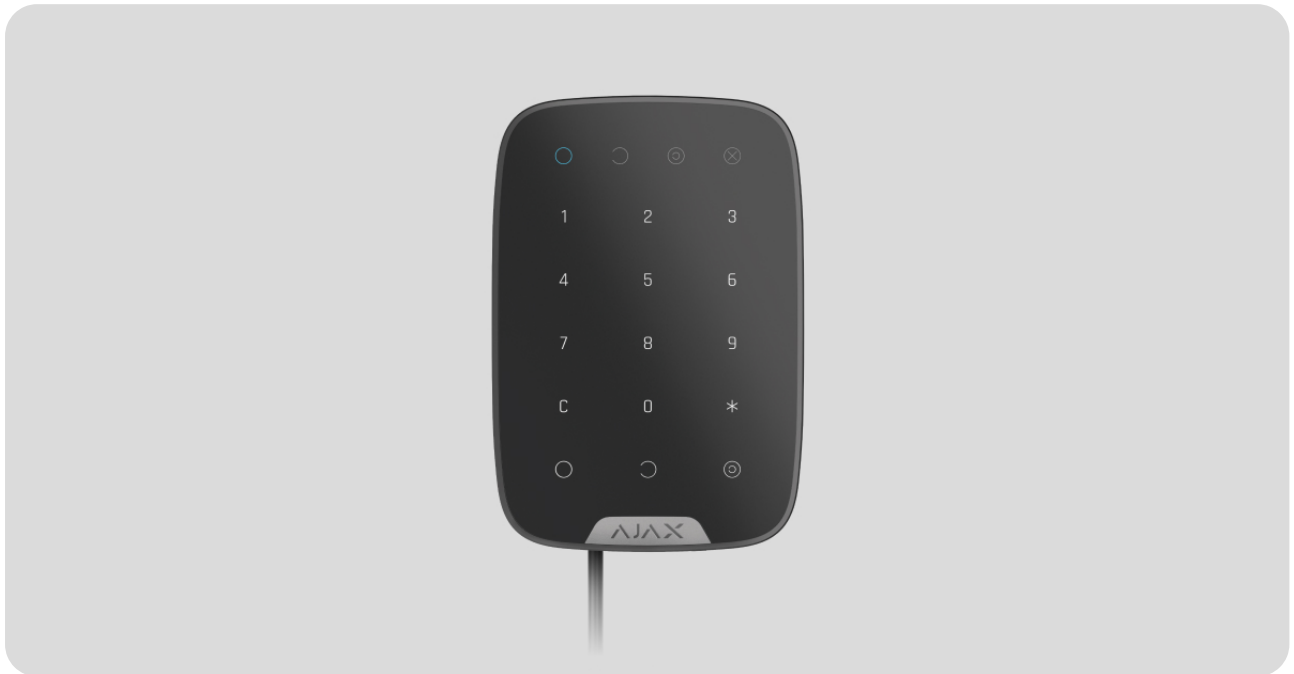


KeyPad Fibra user manual

Updated January 4, 2024



KeyPad Fibra is a wired touch keypad of the Ajax system. Controls the security modes and **Night Mode**. Supports duress code and protected from access code guessing. When it is active, the LED indication notifies about the security mode.



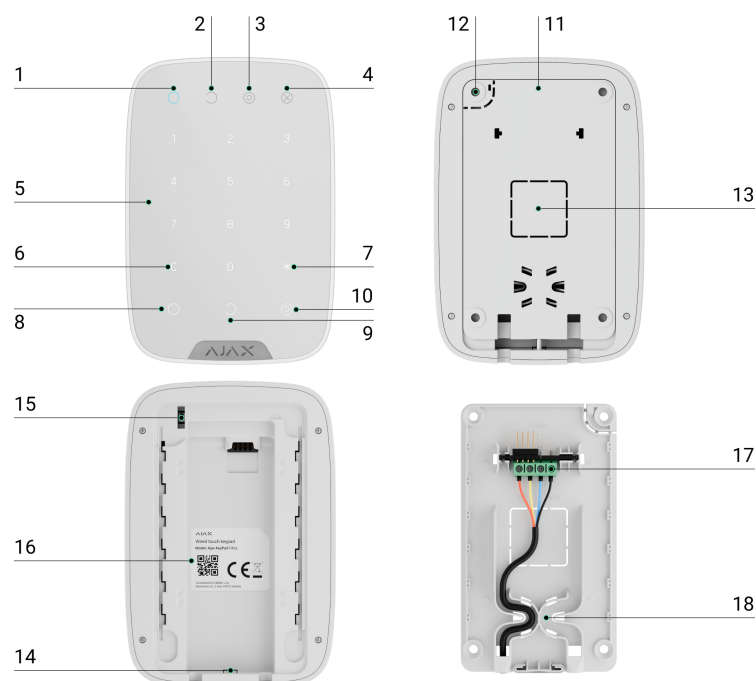
The keypad is compatible with [Hub Hybrid \(2G\)](#) and [Hub Hybrid \(4G\)](#). Connection to other [hubs](#), [radio signal range extenders](#), [ocBridge Plus](#), and [uartBridge](#) is not provided. Integration with other security systems is not provided either.

KeyPad Fibra works as part of the Ajax system, exchanging data with the hub using the secure Fibra wired protocol. The wired connection range is up to 2,000 meters when using a U/UTP cat.5 twisted pair.

KeyPad Fibra is part of the wired Fibra devices line. The installation, sale, and administration of these devices are performed only by accredited Ajax partners.

