Hub User Manual

Updated September 19, 2019

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

How to install the Ajax StarterKit, if you've never done this before. A masterclass from the undisputed cruiserweight champion Oleksandr Usyk.

.

Hub needs Internet access for connection to the cloud server Ajax Cloud – for setting up, control from any point of the world, transmission of event notifications and update of the software. The Ajax Cloud server is located on the capacities of Amazon Web Services. Personal data and detailed system operation logs are stored under multilevel protection, and information exchange with the Hub is carried out via an encrypted channel on a 24-hour basis.

To communicate with the Ajax Cloud, the system uses a wired Ethernet connection and GSM network of a mobile operator.

If possible, please use both Internet connection channels. This will ensure more reliable communication between the Hub and the Ajax Cloud and prevent from failures in the operation of one of the communication service providers.

Hub can be controlled via an app for iOS and Android-based smartphones. Mobile apps allow responding promptly to any notifications of the security system.

Follow the link to download an app for your smartphone:

Android

iOS

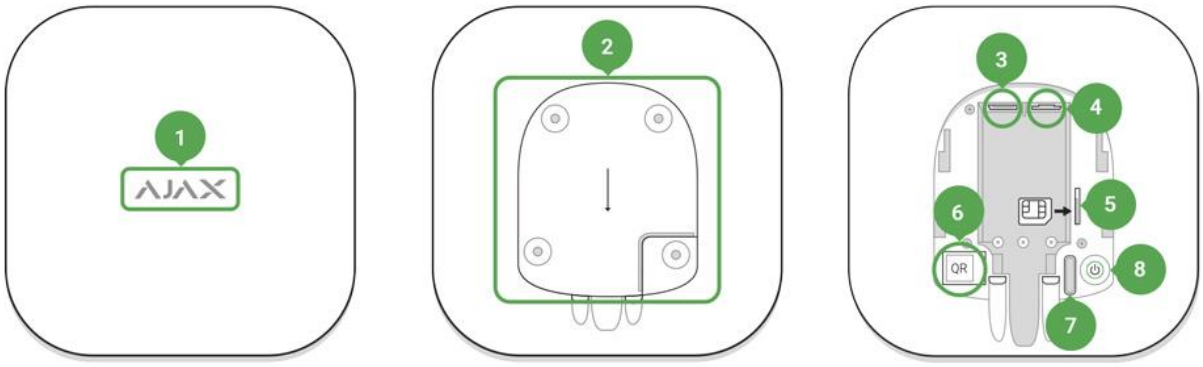
You may set up in the Hub what events and how will be notified to the user. Choose what is more convenient for you: push notifications, SMS, or phone call. If the Ajax system is handed over for servicing to a security company, an alarm signal will be sent it directly, bypassing the server.

Buy intelligent security control panel Hub

Up to 100 Ajax devices are connected to the Hub. The protected Jeweller protocol is used for communication between the devices, with the coverage radius up to 2 km, absent any obstacles.

List of Ajax devices

Hub Sockets and Operational Indication



1. Logo with a light indicator
2. SmartBracket attachment panel (perforated part is required for actuating the tamper in case of any attempt to tear off the Hub from the surface)
3. Socket for connecting a power supply cable
4. Socket for connecting an Ethernet cable
5. Slot for installing a card of a cellular service provider (Micro SIM type)
6. QR code
7. Tamper button
8. On/Off button

Hub Operation Indication by Logo Light

When you click 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.

