Hub User Manual

Updated July 28, 2020

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

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

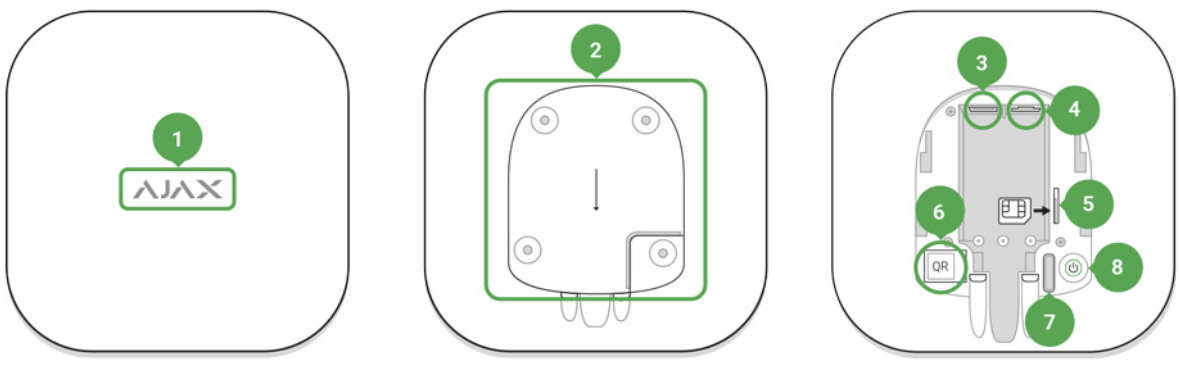
Up to 100 Ajax devices can be connected to the hub. The protected **Jeweller** radio protocol ensures reliable communication between the devices at a distance of up to 2 km in the line of sight.

List of 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.