[Buy KeyPad Fibra](#)

Functional elements



1. Armed LED indicator.

2. Disarmed LED indicator.

3. Night Mode LED indicator.

4. Malfunction LED indicator.

5. Numeric touch button box.

6. Reset button.

7. Function button.

8. Arm button.

9. Disarm button.

10. Night Mode enabling button.

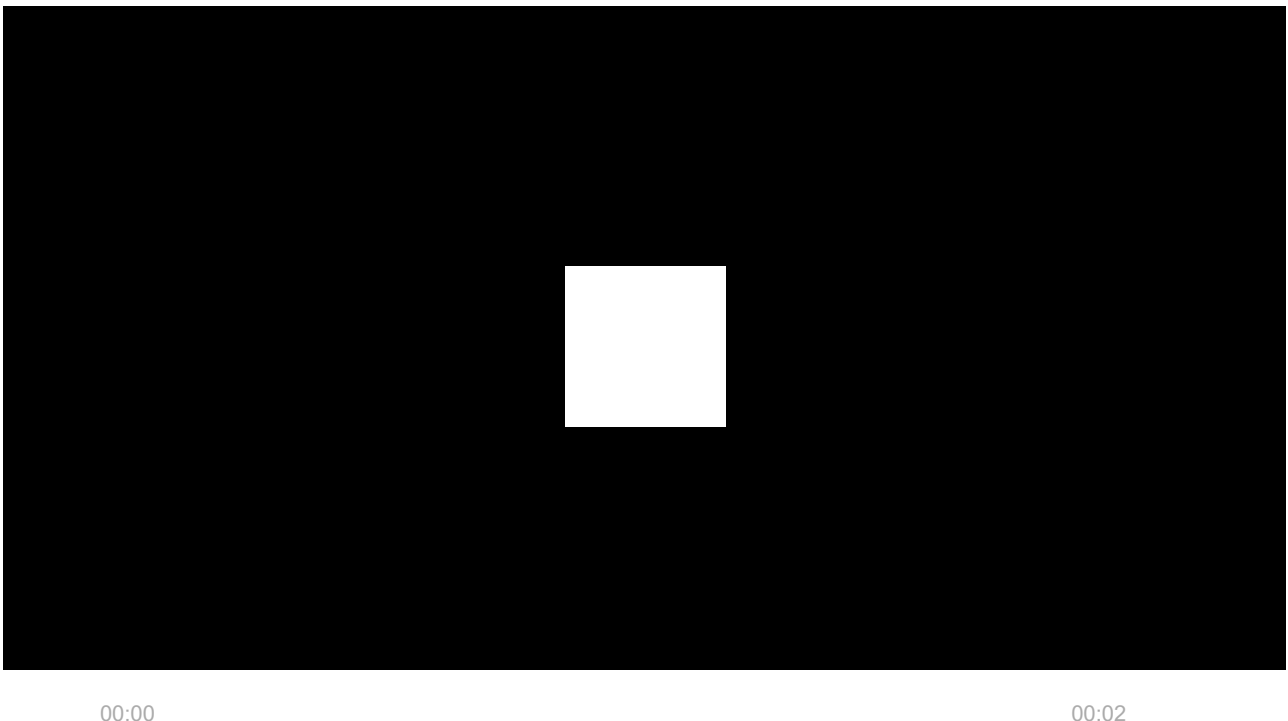
11. SmartBracket mounting panel. To remove the panel, slide it down.

12. Perforated part of the mounting panel. Necessary for tamper triggering in case of any attempt to detach the keypad from the surface. Do not break it off.

13. Perforated parts of the mounting panel for the output of cables.

- 14. The hole for attaching the SmartBracket mounting panel with a screw.
- 15. Tamper button. Indicates an attempt to remove the mounting panel or tear the device off the surface.
- 16. QR code and ID (serial number) of the device. It is used to pair the device with an Ajax system.
- 17. Terminals for connecting the device to the hub.
- 18. Fasteners for fixing cables with ties.

Operating principle



KeyPad Fibra is a touch keypad to control the Ajax system. It controls the security modes of the entire object or individual groups and also allows you to enable or disable the Night Mode.

You can control the security modes with KeyPad Fibra using general or personal codes. Before entering the code, you should activate the KeyPad Fibra by touching any part of the touch panel.

When the keypad is activated, the backlight turns on, and the built-in speaker beeps. Backlight brightness and keypad volume are adjustable in keypad settings in Ajax apps.

If you do not touch the keypad for 4 seconds, KeyPad Fibra reduces the brightness of the backlight, and 8 seconds later goes into power saving mode and turns off the display.



As the keypad goes into power saving mode, it resets the commands entered.

Access codes

KeyPad Fibra supports from 4 to 6 digit codes. Entering the code should be confirmed by pressing one of the buttons: (Arm), (Disarm) and ☾ (Night Mode). Any characters typed accidentally are reset with a button (Reset).

KeyPad Fibra supports code types as follows:

- **Keypad code** — common access code. Set in the settings of each keypad. When used, all events are delivered to Ajax apps on behalf of the keypad.
- **User code** — the personal code of the user who has an Ajax account and is linked to the hub. Each system user sets the code independently in the hub settings. When used, all events are delivered to Ajax apps on behalf of the user. The code works for all keypads that are connected to this hub.
- **Unregistered user code** — the code of the user who does not have an Ajax account. The code is set by an administrator or PRO with system setup rights in the hub settings. When used, events are delivered to Ajax apps with a name associated with this code. The code works for all keypads that are connected to this hub.
- **RRU code** is an access code for the rapid response units (RRU) activated after the alarm and valid for a specified period. When the code is activated and used, events are delivered to Ajax apps with a title associated with this code.