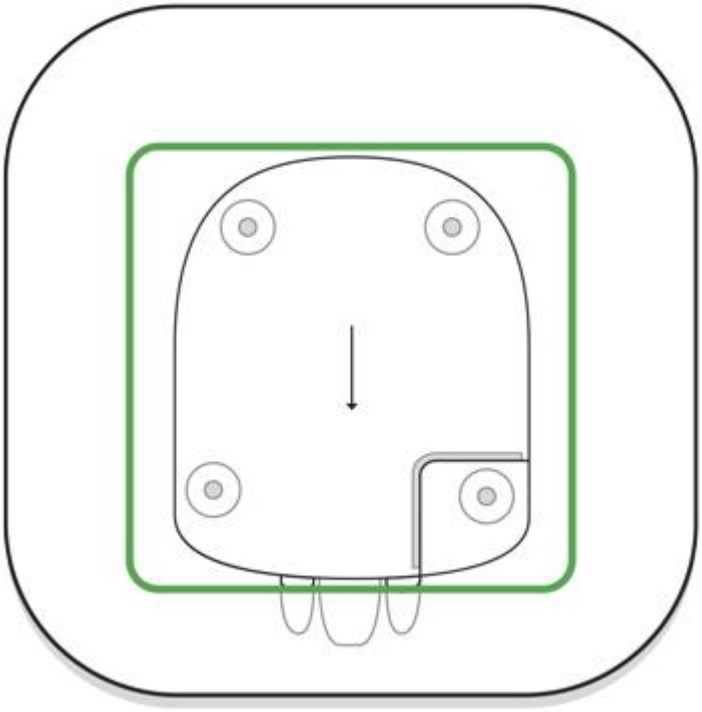
Communication with the Ajax Cloud

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

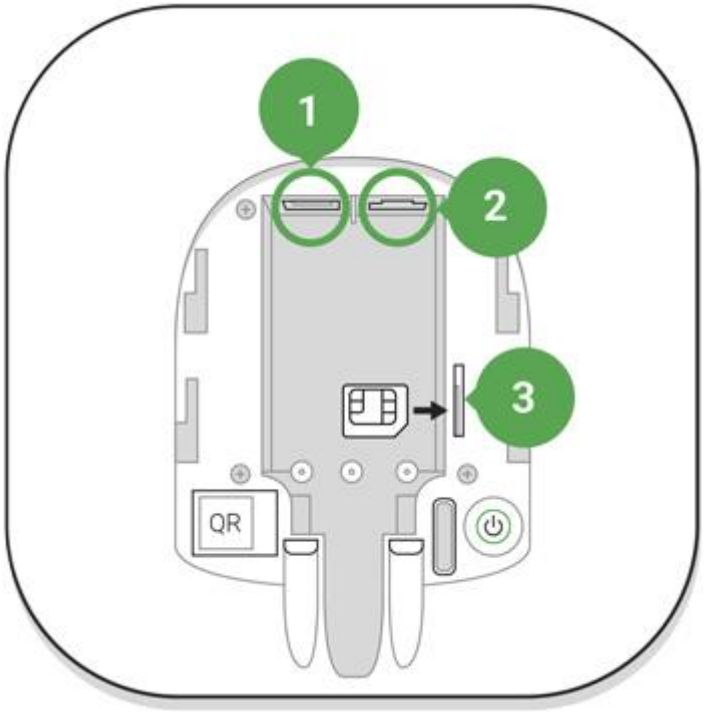
Connection Hub to the Network

1. Open the Hub cover by shifting it down by force.



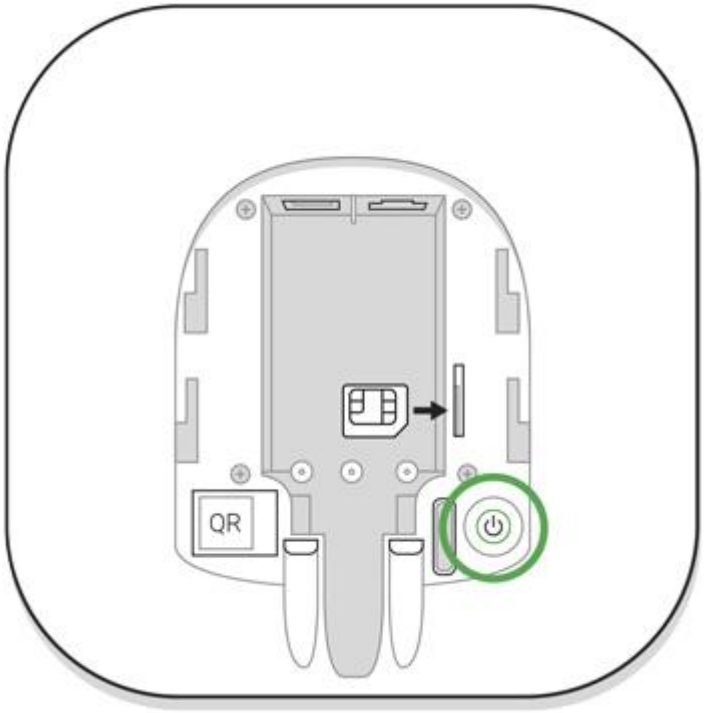
Be careful not to damage the tamper protecting the Hub from hacking!

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



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

3. Press and hold the “on” button for 2 seconds until the logo lights up. The Hub needs approximately 2 minutes to identify the available communication channels.



Bright green or white color of the logo notifies that the Hub has connected to the server

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 set-up of the Hub in the web application or mobile application, you will be able to preset a static IP address.

To connect to the GSM network, you will need a Micro-SIM format mobile operator's card with the disabled PIN code request (PIN code request can be disabled using your mobile phone) and sufficient amount on the account to pay for the GPRS, SMS services and make calls.

In some regions, Hub is sold already complete with a SIM card

If the Hub does not connect to the Ajax Cloud via the GSM network, use Ethernet to set up the network parameters in the mobile application. To prescribe the access point, username and password correctly, please contact the support service of the operator.

Ajax Account

The Ajax security system is set up via the app to which the account of the administrator is connected. The account with the information about the added Hubs is placed on the cloud server Ajax Cloud in encrypted form.

User parameters of the Ajax security system and connected devices are stored locally on the Hub and are inextricably connected with it. Any change of the Hub administrator does not result in any failure in the settings of the devices connected thereto.

The telephone number may be used to create only one Ajax account

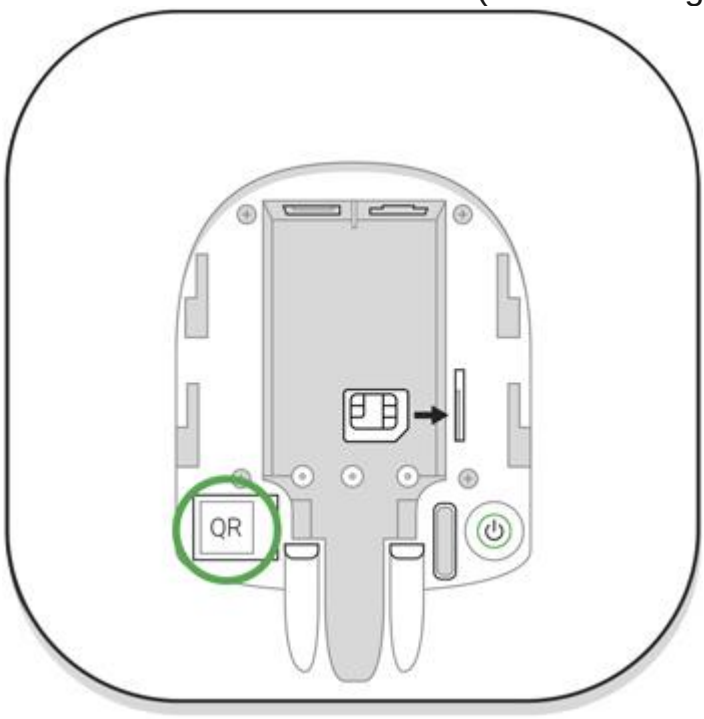
Create an account in the Ajax system in the mobile app following the step-by-step guidance. As part of the process, you will need to confirm your e-mail address and mobile phone number.

