# Hub User manual

Updated May 3, 2023



**Hub** is a central device of the Ajax security system, coordinating the connected devices, and interacting with the user and security company. Hub is developed only for indoor use.

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. 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 Jeweller 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
9. Cable retainer clamp

## LED Indication



00:00 00:06

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 10 seconds. The color of the indicator depends on the number of the connected communication channels. |

## 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
4 — Cable retainer clamp

**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 **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.

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.

If there are already users on the hub, the hub administrator, PRO with full rights or the installation company of the selected hub can add your account to it. You will receive a notification that the hub is already added to another account.

Get in touch with our support to determine who has admin rights on the hub.

User account types and rights



## 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.

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 that cause attenuation and shielding of the radio signal;
- in places with a weak GSM signal;
- close to radio interference sources: less than 1 meter from the router and power cables;

- in premises with temperature and humidity over the permissible limits.

**Hub installation:**

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. Fix the power and Ethernet cables with the supplied cable retainer clamp and screws. Use cables with a diameter no larger than the supplied ones. The cable retainer clamp must fit tightly to the cables so that the hub lid closes easily.

> The cable retainer clamp helps to prevent sabotage — the power and Ethernet cables will not be pulled out on purpose.

3. Put the hub on the lid and fix it with bundled screws.



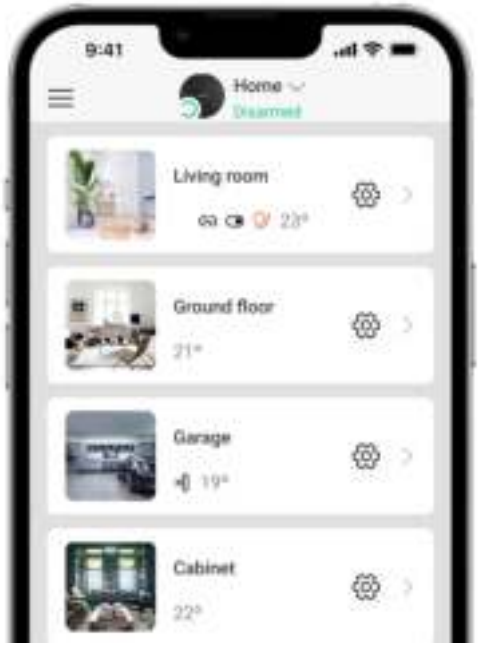
Do not flip the hub when attaching vertically (for instance, on a wall). When properly fixed, the Ajax logo can be read horizontally.

> 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 firmly fixed, the attempt to tear it off triggers the tamper, and the system sends a notification.




## 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.

## 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

> The hub doesn't support uartBridge and ocBridge Plus integration modules.




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).

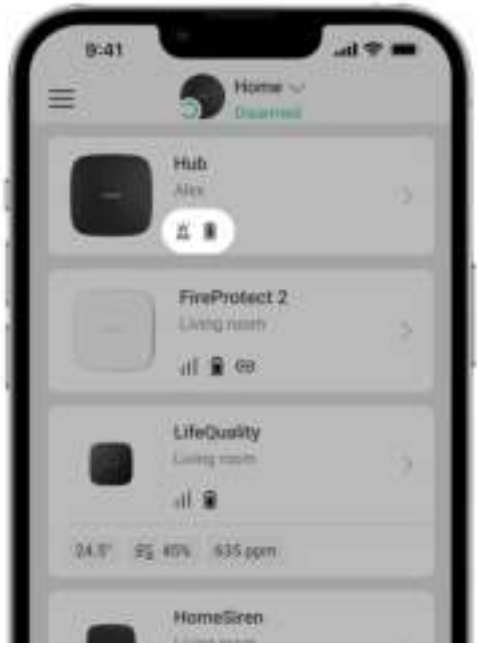
> Connection request is transmitted for a short time when switching on the device.

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**

## Hub icons




Icons display some of Hub 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 |