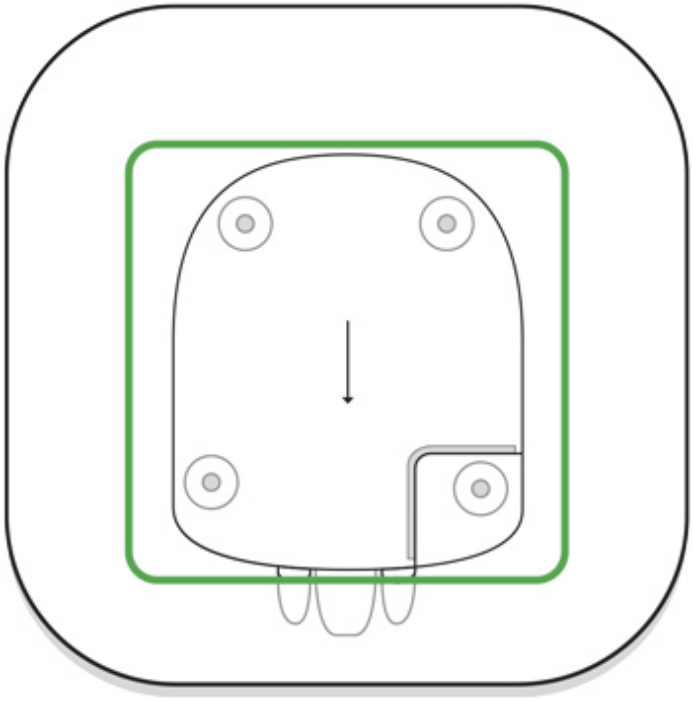
Communication with Ajax Cloud

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

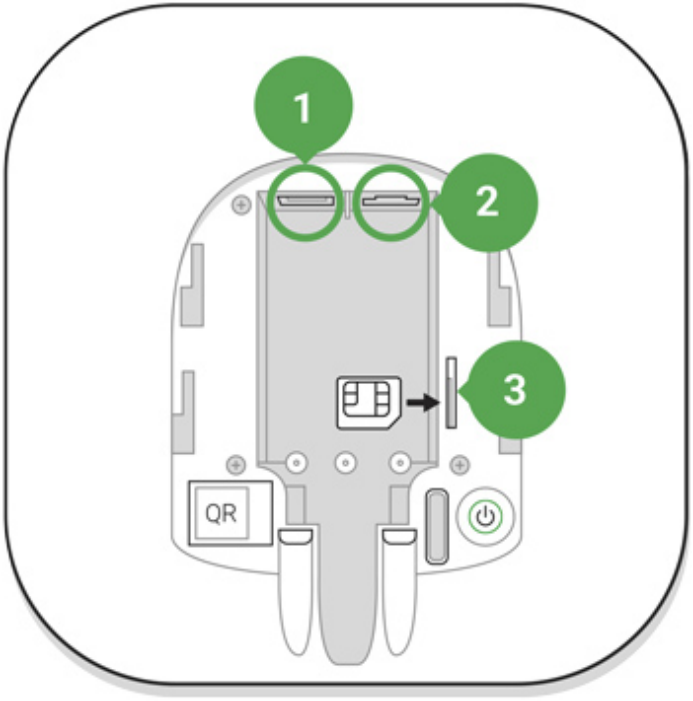
Connecting to the Network

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



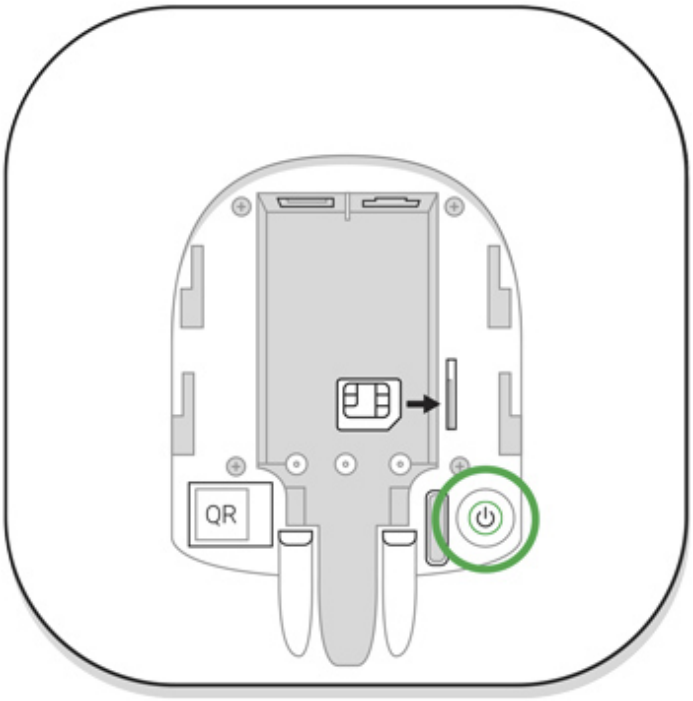
Be careful and do not damage the tamper protecting the hub from dismantling!

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.

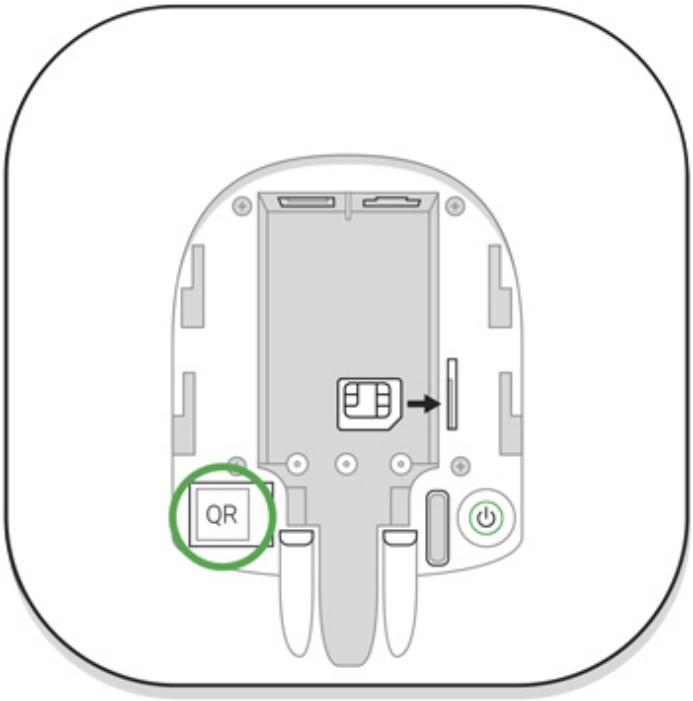
Create the Ajax account in the app following the step-by-step guide. As part of the process, you need to confirm your email and phone number.

