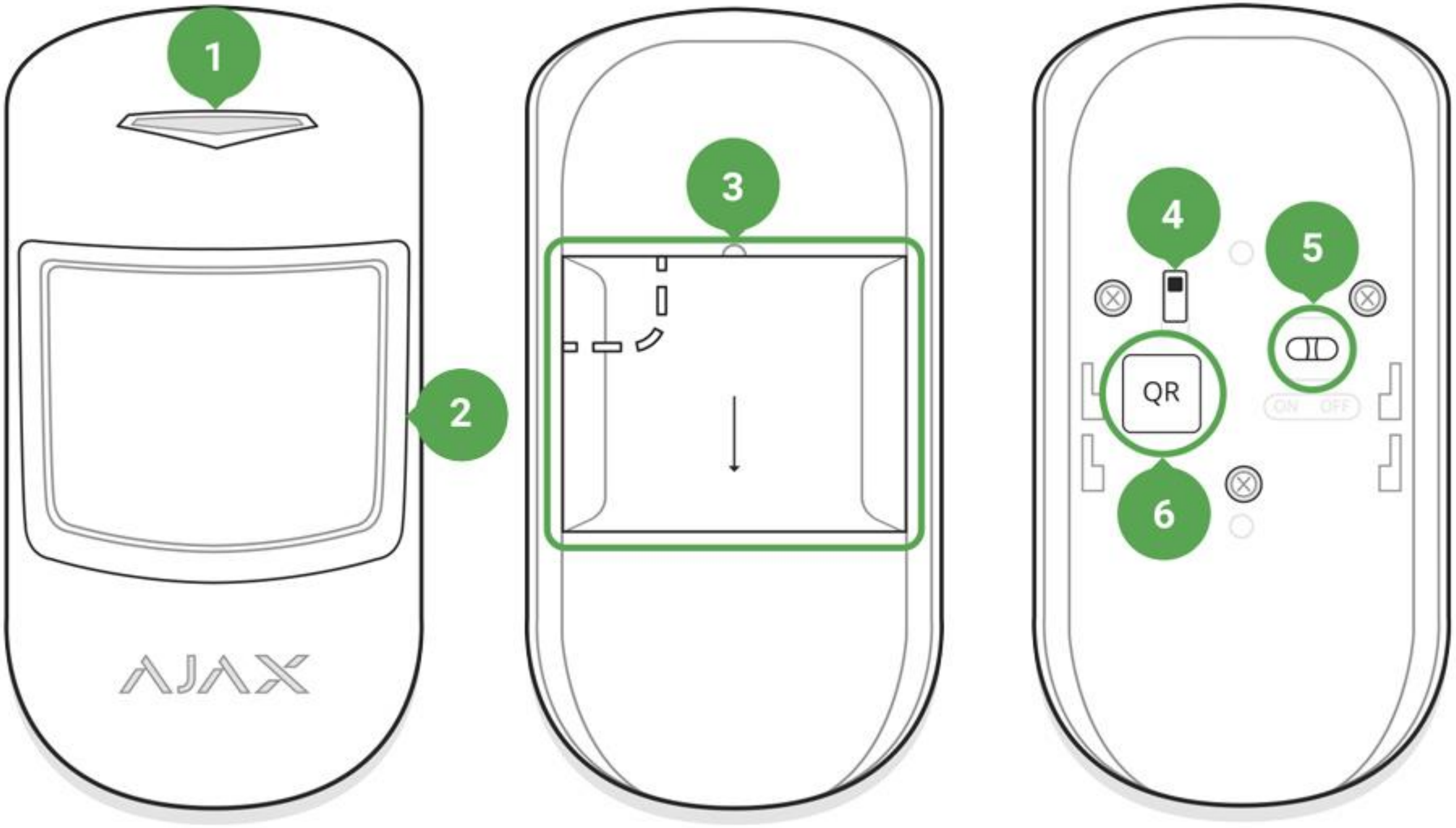
MotionProtect (MotionProtect Plus) operates within the Ajax security system, connected to the hub via the protected Jeweller protocol. The communication range is up to 1700 (**MotionProtect Plus** up to 1200) meters in the line of sight. In addition, the detector can be used as a part of third-party security central units via the Ajax uartBridge or Ajax ocBridge Plus integration modules.

The detector is set up via the Ajax app for iOS, Android, macOS and Windows. The system notifies user of all events through push notifications, SMS and calls (if activated).

The Ajax security system is self-sustaining, but the user can connect it to the central monitoring station of a security company.

Buy motion detector MotionProtect

Functional Elements



1. LED indicator

2. Motion detector lens
3. SmartBracket attachment panel (perforated part is required for actuating the tamper in case of any attempt to dismantle the detector)
4. Tamper button
5. Device switch
6. QR code

Operating Principle

Thermal PIR sensor of MotionProtect detects intrusion into protected room by detecting moving objects whose temperature is close to the temperature of the human body. However, the detector can ignore domestic animals if the suitable sensitivity has been chosen in the settings.

When the **MotionProtect Plus** detects motion, it will additionally carry out radio frequency scanning of the room, preventing false actuation from thermal interferences: air flows from sun-heated curtains and louvre shutters, operating thermal air fans, fireplaces, air conditioning units, etc.

After actuation, the armed detector immediately transmits an alarm signal to the hub, activating the sirens and notifying the user and security company.

If before arming the system, the detector has detected motion, it will not arm immediately, but during the next inquiry by the hub.

Connecting the Detector to the Ajax Security System

Connecting the Detector to the hub

Before starting connection:

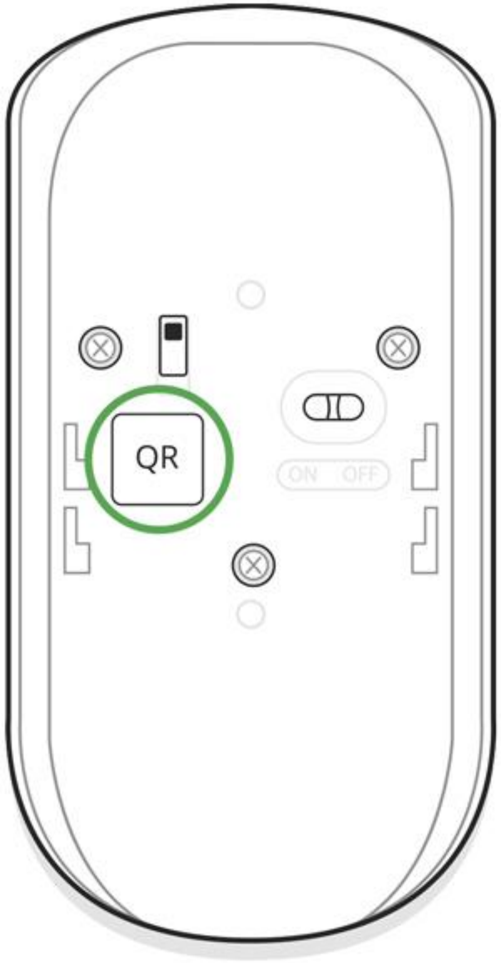
1. Following the hub manual recommendations, install the Ajax application. Create an account, add the hub to the application, and create at least one room.
2. Switch on the hub and check the internet connection (via Ethernet and/or GSM network).
3. Make sure that the hub is disarmed and does not update by checking its status in the app.

Only users with administrator rights can add the device to the hub

How to connect the detector to the hub:

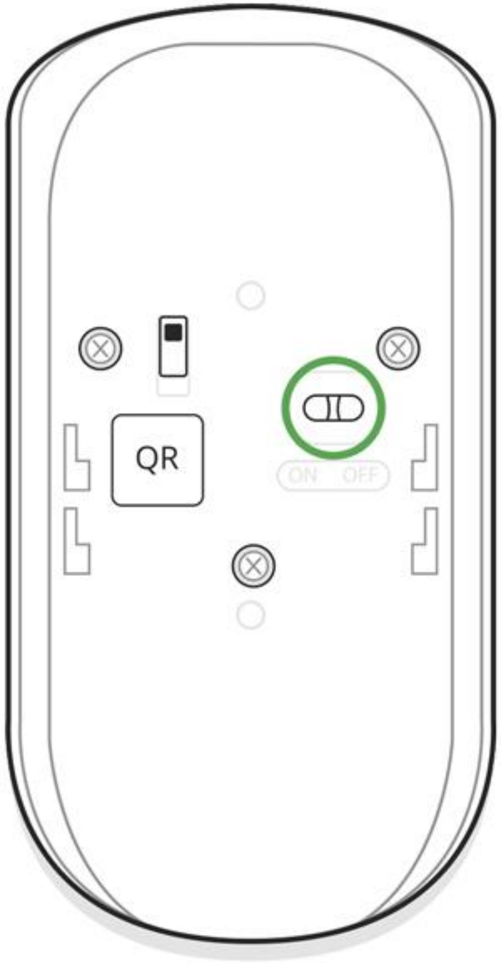
1. Select the **Add Device** option in the Ajax application.

2. Name the device, scan/write manually the **QR Code** (located on the body and packaging), and select the location room.



3. Select **Add** — the countdown will begin.

4. Switch on the device.



For detection and pairing to occur, the detector should be located within the coverage of the wireless network of the hub (at a single protected object).

Request for connection to the hub is transmitted for a short time at the moment of switching on the device.

If the detector failed to connect to the hub, switch off the detector for 5 seconds and retry.

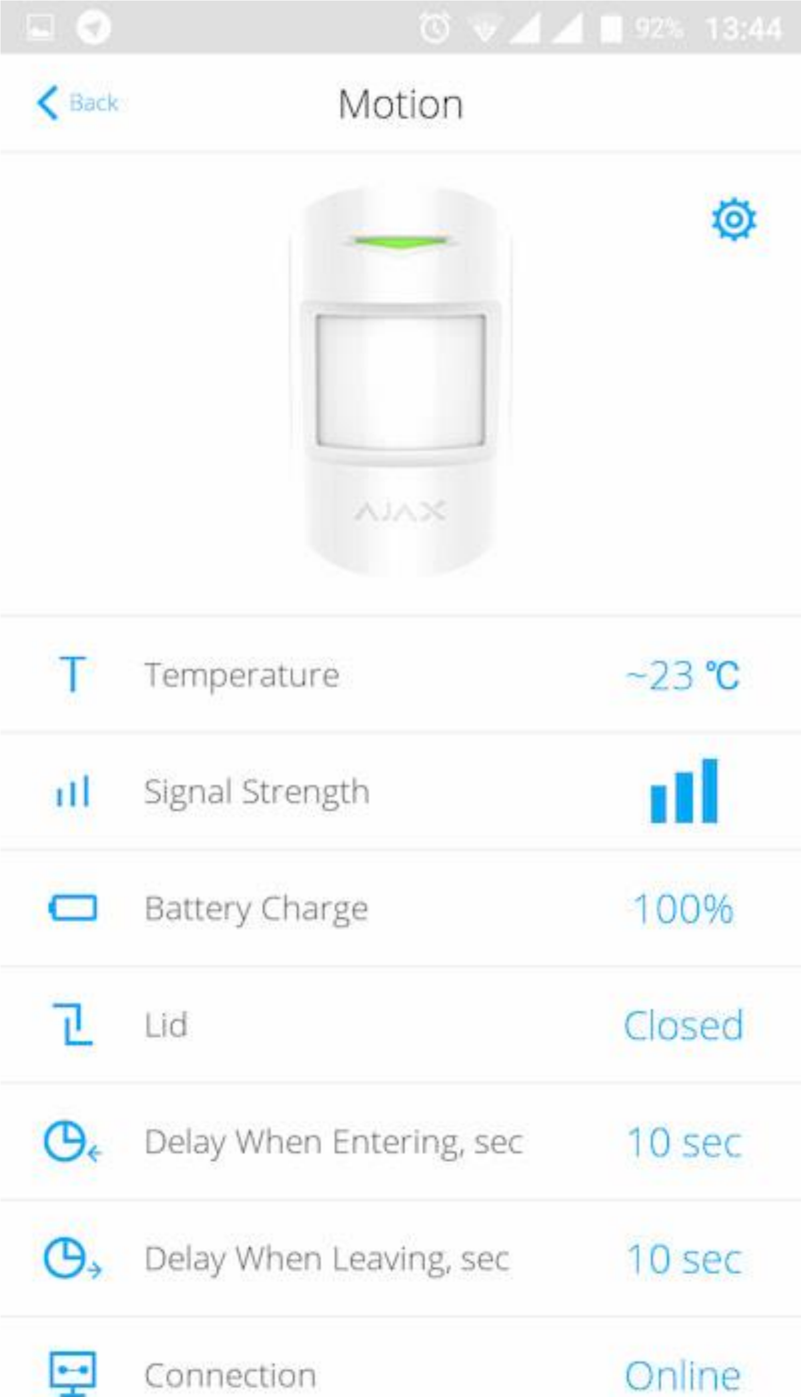
The connected detector will appear in the devices list in the application. Update of the detector statuses in the list depends on the device inquiry time set in the hub settings(default value is 36 seconds).

Connecting the Detector to Third Party security systems

To connect the detector to a third party security central unit with the uartBridge or ocBridge Plus integration module, follow the recommendations in the manuals of these devices.

States

1. Devices
2. MotionProtect | **MotionProtect Plus**

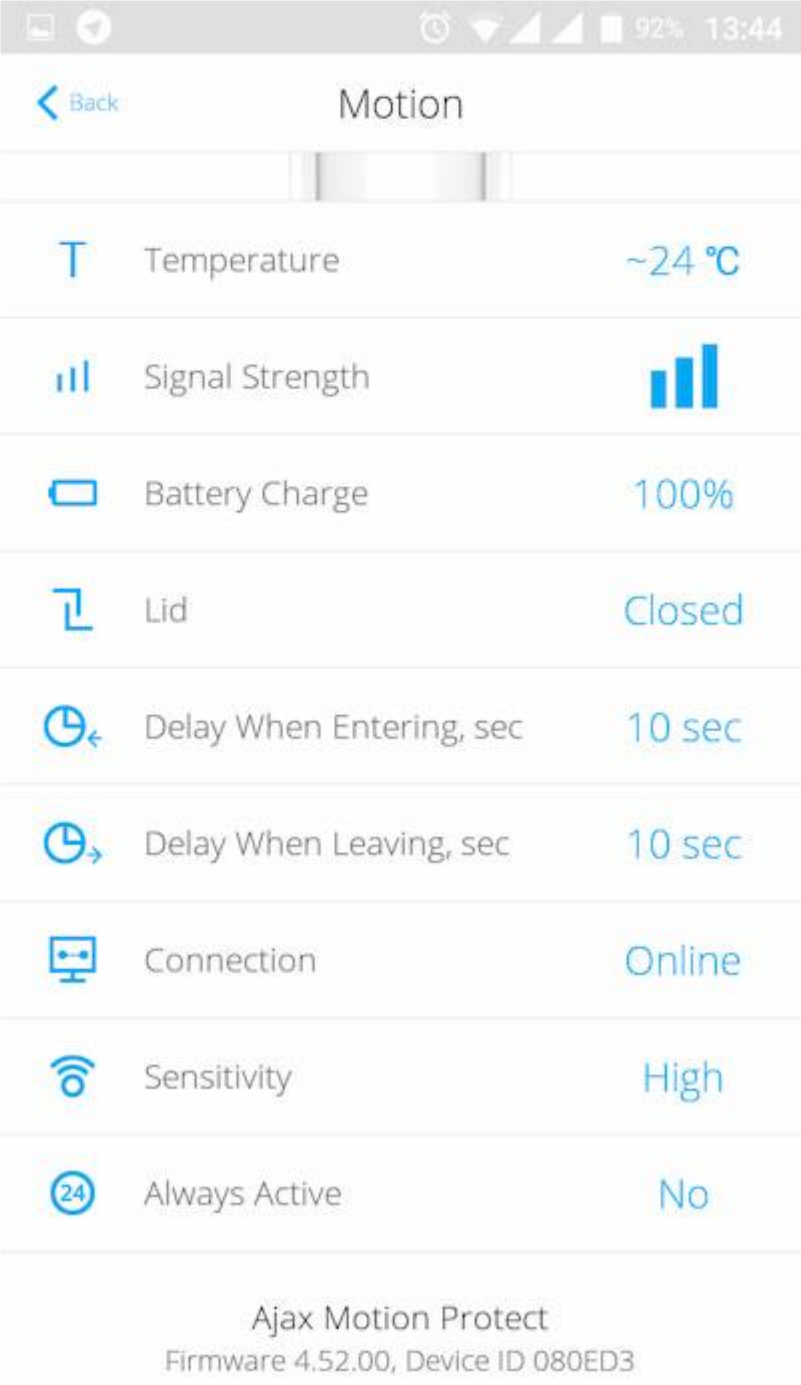


92% 13:44

Back

Motion

Temperature	~23 °C
Signal Strength	▂▅█
Battery Charge	100%
Lid	Closed
Delay When Entering, sec	10 sec
Delay When Leaving, sec	10 sec
Connection	Online



Motion

Temperature	~24 ℃
Signal Strength	
Battery Charge	100%
Lid	Closed
Delay When Entering, sec	10 sec
Delay When Leaving, sec	10 sec
Connection	Online
Sensitivity	High
Always Active	No

Ajax Motion Protect

Firmware 4.52.00, Device ID 080ED3

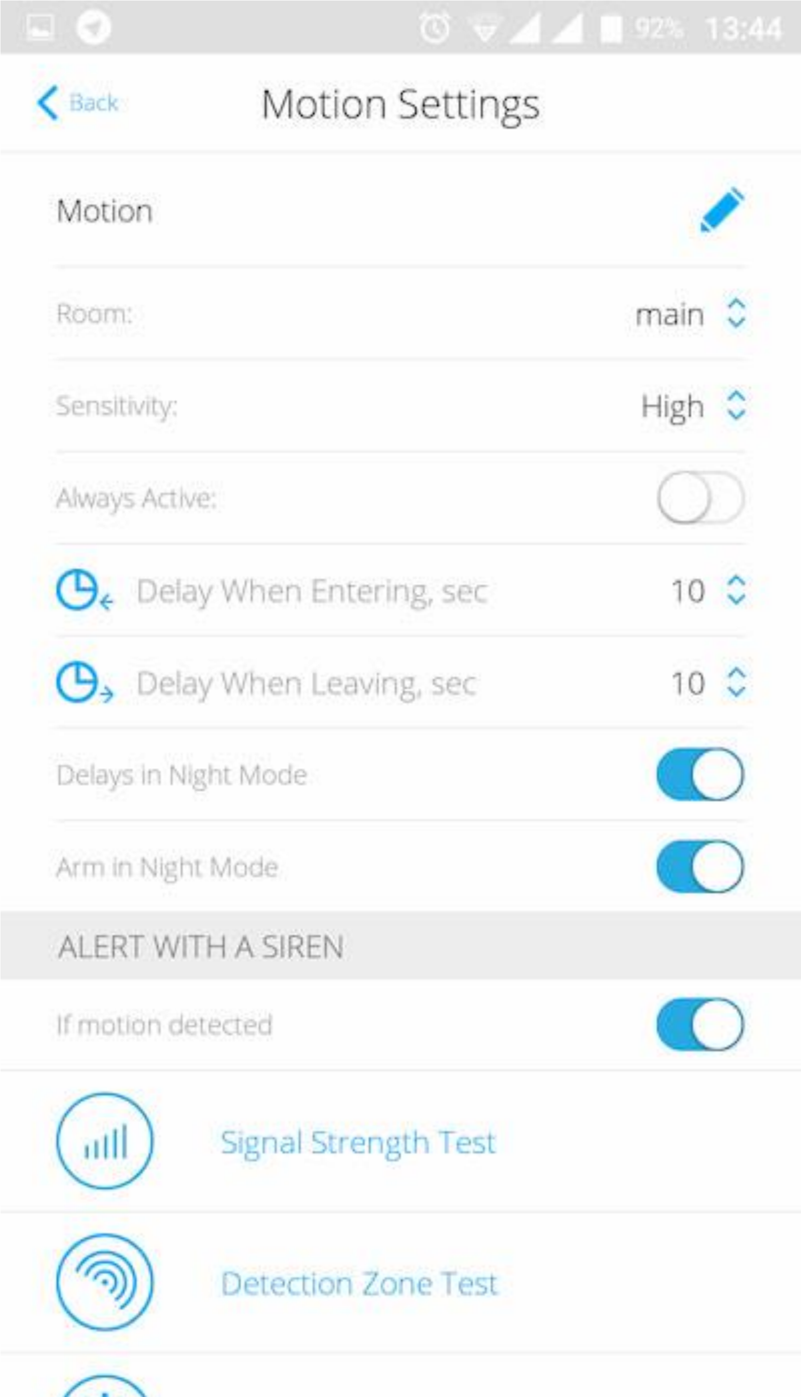
Parameter	Value
Temperature	Temperature of the Detector. Measured on the processor and changes gradually
Jeweller Signal Strength	Signal strength between the hub and the detector
Connection	Connection status between the hub and the detector
Battery Charge	Battery level of the detector, displayed in increments of 25%
Lid	The tamper mode of the detector, which reacts to the detachment of or damage of the body
Delay when entering, sec	Delay time when entering
Delay when leaving, sec	Delay time when exiting
Routed through ReX	Displays the status of using the ReX range extender
Sensitivity	Sensitivity level of the motion sensor
Always Active	If active, the motion detector is always in the armed mode
Firmware	Detector firmware version
Device ID	Device identifier

Settings

1. Devices

2. MotionProtect | **MotionProtect Plus**

3. Settings



Motion Settings

Motion

Room: main

Sensitivity: High

Always Active: ○

Delay When Entering, sec 10

Delay When Leaving, sec 10

Delays in Night Mode ●

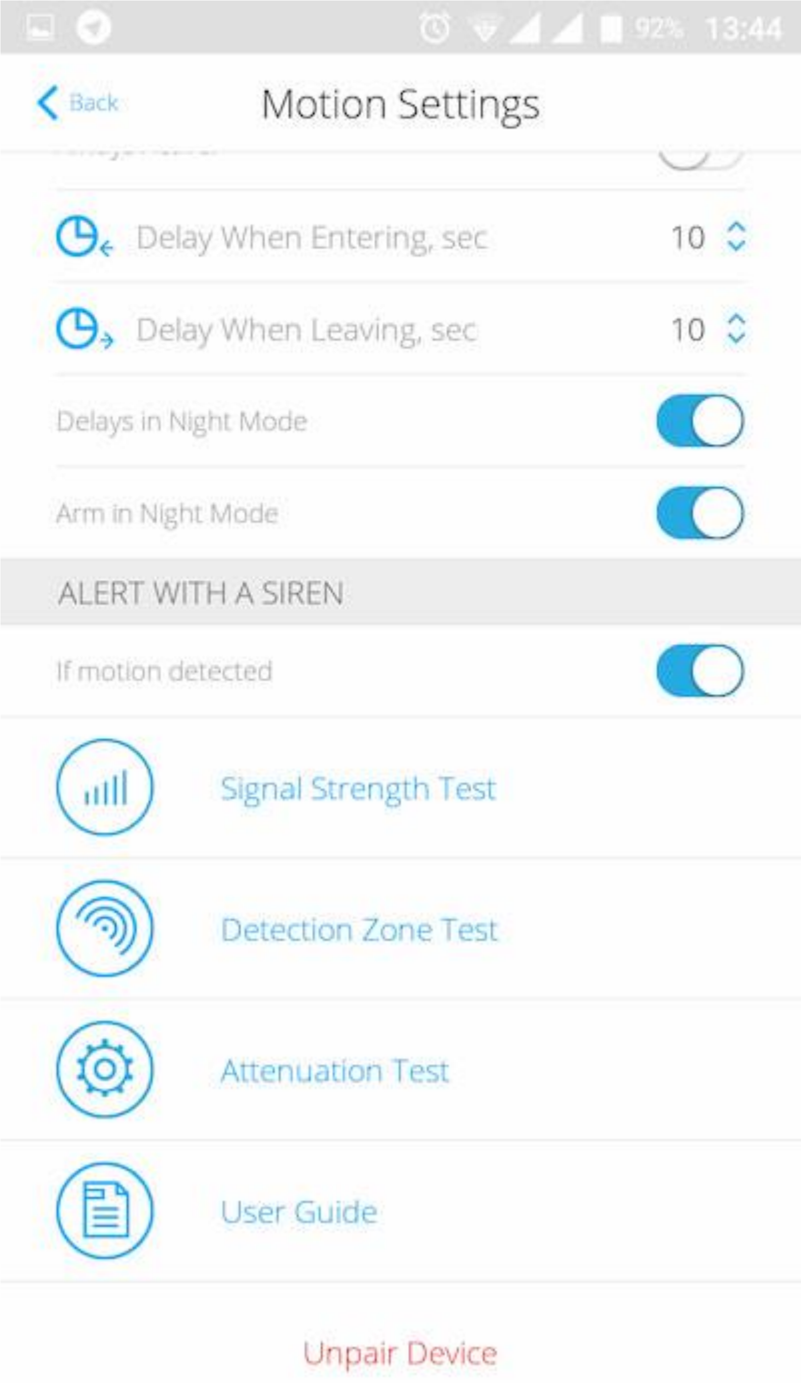
Arm in Night Mode ●

ALERT WITH A SIREN

If motion detected ●

Signal Strength Test

Detection Zone Test



92% 13:44

Back

Motion Settings

Delay When Entering, sec 10

Delay When Leaving, sec 10

Delays in Night Mode ●

Arm in Night Mode ●

ALERT WITH A SIREN

If motion detected ●

Signal Strength Test

Detection Zone Test

Attenuation Test

User Guide

Unpair Device

Setting	Value
First field	Detector name, can be edited
Room	Selecting the virtual room to which the device is assigned
Delay when entering, sec	Selecting delay time when entering
Delay when leaving, sec	Selecting delay time on exit
Delays in night mode	Delay turned on when using night mode
Arm in night mode	If active, the detector will switch to armed mode when using night mode
Sensitivity	Choosing the sensitivity level of the motion sensor. **For MotionProtect:** **High** — for premises with a minimum amount of obstacles, motion is detected as quickly as possible **Medium** — for premises with potential obstacles (windows, air conditioner, heating element, etc) **Low** — ignore pets weighing up to 20 kg and up to 50 cm tall **For MotionProtect Plus:** **High —** the detector disregards cats (under 25 cm) **Medium** — disregards small dogs (under 35 cm)

	Low — disregards animals under 50 cm.
Always active	If active, the detector always registers motion
Alert with a siren if motion detected	If active, HomeSiren and StreetSiren are activated when the motion detected
Jeweller Signal Strength Test	Switches the detector to the signal strength test mode
Detection Zone Test	Switches the detector to the detection area test
Attenuation test	Switches the detector to the signal attenuation test mode (available in detectors with **firmware version 3.50 and later**)
User Guide	Opens the User Guide
Unpair device	Disconnects the detector from the hub and deletes its settings

Before using the detector as a part of the security system, set up the suitable sensitivity level.

Switch the **Always Active** if the detector is located in a room requiring 24-hour control. Regardless of whether the system is set in the armed mode, you will receive notices of any detected motion.

If any motion is detected, the detector activates the LED for 1 second and transmits an alarm signal to the hub and then to the user and central monitoring station (if it is connected).

Detector operation indication

Event	Indication	Note
Turning on the detector	Lights up green for about one second	
Detector connection to the hub, ocBridge and uartBridge	Lights up continuously for a few seconds	
Alarm / tamper activation	Lights up green for about one second	Alarm is sent once in 5 seconds
Battery needs replacing	During the alarm,slowly lights up and goes off green	Replacement of the detector battery is described in the **Battery Replacement** paragraph

Detector Testing

The Ajax security system allows conducting tests for checking the functionality of connected devices.

The tests do not start immediately but within a period of 36 seconds when using the standard settings. The time of the start depends on the settings of the detector polling period (the paragraph on **Jeweller** settings in the hub settings).

Jeweller Signal Strength Test

Detection Zone Test

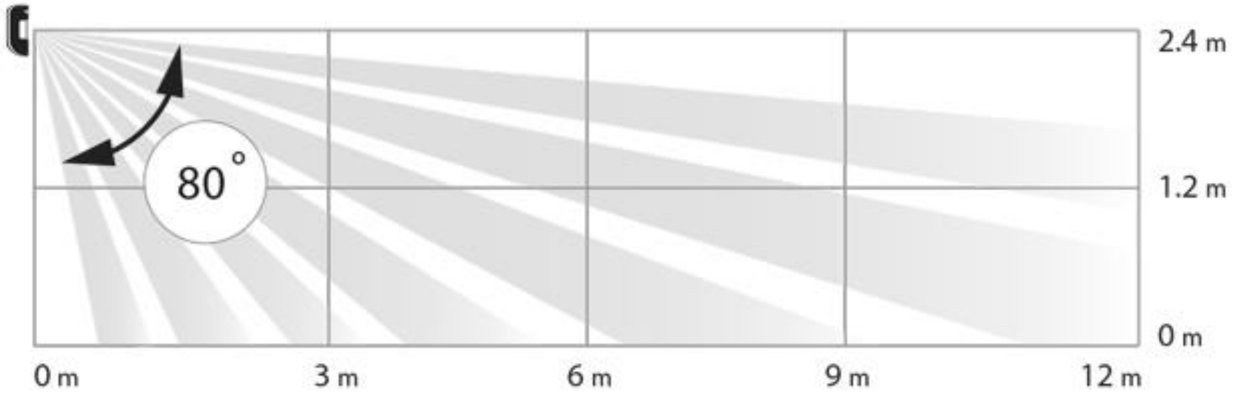
Attenuation test

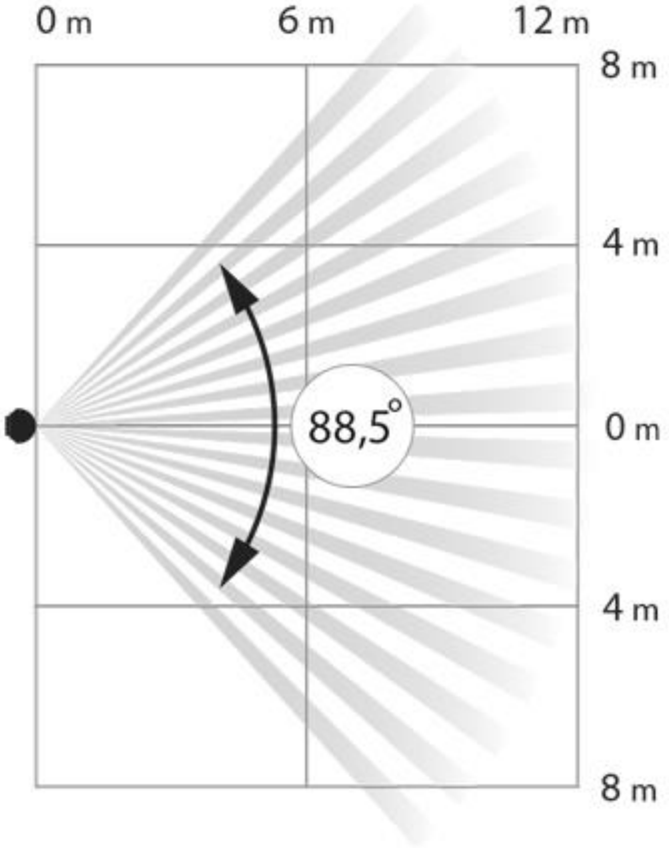
Device installation

Selection of the Detector Location

The controlled area and the efficiency of the security system depends on the location of the detector.

Location of MotionProtect depends on the remoteness from the hub and presence of any obstacles between the devices hindering the radio signal transmission: walls, inserted floors, large-size objects located within the room.





Check the signal level at the installation location

If the signal level is at one bar, we cannot guarantee stable operation of the security system. Take all possible measures to improve the quality of the signal! As a minimum, move the device – even 20 cm shift can significantly improve the quality of reception.

If after moving the device still has a low or unstable signal strength, use the ReX radio signal range extender.

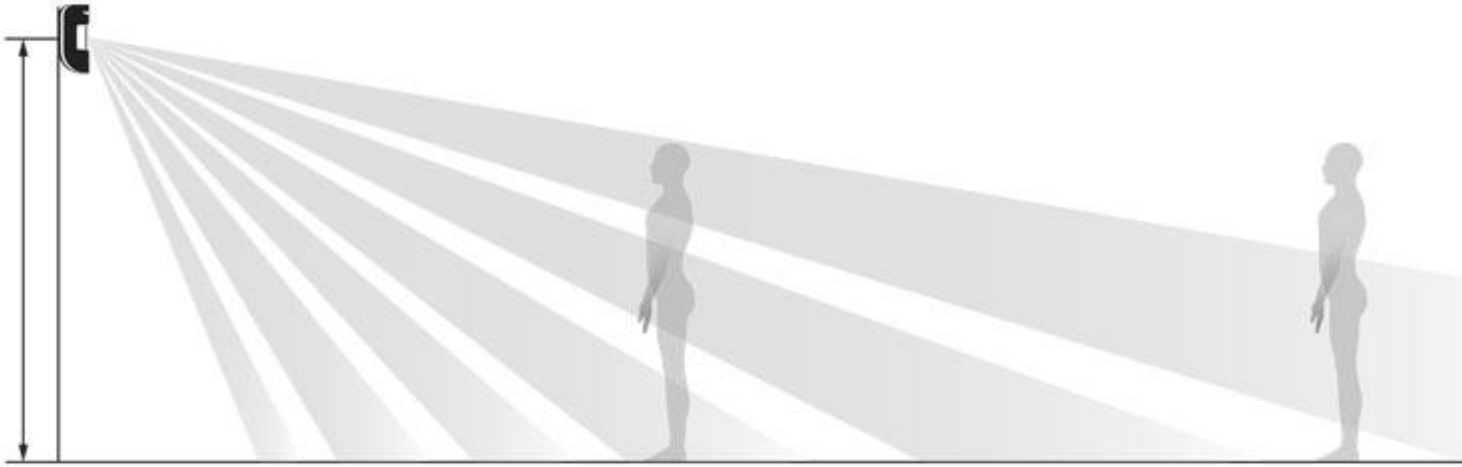
The direction of the detector lens should be perpendicular to the probable way of intrusion into the room

Make sure that any furniture, domestic plants, vases, decorative or glass structures do not block the field of view of the detector.

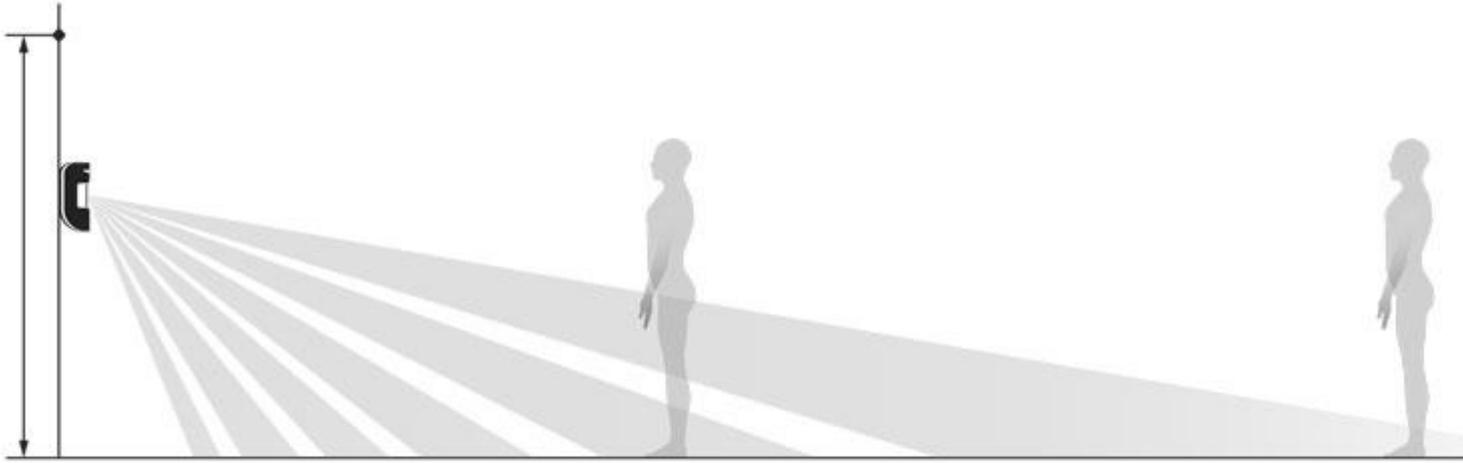
We recommend installing the detector at the height of 2,4 meters.

If the detector is not installed at the recommended height, this will reduce the area of the motion detection zone and impair the operation of the function of ignoring animals.