The number of codes supported depends on the hub model.

KeyPad Fibra also supports arming without entering a code, if the **Arming without Code** function is enabled in the keypad settings. This function is disabled by default.

Duress code

A duress code allows you to simulate alarm deactivation. The Ajax apps and sirens installed at the object will not give you away in this case, and the security company and other users of the security system will be warned about the incident.

Features of the alarm when entering the duress code:

1. Security company monitoring station receives an alarm event **Disarming under duress**. The rapid response team is going to the object.
2. All users of the security system receive a notification with no alarm about disarming the system, and the notification is indicated by a red icon .



If the security system is disarmed with a duress code erroneously, contact the security company monitoring station.

The keypad supports both common and personal duress codes. The common duress code is set in the keypad settings. The personal duress code is set by the user individually in the hub settings.

How to set up a duress code for registered user

How to set up a duress code for a user without an Ajax account

Function button

KeyPad Fibra keypad has the **Function** button. The button can work in one of three modes:

- **Alarm** — the panic button mode. After pressing, the system sends an alarm to the security company monitoring station and users and activates the sirens connected to the system.
- **Mute Interconnected Fire Alarms** — after the Function button is pressed, the system disables the sirens of Ajax fire detectors.
- **Off** — the button is disabled, and after pressing the system does not execute any commands.

Interconnected Fire Alarm muting

KeyPad Fibra can disable interconnected Fire Detectors Alarm by pressing the **Function** button if configured in **Mute Interconnected Fire Alarm** mode. The response of the system to pressing the button depends on the settings and the state of the system:

- **Interconnected Fire Alarms have propagated** — the first pressing of the **Function** button mutes all fire detector sirens, except for those that registered the alarm. Pressing the button again mutes the remaining detectors.
- **Interconnected Alarm Delay Time lasts** — pressing the **Function** button mutes the siren of the triggered Ajax fire detector.

The option works only if the Interconnected Fire Detectors Alarm option is enabled in hub settings.



With the OS Malevich 2.12 update, users can mute fire detector alarms in their groups and at the same time not affect the operation of detectors in those groups to which they do not have access.

[Learn more](#)

Unauthorized Access Auto-Lock

If a wrong code is entered three times within one minute, the keypad will be locked for the time specified in its [settings](#). During this time, the hub will ignore all codes, while simultaneously informing the users of the security system about an attempt to guess the code.

A user or PRO with administrator rights can unlock the keypad through the app. Also, unlocking occurs automatically after the lock time specified in the settings expires.

Two-stage arming

KeyPad Fibra participates in arming in two stages. This process is similar to arming with a personal or common code on a keypad. The process should be completed by re-arming with SpaceControl or restoring the terminating detector (for example, closing the door with DoorProtect Fibra installed).



KeyPad Fibra cannot act as a terminating device in two-stage arming.

[More on two-stage arming](#)

Fibra data transfer protocol

The keypad uses Fibra technology to transmit alarms and events. This is a wired data transfer protocol that provides fast and reliable two-way communication between the hub and the connected devices. Using the bus connection method, Fibra delivers alarms and events instantly, even if 100 devices are connected to the system.

Fibra supports floating key block encryption and verifies each communication session with devices to prevent sabotage and spoofing. The protocol requires regular polling of detectors by the hub with a predetermined frequency to monitor communication and display the status of the system devices in Ajax apps.

[Learn more](#)

Sending events to the monitoring station

An Ajax system can transmit alarms to the [PRO Desktop](#) monitoring app as well as the Central Monitoring Station (CMS) using **SurGard (Contact ID)**, **SIA DC-09 (ADM-CID)**, **ADEMCO 685**, and other proprietary protocols. See a complete list of supported protocols [here](#).

Which CMSs can the Ajax system be connected to

KeyPad Fibra can transmit the following events:

1. The duress code is entered.
2. The panic button is pressed (if the **Function** button works in the panic button mode).
3. The keypad is locked due to an attempt to guess a code.
4. Tamper alarm/recovery.
5. Loss/recovery of connection between KeyPad Fibra and the hub.
6. Activation/deactivation of KeyPad Fibra.
7. Unsuccessful attempt to arm the security system (with the [system integrity check](#) enabled).

When an alarm is received, the monitoring station operator of the security company knows what happened and where the rapid response unit has to be sent. All Ajax devices are addressable, so events, the device type, its assigned name and location (room, group) can be transmitted to PRO Desktop and the CMS. The list of transmitted parameters may differ depending on the type of the CMS and the selected communication protocol.



The device ID, loop (zone) number, and line number can be found in device [states in the Ajax app](#).

Selecting the installation site

When choosing where to place KeyPad Fibra, consider the parameters that affect the operation of the device:

- Fibra Signal Strength.
- Cable length for connecting KeyPad Fibra.



KeyPad Fibra is mounted on a flat vertical surface with the bundled screws. The keypad is intended for indoor installation only. For convenience, we recommend installing the keypad **at a height of 1.3–1.5 meters from the floor**.

Consider the placement recommendations when designing the security system project for your object. The security system should be designed and installed by professionals. The list of authorized Ajax partners is [available here](#).

Do not install KeyPad Fibra

- Outdoors. This could damage the keypad.
- Inside premises with temperature and humidity outside the permissible limits. This could damage the keypad.
- In places where the keypad has an unstable or low signal strength. This can lead to a loss of connection between the hub and the keypad.
- Where articles of clothing, power cables, or an Ethernet cable could be an obstacle to the keypad. This can lead to false clicks on the touch panel of the device.