Your account may combine the roles – administrator of one Hub, user of another Hub.

Adding a Hub to the Ajax Security System app

You must give the app access to all the system functions (in particular, to display notifications)! This is a sine qua non-condition of controlling the Ajax security system from a smartphone/tablet.

1. Enter into your account.
2. Open the menu **Add Hub** and select the suitable method – manually or with a step-by-step guide.
3. At the registration stage, prescribe the name of the Hub and scan the QR code located under the cover (or enter a registration key manually).



4. Wait until the Hub is registered and a new device appears on the application desktop.

Hub 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 should be hidden from direct view.

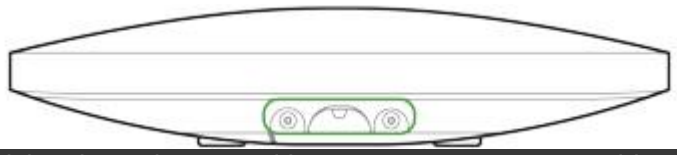
The Hub should be reliably attached to the surface (vertical or horizontal). We strongly discourage using double-sided adhesive tape – it cannot guarantee secure attachment and facilitates disassembly of the device.

Do not install the Hub:

- outside the premises (outdoors);
- nearby or inside any metal objects or mirrors causing attenuation and screening of the signal;
- in places with the low GSM signal and high radio interference level;
- within any premises with the temperature and humidity beyond the range of permissible limits.

Installation of the Hub:

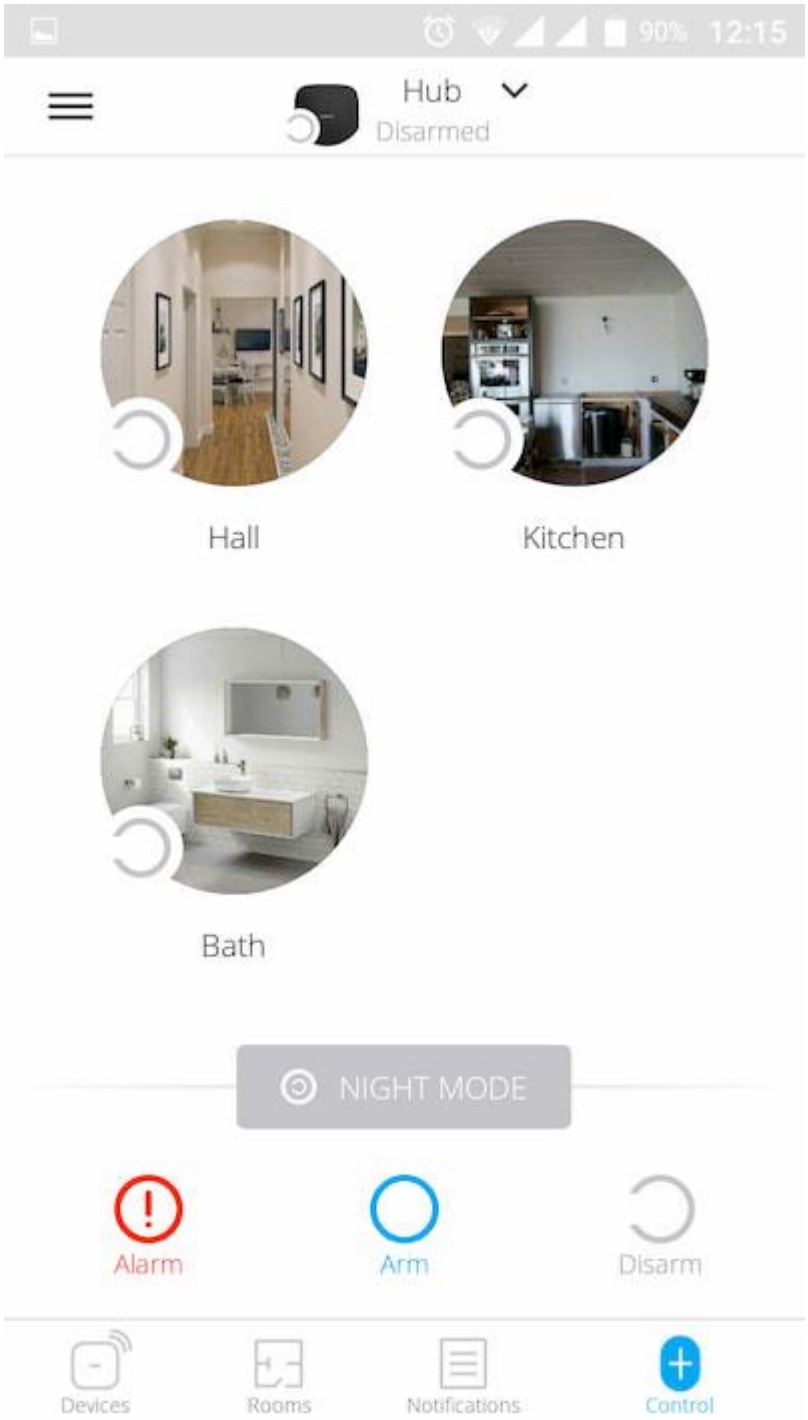
1. Put the Hub on the cover and fix it with bundled screws.
2. Fix the Hub cover on the surface using bundled screws. If using any other attachment hardware, make sure that they do not damage or deform the Hub cover.



Fixing the Hub cover with screws prevents any accidental shifting of the Hub and minimizes the risk of impulse theft of the device.

If the Hub is securely attached, when tearing off the body from the surface, the tamper will be actuated, and you will receive the respective notice.