✓ h = 2,4 m

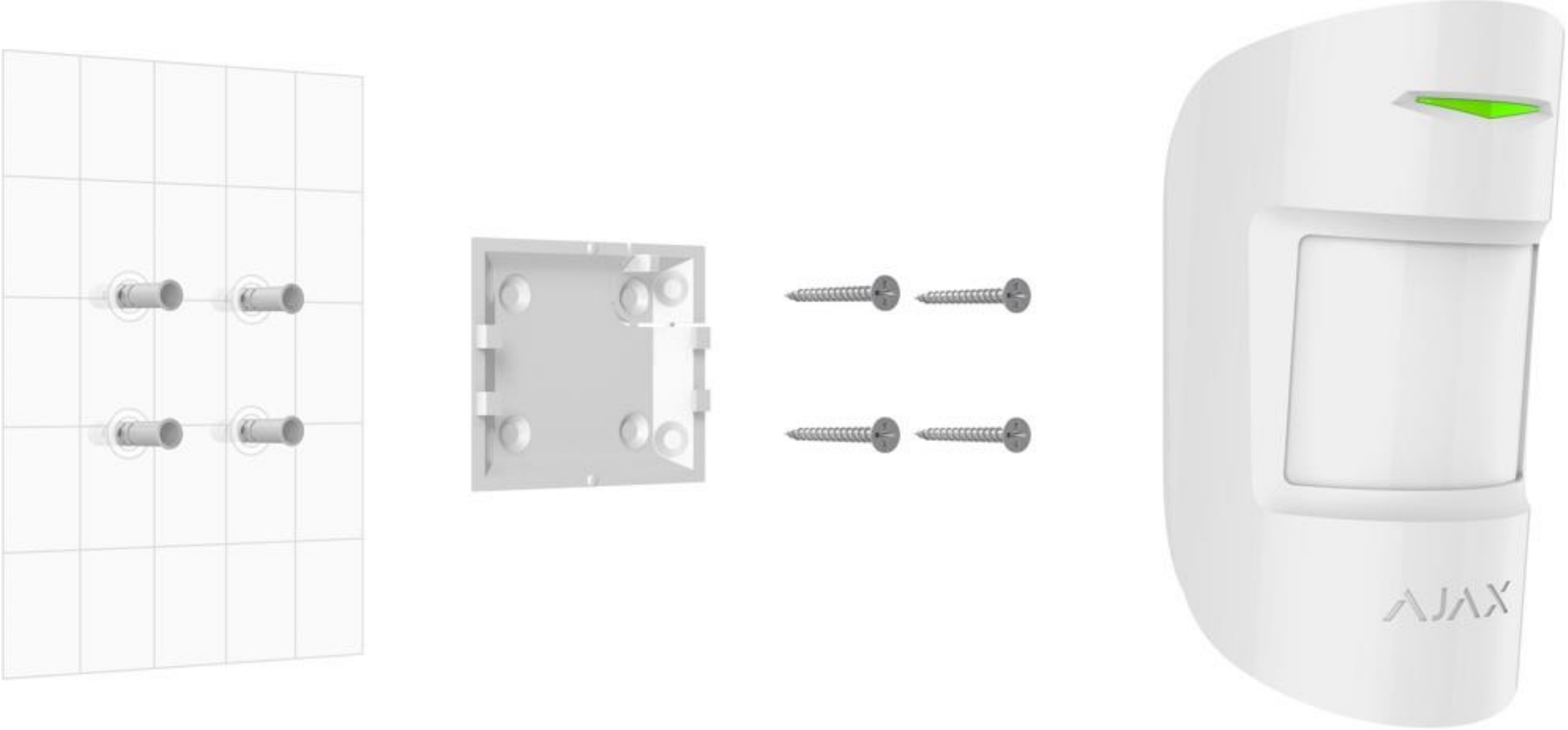


✗ h < 2,4 m

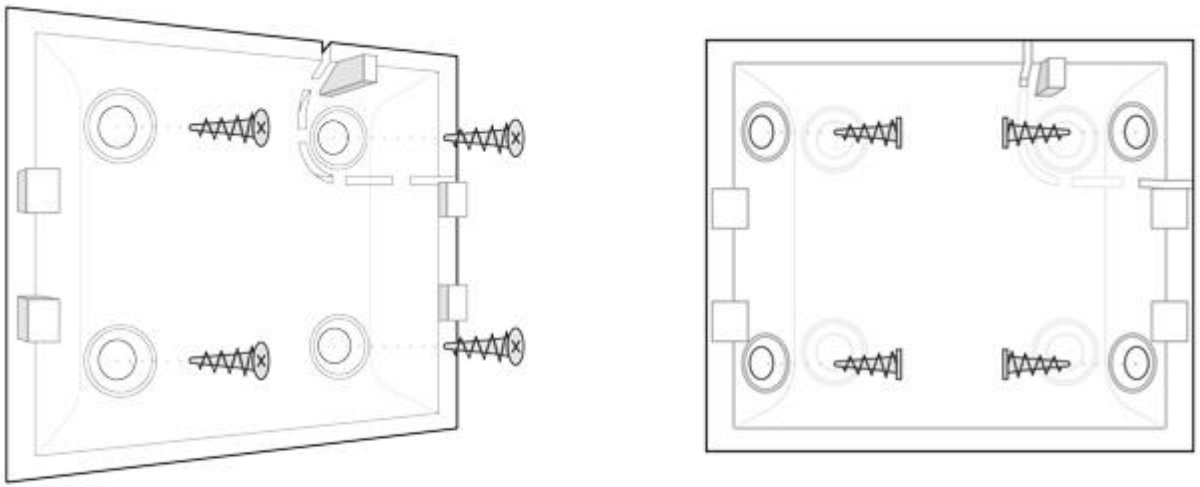


Installation of the Detector

Before installing the detector, make sure that you have selected the optimal location and it is in compliance with the guidelines contained in this manual



The Ajax MotionProtect detector (**MotionProtect Plus**) should be attached to a vertical surface or in the corner.



1. Attach the SmartBracket panel to the surface using bundled screws, using at least two fixing points (one of them – above the tamper). After selecting other attachment screws, make sure that they do not damage or deform the panel.

The double-sided adhesive tape may only be used for temporary attachment of the detector. The tape will run dry in the course of time, which may result in the falling of the detector and actuation of the security system. Furthermore, hitting can damage the device.

2. Put the detector on the attachment panel. When the detector is fixed in SmartBracket, it will blink with an LED – this will be a signal that the tamper on the detector is closed.

   If the LED indicator of the detector is not actuated after installation in SmartBracket, check the status of the tamper in the Ajax Security System application and then the fixing tightness of the panel.

If the detector is torn off from the surface or removed from the attachment panel, you will receive the notification.

Do not install the detector:

1. outside the premises (outdoors)
2. in the direction of the window, when the detector lens is exposed to direct sunlight (you can install **MotionProtect Plus**)
3. opposite any object with the rapidly changing temperature (e.g., electrical and gas heaters) (you can install **MotionProtect Plus**)
4. opposite any moving objects with a temperature close to that of the human body (oscillating curtains above the radiator) (you can install **MotionProtect Plus**)
5. at any places with fast air circulation (air fans, open windows or doors) (you can install **MotionProtect Plus**)
6. nearby any metal objects or mirrors causing attenuation and screening of the signal
7. within any premises with the temperature and humidity beyond the range of permissible limits
8. closer than 1 m from the hub.

Detector Maintenance

Check the operational capability of the Ajax MotionProtect detector on a regular basis.

Clean the detector body from dust, spider webs and other contaminants as they appear. Use soft dry napkin suitable for equipment maintenance.

Do not use any substances containing alcohol, acetone, gasoline and other active solvents for cleaning the detector. Wipe the lens very carefully and gently – any scratches on the plastic may cause reduction of the detector sensitivity.

The pre-installed battery ensures up to 7 years (**MotionProtect Plus** up to 5 years) of autonomous operation (with the inquiry frequency by the hub of 3 minutes). If the detector battery is discharged, the security system will send respective notices and the LED will smoothly lights up and goes out, if the detector detects any motion or if the tamper is actuated.

Battery Replacement

Tech specs

Sensitive element	PIR sensor (**Motion Protect Plus:** PIR and microwave sensor)
Motion detection distance	Up to 12 m
Motion detector viewing angles (H/V)	88,5° / 80°

Pet immunity	Yes, height up to 50 cm, weight up to 20 kg Why motion detectors react to animals and how to avoid it >
Tamper protection	Yes
Frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz, depending on the sales region
Compatibility	Operates with Hub, Hub Plus, Hub 2, ReX, ocBridge Plus, uartBridge
Maximum RF output power	Up to 20 mW
Modulation of the radio signal	GFSK
Radio signal range	Up to 1700 m (any obstacles absent) (**Motion Protect Plus** up to 1200 m)

Power supply	1 battery CR123A, 3 V
Battery life	Up to 7 years (**Motion Protect Plus** up to 5 years)
Operating temperature range	From -10°C to +40°C
Operating humidity	Up to 75%
Overall dimensions	110 x 65 x 50 mm
Weight	86 g (**Motion Protect Plus** – 96 g)
Certification	Security Grade 2, Environmental Class I in conformity with the requirements of EN 50131-1, EN 50131-2-2, EN 50131-5-3 (**Motion Protect Plus** – EN 50131-1, EN 50131-2-4, EN 50131-5-3)

Complete Set

1. MotionProtect (**MotionProtect Plus**)
2. SmartBracket mounting panel
3. Battery CR123A (pre-installed)
4. Installation kit
5. Quick Start Guide

Warranty

Warranty for the “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase and does not apply to the pre-installed battery.

If the device does not work correctly, you should first contact the support service—in half of the cases, technical issues can be solved remotely!

The full text of the warranty

User Agreement

Technical support: support@ajax.systems

DoorProtect User Manual

Updated January 2, 2020

DoorProtect is a wireless door and window opening detector designed for indoor use. It can operate up to 7 years from a pre-installed battery and capable to detect more than one million openings. DoorProtect has a socket for connecting an external detector.

The functional element of DoorProtect is a sealed contact reed relay. It consists of ferromagnetic contacts placed in a bulb that form a continuous circuit under the effect of a constant magnet.

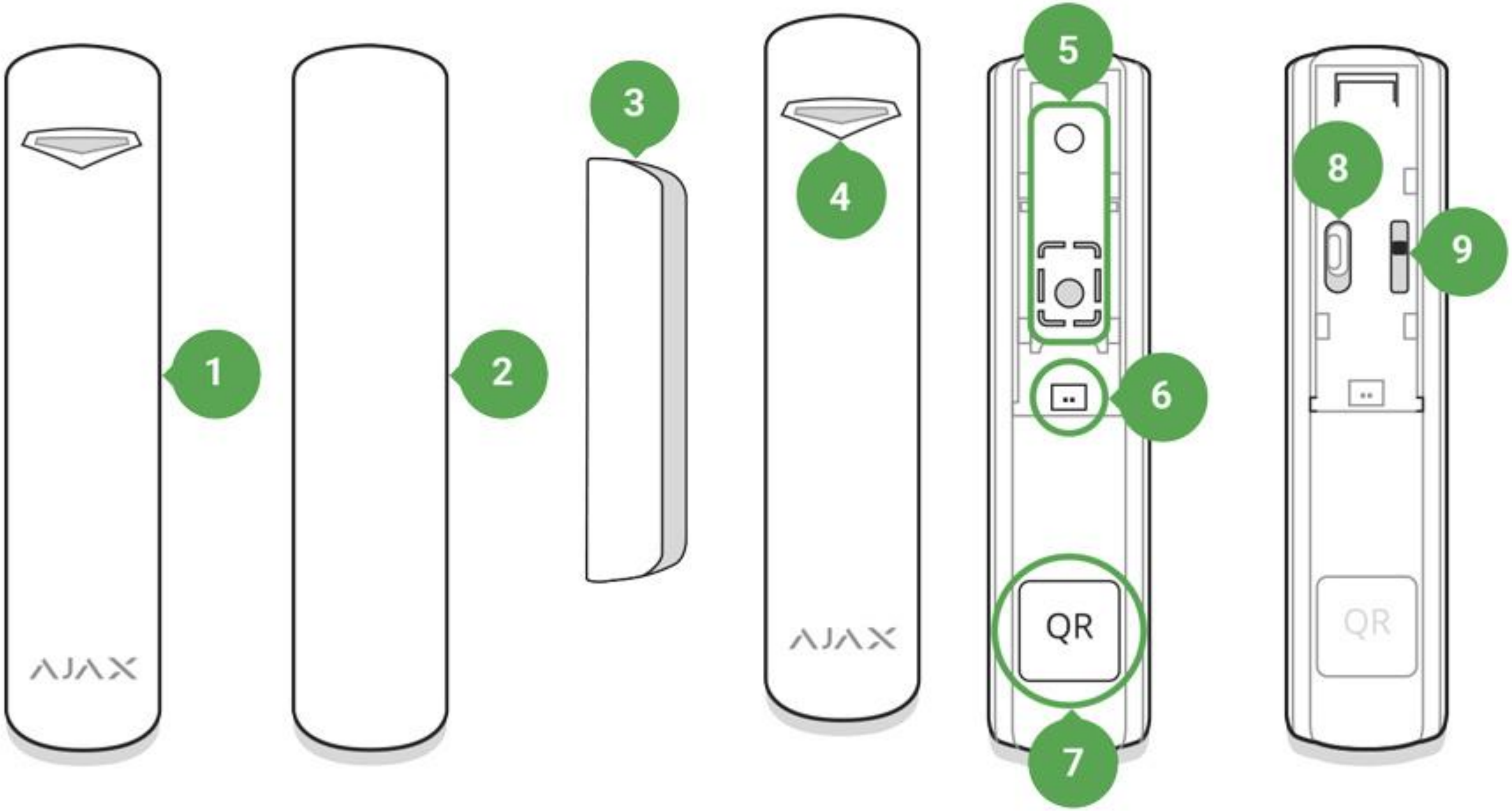
DoorProtect operates within the Ajax security system, connecting via the protected Jeweller radio protocol. Communication range is up to 1,200 m in the line of sight. Using the uartBridge or ocBridge Plus integration modules, DoorProtect can be used as part of third party security systems.

The detector is set up via Ajax apps for iOS, Android, macOS and Windows. The app notifies user of all events through push notifications, SMS and calls (if activated).

The Ajax security system is self-sustaining, but the user can connect it to the central monitoring station of a private security company.

Buy opening detector DoorProtect

Functional Elements



1. DoorProtect
2. Big magnet

3. Small magnet
4. LED indicator
5. SmartBracket attachment panel (perforated part is required for actuating the tamper in case of any attempt to dismantle the detector. Don’t break it out!)
6. External detector connection socket
7. QR code
8. Device switch
9. Tamper button

Operating Principle

DoorProtect consists of two parts: the detector with a sealed contact reed relay, and the constant magnet. Attach the detector to the door frame, while the magnet can be attached to the moving wing or sliding part of the door. If the sealed contact reed relay is within the coverage area of the magnetic field, it closes the circuit, which means thatthe detector is closed. The opening of the door pushes out the magnet from the sealed contact reed relay and opensing the circuit In such a way, the detector recognizes the opening.

A small magnet works at a distance of 1 cm, and the big one — up to 2 cm.

After actuation, DoorProtect immediately transmits the alarm signal to the hub, activating the sirensand notifying the user and security company.

Pairinging the Detector

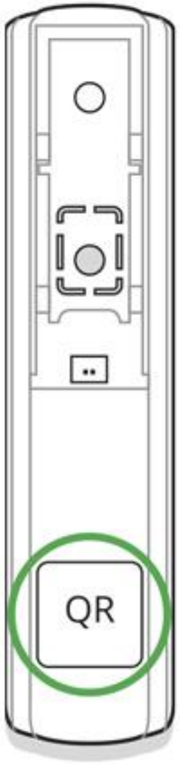
Before starting pairing:

1. Following the hub instruction recommendations, install the Ajax app on your smartphone. Create an account, add the hub to the app, and create at least one room.
2. Go to the Ajax app.
3. Switch on the hub and check the internet connection (via Ethernet cable and/or GSM network).
4. Make sure that the hub is disarmed and does not update by checking its status in the app.

Only users with administor rights can add the device to the hub.

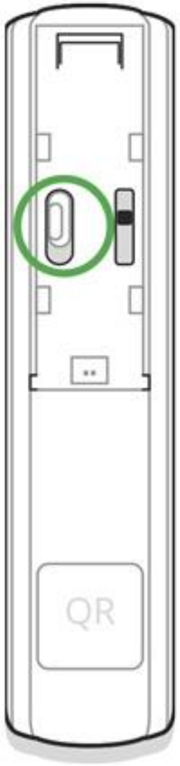
How to pair the detector with the hub:

1. Select the **Add Device** option in the Ajax app.
2. Name the device, scan/write manually the **QR Code** (located on the body and packaging), and select the location room.



3. Select **Add** — the countdown will begin.

4. Switch on the device.



For detection and pairing to occur, the detector should be located within the coverage area of the wireless network of the hub (at a single protected object).

The request for connection to the hub is transmitted for a short period of time at the moment of switching on the device.

If pairing with the hub failed, switch off the detector for 5 seconds and retry it.

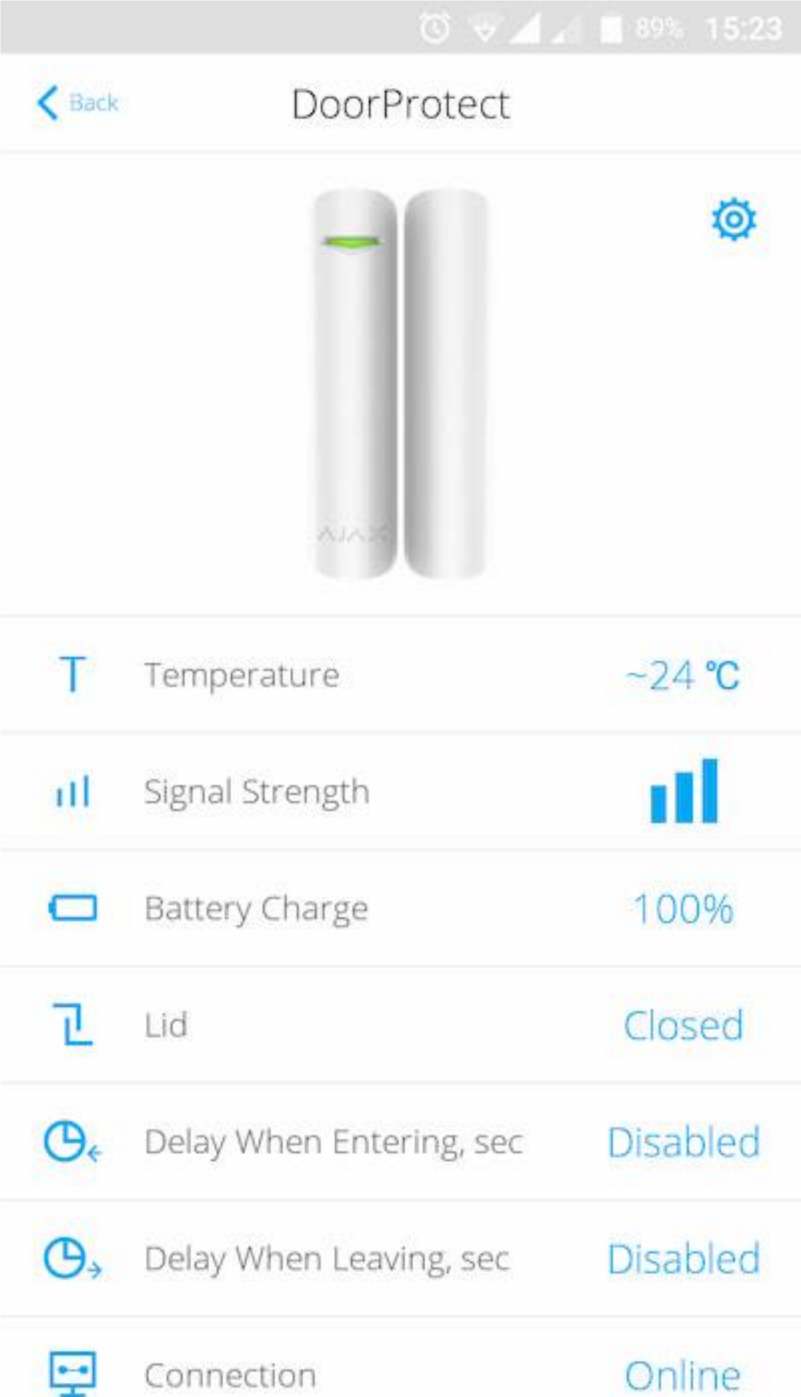
If the detector has paired with the hub,it will appear in the list of devices in the Ajax app. The update of the detectors statuses in the list depends on the detector ping interval set in the hub settings. he default value is 36 seconds.

Connecting to Third Party Security Systems

To connect the detector to a third party security central unit using the uartBridge or ocBridge Plus integration modules, follow the recommendations in the manual of the respective device.

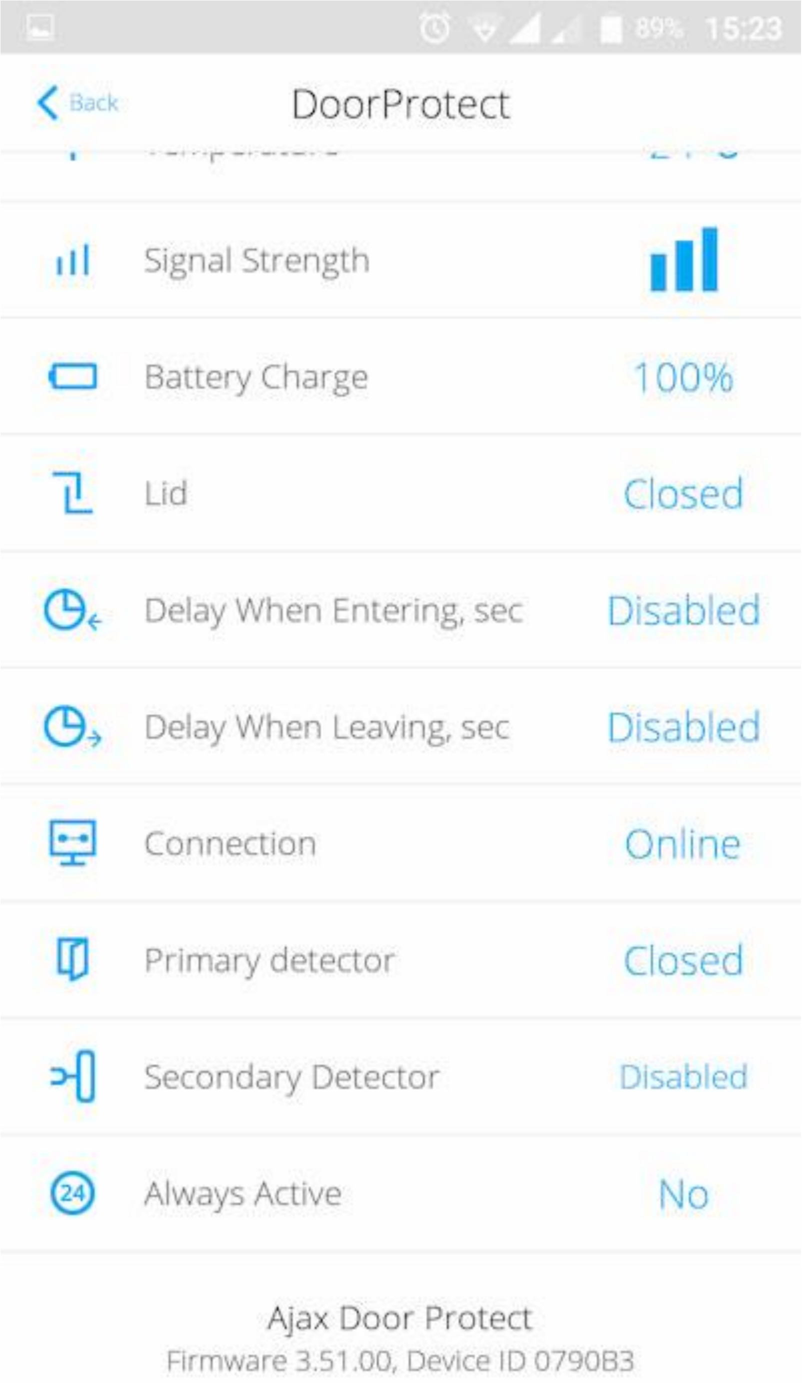
States

1. Devices
2. DoorProtect



DoorProtect

Temperature	~24 ℃
Signal Strength	▮▮▮
Battery Charge	100%
Lid	Closed
Delay When Entering, sec	Disabled
Delay When Leaving, sec	Disabled
Connection	Online



89% 15:23

Back

DoorProtect

Signal Strength	▂▅▇
Battery Charge	100%
Lid	Closed
Delay When Entering, sec	Disabled
Delay When Leaving, sec	Disabled
Connection	Online
Primary detector	Closed
Secondary Detector	Disabled
Always Active	No

Ajax Door Protect

Firmware 3.51.00, Device ID 0790B3

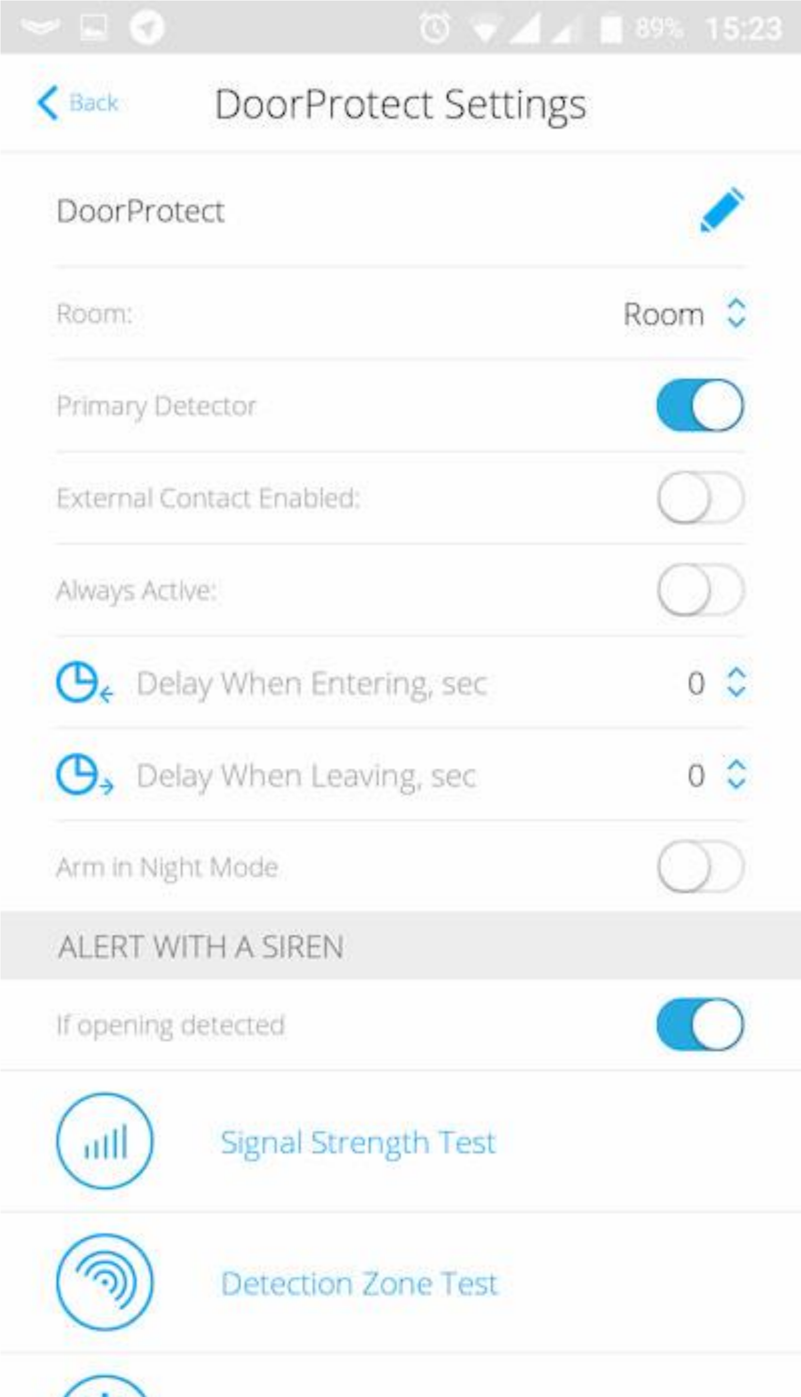
Parameter	Value
Temperature	The temperature of the detector. The temperature is measured on the processor and changes gradually
Jeweller Signal Strength	The signal strength between the hub and the detector
Connection	The connection status between the hub and the detector
Battery Charge	The battery level of the detector, displayed in increments of 25%
Lid	The tamper state, which reacts to detachment or damaging of the detector body
Delay When Entering, sec	The delay time when entering
Delay When Leaving, sec	The delay time when exiting
Routed Through Rex	Indicates if the detector is routed through a radio signal range extender
Primary Detector	The primary detector status
Secondary Detector	The status of the external detector connected to DoorProtect
Always Active	If active, the detector is always in the armed mode
Firmware	The detector firmware version
Device ID	The device identifier

Setting Up

1. Devices

2. DoorProtect

3. Settings



89% 15:23

Back

DoorProtect Settings

DoorProtect

Room: Room

Primary Detector ●

External Contact Enabled: ○

Always Active: ○

Delay When Entering, sec 0

Delay When Leaving, sec 0

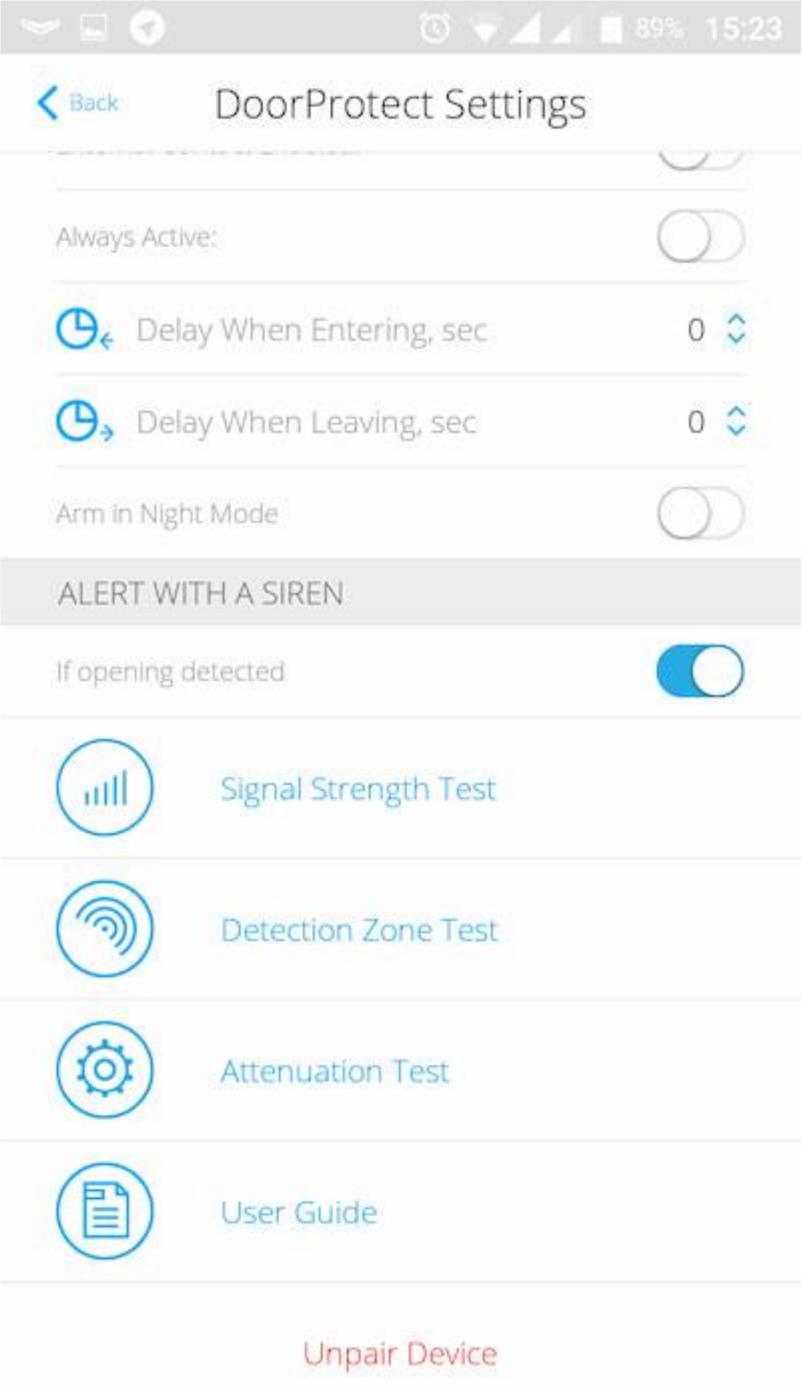
Arm in Night Mode ○

ALERT WITH A SIREN

If opening detected ●

Signal Strength Test

Detection Zone Test



Always Active: ○

Delay When Entering, sec 0

Delay When Leaving, sec 0

Arm in Night Mode ○

ALERT WITH A SIREN

If opening detected ●

Setting	Value
First field	The detector name, can be edited
Room	Selecting the virtual room to which the device is assigned
Delay When Entering, sec	Setting the delay time when entering
Delay When Leaving, sec	Setting the delay time on exit
Delays in night mode	Delay turned on when using night mode
Arm in Night Mode	If active, the detector will switch to the armed mode when using the night mode
Primary Detector	If active, DoorProtect primarily reacts to opening/closing
External Contact Enabled	If active, the detector registers external detector alarms
Always active	If active, the detector always registers opening/closing
Activate the siren if the door or window is open	If active, HomeSiren and StreetSiren are activated when the opening detected
Activate the siren if an external contact opened	If active, HomeSiren and StreetSiren are activated during an external detector alarm
Jeweller Signal Strength Test	Switches the detector to the signal strength test mode
Detection Zone Test	Switches the detector to the detection area test
Attenuation Test	Switches the detector to the signal attenuation test mode (available for detectors with **firmware version 3.50 and later**)
User Guide	Opens the detector User Guide

Unpair Device	Disconnects the detector from the hub and deletes its settings

Indication

Event	Indication	Note
Switching on the detector	Lights up green for about one second	
Detector connecting to the hub, ocBridge and uartBridge	Lights up for a few seconds	
Alarm / tamper activation	Lights up green for about one second	Alarm is sent once in 5 seconds
Battery needs replacing	During the alarm, it slowly lights up green and slowly goes out	Replacement of the detector battery is described in the **Battery Replacement** paragraph

Functionality Testing

The Ajax security system allows conducting tests for checking the functionality of connected devices.

The tests do not start immediately but within 36 seconds by default. The starting time depends on the ping interval (the paragraph on “**Jeweller**” settings in hub settings).

Jeweller Signal Strength Test

Detection Zone Test

Attenuation Test

Installing the Detector

Selecting the location

Location of DoorProtect is determined by its remoteness from the hub and presence of any obstacles between the devices hindering the radio signal transmission: walls, inserted floors, large objects located within the room.

Check the signal level at the installation location

If the signal level is low (one bar), we cannot guarantee stable operation of the security system. Take all possible measures to improve the quality of the signal! As a minimum, move the device — even 20 cm shift can significantly improve the quality of the reception.

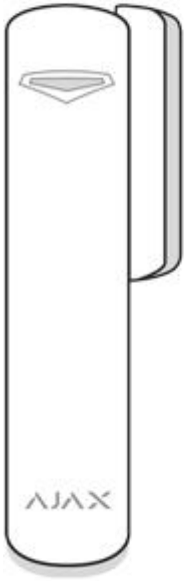
If, after moving, the device still has a low or unstable signal strength, use the ReX radio signal range extender.

The detector is located either inside or outside of the door case (window frame):

When installing the detector in the perpendicular planes (inside the case/frame), use the small magnet. The distance between the magnet and detector should not exceed 1 cm.