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.

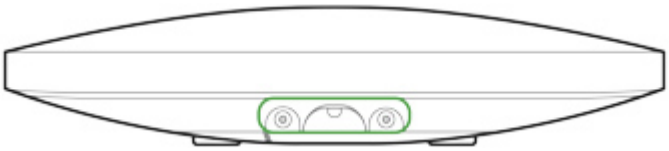
The hub should be reliably attached to the surface (vertical or horizontal). We do not recommend using double-sided adhesive tape: it cannot guarantee secure attachment and simplifies the removal of the device.

Do not place the hub:

- outside the premises (outdoors);
- nearby or inside any metal objects 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. Put the hub on the lid and fix it with bundled screws.

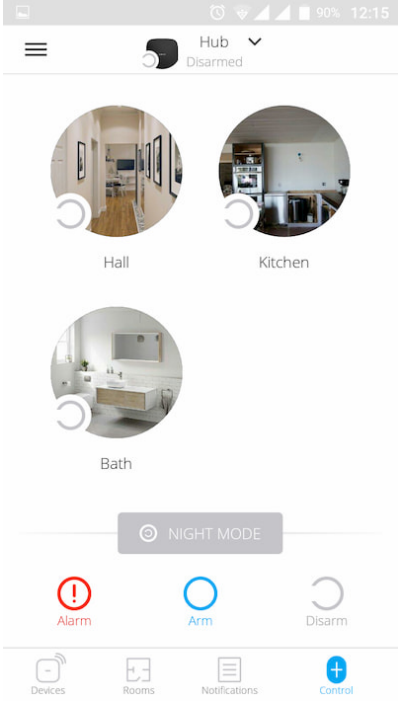


Do not flip the hub when attaching vertically (for instance, on a wall). When properly fixed, the Ajax logo can be read horizontally.

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

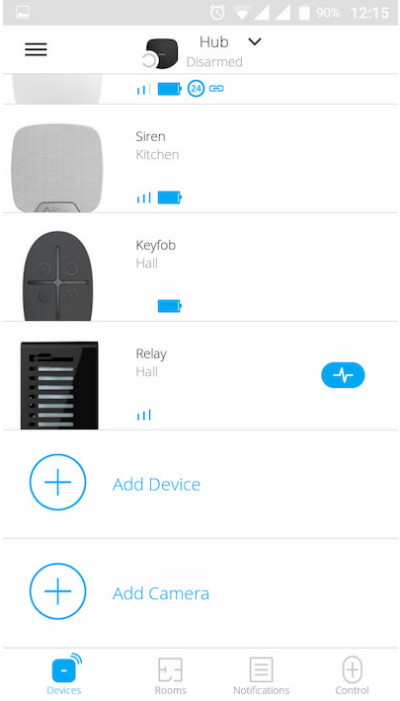
The room is created in the app using the **Add Room** menu.

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



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).