Rooms in the Ajax Security System app



Rooms combine the connected devices. The app can create up to 50 rooms, with each device located only in one room.

Without creating a room, you will not be able to add devices to the Ajax Security System app!

Creating and Setting Up a Room

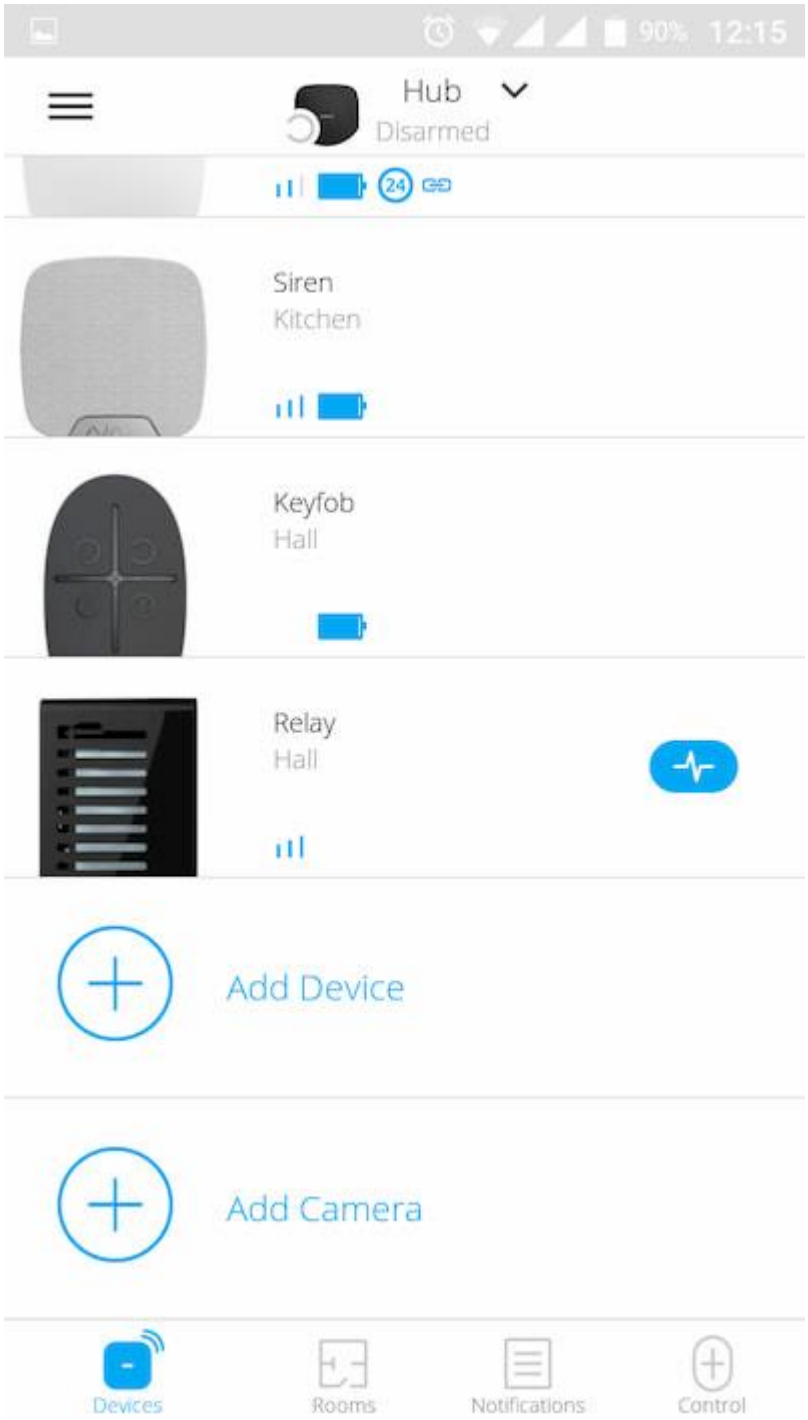
The room is created in the mobile app using the menu **Add Room**.

Assign a name to the room, if wished, attach (or make) a photo – you will easier find the required room in the list.

By pressing on the gear wheel go to the room set-up menu.

To delete a room, move all the devices stored in it to other rooms via the device setup menu. Deleting the room will erase all its settings.

Connecting Devices to the Hub



During the first registration of the Hub in the mobile app, you will be prompted to add devices to guard the room. However, you may refuse and return to this step later.

The device may be only added if the system is disarmed!

1. Open a room in the mobile app and select the option **Add Device**.
2. Give an arbitrary name to the device, read out the **QR code** (or insert the ID manually), select a location room and go to the next step.

3. When the app starts to search and launches countdown, switch on the device – it will blink once with a LED. For the detection and interfacing to occur, the device should be located within the coverage area of the wireless network of the Hub (at a single protected object).

Request for connection to the Hub is transmitted for a short time at the time of switching on the device