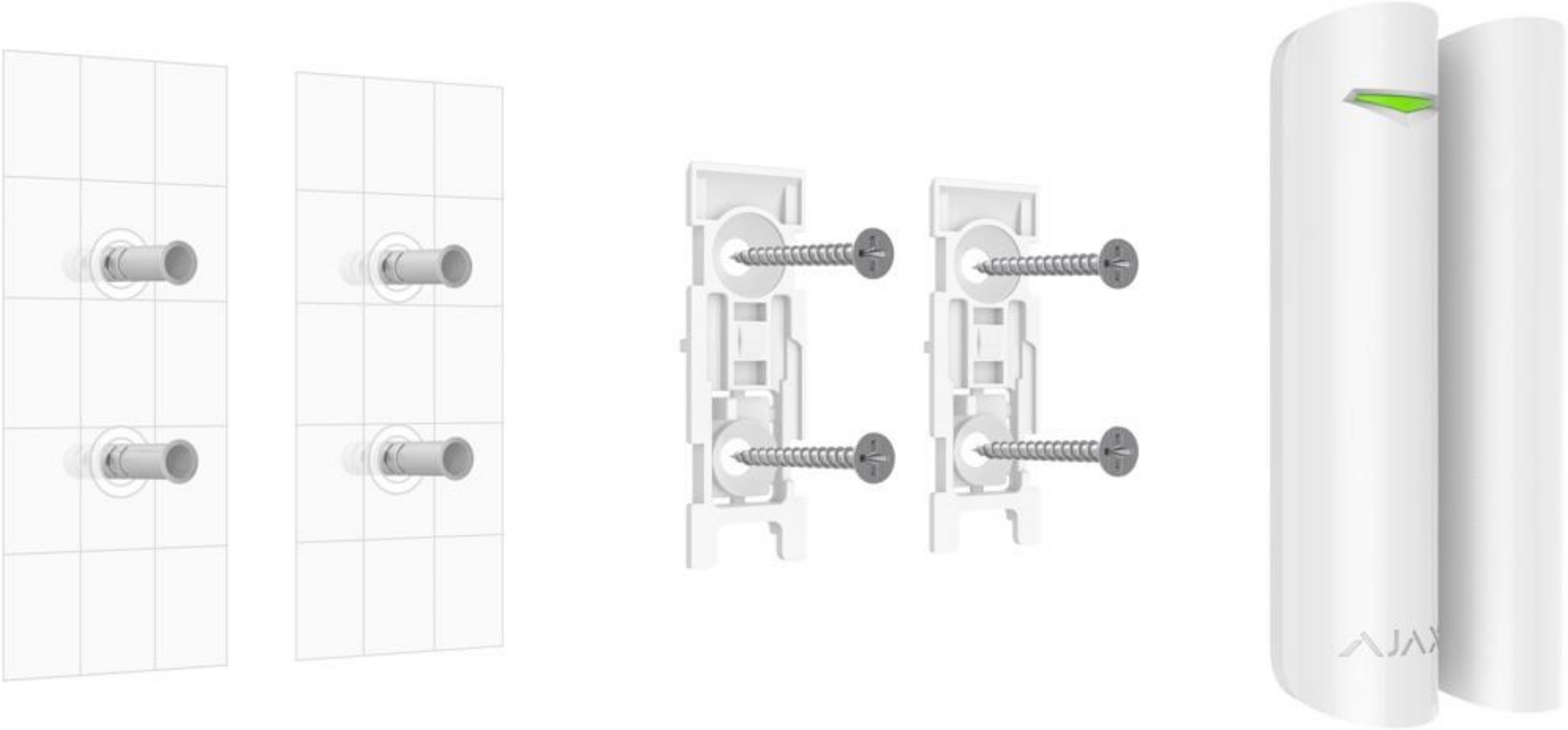
When positioning the parts of DoorProtect in the same plane, use the big magnet. Its actuation threshold — 2 cm.

Attach the magnet to the moving part of the door (window) to the right of the detector. If necessary, the detector may be overturned or positioned horizontally.



Installing the detector

Before installing the detector, make sure that you have selected the optimal location and it complies with the guidelines of this manual!



1. Fix the SmartBracket attachment panels and the magnet using the bundled screws. If using any other attachment hardware, make sure that they do not damage or deform the panel.

> Double-sided adhesive tape may be only used for temporary attachment. The tape will run dry in the course of time, which may result in falling of DoorProtect and actuation of the security system. Furthermore, the device may fail from a hit.

2. Put the detector on the attachment panel. As soon as the detector is fixed in SmartBracket, it will blink with a LEDsignaling that the tamper is closed.

> If the light indicator do not blink after installing in SmartBracket, check the status of the tamper in the Ajax app and then the fixing tightness of the panel.

If the detector is torn off from the surface or removed from the attachment panel, you will receive a notification.

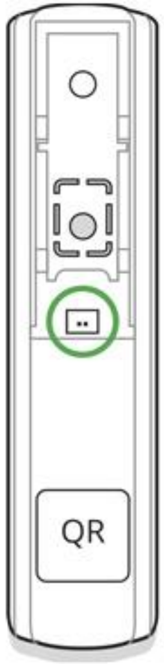
3. Put the magnet on the attachment panel.

Do not install the detector:

1. outside the premises (outdoors);
2. nearby any metal objects or mirrors causing attenuation or interference of the signal;
3. inside any premises with the temperature and humidity beyond the permissible limits;
4. closer than 1 m to the hub.

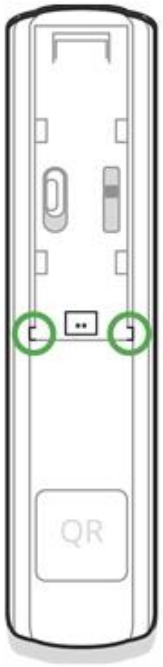
Connecting a Third-Party Wired Detector

A wired detector with the NC contact type can be connected to DoorProtect using the outside-mounted terminal clamp.



We recommend to install a wired detector at a distance not exceeding 1 meter – increasing the wire length will increase the risk of its damage and reduce the quality of communication between the detectors.

To lead out the wire from the detector body, break out the plug:



If the external detector is actuated, you will receive a notification.

Detector Maintenance and Battery Replacement

Check the operational capability of the DoorProtect detector on a regular basis.

Clean the detector body from dust, spider web and other contaminations as they appear. Use soft dry napkin suitable for equipment maintenance.

Do not use any substances containing alcohol, acetone, gasoline and other active solvents for cleaning the detector.

The battery lifetime depends on battery quality, actuation frequency of the detector and ping interval of the detectors by the hub.

If the door opens 10 times a day and the ping interval is 60 seconds, then DoorProtect will operate up to 7 years from the pre-installed battery. Setting the ping interval of 12 seconds, you will reduce the battery life to 2 years.

If the detector battery is discharged, you will receive a notification, and the LED will smoothly light up and go out, if the detector or tamper is actuated.

Battery Replacement

Tech specs

Sensor	Sealed contact reed relay
Detector actuation threshold	1 cm (small magnet) 2 cm (big magnet)
Tamper protection	Yes
Socket for connecting wire detectors	Yes, NC

Frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz depending on the region of sale
Compatibility	Operates with Hub, Hub Plus, Hub 2, ReX, ocBridge Plus, uartBridge
Maximum RF output power	Up to 20 mW
Modulation	GFSK
Radio signal range	Up to 1,200 m (any obstacles absent)
Power supply	1 battery CR123A, 3 V
Battery life	Up to 7 years
Operating temperature range	From -10°C to +40°C
Operating humidity	Up to 75%
Dimensions	Ø 20 x 90 mm
Weight	29 g
Certification	Security Grade 2, Environmental Class I in conformity with the requirements of EN 50131-1, EN 50131-2-6, EN 50131-5-3

Complete Set

1. DoorProtect
2. SmartBracket mounting panel
3. Battery CR123A (pre-installed)
4. Big magnet
5. Small magnet
6. Outside-mounted terminal clamp
7. Installation kit
8. Quick Start Guide

Warranty

Warranty for the “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase and does not apply to the pre-installed battery.

If the device does not work correctly, you should first contact the support service — in half of the cases, technical issues can be solved remotely!

The full text of the warranty

User Agreement

KeyPad User Manual

Updated December 10, 2019

KeyPad is a wireless touch-sensitive keypad controlling the Ajax security system. It arms and disarms a room from the guard mode, informs of the system status, is protected against code guessing and supports “silent alarm” if the code is entered by force.

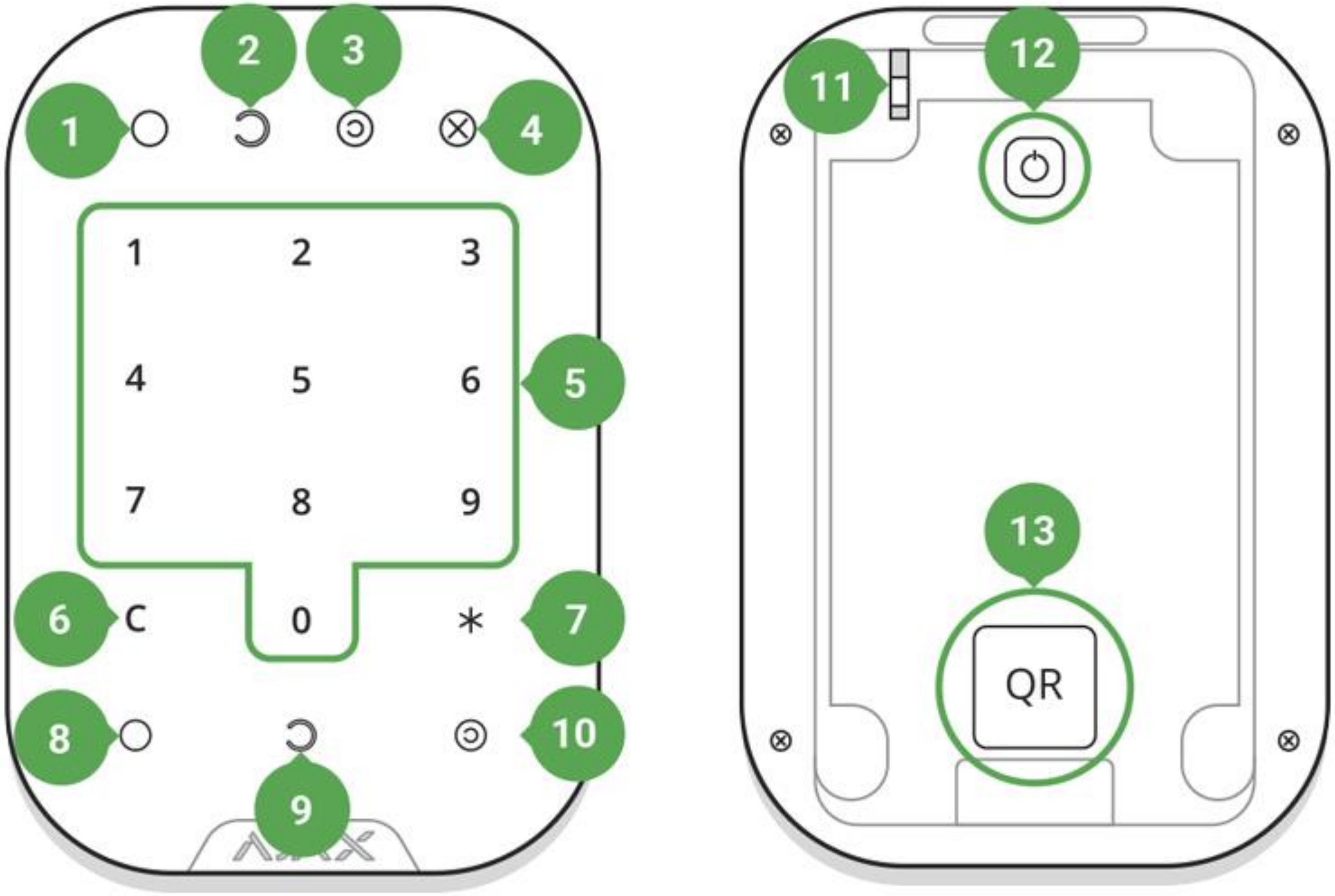
Keypad operates only with the Ajax security system (it may not be used in any third-party security systems), by connecting via the protected Jeweller protocol to the hub. Communication range – up to 1,700 meters, absent any obstacles.

Device works only with hub, and is not compatible with the uartBridge or ocBridge Plus.

The keypad is set up via a mobile application for iOS and Android-based smartphones.

Buy keypad KeyPad

Functional elements



1. Armed mode indicator
2. Disarmed mode indicator

3. Night mode indicator
4. Malfunction indicator
5. The numeric block of touch buttons
6. Clear button
7. Function button
8. Arming button
9. Disarming button
10. Night mode button
11. Tamper button
12. On/Off button
13. QR code

To remove the SmartBracket panel, slide it downward (perforated part is required for actuating the tamper in case of any attempt to tear off the detector from the surface).

Keypad Operating Principle

Keypad is a touch-sensitive keypad panel controlling the security system.

The keypad is a stationary keypad and is located inside a room. It allows to set the system in the armed mode with a digital code or by pressing one button, switch on the night mode, disarm the room, notify the private security company of the forcing to switch off the security system (by no means disclosing the user).

Keypad is furnished with light indicators signaling about the security system status, about any problems with the detectors or interruption of the communication with the hub. Big touch-sensitive buttons are highlighted, if the device is activated by touch – the code may be entered without external lighting. Service life from pre-installed batteries – up to 2 years.

Keypad operation indication

When the keypad wakes up, the LED lights, corresponding to the operating mode of the security system.

Indicators display the current status of the system: in armed mode / disarmed mode / night mode.

Information is up to date even if the status was changed by any other control device – application, fob. The status is updated if the device is waked up by touch.

Event	Indication
LED blinks (X)	Indicator notifies of a fault in the Ajax security system, as well as lights up, if the keypad cannot connect to the hub. You may check the nature of the fault in the Ajax Security System application

Pressing a touch-sensitive button	Short sound signal
The system is set in the armed mode	Short sound signal, LED lights up: “Armed mode” / “Night mode”
The system is disarmed	Two short sound signals, LED lights up: “Removed from the armed mode”
The incorrect master code is entered	Long sound signal, the highlight of the digital block blinks 3 times during the signal sound
The hub refuses to set the system in the armed mode (e.g., a window is opened)	Long sound signal, the current status indicator blinks 3 times during the signal sound
A problem is detected when setting in the armed mode (e.g., the detector is lost)	Long sound signal, the “Fault” indicator blinks 3 times during the signal sound
The hub does not respond to the command – no connection	Long sound signal, the “Fault” indicator lights during the signal sound
The keypad is interlocked due to the password guessing	Long sound signal, the indicators of armed / disarmed /night mode blink simultaneously
Battery low	After successful entering a code and setting the security system in the armed/disarmed mode, the keypad will smoothly blink with the “Fault” indicator. The touch-sensitive buttons will be locked for the time of activity of the indicator. When trying to switch the keypad with the discharged batteries, it will emit a long sound signal, smoothly switch on and off the “Fault” indicator and then the keypad will switch off.

Connecting the Keypad to the hub

Before starting connection:

1. Following the hub instruction recommendations, install the Ajax application on your smartphone. Create an account, add the hub to the application, and create at least one room.
2. Go to the Ajax application.
3. Switch on the hub and check the internet connection (via Ethernet cable and/or GSM network).
4. Ensure that the hub is disarmed and does not start updates by checking its status in the mobile application.

Only users with administrative privileges can add the device to the hub

How to connect the Keypad to the hub:

1. Open a room in the mobile application or web application and select the option **“Add a device”**.
2. Name the device, scan/write manually the QR Code (located on the body and packaging), and select the location room.

3. When the hub starts searching for a device and launches countdown, switch on the KeyPad by pressing the on/off button for 3 seconds – it will blink once with an LED.

   For the detection and interfacing to occur, the detector should be located within the coverage area of the wireless network of the hub (at a single protected object).

   Request for connection to the hub is transmitted for a short time at the time of switching on the device. If the connection to the hub failed keypad will switch off after 5 seconds. Repeat the connection attempt.

   The keypad will appear in the list of devices of the hub. After adding the keypad to the system, it will have the following default codes: 123456 and Duress Code: 123457

Selection of the Keypad Location

While selecting the Keypad location, take account of the keypad distance from the hub and presence of any obstacles between the devices, hindering radio signal transmission: walls, inserted floors, large-size objects located within the room.

Do not install the KeyPad:

1. Near radio transmission equipment, including that operated in 2G/3G/4G mobile networks, Wi-Fi routers, transceivers, radio stations, as well as an Ajax hub (it uses a GSM network).
2. In close proximity to electrical wiring.

3. Close to metal objects and mirrors that cause radio signal attenuation or shading it.
4. Outside the premises (outdoors).
5. In rooms with a temperature and humidity exceeding the appropriate levels.
6. Closer than 1 m from the hub.

Check the signal level at the installation location

During testing, the signal level can be seen in the application and on the keypad panel – blue LEDs (Armed mode), (Disarmed mode) and (c) (Night mode), as well as red X (Fault), are used.

If the signal level is one division, we cannot guarantee stable operation of the security system. Take possible measures to improve the quality of the signal! As a minimum, move the device – even 20 cm shift can significantly improve the quality of reception.

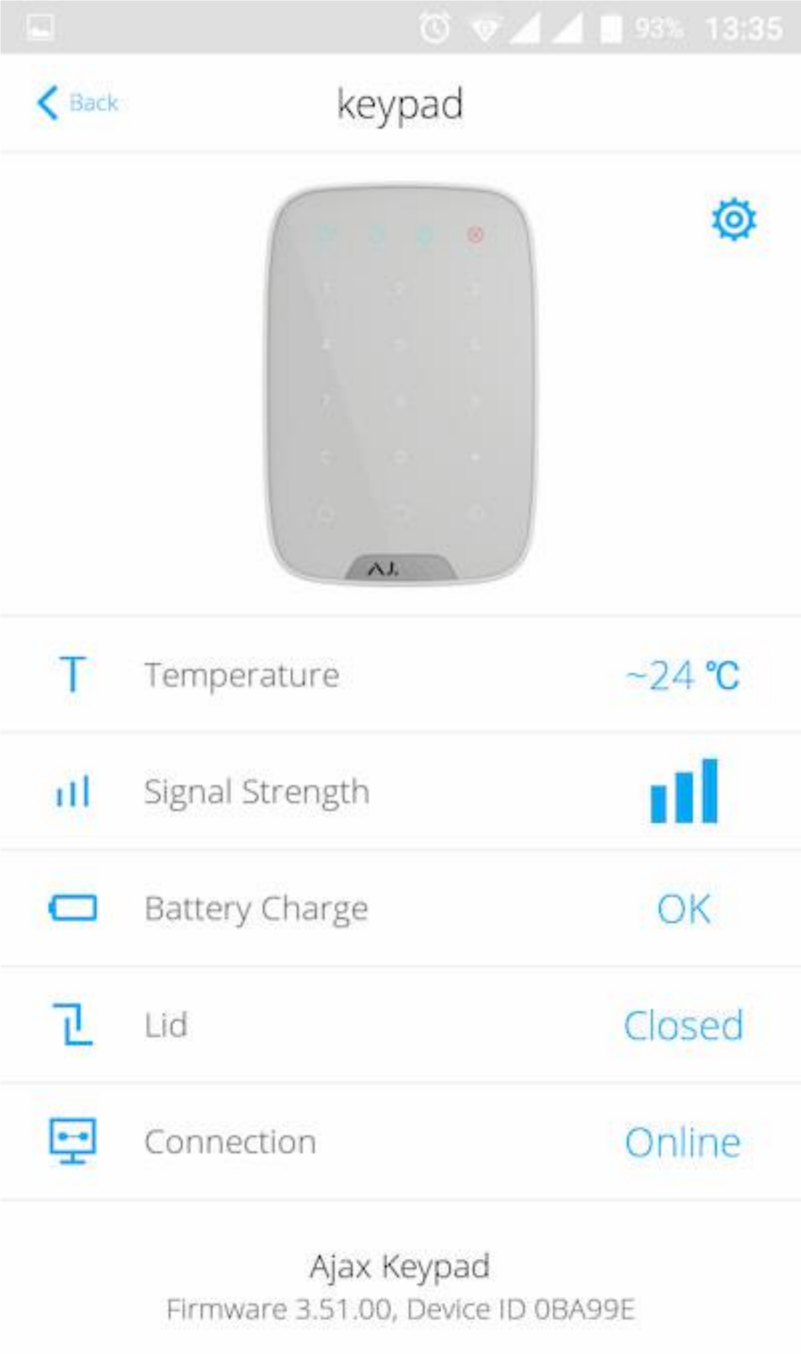
If, after moving, the device still has a low or unstable signal strength, use a radio signal range extender ReX.

The touch-sensitive panel of the keypad is designed for operation with the device mounted on the surface. If you use Keypad in your hands, we cannot guarantee successful operation of the touch-sensitive buttons.

States

1. Devices

2. KeyPad



keypad

Temperature ~24 ℃

Signal Strength

Battery Charge OK

Lid Closed

Connection Online

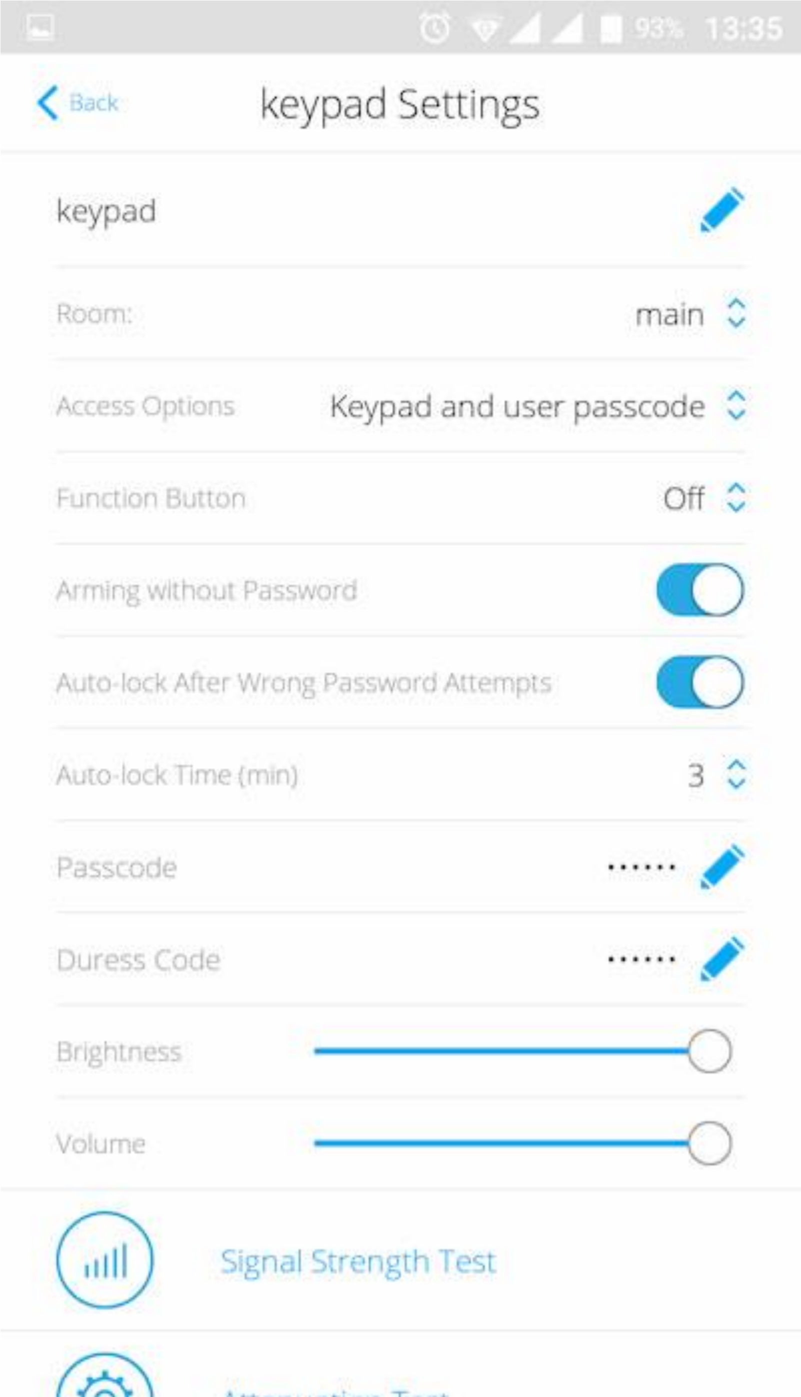
Ajax Keypad

Firmware 3.51.00, Device ID 0BA99E

Parameter	Value
Temperature	Temperature of the device. Measured on the processor and changes gradually
Signal Strength	Signal strength between the hub and the keypad
Battery Charge	Battery level of the device
Lid	The tamper mode of the device, which reacts to the detachment of or damage to the body
Connection	Connection status between the hub and the keypad
Firmware	Detector firmware version
Device ID	Device identifier

Settings

1. Devices
2. KeyPad
3. Settings



keypad Settings

keypad

Room: main

Access Options: Keypad and user passcode

Function Button: Off

Arming without Password: On

Auto-lock After Wrong Password Attempts: On

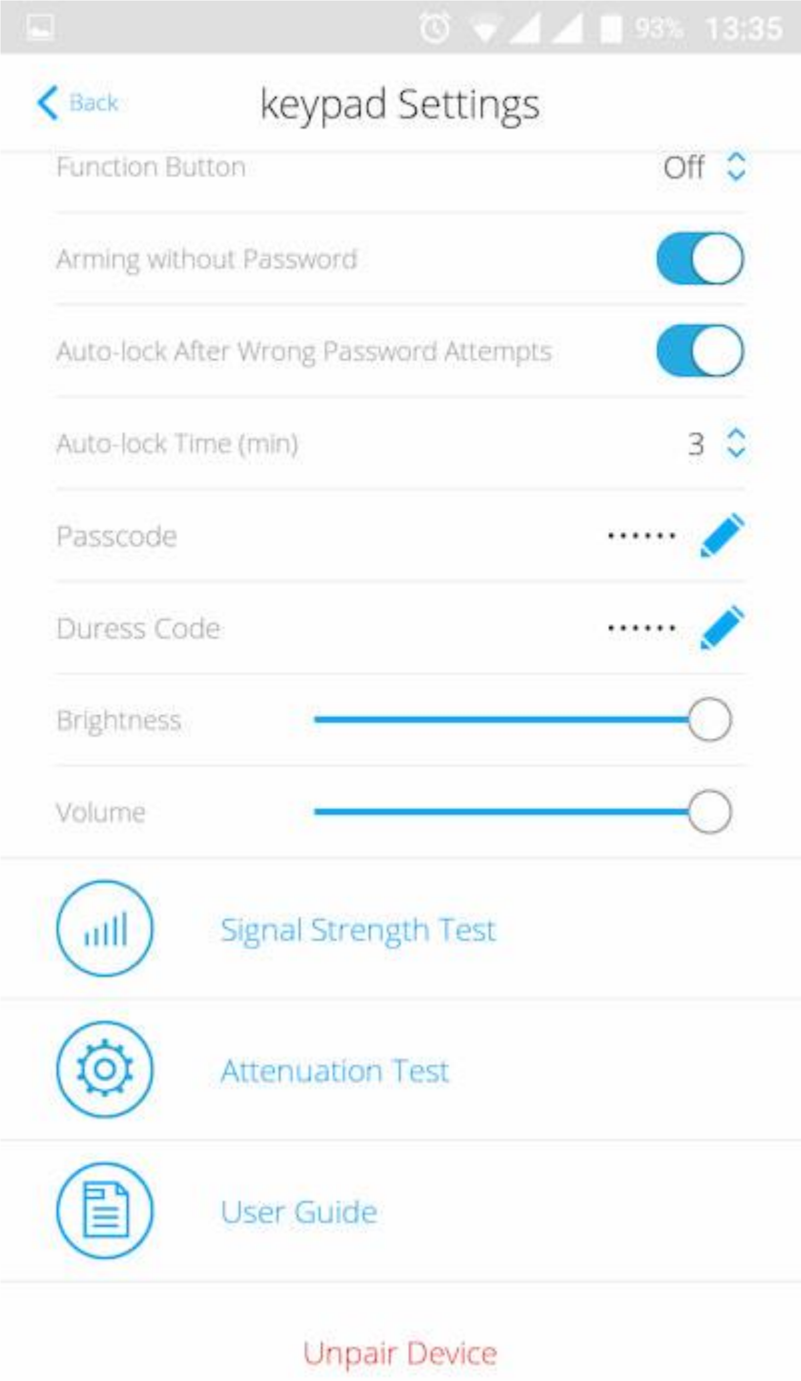
Auto-lock Time (min): 3

Passcode ••••••

Duress Code ••••••

Brightness

Volume



93% 13:35

< Back

keypad Settings

Function Button Off

Arming without Password

Auto-lock After Wrong Password Attempts

Auto-lock Time (min) 3

Passcode ••••••

Duress Code ••••••

Brightness

Volume

Signal Strength Test

Attenuation Test

User Guide

Unpair Device

Setting	Value
First field	Device name, can be edited
Room	Selecting the virtual room to which the device is assigned
Access option	Selecting type of passcodes for arming/disarming Keypad passcode only User passcode only Keypad and User passcode
Function Button	Selecting functionality of the function button Off Send panic alarm Silence fire alarm
Arming without password	Allows to arm the system without password by pressing arm button
Auto-lock after wrong password attempts	If active, in case if three incorrect passwords are entered, the keyboard is locked for the time set in the settings. At this time, you can not disarm the system by keypad
Auto-lock time (min)	Lock period after wrong password attempts
Passcode	Keypad password for arming/disarming

Duress code	Selection a duress code (silent alarm)
Brightness	Brightness of the keypad
Volume	Volume of the keypad
Signal Strength Test	Switches the device to the signal strength test mode
Attenuation Test	Switches the keypad to the signal fade test mode (available in devices with **firmware version 3.50 and later**)
User Manual	Opens the keypad User Manual
Unpair Device	Disconnects the keypad from the hub and deletes its settings

Either a shared or personal password can be set on the keypad for each user.

In order to install a personal password:

1. Go to profile settings (**Hub** **User settings** **Users** **Your profile settings**)
2. Click “**Access Code Settings**” (in this menu you can also see the user identifier)
3. Set the **User Code** and **Duress Code**

Each user sets his own personal password individually!

To control the system using the personal password:

- **Enter:** User identifier * personal password Arming/disarming button

To control the certain group:

- **Enter:** User identifier * personal password * group identifier Arming/disarming button

Functionality Testing

The Ajax security system allows conducting tests for checking the functionality of connected devices.

The tests do not start straight away but within a period of 36 seconds when using the standard settings. The test time start depends on the settings of the detector scanning period (the paragraph on “**Jeweller**” settings in hub settings).

Signal Strength Test

Attenuation Test

Keypad Capabilities

To activate the keypad, touch the touch-sensitive panel – the highlight of the buttons will be activated and a wake-up sound signal will be emitted.

If the battery is low, the highlight switches on at a minimum level, regardless of the settings.

If you do not touch the buttons for 4 seconds, Keypad will reduce the highlight brightness, and after another 12 seconds, the device will go to the sleep mode.

When switching over to the sleep mode, the keypad will clear the entered commands!

The keypad allows using codes with the length of 4-6 digits. The entered code will be sent to the hub after pressing the buttons: (activate the guard mode), (deactivate the guard mode) and (c) (Night mode). Erroneously entered digits can be cleared using the button C (Reset).

If you enter incorrect code three times during 30 minutes, the keypad will be interlocked for the time preset in the settings. The hub will ignore any entered codes, simultaneously notifying the security system users of the attempt of guessing the code. The keypad will be unlocked automatically after expiration of the interlock time or manually by the administrator user.

Keypad also supports setting the system in the armed mode without entering a master code, by pressing the button (activate the armed mode). These features are disabled by default.

If you press the button * (Function) without entering the password, command * will be sent to the hub and the function installed in the hub from the application will be executed.

KeyPad can notify a private security company of the system being removed from the guard mode forcibly – using the **Duress code**. Unlike the panic button of the fob, if such code is entered, the user will not be compromised by actuation of the siren, and the keypad and message in the application will notify of the successful removal of the system from the guard mode.

Keypad Installation

Before installing the detector, make sure that you have selected the optimal location and it is in compliance with the guidelines contained in this manual!

Keypad should be attached to the vertical surface.

1. Attach the SmartBracket panel to the surface using bundled screws, using at least two fixing points (one of them – above the tamper). After selecting other attachment hardware, make sure that they do not damage or deform the panel.

The double-sided adhesive tape may be only used for temporary attachment of Keypad. The tape will run dry in course of time, which may result in the falling of the keypad and damage of the device.

2. Put Keypad on the attachment panel and tighten the mounting screw on the body underside.

   As soon as the keypad is fixed in SmartBracket, it will blink with the LED X (Fault) – this will be a signal that the tamper has been actuated.

If the LED X (Fault) of the keypad is not actuated after installation in SmartBracket, check the status of the tamper in the Ajax Security System application and then the fixing tightness of the panel.

If the keypad is torn off from the surface or removed from the attachment panel, you will receive the notification.

Keypad Maintenance and Battery Replacement

Check the Keypad operating capability on a regular basis.

The battery installed in the keypad ensures up to 2 years of autonomous operation (with the inquiry frequency by the hub of 3 minutes). If the Keypad battery is low, the security system will send the relevant notices, and the **"Fault"** indicator will smoothly lights up and goes out after each successful password entry.

Battery Replacement

Complete Set

1. KeyPad
2. SmartBracket mounting panel
3. Batteries AAA (pre-installed) – 4 pcs

4. Installation kit
5. Quick Start Guide

Technical Specifications

Sensor type	Capacitive
Tamper protection	Yes
Protection against passcode guessing	Yes
Frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz depending on the region of sale
Compatibility	Operates only with Hub, Hub Plus, Hub 2 and ReX
Maximum RF output power	Up to 20 mW
Modulation of the radio signal	GFSK
Radio signal range	Up to 1,700 m (if there are no obstacles
Power supply	4 x AAA batteries
Power supply voltage	3 V
Battery life	Up to 2 years

Operating temperature range	From -10°C to +40°C
Operating humidity	Up to 75%
Overall dimensions	150 x 103 x 14 mm
Weight	197 g
Certification	Security Grade 2, Environmental Class II in conformity with the requirements of EN 50131-1, EN 50131-3, EN 50131-5-3

Warranty

Warranty for the “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase and does not apply to the pre-installed battery.

If the device does not work correctly, you should first contact the support service—in half of the cases, technical issues can be solved remotely!

The full text of the warranty

User Agreement

Technical support: support@ajax.systems

SpaceControl User Manual

Updated December 11, 2019

SpaceControl is a miniature key fob controlling the security system at a distance up to 1300 meters absent any obstacles. It allows to set the Ajax security system in the armed, night or disarmed mode, as well as switch on an alarm.

As it is the two-way communication, you will know whether the system has received the SpaceControl command.

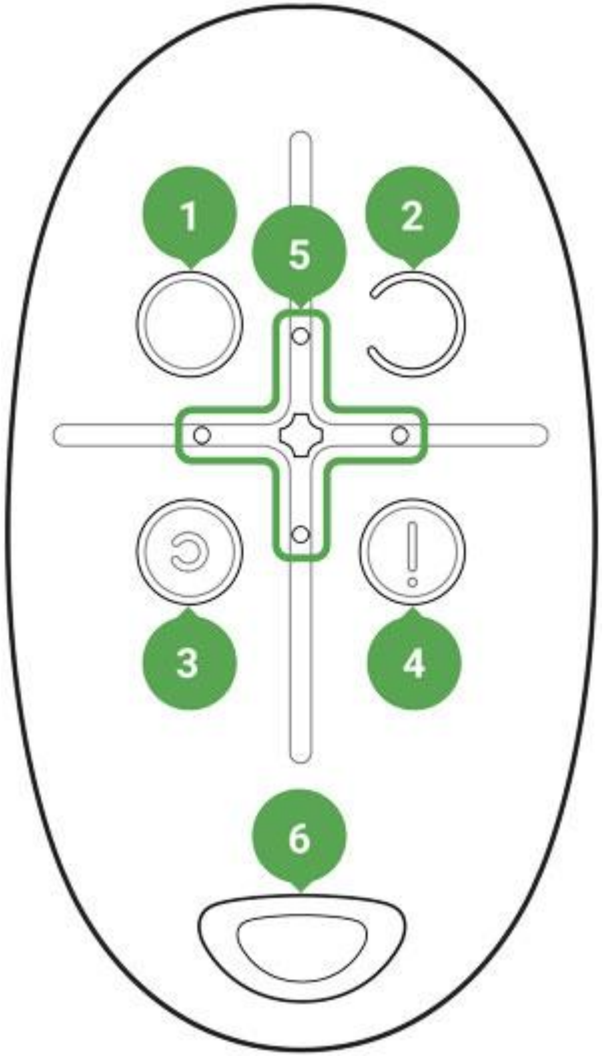
Operating as part of the Ajax security system, the key fob is connected to the hub via the protected Jeweller protocol. In addition, the key fob can be used to control any third party security central unit through the uartBridge or ocBridge Plus integration module.

The fob is set up through the iOS and Android-based mobile application for smartphones or web application.

The Ajax system is self-sustaining, but the user can connect it to the monitoring station of a security company.

Buy key fob SpaceControl

Functional elements



1. System arming button

2. System disarming button
3. Night mode button
4. Panic button (activates the alarm)
5. Light indicators
6. The hole for attaching the key fob

> Buttons can be assigned when using a key fob with hub and Ajax uartBridge. At the moment, the feature of modification of commands (and deactivation) of the key fob buttons when using with the Ajax hub is not available.

Using the key fob

Maximum connection distance between the key fob and the hub – 1,300 meters. This distance is reduced by walls, inserted floors and any objects hindering the signal transmission.

SpaceControl operates only with one security system (Ajax or third-party system via the integration module). If you connect the key fob to a new security system, it will cease to interact with the previous system. However, the key fob will not be automatically deleted from the list of devices of the hub.

