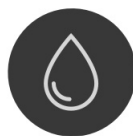


Hub 2 User Manual

Updated July 3, 2020



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



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.

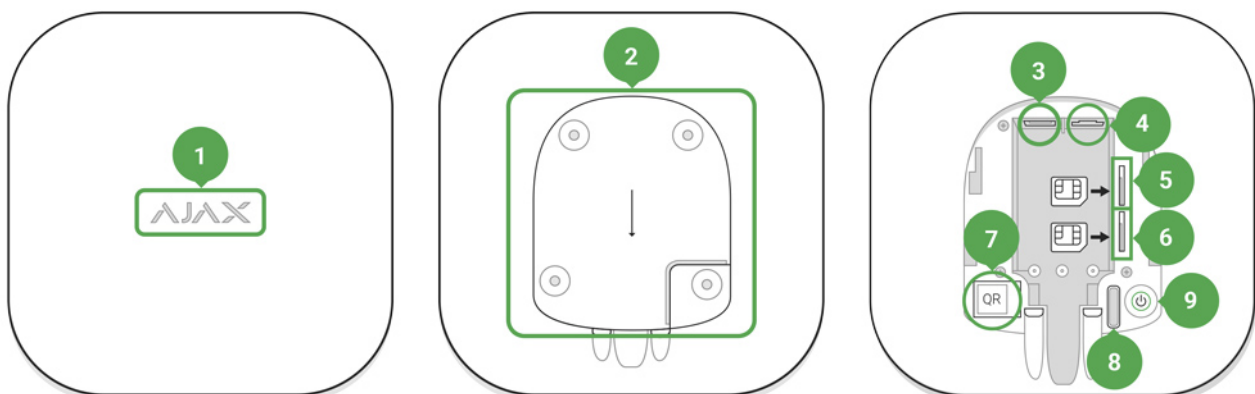
Use scenarios to automate the security system and decrease the number of routine actions. Adjust the security schedule, program actions of automation devices (Relay, WallSwitch or Socket) in response to an alarm, pressing of the Button or by schedule. A scenario can be created remotely in the Ajax app.

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.

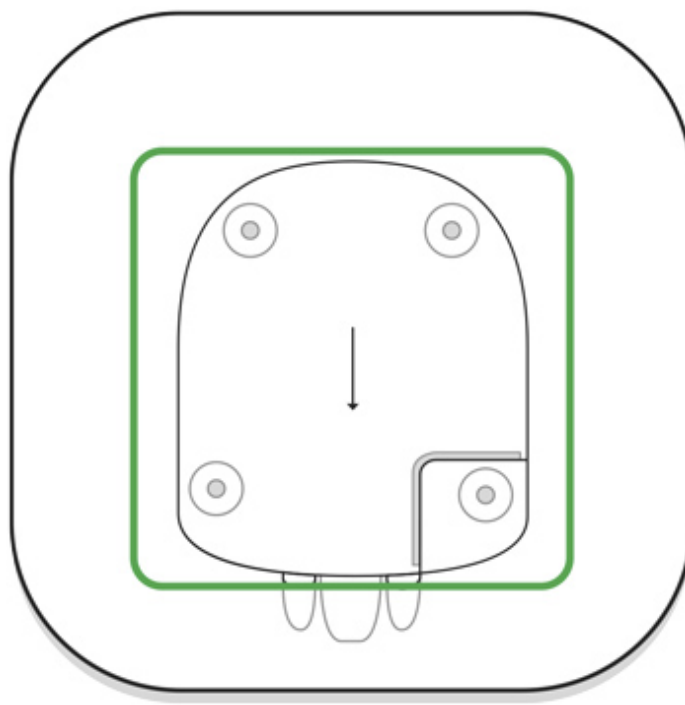
Security requirements

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.

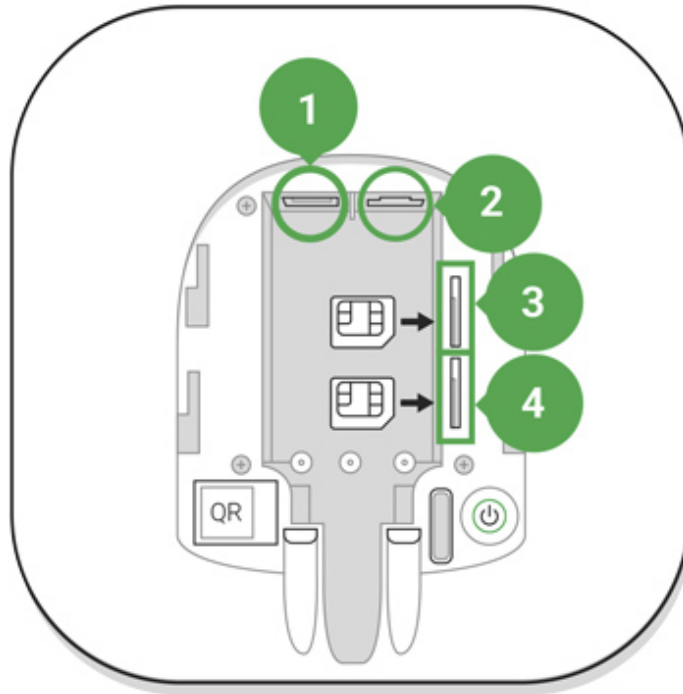
It is strictly prohibited to disassemble the device under voltage! Do not use the device with a damaged power cable.

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.



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](#)

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

The hub and connected devices settings are in the Hub Settings menu (under the gear icon) .

Customizable parameters:

Users — define who has access to your security system, what rights are granted to them, how the hub notifies of events.



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



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

Ethernet — configure the Ethernet connection.

