

Hub BP Jeweller user manual



Hub BP Jeweller is a wireless control panel powered by an external battery. It supports photo verification. The hub is connected to the Ajax Cloud server via two SIM cards (2G/3G/LTE) and has external antenna connectors for cellular, Jeweller, and Wings communication channels.

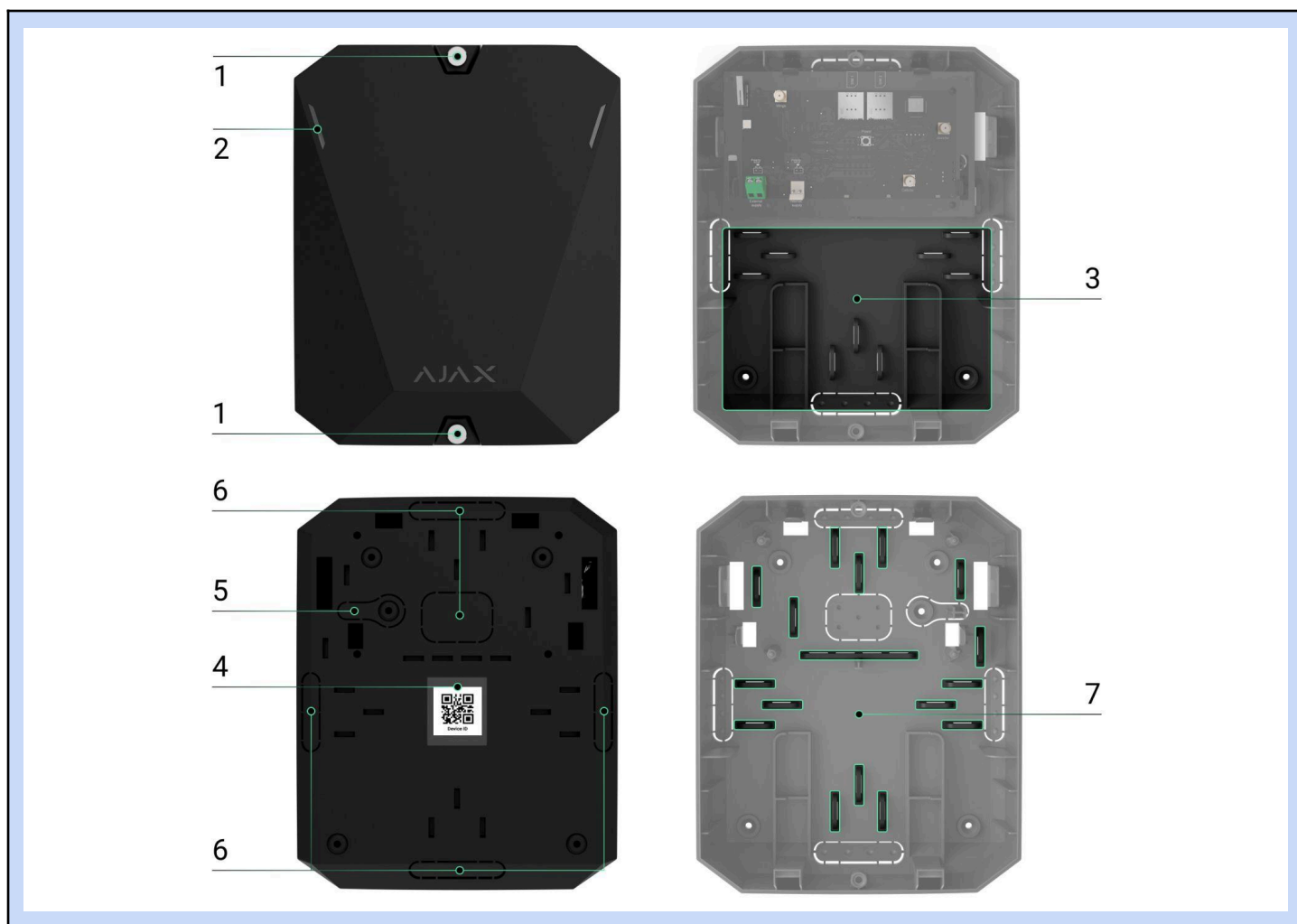
To be connected to the Ajax Cloud server, Hub BP Jeweller requires internet access. Two SIM cards are used as available communication channels.

👉 [Buy Hub BP Jeweller](#)

👉 [Buy External Antenna](#)

Functional elements

Casing elements

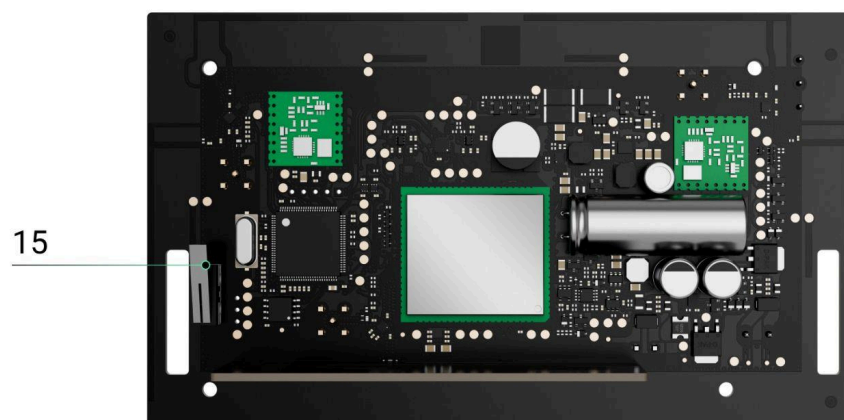
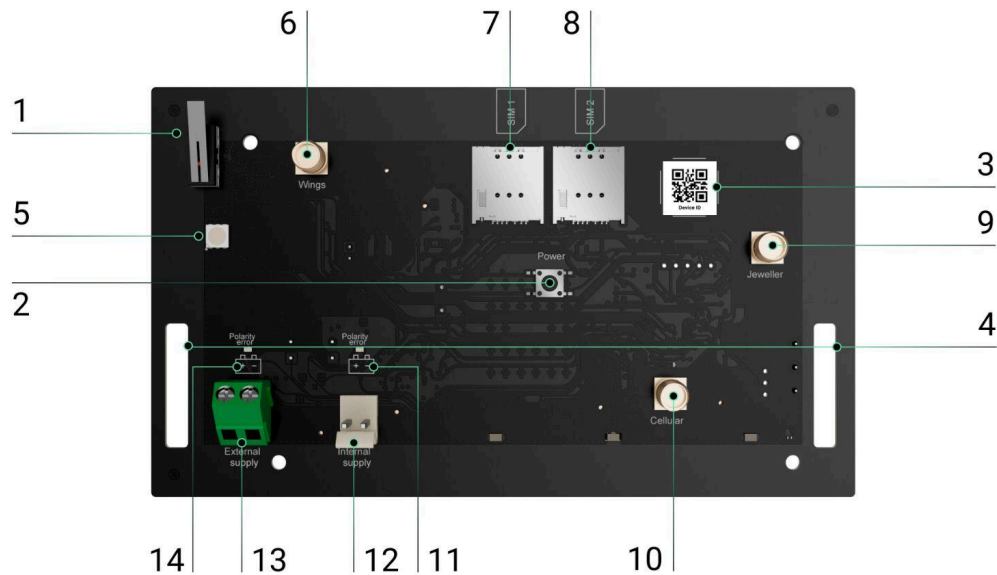


1. Screws that secure the casing lid. To unscrew them, use a bundled hexagon key (Ø 4 mm).
2. Light guides for the hub state indication.
3. Part with holders for a internal battery.

An internal battery is not included.

4. QR code and ID (serial number) of the control panel.
5. Perforated part of the casing. It is necessary for the tamper to trigger in case of any attempt to detach the device from the surface. Do not break it off.
6. Perforated parts of the casing for leading out the power wires and antenna cables.
7. Cable fasteners.

Board elements



1. First tamper button.
2. Power button.
3. QR code. Use it to add the hub to the space in an Ajax app.
4. Fixing points to attach the Hub BP Jeweller board into the casing.
5. LED indicator.
6. External antenna connector for Wings communication channel (SMA female connector).
7. Slot 1 for micro SIM.
8. Slot 2 for micro SIM.
9. External antenna connector for Jeweller communication channel (SMA female connector).
10. External antenna connector for cellular communication channel (SMA female connector).
11. Polarity error indicator for an internal battery.
12. Internal battery connector.
13. External power source terminal connector.
14. Polarity error indicator for an external power source.
15. Second tamper button.

Operating principle

Hub BP Jeweller is a control panel of an Ajax system. It controls the operation of connected devices.

