

Tips for installing and configuring wired Fibra devices

Updated May 24, 2024



Fibra is a professional product line of Ajax wired devices. Only accredited partners who have passed **specialized training** can sell, install, and administer devices of this product line.

We have prepared this material to help professionals who work with the Ajax product line of wired devices or are just planning this. It includes answers to basic questions about wired devices, tips for installing and configuring them, and links to useful educational materials.



Superior, Fibra, and Baseline product lines are mutually compatible. This opens up numerous possibilities for building systems of any configuration.

This manual will be helpful for both design engineers and installers or commissioning engineers. It supplements user manuals for each device. Therefore, before reading it, we recommend that you learn the [user manuals for Fibra devices](#).

Project design

It is essential to properly design the security system project to ensure that system devices are installed and configured correctly. The project must take into account the number and types of devices at the object, their exact location and installation height, the length of Fibra lines, the type of cable used, and other parameters. In addition, an accurate project can help solve system issues in the future. For example, if one of the detectors fails, it will be easier to find and replace it with a similar one.

Before creating a project, it is necessary to consult the client. Find out their needs, concerns, how they use the object, and what they expect from the security system. For example, the client only needs protection from burglars, or they also need a flood prevention system.

Also, before designing a security system project, it is necessary to visit the object, inspect it, and consult the utility system projects. The actual object may differ from the plan, which is also important to consider. In addition, it will help to identify less obvious factors that may affect the security system realization. For example, how the sun's rays fall into the apartment or where the owners will install the air conditioner.

Object analysis

In the analysis stage, you need to work through every way an intruder can use to enter the protected area. Security devices must control all doors, windows, gates, fence doors, and other entrances and exits.



If the object has roof windows, you should pay attention to them as well. The intruder can get into the room through the roof.

It is also necessary to consider all possible sources of alarms at the object and their types. This will help to ensure the overall security of the object. For example, for early fire detection, install the wireless [Ajax fire detectors](#) in the kitchen and integrate [Button](#) and [DoubleButton](#) alarm into the store's cash registers.

Interior solutions are also taken into account in the analysis and project design. For example, a cabinet should not block the view of the detector, a lamp should not illuminate the photo camera of the detector supporting photo verification, and in a room with a fireplace or air conditioner, it is better to install a motion detector with an additional microwave sensor.



The minimum distance between motion detectors with additional microwave sensors ([MotionProtect Plus Jeweller](#), [MotionProtect S Plus Jeweller](#), and [MotionProtect Plus Fibra](#)) should be at least **20 centimeters**. Otherwise, it can decrease detection quality or trigger false alarms due to wave interference of K-band microwave sensors.

Be sure to check with the client if there will be animals at the object – this affects the settings of motion detectors, their location, and installation height.

Check if there are items of particular importance at the object – for example, expensive paintings, vases, or safes. Separate detectors can be used to protect such items. For example, install [DoorProtect Plus Fibra](#) inside the safe. It will activate the alarm if anyone tries to break into the safe.



Using hybrid hubs of Ajax systems, you can expand the system with wireless devices. For example, with smart sockets, relays, or detectors.

Selecting the devices

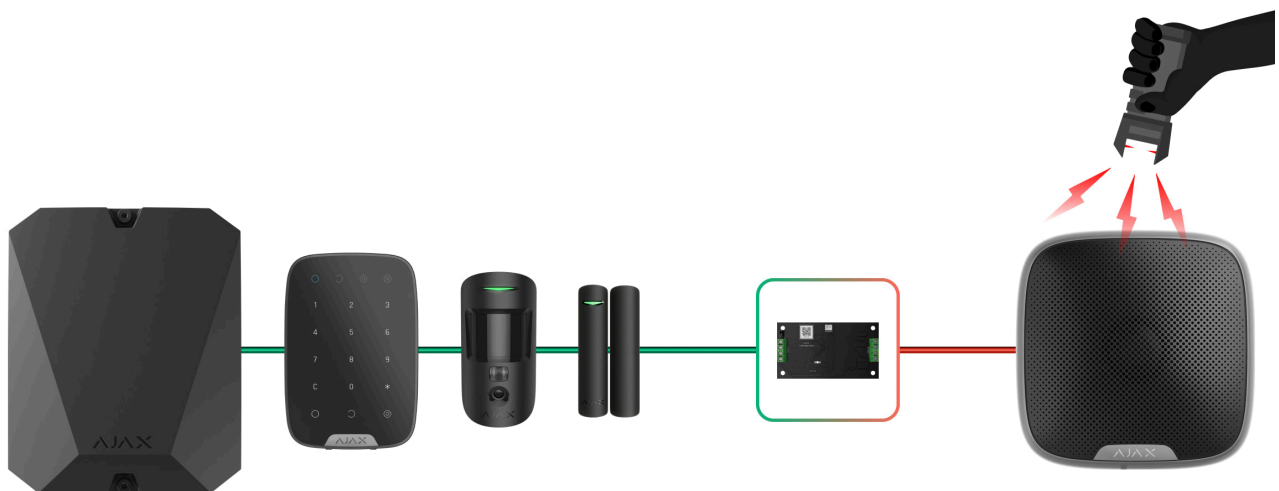
Based on the analysis results, detectors and devices are selected that effectively meet the requirements of the client and protect the object.