The key fob can:

- **Arm the system** — press the button (O) once
- **Arm the system in the night mode —** press the button (c) once
- **Disarm the system** — press the button (C) once
- **Switch on an alarm —** press the button (!) once

To disconnect the actuated security system (siren), press the disarming mode (C) on the key fob.

Operational Indication

Depending on the firmware version, the SpaceControl key fob LEDs indicate the status with red or green light.

The key fob reports its status only after any button is pressed.

Indication	Event
4 green key fob LEDs blink 6 times	The key fob is not registered with any security system
Two green LEDs next to the pressed button light up once	The key fob command has been sent over to the security system
The LEDs next to the pressed button quickly blink green 4 times when a key fob with **firmware version 3.16 and lower** is used	The command has not been delivered as the security system is too far away and cannot receive the command

The central LED lights up red briefly when a key fob with **firmware version 3.18 and later** is used	
Two LEDs next to the button light up green twice. Then 4 key fob LEDs blink green 6 times	The key fob has been removed from the security system devices
The central LED lights up green for a few seconds	Linking a key fob to the security system
The central LED lights up green for approximately half a second when a key fob with f**irmware version 3.18 and later** is used	The system has executed the key fob command
The central LED lights up red for approximately half a second when a key fob with **firmware version 3.18 and later** is used	The system has not executed the key fob command — integrity verification is enabled in the system and one of the devices is faulty What is system integrity check?
After the main indication, the central LED lights up green once and gradually goes out when a key fob with **firmware version 3.16 and lower** is used After the main indication, the central LED lights up red once and goes out gradually when a key fob with **firmware version 3.18 and later** is used	The key fob battery needs replacement. In this case, the key fob commands are delivered to the security system. Battery replacement
Continuous short flashes of green light when a key fob with **firmware version 3.16 and lower** is used	The battery charge level is unacceptably low. The battery needs replacement.

Continuous short flashes of red when a key fob with **firmware version from 3.18 to 3.52**is used Key fobs with **firmware version 3.53 and later** do not function when the battery charge level is unacceptably low, do not communicate commands to the hub, and do not notify with LED indication	In this operation mode, the key fob commands are not delivered to the security system. Battery replacement

Connecting the key fob to the Ajax Security System

Connection to hub

Before starting connection:

1. Following the hub instruction recommendations, install the Ajax application on your smartphone. Create an account, add the hub to the application, and create at least one room.
2. Go to the Ajax application.
3. Switch on the hub and check the internet connection (via Ethernet cable and/or GSM network).

4. Ensure that the hub is disarmed and does not start updates by checking its status in the mobile application.

> Only users with administrative privileges can add the device to the hub.

How to connect key fob to hub:

1. Select the **Add Device** option in the Ajax application.
2. Name the device, scan/write manually the **QR Code** (located inside the body, on the battery fixture and packaging), and select the location room.
3. Select **Add** — the countdown will begin.
4. Simultaneously press the button for armed mode (o) and the **panic button** (!) – the key fob will blink with the central LED. For the detection and interfacing to occur, the key fob should be located within the coverage area of the wireless network of the hub (at a single protected object).

   Request for connection to the hub is transmitted for a short time at the time of switching on the device.

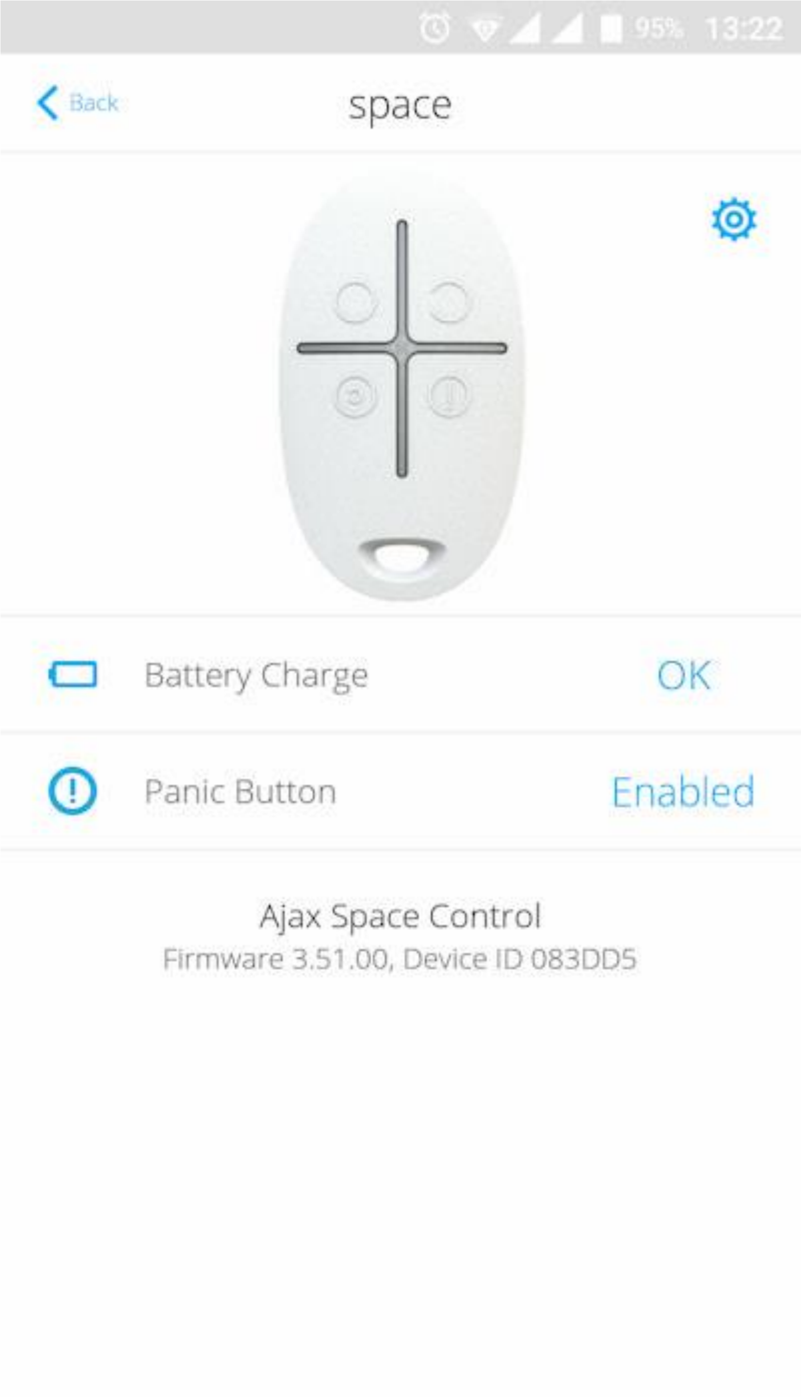
The key fob connected to the hub will appear in the list of devices of the hub in the application.

Connecting the key fob to Third Party Security Systems

To connect the key fob to a third party security central unit using the Ajax uartBridge or Ajax ocBridge Plus integration module, follow the recommendations in the manual of the respective device.

States

1. Devices
2. SpaceControl



space

Battery Charge OK

Panic Button Enabled

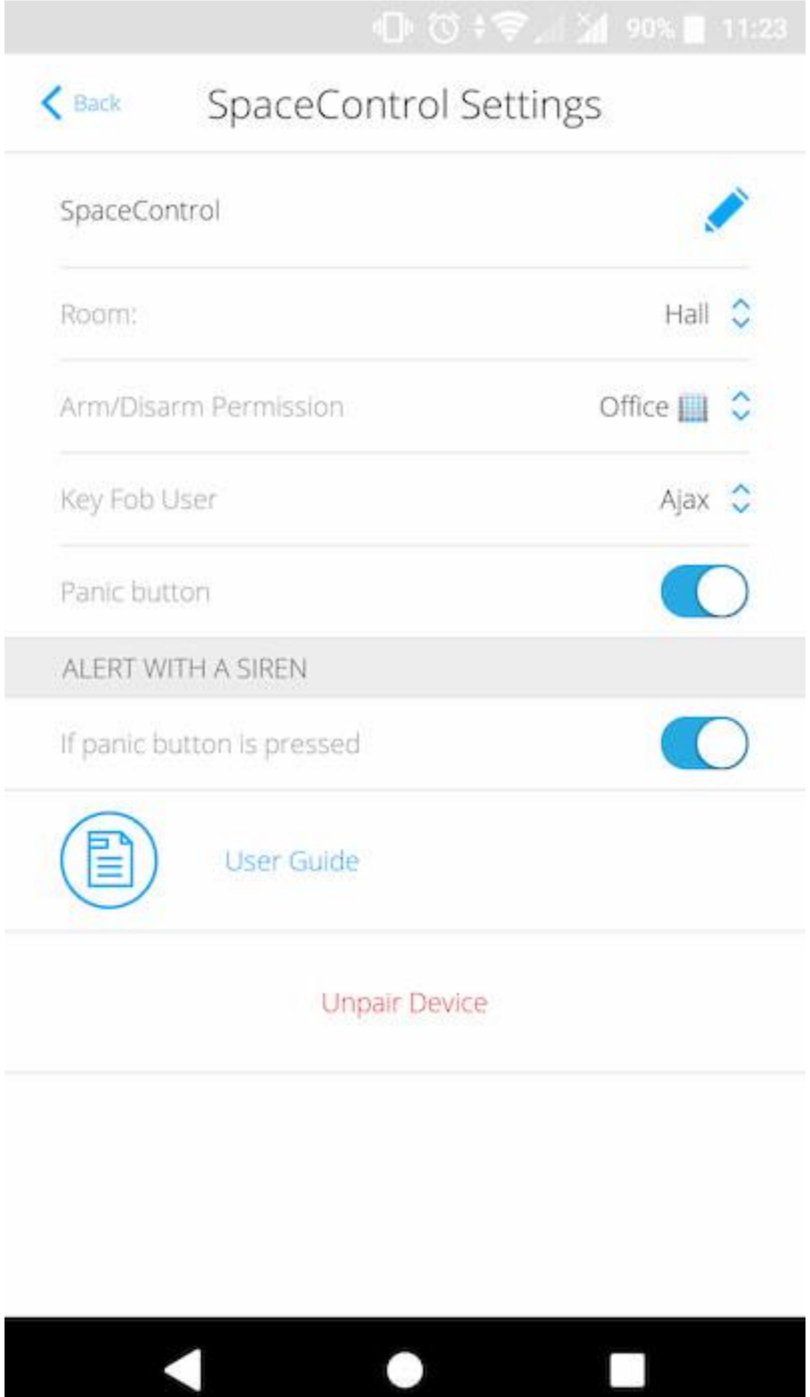
Ajax Space Control

Firmware 3.51.00, Device ID 083DD5

Parameter	Value
Battery Charge	Battery level of the key fob
Panic Button	Panic button status
Firmware	Firmware version of the key fob
Device ID	Device identifier

Setting Up the key fob

1. Devices
2. SpaceControl
3. Settings



SpaceControl Settings

SpaceControl

Room: Hall

Arm/Disarm Permission Office

Key Fob User Ajax

Panic button

ALERT WITH A SIREN

If panic button is pressed

User Guide

Unpair Device

Setting	Value
First field	Device name, can be edited
Room	Selecting the virtual room to which the device is assigned
Arming/disarming permission	Selection of a security group that the key fob manages. You can select **All groups** or a single group. 👆*Configuration is available only after group mode activation*
Key fob user	Selection key fob user. **Key fob is unassigned:** Key fob events are sent to Ajax apps under the key fob name. Security mode management rights are determined by key fob settings. **Key fob is assigned to user:** Key fob events are sent to Ajax apps under the user’s name. The key fob has the same security mode management rights as the user.
Panic Button	Turning on/off the panic button

Alert with a siren if panic button is pressed	If active, HomeSiren and StreetSiren are activated after panic button pressing
User Manual	Opens the device User Manual
Unpair Device	Disconnects the device from the hub and deletes its settings

Key fob Maintenance and Battery Replacement

When cleaning the key fob body use any means suitable for equipment maintenance.

Do not use for cleaning SpaceControl any substances containing alcohol, acetone, gasoline and other active solvents.

The pre-installed battery provides up to 5 years of operation of the key fob during normal use (one arming and disarming of the security system per day). More frequent use can reduce battery life. You can check battery level at any time in the Ajax app.

The pre-installed battery is sensitive to low temperatures and if the key fob is significantly cooled, the battery level indicator in the app may show incorrect values until the key fob gets warm.

The value of the battery level is not updated regularly, but only after pressing one of the buttons at the key fob.

When the battery is discharged, the user will receive a notification in the Ajax app, and the key fob LED will slowly light up and go out red each time the button is pressed (key fobs with **firmware version 3.16 and lower** light up green).

Battery replacement

Tech Specs

Number of buttons	4
Panic button	Yes
Frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz depending on the region of sale
Compatibility	Operates with Hub, Hub Plus, Hub 2, ReX, ocBridge Plus, uartBridge
Effective radiated power	6.01 dBm / 3.99 mW (limit 20 mW)
Modulation of the radiosignal	GFSK
Radio signal range	Up to 1,300 m(any obstacles absent)
Power supply	1 battery CR2032A, 3 V
Service life from the battery	Up to 5 years (depending on the usage frequency)

Operating temperature range	From -25°C to +50°C
Operating humidity	Up to 95%
Overall dimensions	65 x 37 x 10 mm
Weight	13 g
Certification	Security Grade 2, Environmental Class III in conformity with the requirements of EN 50131-1, EN 50131-3, EN 50131-5-3

Complete Set

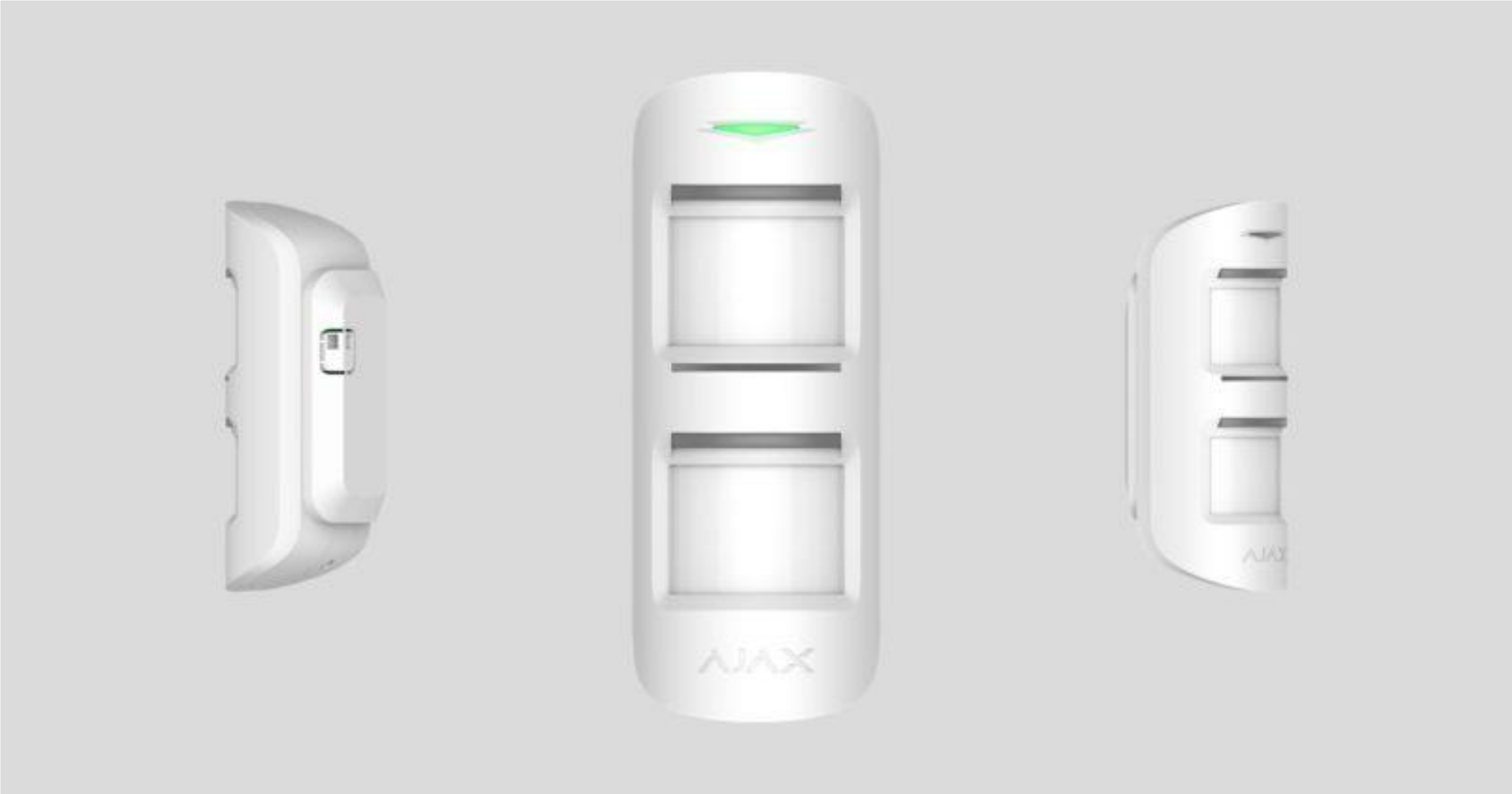
1. SpaceControl
2. Battery CR2032 (pre-installed)
3. Quick Start Guide

Warranty

Warranty for the “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase and does not apply to the pre-installed battery.

MotionProtect Outdoor User Manual

Updated January 8, 2020



MotionProtect Outdoor is a wireless outdoor motion detector for the Ajax security system. The detector communicates with the hub via protected Jeweller radio protocol at a distance up to 1,700 meters in the line of sight.

MotionProtect Outdoor features protection against blocking the detector view (anti-masking system) and triggering by pets (pet immunity). The motion detection distance is adjustable: from 3 up to 15 meters.

MotionProtect Outdoor can operate both on pre-installed batteries or use an external power supply. Depending on the detector settings, the batteries’ life is up to 5 years.

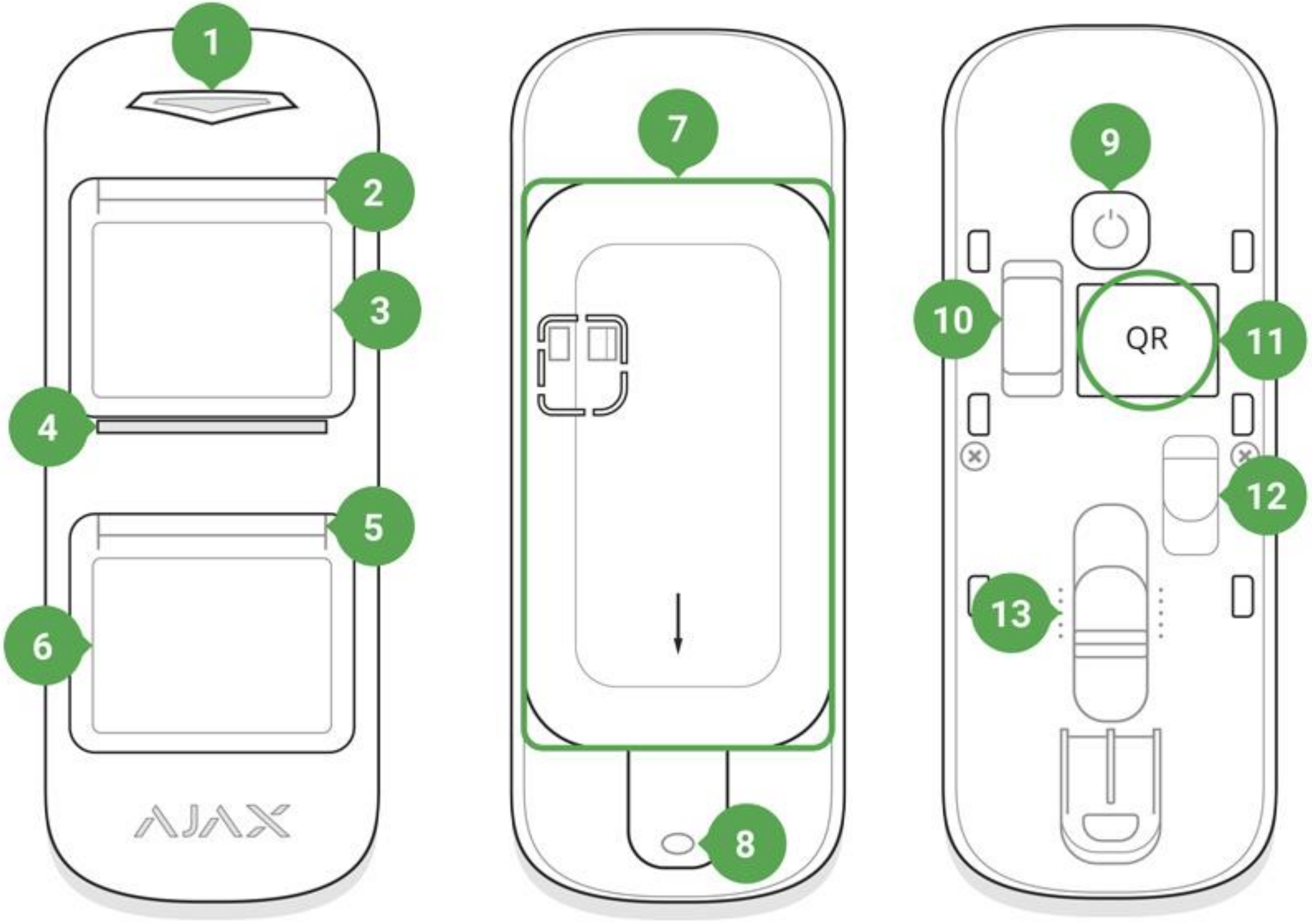
MotionProtect Outdoor does not support connection via the ocBridge Plus and uartBridge integration modules.

The user can configure the detector via the Ajax app for iOS, Android, macOS, and Windows. The security system notifies users of all events through push notifications, SMS, and calls (if activated).

The Ajax security system can be connected to a central monitoring station of a security company.

Buy outdoor motion detector MotionProtect Outdoor

Functional Elements



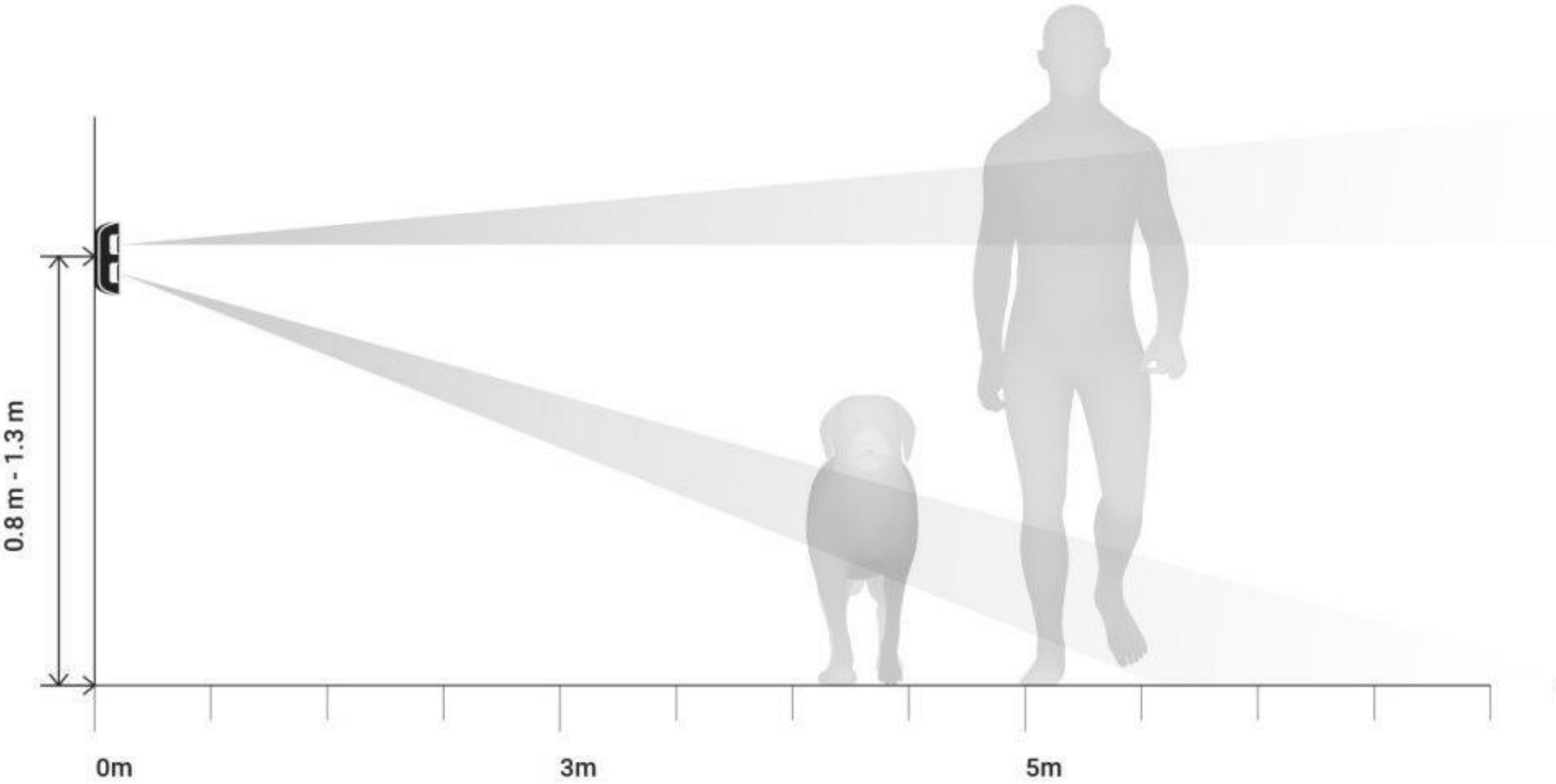
1. Main light indicator

2. Upper light indicator and masking sensor
3. Upper motion sensor lens
4. Varnish masking sensor
5. Lower light indicator and masking sensor
6. Lower motion sensor lens
7. SmartBracket attachment panel (perforated part is required for actuating the tamper button in case of any attempt to dismantle the detector)
8. The hole for attaching SmartBracket panel with a screw
9. “On” button
10. Tamper button
11. QR Code
12. Connector for external power supply cable outlet
13. Scrollbar for adjusting the motion detection range

Operating Principle

When the system is armed, the detector continuously receives signals from two PIR sensors. If both sensors detect identical motion, MotionProtect Outdoor instantly transmits an alarm signal to the hub and blinks with a green LED. MotionProtect Outdoor ignores animals, birds, insects, as well as swaying plants and trees.

By a motion alarm, the security system also can activate sirens and notify a security company if connected.


0.8 m - 1.3 m
0m
3m
5m

The detector recognizes motion and sends the first alarm immediately, but next alarms until disarming are transmitted no more than once in 5 seconds.

If a motion is detected before the system is armed, the detector will be armed not immediately, but during the next polling by the hub.

Learn more about the algorithm of the detector operation

Anti-masking system

Masking is an attempt to block in any way the view of the detector's lens.

MotionProtect Outdoor detects the following types of masking:

- An obstacle in front of both lenses (an object on the height of the detector and at a distance of up to 20 cm in front of it)
- An obstacle in front of any of the lenses (an object at a distance of up to 10 cm in front of one of the lenses)
- Painting or pasting any of the lenses with an opaque substance
- Pasting the detector front side with an opaque substance
- Applying an aerosol or painting the detector front side with lacquer/paint

If one or more types of masking are detected, the detector generates a masking alarm and lights up a green LED for 1 second.

MotionProtect Outdoor detects masking regardless of the security state: armed or disarmed.

Response time to masking

Masking type	Active mode (detector is armed)		Passive mode (detector is disarmed)	
	Time to alarm, s	Time to restore, s	Time to alarm, s	Time to restore, s
An obstacle in front of both lenses	1	5,4	300	18
An obstacle in front of any of the lenses	150	13	150	5,4
Pasting or painting any of the lenses	150	13	150	5,4
Pasting the detector front side	150	9	300	18

Applying aerosol or painting the detector front side with lacquer/paint	150	9	150	9

Connecting

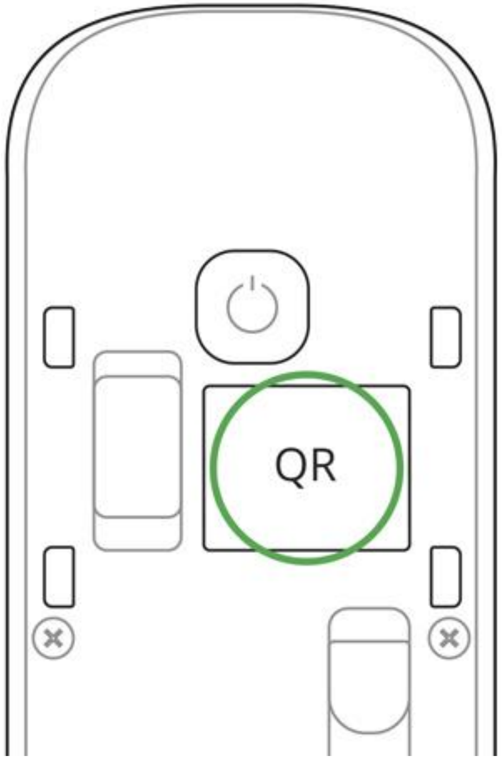
Before starting connection:

1. Following the hub user guide, install the Ajax app. Create the account, add the hub, and create at least one room.
2. Switch on the hub and check the internet connection (via Ethernet cable and/or GSM network).
3. Make sure that the hub is disarmed and does not update by checking its status in the Ajax app.

Only users with administrator rights can add the device to the hub

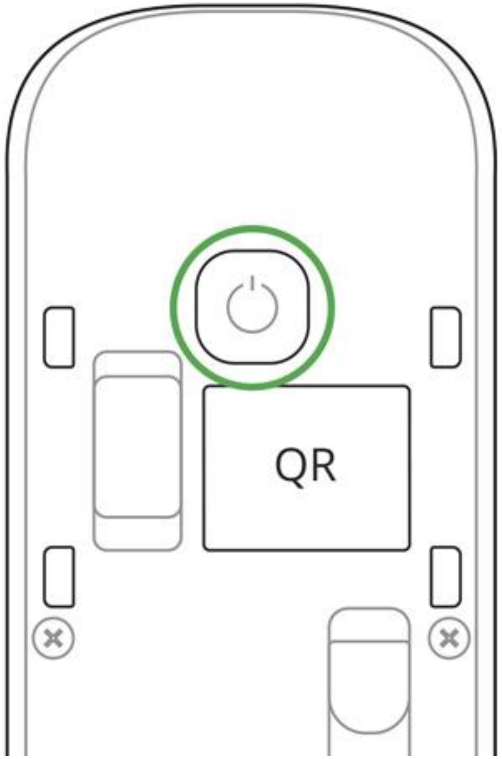
How to connect the device to the hub:

1. Select the **Add Device** option in the Ajax application.
2. Name the device, scan/write manually the **QR Code** (located on the body and packaging), and select the location room.



3. Select **Add** — the countdown will begin.

4. Switch on the device by pressing the on/off button for 3 seconds.



For the detection and interfacing to occur, the detector should be located within the coverage area of the wireless network of the hub (at a single protected object). Request for connection to the hub is transmitted for a short time at the time of switching on the device.

MotionProtect Outdoor turns off automatically after 6 seconds, if it failed to connect to the hub. To retry the connection, you do not need to switch off the device. If the detector has already been assigned to another hub, turn off MotionProtect Outdoor, and then follow the standard addition procedure.

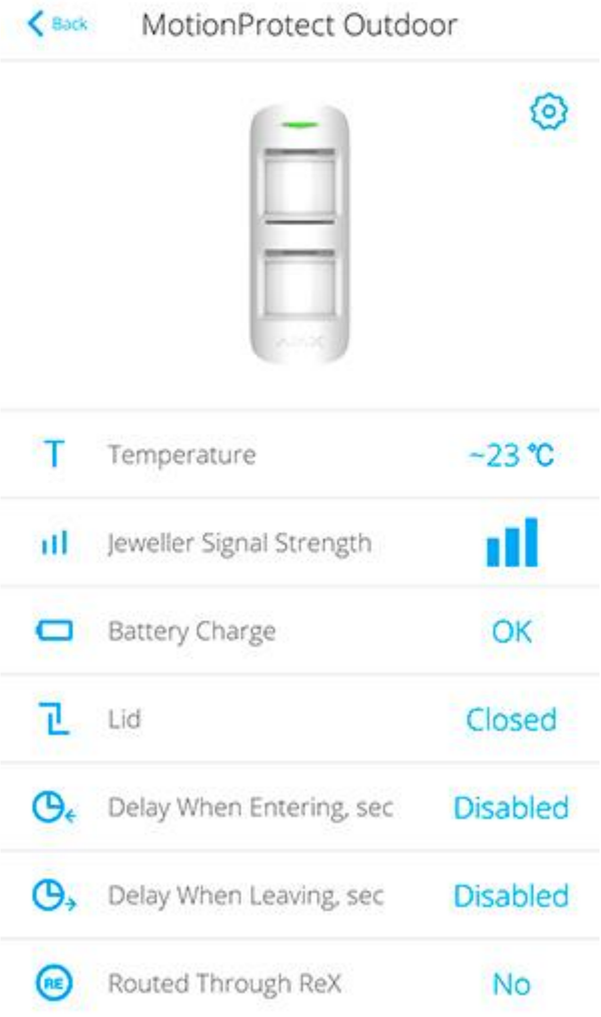
If the connection to the hub failed, repeat the connection attempt after 30 seconds.

The device connected to the hub will appear in the list of devices of the hub in the app. The update of the detector statuses in the list depends on the device ping interval set in the hub settings (the default value is 36 seconds).

To avoid masking alarms, switch off anti-masking in the device settings before the installation!

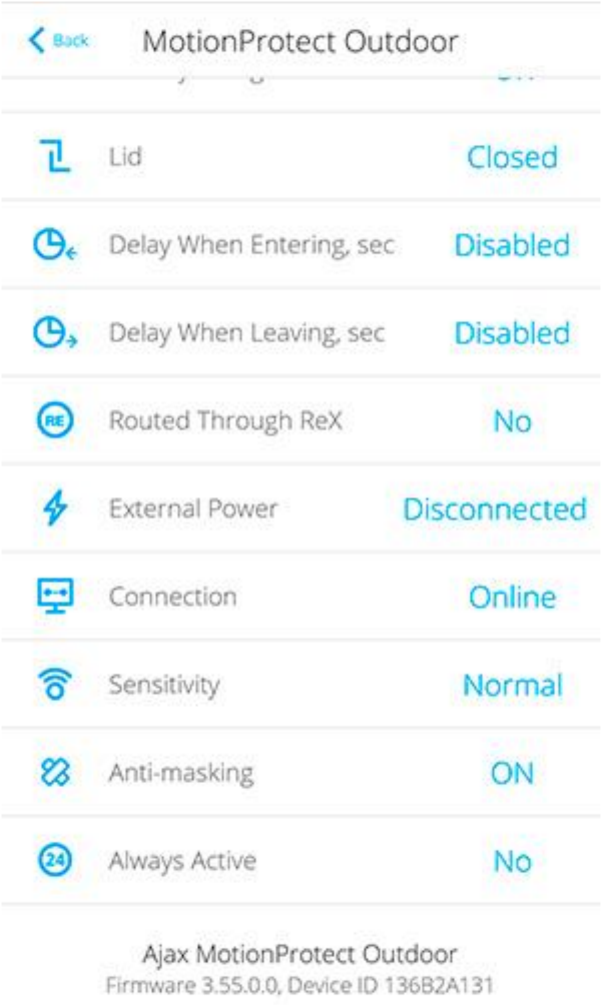
States

1. Devices
2. MotionProtect Outdoor



MotionProtect Outdoor

Temperature	~23 ℃
Jeweller Signal Strength	▮▮▮
Battery Charge	OK
Lid	Closed
Delay When Entering, sec	Disabled
Delay When Leaving, sec	Disabled
Routed Through ReX	No



MotionProtect Outdoor

Lid Closed

Delay When Entering, sec Disabled

Delay When Leaving, sec Disabled

Routed Through ReX No

External Power Disconnected

Connection Online

Sensitivity Normal

Anti-masking ON

Always Active No

Ajax MotionProtect Outdoor
Firmware 3.55.0.0, Device ID 136B2A131

Parameter	Value

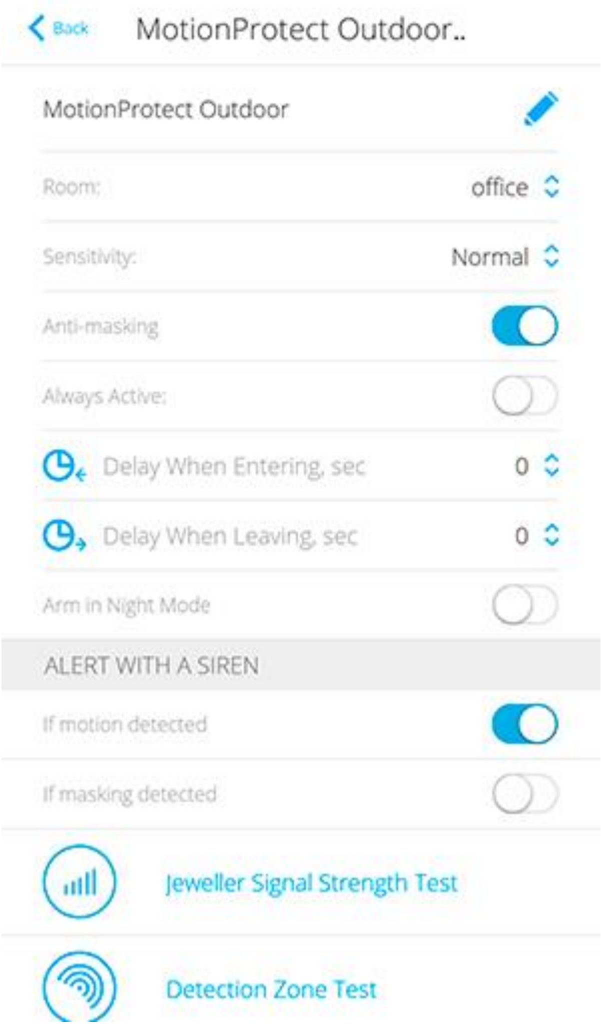
Temperature	Temperature of the Detector. Measured on the processor and changes gradually
Jeweller Signal Strength	Signal strength between the hub and the detector
Connection	Connection status between the hub and the detector
Battery Charge	Battery level of the detector, displayed in increments of 25%
Lid	The tamper mode of the detector, which reacts to the detachment of or damage to the body
Delay when entering, sec	Delay time when entering
Delay when leaving, sec	Delay period after the security system is armed
Routed Through ReX	Displays the status of using the ReX range extender
External Power	Displays the status of using the external power supply
Sensitivity	Sensitivity level of the motion detector: low, normal, high
Anti-masking	Has the anti-masking option been enabled
Always Active	When turned on, the motion detector always detects movement
Firmware	Detector firmware version
Device ID	Device identifier

Settings

1. Devices

2. MotionProtect Outdoor

3. Settings



MotionProtect Outdoor..