Fibra Signal Strength

The Fibra signal level is determined by the number of undelivered or corrupted data packages over a certain period. The icon  in the **Devices**  tab in Ajax apps indicates the signal strength:

- **Three bars** — excellent signal strength.
- **Two bars** — good signal strength.
- **One bar** — low signal strength, stable operation is not guaranteed.
- **Crossed out icon** — no signal, stable operation is not guaranteed.

The following factors affect the signal strength:

- The number of detectors connected to one Fibra line.
- Cable length and type.
- The correctness of wire connections to the terminals.

Design

To correctly install and configure security system devices, it is important to properly design the security system. The design must consider the number and types of devices at the object, their exact location and installation height, the length of wired Fibra lines, the type of cable used, and other parameters. Tips for designing Fibra wired systems are available [in this article](#).

Topologies

Currently, Ajax systems support two topologies: **Beam (Radial wiring)** and **Ring**.



Connecting devices using a **Ring** topology will be implemented in the next OS Malevich updates. Hardware update of Hub Hybrid is not required.

Beam connection method (Radial wiring) occupies 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 breakpoint will lose connection with the hub.

Ring connection method occupies two Fibra lines of the hub. If the ring breaks in one place, no device will be disabled. The ring reconfigures into two lines, which continue to operate normally. Users and the security company will receive notification about the break.

Beam (Radial wiring)	Ring
-----------------------------	-------------

- occupies one Fibra line of the hub
- up to 8 beams with 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

- occupies two Fibra lines of the hub
- up to 4 rings with 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 built on the same hub. For example, you can use two ring connections and four beam (radial) connections.

Different types of devices can be connected to the same Fibra line. For example, you can connect opening detectors, motion detectors with photo verification support, sirens, and keypads to the same line.

The devices are connected to the Fibra line one by one, as shown on the figure. Line branching is not supported.

For the **Beam (Radial)** topology, be sure to install a 120 Ohm terminating resistor at the end of the line (included in the hub complete set). The terminating resistor is connected to the signal terminals of the last detector on the line.

Cable length and type

The maximum range of a wired connection using the **Beam (Radial)** topology is 2,000 meters, and using the **Ring** topology – 500 meters.



Recommended cable types:

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

If you use a different type of cable, the communication range for wired connections may vary. No other types of cables have been tested.

Verification using a calculator

To make sure that the project is calculated correctly and that such a system will work in real practice, we have developed a [communication range calculator of Fibra lines](#). The calculator helps to check the quality of communication and cable length for wired Fibra devices with the selected configuration at the system design stage.

Additional information

The maximum current that Hub Hybrid can supply in total for all Fibra lines is 600 mA. The total current consumption of the devices in the system depends on the type of cable, its length, the type of connected device, the quality of the connection of conductors, and other factors. Therefore, after selecting devices, we recommend verifying the project using the [Fibra calculator](#).

Up to 100 devices can be connected to Hub Hybrid at default settings.

Preparing for installation

Cable arrangement

When preparing to route cables, check the electrical and fire safety regulations in your region. 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 recommended to hide them. For example, behind the 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.

Consider 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.

Cable routing

When routing cables for a security system, consider 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. Before installation, we recommend you read the [selecting the installation site](#) section of this manual.

Try to avoid any deviations from the security system project design. Violation of the basic installation rules and the recommendations of this manual lead to incorrect operation, as well as loss of connection with the KeyPad Fibra.

Check the cables for bends and physical damage before installation. Replace the damaged cables.

Signal cables of Fibra devices must be laid at a distance of at least 50 cm from the power cables when laying parallel, and, if they intersect, at a 90° angle.

Observe the permissible bend radius of the cable. It is specified by the manufacturer in the cable specifications. Otherwise, you risk damaging or

breaking the conductor.

Fibra devices are connected to the line one by one. Line branching is not supported.

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 tips. This ensures reliable connection and protects the conductor from oxidation. Recommended cable lug sizes: 0.75 to 1 mm².

Installation and connection



Before installing KeyPad Fibra, make sure that you have selected the optimal location and that it meets the requirements of this manual. Cables should be hidden from prying eyes and located in places inaccessible to intruders to reduce the chance of sabotage. Ideally, run the cables in the walls, floors, or ceilings.

When connecting to the device terminals, do not twist the wires together; solder them. The ends of the wires that will be inserted into the terminals should be tinned or crimped with special tips. This will ensure a reliable connection.

Observe safety procedures and regulations for electrical installation work when connecting the device.

Connecting KeyPad Fibra to the hub

1. Remove the SmartBracket mounting plate from the keypad. To do this, lightly press the panel and slide it down.
2. Remove the KeyPad Fibra board from the holders on the mounting panel, pulling them to the sides and pulling the board towards you.

3. Prepare holes for cable output in advance. To output cables from the back of the keypad, break out the perforated part on the SmartBracket mounting panel. To output cables from the bottom of the keypad, make holes in the bottom of the enclosure using a drill bit, a special milling cutter for small holes, or hand-cutting tools.

To output cables from the back of the keypad.	To output cables from the bottom of the keypad.

4. Disconnect the external power and the hub backup battery.

- 1 — external power supply
- 2 — backup battery

5. Run the cable into the hub enclosure. Connect the wires to the hub line.

- +24V** — power supply terminal of 24 V $\overline{\text{=}}$.
- A, B** — signal terminals.
- GND** — ground.