You can connect up to 100 wireless Ajax devices to Hub BP Jeweller. Connected devices protect against intrusion, fire, and flooding and also allow you to control electrical appliances according to scenarios or manually – in a mobile app or by pressing the panic button, [LightSwitch](#), or [keypad with a touch screen](#).

To monitor the operation of all security system devices, the hub communicates with the connected devices using two [encrypted protocols](#):

1. **Jeweller** is a radio protocol for transmitting events and alarms from Ajax wireless devices. The communication range is up to 2,000 m without obstacles, such as walls, doors, or inter-floor constructions.
2. **Wings** is a radio protocol for transmitting photos from MotionCam and MotionCam Outdoor detectors. The communication range is up to 2,000 m without obstacles, such as walls, doors, or inter-floor constructions.

👉 [Learn more about Jeweller and Wings](#)

If a detector is triggered, the system raises an alarm in less than a second. In case of an alarm, the hub activates the sirens, starts the scenarios, and notifies the security company's monitoring station and all users.

Sabotage protection

Hub BP Jeweller has two SIM card slots for connecting to the Ajax Cloud server. This allows you to connect the device to two different mobile network operators at the same time. If one of them is unavailable, the hub automatically switches to another one and informs the security company's monitoring station and system users.

When a jamming attempt is detected, the system switches to an idle radio frequency and sends notifications to the security company's monitoring station and system users.

👉 [What is security system jamming](#)

The hub regularly checks the quality of communication with all connected devices. If any device loses connection with the control panel, upon expiry of the time specified by the administrator, all system users (depending on the settings), as well as the security company's monitoring station, will receive a notification about the incident.

👉 [Learn more](#)

No one can turn off the hub unnoticed, even when the facility is disarmed. If an intruder tries to open the hub casing, the tamper button will trigger immediately. The alarm notification will be sent to the security company and system users.

👉 [What is a tamper](#)

The hub rechecks the Ajax Cloud connection at regular intervals. The ping period is specified in the hub settings. If a minimum ping period is set, the server may notify the users and the security company in as little as 60 seconds after the connection is lost.

👉 [Learn more](#)

OS Malevich

Hub BP Jeweller is run by the real-time operating system OS Malevich. It is protected from viruses and cyber-attacks.

OS Malevich brings new features and functionality to the Ajax security system through over-the-air updates. The update does not require the involvement of an installation engineer or user.

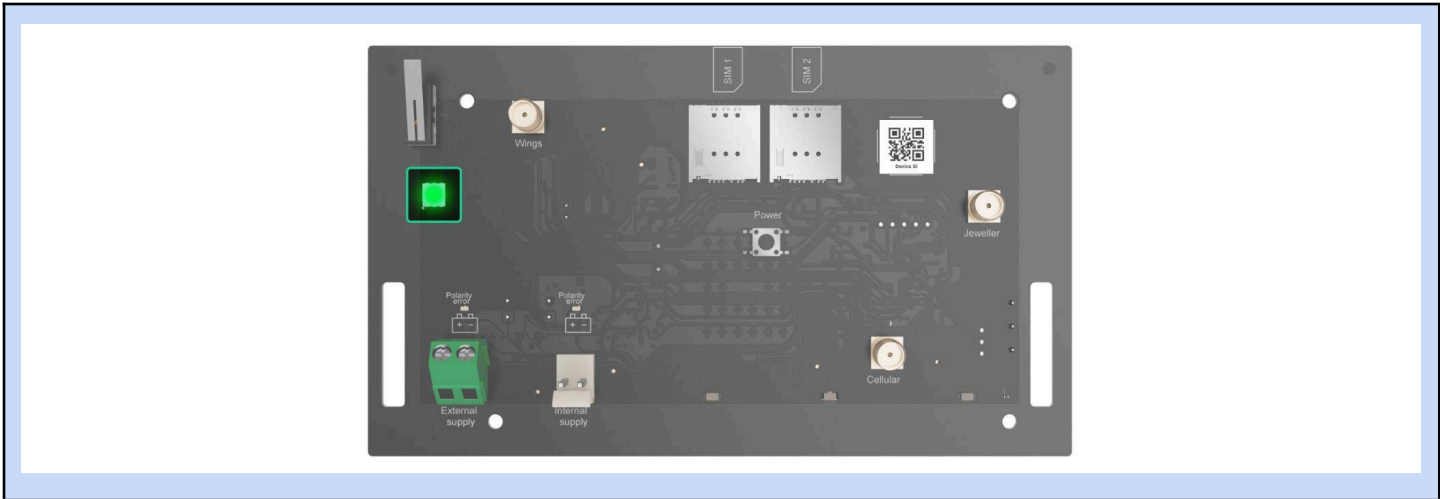
The update takes up to 2 minutes with the security system disarmed and the internal or external power source connected.

👉 [How OS Malevich updates](#)

Indication

Hub has two LED indication modes:

- **Hub – server connection.**
- **British disco.**



Hub – server connection

Hub – server connection mode is enabled by default. The hub LED has a list of indications showing the system state or events occurring. Hub BP Jeweller can light up red, white, purple, yellow, blue, or green, depending on the state.

Users can also monitor the Hub BP Jeweller states in Ajax apps.

Indication	Event	Note
------------	-------	------

Lights up green.	The communication channel is connected: via one or two SIM cards.  Learn more	When operating on an internal battery only, the indicator will blink every 10 seconds.
Lights up red.	The hub is not connected to the internet or the Ajax Cloud server.	When operating on an internal battery only, the indicator will blink every 10 seconds.

If you see an indication while using the system that is not listed in this user manual, please contact the [Ajax support service](#).

British disco

The function can be enabled in the hub settings in the PRO app (Hub → Settings → Service → LED indication).

Indication	Event	Note
Hub state changes		
White LED flashes once per second.	Two-Stage Arming or Delay When Leaving .	One of the devices is performing Two-Stage Arming or Delay When Leaving .
Green LED flashes once per second.	Entry indication.	One of the devices is performing Delay When Entering .
White LED lights up for 2 seconds.	Arming is completed.	The hub (or one of the groups) is changing its state from Disarmed to Armed.
Green LED lights up for 2 seconds.	Disarming is completed.	The hub (or one of the groups) is changing its state from Armed to Disarmed.
Alerts and malfunctions		
Red and purple LED flashes in sequence for 5 seconds.	Confirmed hold-up alarm.	There is an unrestored state after a confirmed hold-up alarm. The indication is displayed only if Restoration after confirmed hold-up alarm is enabled in the settings.

Red LED lights up for 5 seconds.	Hold-up alarm.	There is an unrestored state after a hold-up alarm. The indication is not displayed if there is a confirmed hold-up alarm state. The indication is displayed only if Restoration after hold-up alarm is enabled in the settings.
Red LED flashes.	The number of flashes equals the Device No. of a hold-up device (DoubleButton), the first to generate the hold-up alarm.	There is an unrestored state after the confirmed or unconfirmed hold-up alarm: • Single hold-up alarm or • Confirmed hold-up alarm
Yellow and purple LED flashes sequentially for 5 seconds.	Confirmed intrusion alarm.	There is an unrestored state after the confirmed intrusion alarm. The indication is displayed only if Restoration after confirmed intrusion alarm is enabled in the settings.
Yellow LED lights up for 5 seconds.	Intrusion alarm.	There is an unrestored state after the intrusion alarm. The indication is not displayed if there is a confirmed intrusion alarm condition. The indication is displayed only if Restoration after intrusion alarm is enabled in the settings.
Yellow LED flashes.	The number of flashes equals the Device No. that first generated the intrusion alarm.	There is an unrestored state after the confirmed or unconfirmed intrusion alarm: • Single intrusion alarm or • Confirmed intrusion alarm

Red and blue LED flashes in sequence for 5 seconds.	Lid opening.	There is an unrestored tamper state or an open lid on any of the devices, or the hub. The indication is displayed only if Restoration after Lid opening is turned on in the settings
Yellow and blue LED flashes in sequence for 5 seconds.	Other malfunctions.	There is an unrestored fault state or a malfunction of any device or the hub. The indication is displayed only if Restoration after faults is enabled in the settings. Currently, Restoration after faults is not available in Ajax apps.
Dark blue LED lights up for 5 seconds.	Temporary deactivation.	One of the devices is temporarily deactivated or the lid state notifications are disabled.
Blue LED lights up for 5 seconds.	Automatic deactivation.	One of the devices is automatically deactivated by an opening timer or the number of detections.
Green and blue LED flashes in sequence.	Alarm timer expiration. Learn more about the Alarm confirmation feature	Displayed after the alarm timer expires (to confirm the alarm).

