Hub User Manual

Updated September 28, 2021

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

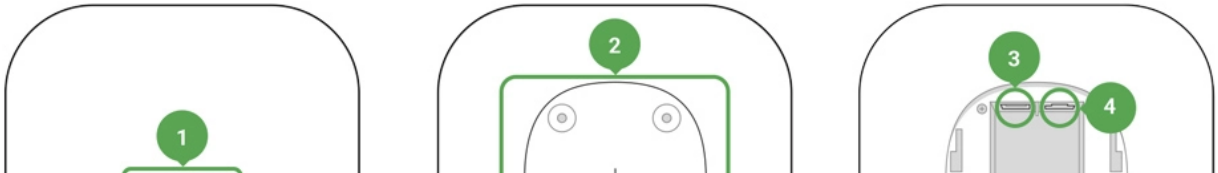
Up to 100 Ajax devices can be connected to the hub. The protected **Jeweller** radio protocol ensures reliable communication between the devices at a distance of up to 2 km in the line of sight.

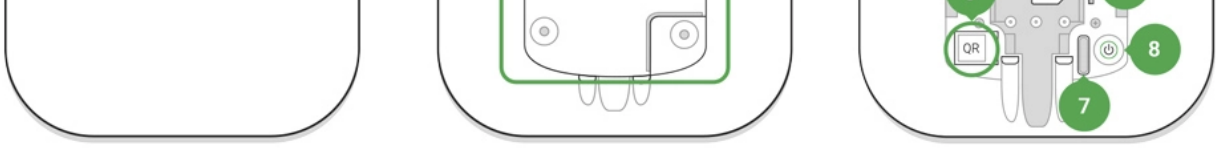
List of Ajax devices

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

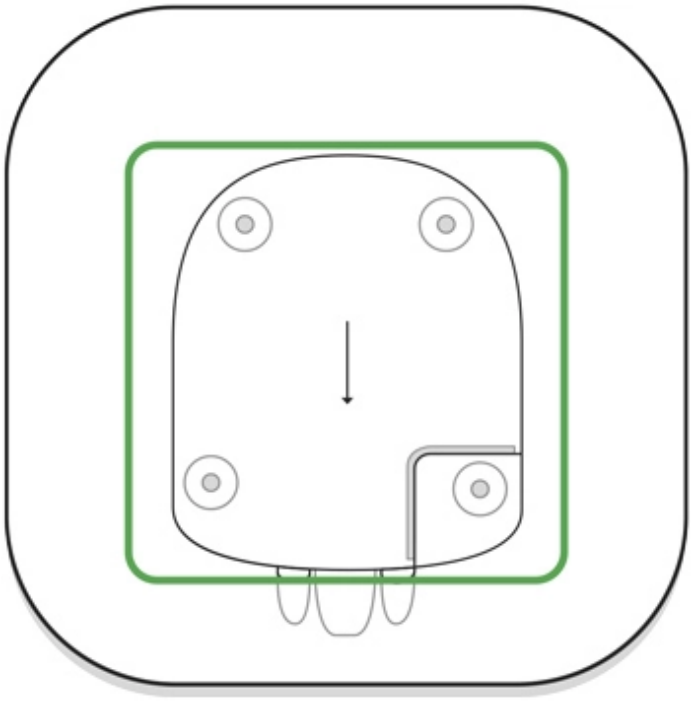
LED Indication

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

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.

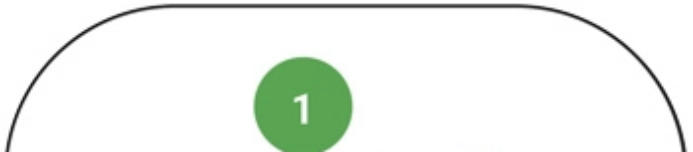
Connecting to the Network

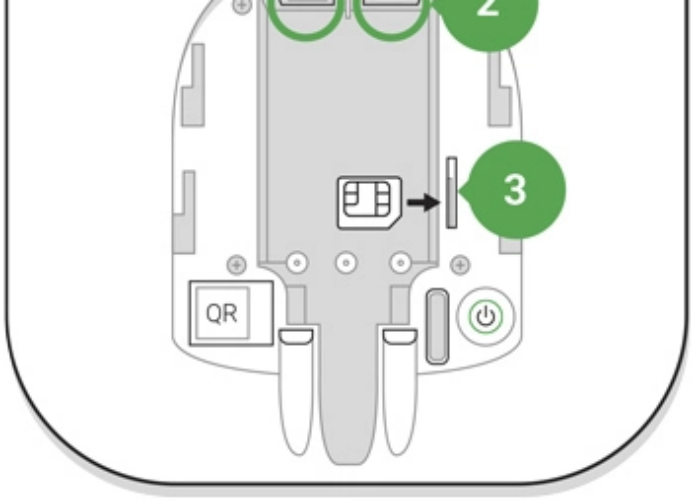
1. Open the hub lid by shifting it down with force.