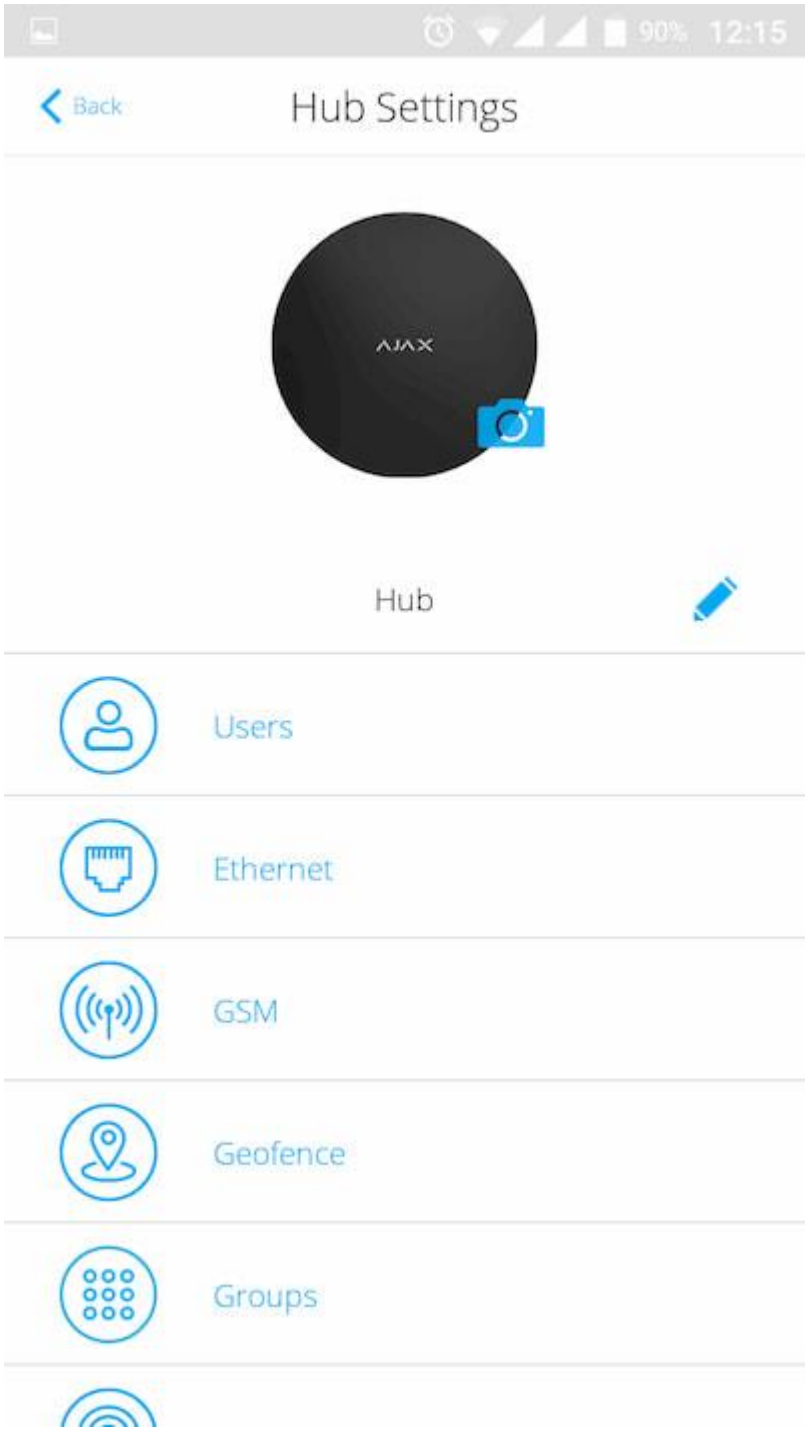
If the connection to the Hub failed on the first try, switch off the device for 5 seconds and repeat the attempt.

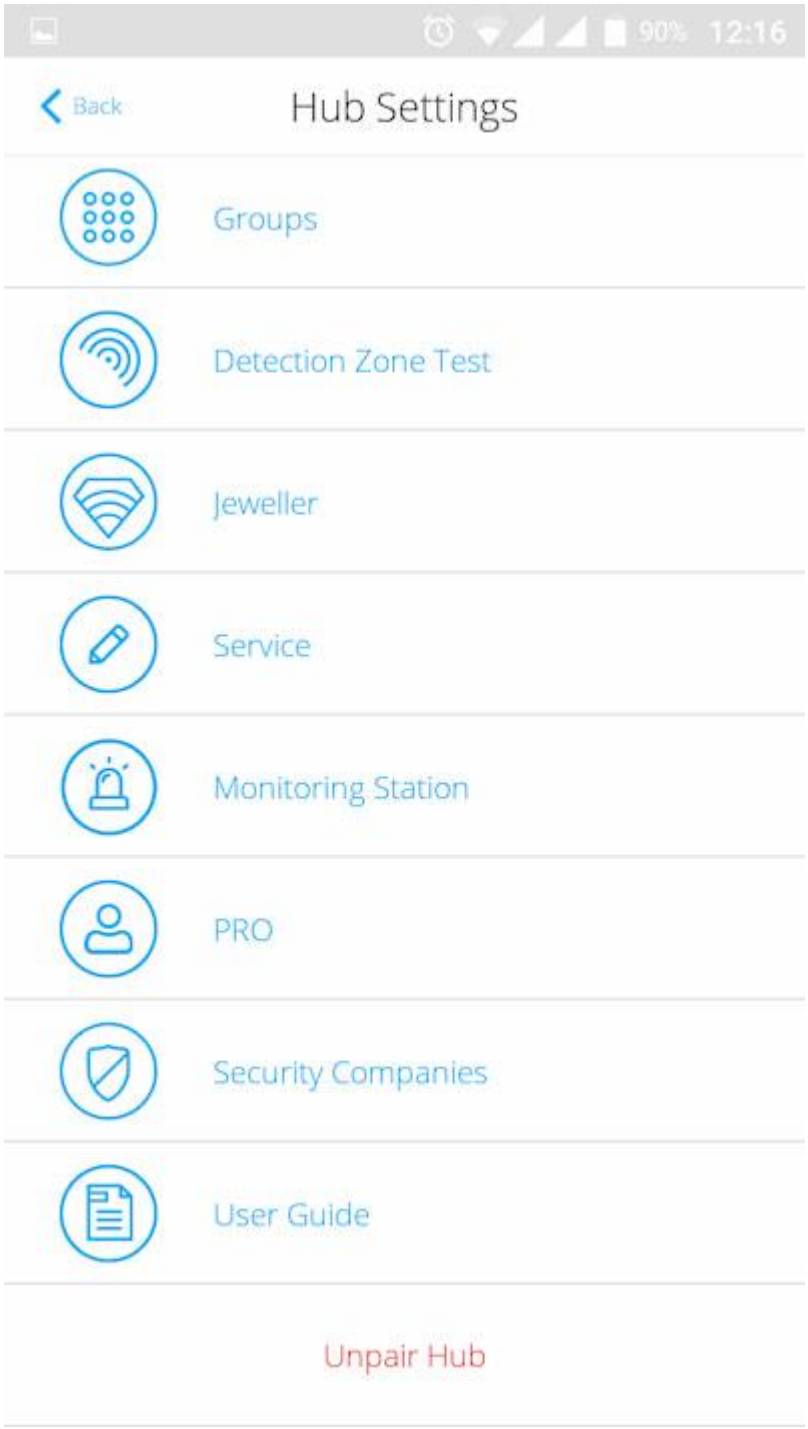
Up to 10 cameras or NVRs that support RTSP protocol can be connected to the Ajax Hub.