When nothing is happening in the system (no alarm, malfunction, lid opening, etc.), the LED lights up green.

Access to indications

Hub BP Jeweller users can see the **British disco** indication after they:

- Arm/disarm the system using the Ajax keypad.
- Enter the correct user ID or personal code on the keypad and perform an action that has already been performed (for example, the system is disarmed, and the disarm button is pressed on the keypad).
- Press the SpaceControl button to arm/disarm the system or activate **Night Mode**.
- Arm/disarm the system using Ajax apps.

All users can see the **Hub state changes** indication.

Alert indication

If the system is disarmed and any of the indications from the table are present, the yellow LED flashes once per second.

If there are several states in the system, the indications are displayed one by one, in the same sequence as shown in the table.

Ajax account

To configure the system, install the [Ajax app](#) and create an account. Installers and security and monitoring companies use Ajax PRO accounts to configure the system for users.

👉 [How to create the Ajax account](#)

👉 [How to create the Ajax PRO account](#)

There is no need to create a new account for each hub, as one account can manage multiple systems. Separate access rights can be configured for each hub if needed.

Both user and system settings, as well as parameters of connected devices are stored in the hub. Changing the hub admin, adding or removing users does not reset the settings of devices added to the hub.

Connecting the hub to Ajax Cloud

To be connected to the Ajax Cloud server, Hub BP Jeweller requires internet access. The connection is needed for the operation of Ajax apps, remote setup and management of the system, and sending push notifications to users.

Hub BP Jeweller is connected to the internet via a cellular network. To increase the system's reliability and availability, populate both SIM card slots.

To connect to the cellular network, you need to install a micro SIM card with a PIN code request disabled and a sufficient amount of funds on the account to pay for services as per the operator's tariff. To disable the PIN code request, insert the SIM card into the phone.

As the hub connects to the internet only via the cellular network, it automatically sets the APN settings based on the installed SIM card to establish the internet connection. This feature is controlled by the **APN auto select** setting and is enabled by default for both SIM cards.

To connect the hub to Ajax Cloud:

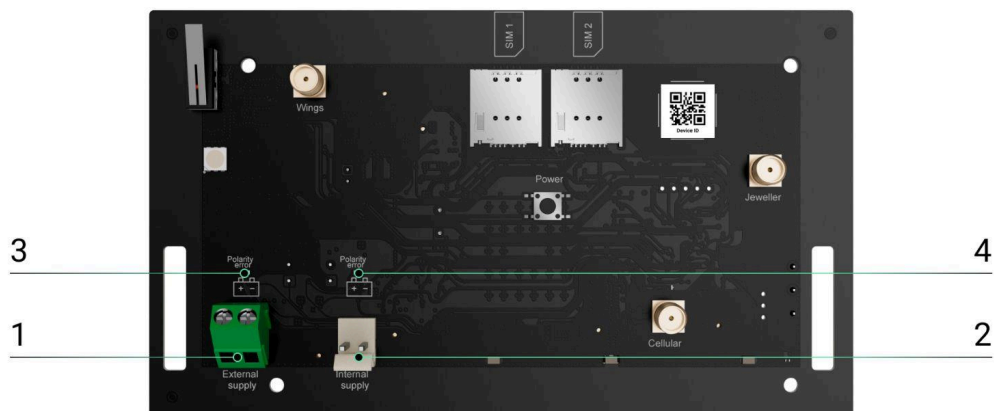
1. Unscrew the screws that secure the casing if installed. To do this, use a Ø 4 mm hexagon key included in the hub complete set.



2. Remove the lid of the hub casing.



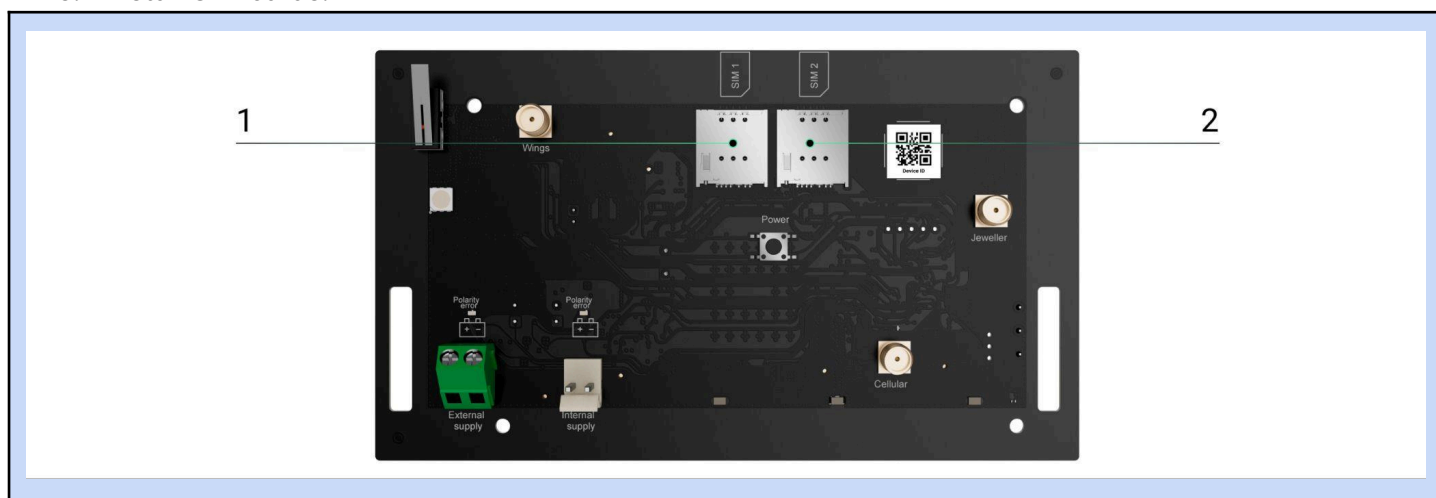
3. Install the Hub BP Jeweller board into the casing.
4. Connect the power supply to the appropriate connectors:



- 1 – External power source terminal connector.
- 2 – Internal battery connector. Connect a 12 V_{DC} battery.
- 3 – **Polarity error** indicator for a external power source.
- 4 – **Polarity error** indicator for a internal battery.

Indicators 3 and 4 light up in case of polarity reversal when connecting the power supply (when the power supply “-” is connected to the terminal “+” and vice versa).

5. Install SIM cards:



- 1 – Slot 1 for micro SIM.
- 2 – Slot 2 for micro SIM.

6. Hold down the hub's power button. As soon as the hub is on, the LED on the hub board will light up.
7. Wait until the control panel is connected to the internet. The green LED indicates that the hub is ready for operation.

After the hub is connected to the internet and added to the Ajax app, if necessary, you can manually configure the network parameters for another SIM card. In the SIM card settings, deactivate the **APN auto select** setting and configure roaming, APN, user name, and password. To find out these parameters, contact the support service of your mobile operator.

Do not deactivate the **APN auto select** setting or manually configure the network parameters for the current SIM card that provides an internet connection, as doing so may cause the connection to be lost, and the hub will go offline.

👉 [How to set or change the hub APN settings](#)

Adding a hub to the Ajax app

Use the latest [Ajax apps](#) and [OS Malevich](#) versions to access all available features and ensure proper system operation.

Granting access to all system functions (to display notifications in particular) is a mandatory condition for managing the Ajax system via the smartphone/tablet.

1. Open the Ajax app and log in to your account.
2. Select a space or create a new one.

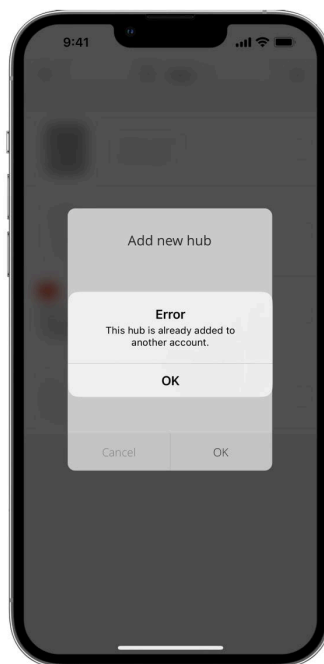
👉 [What is a space](#)

👉 [How to create a space](#)

3. Open the **Add Hub** menu and select how to add a new hub: manually or using a step-by-step tutorial.
4. At the registration stage, type the hub name and scan the QR code on the casing's back (or enter the ID manually).
5. Wait until the hub is registered and displayed in the app.