When selecting devices, consider their detection zone and alarm detection range. This is necessary to avoid blind spots and false alarms. For example, if you install a

big opening detector magnet at the maximum distance (2 cm) from the device, the detector may not respond to opening or give false alarms.

For the correct selection of devices, it is important to know the system's operating principle, the differences between the detectors, and in what situations which device is better to use. To do this, you should study the user manual for each device you want to use in the project.

Use LineProtect Fibra to secure the hub and devices on the line from short circuits and sabotage. The module can be installed at any point of the Fibra line. It protects devices on the line installed between LineProtect and the hub, as well as the hub itself. However, the module does not protect devices located between LineProtect and the end of the line (the last device on the line).



If a wired security system is already installed at the object, you can integrate these detectors into the Ajax system. Third-party wired devices can be connected to the Ajax system using MultiTransmitter Fibra.

Both system logic and hardware limit the maximum number of devices. The system logic includes limitations on the number of devices. For example, you can connect up to 5 radio signal range extenders and up to 10 wired and wireless Ajax sirens to Hub Hybrid (2G). System logic limitations can be found in the control panel user manual on our support website, as well as on the hub comparison page.

The hardware part includes power limitations. The maximum current that Hub Hybrid can supply in total for all Fibra lines is 14.4 W (600 mA). Please note that the total current consumption of the devices in the system depends on the type of

cable, its length, the type of connected device, the conductors connection state, and other factors. Therefore, we recommend verifying the project using our [online calculator](#) after selecting devices. It will accurately show whether the capacity of the power supply system is enough for the particular device configuration.

Topologies

Fibra is a data transfer protocol for the Ajax wired devices. At the physical level, Fibra resembles a bus connection: the detectors are connected to the control panel using a four-core cable. Currently, Ajax systems support three topologies – **Beam (Radial wiring)**, **Ring**, and **Tree**.



Beam connection (Radial wiring) uses one Fibra line of the hub. Only the segment that remains physically connected to the hub will function in the event of a line break. All devices connected after the breaking point will lose connection with the hub.



Ring connection uses two Fibra lines of the hub. In the event of a ring break in one place, not a single device will be disabled: two lines are formed that will continue to function normally and transmit events to the hub. Users and security company will receive notification about the line break.

Beam (Radial wiring)	Ring
<ul style="list-style-type: none"> • uses one Fibra line of the hub • up to 8 lines on the same hub • up to 2,000 m of wired communication for the same line • a terminating resistor is installed at the end of the line 	<ul style="list-style-type: none"> • uses two Fibra lines of the hub • up to 4 rings on the same hub • up to 500 m of wired communication for the same ring • no terminating resistor is installed at the end of the line

Both device connection topologies can be used on the same hub. For example, you can use two Ring connections and four Beam (Radial) connections.



We recommend connecting devices using the **Ring** topology (hub-device-hub) if possible. This improves the antisabotage protection of the system.