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

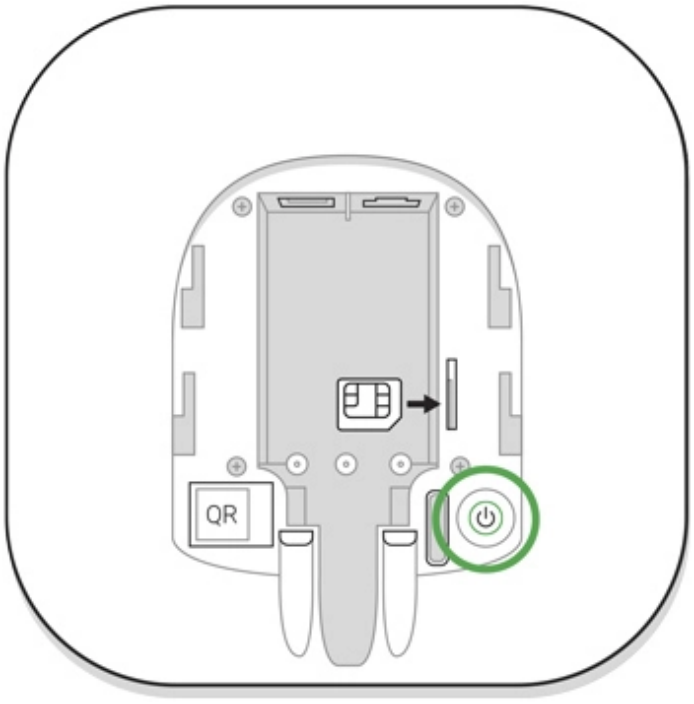
2. Connect the power supply and Ethernet cables to the sockets.





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

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

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.

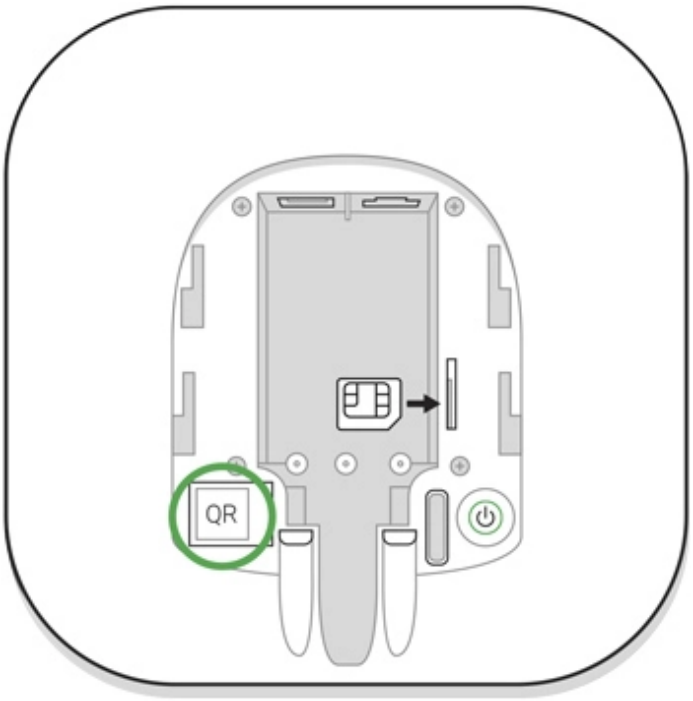
One phone number may be used to create only one Ajax account.

Create the Ajax account in the app following the step-by-step guide. As part of the

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.

Installation

Prior to installing the hub, make sure that you have selected the optimal location: the SIM

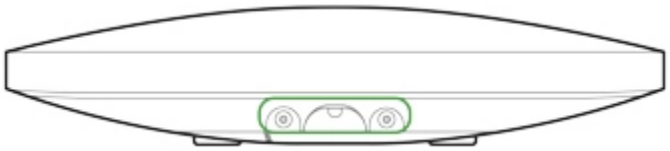
The hub should be reliably attached to the surface (vertical or horizontal). We do not recommend using double-sided adhesive tape: it cannot guarantee secure attachment and simplifies the removal of the device.

