Hub 2 User Manual

Updated December 7, 2020

Ajax is a wireless security system that protects against <u>intrusions</u>, <u>fires</u>, and <u>floods</u>, and allows users to <u>control electrical appliances</u> directly from a <u>mobile app</u>. The system responds immediately to threats informing you and the security company about any incident. Is used inside premises.

Hub 2 is an intelligent security system control panel that supports detectors with visual alarm verification, that developed only for indoor use. Representing a key element of the security system, Hub 2 controls the operation of Ajax devices and, in the event of a threat, communicates the alarm signals immediately informing the owner and the central monitoring station of the incidents.

Hub 2 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. The personal data and system operation logs are stored under multilevel protection, and information exchange with Hub 2 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 (two 2G SIM cards). Please use all these communication channels to ensure more reliable communication between the hub and Ajax Cloud.

Hub 2 can be controlled via the **app** for iOS, Android, macOS, or Windows. The app allows responding promptly to any notifications of the security system. 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.

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, 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

Buy intelligent security control panel Hub 2

Functional elements
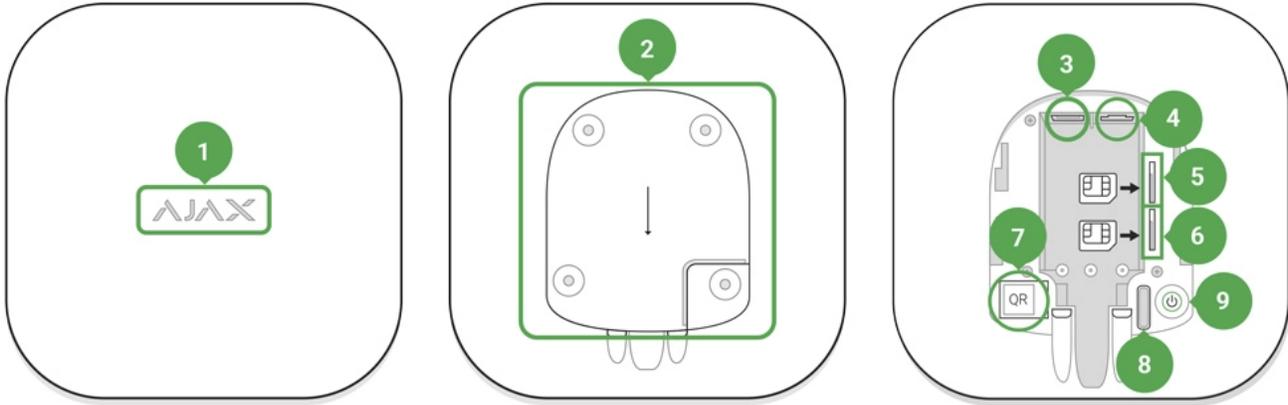
1. **LED logo**

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. **Slot for the micro SIM**

7. **QR Code**

8. **Tamper button**

9. **Power button**

Operational Principles

The hub collects information regarding the operation of the connected devices in an encrypted form, analyzes the data and, in the case of an alarm, informs the system owner of the danger in less than a second and communicates the alarm directly to the central monitoring station of the security company.

In order to communicate with the devices, monitor their operation, and respond quickly to threats, Hub 2 uses the Jeweller radio technology. For visual data transmission, Hub 2 uses Wings: a high-speed radio protocol based on the Jeweller technology. Wings also uses a dedicated antenna to improve channel reliability.

All Ajax devices

LED Indication

The LED logo can light up red, white or green depending on the status of the device.

Event	Light indicator
Ethernet and at least one SIM card are connected	Lights up white
Only one communication channel is connected	Lights up green
The hub is not connected to the internet or there is no connection with the Ajax Cloud service	Lights up red
No power	Lights up for 3 minutes, then blinks every 20 seconds. The color of the indicator depends on the number of the connected communication channels.

Ajax Account

Hub 2 can be controlled via the **app** for iOS, Android, macOS, or Windows.