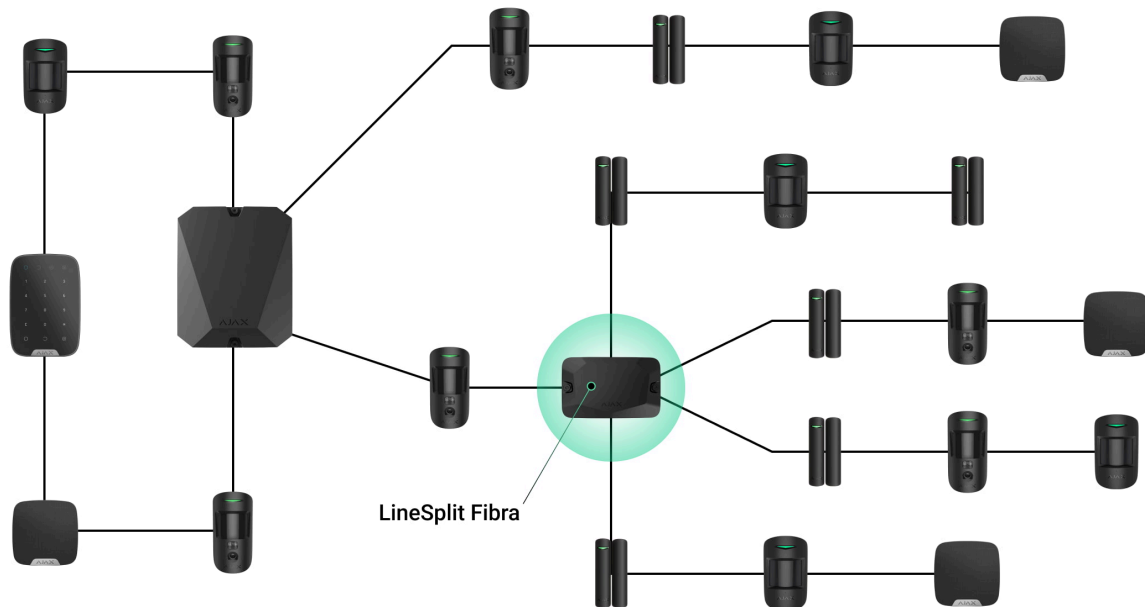
Fibra technology is notable for its versatility and energy efficiency. Different types of devices can be connected to a single Fibra line. For example, you can simultaneously connect opening detectors, motion detectors with photo verification support, sirens, and keypads to the same line.

Wired Fibra devices are energy efficient: detectors consume up to 30–50 mW on average, which is significantly less than the average performance of existing wired detectors from other manufacturers.

The devices are connected to the Fibra line one by one, as shown in the diagram. Line branching and the **Tree** topology are only allowed when using [LineSplit Fibra](#).

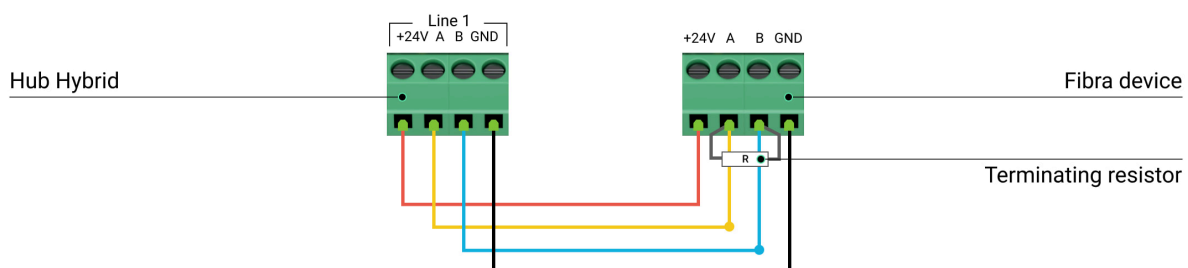


LineSplit divides one Fibra line into four lines. Each output line can be up to 2,000 meters long when connected using a U/UTP cat.5 twisted pair cable. LineSplit can be installed at any point of the line, including after another LineSplit.



The output lines created with LineSplit do not support the **Ring** topology.

When using the **Beam** topology, a 120 Ω terminating resistor is required at the end of the line. It is connected to the signal terminals of the last detector on the line. Terminating resistors are included in the Hub Hybrid complete set.



Cable length and type

When using the **Beam (Radial)** topology, the maximum range of a wired connection is 2,000 meters, and it's 500 meters when using the Ring topology. This brings

flexibility when designing the system project. You can run a cable in a way that is not obvious to an intruder, covering different devices in all rooms. This way, when trying to sabotage the line, the intruder will manage to disable only some devices, while the protection of the entire room will remain intact.