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

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.

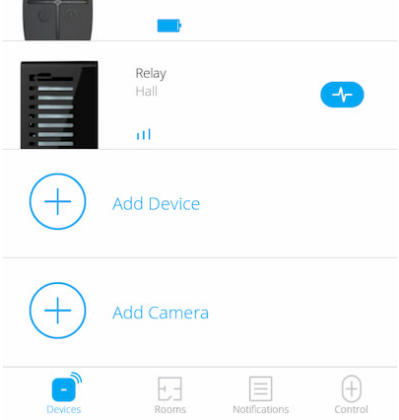
Please assign a name for the room, and optionally, attach (or make) a photo: it helps to find the needed room in the list quickly.

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 at the moment of switching on the device.

Icons

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

Icons	Meaning
	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 from the list.

	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

	and send SMS messages even if the **Not connected** status is displayed in this field
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 Jeweller frequencies at the hub installation site. 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 **What is a direct connection?**

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 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.

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

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

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

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.

> 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

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.

How to enable and configure group mode in the Ajax security system

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

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

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.

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.

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	PD 6662 Setting Wizard Server Connection Sirens settings

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

- **Hub-Server Polling Interval, sec.** 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.
- **Deley of Server Connection Failure Alarm, sec.** 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*

notification about loss of connection via one of the communication channels. Set in the range from 3 to 30 minutes.

The time of sending a notification about the loss of connection via one of the communication channels is calculated with the formula:

*(Polling interval * 4) + Time filter + Loss Notification delay*

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.

Feature implementation in StreetSiren

Feature implementation in StreetSiren DoubleDeck

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/KeyPad Plus.

Learn more

System Integrity Check

Restoration 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

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.

- **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 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.

- **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

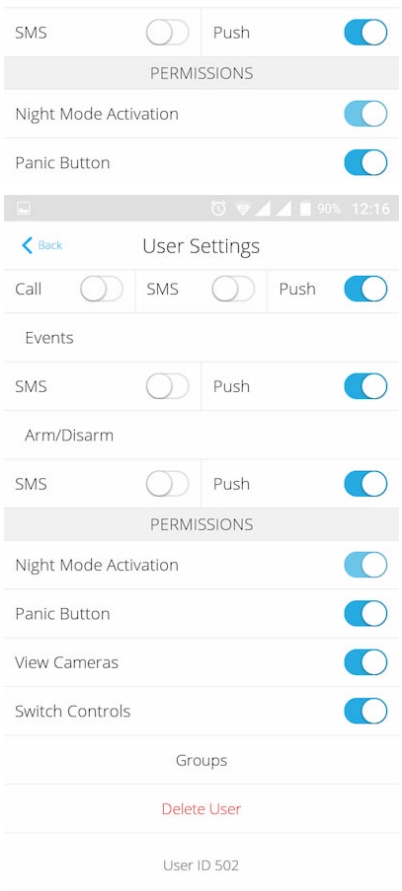
you want to import data.

Learn more about data import

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

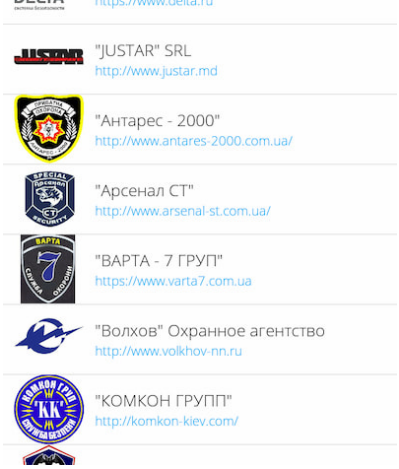
Settings Reset

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)


SMS
Push
PERMISSIONS
Night Mode Activation
Panic Button
90% 12:16
Back
User Settings
Call
SMS
Push
Events
SMS
Push
Arm/Disarm
SMS
Push
PERMISSIONS
Night Mode Activation
Panic Button
View Cameras
Switch Controls
Groups
Delete User
User ID 502

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

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.

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) **Learn more**
Communication channels	GSM 850/900/1800/1900 MHz GPRS, Ethernet

Technical support: **support@ajax.systems**