MotionProtect Outdoor

Room: office

Sensitivity: Normal

Anti-masking ●

Always Active: ○

Delay When Entering, sec 0

Delay When Leaving, sec 0

Arm in Night Mode ○

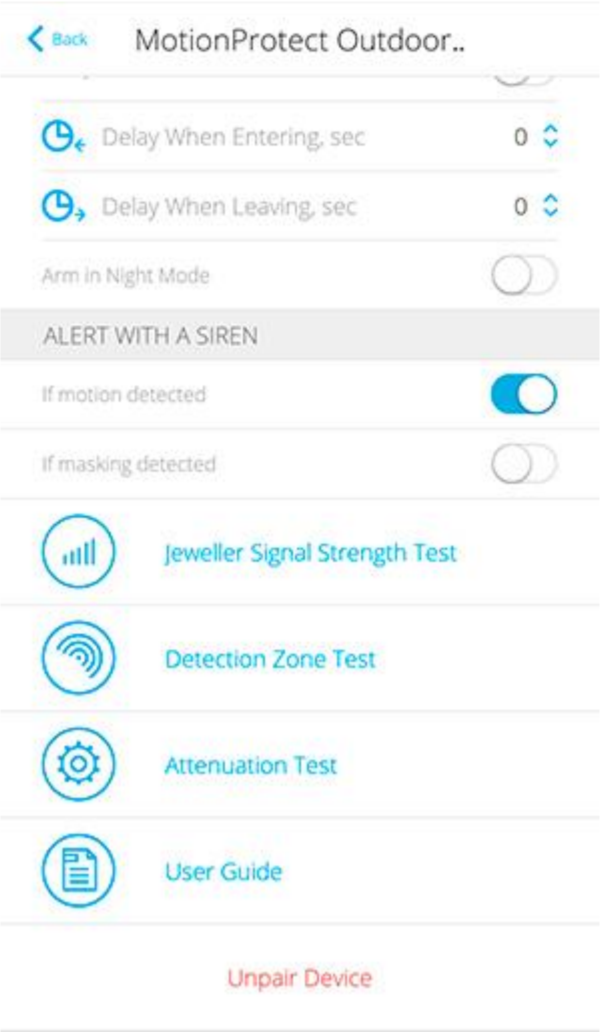
ALERT WITH A SIREN

If motion detected ●

If masking detected ○

Jeweller Signal Strength Test

Detection Zone Test



Delay When Entering, sec 0

Delay When Leaving, sec 0

Arm in Night Mode ○

ALERT WITH A SIREN

If motion detected ●

If masking detected ○

Setting	Value
First field	Detector name, can be edited

Room	Selecting the virtual room to which the device is assigned
Delay when entering, sec	Selecting delay time when entering
Delay when leaving, sec	Delay period after the security system is armed
Delays in night mode	When enabled, the detector will experience a delay in the night mode
Arm in night mode	When turned on, the detector will switch to armed mode when using night mode
Sensitivity	Choosing the sensitivity level of the motion sensor: High Normal Low
Anti-masking	If active, sensor will always detect masking
Always active	When turned on, the detector always registers motion
Alert with a siren if motion detected	If active, HomeSiren and StreetSiren are activated when the motion detected
Jeweller Signal Strength Test	Switches the detector to the Jeweller signal strength test mode
Detection Zone Test	Switches the detector to the detection area test: General motion detector test

	Upper motion detector test Lower motion detector test Masking sensor test
Attenuation test	Switches the detector to the signal fade test mode (available in detectors with **firmware version 3.50 and later**)
User Guide	Opens the detector User Guide
Unpair Device	Disconnects the detector from the hub and deletes its settings

Indication

MotionProtect Outdoor light indicator may light up red or green depending on the device status.

Indication When Pressing the “On” button

Event	**Indication**
Pressing the power button (detector is switched on)	Lights up red while the button is held down

Switching on	Lights up green while the device is switching on
Switching off	Initially lights up red, then blinks three times

Turned-on detector indication

Event	Indication	Note
Detector connection to the hub	Lights up green for a few seconds	
Hardware error	Blinks red continuously	The detector requires repair, please contact Support Service
Motion- and masking-triggered alarm or tamper button triggering	Lights up green for about one second	
Battery needs replacing	During the alarm, it slowly lights up green and slowly goes out	Replacement of the detector battery is described in the **Battery Replacement** paragraph

Functionality Testing

The Ajax security system allows conducting tests for checking the functionality of connected devices.

The tests do not start immediately but within a period of 36 seconds when using default settings. The test time start depends on the settings of the detector ping interval (the “**Jeweller**” menu in the hub settings).

Jeweller Signal Strength Test

Detection Zone Test

Attenuation test

According to the requirements of EN50131, the level of the radio signal sent by wireless devices is reduced during the test mode.

Choosing an installation place

Before installing the detector, conduct the Jeweller signal strength test.

Install MotionProtect Outdoor at the height of 0.8 – 1.3 m, ensuring the upper lens axis to be parallel to the ground, and the supposed intrusion path is perpendicular to the lens axis.

MotionProtect Outdoor sends an alarm to the hub only if both PIR sensors detect identical motion. The difference in time of motion detection should not exceed 1.5 seconds.

Check the detector functioning at the alleged installation place. When choosing the location of MotionProtect Outdoor, take into account the radio signal communication range.

If the signal level is low (one bar), we cannot guarantee the stable operation of the detector. Take all possible measures to improve the quality of the signal. At least, move the detector: even a 20 cm shift can significantly improve the quality of signal reception.

If the detector has low or unstable signal strength even after moving, use a ReX radio signal range extender.

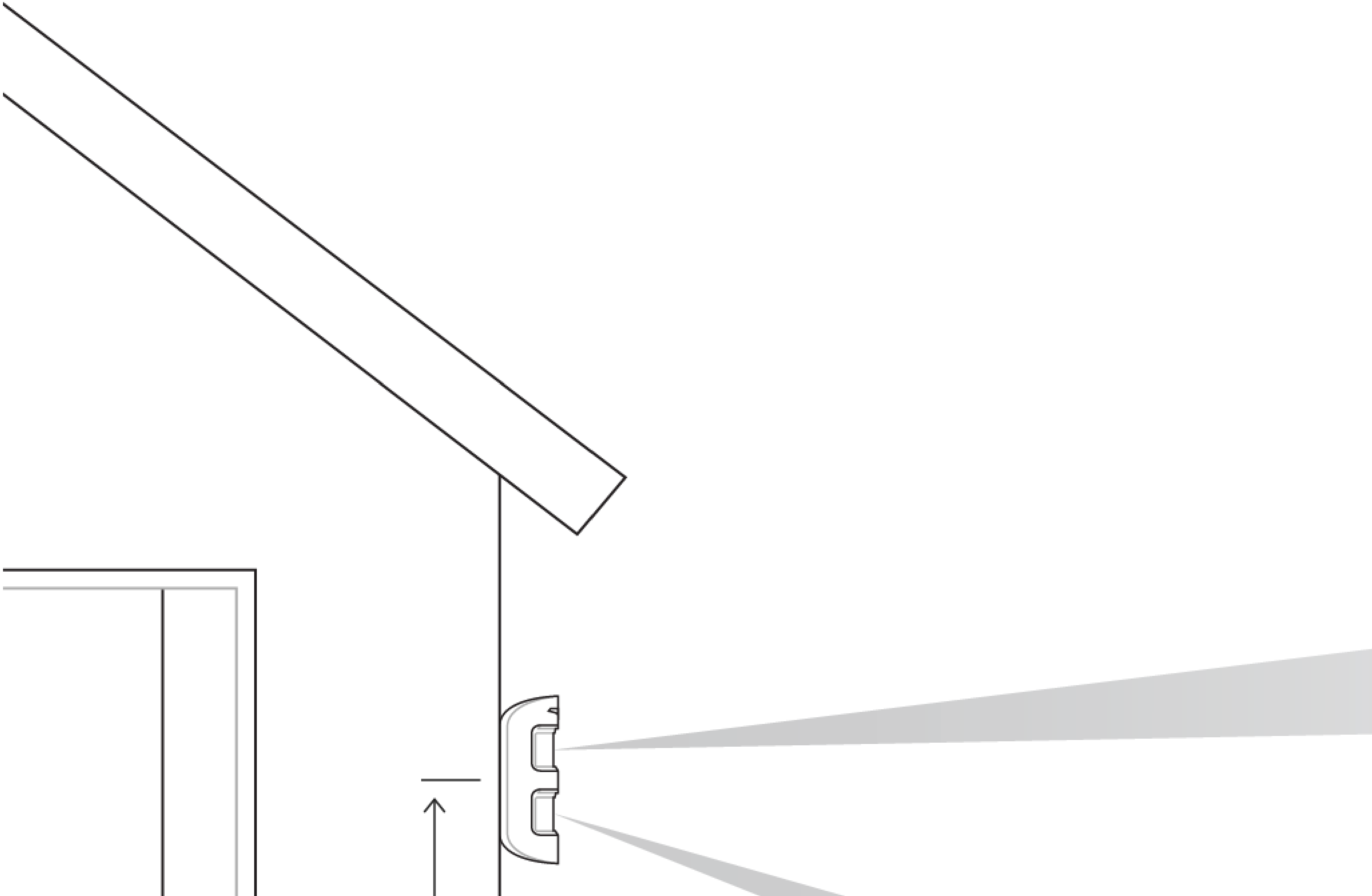
Be careful when mounting the attachment panel. Excessive force during its mounting can lead to deformation of the panel and, consequently, to the inability to install the detector or to its unreliable fixation. Attach SmartBracket with the bundled fixing tools. Using any other tools, e.g., large diameter screws may damage the attachment panel. We do not recommend using double-sided adhesive tape for permanent mounting. The tape runs dry with time, which can cause falling, false triggering, and detector malfunction.

Do not install the detector:

- Opposite the trees whose leaves can be in the detection zone of the upper and lower PIR sensors of the detector.
- Opposite the bushes higher than 80 cm.
- Near metal objects and mirrors (they can shield the radio signal and lead to its attenuation).
- Closer than 1 meter from the hub.

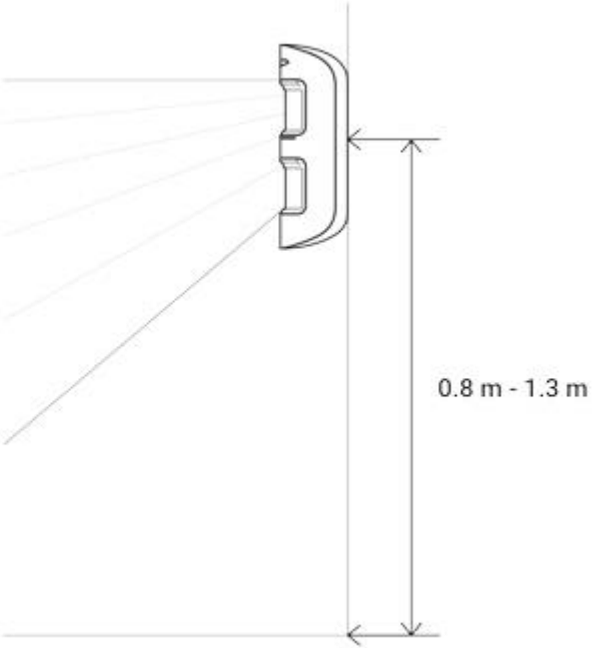
Note that MotionProtect Outdoor does not detect movement behind the glass. Therefore, do not install the detector in locations where glass objects can obstruct the detector’s view. For example, in places where a glass door can obstruct the view of the device.

Install detector at a height 0.8 to 1.3 meters so that its upper lens looks parallel to the ground. If the site is uneven, the installation height is considered from the highest point of the territory controlled by the detector.

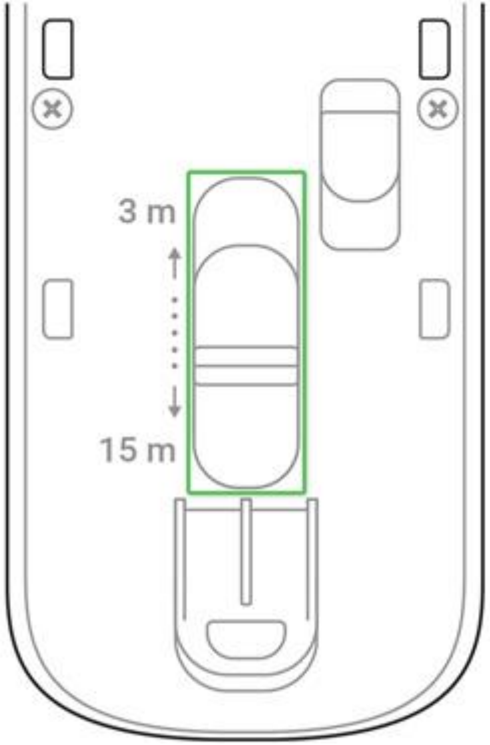


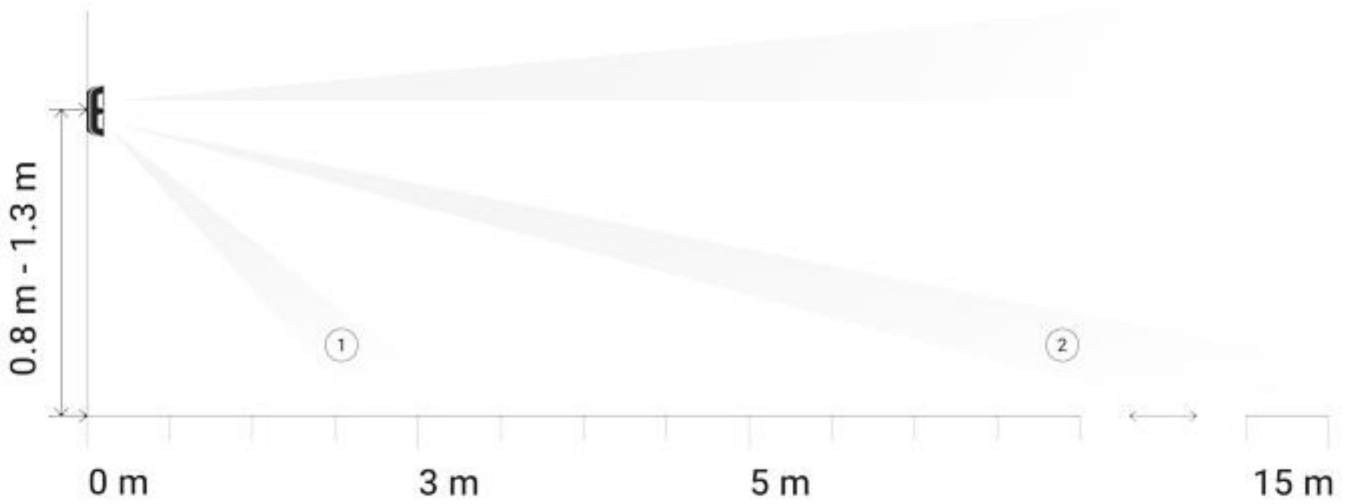
Detector installation procedure

1. Fix the SmartBracket attachment panel on the surface temporarily using bundled screws or double-sided adhesive tape. Consider the installation height: 0.8 – 1.3 meters.



2. Select the motion detection distance (3 to 15 m) using the adjustment scroll bar.

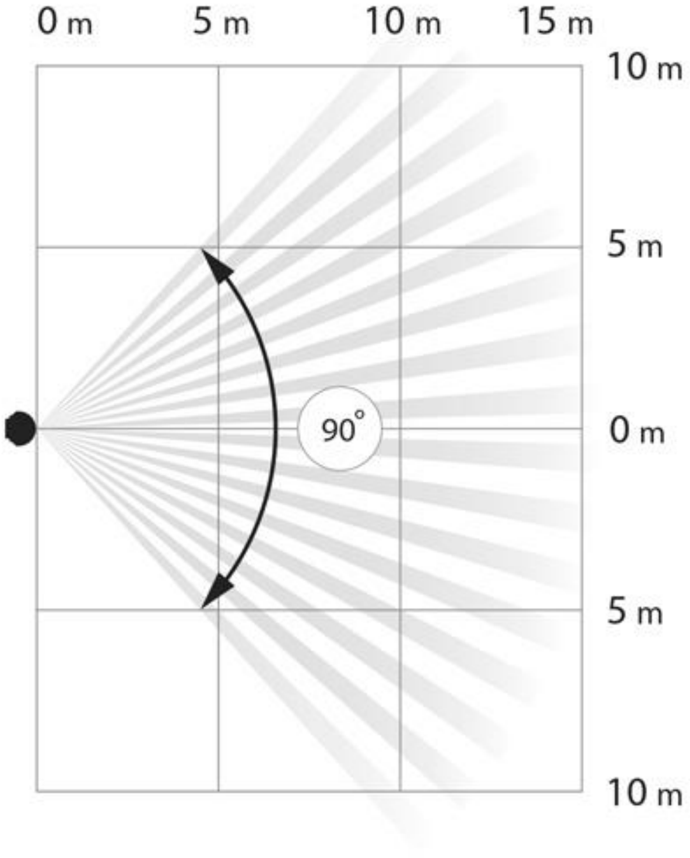




The lower PIR sensor beam direction with the specified minimum (1) and maximum (2) detection range

3. Put MotionProtect Outdoor on the SmartBracket attachment panel. Leave the detection area (horizontal detection angle — 90°) and make sure that there are no moving objects within the detection area to calibrate anti-masking

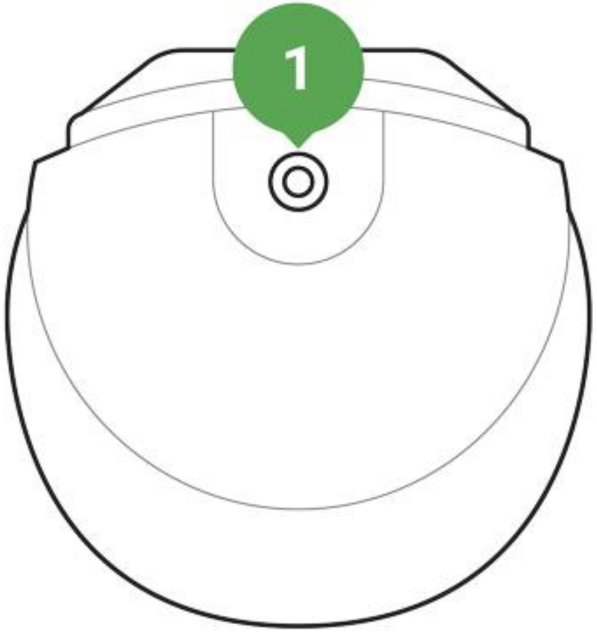
sensors properly.



Attention! The anti-masking sensors will begin to calibrate automatically when the detector has been put on the SmartBracket attachment panel. Calibration lasts up to 30 seconds and is followed by the flashing upper and lower LED indicators.

4. Conduct the Detection Zone Test for upper and lower sensors separately, both sensors simultaneously, and anti-masking test in the Ajax app. If the detector does not react to motion, select the appropriate sensitivity level, detection range, and check the detector slope angle.

5. If all tests have been appropriately passed, fix the SmartBracket to the surface with screws permanently, put MotionProtect Outdoor on the attachment panel, and wait until the end of calibration. Fix the detector on the attachment panel with the bundled screw.



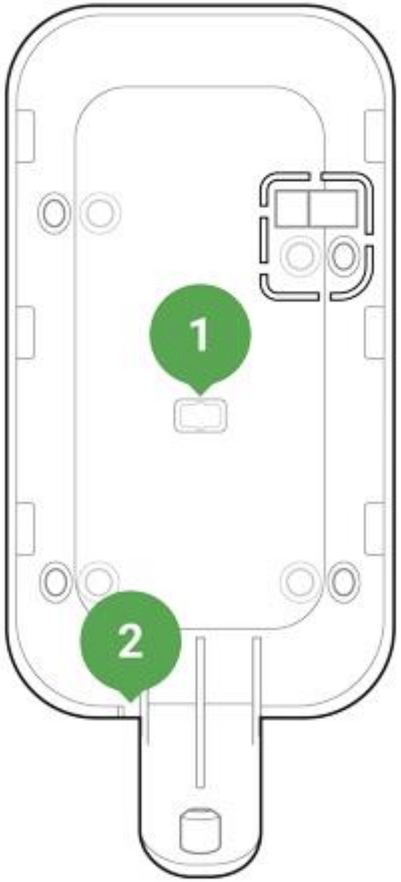
Connecting External Power Supply

MotionProtect Outdoor can use external power supply 5-28 V DC, 200 mA. If the external power supply is connected, there is no need to remove the pre-installed batteries. Batteries provide the detector with the backup power source.

To connect the external power supply:

1. Disassemble the detector body: remove the screws and open the lid.

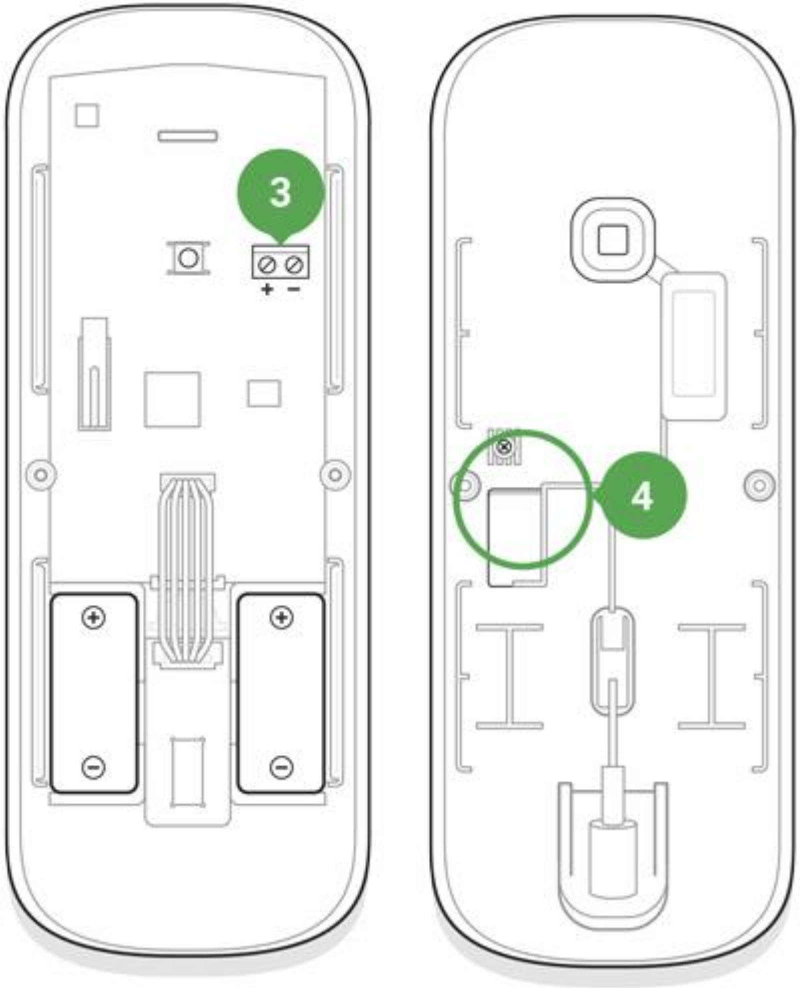
2. Break off special caps on the SmartBracket attachment panel:



1. A cap for putting out the power supply wire behind the SmartBracket attachment panel
2. A cap for putting out the power supply wire below the SmartBracket attachment panel

3. Run the external power supply dead wire through the attachment panel and cap.

4. Connect the cable to the terminal strips observing polarity. Fix the wire with the clamp.



3. Terminal strips on the detector board
4. The clamp on the back of the detector body

5. Switch on the power supply. The value of the **External Power Supply** field in the detector settings will change to **Connected**.

Use grounded power supply source only!

6. Fix the rear of the body with screws, install the detector and wait until the end of calibration.

Maintenance

Check the operational capability of the detector regularly. Clean the detector body from dust, spider web, and other contaminants as they appear. Use soft dry napkin suitable for tech equipment.

Do not use any substances containing alcohol, acetone, gasoline, and other active solvents to clean the detector.

The pre-installed battery ensures up to 5 years of autonomous operation (with the 3 minutes ping interval by the hub). If the detector battery is low, the system notifies the user, and the LED indicator smoothly lights up and goes off if a glass break is detected or the tamper is triggered.

Battery replacement

Tech Specs

Sensing element	PIR sensor, 2 pcs
Detection angle, horizontal	90°
Motion detection distance	Adjustable, 3–15 m when the detector is installed at 1 m height
Protection against masking	Yes
Pet ignoring function	Yes, height up to 80 cm when the detector is installed at 1 m height Why motion detectors react to animals and how to avoid it >
Protection against false triggering	Yes, algorithmic analysis
Frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz, depending on the sales region
Compatibility	Operates only with Hub, Hub Plus, Hub 2 and ReX
Maximum radio signal power	Up to 20 mW
Radio signal modulation	GFSK
Radio signal range	Up to 1,700 m (where there are no obstacles)

Power supply	2 x CR123A, 3 V
Battery life	Up to 5 years
External power	5 – 28 V DC, 200 mA
Usage	Indoors and outdoors
Body protection level	IP55
Anti-tamper switch	Yes
Operating temperature range	From -25°C to +60°C
Operating humidity	Up to 95%
Overall dimensions	183 x 70 x 65 mm
Weight	322 g

Complete set

1. MotionProtect Outdoor
2. SmartBracket mounting panel
3. CR123A battery — 2 pcs. (pre-installed)
4. Installation kit

5. Quick Start Guide

Warranty

Warranty for the “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase and does not apply to the pre-installed battery.

If the device does not work correctly, you should first contact the support service—in half of the cases, technical issues can be solved remotely!

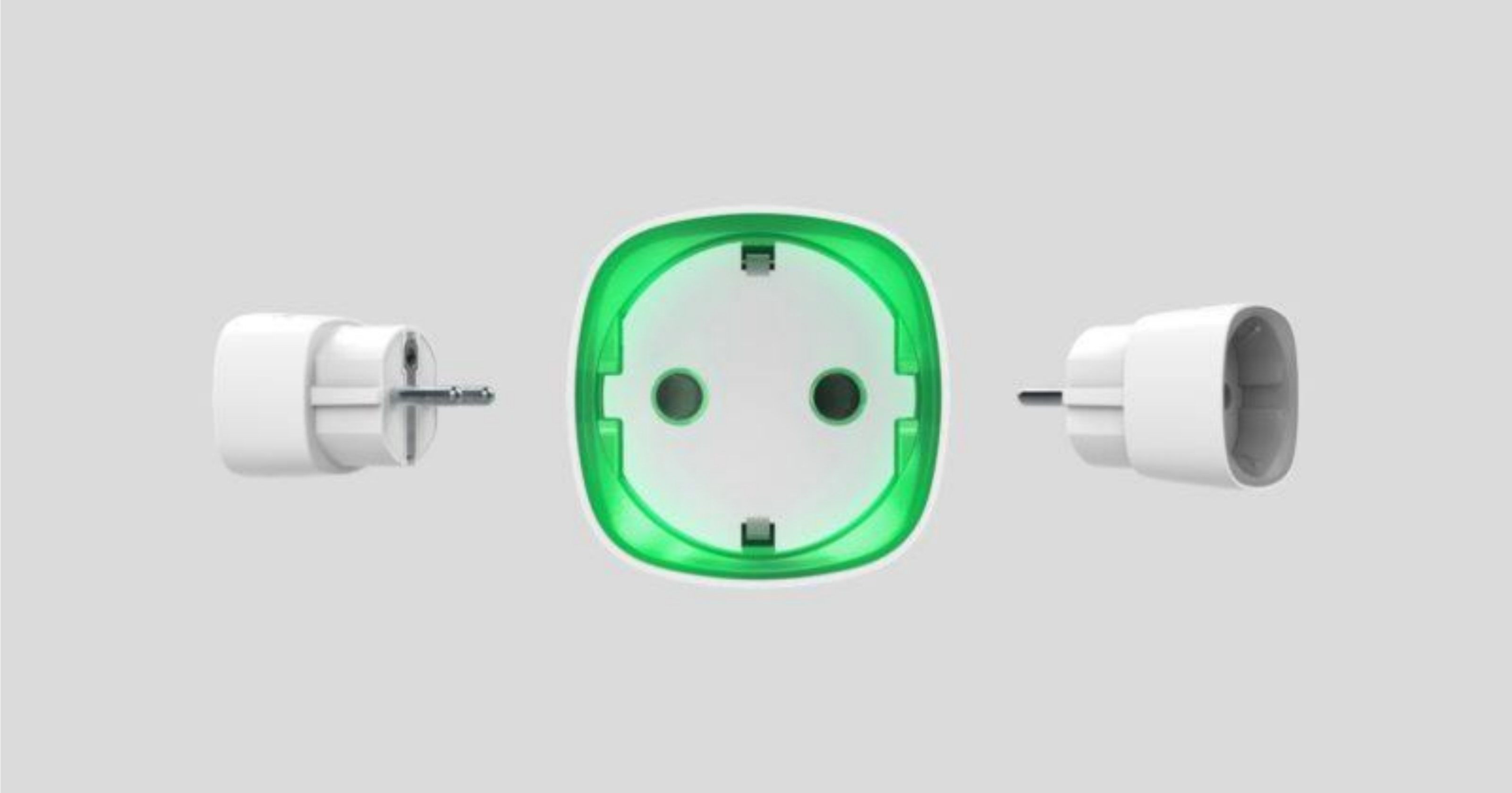
The full text of the warranty

User Agreement

Technical support: support@ajax.systems

Socket User Manual

Updated December 12, 2019



Socket — wireless smart plug with energy monitor, performed as a European type socket-to-plug adapter (Schuko type F) designed for controlling the power supply of electrical devices and rated at a load of up to 2.5 kW. It is equipped with overload protection, energy consumption meter and load level indicator. The device is connected to the Ajax security system via Jeweller secure technology, the communication range is up to 1,000 m without obstacles.

Socket only operates with Ajax hubs. Connection to uartBridge or ocBridge Plus integration modules is not provided

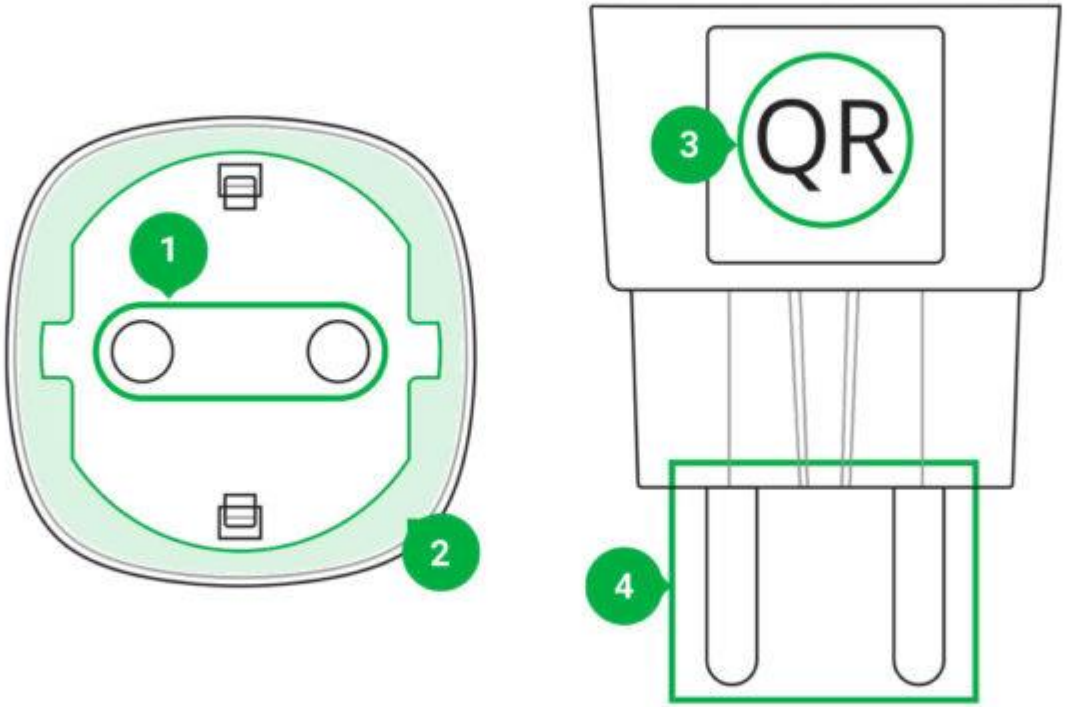
Use scenarios to program actions of automation devices (Relay, WallSwitch, Socket) in response to an alarm, pressing of the Button or by schedule. A scenario can be created remotely in the Ajax app.

How to create and configure a scenario in the Ajax security system

The Ajax security system is self-sustaining, but the user can connect it to the central monitoring station of a private security company.

Buy smart plug Socket

Functional Elements



1. Two-pin socket
2. LED border
3. QR Code
4. Two-pin plug

Socket Operating Principle

Socket turns on/off 230 V power supply according to the scenarios or at user command via the Ajax Security System application.

Socket is furnished with a protection system against voltage variation beyond the range of 184 – 253 V or over-current protection above 11A. In this case, power supply is interrupted, resuming after normalization of the voltage and current values.

Maximum resistive load — 2.5 kW. In the case of inductive or capacitive loads, the maximum current is reduced to 8 A at 230 V AC!

You may view the consumed power of the electrical appliances connected via Socket through the application. There is a consumed electricity meter.

Under insignificant loads (below 25 W), inaccurate current and power consumption readings may be displayed due to hardware limitations.

Connecting to the hub

Before starting connection:

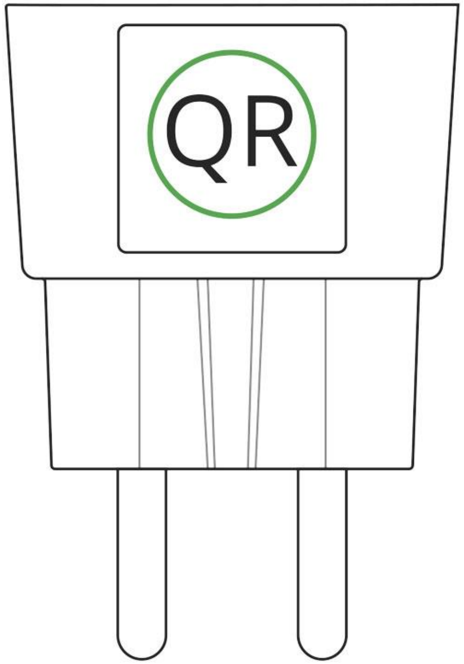
1. Following the hub instruction recommendations, install the Ajax application on your smartphone. Create an account, add the hub to the application, and create at least one room.
2. Go to the Ajax application.
3. Switch on the hub and check the internet connection (via Ethernet cable and/or GSM network).
4. Ensure that the hub is disarmed and does not start updates by checking its status in the mobile application.
5. Connect Socket to the power supply and wait for 30 seconds.