To configure the system, install the Ajax app and create the Ajax account. We recommend using the Ajax Security System app to manage one or several hubs. If you plan to manage over one hundred hubs, we recommend using **Ajax PRO: Tool**

for Engineers (for iOS or Android) or **Ajax PRO Desktop** (for Windows or macOS). You will need to confirm your email address and your phone number as part of the process. Note that you can use your phone number and your email address to create only one Ajax account! You do not need to create a new account for each hub—you can add several hubs to one account.

> ⓘ An account with information regarding the added hubs is uploaded to the cloud-based Ajax Cloud service in an encrypted form.

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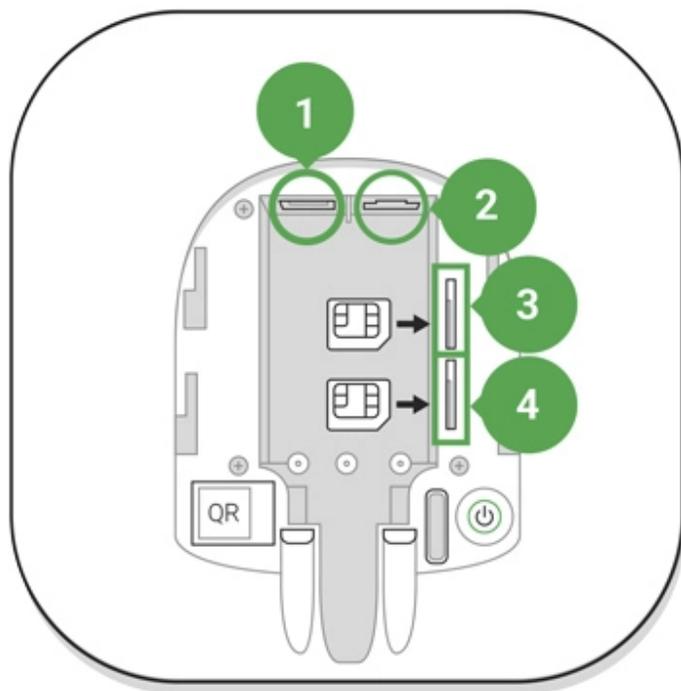
It is strictly prohibited to disassemble the device under voltage! Do not use the device with a damaged power cable.

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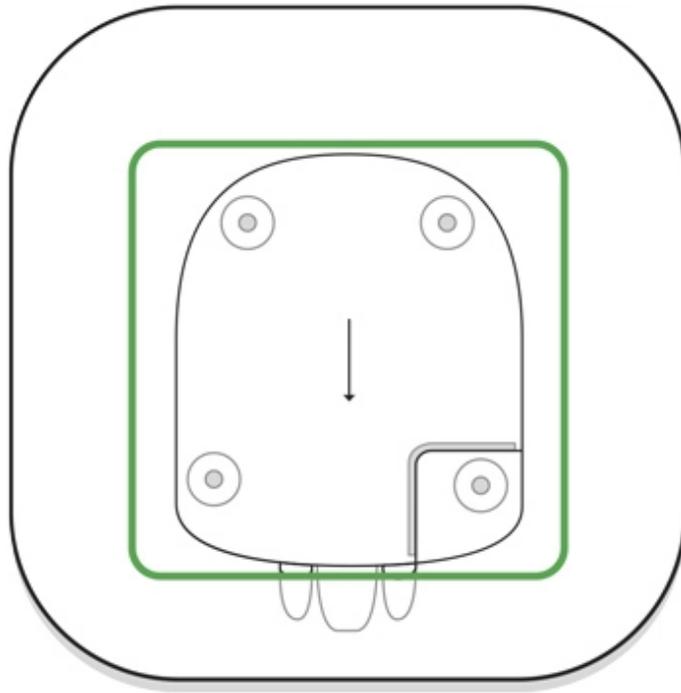
2. Connect the power supply and Ethernet cables to the sockets.

1 — Power Socket

2 — Ethernet socket

3, 4 — Slots for micro-SIM cards connection

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.