If there are already users on the hub, the hub admin, PRO with the rights to configure the system, or the installation company maintaining the selected hub can add your account. You will be notified that the hub has already been added to another account. Contact our [Technical Support](#) to determine who has admin rights on the hub.

👉 [User account types and rights](#)

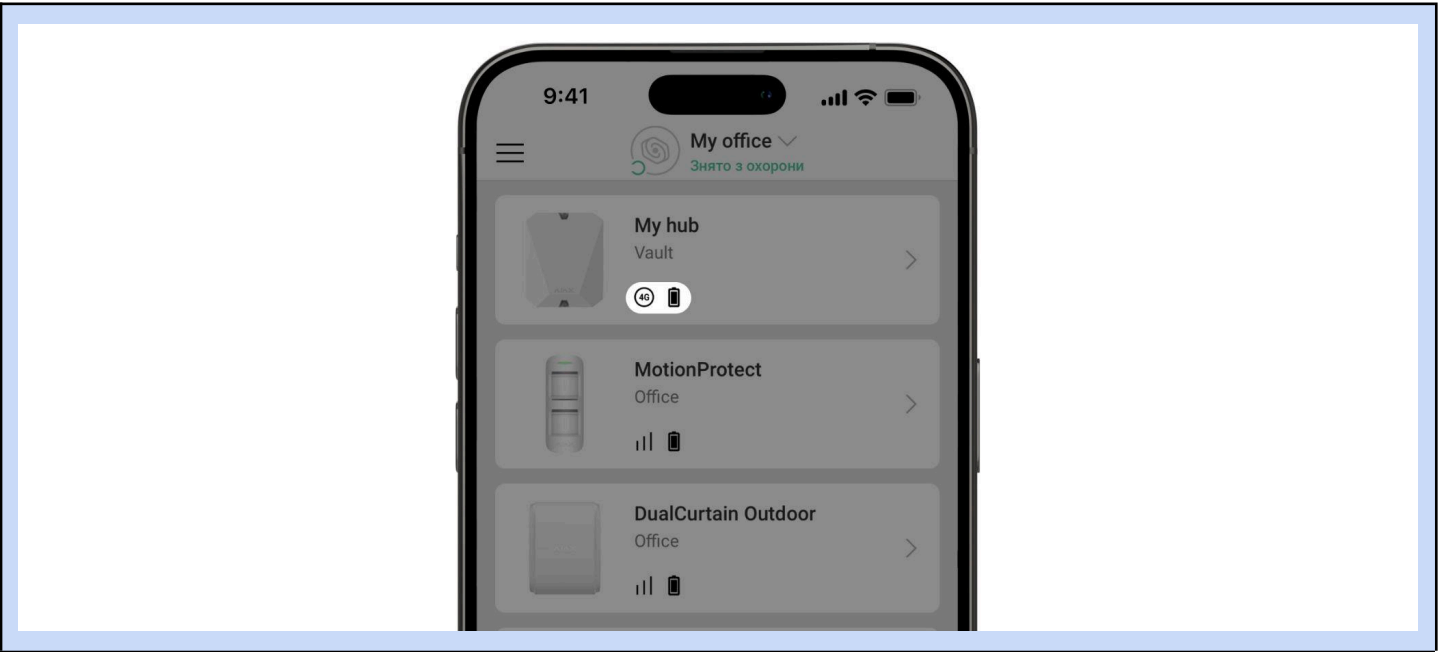


Malfunctions

The hub may notify about malfunctions. Tapping on ⓘ opens the list of all malfunctions. The **Malfunctions** field is available in device **States** and is displayed only if a malfunction is detected, e.g.:

- **Battery isn't found.**
- **Battery doesn't charge.**
- **Flash memory error.**

Icons

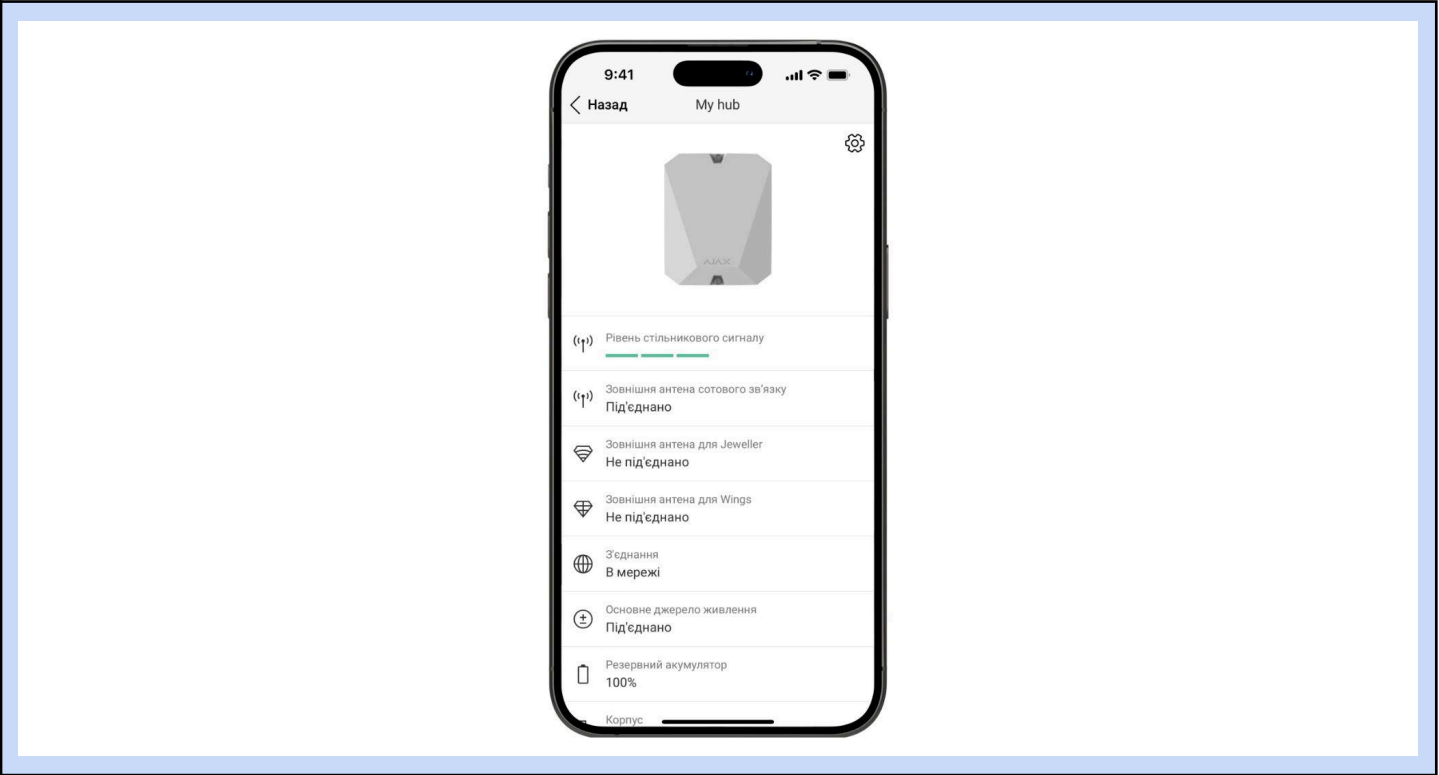


Icons display some of the Hub BP Jeweller statuses. You can view them in the Ajax app, in the **Devices** tab.

Icon	Meaning
2G	The hub operates in the 2G network.
3G	The hub operates in the 3G network.
4G	The hub operates in the 4G (LTE) network.
	The SIM card is faulty or has a PIN code set up. Check SIM card operation in the phone and disable the PIN code request.
	The hub battery charge level. Displayed in 5% increments.
	An internal battery is not connected.

	The external power source voltage is lower than permissible.
	The hub is directly connected to the monitoring station of the security company. The icon is not displayed if direct connection is not available or not configured. Learn more
	The hub is not directly connected to the central monitoring station of the security company. The icon is not displayed if direct connection is not available or not configured. Learn more

States



States can be found in the [Ajax app](#):

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

Parameter	Meaning
Malfunction	Tap the [icon] button to open the list of the hub malfunctions. The field appears only if a malfunction is detected.
Cellular signal strength	The signal strength of the active SIM mobile network.