Cellular — switch on/off GSM 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).



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

Groups — open group mode settings.

The capabilities the group mode:

- Manage the security of separate premises or groups of detectors.
The office is secured while the cleaner works in the kitchen.
- Differentiation of access to the administration tools of the security modes.
Employees of the marketing department do not have access to the law office.



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

Security Schedule — set a schedule to arm/disarm the security system automatically.



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

Detection Zone Test — run the detection zone test for the connected devices. The test determines the sufficient distance to trigger the alarm.



What is Detection Zone Test

Jeweller — configure the hub-detector ping interval and number of undelivered packets that determines connection failure.

- **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. (36 seconds by default).
- **Number of undelivered packets to determine connection failure** — a counter of undelivered packets (30 packets by default).

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

$$\text{Polling interval} * (\text{number of undelivered packets} + 1 \text{ correction packet})$$

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.

Keep in mind that the ping interval can reduce 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 — opens service settings of the hub.

Connection settings for the Hub and the Ajax Cloud service:

- **Server Ping Interval** — regulates the interval of sending pings from the hub to the server (range of 10 to 300 s). The recommended and default value is 60 s.
- **Connection Failure Alarm Delay** — regulates the alarm notification delay of the server connection loss. It is activated after 3 unsuccessful hub-server polls. The delay can be set in the range of 30 to 600 s. The recommended and default value is 300 s.

The time for generation of the message of the connection loss between the server and the hub is calculated as follows:

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

With the default settings, the Ajax Cloud service reports a hub loss after 9 minutes:

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



How quickly the loss of connection between the hub and the Ajax Cloud service is detected

- **LED Brightness.** Adjustment of the brightness of the LED logo. Available values are from 1 to 10 (the default value is 10).
- **System Integrity Check.** If enabled, the hub checks the status of all devices before arming: battery charge, tamper, connection. If a problem is detected, the hub does not arm the system and displays a warning.

- **Arming Permission** (the option becomes available only after enabling **System Integrity Check**). If enabled, the security system can be armed even with detected malfunctions.

To arm the security system with malfunctions through the Ajax app:

1. Activate the security mode: you will receive a notification with a list of malfunctions.
2. Confirm arming by pressing **Arm**.

To confirm arming with malfunctions using the KeyPad keyboard or SpaceControl key fob:

1. Activate the armed mode — you will receive a refusal.
2. Confirm the arming of the system by re-activating the armed mode within 30 s.



What is system integrity check?

- **Automatic software updates.** Configuring automatic OS Malevich firmware updates. When the hub is switched on, it automatically updates its firmware if a new version is available.



How OS Malevich updates

FireProtect and FireProtect Plus fire detector configuration

- **Interconnected FireProtect alarm.** The function activates built-in sirens of all fire detectors if at least one of them is triggered.



Interconnected alarms are supported by FireProtect and FireProtect Plus detectors with firmware versions 3.42 and higher. Please note that when you turn on the Interconnected Alarms, you cannot set the hub-detector ping interval (Jeweller settings) of more than 48 seconds.



What is an interconnected FireProtect alarms?

- **Ignore the first alarm.** Snooze feature for alarms to check for the presence of smoke.

The option works as follows:

1. The smoke alarm is triggered.
2. The built-in 30 s timer inside the detector is activated.
3. If, after 30 s smoke is detected, the alarm is transmitted to the hub.

This setting is recommended for premises with potential sources of false alarms, for example, if the detector is installed at the location where drafts are likely to occur.

- **Hub logs.** The settings for collecting and storing Ajax security system logs. You can disable logs or select a transmission channel:
 - Ethernet
 - Wi-Fi (only in Hub Plus)
 - No — logging is disabled





We do not recommend disabling logs as this information can help in the event of errors in the operation of the system!

Siren activation settings

- **If the hub or detector body is open.** When the function is active, the hub activates the connected sirens if the body of the hub, detector or any other Ajax device is open.
- **If the panic button is pressed in the app.** If enabled, the hub activates the connected sirens if the panic button is pressed in the Ajax app.



Disable the response of the siren by pressing the panic button on the SpaceControl key fob in the key fob settings (**Devices**  > **SpaceControl** > **Settings** )

Monitoring Station — configure CMS connection settings.



The events and alarms can be communicated to the central monitoring station of the security company without these settings



What the Monitoring Station is

PRO — configure PRO-accounts connected to the hub. 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.

Security Companies — choose and connect a security company in your region. The region is determined by the GPS data or the regional settings of your smartphone.

User Guide — opens the Hub 2 user guide.

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	<ul style="list-style-type: none">• Loss of connection between the device and the hub• Jamming• Low battery charge in device or hub• Masking• Tampering with the detector body	Push notifications SMS
Alarm	<ul style="list-style-type: none">• Intrusion• Fire• Flood• The hub has lost connection with the Ajax Cloud service	Calls Push notifications SMS
Events	<ul style="list-style-type: none">• Switching on/off WallSwitch,	Push notifications

	<u>Relay, Socket</u>	SMS
Arming/Disarming	<ul style="list-style-type: none"> • 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.

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
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	<ul style="list-style-type: none"> • 2 SIM cards (GSM 850/900/1800/1900 MHz GPRS) • Ethernet
Operating temperature range	From -10°C to +40°C
Operating humidity	Up to 75%
Dimensions	163 × 163 × 36 mm
Weight	362 g

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 function properly, we recommend that you first contact the support service as technical issues can be resolved remotely in half of the cases!



[Warranty](#)



[User agreement](#)

Technical support: support@ajax.systems



Need help?

In this section you'll find detailed manuals and educational videos about all features of Ajax. And in case you need help of a technical specialist, we're available 24/7.

Send request