> ℹ️ 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.

4. 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. 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.

Adding a hub to the Ajax app

1. Open 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. When using Android, we recommend to follow **push notifications configuration instructions**.

2. Login into your account. Open the **Add Hub** menu and select the way of registering: manually or step-by-step guidance.

3. 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 app desktop 📶.

Security 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.

Changing the hub administrator does not affect the settings of the connected devices.

Ajax security system user rights

Hub statuses

Icons

Icons display some of Hub 2 statuses. You can see them in the Ajax app, in the **Devices** menu.

Icons	Meaning
2G	2G connected
	SIM card is not installed
	The SIM-card is defective or has a PIN-code on it
	Hub battery charge level. Displayed in 5% increments
	Hub malfunction is detected. The list is available in hub states list
	The hub is directly connected to the central monitoring station of the security organization
	The hub have lost connection with the central monitoring station of the security organization via direct connection

States

States can be found in the **Ajax app**:

1. Go to the **Devices** tab.

2. Select Hub 2 from the list.

Parameter	Meaning

Malfunction	Click ⓘ to open the list of hub malfunctions. The field appears only if a malfunction is detected
Cellular signal strength	Shows the signal strength of the mobile network for the active SIM card. We recommend installing the hub in places with the signal strength of 2-3 bars. If the signal strength is weak, the hub will not be able to dial-up or send an SMS about an event or alarm
Battery Charge	Battery level of the device. Displayed as a percentage **How battery charge is displayed in Ajax apps**
Lid	Status of the tamper that responds to hub dismantling: • Closed — the hub lid is closed • Opened — the hub removed from SmartBracket holder **What is a tamper?**
External power	External power supply connection status: • Connected — the hub is connected to external power supply • Disconnected — no external power supply
Connection	Connection status between the hub and Ajax Cloud: • Online — the hub is connected to Ajax Cloud • Offline — the hub is not connected to Ajax Cloud
Cellular data	The hub connection status to the mobile Internet:

	- Connected — the hub is connected to Ajax Cloud via mobile Internet - Disconnected — the hub is not connected to Ajax Cloud via mobile Internet If the hub has enough funds on the account or has bonus SMS/calls, it will be able to make calls and send SMS messages even if the **Not connected** status is displayed in this field
Active SIM card	Displays the active SIM card: SIM card 1 or SIM card 2
SIM card 1	The number of the SIM card installed in the first slot. Copy the number by clicking it
SIM card 2	The number of the SIM card installed in the second slot. Copy the number by clicking it
Ethernet	Internet connection status of the hub via Ethernet: - Connected — the hub is connected to Ajax Cloud via Ethernet - Disconnected — the hub is not connected to Ajax Cloud via Ethernet
Average Noise (dBm)	Noise power level at the hub installation site. The first two values show the level at Jeweller frequencies, and the third — at Wings frequencies. The acceptable value is -80 dBm or lower
Monitoring Station	The status of direct connection of the hub to the central monitoring station of the security organization: - Connected — the hub is directly connected to the central monitoring station of the security organization - Disconnected — the hub is not directly connected to the central monitoring station of the security organization If this field is displayed, the security company uses a direct connection to receive events and

| | security system alarms. |
Hub model	Hub model name
Hardware version	Hardware version. Unable to update
Firmware	Firmware version. Can be updated remotely
ID	ID/serial number. Also located on the device box, on the device circuit board, and on the QR code under the SmartBracket panel

Rooms in the Ajax app

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!