Only users with administrative rights can add the device to the hub.

How to connect Socket to the hub:

1. Select the **Add Device** option in the Ajax application.

2. Name the device, scan/write manually the **QR Code** (located on the body and packaging), and select the location room.



3. Select **Add** — the countdown will begin.

4. The device should automatically be added to the hub.

   If the Socket was previously assigned to the hub, connect a device with a load of at least 22 W for 5 s in the application during countdown (e.g. an electric kettle or iron) and then disconnect the load.

> The Socket will not be assigned to the hub if the smart socket communicates with another hub

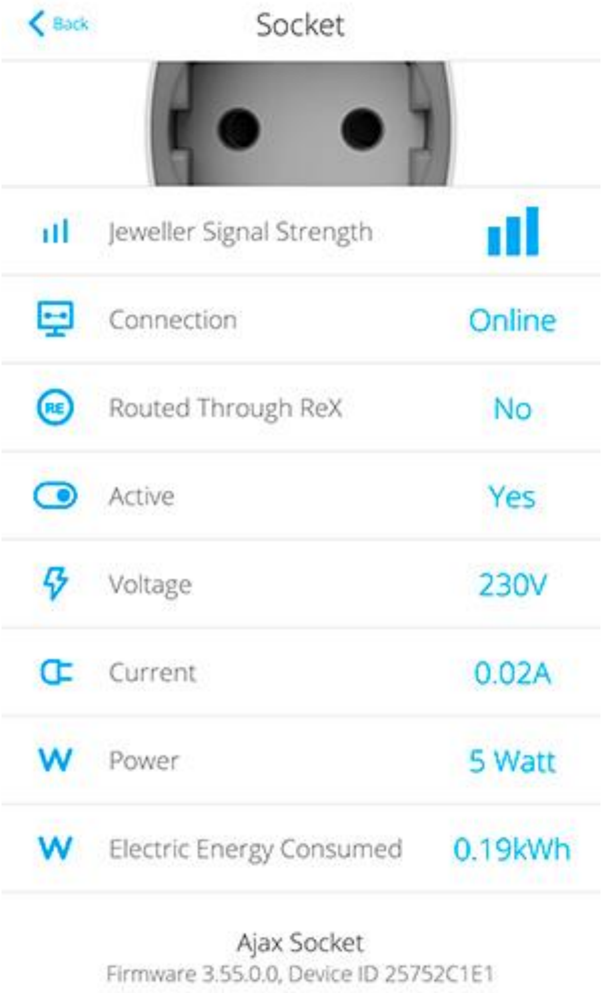
For the detection and interfacing to occur, the device should be located within the coverage area of the wireless network of the hub (at a single protected object). Request for connection to the hub is transmitted for a short time at the time of switching on the device.

If the connection to Ajax hub failed, wait 30 seconds and then try to add the device again.

Socket connected to the hub will appear in the list of devices of the hub in the application. Update of the detector statuses in the list depends on the device inquiry time set in the hub settings, with the default value – 36 seconds.

States

1. Devices
2. Socket



Socket

Jeweller Signal Strength	
Connection	Online
Routed Through ReX	No
Active	Yes
Voltage	230V
Current	0.02A
Power	5 Watt
Electric Energy Consumed	0.19kWh

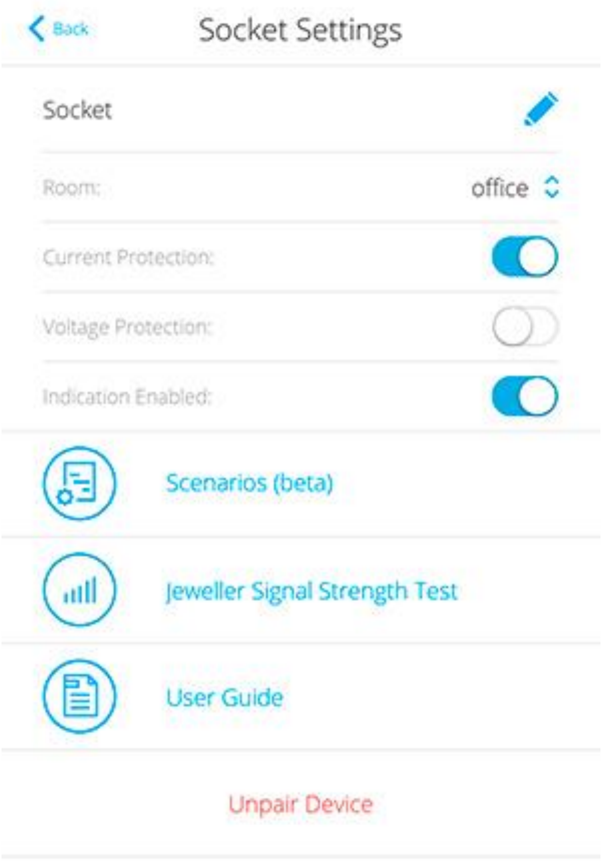
Ajax Socket
Firmware 3.55.0.0, Device ID 25752C1E1

Parameter	Value

Jeweller Signal Strength	Signal strength between the hub and the Socket
Connection	Connection status between the hub and the Socket
Routed Through ReX	Displays the status of using the ReX range extender
Active	State of the Socket (turned on/off)
Voltage	The current input voltage level of Socket
Current	Current at the Socket input
Power	Current consumption in W
Electric energy consumed	The electric power consumed by the device connected to the Socket. The counter is reset when the Socket lose the power
Firmware	Device firmware version
Device ID	Device identifier

Settings

1. Devices
2. Socket
3. Settings



Socket Settings

Socket

Room: office

Current Protection: ☑

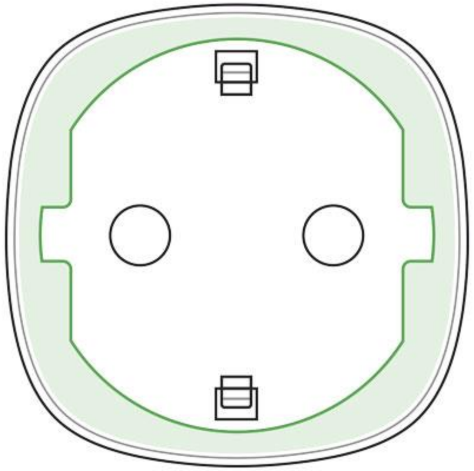
Voltage Protection: ☐

Indication Enabled: ☑

Setting	Value
First field	Device name, can be edited

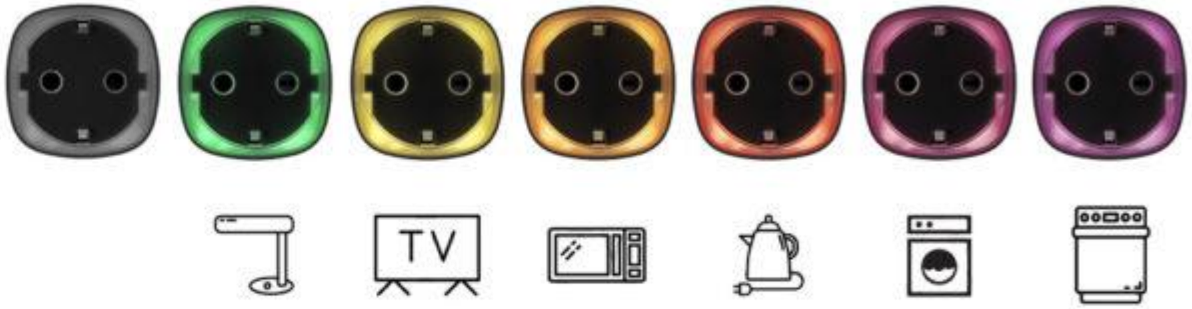
Room	Selecting the virtual room to which the device is assigned
Current protection	If active, power supply will be switched off if the strength of current exceeds 11A, in the inactive state the threshold is 16 A (or 13 A, if continues for 5 seconds)
Voltage protection	If active, power supply will be switched off in case of a voltage surge beyond the range of 184 – 253 V
Indication	The LED border shows the load level by means of color.
Scenarios	Opens the menu for creating and configuring scenarios Jeweller Signal Strength Test
Jeweller Signal Strength Test	Switches the device to the signal strength test mode
User Guide	Opens the Socket User Guide
Unpair Device	Disconnects the device from the hub and deletes its settings

Indication



The Socket informs the user of the power level consumed by connected appliances using the LED border.

If the load is more than 3 kW (purple), the current protection activates.



Load level	Indication
No power on the Socket	Don’t have any indication
Socket turned off	Blue

Socket turned on, no load	Green
~550 W	Yellow
~1250 W	Orange
~2000 W	Red
~2500 W	Dark red
~3000 W	Purple
One or more defenses triggered	Smoothly lights up and goes out red
Hardware failure	Quick red flashes

The exact power can be seen in the Ajax Security System application.

Functionality Testing

The Ajax security system allows conducting tests for checking the functionality of connected devices.

The tests do not start straight away but within a period of 36 seconds when using the standard settings. The test time start depends on the settings of the detector scanning period (the paragraph on “**Jeweller**” settings in hub settings).

Signal Strength Test

Installation of the Device

When choosing an installation place for the Socket, please consider the device remoteness from the hub and presence of objects that may obstruct the RF signal.

Do not install the device near sources of magnetic fields (magnets, magnetized objects, wireless chargers, etc.) and inside rooms with temperature and humidity outside the permissible limits!

To check the quality of the communication with the hub, test the signal strength in the Ajax Security System application for at least one minute.

If the device has a low or unstable signal strength, use a radio signal range extender ReX.

The Socket is designed to connect to a European two-pin socket (Schuko type F).

Maintenance

The device does not require maintenance.

Tech specs

Actuating element	Electromagnetic relay
Service life	At least 200,000 switches
Voltage and type of external power supply	230 V ±10% AC 50 Hz
Voltage protection for 230 V mains	Yes, 184–253 V
Maximum load current	11 A (continuous), 13A (up to 5 s)
Maximum current protection	Yes, 11 A if the protection is turned on, up to 13 A if the protection is turned off
Maximum temperature protection	Yes, +85°C. The socket turns off automatically if the temperature is exceeded
Electric shock protection class	Class I (with grounding terminal)
Energy consumption parameter check	Yes (current, voltage, power consumption)
Load indicator	Yes
Output power (resistive load at 230 V)	Up to 2.5 kW
Average energy consumption of the device on standby	Less than 1 W·h
Frequency band	868.0 – 868.6 MHz
Compatibility	Operates only with Hub, Hub Plus, Hub 2 and ReX
Maximum radio signal power	8,97 mW (limit 25 mW)
Radio signal modulation	GFSK
Radio signal range	Up to 1000 m (when there are no obstacles)

Operating temperature range	From 0°C to +40°C
Operating humidity	up to 75%
Protection class	IP20
Overall dimensions	65.5 x 45 x 45 mm (with plug)
Weight	58 g

In case of using inductive or capacitance load, the maximum switched current is reduced to 8 A at 230 V AC!

Complete Set

1. Socket
2. Quick Start Guide

Warranty

Warranty for the “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase.

Relay User Manual

Updated December 13, 2019

Relay is a wireless relay with a potential-free dry contact intended for switching appliances and devices on and off, powered by a 7–24 V DC source. The relay also has a pulse equipment control function. It is connected to the Ajax security system by the Jeweller secure protocol, the distance range is up to 1,000 meters if there are no obstacles.

The relay should be only installed by a qualified electrician! Regardless of the type of the electrical circuit in which the device is installed.

The built-in relay contacts are not galvanically connected to the device itself, so they can be connected to input control circuits for different equipment, imitating a button, switch, etc.

Operates only with Ajax hubs. Not compatible with the uartBridge or ocBridge Plus

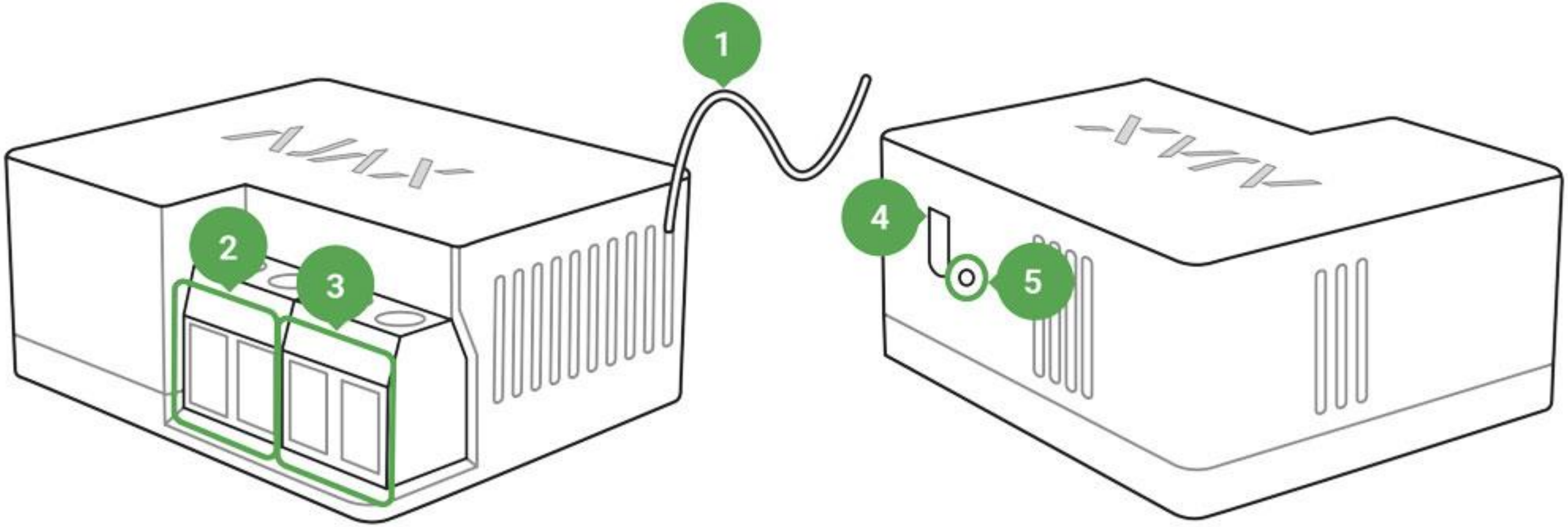
Use scenarios to program actions of automation devices (Relay, WallSwitch or Socket) in response to an alarm, pressing of the Button or by schedule. A scenario can be created remotely in the Ajax app.

How to create and configure a scenario in the Ajax security system

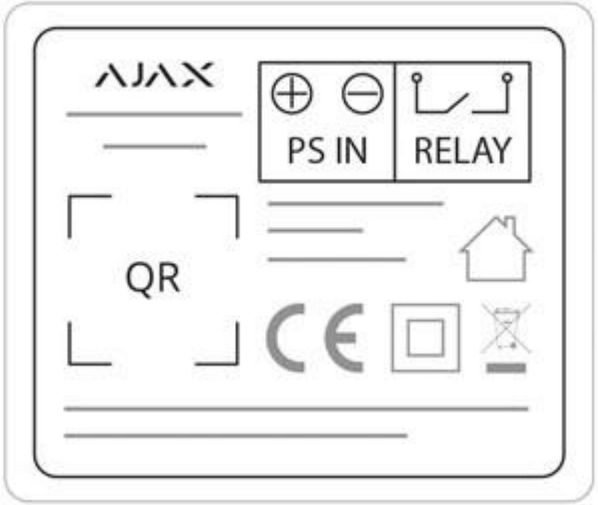
The Ajax security system is self-sustaining, but the user can connect it to the central monitoring station of a private security company.

Buy low-tension relay Relay

Functional Elements



1. Antenna
2. Power supply terminal block
3. Contacts terminal block
4. Function button
5. Light indicator



- **PS IN terminals** — “+” and “-” contact terminals, 7-24 V DC power supply.
- **Relay terminals** — output potential-free terminals of Relay contact terminals.

Relay Operating Principle

IMPORTANT: Do not connect the Relay power supply terminals to 110–230 V electric mains! Do not connect the Relay to a power supply with a voltage exceeding 36 V. It creates a fire hazard and will damage the device!

The Relay is powered by a 7–24 V DC source. The recommended voltage values for the Relay are 12 V and 24 V.

The Relay connection and setup is carried out via the Ajax Security System mobile app.

The built-in relay contacts are not galvanically connected to the device itself, so they can be connected to input control circuits for different equipment, imitating a button, switch, etc.

Relay can be used to power various loads (sirens, water shut off valves, electromagnetic locks).
The miniature body of the device enables it to be installed inside a junction box, electric switchboard, or the cases of switching units.

The device relay closes and opens the contact terminals on command via the Ajax Security System application. The feasibility of automatic turning on/off of the Relay in response to the arming or disarming of the system has also been implemented.

Relay operation modes:

- **Bistable** — the relay operates in the switch mode closing/opening contact terminals.
- **Pulse** —the relay closes/opens contact terminals for a specified period of time.

In the pulse mode, the Relay will close/open contact terminals for 0.5 to 15 seconds and then it will automatically perform the reverse action.

Connecting to the hub

Before starting connection:

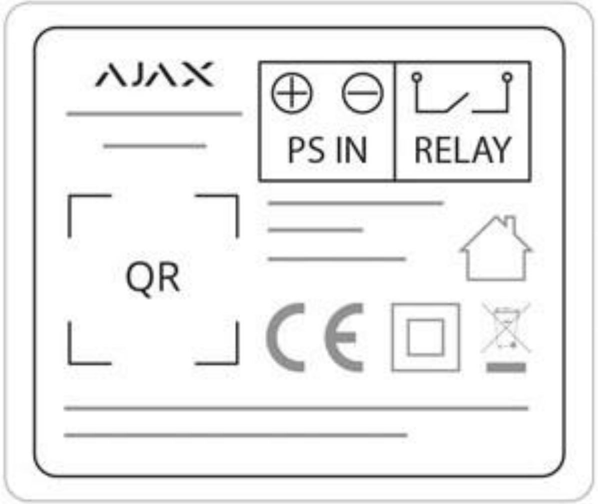
1. Following the hub instruction recommendations, install the Ajax application on your smartphone. Create an account, add the hub to the application, and create at least one room.
2. Go to the Ajax application.
3. Switch on the hub and check the internet connection (via Ethernet cable and/or GSM network).
4. Ensure that the hub is disarmed and does not start updates by checking its status in the mobile application.
5. Connect Relay to the power supply and wait for 30 seconds.

Only users with administrative privileges can add the device to the hub

How to connect the detector to the hub:

1. Select the **Add Device** option in the Ajax application.

2. Name the device, scan/write manually the **QR Code** (located on the body and packaging), and select the location room.



3. Select **Add** — the countdown will begin.
4. Press the Relay function button.

   For the detection and interfacing to occur, the device should be located within the coverage area of the wireless network of the hub (at a single protected object).

   Request for connection to the hub is transmitted for a short time at the time of switching on the device.

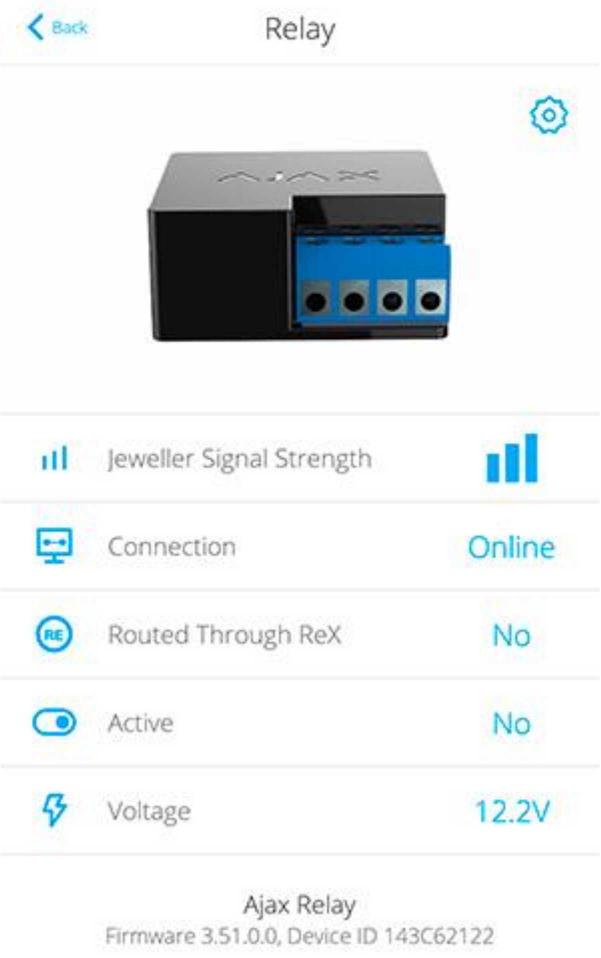
   If the connection to the hub fails, wait for 30 seconds and retry the connection procedure.

   The Relay connected to the hub will appear in the list of devices of the hub in the application. Update of the detector statuses in the list depends on the device inquiry time set in the hub settings, with the default value – 36 seconds.

Once the relay is switched on for the first time, it will be disengaged! Once the Relay is removed from the Ajax system, the switch will disengage the relay!

State

1. Devices
2. Relay



Jeweller Signal Strength

Connection Online

Routed Through ReX No

Active No

Voltage 12.2V

Ajax Relay

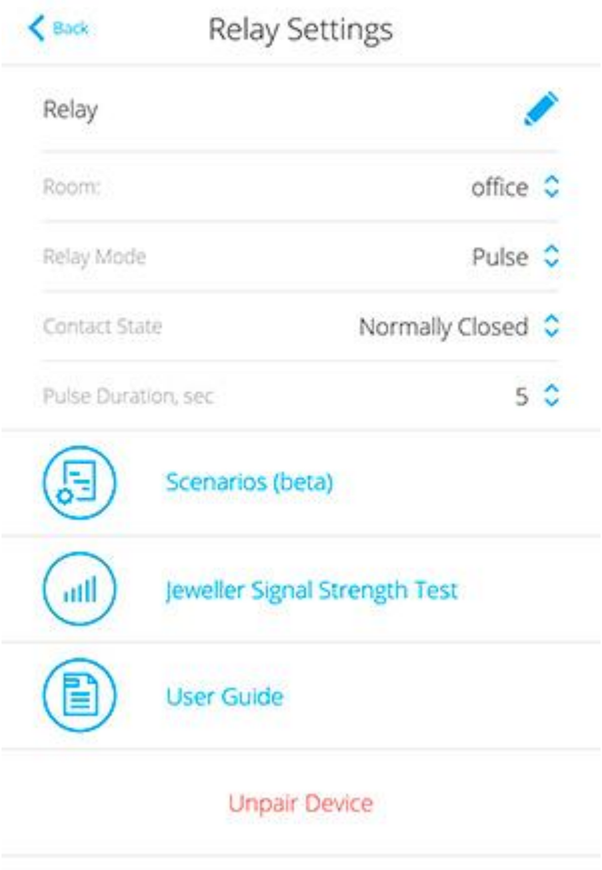
Firmware 3.51.0.0, Device ID 143C62122

Parameter	Value
Jeweller Signal Strength	Signal strength between the hub and the relay

Connection	Connection status between the hub and the relay
Routed Through ReX	Displays the status of using the ReX range extender
Active	State of the relay contacts (closed / open)
Voltage	The current input voltage level of Relay
Firmware	Device firmware version
Device ID	Device identifier

Settings

1. Devices
2. Relay
3. Settings



Relay

Room: office

Relay Mode Pulse

Contact State Normally Closed

Pulse Duration, sec 5

Settings	Value
First field	Device name, can be edited

Room	Selecting the virtual room to which the device is assigned
Relay mode	Choosing the relay operation mode Pulse Bistable
Contact state	Normal contact state Normally closed Normally open
Pulse duration, sec	Selecting the pulse duration in the pulse mode (from 0.5 to 15 seconds)
Scenarios	Opens the menu for creating and configuring scenarios
Jeweller Signal Strength Test	Switches the relay to the signal strength test mode
User Manual	Opens the Relay Manual
Unpair Device	Disconnects the relay from the hub and deletes its settings

Voltage protection — the contact will be opened when the voltage falls outside the limits of 6.5–36.5 V.

Temperature protection — the contact will be opened when the threshold temperature of 85°C is reached inside the Relay.

Indication

The Relay light indicator may light up green depending on the device status.

The green LED of Relay will blink intermittently if it is not assigned to the hub. When the functional button is pressed, the green LED lights up.

Functionality Testing

The Ajax security system allows conducting tests for checking the functionality of connected devices.

The tests do not start straight away but within a period of 36 seconds when using the standard settings. The test time start depends on the settings of the detector scanning period (the paragraph on “**Jeweller**” settings in hub settings).

Signal Strength Test

Installation of the Relay

The relay should be only installed by a qualified electrician! Regardless of the type of the electrical circuit in which the device is installed.

Communication range with the hub absent any obstacles between the devices – up to 1,000 meters. Take account of this when choosing the location for Relay.

If the device has a low or unstable signal strength, use a radio signal range extender ReX.

1. De-energize the cable to which Relay will be connected.
2. Connect the power supply cable to the Relay terminals, and then the Relay contact terminals to the required circuit with wires/cable of a sufficient cross-section. It’s recommended to use cables with cross-section of 1.5 – 2 mm^2.
3. If the device is installed in a connection box, install the antenna outside. The further the antenna is located away from metal structures, the less the chance of radio signal shielding. The antenna must not be shortened under any circumstances.

During the Relay installation and operation, follow the general electrical safety rules for using electrical devices, as well as the requirements of the electrical safety regulations. It is expressly prohibited to disassemble the device.

Do not install the Relay:

1. Outside the premises (outdoors).
2. In metal junction boxes and electric service panels.

3. In rooms with a temperature and humidity outside the allowable limits.
4. Closer than 1 m from the hub.

Maintenance

The device does not require maintenance.

Tech Specs

Actuating element	Electromagnetic relay
The service life of the relay	200,000 switchings
Supply voltage range	7 – 24 V (DC only)
Voltage protection	Yes, min — 6.5 V, max — 36.5 V
Maximum load current*	5 A at 24 V DC, 13 A at 230 V AC
Maximum current protection	No
Output power* (resitive load 230 V)	Up to 3 kW

Parameter control	Yes (voltage)
Device energy consumption	Less than 1 W·h
Frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz depending on the region of sale
Compatibility	Operates only with Hub, Hub Plus, Hub 2 and ReX
Effective radiated power	3.99 mW (6.01 dBm), limit — 25 mW
Modulation of the radio signal	GFSK
Maximum distance between the device and the hub	Up to 1000 m (any obstacles absent)
Communication ping with the receiver	12 – 300 sec (36 sec default)
Shell protection rating	IP20
Operation temperature range	From 0°C to +64°C (ambient)
Max. temperature protection	Yes, over 65°C at the place of installation or over 85°C inside the Relay
Operating humidity	Up to 75%
Dimensions	39 x 33 x 18 mm
Weight	25 g

If using inductive or capacitive load, the maximum commutated current decreases to 3 A at 24 V DC and to 8 A at 230 V AC!

Complete Set

1. Relay
2. Connecting wires – 2 pcs
3. Quick Start Guide

Warranty

Warranty for the “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase.

If the device does not work correctly, you should first contact the support service—in half of the cases, technical issues can be solved remotely!

The full text of the warranty

User Agreement

Technical support: support@ajax.systems

WallSwitch User manual

Updated December 16, 2019

WallSwitch is a device that combines a wireless power on/off relay for electrical appliances and a power consumption meter. The miniature body of the device is adapted for installation in a European type socket.

WallSwitch should be only installed by a qualified electrician! Regardless of the type of the electrical circuit in which the device is installed.

WallSwitch operates only with the Ajax security system (it may not be used in any third-party security systems), by connecting via the protected Jeweller protocol to the hub. Communication range – up to 1,000 meters, absent any obstacles.

Operates only with Ajax hubs. Connection to ocBridge and uartBridge integration modules is not provided.

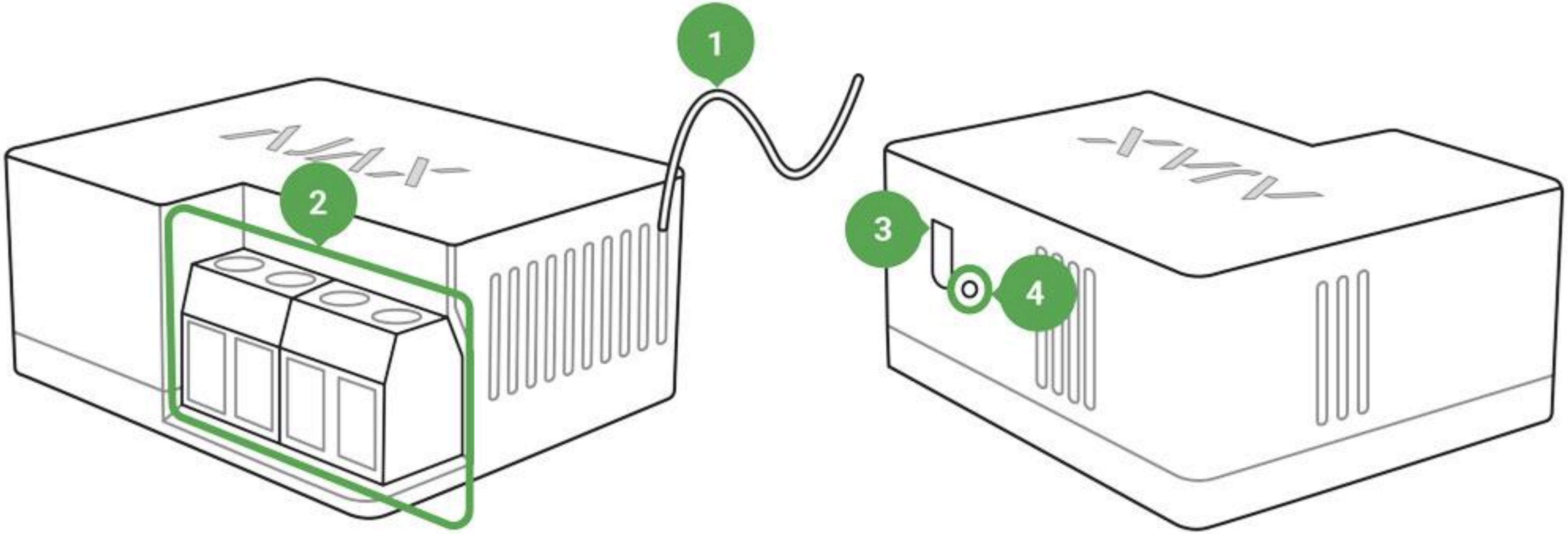
Use scenarios to program actions of automation devices (Relay, WallSwitch or Socket) in response to an alarm, pressing of the Button or by schedule. A scenario can be created remotely in the Ajax app.

How to create and configure a scenario in the Ajax security system

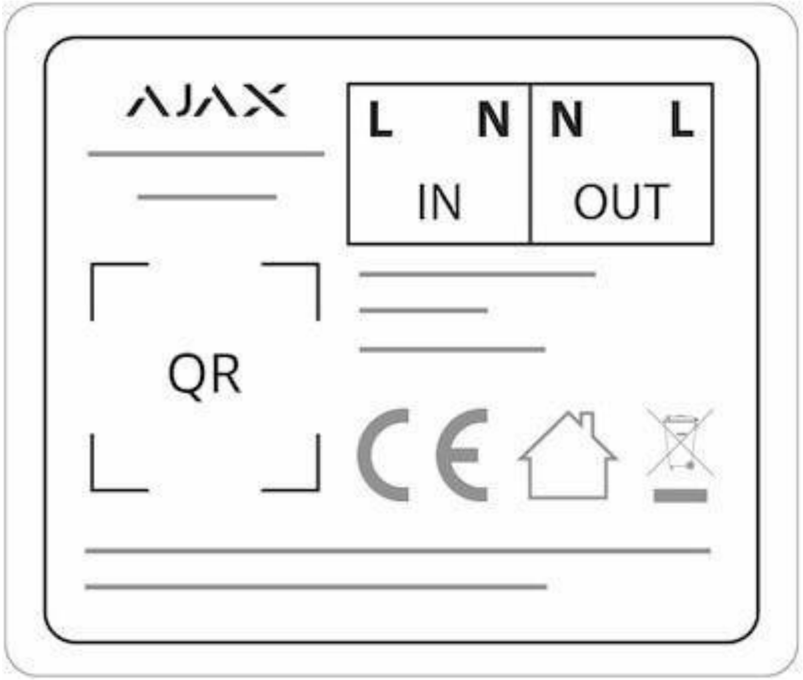
The Ajax security system is self-sustaining, but the user can connect it to the central monitoring station of a private security company.

Buy power relay WallSwitch

Functional Elements



1. Antenna
2. Terminal blocks
3. Functional button
4. Light indicator



IN terminals:

- **L terminal** — power supply phase terminal.
- **N terminal** — power supply neutral terminal.

OUT terminals:

- **N terminal** — connected device neutral output contact terminal.
- **L terminal** — connected device phase output contact terminal.

WallSwitch Operating Principle

The WallSwitch input terminals are connected to the mains, and the output terminals are connected to the socket or electrical appliance/electrical system of the room. WallSwitch turns on/off 230 V power supply according to the scenarios or at user command via the Ajax Security System application.

WallSwitch is furnished with a protection system against voltage variation beyond the range of 184V – 253V or overcurrent protection above 13A. In this case, the power supply is interrupted, resuming after normalization of the voltage and current values.

The maximum resistive load on the relay is 3 kW.

You may view the consumed power of the electrical appliances connected via WallSwitch through the application. There is a consumed electricity meter in place.

Connecting to the hub

Before starting connection:

1. Following the hub instruction recommendations, install the Ajax application on your smartphone. Create an account, add the hub to the application, and create at least one room.

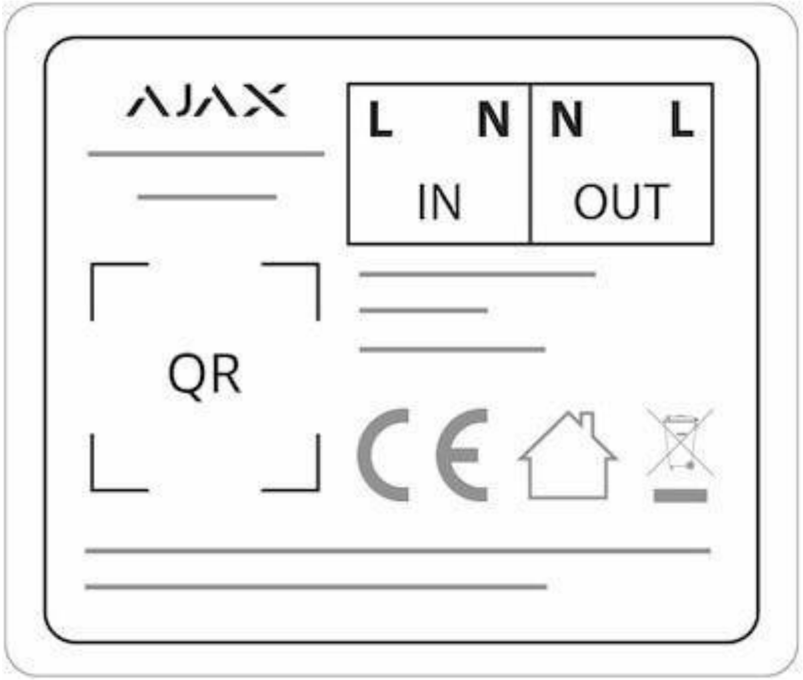
2. Go to the Ajax application.
3. Switch on the hub and check the internet connection (via Ethernet cable and/or GSM network).
4. Ensure that the hub is disarmed and does not start updates by checking its status in the mobile application.
5. Connect WallSwitch to the power supply and wait for 30 seconds.

> Only users with administrative privileges can add the device to the hub.

How to connect the WallSwitch to the hub:

1. Select the **Add Device** option in the Ajax application.

2. Name the device, scan/write manually the **QR Code** (located on the body and packaging), and select the location room.



3. Select **Add** — the countdown will begin.

4. Press the WallSwitch functional button (or apply the load to the device no less than 20 W, e.g. by switching on an iron or electric kettle).

For the detection and interfacing to occur, the device should be located within the coverage area of the wireless network of the hub (at a single protected object).

Request for connection to the hub is transmitted for a short time at the time of switching on the device.