Take into account the places of possible signal interference. If the cable is routed near motors, generators, transformers, power lines, control relays, and other sources of electromagnetic interference, use twisted-pair cable in these areas.



Recommended cable types:

- U/UTP cat.5, $4 \times 2 \times 0.51$, copper conductor.
- Signal cable 4×0.22 , copper conductor.

We recommend mounting cables inside walls, floors, and ceilings. This will provide greater security; the wires will not be visible, and it will be impossible for an intruder to access them.

If this is not possible and external cable laying is used at the object, hide the cable from prying eyes. Use protective corrugated pipes or cable trays for this. Find these and other nuances in the [cable management](#) section.

Verification using a calculator

To ensure that the project is calculated correctly and that such a system will work in practice, we have developed two calculators: [Jeweller radio communication range calculator](#) and [Fibra line range calculator](#).

These tools are essential for project verification. Calculators check the quality of radio communication between the hub and system devices, and the cable length of wired devices for the selected configuration.

Preparatory work

Cable arrangement

When preparing to lay cables, check the electrical and fire safety regulations in your area. Strictly follow these standards and regulations.

It is safest to route cables inside walls, floors, and ceilings: this way, they will be invisible and unavailable for intruders. It also ensures their greater durability – the cable will be affected by fewer external factors affecting the conductor's natural wear and insulating layer.

As a rule, security system cables are laid during the construction or repair stage, and after wiring at the object.

If impossible to install cables inside the walls, route them so that the cable is sufficiently protected and hidden from prying eyes. For example, in a cable tray or a protective corrugated pipe. It is desirable to hide such trays or pipes, for example, behind furniture.

We recommend using protective pipes, cable conduits, or corrugated pipes to protect cables, regardless of whether they are routed inside the wall or not. The cables should be arranged carefully: no sagging, tangling, or twisting is allowed.

Cable routing

When laying cables for a security system, you need to know not only the general requirements and rules for electrical installation work but also the specific installation features of each device: installation height, mounting method, how the cable is inserted into the enclosure, and other parameters. These details are available in the user manuals of the devices. You can find and view them on our [support website](#).

Try to avoid any deviations from the security system design. For example, an increase in cable length can lead to a loss of connection between wired detectors and the hub. And changing the connection order of the devices or replacing them can affect the security of the object.

Cover the cable ends with a plastic bag or film if routing is carried out at the stage of repair of the object. In such a way they will be protected from paint or plaster. The ingress of such materials to the end of the cable can significantly affect the signal quality between the hub and the system devices.

Preparing cables for connection

Remove the insulating layer of the cable and strip the cable with a special insulation stripper. It strips the cable properly without damaging the conductor. The ends of the wires that will be inserted into the detector's terminals should be tinned or crimped with a sleeve. This ensures reliable connection and protects the conductor from oxidation.

Recommended cable lug sizes: 0.75 to 1 mm².

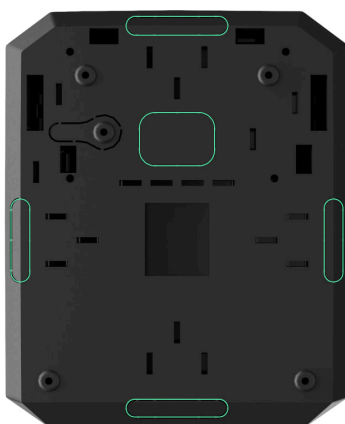


Specific features of [DoorProtect Fibra](#), [DoorProtect Plus Fibra](#), and [GlassProtect Fibra](#) enclosures exclude the use of insulated cable lugs. To connect these detectors, use a ferrule lug without insulation with a minimum cross-section of 0.5 mm² and up to 6 mm in length.

Installing and connecting the system

Installing the control panel and connecting the lines

To insert cables into the hub, prepare holes in the enclosure in advance.



The hub enclosure is as well prepared for installation as possible: all the necessary holes for mounting the control panel have already been made, and the hub complete set includes screws and dowels for quick installation.