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

Setting Up the Hub

Settings of the Hub and the devices connected thereto are located in the menu **Hub Settings** .


90% 12:15
Back
Hub Settings
AJAX
Hub
Users
Ethernet
GSM
Geofence
Groups



Adjustable parameters:

- **Users** — who have access to your security system, what rights are granted to them, how the Hub notifies of events.
- **Ethernet** — set-up of a wired Ethernet connection.
- **GSM** — switching on/off cellular communication, set-up of the connection and verification of the account.

- **Geofence** — a reminder of arming/disarming the security system from the intrusion detection mode, if a specific zone is crossed.

  User location is determined based on the data of the GPS antenna and iBeacon beacons (only for Apple equipment).

- **Groups** — groups mode settings.
- **Detection zone test** — testing the detection zone of the devices connected to the Hub.
- **Jeweller** — identification of the Hub-detector inquiry interval and the number of undelivered data packets.

  The inquiry interval of the detectors by the Hub determines how frequently the devices exchange data. The smaller the interval is (in seconds), the quicker the Hub learns about events of the connected devices and the devices receive commands from the Hub. The value of the number of undelivered packets determines how quickly the Hub learns about the loss of the connected device.

  Calculation of the time for giving the alarm (with the default parameters):

  (8 packets + 1 corrective) x 36 seconds inquiry interval = 5 minutes 24 seconds

  At that, information about any alarm or sabotage is transmitted immediately. We should keep in mind that the small interval limits the maximum number of connected devices:

Interval	Connection limit
12 seconds	39 devices
24 seconds	79 devices
36 and more seconds	100 devices

- **Service** — a group of service settings of the Hub.

  Connection failure alarm delay — time period regulating the delay of notification of the lost communication with the server.

  Server ping interval — the interval of sending pings from the Hub to the server.

Time to the generation of a message of the lost communication between the server and the Hub is calculated as follows (with the default parameters):

(3 pings + 1 corrective) x 30 seconds inquiry interval + 300 seconds time filter = 7 minutes

You can change the settings for auto-update of the hub (enabled by default).

How to turn off hub firmware auto-update

- **Monitoring Station** — connection to the CMS settings.
- **PRO** — PRO-accounts on the Hub.
- **Security Companies** — security companies in your region.

Reset of the Hub Settings

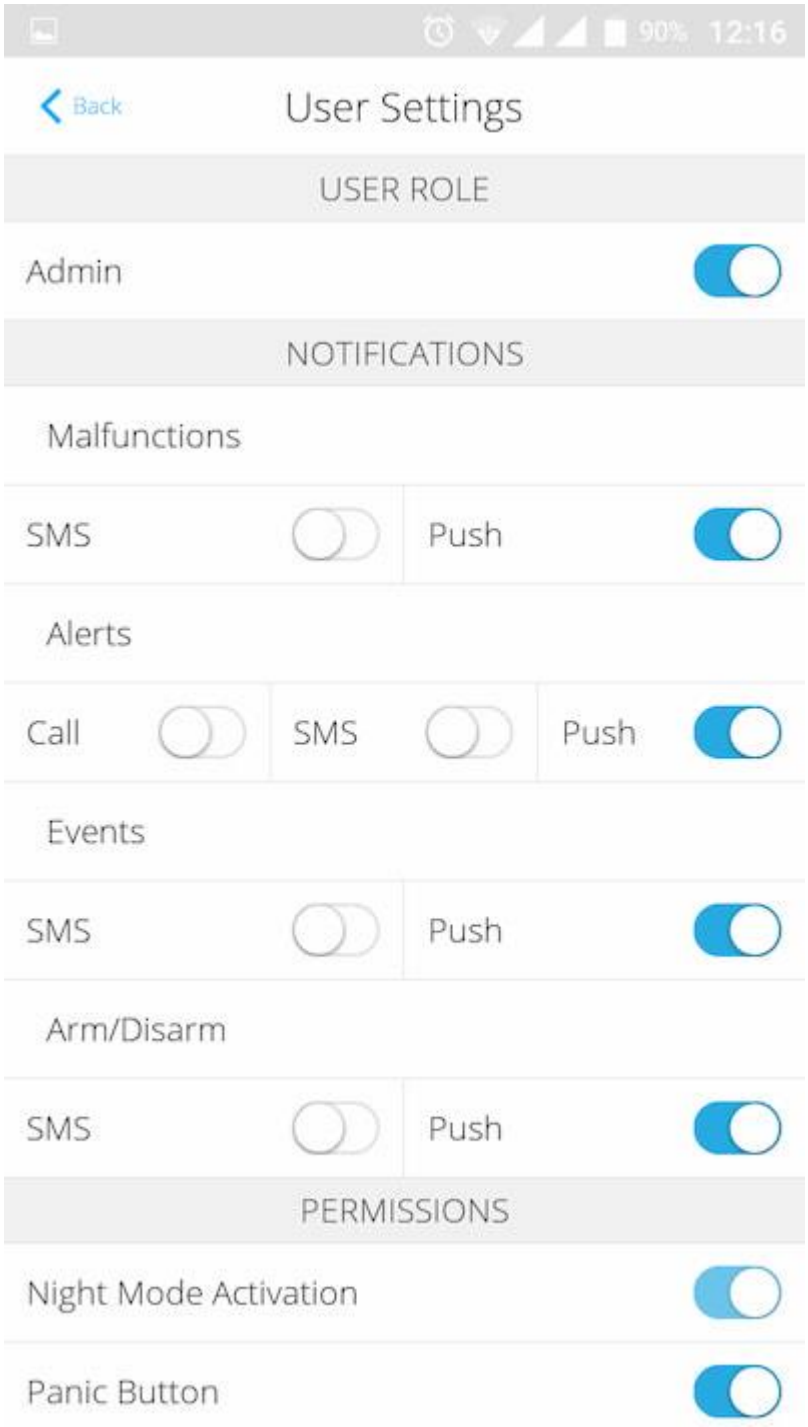
To return the Hub to the factory settings, switch it on, then hold the “on” button for 30 seconds (logo will start blinking red).