6. Run the cable from the hub into the mounting panel of the keypad through the holes made. If the cable is routed from the bottom of the keypad, pass it through the special channels on the mounting panel. They are necessary for a more reliable fixation of the cable.
7. If the keypad is not the last device in the connection line, prepare a second cable in advance. The ends of the wires of the first and second cables,

which will be inserted into the keypad terminals, must be tinned and soldered together, or crimped with special tips.

8. Attach the mounting panel to a vertical surface at the chosen installation location using the bundled screws. When attaching, use all fixing points. One of them, in the perforated part of the mounting panel, is needed to trigger the tamper in case of an attempt to tear the device off the surface.
9. Install the KeyPad Fibra board on special mounting panel holders.
10. Connect the wires to the terminals according to the scheme below. Follow the polarity and connection order of the wires. Securely fasten the wires to the terminals.

+24V — power supply terminal of 24 V_{DC}.

A, B — signal terminals.

GND — ground.

11. If the keypad is the last in the line, install a terminating resistor in case of **Beam (Radial) connection** by connecting it to the signal terminals of the device. For **Ring connection** terminating resistor is not needed.

More about topologies to connect Ajax devices



If possible, we recommend connecting devices using the **Ring** topology (hub — device — hub). This improves the antisabotage protection of the system.

12. Connect the backup battery and external power supply to the hub. Turn on the hub.
13. Reattach the keypad to the SmartBracket mounting panel. Fix the keypad with the bundled screw at the bottom of the enclosure.

14. Add device to the system.

15. Run a Fibra Signal Strength Test. The recommended signal strength is two or three bars. If the signal strength is one or zero bars, check the connection correctness and the cable integrity.

Adding to the system



The keypad is compatible only with Hub Hybrid (2G) and Hub Hybrid (4G). Fibra devices can only be added and configured through the app by a PRO user with full rights.


Types of accounts and their rights

Before adding a device

1. Install the PRO app. Log in to a PRO account or create a new account if you don't have one.
2. Add a hub compatible with the device to the app, make the necessary settings, and create at least one virtual room.
3. Make sure that the hub is on and has Internet access via Ethernet and/or mobile network. You can check the connection in the Ajax app or by looking at the LED on the hub board: it should light up white or green.
4. Make sure the hub is not armed and does not start updates by checking its status in the Ajax app.
5. Make sure the device is physically connected to the hub.


How to add KeyPad Fibra

To add the keypad manually

1. Open the PRO app. Select the hub you want to add KeyPad Fibra to.
2. Go to the **Devices**  tab and click **Add Device**.

3. Assign a name to the device.
4. Scan or type in the QR code manually. The QR code is located on the back of the enclosure under the SmartBracket mounting panel and on the packaging.
5. Select a virtual room and a security group if the group mode is enabled.
6. Press **Add**.

To add the keypad automatically

1. Open the PRO app. Select the hub you want to add KeyPad Fibra to.
2. Go to the **Devices**  tab and click **Add Device**.
3. Select **Add All Fibra Devices**. The hub will scan all Fibra lines. After scanning, all devices physically connected to the hub will be displayed in the **Devices tab**. **The order of the devices will depend on which line they are connected to.**
4. In the list of available devices to add click on the device you need. The LED indicator of this device will start flashing. This way, you'll know exactly which device you're adding, how to name it correctly, and which room and group it should be assigned to.
5. To add a device, specify a name, room, and security group if the group mode is enabled. Press **Add**. If the device was successfully added to the hub, it disappears from the list of devices available for adding and displays on the **Devices** tab in the app.





KeyPad Fibra works with one hub only. After connecting to a new hub, the keypad stops exchanging commands with the old one. Once added to a new hub, KeyPad Fibra is not removed from the list of devices of the old hub. This must be done manually in Ajax apps.

Functionality testing


The Ajax system offers several types of tests to help you choose the right installation place for the devices. Tests do not start straight away but not later than over a single “hub–devices” polling period.




Fibra Signal Strength Test is available for KeyPad Fibra. The test allows you to determine the strength and stability of the signal at the installation site.

To run a test

1. Select the hub if you have several of them or if you are using the [PRO app](#).
2. Go to the **Devices**  menu.
3. Select **KeyPad Fibra**.
4. Go to the KeyPad Fibra settings by clicking on the gear icon .
5. Select the **Fibra Signal Strength Test**.
6. Run the test following the prompts of the app.


Icons

The icons show some of the device states. You can view them in Ajax apps in the **Devices**  tab.

Icon	Meaning
	Fibra Signal Strength — displays the signal strength between the hub and the keypad. Recommended value is 2–3 bars. Learn more
	KeyPad Fibra is disabled. Learn more
	KeyPad Fibra has tamper triggering events disabled. Learn more

States

The states include information about the device and its operating parameters. The states of KeyPad Fibra can be found in the Ajax app:

1. Go to the **Devices**  tab.
2. Select **KeyPad Fibra** from the list of devices.



Parameter	Meaning
Malfunction	<p>Clicking on ⓘ opens the list of KeyPad Fibra malfunctions.</p> <p>The field is displayed only if a malfunction is detected.</p>
Temperature	<p>Device temperature. Measured on the processor and changes gradually.</p> <p>Acceptable error between the value in the app and the room temperature is 2°C.</p> <p>The value is updated as soon as the device identifies a temperature change of at least 2°C.</p> <p>You can configure a scenario by temperature to control automation devices</p> <p>Learn more</p>
Fibra Signal Strength	<p>Signal strength between the hub and KeyPad Fibra. The recommended value is two or three bars.</p> <p>Fibra is a protocol for transmitting KeyPad Fibra events and alarms.</p> <p>Learn more</p>