The hub is mounted on a vertical surface hidden from prying eyes. When mounting, use all fixing points on the enclosure. Be sure to use the fixing point on the perforated part of the enclosure: it is necessary to trigger the tamper in case of attempts to tear it off the surface.



Install the hub only in the bundled enclosure. This is necessary for triggering the tampers located on both sides of the board. The tamper on the front side of the board reports an alarm in case of removal of the enclosure lid, and the tamper in the back reports attempts to detach the enclosure from the surface.

Before connecting the cables, turn off the hub, de-energize it, and disconnect the backup battery. When connecting the cables, be sure to observe the polarity and connection order of the wires. Securely fasten the conductors to the terminals. The hub enclosure provides fasteners for arranging and fixing cables with plastic ties.

How to install and connect Hub Hybrid

Installing the devices of the system

Each device has a SmartBracket mounting panel or special holes in the enclosure for mounting on a surface.

Before installation, remove the mounting panel or the part of the enclosure intended for mounting the device. Prepare holes for the output of cables in the mounting panel or part of the enclosure. Carefully break out the perforated part or drill it if it is allowed in the user manual of this device.

Places to make holes for cable output:



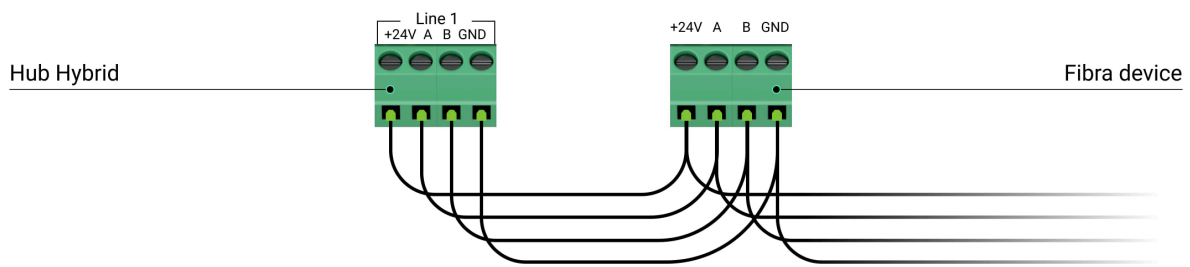
Make sure the selected installation location complies with the user manual. All manuals can be found on our [support website](#).

Before installation, remove the board with the terminal block and run the cable through the hole. Then fix the mounting panel or part of the enclosure to the surface using all fixing points, including the perforated part that is needed to trigger the tamper if an attempt is made to dismantle the device. Use only bundled screws; other fasteners may damage or deform the mounting panel or device enclosure during installation.

After fixing the panel or part of the enclosure to the surface, reinstall the board with the terminals on special holders. After connecting the cables to the terminals of the board, install the rest of the device and secure the enclosure with the bundled screw. A screw hole is located at the bottom of each device.

Connecting Fibra devices

The devices are connected to the Fibra line one by one, as shown in the diagram. Branching of lines is not allowed.



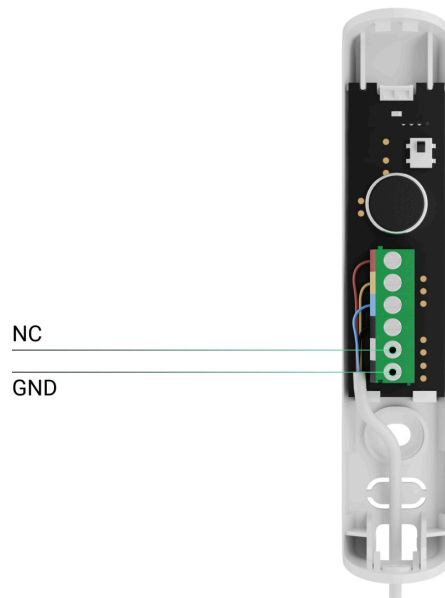
There are 4 terminals on the device board:

+24V – power

A, B – signal terminals

GND – ground

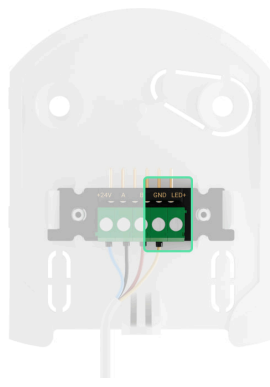
DoorProtect Fibra, DoorProtect Plus Fibra, Glass Protect Fibra detectors have additional terminals for connecting third-party detectors with an NC (normally closed) contact type.