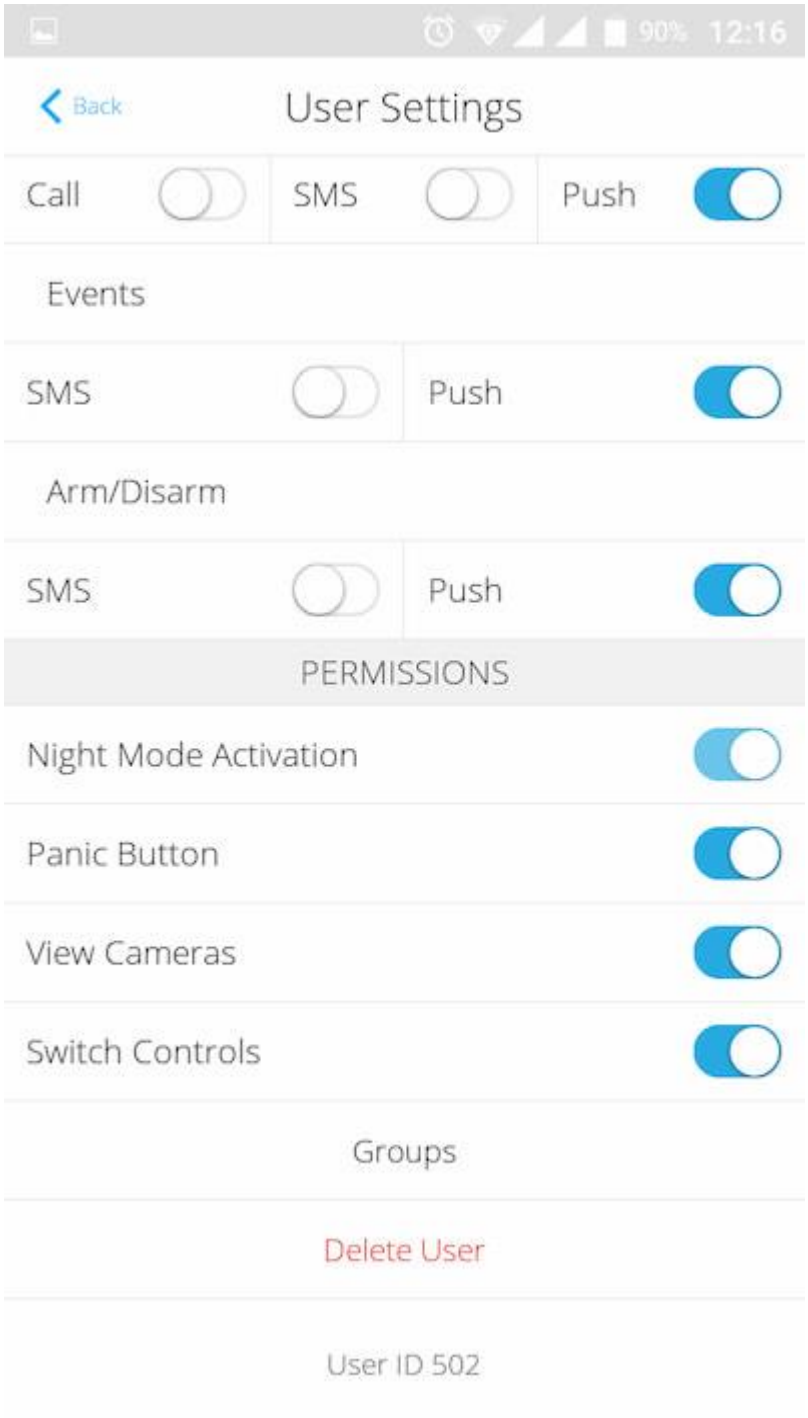
At that, all the connected detectors, room settings and user settings will be deleted. User profiles will remain connected to the system.

Users

After adding a Hub to the account, you will become the administrator of this device. One Hub may have up to 50 users/administrators. The administrator can invites users to the security system and determines their rights.

Event and Alarm Notifications


90% 12:16
Back
User Settings
USER ROLE
Admin
NOTIFICATIONS
Malfunctions
SMS
Push
Alerts
Call
SMS
Push
Events
SMS
Push
Arm/Disarm
SMS
Push
PERMISSIONS
Night Mode Activation
Panic Button



The Hub notifies the user of events using three methods: mobile push notifications, SMS and phone calls.