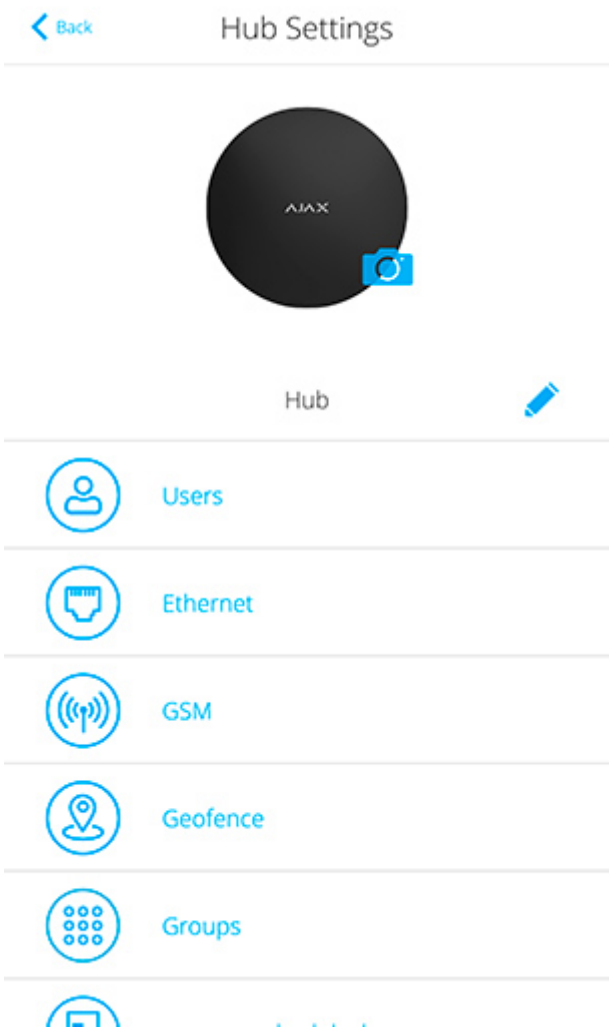
Connection request is transmitted for a short time at the moment of switching on the device.

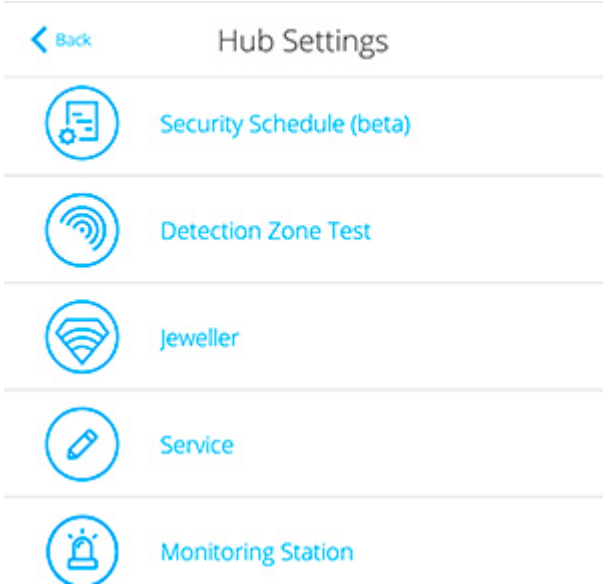
If the connection fails on the first try, switch off the device for 5 seconds and retry.

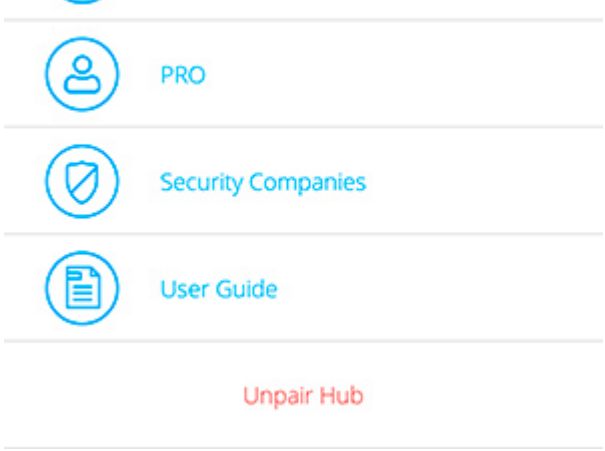
Up to 10 cameras or DVRs that support RTSP protocol can be connected to Hub.