The name of the room is indicated in the notification of the device event or detector alarm.
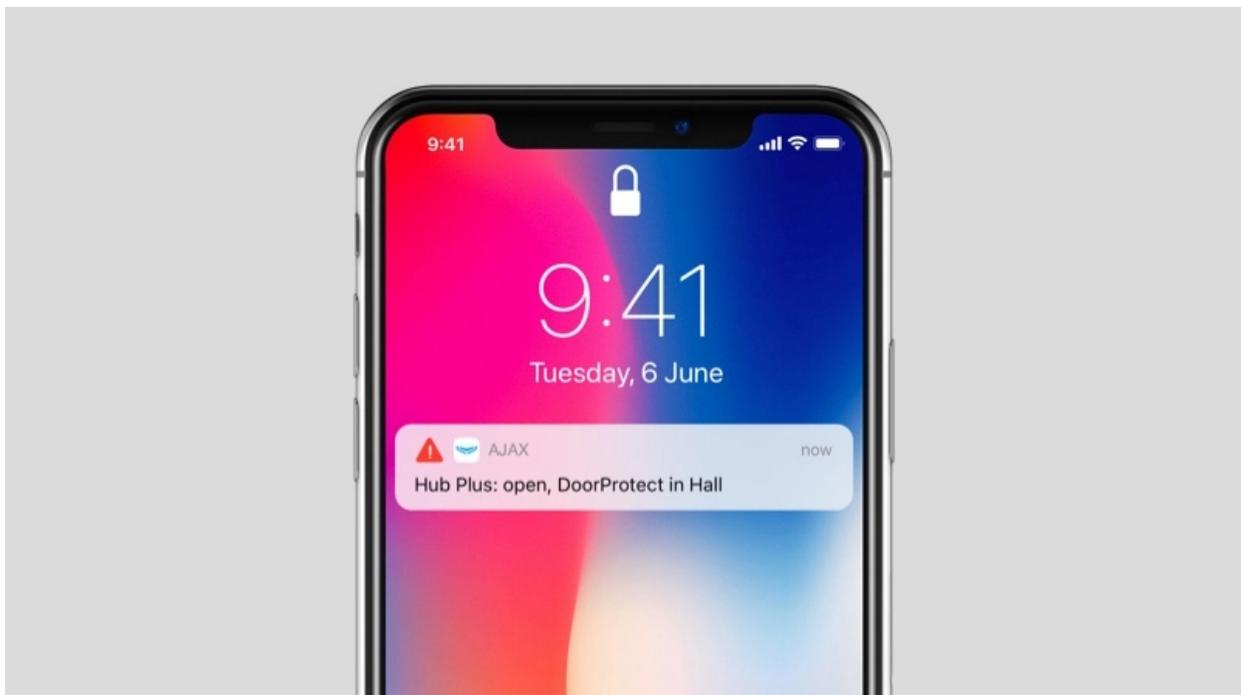
The room is created in the app using the **Add Room** menu.

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

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!

Pairing **device with hub**:

1. In the **Ajax app**, open the room and select **Add Device**.

2. Name the device, scan its QR code (or enter it manually), select a group (if group mode is enabled).

3. Click **Add** — the countdown for you to add a device will begin.

4. 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).

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

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

Video surveillance

You can connect third-party cameras to the security system: seamless integration with Dahua, Hikvision, and Safire IP cameras and video recorders has been implemented, and you can also connect third-party cameras supporting RTSP protocol. You can connect up to 25 video surveillance devices to the system.

How to add a Dahua camera or video recorder to the hub

How to add a Hikvision/Safire camera or video recorder to the hub

Settings

Settings can be changed in the **Ajax app**:

1. Go to the **Devices** tab 🔲 .

2. Select Hub 2 from the list.

3. Go to **Settings** by clicking on the icon ⚙️.

ⓘ Note that after changing the settings, you should click the **Back** button to save them.

Avatar is a customized title image for Ajax security system. It is displayed in the hub selection menu and helps to identify the required object.

To change or set an avatar, click on the camera icon and set up the desired picture.

Hub name. Is displayed in the SMS and push notification text. The name can contain up to 12 Cyrillic characters or up to 24 Latin characters.

To change it, click on the pencil icon and enter the desired hub name.

Users — user settings for a security system: what rights are granted to users and how the security system notifies them of events and alarms.

To change the user settings, click on ⚙ opposite the user name.

[How the Ajax security system notifies users of alerts](#)

[How to add new users to the hub](#)

Ethernet — settings for wired Internet connection.