NC – terminal for connecting an external contact/roller shutter detector (for DoorProtect Plus Fibra)

GND – ground

HomeSiren Fibra siren has an additional terminal for connecting a remote LED.



Connect devices only to a hub that is off and de-energized. Be sure to follow the polarity and connection order of the wires. Securely fix the cable to the terminals, and secure the cable itself with cable ties using the fasteners inside the mounting panel.

Configuring the system

Adding a hub to the Ajax PRO app

You can add and configure **Hub Hybrid** only in the Ajax PRO apps. Before adding a hub to the app, register an account.

Connect Ethernet cable and/or SIM cards, an external power supply, and backup battery to the hub.

Turn on the hub and wait until the LED indicator lights up green or white, which is to indicate the connection with Ajax cloud. Read more about LED indication in the [user manual](#).

Pay attention to the complete set of the hub to prepare the necessary components for its connection in advance.

Included in the complete set	Not included in the complete set
<ul style="list-style-type: none">Ethernet cable (1 meter)	<ul style="list-style-type: none">12 V\equiv backup battery

- | | |
|---|--|
| <ul style="list-style-type: none">• power cable (1 meter)• cable for connecting a 12 V= backup battery• one mini SIM card (depending on the sales region) | <ul style="list-style-type: none">• second mini SIM card |
|---|--|

Add the hub to the app by scanning the device's QR code or entering its ID manually. The QR code with an ID is located on the hub board, the back of the enclosure, and the packaging.

Hub settings

A full description of all settings is available in the [Hub Hybrid User manual](#). In this section, we will discuss important points, useful features, and non-obvious settings.

Communication channels

We recommend connecting the hub using all communication channels simultaneously: Ethernet and two SIM cards. The system will be protected even if one of the cellular operators has outages. In the app, the statuses of connection to communication channels are available at any time.

When connecting SIM cards, set the APN and other network settings recommended by the cellular operator. If the network uses static IP addresses, they should also be specified in the Ethernet settings.

How to find out that the hub has lost Internet connection

Groups

Wired Fibra devices can be combined into one security group with wireless devices regardless of their physical connection and location. Activate and configure [Group Mode](#) if required by the project. The maximum number of security groups for Hub Hybrid is 25.

Security schedule

Ajax system allows you to set a security schedule for an object. Scenarios allow you to change the security mode for individual security groups, [Night Mode](#), or the entire system at a specified time.

System setup according to PD 6662:2017 requirements

If the project should comply with the requirements of the British standard [PD 6662:2017](#), you need to configure the following functions:

- [Alarm confirmation](#)
- [System integrity check](#)
- [System restoration after alarm](#)
- [Two-stage arming](#)
- [Alarm transmission delay when disarming](#)
- [Device auto deactivation by timer](#)

There are two ways to configure your security system according to PD 6662: manually or using the wizard in the app. To use the wizard, go to the hub service settings, click Wizard and follow the app prompts. In case of manual setup, each function is configured separately.

[Learn more](#)

Adding devices to the system

Two ways of adding devices are available:

1. **Manually** – standard procedure for adding a device. To add a device, you need to scan its QR code or enter the ID manually. Suitable for adding wireless devices, a small amount of wired devices, and convenient for replacing a broken device during service.

2. Automatically – adding wired devices using the lines scan feature. Suitable for adding a large number of Fibra devices that are connected to the lines. This feature will help reduce the time for system setup: after scanning, the list of connected Fibra devices is sorted by Fibra lines, and for identification, the device will light the LED upon a command from the app. An alternative way to identify devices is also available – when an alarm occurs, the detector or device is displayed at the very top of the list. You can start scanning lines both in the menu for adding devices and in the hub settings.

For more information on automatic lines scanning, see the manuals for each Fibra device on our [support website](#).

Device setup

A full description of all settings for each device can be found on our [support website](#). In this section, we will discuss important points, useful features and non-obvious settings, sometimes forgotten.

Delay When Entering/Leaving

[Delay When Entering/Leaving](#) is the time the user has to change the security mode of the security system after entering or leaving the premises.