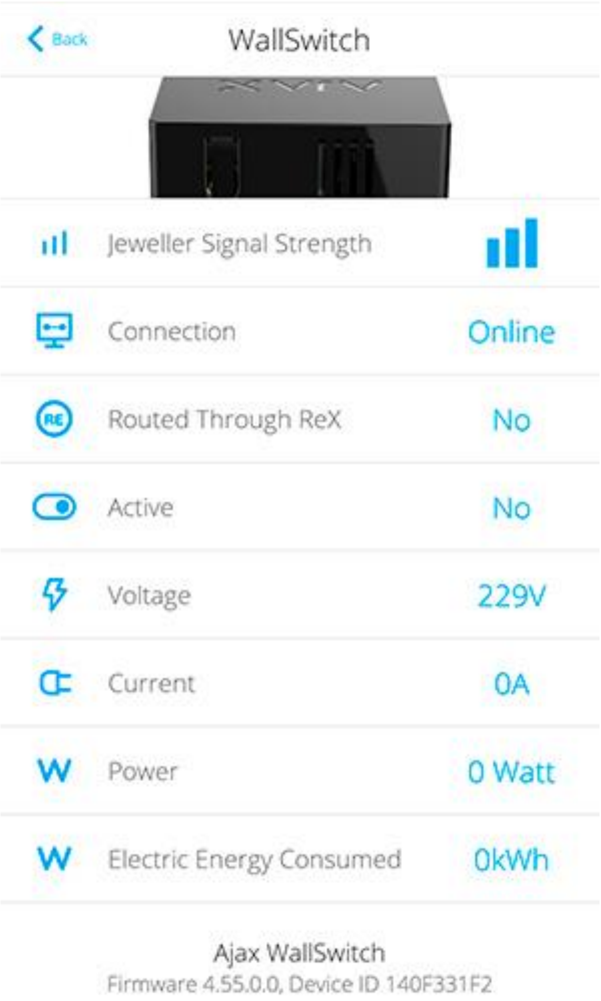
If the connection to the hub fails, wait for 30 seconds and retry the connection procedure.

The WallSwitch connected to the hub will appear in the list of devices of the hub in the application. Update of the detector statuses in the list depends on the device inquiry time set in the hub settings, with the default value – 36 seconds.

When switching on for the first time, the relay is in open status! After deleting WallSwitch from the system, the Ajax switch opens the relay!

States

1. Devices
2. WallSwitch



Back

WallSwitch

Jeweller Signal Strength

Connection: Online

Routed Through ReX: No

Active: No

Voltage: 229V

Current: 0A

Power: 0 Watt

Electric Energy Consumed: 0kWh

Ajax WallSwitch

Firmware 4.55.0.0, Device ID 140F331F2

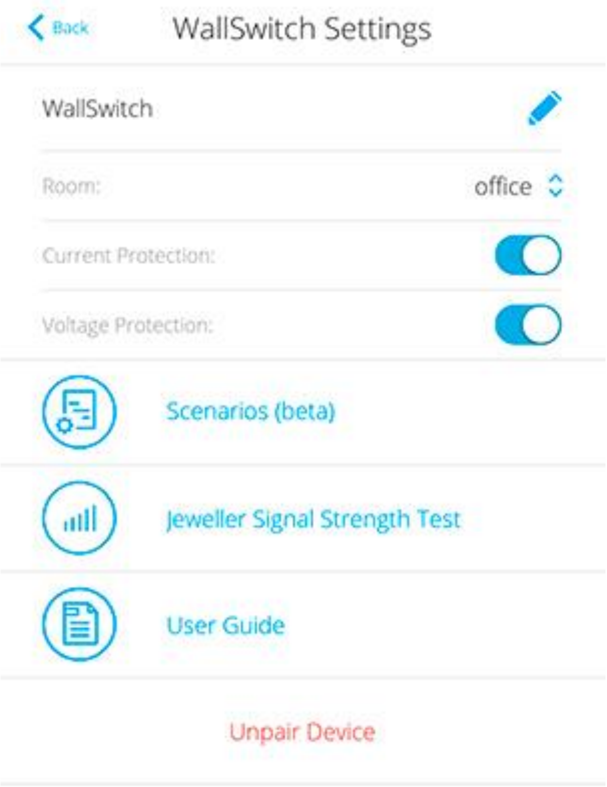
Parameter	Value
Jeweller Signal Strength	Signal strength between the hub and the relay

Connection	Connection status between the hub and the relay
Routed Through ReX	Displays the status of using the ReX range extender
Active	State of the relay (turned on/off)
Voltage	The current input voltage level of WallSwitch
Current	Current at the relay input
Power	Current consumption in W
Electric energy consumed	The electric power consumed by the device connected to the relay. The counter is reset when the relay loses the power
Firmware	Device firmware version
Device ID	Device identifier

Settings

1. Devices
2. WallSwitch

3. Settings



WallSwitch

Room: office

Current Protection:

Voltage Protection:

Setting	Value

First field	Device name, can be edited
Room	Selecting the virtual room to which the device is assigned
Current protection	If active, power supply will be switched off if the strength of current exceeds 13 A, in the inactive state the threshold is 19,8 A (or 16 A, if continues for 5 seconds)
Voltage protection	If active, power supply will be switched off in case of a voltage surge beyond the range of 184 – 253 V, in the inactive state — 0 – 500 V
Scenarios	Opens the menu for creating and configuring scenarios
Jeweller Signal Strength Test	Switches the device to the Jeweller signal strength test mode
User Manual	Opens the WallSwitch User Manual
Unpair Device	Disconnects the relay from the hub and deletes its settings

Indication

The WallSwitch light indicator may light up green depending on the device status.

The green LED of WallSwitch will blink intermittently if it is not assigned to the hub. When the functional button is pressed, the green LED lights up.

Functionality testing

The Ajax security system allows conducting tests for checking the functionality of connected devices.

The tests do not start straight away but within a period of 36 seconds when using the standard settings. The test time start depends on the settings of the detector scanning period (the paragraph on “**Jeweller**” settings in hub settings).

Signal Strength Test

Installation of the Device

WallSwitch should be only installed by a qualified electrician! Regardless of the type of the electrical circuit in which the device is installed

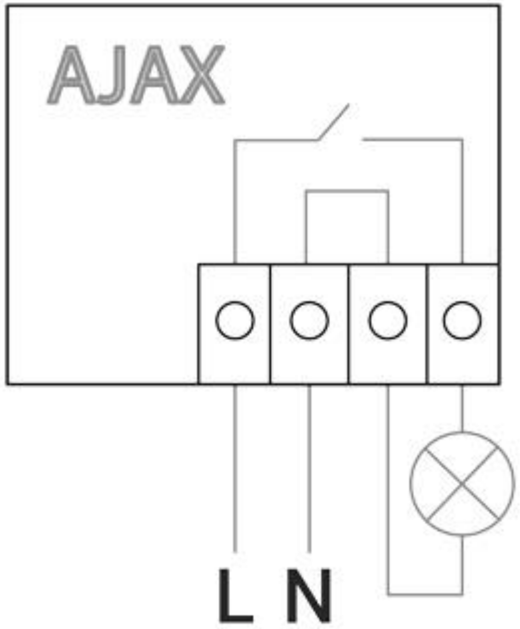
WallSwitch is designed for installation inside a socket box with the diameter 50 mm and more and the depth no less than 70 mm. The relay can also be installed within extension cords and other circuits powered by 230 V.

Communication range with the hub absent any obstacles between the devices – up to 1,000 meters. Take account of this when choosing the location for WallSwitch.

If the device has a low or unstable signal strength, use a radio signal range extender ReX.

Installation process:

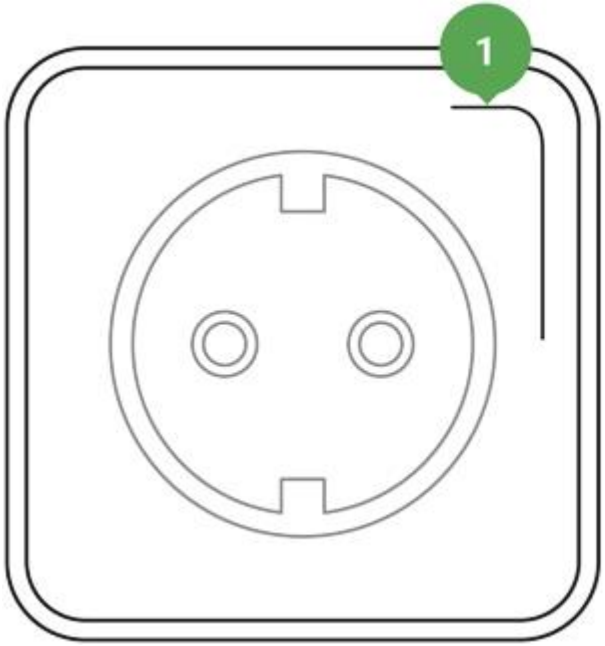
1. De-energize the cable to which WallSwitch will be connected.
2. Connect the cable of the power system of the room to the WallSwitch terminals according to the following scheme:



3. Connect a socket to the WallSwitch using bundled connecting wires or an electrical appliance using a cable with the sufficient cross-section. It’s recommended to use cables with cross-section of 1.5 – 2 mm^2.

Do not connect more than 3 kW load to the WallSwitch. When connecting the load, strictly observe the connection diagram since an incorrect connection may cause the device to malfunction and/or damage the property.

In installing the WallSwitch in the socket box, lead out the antenna to the outside and place it under the plastic frame of the socket. The more distanced the antenna is from metal structures, the lower is the risk of screening (and impairment) of the radio signal.



1 — recommended antenna location

In no case, do not shorten the antenna! Its length is optimal for operation within the used radio frequency range!

During installation and operation of WallSwitch, please adhere to general rules of electrical safety when using electrical appliances, as well as the requirements of electrical safety regulations.

It is expressly forbidden to disassemble the device. Do not use the device with damaged power cables.

Do not install the relay:

1. Outside
2. In metal wiring boxes and electrical panels
3. In places with temperature and humidity exceeding the permissible limits
4. Closer than 1 m from the hub

Maintenance

The device does not require maintenance.

Tech specs

Actuating element	Electromagnetic relay
The service life of the relay	200,000 switching-ons
Supply voltage	110 – 240 V AC ± 10% 50/60 Hz

Voltage protection	For 230 V mains: max — 253 V, min — 184 V For 110 V mains: max — 126 V, min — 77 V
Maximum load current	13 A
Maximum current protection	Yes, 13 A
Power output (resistance load 230 V)	Up to 3 kW
Electricity meter function	Yes
Power consumption parameters control	Yes: current, voltage, consumed power
The power consumption of the device in the standby mode	Less than 1 W·h
Frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz depending on the region of sale
Compatibility	Operates only with Hub, Hub Plus, Hub 2 and ReX
Maximum RF output power	Up to 25 mW
Modulation	GFSK
Radio signal range	Up to 1,000 m (any obstacles absent)
Shell protection rating	IP20
Operating temperature range	From 0°C to +64°C
Maximum temperature protection	Yes, 65°C
Operating humidity	Up to 75%

Overall dimensions	39 x 33 x 18 mm
Weight	30 g

Complete Set

1. WallSwitch
2. Connecting wires – 2 pcs
3. User Manual

Warranty

Warranty for the “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase.

If the device does not work correctly, you should first contact the support service—in half of the cases, technical issues can be solved remotely!

The full text of the warranty

HomeSiren User Manual

Updated December 10, 2019

HomeSiren is a wireless home siren with the capacity up to 105 dB. It can be quickly installed and set up, is furnished with a LED (plus allows connecting an external LED), and can operate up to 5 years from a battery.

HomeSiren operates within the Ajax security system, by connecting via the protected Jeweller protocol to the hub. The communication range is up to 2,000 meters if there are no obstacles.

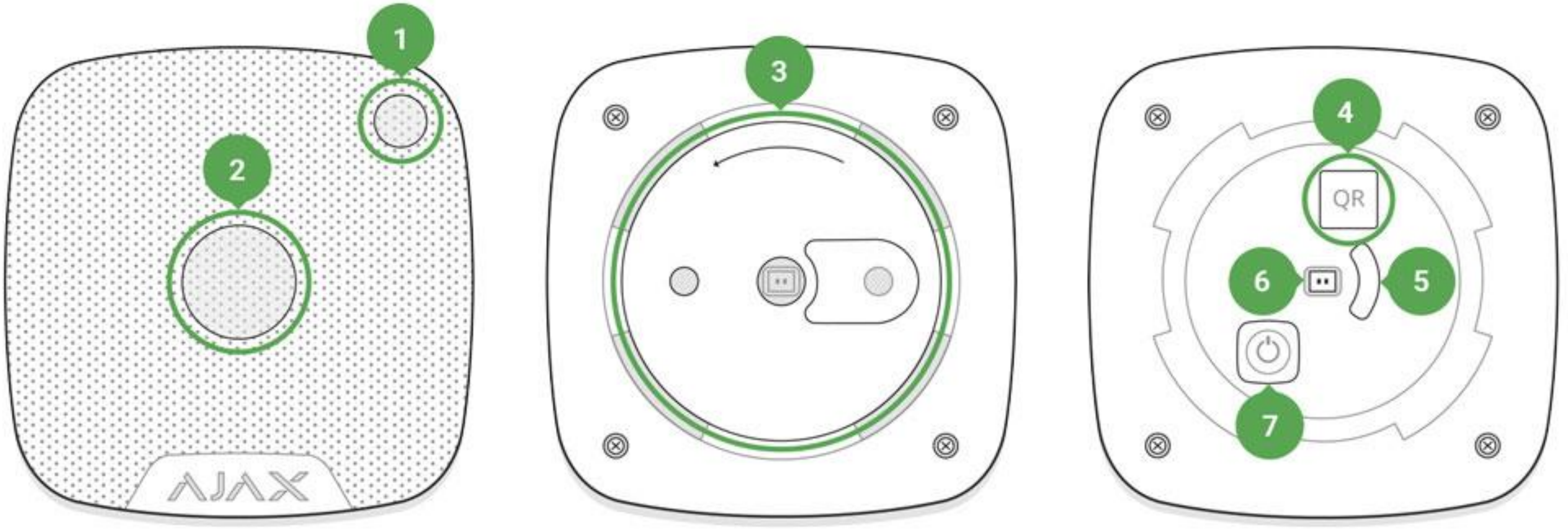
The siren is set up via a mobile application for iOS and Android-based smartphones. The user is notified of all events through push notifications, SMS messages and calls (if activated).

Operates only with Ajax hubs. Connection to ocBridge and uartBridge integration modules is not provided.

The Ajax security system is self-sustaining, but the user can connect it to the central monitoring station of a private security company.

Buy home siren HomeSiren

Functional elements



1. Light indicator
2. Siren buzzer covered with a fabric
3. SmartBracket attachment panel (perforated part is required for actuating the tamper in case of any attempt to tear off the siren from the surface)
4. QR code

5. Tamper button
6. Socket for connecting an outside-mounted light indicator
7. On/off button

HomeSiren Operating Principle

The siren significantly improves the efficiency of the security system, being the most operational means of response to the intrusion into a room. With a high probability, its alarm signal will be sufficient to frighten away the intruders.

The device is furnished with a loud buzzer – the sound of the siren can be heard from far. Subject to correct installation, it would be hard to dismount and deactivate the actuated siren: the body is firm, the power supply is autonomous, and the on/off button will be blocked when the security system is set in the guard mode.

Connecting the Siren to the hub

The HomeSiren siren operates only with the Ajax security system. Up to 10 sirens may be connected to the Ajax hub

Before starting connection:

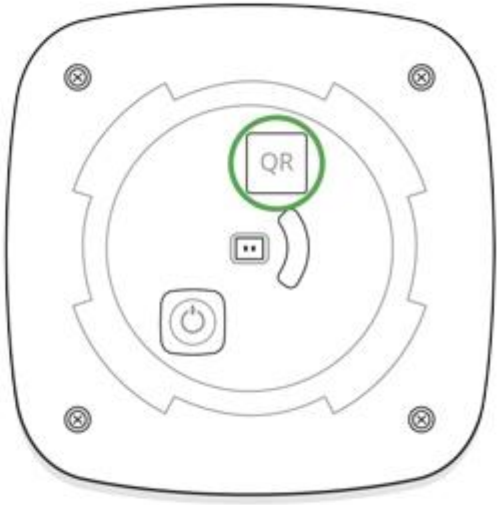
1. Following the hub instruction recommendations, install the Ajax application on your smartphone. Create an account, add the hub to the application, and create at least one room.
2. Go to the Ajax application.
3. Switch on the hub and check the internet connection (via Ethernet cable and/or GSM network).
4. Ensure that the hub is disarmed and does not start updates by checking its status in the mobile application.

> Only users with administrative privileges can add the device to the hub

How to connect the siren to the hub:

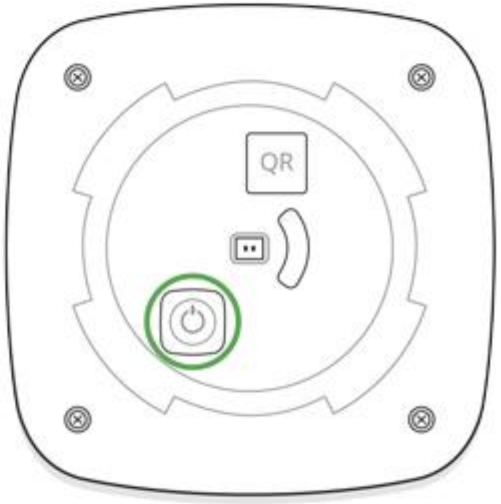
1. Select the **Add Device** option in the Ajax application.

2. Name the device, scan/write manually the **QR Code** (located on the body and packaging), and select the location room.



3. Select **Add** — the countdown will begin.

4. Switch on the device (by pressing on/off button for 3 seconds).



For the detection and interfacing to occur, the siren should be located within the coverage area of the wireless network of the hub (at a single protected object). If the device was already assigned to another hub, switch off HomeSiren and then perform the standard adding procedure.

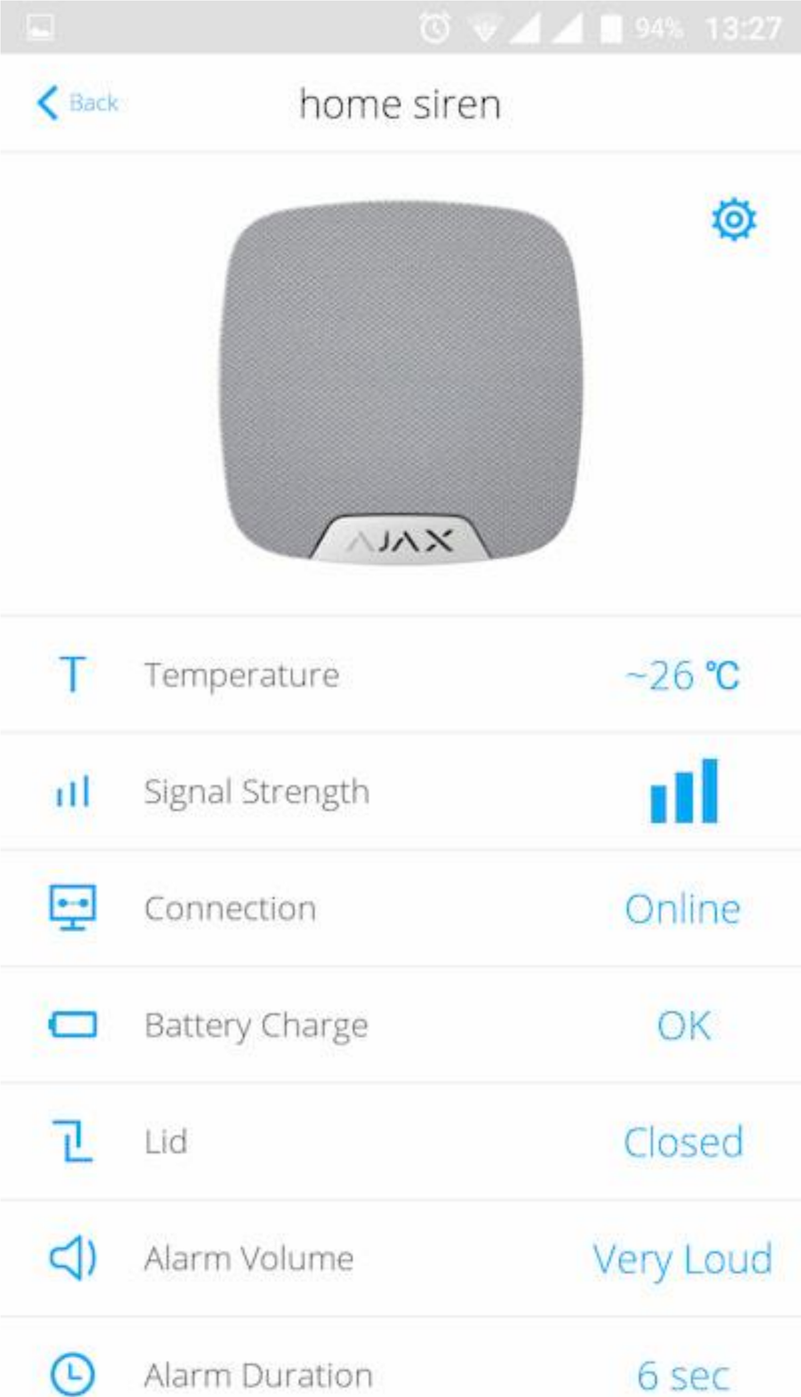
Request for connection to the hub is transmitted for a short time at the time of switching on the device.

If the connection to the Ajax hub failed, the siren will switch off after 6 seconds. You may repeat the connection attempt then. To retry the connection, you do not need to turn off the device.

The siren connected to the hub will appear in the list of devices of the hub in the application. Update of the siren statuses in the list depends on the device inquiry time set in the hub settings, with the default value – 36 seconds.

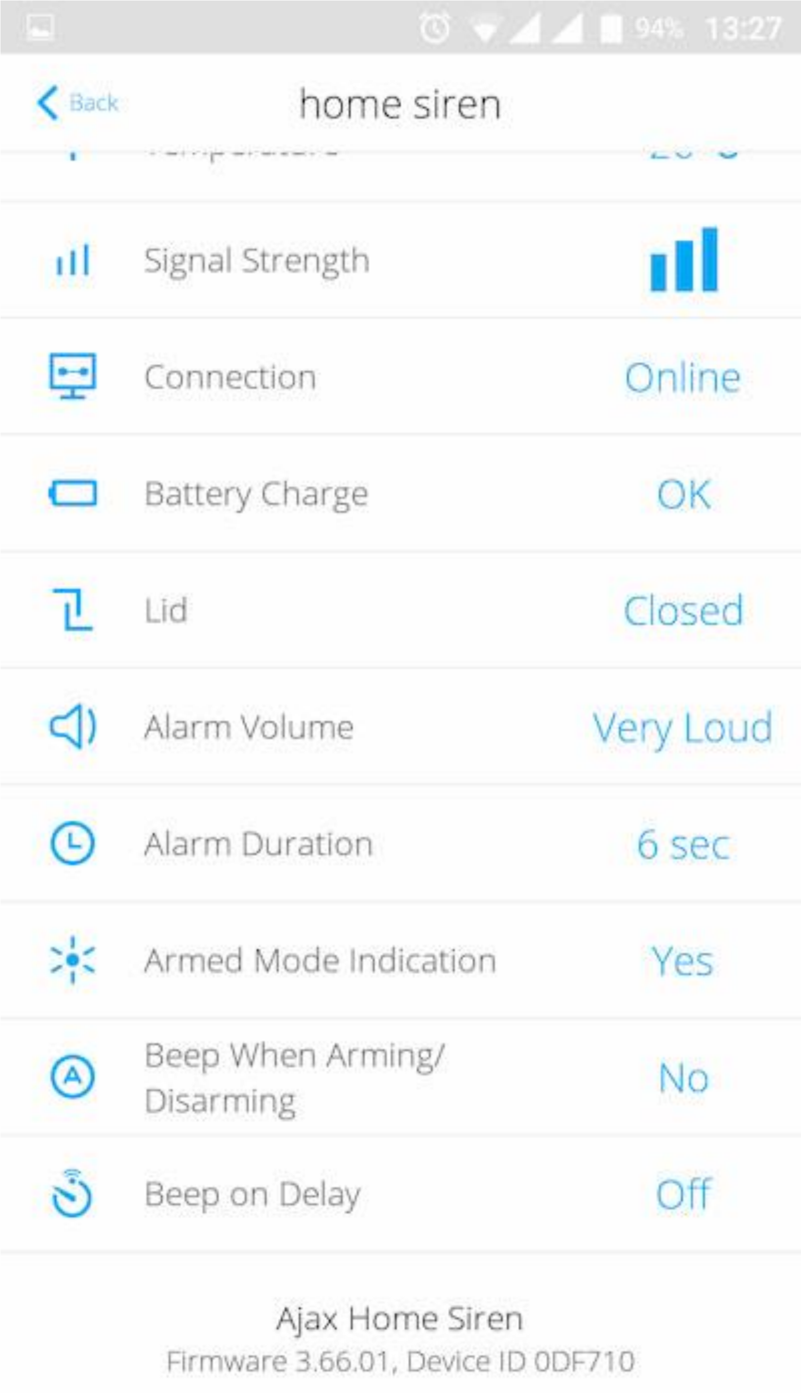
States

1. Devices
2. HomeSiren



home siren

Temperature	~26 ℃
Signal Strength	▂▄▆
Connection	Online
Battery Charge	OK
Lid	Closed
Alarm Volume	Very Loud
Alarm Duration	6 sec



home siren

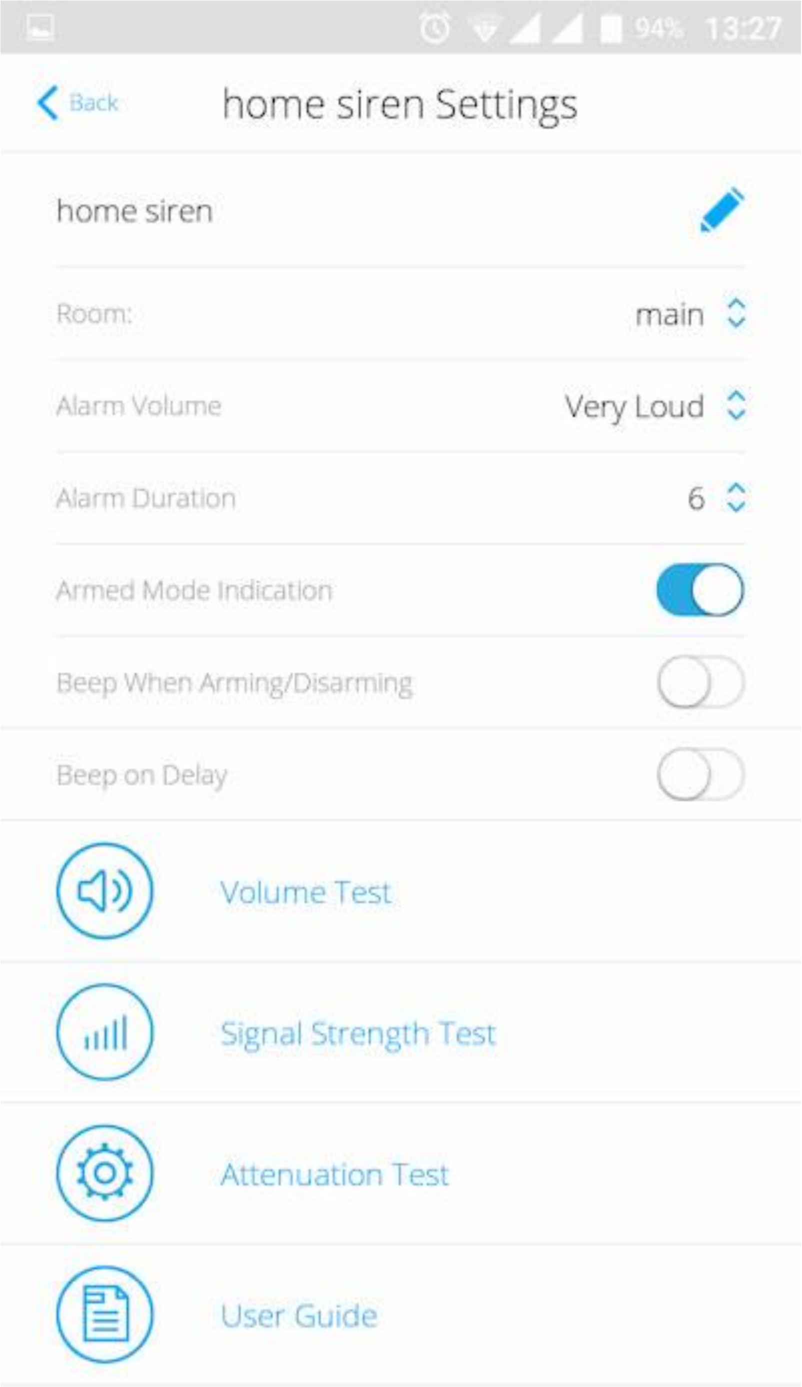
Signal Strength	▂▄▆
Connection	Online
Battery Charge	OK
Lid	Closed
Alarm Volume	Very Loud
Alarm Duration	6 sec
Armed Mode Indication	Yes
Beep When Arming/ Disarming	No
Beep on Delay	Off

Ajax Home Siren
Firmware 3.66.01, Device ID 0DF710

Parameter	Value
Temperature	Temperature of the device. Measured on the processor and changes gradually
Signal Strength	Signal strength between the hub and the siren
Connection	Connection status between the hub and the siren
Battery Charge	Battery level of the device
Lid	The tamper mode of the device, which reacts to the detachment of or damage to the body
Alarm Volume	Volume level in case of alarm
Alarm Duration	Duration of the alarm sound
Armed mode indication	If active, the siren LED blinks once every 3 seconds when the security system is armed
Beep when arming/disarming	If active, the siren warns about the activation and deactivation of the guard mode by the LED and a short sound signal
Beep on delay	If activated, siren will beep delays (available in devices with **firmware version 3.50 and later**)
Firmware	Detector firmware version
Device ID	Device identifier

Setting Up the Detector

1. Devices
2. HomeSiren
3. Settings



home siren Settings

home siren

Room: main

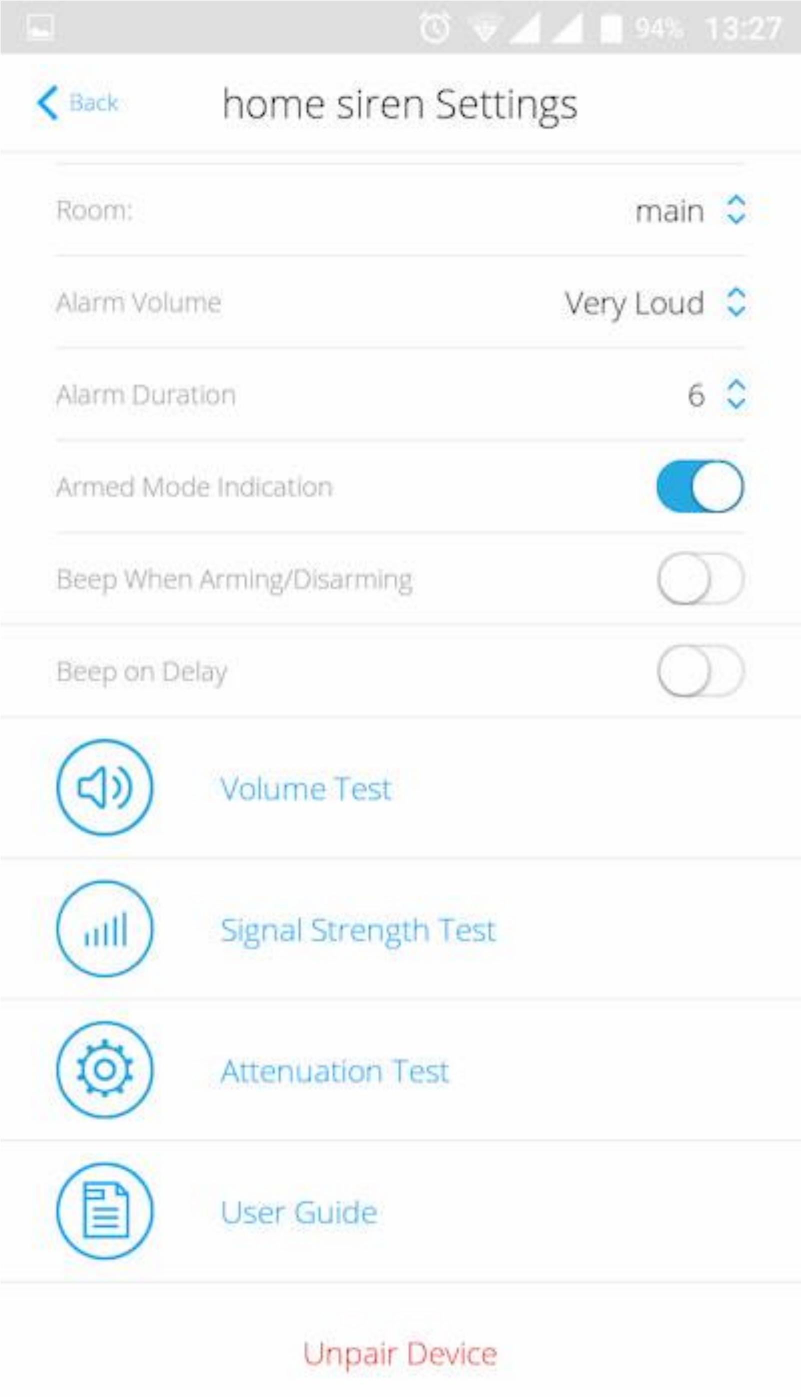
Alarm Volume: Very Loud

Alarm Duration: 6

Armed Mode Indication: ●

Beep When Arming/Disarming: ○

Beep on Delay: ○



home siren Settings

Room: main

Alarm Volume Very Loud

Alarm Duration 6

Armed Mode Indication ●

Beep When Arming/Disarming ○

Beep on Delay ○

Setting	Value
First field	Device name, can be edited
Room	Selecting the virtual room to which the device is assigned
Alarm Volume	Volume level in case of alarm: Very Loud, Loud, Quiet
Alarm Duration	The setting determines how long the siren sounds, if the alarm is activated (from 3 to 180 seconds per each actuation)
Armed mode indication	If active, the siren LED blinks once every 3 seconds when the security system is armed
Beep when arming/disarming	If active, the siren warns about the activation and deactivation of the guard mode by the LED and a short sound signal
Beep on delay	If active, siren will beep delays (available in devices with **firmware version 3.50 and later**)
Volume test	Start a volume test of the siren
Signal Strength Test	Switches the device to the signal strength test mode
Attenuation Test	Switches the siren to the signal fade test mode (available in devices with **firmware version 3.50 and later**)
User Manual	Opens the siren User Manual
Unpair Device	Disconnects the siren from the hub and deletes its settings

Indication

Event	Indication
Alarm	Emits an acoustic signal (the duration depends on the settings) and all LED signaling ceases
Switching on the device	LED lights up once
Switching off the device	LED will light up for 1 second, then blink three times
Registration failed	LED lights up and goes out, then the siren switches off
Security system set in the armed mode (if the indication is activated)	Blinks once with a LED and emits a short sound signal
Security system is disarmed (if the indication is activated)	Blinks twice with a LED and emits two short sound signals
Siren in the armed mode (if the indication is activated)	LED lights up for a short time every 3 seconds
Battery low	LED smoothly lights up and goes out when the system is armed or disarmed (if the indication is activated), the tamper is actuated or alarm is given

Performance testing

The Ajax security system allows conducting tests for checking the functionality of connected devices.

The tests do not start straight away but within a period of 36 seconds when using the standard settings. The test time start depends on the settings of the devices scanning period (the paragraph on “**Jeweller**” settings in hub settings).

Volume Level Test

Signal Strength Test

Attenuation Test

Installing the Siren

Location of the HomeSiren determines its remoteness from the hub and presence of any obstacles between the devices, hindering the radio signal and sound transmission: walls, inserted floors, large-size objects located within the room.

Check the signal level at the installation location.

The communication range is up to 2000 meters if there are no obstacles. Please consider it when choosing an installation place for HomeSiren.

If the signal level is one division, we cannot guarantee stable operation of the security system. Take possible measures to improve the quality of the signal! As a minimum, move the device – even 20 cm shift can significantly improve the quality of reception.

If, after moving, the device still has a low or unstable signal strength, use a radio signal range extender ReX.

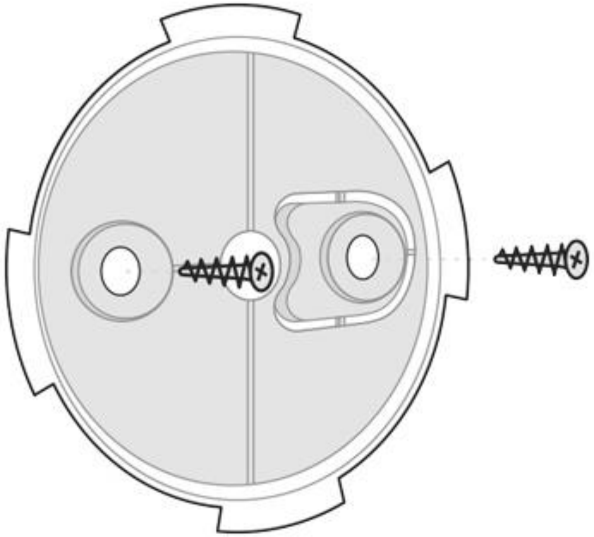
Recommended installation height – 2.5 meters and more. This will complicate the access to the device for intruders in case of intrusion.