- Ethernet — allows you to enable and disable Ethernet on the hub

- DHCP / Static — selection of the type of the hub IP address to receive: dynamic or static

- IP Address — hub IP Address

- Subnet mask — subnet mask in which the hub operates

- Router — gateway used by the hub

- DNS — DNS of the hub

GSM — enabling/disabling cellular communication, configuring connections, and checking account.

- Cellular Data — disables and enables SIM cards on the hub

- Roaming — if it is activated, the SIM cards installed in the hub can work in roaming

- Ignore network registration error — when this setting is activated, the hub ignores errors when trying to connect via a SIM card. Activate this option if the SIM card cannot connect to the network

- Disable Ping Before Connecting — when this setting is activated, the hub ignores operator communication errors. Activate this option if the SIM card cannot connect to the network

- SIM card 1 — displays the number of the SIM card installed. Click on the field to go to the SIM card settings

- SIM card 2 — displays the number of the SIM card installed. Click on the field to go to the SIM card settings

SIM card settings

Connection settings

- **APN**, **User name**, and **Password** — settings for connecting to the Internet via a SIM card. To find out the settings of your cellular operator, contact your provider's support service.

  How to set or change APN settings in the hub

Mobile data usage

- **Incoming** — the amount of data received by the hub. Displayed in KB or MB.

- **Outgoing** — the amount of data sent by the hub. Displayed in KB or MB.

> ℹ️ Keep in mind that data is counting on the hub and may differ from your operator's statistics.

Reset statistics — resets statistics on incoming and outgoing traffic.

Check balance

- **USSD code** — enter the code that is used to check the balance in this field. For example, *111#. After that, click **Check balance** to send a request. The result will be displayed under the button.

Geofence — configuring reminders for arming/disarming the security system when crossing a specified area. The user location is determined using the smartphone GPS module.

[What geofences are and how they function](#)

Groups — group mode configuration. This allows you to:

- Manage the security modes for separate premises or groups of detectors. For example, the office is armed while the cleaner works in the kitchen.

- Delimit access to control of security modes.
  For example, the marketing department employees do not have access to the law office.

[OS Malevich 2.6: a new level of security](#)

Security Schedule — arming/disarming the security system by the schedule.

[How to create and configure a scenario in the Ajax security system](#)

Detection Zone Test — running the detection zone test for the connected detectors. The test determines the sufficient distance for the detectors to register alarms.

What is Detection Zone Test

Jeweller — configuring the hub-detector ping interval. The settings determine how frequently the hub communicates with devices and how quickly the loss of connection is detected.

Learn more

- **Detector Ping Interval** — the frequency of connected devices polling by the hub is setting in the range of 12 to 300 s (36 s by default)
- **Number of undelivered packets to determine connection failure** — a counter of undelivered packets (8 packets by default).

The time before raising the alarm by the communication loss between hub and device is calculated with the following formula:

*Ping interval * (number of undelivered packets + 1 correction packet).*

The shorter ping interval (in seconds) means faster delivery of the events between the hub and the connected devices; however, a short ping interval reduces the battery life. At the same time, alarms are transmitted immediately regardless of the ping interval.

We do not recommend reducing the default settings of the ping period and interval.

Note that the interval limits the maximum number of connected devices:

Interval	Connection limit
12 s	39 devices
24 s	79 devices
36 s or more	100 devices

> ⓘ Regardless of settings, the hub supports 10 connected sirens maximum!

Service is a group of hub service settings. These are divided into 2 groups: general settings and advanced settings.

General settings

Time zone

Selecting the time zone in which the hub operates. It is used for scenarios by schedule. Therefore, before creating scenarios, set the correct time zone.

Learn more about scenarios

LED Brightness

Adjustment of the hub logo LED backlight brightness . Set in the range of 1 to 10. The default value is 10.

Firmware Auto-Update

Configuring automatic OS Malevich firmware updates.