	Install the hub in places where the cellular communication level reaches 2-3 bars. If the hub is installed in a place with weak or unstable signal strength, it will not be able to call or send an SMS about an event or alarm. Consider using ExternalAntenna.
External antenna for cellular	External antenna connection status: • Connected – the antenna is connected to a cellular port. • Not connected – the antenna is not connected to a cellular port. • Damaged – the antenna is broken. External antenna breakage detection is possible only when the hub casing is closed properly.
External antenna for Jeweller	External antenna connection status: • Connected – the antenna is connected to a Jeweller port. • Not connected – the antenna is not connected to a Jeweller port. • Damaged – the antenna is broken. External antenna breakage detection is possible only when the hub casing is closed properly.
External antenna for Wings	External antenna connection status: • Connected – the antenna is connected to a Wings port. • Not connected – the antenna is not connected to a Wings port. • Damaged – the antenna is broken. External antenna breakage detection is possible only when the hub casing is closed properly.
Connection	The status of connection between the hub and Ajax Cloud: • Online – the hub is connected to Ajax Cloud.

	• Offline – the hub is not connected to Ajax Cloud. Check the hub internet connection. If the hub is not connected to the server, the icons of the hub and all connected devices become semi-transparent in the list of devices.
External power source	External power source connection status: • Connected – the hub is connected to an external power source. • Disconnected – there is no external power source. Check the connection of Hub BP Jeweller to an external power source. If the voltage is not sufficient, the hub will report Low Voltage.
Internal battery	At a charge level of 20% and below, the hub will report a low battery charge. If the battery is not connected to the hub, the status Battery not installed is displayed. Learn more
Lid	The status of tamperers that respond to dismantling or opening of the hub casing: • Closed – the hub lid is closed. The normal state of the hub casing. • Open – the hub casing is open, or the casing's integrity is otherwise compromised. Check the state of the hub casing. The hub detects casing lid opening if either or both tamper buttons are triggered. If the casing lid is open, detection of the external antenna breakage is impossible. Learn more
Cellular data	Mobile internet connection status of the hub: • Connected – the hub is connected to Ajax Cloud via mobile internet. • Not connected – the hub is not connected to Ajax Cloud via mobile internet. Check the Hub BP Jeweller connection to the internet via the mobile network. If the cellular signal strength reaches 1–3 bars, and the hub has enough funds and/or has bonus

	SMS/calls, it will be able to call and send SMS, even if this field displays the Not connected status.
Active	Displays active SIM card: • SIM card 1 – the hub works with a SIM card installed in the first slot. • SIM card 2 – the hub works with a SIM card installed in the second slot.
SIM 1	The number of the SIM card installed in the first slot. To copy the number, tap on it. If the phone number is displayed as an Unknown number, the operator has not written it to the memory of the SIM card.
SIM 2	The number of the SIM card installed in the second slot. To copy the number, tap on it. If the phone number is displayed as an Unknown number, the operator has not written it to the memory of the SIM card.
Average noise (dBm)	Average noise in the radio channel. Measured in the place where the hub is installed. The first two values show the level at Jeweller frequencies, and the third – at Wings frequencies. The acceptable value is –80 dBm or lower. For example, –95 dBm is considered acceptable, and –70 dBm is invalid. What is security system jamming
Monitoring station	The status of direct connection of the hub to the central monitoring station of the security company: • Connected – the hub is directly connected to the security company's central monitoring station. • Not connected – the hub is not directly connected to the security company's central monitoring station. If this field is displayed, the security company uses direct connection to receive events and security system alarms. Learn more

Scheduled wake-up	Available with OS Malevich 2.30 and later versions. The status of the scheduled wake-up feature. The feature allows setting the date and time when the hub wakes up on demand from the battery saving mode and becomes active for configuration and management. The available states are: • Not set — the scheduled wake-up is not set. • Date, time — the next wake-up on demand is scheduled for the specified date and time. Tap  to open the feature settings. Settings are available only in Ajax PRO apps.
Hub model	Hub model name. Differences between Ajax hubs
Hardware version	Hub BP Jeweller hardware version. Not updated.
Firmware	Hub BP Jeweller firmware version. Updates remotely. Learn more
Device ID	Identifier (first 8 digits of the serial number) of the hub. The identifier is located on the device box and on the board under the QR code.
IMEI	A unique 15-digit serial number for identifying the hub's modem on a GSM network. It is shown only when a SIM card is installed in the hub.

Selecting the installation site

Fix the Hub BP Jeweller casing on a vertical surface using bundled fasteners. All the necessary holes for fastening have already been made in the casing.

It is necessary to fix the hub vertically so that the tamper responds if someone tries to detach a device. Learn the battery documentation before installing because some batteries can be mounted only vertically (with terminals upward). Another installation position could cause fast battery degradation.

It is advisable to choose an installation site where the hub is hidden from prying eyes, for example, in a pantry. This will help reduce the likelihood of sabotage or security system jamming. Note that the device is intended for indoor installation only.

Select a location where the hub can be connected via two SIM cards. The cellular signal strength at the installation site should be stable and reach 2-3 bars. In places with poor signal reception, it is recommended to install an external antenna. We do not guarantee the correct operation of the unit with a low cellular signal strength.

When choosing a location, take into account the distance between the hub and wireless devices and the presence of obstacles between them that may interfere with the passage of the radio signal. Such obstacles may include walls, raised floors, or large objects in the room. Use an external antenna if necessary.

To roughly calculate the signal strength at the site where wireless devices are installed, use our [radio communication range calculator](#).

Run the Jeweller and Wings signal strength tests. The stable signal strength of 2–3 bars with all connected devices should be provided at the chosen installation site. With a signal strength of 1 or 0 bars, we do not guarantee stable operation of the security system.

If the system has devices with signal strength of 1 or 0 bars, consider using ExternalAntenna or relocating the hub or device. If this is not possible or the device still has low or unstable signal strength after being moved, use [range extenders](#).

Professional installation instruction

Please be advised that due to the unique function supplied by this product, the device is intended for use with our digital application and licensed third-party only. The product will be distributed through controlled distribution channel and installed by trained professional and will not be sold directly to the general public through retail store.

1. Installation personal

This product is designed for specific application and needs to be installed by a qualified personal who has RF and related rule knowledge. The general user shall not attempt to install or change the setting.

2. Installation location

The product shall be installed at a location where the radiating antenna can be kept 20 cm from nearby person in normal operation condition to meet regulatory RF exposure requirement.

3. External antenna

Use only the antennas which have been approved by the applicant. The non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of FCC/IC limit and is prohibited.

4. Installation procedure

Please refer to user's manual for the detail.

5. Warning

Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in relevant rules. The violation of the rule could lead to serious federal penalty.

Detachable antenna usage

This radio transmitter (IC: HUBPNA1AFA, FCC ID: 2AX5VHUBPNA1AFA; 2AX5VHUBPNA1AUX) has been approved by FCC/ISED to operate with the antenna type listed below with maximum permissible gain indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Approved antenna(s) list

Antenna type	Antenna Model Name	Brand	Manufacturer	Antenna gain (dBi)					
				Frequency (MHz)					
				905-926.5	700	1710	1990	2170	2650
PCB	External antenna	AJAX	AJAX	-2	-3	-0	-0.5	-1	-0

Installation of the control panel

During installation and operation of the Ajax security system, adhere to the rules and requirements of regulatory legal acts on electrical safety. Do not disassemble the device while it is energized or use it with a damaged power cable.

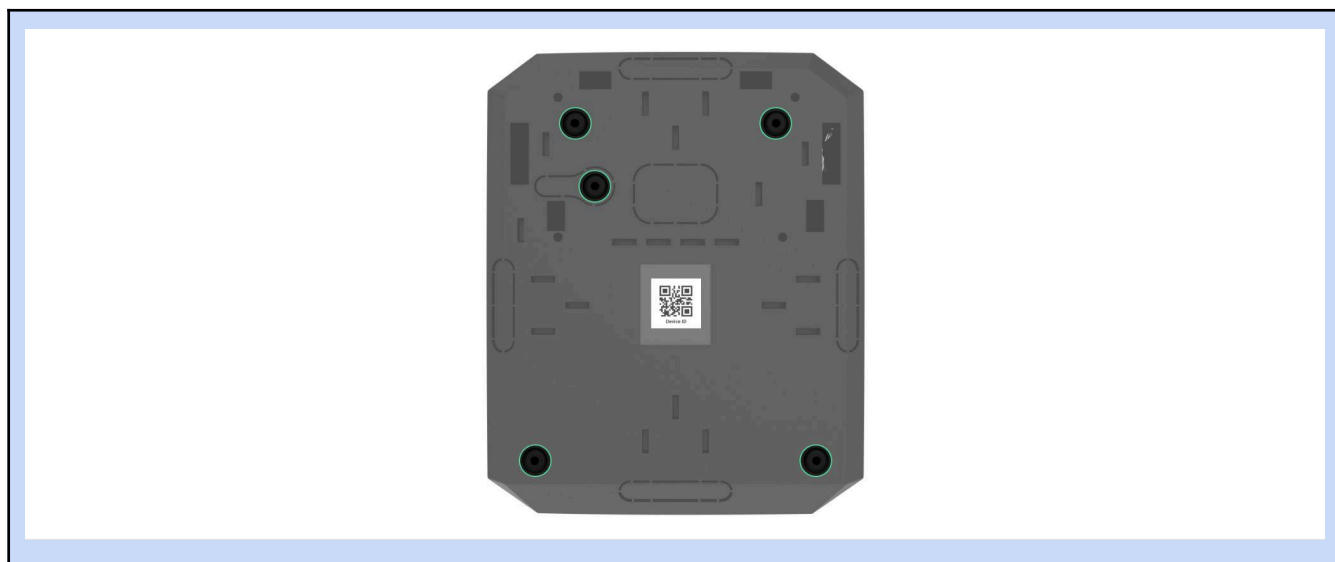
Before installation, make sure that you have selected the optimal location for the device and that it complies with the requirements of this manual.