Siren Installation

Before installing the siren, make sure that you have selected the optimal location and it is in compliance with the conditions contained in this manual!

Installation process

1. Fix the SmartBracket panel on the surface using bundled screws. After selecting other attachment hardware, make sure that they do not damage or deform the panel.



The double-sided adhesive tape may be only used for temporary attachment of the siren. The tape will run dry in course of time, which may result in the falling and damage of the device.

2. Put the siren on the SmartBracket panel and turn it clockwise. When installing in the attachment panel, the tamper will switch and the siren will blink with a LED.

   If the light indicator of the siren is not actuated after installation in SmartBracket, check the tamper mode in the Ajax Security System application and then the fixing tightness of the device on the panel.

In case of any attempt to dismount the siren, you will receive the notification.

Do not install the siren:

1. outside the premises (outdoors)
2. in places where the acoustic signal will be attenuated (inside furniture, behind thick curtains, etc.)
3. nearby any metal objects or mirrors causing attenuation and screening of the signal
4. within any premises with the temperature and humidity beyond the range of permissible limits
5. closer than 1 m from the hub.

External LED connection

The outside-mounted LED connected to the HomeSiren is paralleled with the built-in LED of the device and completely repeats its indication.

For connection, use the contact on the rear side of the siren body and observe the polarity during the connection. Black terminal wire — “+” contact.

Outlet power supply: 3 V, 10 mA.

Siren Maintenance and Battery Replacement

Check the operational capability of the HomeSiren on a regular basis.

Clean the siren body from dust, spider web and other contaminations as they appear. Use soft dry napkin suitable for equipment maintenance.

Do not use for cleaning the siren any substances containing alcohol, acetone, gasoline and other active solvents.

The batteries installed in the siren ensure up to 5 years of autonomous operation (with the inquiry frequency by the hub of 1 minute) or at least 6 hours of the buzzer sound. If the battery is discharged, the security system will send respective notices and the LED will smoothly light up and goes out when the armed mode is activated.

Battery Replacement

Tech specs

Type of notification	Acoustic and LED
Sound notification volume	81 – 105 dB at a distance of 1 m (adjustable)
Operating frequency of the buzzer	3.4 ± 0.5 kHz
Tamper protection	Yes

Frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz depending on the region of sale
Compatibility	Operates only with Hub, Hub Plus, Hub 2 and ReX
Maximum RF output power	Up to 25 mW
Radio signal modulation	GFSK
Radio signal range	Up to 2,000 m (any obstacles absent)
Battery supply	2 x CR123A, 3 V
Battery life	Up to 5 years
Socket for connecting an external light indicator	Yes (power supply 3 V, 10 mA)
Body protection level	IP50
Operating temperature range	From -10°C to + 40°C

Operating humidity	Up to 75%
Overall dimensions	75 x 76 x 27 mm
Weight	97 g
Certification	Security Grade 2, Environmental Class II in conformity with the requirements of EN 50131-1, EN 50131-4, EN 50131-5-3

Complete Set

1. HomeSiren
2. SmartBracket mounting panel
3. Battery CR123A (pre-installed) – 2 pcs
4. LED connection clamp
5. Installation Kit
6. Quick Start Guide

Warranty

Warranty for the “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase and does not apply to the pre-installed battery.

If the device does not work correctly, you should first contact the support service — in half of the cases, technical issues can be solved remotely!

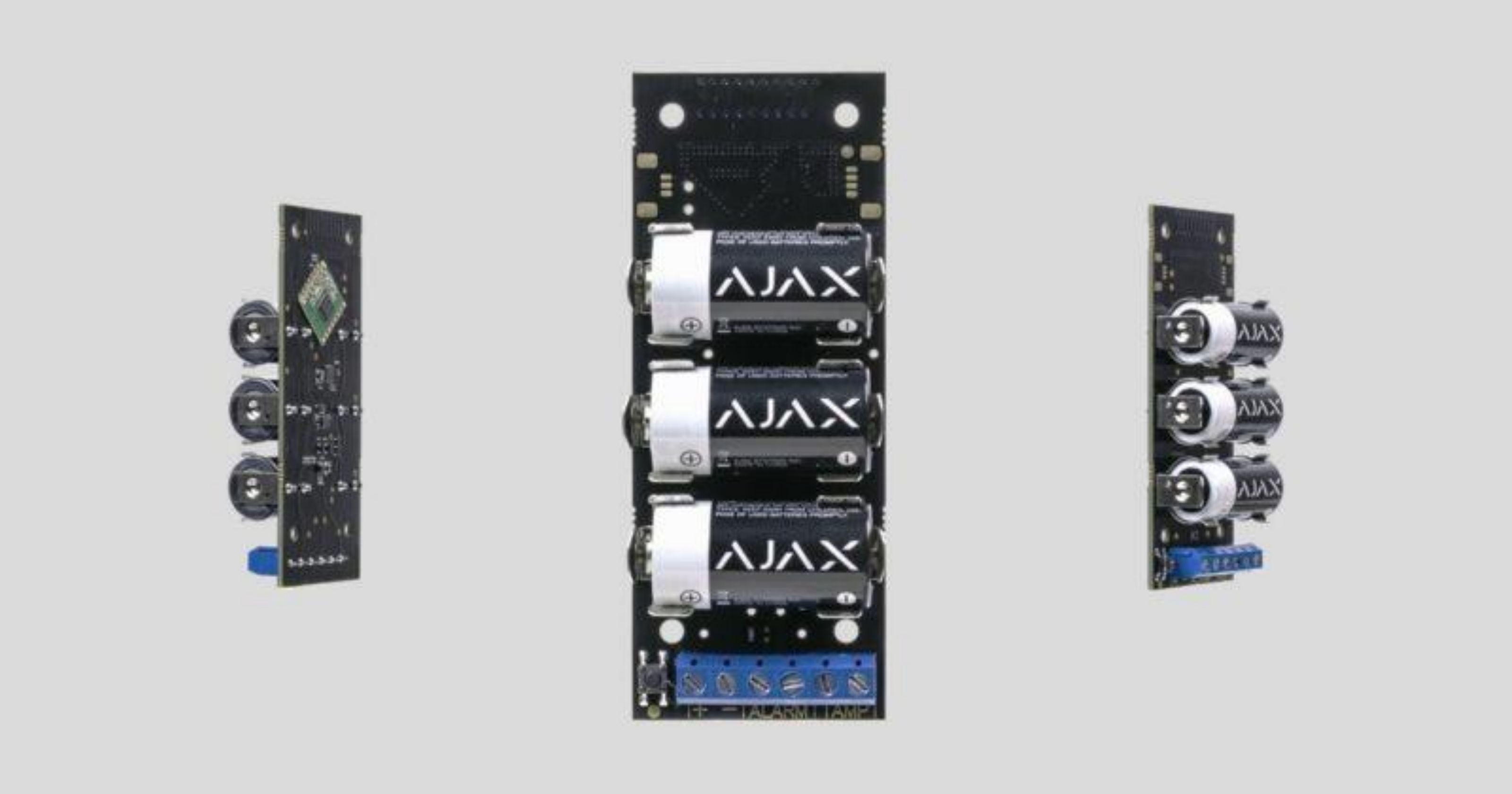
The full text of the warranty

User Agreement

Technical support: support@ajax.systems

Transmitter User Manual

Updated December 11, 2019



Transmitter is a module for connecting third-party detectors to Ajax security system. It transmits alarms and warns about the activation of the external detector tamper and it is equipped with own accelerometer, which protects it from dismounting. It runs on batteries and can supply power to the connected detector.

Transmitter operates within the Ajax security system, by connecting via the protected Jeweller protocol to the hub. It is not intended to use the device in third-party systems.

Not compatible with the uartBridge or ocBridge Plus

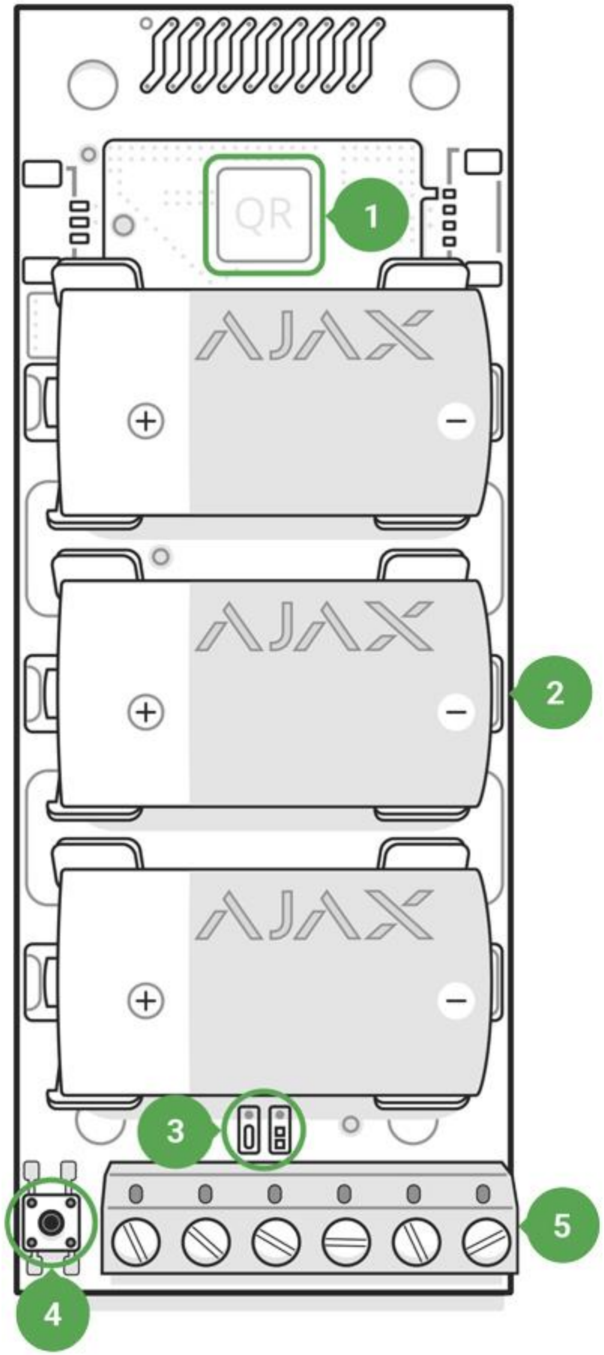
The communication range can be up to 1,600 meters provided that there are no obstacles and the case is removed.

Transmitter is set up via a mobile application for iOS and Android based smartphones.

The Ajax security system is self-sustaining, but the user can connect it to the central monitoring station of a security company.

Buy integration module Transmitter

Functional Elements


QR
1
AJAX
AJAX
AJAX
2
3
4
5

1. QR code with the device registration key.
2. Batteries contacts.
3. LED indicator.
4. ON/OFF button.
5. Terminals for detector power supply, alarm and tamper signals.

Operation procedure

The Transmitter serves for connecting the external alarm sources to Ajax system: indoor and outdoor detectors tracking motion, opening, vibrations, breaks, fire, gas, leakage, etc. Compatible with detectors with NC/NO contacts.

Transmitter receives information about alarms and the activation of the external detector tamper button through the terminals. A separate pair of terminals ensures power supply to the external detector from the module batteries with 3.3 V.

Connecting to the hub

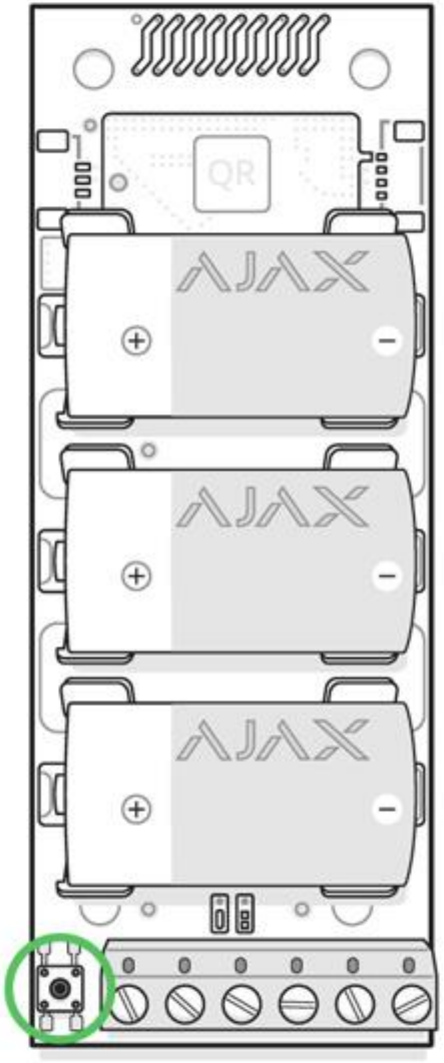
Before starting connection:

1. Following the hub instruction recommendations, install the Ajax application on your smartphone. Create an account, add the hub to the application, and create at least one room.
2. Go to the Ajax application.
3. Switch on the hub and check the internet connection (via Ethernet cable and/or GSM network).
4. Ensure that the hub is disarmed and does not start updates by checking its status in the mobile application.

Only users with administrative privileges can add the device to the hub

How to connect the Transmitter to the hub:

1. Select the **Add Device** option in the Ajax application.
2. Name the device, scan/write manually the **QR Code** (located on the body and packaging), and select the location room.
3. Select **Add** — the countdown will begin.
4. Switch on the device (by pressing on/off button for 3 seconds).



QR
AJAX
AJAX
AJAX

For the detection and interfacing to occur, the device should be located within the coverage area of the wireless network of the hub (at a single protected object).

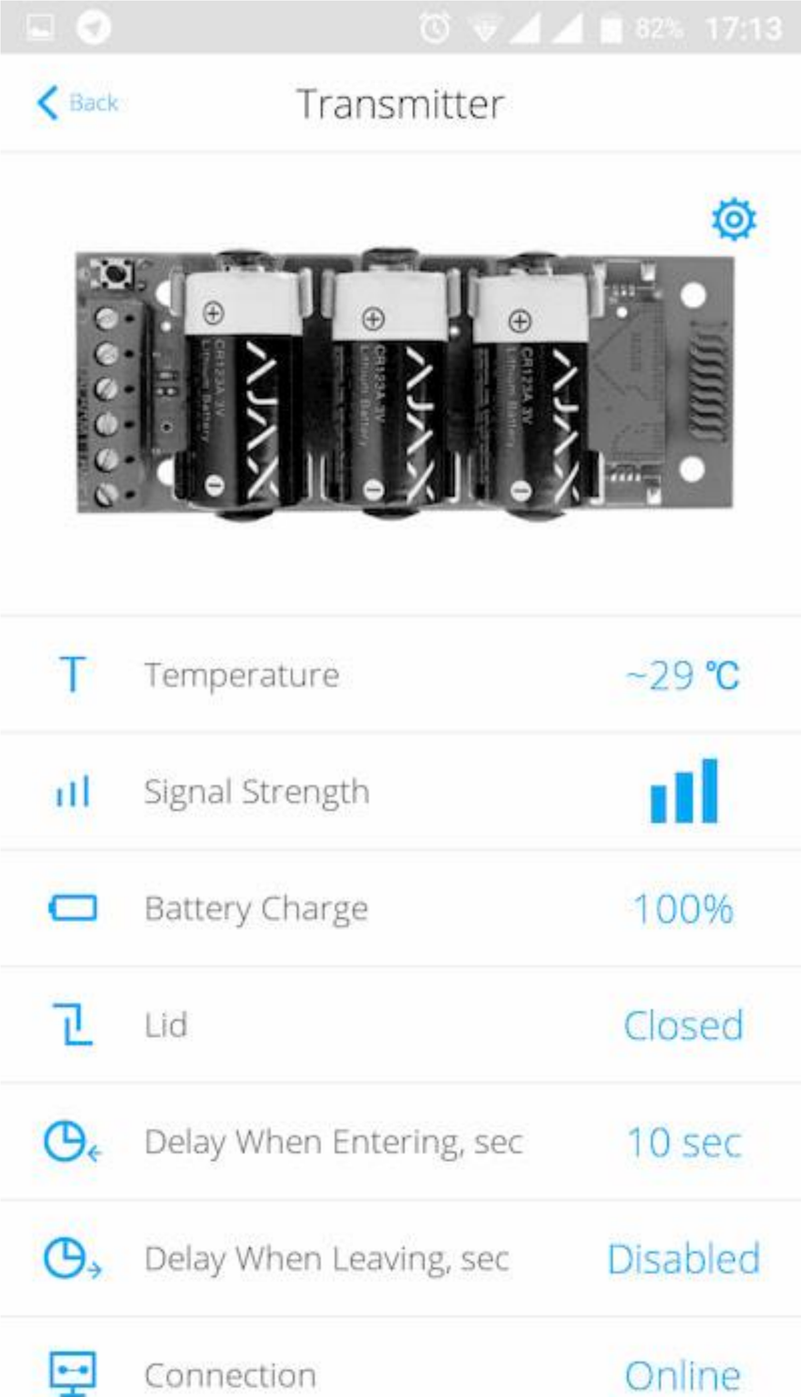
Request for connection to the hub is transmitted for a short time at the time of switching on the device.

If the connection to the Ajax hub failed, the Transmitter will switch off after 6 seconds. You may repeat the connection attempt then.

The Transmitter connected to the hub will appear in the list of devices of the hub in the application. Update of device statuses in the list depends on the device inquiry time set in the hub settings, with the default value – 36 seconds.

States

1. Devices
2. Transmitter



Transmitter

Temperature ~29 ℃

Signal Strength

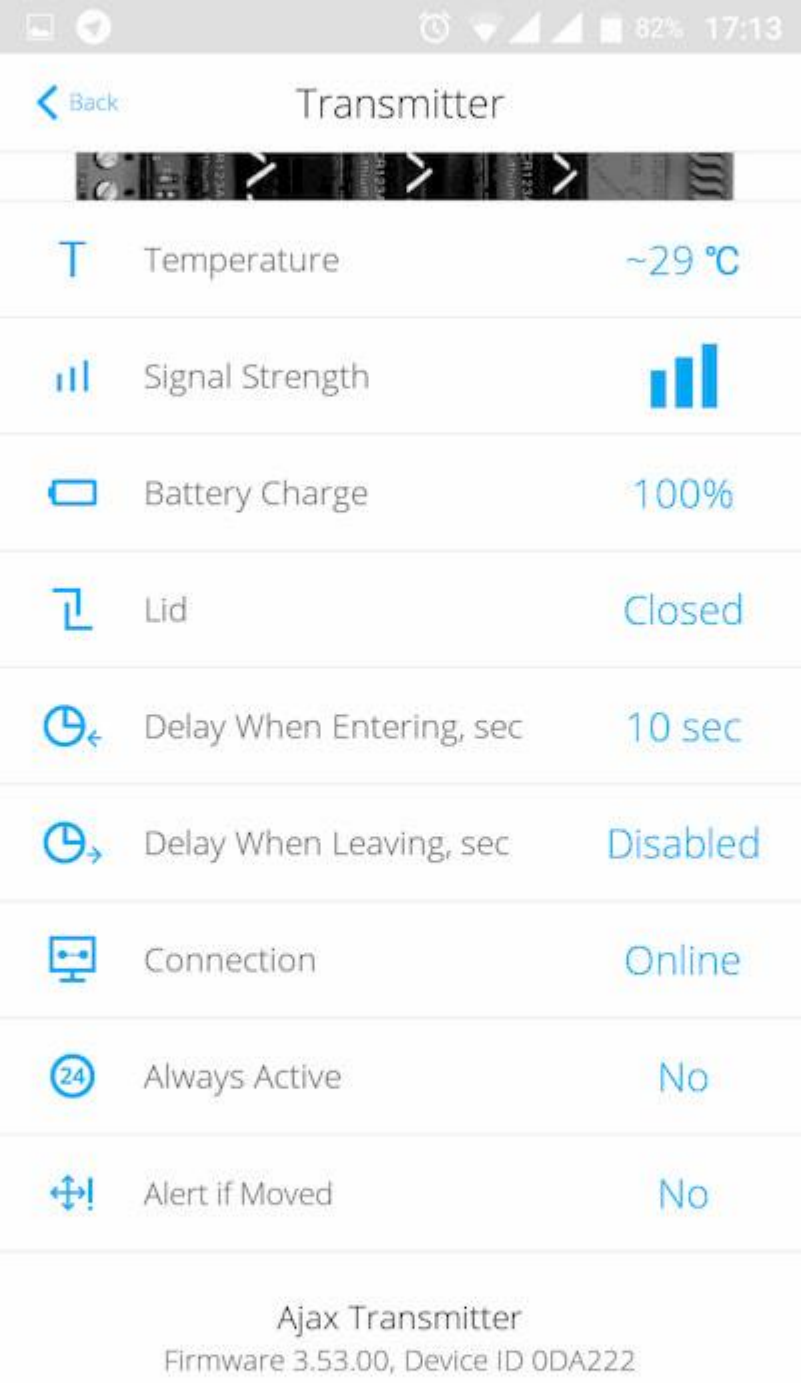
Battery Charge 100%

Lid Closed

Delay When Entering, sec 10 sec

Delay When Leaving, sec Disabled

Connection Online



Transmitter

Temperature	~29 ℃
Signal Strength	▂▄▆
Battery Charge	100%
Lid	Closed
Delay When Entering, sec	10 sec
Delay When Leaving, sec	Disabled
Connection	Online
Always Active	No
Alert if Moved	No

Ajax Transmitter
Firmware 3.53.00, Device ID 0DA222

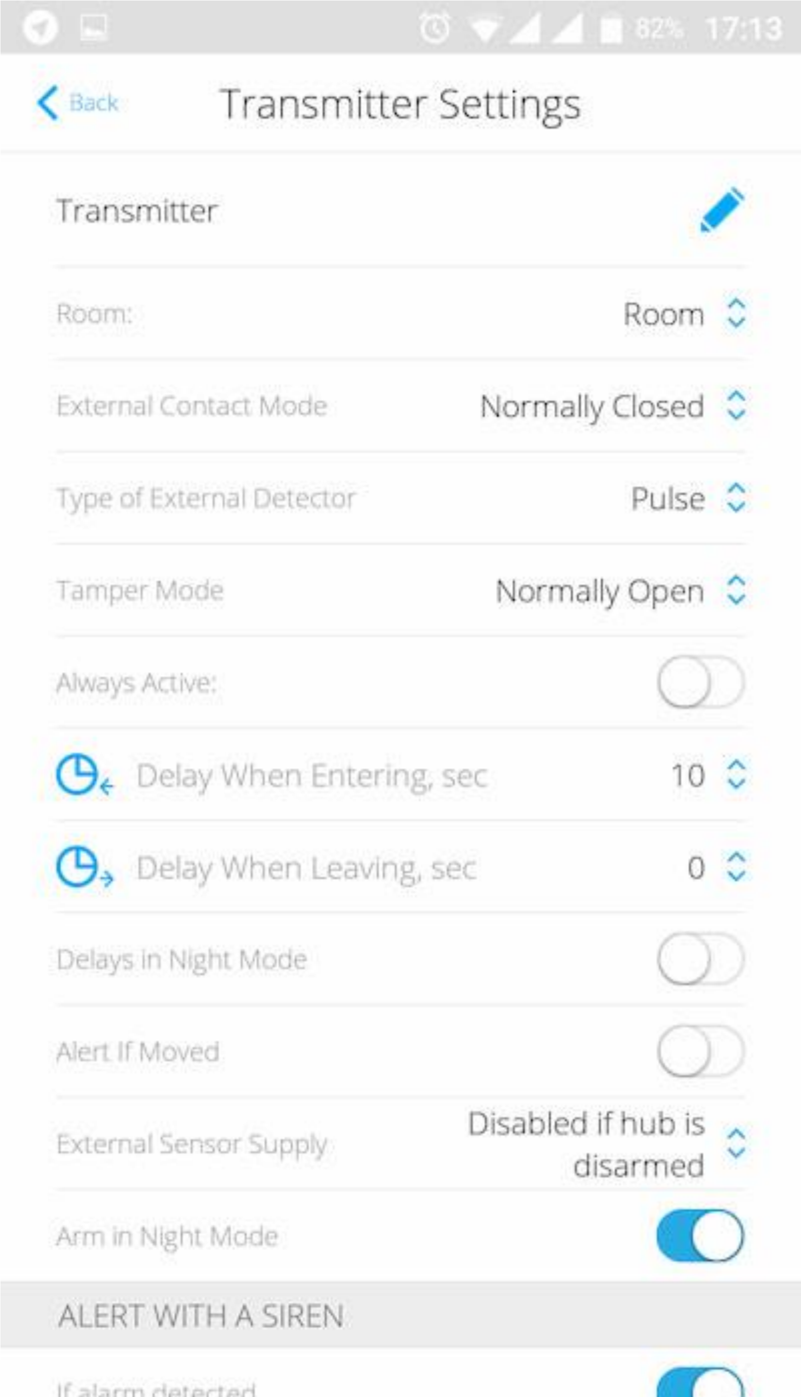
Parameter	**Value**
Temperature	Temperature of the device. Measured on the processor and changes gradually
Signal Strength	Signal strength between the hub and the device
Battery Charge	Battery level of the device, displayed in increments of 25%
Lid	The tamper terminal state
Delay when entering, sec	Delay time when entering
Delay when leaving, sec	Delay time when exiting
Connection	Connection status between the hub and the Transmitter
Always Active	If active, the device is always in an armed mode
Alert if moved	It turns on the Transmitter accelerometer, detecting device movement
Firmware	Detector firmware version
Device ID	Device identifier

Settings

1. Devices

2. Transmitter

3. Settings



Transmitter Settings

Transmitter

Room: Room

External Contact Mode Normally Closed

Type of External Detector Pulse

Tamper Mode Normally Open

Always Active: ○

Delay When Entering, sec 10

Delay When Leaving, sec 0

Delays in Night Mode ○

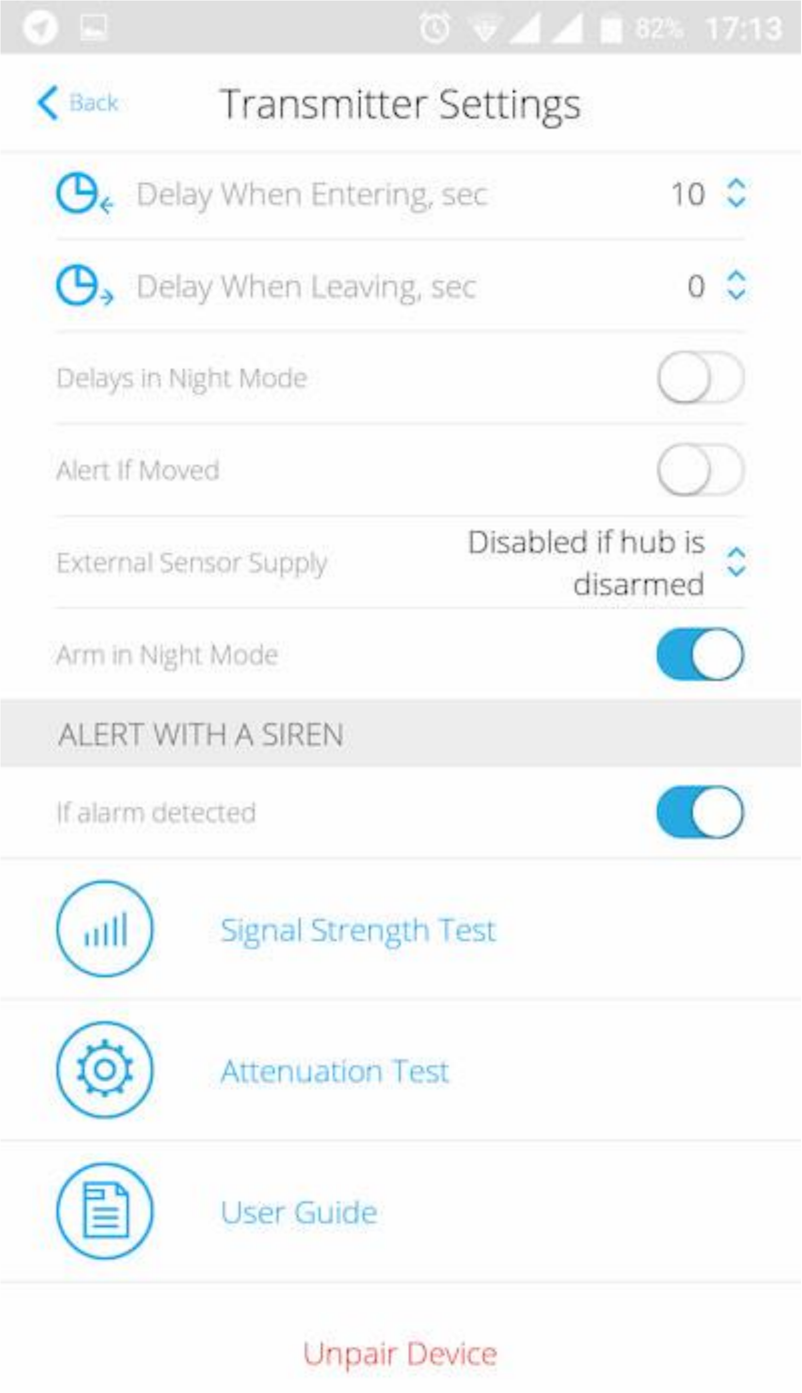
Alert If Moved ○

External Sensor Supply Disabled if hub is disarmed

Arm in Night Mode ●

ALERT WITH A SIREN

If alarm detected ●



Transmitter Settings

Delay When Entering, sec 10

Delay When Leaving, sec 0

Delays in Night Mode ○

Alert If Moved ○

External Sensor Supply Disabled if hub is disarmed

Arm in Night Mode ●

ALERT WITH A SIREN

If alarm detected ●

Setting	Value
First field	Device name, can be edited
Room	Selecting the virtual room to which the device is assigned
Contact status of the external detector	Selection of the external detector normal status: Normally closed (NC) Normally opened (NO)
Type of the external detector	Selection of the external detector type: Pulsed Bistable
Tamper mode	Selection of the normal tamper mod for an external detector: Normally closed (NC) Normally opened (NO)
Always active	When the mode is active, the Transmitter transmits alarms even when the system is disarmed
Delay when entering, sec	Selecting delay time when entering
Delay when leaving, sec	Selecting delay time on exit

Delays in night mode	Delay turned on when using night mode
Alert if moved	The accelerometer turning on the Transmitter to provide an alarm in the event of device movement
Power supply of the external detector	Turning the power on in 3.3 V external detector: Disabled if hub is disarmed Always disabled Always active
Arm in night mode	If active, the device will switch to armed mode when using night mode
Activate the siren if an alarm is detected	If active, HomeSiren and StreetSiren actuate if an alarm is detected
Signal Strength Test	Switches the device to the signal strength test mode
Attenuation Test	Switches the device to the signal fade test mode (available in detectors with **firmware version 3.50 and later**)
User Guide	Opens the device User Guide
Unpair Device	Disconnects the device from the hub and deletes its settings

Set the following parameters in the Transmitter settings:

- **The state of the external detector contact**, which can be normally closed or normally open.
- **The type (mode) of the external detector** that can be bistable or pulse.

- **The tamper mode**, which can be normally closed or normally open.
- **The accelerometer-triggered alarm** — you can turn this signal off or on.

Select the power mode for the external detector:

- **Turned off when the hub is disarmed** — the module stops powering the external detector upon disarming and does not process signals from the ALARM terminal. When arming the detector, the power supply resumes, but the alarm signals are ignored for the first 8 seconds.
- **Always disabled** — the Transmitter saves energy by turning off the power of the external detector. The signals from the ALARM terminal are processed both in the pulse and bistable modes.
- **Always active** — this mode should be used if there are any problems in the “Turned off when the hub is disarmed”. When the security system is armed, signals from the ALARM terminal are processed no more than once in three minutes in the pulse mode. If the bistable mode is selected, such signals are processed instantly.

If the “Always active” operating mode is selected for the module, the external detector is powered only in the “Always active” or the “Turned off when the hub disarmed” mode, regardless of the security system status.

Indication

Event	Indication
The Module is switched on and registered	The LED lights up when the ON button is briefly pressed.

Registration failed	LED blinks for 4 seconds with an interval of 1 second, then blinks 3 times rapidly (and automatically switches OFF).
The Module is deleted from the list of hub devices	LED blinks for 1 minute with an interval of 1 second, then blinks 3 times rapidly (and automatically switches OFF).
The Module has received alarm/tamper signal	The LED lights up for 1 second.
Batteries are discharged	Smoothly lights up and goes out when the detector or tamper is activated.

Performance testing

The Ajax security system allows conducting tests for checking the functionality of connected devices.

The tests do not start straight away but within a period of 36 seconds when using the standard settings. The test time start depends on the settings of the detector scanning period (the paragraph on “**Jeweller**” settings in hub settings).

Signal Strength Test

Attenuation Test

Connection of the Module to the wired detectora

Location of the Transmitter determines its remoteness from the hub and presence of any obstacles between the devices hindering the radio signal transmission: walls, inserted floors, large-size objects located within the room.

Check the signal strength level at the installation location

If the signal level is one division, we cannot guarantee stable operation of the security system. Take possible measures to improve the quality of the signal! As a minimum, move the device – even 20 cm shift can significantly improve the quality of reception.

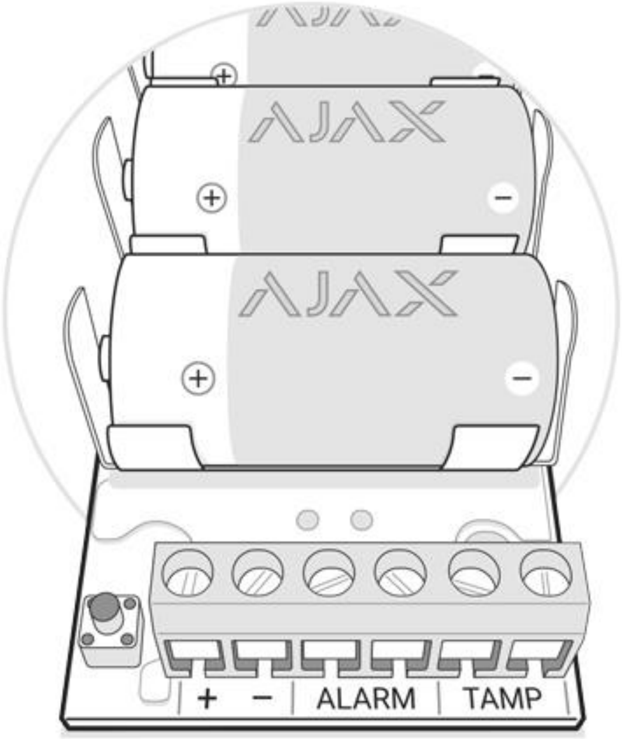
If, after moving, the device still has a low or unstable signal strength, use a radio signal range extender ReX.

The Transmitter should be encased inside the wired detector case. The Module requires a space with the following minimum dimensions: 110 x 41 x 24 mm. If the installation of the Transmitter within the detector case is impossible, then any available radiotransparent case could be used.

1. Connect the Transmitter to the detector through the NC/NO contacts (choose the relevant setting in the application) and COM.

The maximum cable length for connecting the sensor is 150 m (24 AWG twisted pair). The value may vary when using different type of cable.

The function of the Transmitter’s terminals



+ – — power supply output (3.3 V)

ALARM — alarm terminals
TAMP — tamper terminals

IMPORTANT! Do not connect external power to the Transmitter’s power outputs. This may damage the device

2. 2. Secure the Transmitter in the case. Plastic bars are included in the installation kit. It is recommendable to install the Transmitter on them.

Maintenance and Battery Replacement

The device does not require maintenance when mounted in the housing of a wired sensor.

Battery Replacement

Tech Specs

Connecting a detector	ALARM and TAMPER (NO/NC) terminals
Mode for processing alarm signals from the detector	Pulse or Bistable
Power	3 x CR123A, 3V batteries
Capability to power the connected detector	Yes, 3.3V
Protection from dismounting	Accelerometer
Frequency band	868.0–868.6 MHz or 868.7 – 869.2 MHz, depends on sales region
Compatibility	Operates only with Hub, Hub Plus, Hub 2 and ReX
Maximum RF output power	Up to 20 mW
Modulation	GFSK

Communication range	Up to 1,600 m (any obstacles absent)
Ping interval for the connection with the receiver	12–300 sec
Operating temperature	From -25°C to +50°C
Operating humidity	Up to 75%
Dimensions	100 x 39 x 22 mm
Weight	74 g

Complete Set

1. Transmitter
2. Battery CR123A — 3 pcs
3. Installation kit
4. Quick Start Guide

Warranty

Warranty for the “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase and does not apply to the pre-installed battery.

If the device does not work correctly, you should first contact the support service—in half of the cases, technical issues can be solved remotely!

The full text of the warranty

User Agreement

Technical support: support@ajax.systems