- **If enabled**, the firmware is automatically updated when a new version is available, when the system is not armed, and external power is connected.

- **If disabled**, the system does not update automatically. If a new firmware version is available, the app will offer to update the OS Malevich.

How OS Malevich updates

Hub logs

i	Logs are files containing information about system operation. They can help sort out the problem in case of errors or failures.

The setting allows you to select the transmission channel for the hub logs or disable their recording:

- Ethernet

- No — logging is disabled

⚠️	We do not recommend disabling logs as this information may be helpful in the event of errors in the operation of the system!

How to send an error report

Advanced settings

The list of advanced hub settings depends on the type of application: standard or PRO.

Ajax Security System	Ajax PRO
Server connection Sirens settings Fire detectors settings System integrity check	PD 6662 Setting Wizard Server connection Sirens settings Fire detectors settings System integrity check Alarm confirmation

	Restore after alarm
	Arming/disarming process
	Devices Auto Deactivation

PD 6662 Setting Wizard

Opens a step-by-step guide on how to set up your system to comply with the British security standard PD 6662:2017.

Learn more about PD 6662:2017

How to configure the system to comply with PD 6662:2017

Server connection

The menu contains settings for communication between the hub and the Ajax Cloud:

- **Server Ping Interval**. Frequency of sending pings from the hub to Ajax Cloud server. It is set in the range of 10 to 300 s. The recommended default value is 60 s.

- **Connection Failure Alarm Delay**. It is a delay to reduce the risk of a false alarm associated with the Ajax Cloud server connection loss. It is activated after 3 unsuccessful hub-server polls. The delay is set in the range of 30 to 600 s. The recommended default value is 300 s.

The time to generate a message regarding the loss of communication between the hub and the Ajax Cloud server is calculated using the following formula:

$$(Ping\ interval * 4) + Time\ filter$$

With the default settings, Ajax Cloud reports the hub loss in 9 minutes:

$$(60\ s * 4) + 300\ s = 9\ min$$

- **Disable alerts when the connection with the server is lost**. Ajax apps can notify about the hub-server communication loss in two ways: with a standard push notification signal or with a siren sound (enabled by default). When the option is active, the notification comes with a standard push notification signal.

Sirens settings

The menu contains two groups of siren settings: siren activation parameters and siren after-alarm indication.

Siren activation parameters

If the hub or detector lid is open. If enabled, the hub activates the connected sirens if the body of the hub, detector, or any other Ajax device is open.

If in-app panic button is pressed. When the function is active, the hub activates the connected sirens if the panic button was pressed in the Ajax app.

> ⓘ You can disable the sirens reaction when pressing the panic button on the SpaceControl key fob in the key fob settings (Devices → SpaceContol → Settings ⚙).

Settings of siren after-alarm indication

> ⚠ This setting is only available in PRO Ajax apps

The siren can inform about triggering in armed system by means of LED indication. Thanks to this feature, system users and passing security companies patrols can see that the system was triggered.

Feature implementation in HomeSiren

Feature implementation in StreetSiren

Fire detectors settings

Settings menu of FireProtect and FireProtect Plus fire detectors. Allows configuring interconnected FireProtect alarms of fire detectors.

The feature is recommended by European fire standards, which require, in the event of a fire, a warning signal power of at least 85 dB at 3 meters from the sound source. Such sound power wakes up even a soundly sleeping person during a fire. And you can quickly disable triggered fire detectors using the Ajax app, Button, or KeyPad.

Learn more

System integrity check

The **System integrity check** is a parameter that is responsible for checking the status of all security detectors and devices before arming. Checking is disabled by default.

Learn more

Alarm confirmation

⚠️ This setting is only available in PRO Ajax apps

Alarm confirmation is a special event that the hub sends to the CMS and system users if several certain devices have triggered within a specified period of time. By responding to confirmed alarms only, the security company and the police reduce the number of visits on false alarms.