To install Hub BP Jeweller:

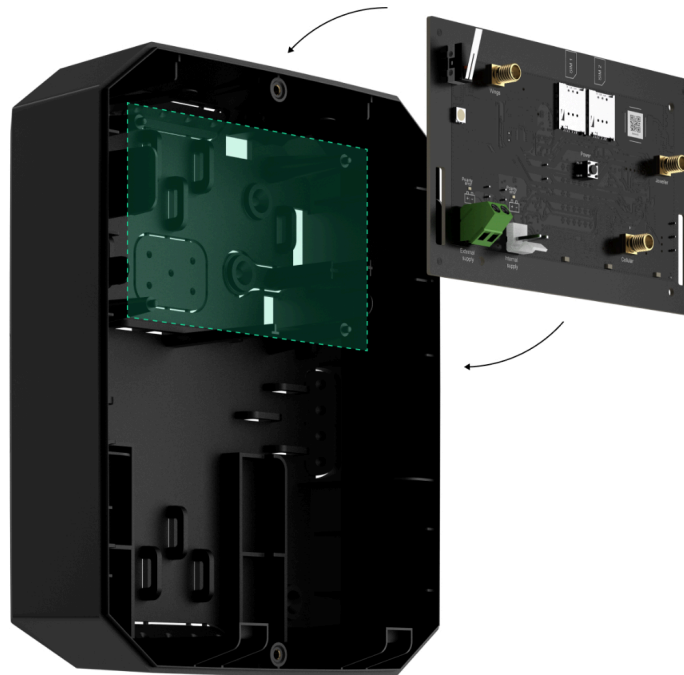
1. Prepare the cable outputs in advance by carefully breaking out the perforated parts of the Hub BP Jeweller casing.



2. Secure the casing on the vertical surface at the selected installation location with the bundled screws using all fixation points. One of them is in the perforated part above the tamper – it is required for tamper triggering in case of any attempt to detach the hub casing.



3. Place the Hub BP Jeweller board into the casing on the holders.



4. Connect a 6–12 V $\equiv$ external power source.
5. Connect a 12 V $\equiv$ internal battery. Do not connect third-party power sources, as this may cause the hub to fail.

Use a 12 V $\equiv$ battery. The maximum dimensions of the battery to be installed in the casing are 151 × 65 × 94 mm, and the battery weight is 5 kg. For such battery configuration, special holders are provided in the hub casing.

6. If necessary, connect ExternalAntenna to the appropriate communication port.

Before installation, make sure you read [the antenna user manual](#).

7. Turn on the hub.
8. Install the lid on the hub casing and fix it with the bundled screws.
9. Check the status of the hub casing in the [Ajax app](#). If the app shows a tamper alarm, check the tightness of the hub's casing.

Do not install the hub

1. Outdoors. This could result in a failure of the control panel.
2. Near the metal objects and mirrors. They can cause attenuation or shielding of the radio signal. This could result in the loss of connection between the hub and wireless Ajax devices. If it is necessary to install in such condition, use ExternalAntenna to overcome obstacles of the signal.
3. In places with high levels of radio interference. This could result in the loss of connection between the hub and wireless Ajax devices or false notifications about [security system jamming](#). If necessary, use ExternalAntenna to move the reception spot.
4. Less than 1 meter away from the router and power cables. This could result in the loss of connection between the hub and wireless devices.
5. Less than 1 meter away from Jeweller devices. This could result in the loss of connection between the hub and these devices.
6. In places where the hub will have a signal strength of 1 or 0 bars with connected devices. This could

result in the loss of connection between the hub and these devices. Use ExternalAntenna if necessary.

7. Inside premises with temperature and humidity beyond the permissible limits. This could result in a failure of the control panel.
8. In places with no cellular signal or 1 bar signal strength. We do not guarantee correct operation of the device with a low cellular signal strength. Use ExternalAntenna if necessary.

Hub settings

Settings can be changed in the [Ajax app](#):

1. Select the space if you have several of them or if you are using a PRO app.
2. Go to the **Devices** tab.
3. Select **Hub BP Jeweller** from the list.
4. Go to **Settings** by tapping on the gear icon [gear icon] in the upper right corner.
5. Set the required parameters.
6. Tap on **Back** to save the new settings.

Name

The hub name is displayed in the SMS and push notification text. The name can contain up to 12 Cyrillic characters or 24 Latin characters.

Room

Selection of the hub virtual room. The room name is displayed in the SMS and push notification text.

Cellular

Configuring connections and checking accounts.

Modem settings

- **Cellular data** – can't be disabled.
- **Roaming** – if it is enabled, a SIM card installed in the hub can work while roaming.
- **Ignore network registration error** – when this setting is enabled, the hub ignores errors when trying to connect via a SIM card. Enable this option if a SIM card cannot connect to the network.
- **Disable communication check with the operator** – when this setting is enabled, the hub ignores operator communication errors. Enable this option if a SIM card cannot connect to the network.

SIM cards

- **SIM 1** and **SIM 2** – displays the number of installed SIM cards. Tap on the field to go to the SIM card settings.

SIM card settings

- **APN, Username, and Password** – settings for connecting to the internet via a SIM card. To find out your cellular operator's settings, contact your provider's support service.

- **APN auto select** — if this option is enabled, the access point is set automatically based on the installed SIM card.

 [Learn more](#)

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.

Remember that data is calculated by the hub and may differ from your operator's statistics.

Reset statistics — resets statistics on incoming and outgoing traffic.

Check balance

Enter the balance check **USSD code** (provided by your operator) and tap **Check balance**.

 [Learn more](#)

Communication method

It is possible to select the preferred antenna to use for transmitting cellular data:

- **Auto-switching between antennas** — the hub will prioritize the external antenna if it is available (connected and not damaged).
- **External** — the hub does not switch to an internal antenna and tries to work with an external one.
- **Built-in** — the hub uses an internal antenna.

This setting is only available in [Ajax PRO apps](#).

Keypad access codes

Setting up keypad passwords for people who are not registered in the system.

This is convenient, for example, to provide a cleaning company with access to security management. Knowing the access code, you just need to enter it on the [Ajax keypad](#) to arm or disarm the system.

To set up an access code for an unregistered person in the system:

1. Press **Add code**.
2. Set up **Username** and **Access Code**.
3. Press **Add**.

If you want to set up a duress code, change an access code, settings for access to groups, Night mode, code ID, temporarily disable or delete this code, select it in the list, and make changes.

The created access codes are valid for all keypads connected to the hub. **Hub BP Jeweller** supports up to 50 access codes.

👉 [How to manage security with access codes on KeyPad Jeweller](#)

Security schedule

Settings for scheduled arming/disarming of the system.

Video about the security schedule - <https://youtu.be/DZ4WhEqyiWA>

👉 [Learn more](#)

Detection zone test

Starts the detection zone test for connected detectors. This test determines whether the detectors operate correctly and defines the distance at which they detect alarms.

👉 [Learn more](#)

Jeweller

Configure the hub–detector ping interval. The settings determine how frequently the hub communicates with devices and how quickly the loss of connection is detected.

👉 [Learn more](#)

- **Detector ping interval, sec** — determines the frequency of connected devices polling by the hub. The shorter interval (in seconds) means faster delivery of the events between the hub and connected devices (36 seconds by default).
- **Number of missed pings to determine connection failure** — a counter of undelivered packets (8 packets by default).

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

$$\text{Detector ping interval} \times \text{Number of missed pings to determine connection failure}$$

It is important to keep in mind that the reduction in the polling interval reduces the bundled battery life.