Connection via Fibra	<p>The connection status between the hub and KeyPad Fibra:</p> <ul style="list-style-type: none"> • Online — the keypad is connected to the hub. • Offline — the keypad has lost connection with the hub. Check the keypad connection to the hub.
Line Voltage	<p>The voltage value on the Fibra line to which the keypad is connected.</p>
Lid	<p>The status of the tamper that responds to detachment of the device from the surface or opening of the enclosure:</p> <ul style="list-style-type: none"> • Closed — the keypad is installed on the SmartBracket mounting panel. Normal state of the enclosure. • Open — the keypad is removed from the SmartBracket mounting panel or the enclosure integrity is otherwise compromised. Check the state of the keypad enclosure. <p>Learn more</p>
Permanent Deactivation	<p>Shows the status of the device permanent deactivation function:</p> <ul style="list-style-type: none"> • No — the device operates in normal mode and transmits all events. • Lid only — a user with system configuration rights has disabled tamper triggering notifications. • Entirely — a user with system configuration rights has excluded the keypad from the system operation. The device does not follow system commands and does not report alarms or other events. <p>Learn more</p>

One-Time Deactivation	<p>Shows the status of the keypad one-time deactivation setting:</p> <ul style="list-style-type: none"> • No — the keypad operates in normal mode. • Lid only — notifications on the keypad tamper triggering are disabled until the first disarm. • Entirely — the keypad is entirely excluded from the operation of the system until the first disarm. The device does not execute system commands and does not report alarms or other events. <p>Learn more</p>
Firmware	KeyPad Fibra firmware version.
Device ID	KeyPad Fibra ID (serial number). Also available on the back of the keypad enclosure and on the packaging.
Device №	KeyPad Fibra loop (zone) number.
Line №	The number of the Fibra line of a hub to which KeyPad Fibra is physically connected.

Settings

To change the keypad settings in the Ajax app:

1. Go to the **Devices**  tab.
2. Select **KeyPad Fibra** from the list.
3. Go to **Settings** by clicking on the gear icon .
4. Set the required settings.
5. Click **Back** to save the new settings.

Settings	Meaning
Name	<p>Keypad name. Displayed in the list of hub devices, text of SMS and notifications in the events feed.</p> <p>To change the name, click on the text field.</p> <p>The name can contain up to 12 Cyrillic characters or up to 24 Latin characters.</p>
Room	<p>Choosing a KeyPad Fibra virtual room.</p> <p>The room name is displayed in the text of SMS and notifications in the events feed.</p>
Group Management	<p>The parameter is available only when <u>group mode</u> is enabled.</p> <p>Each keypad can be configured to control a separate security group. By default, the keypad controls all security groups in the system.</p> <p>When <u>group mode</u> is disabled, the keypad controls the security of the entire system.</p>
Access Settings	<p>Setting the method to control system security modes:</p> <ul style="list-style-type: none"> • Keypad codes only – a common keypad code is used to change the security mode. • User codes only – personal user codes are used to change the security mode. • Keypad and user codes – to change the security mode, both the common keypad code and personal user codes are used.
Keypad Code	<p>Selecting a common keypad code to control system security modes. Contains 4–6 digits.</p>
Duress Code	<p>Selecting a common <u>duress code</u> of the keypad. Contains 4–6 digits.</p>

Function Button	<p>Selecting the operation mode of the Function button:</p> <ul style="list-style-type: none"> • Off — the button is disabled and does not execute any commands when pressed. • Alarm — when the button is pressed, the system sends an alarm to all users and the monitoring station of a security company. • Mute Fire Alarm — when pressed, disables the <u>Ajax fire detectors</u> alarm. The option works only if the <u>Interconnected fire detectors alarm</u> option is enabled.
Arming without Code	<p>The option allows you to arm the system without entering a code. To do this, simply activate the keypad with a touch and press the arming or <u>Night Mode</u> enabling button.</p>
Unauthorized Access Auto-Lock	<p>If active, the keypad is locked for the pre-set time if an incorrect password is entered more than three times in a row within one minute.</p> <p>It is not possible to disarm the system using the keypad during this time.</p> <p><u>Learn more</u></p>
Auto-lock Time, min	<p>The parameter is available when the option Unauthorized Access Auto-Lock is enabled.</p> <p>Allows you to select the keypad lock period when trying to guess a code:</p> <ul style="list-style-type: none"> • 3 minutes • 5 minutes • 10 minutes • 20 minutes • 30 minutes • 60 minutes • 90 minutes



	<ul style="list-style-type: none"> • 180 minutes
Brightness	<p>Selecting the brightness of the keypad backlight: 0 to 5 (0 – backlight is off, 5 – very bright backlight).</p> <p>The backlight is on only when the keypad is active.</p> <p>This option does not affect the brightness level of the security mode indicators.</p>
Buttons Volume	<p>Selecting the sound volume level when pressed: 0 to 14 (0 – the sound of pressing is disabled, 14 – very loud sound of pressing).</p>
Alert with a siren if panic button is pressed	<p>The option is available only if for the Function button the Alarm operation mode is configured.</p> <p>When the option is enabled, the <u>sirens</u> connected to the security system give an alert when pressing the Function button.</p>
Fibra Signal Strength Test	<p>Switches the keypad to the Fibra signal strength testing mode.</p> <p>The test allows you to check the signal strength between the hub and the keypad over the Fibra wired data transfer protocol to determine the optimal installation location.</p> <p><u>Learn more</u></p>
User Guide	<p>Opens the KeyPad Fibra user manual in the Ajax app.</p>
Permanent Deactivation	<p>Allows the user to disable the device without removing it from the system.</p> <p>Three options are available:</p> <ul style="list-style-type: none"> • Entirely – the device does not execute system commands and does not participate in automation scenarios, and the system ignores alarms and other device notifications.