It is set separately in the settings of each detector. Ajax sirens can notify the countdown of delays with sound—this function is additionally activated in the siren settings.

Night Mode

[Night Mode](#) is a security mode in which only a part of the detectors are activated.

Night Mode can only work with opening, glass breaking, and motion detectors. Night Mode is disabled by default and is set up in each detector's settings.

Siren response to alarms

This setting turns on the sirens when the detector is triggered. It is configured separately for each detector. The siren will work with the volume and duration of the alarm signal set in the siren settings.

Chime

When the Chime (opening notifications) function is enabled, the sirens make a special sound to indicate that the opening detectors are triggered when the system is disarmed. The feature is used, for example, in stores, to notify employees that someone has entered the building.

Notification settings are made in two stages: setting up sirens and setting up opening detectors. In the settings of the opening detectors, the function itself is activated. In the siren settings, you need to activate the function, and select the volume and sound of the notification.

Keypad access codes

Access codes are needed to manage security modes using Ajax keypads. Access code and duress code can be general or personal. General codes are set in the keypad settings, while personal codes are set in the hub settings directly by the user from their personal account.

Motion detector sensitivity

Configured for each detector separately based on the specifics of the project: the pets, a fireplace, or other possible thermal interference. For outdoor motion detectors, the detection distance is also adjusted using the slider on the back of the enclosure.

Automation scenarios

For automation devices such as Relay, WallSwitch, and Socket, you can configure the response to detector alarms, change the security mode, and program a scheduled action or action upon pressing Button in control mode. For example, to turn on street lighting in case of alarm from motion detectors installed around the perimeter. Scenarios are created and edited in the settings of automation devices.

Detectors of the MotionCam series, with the support of the [Photos by Scenario](#) feature, can take photos in case of alarms from other Ajax devices or at a [specified time](#). You can create such a scenario in the **Privacy Settings** of the hub or in the settings of the detector itself.

System testing

The Ajax system offers the following tests to help choose the correct installation location for devices and check their functionality:

- [Jeweller Signal Strength Test](#)
- [Wings Signal Strength Test](#)
- [Fibra Signal Strength Test](#)
- [Detection Zone Test](#)
- [Attenuation Test](#)
- [Lines Power Test](#)

The Jeweller, Wings, and Fibra Signal Strength Tests determine the strength and stability of the signal at the intended location of the device.

Detection Zone Test helps to determine at what distance the detector will detect alarms in the current installation location.

Signal Attenuation Test allows you to artificially reduce or increase the power of the radio transmitter. The test simulates a change in the environment in the room to check the stability of the connection between the device and the hub.

Lines Power Test simulates the maximum possible power consumption of Fibra wired devices: detectors give alarms, keypads are activated, sirens are turned on. If the system passes the test, all its wired devices will have enough power supply in any situation.

After installation

Training for clients

Users need to download the Ajax Security System app and register an account to use the system. After registration, the installer adds all users to the hub and helps them set up notifications and access codes (if the system includes keypads).

Tell the client how to manage the system, and briefly explain the logic of the **Group Mode** and **Night Mode** operation if they are used. If there are scenarios in the system, explain how they work.

Leave your contacts or company contacts if you have any questions about the system. Also, the client can contact our support team 24/7 with any questions about the operation of the system, devices, app, and account.

Contacts of Ajax technical support

- [e-mail](#)
- [Telegram](#)
- Phone: 0 (800) 331 911

Maintenance

Check the functioning of the system regularly. The optimal frequency of checks is regulated by the laws and regulations of the state where the system is installed. Check the battery charge of your wireless device and change the batteries, if necessary. Check the fastening of the wires in the terminals. Run the functionality tests. Regular checks are important and will help detect and prevent malfunctions.

Client support

To ensure that the system meets the requirements of the client and remains future-proof, we regularly release new devices, app updates, as well as new versions of firmware for hubs and range extenders.

Clients are always happy to get new features through free firmware and app updates, and you, in turn, can offer them new devices and quality remote service.

Therefore, we advise you to build communication with clients after the system installation and inform them about any additional features, and new devices and system functions. We regularly notify partners and all users of PRO apps about the release of updates using email newsletters. You can also find company news in [our Blog](#).

Subscribe to the newsletter about safe life. No spam

Subscribe