## Hub states



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

1. Go to the **Devices** tab .
2. Select Hub from the list.

| Parameter | Meaning |
|---|---|
| Malfunction | Click ⓘ to open the list of Hub malfunctions.<br><br>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<br><br>**How battery charge is displayed in Ajax apps** |
| Lid | Status of the tamper that responds to hub dismantling:<br><br>• **Closed** — the hub lid is closed<br><br>• **Opened** — the hub removed from SmartBracket holder<br><br>**What is a tamper?** |
| External power | External power supply connection status:<br><br>• **Connected** — the hub is connected to external power supply<br><br>• **Disconnected** — no external power supply |
| Connection | Connection status between the hub and Ajax Cloud:<br><br>• **Online** — the hub is connected to Ajax Cloud<br><br>• **Offline** — the hub is not connected to Ajax Cloud |
| Cellular data | The hub connection status to the mobile Internet:<br><br>• **Connected** — the hub is connected to Ajax Cloud via mobile Internet |

| | |
|---|---|
| | • **Disconnected** — the hub is not connected to Ajax Cloud via mobile Internet<br><br>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 |
| Ethernet | Internet connection status of the hub via Ethernet:<br><br>• **Connected** — the hub is connected to Ajax Cloud via Ethernet<br><br>• **Not connected** — the hub is not connected to Ajax Cloud via Ethernet |
| Average Noise (dBm) | Noise power level at Jeweller frequencies at the hub installation site.<br><br>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:<br><br>• **Connected** — the hub is directly connected to the central monitoring station of the security organization<br><br>• **Disconnected** — the hub is not directly connected to the central monitoring station of the security organization<br><br>If this field is displayed, the security company uses a direct connection to receive events and security system alarms<br><br>**What is a direct connection?** |
| 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 |

## Settings

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

1. Go to the **Devices** tab .
2. Select Hub 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**

**Hub name**

**Users**

**Ethernet**

**Cellular**

**Geofence**

**Groups**

**Security schedule**

**Detection zone test**

**Jeweller**

**Service**

**Monitoring Station**

**Installers**

**Security Companies**

**User Guide**

**Data Import**

**Unpair hub**

## Settings Reset

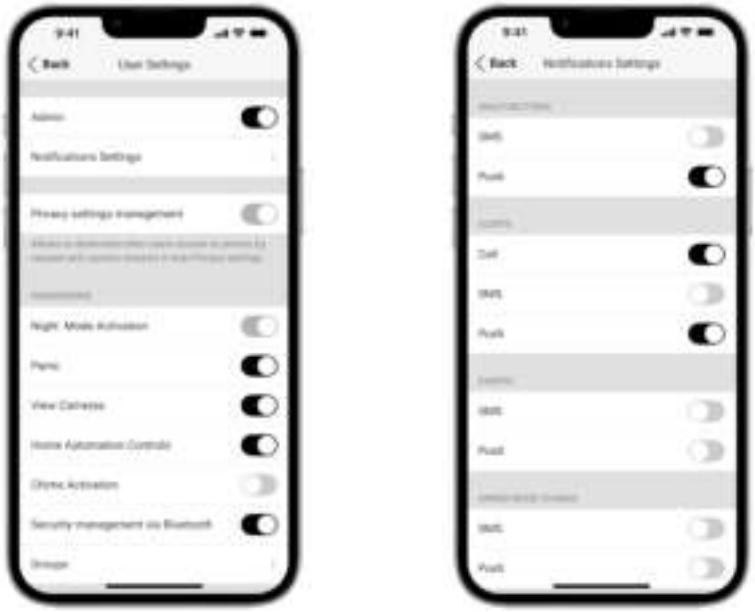
To return the hub to the factory default settings, switch it on, then hold the power button for 30 seconds (logo will start blinking red).

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



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 |
|---|---|---|
| Malfunctions | • Loss of connection between the device and the hub<br>• Jamming<br>• Low battery charge in device or hub<br>• Masking<br>• Tampering with the detector body | • Push notifications<br>• SMS |
| Alarm | • Intrusion<br>• Fire | • Calls<br>• Push notifications |

| | | |
|---|---|---|
| | • Flood<br>• Loss of connection between the hub and the Ajax Cloud server | • SMS |
| Events | • Activation of **WallSwitch**, **Relay**, **Socket** | • Push notifications<br>• SMS |
| Arming/Disarming | • Arming/Disarming entire premises or group<br>• Turning on **Night mode** | • Push notifications<br>• SMS |

- **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.

We call only in the event of an alarm to get your attention and reduce the feasibility of you missing an important 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.

> The hub does not notify users of opening detectors triggering in the Disarmed mode when the Chime feature is enabled and configured. Only the sirens connected to the system notify about the opening.
>
> What is Chime

How Ajax notifies users of alerts

## Connecting a Security Company




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 SurGard (Contact ID), ADEMCO 685, SIA (DC-09), and other proprietary protocols. A complete list of supported protocols is available **at the link**.

## 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.

## Technical Specifications

**All technical specifications of Hub**

**Compliance with standards**

## Warranty

Warranty for the Limited Liability Company “Ajax Systems Manufacturing” 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**

Subscribe to the newsletter about safe life. No spam

Email

Subscribe