	<ul style="list-style-type: none"> • Lid only — the system ignores the device tamper triggering notifications. • No — the device operates in normal mode and transmits all events. <p>Learn more</p>
One-Time Deactivation	<p>Allows the user to disable events of the device until the first disarm.</p> <p>Three options are available:</p> <ul style="list-style-type: none"> • No — the device operates in normal mode. • Lid only — notifications on the device tamper triggering are disabled while the armed mode is active. • Entirely — the device is completely excluded from the operation of the system while the armed mode is active. The device does not execute system commands and does not report alarms or other events. <p>Learn more</p>
Delete Device	<p>Unpairs KeyPad Fibra from the hub and deletes its settings.</p>

Codes setting

Keypad access code

To generate a keypad access code, in apps:

1. Go to the **Devices**  menu.
2. Select the keypad for which you want to set up an access code.
3. Go to Settings by clicking on the gear icon .
4. Find the **Keypad Code** item and click it.



5. Set the keypad code. Contains from 4 to 6 digits.

6. Press **Done**.

User access code

Registered user access code



Each user registered in the system can set a personal access code. To do this in the app:

1. Go to the **Devices**  menu.
2. Select a hub.
3. Go to Settings by clicking on the gear icon .
4. Open the **Users** menu.
5. Find your account in the list and click on it.
6. Go to the **Passcode Settings** item.
7. Set the user code. Contains from 4 to 6 digits.
8. Click **OK**.
9. Click **Back** to save the settings.

Access code for a user without an account

With an [OS Malevich 2.13.1](#) update, Ajax keypads support codes for users not connected to the hub. This is convenient, for example, for creating a cleaning company code.

To create an access code for a user without an account, in apps:



1. Go to the **Devices**  menu.
2. Select the hub in the list.
3. Go to Settings by clicking on the gear icon .
4. Go to the **Keypad Access Codes** menu.

5. Press **Add code**. Set up Username and Access Code. Contains from 4 to 6 digits.
6. Click **Add** to save the data.

Duress code



Keypad duress code

To generate a keypad duress code, in apps:

1. Go to the **Devices**  menu.
2. Select the keypad for which you want to set up a duress code.
3. Go to Settings by clicking on the gear icon .
4. Find the **Duress Code** item and click on it.
5. Set the keypad duress code. Contains from 4 to 6 digits.
6. Press **Done**.



Registered user duress code

Each user registered in the system can set a personal duress code. To do this in the app:

1. Go to the **Devices**  menu.
2. Select a hub.
3. Go to Settings by clicking on the gear icon .
4. Open the **Users** menu.
5. Find your account in the list and click on it.
6. Go to the **Passcode Settings** item.
7. Set the user duress code. Contains from 4 to 6 digits.
8. Click **OK**.
9. Click **Back** to save the settings.

Duress code for a user without an account

To create a duress code for a user without an account, you first should create the personal access code for such a user. To do this in the app:

1. Go to the **Devices**  menu.
2. Select the hub in the list.
3. Go to Settings by clicking on the gear icon .
4. Go to the **Keypad Access Codes** menu.
5. Select a user from the list.
6. Go to the **Duress Code** menu.
7. Set the duress code. Contains from 4 to 6 digits.
8. Press **Done**.
9. Click **Save** to save the changes.





RRU code

Only a PRO with the rights to configure the system can create and configure the RRU codes in the Ajax PRO apps. More information about configuring this feature you can find in this article.



The RRU codes are supported by hubs (except the Hub model) with OS Malevich 2.17 and higher.

Security modes control using access codes


Using common or personal code, you can control the Night Mode and the security of the entire object or separate groups. Entering the code should be confirmed by pressing one of the buttons  (Arm),  (Disarm) and  (enable Night Mode). Erroneously entered digits are reset with the button .

Arming with a personal code
Arming with a common code



KeyPad Fibra is locked for the time specified in the settings if an incorrect password is entered three times in a row within 1 minute. The corresponding notifications are sent to users and to the monitoring station of the security company. A hub administrator or PRO with administrator rights can unlock the keypad in the Ajax app.


Security control of the object using a keypad code

1. Activate the keypad by touching any touch button.
2. Enter the **Keypad Code**.
3. Press the button (Arm), (Disarm) or  (Night Mode).

For example, to arm the system:

1234 →

Security control of the group using a keypad code

1. Activate the keypad by touching any touch button.
2. Enter the **Keypad Code**.
3. Press the **Function** button.
4. Enter the Group ID.
5. Press the button (Arm), (Disarm) or  (Night Mode).

For example, to arm the group:

1234 → * → 2 →

If a security group is assigned to the keypad in its settings, you do not need to enter the group ID. To control the security of this group, it is enough to enter the keypad code or user code.



If KeyPad Fibra is configured to control a separate security group, enabling the Night Mode for this group is only possible with a user code. The user should have an access right to control this group.

Rights in the Ajax security system

Security control of an object using a user code

1. Activate the keypad by touching any touch button.
2. Enter the User ID.
3. Press the **Function** button.
4. Enter the **User code**.
5. Press the button (Arm), (Disarm) or 🌀 (Night Mode).


For example, to arm the system:

2 → * → 1234 →

Security control of the group using a user code

1. Activate the keypad by touching any touch button.
2. Enter the User ID.
3. Press the **Function** button.
4. Enter the **User code**.
5. Press the **Function** button.