Notifications are set up in the menu **Users**:

Event types	For what it is used	Types of notif
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

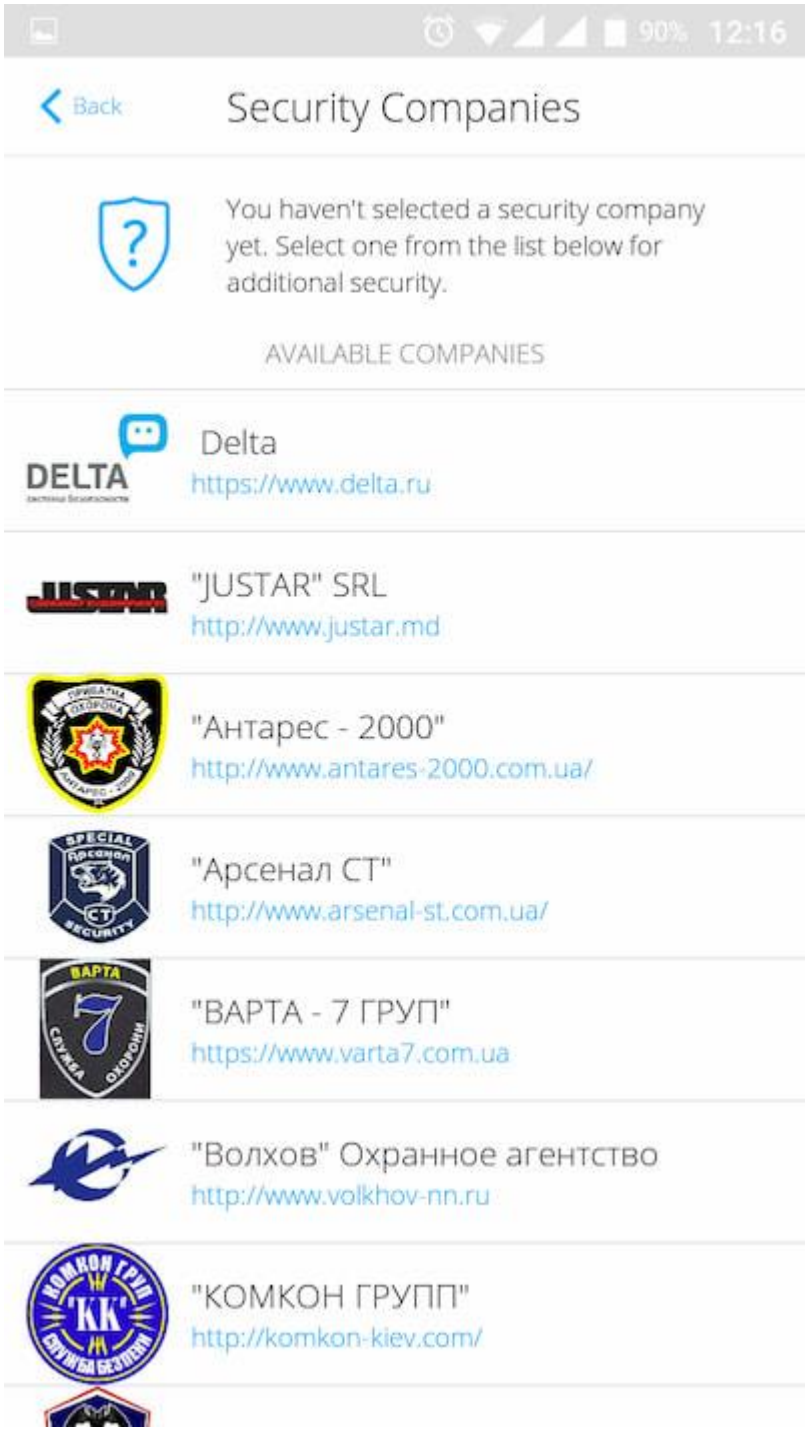
- **Push notification** – is sent by the server Ajax Cloud to the Ajax Security system app, if the Internet connection is available.
- **SMS message** – is sent to the telephone number indicated by the user during registration of the Ajax account.
- A **phone call** refers to the hub calling the phone number specified in the account of the Ajax app.

  We call only in the event of an alarm to get your attention and reduce the feasibility of you missing a critical alert. It is recommended that you 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 that you save the phone number associated with the hub SIM card in your contacts list.

Notification settings may be only changed for registered users.

Connecting the Ajax System to a Security Company



The list of organizations connecting the Ajax system to the central monitoring station is provided in the menu **Security Companies** of the Hub settings.

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

Connection to the central monitoring station (CMS) is made via the Contact ID or SIA protocols.

Maintenance of the Ajax System

Check the operational capability of the Ajax security system on a regular basis.

Clean the body of the Hub from dust, spider web and other contaminations as they appear. Use soft dry napkin suitable for equipment maintenance.

Do not use for cleaning the Hub any substances containing alcohol, acetone, gasoline and other active solvents.

How to replace hub battery

Complete Set of the Hub

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

In installing and operating 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 cord.

Tech Specs

Maximum number of connected devices	100
Maximum number of the groups	9
Maximum number of the Hub users	50
Maximum number of logical rooms	50
Power supply	110 – 240 V AC, 50 / 60 Hz
Accumulator unit	Li-Ion 2 A·h (up to 15 hours of autonomous operation inactive Ethernet connection)
Tamper protection	Yes
Frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz depending region of sale
Effective radiated power	8.20 dBm / 6.60 mW (limit 25 mW)
Modulation of the radiosignal	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 x 163 x 36 mm
Weight	350 g
Certification	Security Grade 2, Environmental Class I SP2 (GSM-S (LAN) DP3 in conformity with the requirements of E and EN 50136

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!

The full text of the warranty

User Agreement

Technical support: support@ajax.systems