Learn more

Restore after alarm

> ⚠️ This setting is only available in PRO Ajax apps

The feature does not allow arming the system if an alarm has been registered previously. For arming, the system should be restored by an authorized user or PRO user. The types of alarms that require system restore are defined when configuring the function.

The function eliminates situations when the user arms the system with detectors that generate false alarms.

Learn more

Arming/disarming process

> ⚠️ This setting is only available in PRO Ajax apps

The menu allows to enable arming in two stages, as well as set Alarm Transmission Delay for security system disarming process.

What is Two-Stage Arming and why is it needed

What is Alarm Transmission Delay and why is it needed

Devices Auto Deactivation

> ⚠️ This setting is only available in PRO Ajax apps

The Ajax security system can ignore alarms or other events of devices without removing them from the system. Under certain settings, notifications about events of a specific device will not be sent to the CMS and security system users.

There are two types of **Devices Auto Deactivation**: by the timer and by the number of alarms.

What is Devices Auto Deactivation

It is also possible to manually disable a specific device. Learn more about deactivating devices manually here.

Clear notifications history

Clicking the button deletes all notifications in the hub events feed.

Monitoring Station — the settings for direct connection to the security company's central monitoring station. Parameters are set by security company engineers. Keep in mind that events and alarms can be sent to the central monitoring station of the security company even without these settings.

"Monitoring Station" tab: what is it?

- **Protocol** — the choice of the protocol used by the hub to send alarms to the central monitoring station of the security company via a direct connection. Available protocols: Ajax Translator (Contact-ID) and SIA.

- **Connect on demand**. Enable this option if you need to connect to the CMS (Central Monitoring Station) only when transmitting an event. If the option is disabled, the connection is maintained continuously. The option is available only for the SIA protocol.

- **Object number** — the number of an object in the monitoring station (hub).

Primary IP address

- **IP address** and **Port** are settings of the primary IP address and port of the security company server to which events and alarms are sent.

Secondary IP address

- **IP address** and **Port** are settings of the secondary IP address and port of the security company server to which events and alarms are sent.

Alarm sending channels

In this menu, channels for sending alarms and events to the central monitoring station of the security company are selected. Hub 2 Plus can send alarms and events to the central monitoring station via **Ethernet** and **EDGE**. We recommend that you use all communication channels at once — this will increase the transmission reliability and secure against failures on the telecom operators' side.

- **Ethernet** — enables event and alarm transmission via Ethernet.

- **GSM** — enables event and alarm transmission via the mobile Internet.

- **Periodic Test Report** — if enabled, the hub sends test reports with a given period to the CMS (Central Monitoring Station) for additional monitoring of object connection.

- **Monitoring Station Ping Interval** — sets the period for sending test messages: from 1 minute to 24 hours.

Encryption

Event transmission encryption settings in the SIA protocol. AES 128-bit encryption is used.

- **Encryption** — if enabled, events and alarms transmitted to the central monitoring station in SIA format are encrypted.

- **Encryption key** — encryption key of transmitted events and alarms. Must match the value on the Central Monitoring Station.

Panic button coordinates

- **Send coordinates** — if enabled, the pressing of a panic button in the app sends the coordinates of the device on which the app is installed and panic button is pressed, to the central monitoring station.

Alarm Restore on ARC

The setting allows you to select when the alarm restore event will be sent to the CMS: immediately/upon detector restore (by default) or upon disarming.

Learn more

Installers — PRO users settings (installers and representatives of security companies) of the security system. Determine who has access to your security system, the rights that are granted to PRO users, and how the security system notifies them about the events.

How to add PRO to the hub

Security companies — a list of security companies in your area. The region is determined by the GPS data or the regional settings of your smartphone.

User Guide — opens the Hub 2 user guide.

Data Import — a menu for automatical transferring devices and settings from another hub. **Keep in mind that you are in the settings of the hub on which you want to import data.**

Learn more about data import

Unpair hub — removes your account from the hub. Regardless of this, all the settings and connected detectors remain saved.