6. Enter the Group ID.

7. Press the button (Arm), (Disarm) or  (Night Mode).

For example, to arm the group:

$2 \rightarrow * \rightarrow 1234 \rightarrow * \rightarrow 5 \rightarrow$

If a security group is assigned to the keypad in its settings, you do not need to enter the group ID. To control the security of this group, it is enough to enter the user code.

Using a duress code



Scenarios and sirens react to disarming under duress in the same way as to normal disarming.

To use the keypad duress code

1. Activate the keypad by touching any touch button.
2. Enter the **Keypad Duress Code**.
3. Press the (Disarm) button.

For example:

$4321 \rightarrow$

To use the user duress code

1. Activate the keypad by touching any touch button.
2. Enter the User ID.
3. Press the * (Function button).
4. Enter the **User Duress Code**.
5. Press the (Disarm) button.

For example:

2 → * → 4422 →

Using the RRU code

The RRU code is activated after triggering the alarm during the time configured in the hub settings, and it is valid for a specified period. This ensures that such code will only be used in case of risk, unlike keypad or user codes.

How to configure the RRU code


Security control of the object using the RRU code:

Enter **RRU Code** and press the **arming** / **disarming** / **Night Mode activation**  button.

For example:

1234 →

Security control of the group using the RRU code:

Enter **RRU Code**, press *****, enter Group ID, and press the **arming** / **disarming** / **Night Mode activation**  button.

For example:

1234 → * → 2 →

LED indication

KeyPad Fibra can report the current security mode, button pressings, malfunctions, and other conditions with LED indication and a sound signal.



The current security mode is displayed by the backlight after the keypad is activated. The information about the security mode is relevant, even if it is changed using another Ajax device (SpaceControl or another keypad) or an app.

Event	LED indication	Note
Touch button pressed.	Short beep, the current system security status LED blinks once.	The volume of the beep and the brightness of the backlight depend on the keypad settings.
The system is armed.	Short beep, Armed or Night Mode LED lights up.	
The system is disarmed.	Two short beeps, Disarmed LED lights up.	
Wrong code entered.	Long beep, digital unit LED backlight blinks 3 times.	
The armed mode cannot be activated (for example, a window is open, and the System Integrity Check is enabled).	Long beep, the current security status LED blinks 3 times.	
The hub does not respond to the command — there is no connection.	Long beep, LED indicator X (Malfunction) is light.	
The keypad is locked due to an attempt to guess a code.	Long beep, security status indicators and keypad backlight blink 3 times.	

Sound notifications of malfunctions

If any device is offline or the battery is low, KeyPad Fibra can notify system users with an audible sound. The keyboards' LEDs **X** will blink. Malfunction notifications will be displayed in the events feed, SMS text, or push notification.

To enable sound notifications of malfunctions, use Ajax PRO and PRO Desktop apps:

1. Click **Devices** , choose hub and open its settings 
Click **Service** → **Sounds and Alerts**

2. Enable toggles: **If battery of any device is low** and **If any device is offline**.

3. Click **Back** to save settings.



Sound notifications of malfunctions settings are available for all hubs (except the Hub model) with firmware version OS Malevich 2.15 or higher.

Sound notifications of malfunctions are supported by KeyPad Fibra with firmware version 6.57.11.12 or higher.

Event	Indication	Note
If any device is offline.	Two short sound signals, Malfunction indicator X blinks twice. Beep once per minute until all devices in the system are online.	Users can delay sound indication for 12 hours.
If KeyPad Fibra is offline.	Two short sound signals, Malfunction indicator X blinks twice. Beep once per minute until the keyboard in the system is online.	It's impossible to delay sound indication.
If battery of any device is low.	Three short sound signals, Malfunction indicator X blinks three times. Beep once per minute until the battery is restored or the device is removed.	Users can delay sound indication for 4 hours.

Sound notifications of malfunctions appear when the keypad indication is finished. If several malfunctions occur in the system, the keypad will notify about the loss of connection between the device and the hub first.

KeyPad Fibra malfunctions

If a keypad malfunction is detected, a malfunction counter is displayed in Ajax apps in the upper left corner of the device icon.

All malfunctions can be seen in the States of devices. Fields with malfunctions will be highlighted in red.

KeyPad Fibra malfunctions

- The keypad temperature is out of acceptable limits.
- The keypad enclosure is open or detached from the surface (tamper button triggering).
- No connection between the keypad and the hub via the Fibra protocol.
- Low voltage of the KeyPad Fibra power supply line.

Maintenance

Check the functioning of your keypad regularly. The optimal frequency of checks is once every three months.

Clean the enclosure and keypad touch panel from dust, cobwebs, and other contaminants as they emerge. To do this, turn off the keypad first to avoid false alarms in the attempt to guess a code. Use a soft dry cloth suitable for equipment care.

Wipe the touch panel gently: scratches can reduce the sensitivity of the keypad. Do not use substances that contain alcohol, acetone, petrol, or other active solvents to clean the keypad.

Technical specifications

[All technical specifications](#)

Complete set

1. KeyPad Fibra.
2. SmartBracket mounting panel.
3. Installation kit.
4. Quick Start Guide.

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 the Ajax Technical Support first. In most cases, technical issues can be resolved remotely.

Warranty Obligations

User Agreement

Contact Technical Support:

- e-mail
- Telegram

Manufactured by “AS Manufacturing” LLC

Subscribe to the newsletter about safe life. No spam

Email

Subscribe