Note that the ping interval reduces the maximum number of connected devices:

Detector Ping Interval	Connection limit
12 seconds	39 devices

24 seconds	79 devices
36 and more seconds	100 devices

Irrespective of the settings, you can connect up to 10 sirens or keypads with a built-in buzzer and 5 range extender to the hub.

Radio interference detection

- **Advanced radio interference detection**
- **Send radio interference detection event as alarm**

Communication method

It is possible to select the preferred antenna to use for Jeweller and Wings channels:

- **Auto-switching between antennas** — the hub will prioritize the external antenna if it is available (connected and not damaged).
- **External** — the hub does not switch to an internal antenna and tries to work with an external one.
- **Built-in** — the hub uses an internal antenna.

This setting is only available in [Ajax PRO apps](#).

Service

Group of hub service settings. These are divided into two groups: general settings and advanced settings.

General settings

LED brightness

Adjustment of the hub logo LED backlight brightness. Set in the range of 1 to 10. The default value is 10.

Firmware update

The menu contains the hub firmware update settings.

- **Firmware auto-update** configures automatic OS Malevich updates (enabled by default):
 - **If enabled**, the firmware is automatically updated when a new version is available. The system should be disarmed, and external power should be connected to the hub.
 - **If disabled**, the system does not update automatically. If a new firmware version is available, the app will offer to update the OS Malevich.
- **Check for new version** allows manually checking and installing firmware updates when available or assigned to the hub. This option is available only when the **Firmware auto-update** setting is enabled.

[How OS Malevich updates](#)

Hub system logging

Logs are files containing information about system operation. They can help sort out the problem in case of errors or failures.

The setting allows you to select the transmission channel for the hub logs or disable their recording:

- **Off**
- **Cellular**

Logging is turned off by default because it increases network data consumption and decreases battery life. In case of system errors, select the **Cellular** option to send logs via cellular networks.

[How to report a problem in the Ajax app on iOS](#)

[How to report a problem in the Ajax app on Android](#)

'While hub offline' events amount

Events during communication failure with the server are recorded in the hub buffer and will be delivered to Ajax apps after the connection is restored.

This setting allows you to choose the number of the last events, that hub will send to Ajax apps after returning online.

You can select between **100** (default value) and **1000** events with increment of **50** events.

[Learn more](#)

Advanced settings

The list of advanced hub settings depends on the type of application: standard or PRO.

Ajax Security System	Ajax PRO
Server connection Sounds and alerts Fire detectors settings System integrity check	PD 6662 setting wizard Server connection Sounds and alerts Battery settings Fire detectors settings System integrity check Alarm confirmation Restoration after alarm Arming/disarming process Devices auto deactivation

PD 6662 setting wizard

Opens a step-by-step guide on how to set up your system to comply with the PD 6662:2017 British security standard.

This setting is only available in [Ajax PRO apps](#).

 [Learn more](#)

Server connection

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

- **Delay 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.
- **Hub-server polling interval, sec.** Frequency of sending pings from the hub to the Ajax Cloud server. It is set in the range of 10 to 300 s. The recommended default value is 60 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:

$$(Ping\ interval \times 3) + Time\ filter$$

With the default settings, Ajax Cloud reports the hub loss in 8 minutes:

$$(60\ s \times 3) + 300\ s = 8\ min$$

- **Get notified of server connection loss without alarm.** Ajax apps can notify about the hub–server communication loss in two ways: with a standard push notification signal or with a siren sound (enabled by default). When the option is active, the notification comes with a standard push notification signal.
- **Notify of connection loss over channels.** A system can notify both the users and the security company about the loss of connection, even via one of the communication channels.

In this menu, you can choose the connection loss of which channels will be reported by the system, as well as the delay for sending such notifications:

- Cellular
- **Loss notification delay, min** — time of the delay before sending the notification about the 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

Sounds and alerts

The menu contains siren activation parameters.

Alert with siren

- **If lid of hub or any detector is open.** If enabled, the hub activates connected [sirens](#) in case the lid of the hub, detector, or any other Ajax device is open.
- **If in-app panic button is pressed.** If enabled, the hub activates connected sirens if the panic button is pressed in the Ajax app.
- **Restart alarm signal on triggering of each detector.**

Beep with keypad

- **If battery of any device is low.**
- **If any device is offline.**

This setting is only available in [Ajax PRO apps](#).

Battery settings

The menu contains settings for hub power sources.

- **Internal battery type.** This option allows you to select the proper battery type so that the hub can set the right voltage level for it.
 - **Ajax non-rechargeable lithium battery.**
 - **Rechargeable lead-acid battery.**
 - **Other battery type.** This option allows specifying custom voltage levels.
- **Internal battery low voltage level.** At this voltage level, the hub warns when the internal battery is low. This option is available if the **Other battery** type option is selected for the **Internal battery type**.
- **Internal battery cut-off voltage.** If the hub is powered by an internal battery, it will automatically shut down at this voltage. This option is available if the **Other battery** type option is selected for the **Internal battery type**.

If the hub is powered by an internal battery only, the Internal battery cut-off voltage cannot be set higher than the battery's current voltage level.

- **External battery low voltage level.** At this voltage level, the hub alerts you when the external power source discharges.
- **Internal battery.** Allows selecting whether the internal battery is charged from the external power source.
- **Internal battery charging speed.** Allows you to select the appropriate charging speed depending on the type of external power source. This option is available if the **Rechargeable lead-acid battery** option is selected for the **Internal battery type**.
- **Battery power saver.** Allows you to activate battery saving mode for the chosen power source.
 - **Saving mode when working from external battery.**
 - **Saving mode when working from internal battery.**

When either or both options are enabled, it is possible to set up:

- **Activity period.** It is the time during which the hub and added devices are activated for sending events to users and CMS.

- **Server polling interval.** It is the time during which the hub communicates with the server to confirm its availability.
- **Wake-up via SMS.** If enabled, the hub and its devices can be temporarily activated by sending an SMS with the password to the hub's SIM card number.
- **SMS password.** The password that should be included in the SMS sent to the hub's SIM card number to wake up the hub on demand. The password must be 6-24 letters, numbers, or special characters without spaces.

To wake up the hub via SMS, send an SMS to the hub's SIM card number with the hub ID (i.e., Device ID), SMS password, and "WFB" text.

Example of SMS text: *000ABC11 12345ab WFB*

- *000ABC11* – a hub ID (i.e., Device ID);
- *12345ab* – an SMS password;
- *WFB* – a required text in the SMS.

Battery settings are only available in [Ajax PRO apps](#).

The **Wake-up via SMS** feature is available with [OS Malevich 2.30](#) and later versions.

Fire detectors settings

Menu of the [Ajax fire detectors](#) settings. Allows configuring Interconnected Fire Detectors Alarm.

The feature is recommended by European fire standards, which require a warning signal power of at least 85 dB at 3 meters from the sound source in the event of a fire. Such sound power wakes up even a soundly sleeping person during a fire. Using the Ajax app, Button, or KeyPad, you can quickly disable triggered fire detectors.

👉 [Learn more](#)

System integrity check

This parameter is responsible for checking the state of security detectors, devices and [followed groups](#) before arming the system. **System integrity check** is disabled by default.

👉 [Learn more](#)

Alarm confirmation

This setting is only available in [Ajax PRO apps](#).

Alarm confirmation is a special event that the hub sends to the CMS and system users if several certain devices have triggered within a specified period of time. By responding to confirmed alarms only, the security and monitoring companies and the police reduce the number of visits to false alarms.

👉 [Learn more](#)

Restoration after alarm

This setting is only available in [Ajax PRO 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 a PRO user. The types of alarms that require system restoration 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

This setting is only available in [Ajax PRO apps](#).

The first **Compliance with Standard** option allows selecting a specific standard to set the security system according to existing requirements. Once you select the required standard, the menu will show the appropriate arming/disarming settings below. The following standards are available:

- **EN 50131** – European standard for intrusion and hold-up alarm systems, which also describes the security grades concept.
- **PD 6662** – British standard for intrusion and hold-up alarm systems, aimed to reduce the number of unconfirmed alarms and ensure police reaction only to real threats.
- **VdS** – German standard for intruder and hold-up alarm systems, which regulates arming/disarming process.
- **ANSI/SIA CP-01-2019** – American standard for security systems that regulates features and requirements to reduce false alarms caused by users or equipment.

EN 50131

Once **EN 50131** is activated, you can set the parameters of the functions **Two-stage arming**, **Exit time restart**, and **Exit error** in the arming settings, as well as set the **Alarm transmission delay** in the disarming settings.