Settings Reset

Reset the hub to the factory settings:

1. Switch on the hub if it is turned off.

2. Remove all users and installers from the hub.

3. Hold the power button for 30 s — the Ajax logo on the hub will start blinking red.

4. Remove the hub from your account.

Events and Alarms Notifications

The Ajax security system informs the user about alerts and events using three types of notifications: push notifications, SMS, and phone calls. The alert settings can be changed only for registered users.

Types of events	Purpose	Types of notifications
Malfunctions		Push notifications
	• Loss of connection between the device and the hub	
		SMS

	• Jamming • Low battery charge in device or hub • Masking • Tampering with the detector body	
Alarm	• Intrusion • Fire • Flood • The hub has lost connection with the Ajax Cloud service	Calls Push notifications SMS
Events	• Switching on/off **WallSwitch**, **Relay**, **Socket**	Push notifications SMS
Arming/Disarming	• Arming/Disarming entire premises or group • Switching on Night mode	Push notifications SMS

How Ajax notifies the users about alarms

Connecting a security company

The list of organizations that connect the system to the central monitoring stations of the organizations may be found in the **Security companies** menu (**Devices** 📱 > **Hub** > **Settings** ⚙ > **Security companies**):

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

Connection to the Central Monitoring Station (CMS) is implemented via the Contact ID or SIA protocol.

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 device developed only for indoor use.

Make sure that communication between the hub and all connected devices is stable. If the signal strength is low (a single bar), we do not guarantee a stable operation of the security system. Implement all potential measures to improve the quality of the signal! At least, relocate the hub: even 20 cm shifting can significantly enhance the signal reception.

If, after the relocation, signal strength is still low or unstable, use the **ReX radio signal range extender**.

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.

Hub installation:

1. Fix the SmartBracket mounting panel (the hub lid) with bundled screws. When using any other fixing accessories, make sure that they do not damage or deform the hub lid.

> ⚠️ We do not recommend using double-sided adhesive tape: it cannot guarantee secure attachment and simplifies the removal of the device.

2. Put the hub on the lid and check the tamper status in the Ajax app.

3. To ensure higher reliability, fix the hub on the lid with bundled screws.

Do not flip the hub when attaching vertically (for instance, on a wall). When properly fixed, the Ajax logo can be read horizontally.

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

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

Do not disassemble or modify the hub or any of its parts: this can affect the normal operation of the device or cause its failure.

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.

- Close to radio interference sources: less than 1 meter from the router and power cables.

- Inside any premises with the temperature and humidity beyond the range of permissible limits.

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

The package includes

1. Hub 2

2. Power cable

3. Ethernet cable

4. Installation kit

5. Micro SIM (not included some countries)

6. Quick Start Guide

Technical Specifications

Classification	Intelligent security system control panel supporting ethernet and two SIM cards
Maximum number of connected devices	Up to 100
Connected ReX	Up to 5
Security groups	Up to 9
Security system users	Up to 50
Video surveillance	Up to 25 cameras or DVRs
Rooms	Up to 50
Scenarios	Up to 32 (Reactions by arming and disarming are not included in the overall limit of the hub's scenarios)
Central Monitoring Station communication protocols	Contact ID, SIA

	Photo verification integrated in Manitou, ABsistemDC(NG), WBB, Horus, V1/F1 and SBN
Power supply	110 – 240 V AC, 50 / 60 Hz
Built-in rechargeable battery	Li-Ion 2 A·h (up to 16 hours of battery life when Ethernet connection is disabled)
Energy consumption from the grid	10 W
Tamper proof	Available, tamper
Operating frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz, depending on the sales region
RF output power	8.20 dBm / 6.60 mW (limit 25 mW)
Radio signal modulation	GFSK
Radio signal range	Up to 2,000 m (any obstacles absence)
Communication channels	• 2 SIM cards (GSM 850/900/1800/1900 MHz GPRS) • Ethernet
Installation	Indoors
Operating temperature range	From -10°C to +40°C
Operating humidity	Up to 75%
Dimensions	163 × 163 × 36 mm
Weight	362 g