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

- **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** > **SpaceContol** > **Settings**)

- **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

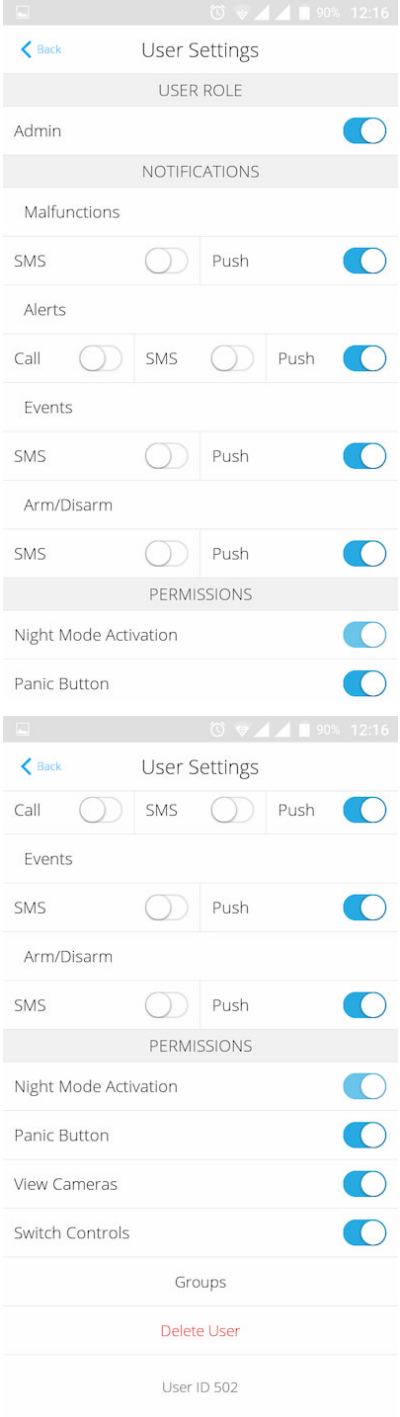
To return the hub to the factory default settings, switch it on, then hold the power button for 30 seconds (logo will start blinking red).

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



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

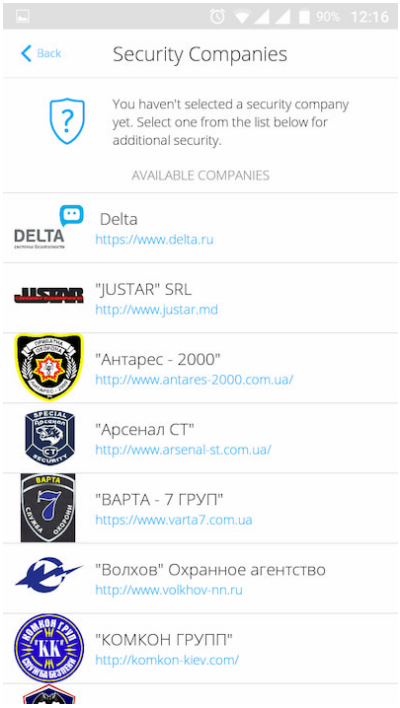
- **Push notification** is sent by Ajax Cloud to the Ajax Security system app, if an Internet connection is available.
- **SMS** is sent to the phone number indicated by the user when registering the Ajax account.
- The **phone call** means that the hub calls the number specified in the Ajax account.

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



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
Video surveillance	Up to 10 cameras or DVRs
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)
Energy consumption from the grid	10 W
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 × 163 × 36 mm
Weight	350 g
Certification	Security Grade 2, Environmental Class II 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!