👉 [How to configure an Ajax system according to the EN 50131 requirements](#)

PD 6662

Once **PD 6662** is selected, the menu shows the number of arming/disarming settings that allow configuring the system to comply with standard requirements.

👉 [Learn more about the PD 6662 standard](#)

Use the corresponding step-by-step guide in the Ajax PRO app for a quick and convenient system setup according to **PD 6662**. Go to Hub → Settings  → Service → **PD 6662 Setting Wizard** and follow the app prompts.

VdS

Once **VdS** is selected, all devices in the system operate without delay when leaving, but entry delays will still work.

The system automatically checks that all doors and locks are closed. The door is locked with the third-party **Blocking element** when arming the system. Additionally, the system checks whether the door is blocked to ensure that the system is armed according to the unavoidability principle (German: Zwangsläufigkeit).

The system can't be armed if it has malfunctions. If there are any malfunctions or the door is not locked, the system notifies of the unsuccessful arming event.

[Learn more](#)

ANSI/SIA CP-01-2019

An Ajax system controlled by the hub with [OS Malevich 2.19](#) or higher can be configured following the requirements of ANSI/SIA CP-01-2019.

Only [Hub 2 \(4G\) Jeweller](#) and [Hub 2 Plus Jeweller](#) are certified according to ANSI/SIA CP-01-2019.

Once **ANSI/SIA CP-01-2019** is selected, you can configure **Exit Time Restart** and **Unvacated Premises** for the arming settings. For the disarming settings, you can select what devices should make an annunciation on **Alarm Cancellation** or **Alarm Abort** and adjust the **Alarm Abort Window** timeout.

Also, this standard requires enabling a number of features for the system, such as **Delay When Entering/Leaving**, **cross zoning***, **Devices Auto Deactivation**, and **system testing**. These features are configured in the hub and certain device settings.

👉 [How to set up the ANSI/SIA CP-01-2019 compliant system](#)

* The **cross zoning** functionality will be available in the next OS Malevich updates.

Devices auto deactivation

This setting is only available in [Ajax PRO apps](#).

The Ajax system can ignore alarms or other events of devices without removing them from the system. Under certain settings, notifications about specific device events will not be sent to the CMS and system users.

👉 [Learn more](#)

It is also possible to manually disable a specific device. Learn more about deactivating devices manually [here](#).

LED indication

This setting is only available in [Ajax PRO apps](#).

In this menu, you can select the system states and events that the hub's LED indicators will display. One of two functions can be chosen:

- **Hub-server connection** — hub's LEDs display if a hub is connected to the power supply and the internet.
- **British disco** — hub's LEDs display information about system alerts and malfunctions, security mode changes, and delays when entering/leaving.

After-alarm indication

Select events that sirens or keypads with a built-in LED will indicate with regular double flashing until the system is disarmed.

- **Confirmed intrusion/hold-up alarm.**
- **Single intrusion/hold-up alarm.**
- **Lid opening.**

User guide

Opens the Hub BP Jeweller user manual in the Ajax app.

Transfer settings to another hub

Menu for transferring devices and settings from another hub. **Keep in mind that you are in the settings of the hub to which you want to import data.**

 [Learn more](#)

Remove hub

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

Space settings

Settings can be changed in the [Ajax app](#):

1. Select the space if you have several of them or if you are using a PRO app.
2. Go to the **Control** tab.
3. Go to **Settings** by tapping the gear icon [gear icon] in the bottom right corner.
4. Set the required parameters.
5. Tap **Back** to save the new settings.

 [How to configure a space](#)

Hub settings reset

Resetting the hub to the factory settings:

1. Turn on the hub if it is off.
2. Remove all users and installers from the hub.
3. Hold the power button for 30 seconds – the LED indicator on the hub board will start blinking red.
4. Remove the hub from your account.

Additional features

Video surveillance connection

Hub BP Jeweller is compatible with [Ajax cameras and NVRs](#) and with third-party cameras that support RTSP protocol or SDK integration.

 [How to connect cameras to the Ajax system](#)

Cameras and NVRs that can be connected to Hub BP Jeweller:

Devices	Quantity
Ajax cameras via Ajax NVRs	up to 224
Third-party cameras via Ajax NVRs using ONVIF	up to 224
Standalone Ajax cameras	up to 492
Standalone third-party cameras using RTSP or SDK	up to 10

Scenarios

Hub BP Jeweller allows creating 32 scenarios and minimizing the human factor impact on safety. The hub can manage the security of the entire facility or group according to a schedule; activate the smoke machine if intruders enter the room; de-energize the room and turn on emergency lighting in case of fire; shut off water in the event of a leak; control lighting devices, electric locks, roller shutters, and garage doors – when changing the security mode by pressing a button or by a detector alarm.

Scenarios can be used to reduce the number of routine actions and increase productivity. Ajax automation devices respond to changes in temperature and air quality. For example, configure the heating to turn on at low temperatures, control the supply system, humidifier, and air conditioner to maintain a comfortable climate.

 [How to create and customize a scenario](#)

Photo verification

Hub BP Jeweller supports both MotionCam and MotionCam Outdoor wireless motion detectors. When triggered, the detectors take a series of shots you can use to evaluate the unfolding of the events at the facility over time. This relieves users of unnecessary anxiety and prevents security companies from sending unnecessary patrol dispatches.

The detector activates the camera when armed and detects movement. Only users with access to the events feed and authorized employees of the security company can see visual alarm verifications, provided that the security system is connected to the monitoring station.

If the **Photo on Demand** feature is activated, the detectors can take a photo upon the command of a system user or PRO user with the appropriate rights. The taking of a photo is always registered in the hub's events feed.

The shots are protected by encryption at every stage of transmission. They are stored on the Ajax Cloud server and are not processed or analyzed.

[Learn more](#)

Maintenance

Check the functioning of Hub BP Jeweller and connected devices regularly. The optimal frequency of checks is once every three months. Clean the hub casing from dust, cobwebs, and other contaminants as they emerge. Use a soft, dry cloth suitable for equipment care.

Do not use substances containing alcohol, acetone, petrol, and other active solvents to clean the device.

Technical specifications

👉 [All technical specifications of Hub BP Jeweller](#)

👉 [Compliance with standards](#)

Complete set

1. Hub BP Jeweller.
2. Installation kit.
3. Quick start guide.

Recommended batteries

We recommend using zinc-air alkaline batteries for extended battery life. Before connecting this battery type, make sure to remove the stickers from it or open the air shutoff valves. If possible, leave the battery with access to the air for 2 hours. Air is needed to start a chemical reaction inside the battery and ensure its proper operation.

Before connecting the external battery, carefully read the manufacturer's instructions. They contain guidance on safe use and recommended parameters.

Zinc-air batteries are **not** rechargeable. Parameter **Charge rate** is specified for use cases when an

internal rechargeable battery is being charged by an external battery.

List of recommended external zinc-air batteries to power the Hub BP Jeweller

Manufacturer	Model	Voltage, V	Capacity, Ah	Charge rate	Months ¹ of operation in full function mode ²	Months ¹ of operation in Battery power saver mode ²
Cegasa	eZ8 12/600	12	600	slow	18	69
Cegasa	eZ8 9/600	9	600	slow	14	56
UPOWER	8PFP330	12	330	slow	12	49
Masterbattery	MC-ZA1200-7.5	7,5	1200	standard	19	42
Masterbattery	MC-KOMPACT700	12	600	standard	18	42
Masterbattery	MC-KOMPACT800-6V (0,6A)	6	800	slow	19	41
Masterbattery	MC-KOMPACT800-6V (1A)	6	800	standard	18	41
Masterbattery	MC-ZA800-12	12	800	slow	18	41
Cegasa	eZ8 9/400	9	360	slow	9	38
Masterbattery	MC-KOMPACT600	12	600	slow	14	37
Maxi	ZZ12-600	12	600	slow	15	37
Masterbattery	MC-ZA500-12	12	500	disable	13	35
Masterbattery	MC-ZA400-12	12	400	disable	11	32
Cegasa	E/Z8 7,5/400	7,5	330	disable	7	29
Safire	SF-BATT-75V-3200WH	7,5	430	disable	9	27
Masterbattery	MC-ZA300	6	300	disable	5	18

¹ At temperatures of 25 °C.

² Internal battery isn't charged.

Warranty

Warranty for the Limited Liability Company "Ajax Systems Manufacturing" products is valid for 2 years after the purchase.

If the device does not function correctly, please contact Ajax Technical Support first. In most cases, technical issues can be resolved remotely.

[Warranty obligations](#)

[User Agreement](#)

Contact Technical Support:

- [email](#)
- [Telegram](#)
- Phone: **0 (800) 331 911**

