KeyPad Fibra User Manual

Updated March 11, 2022

KeyPad Fibra is a wired touch keypad for controlling the Ajax security system. Supports “silent alarm” if the duress code is entered. Informs about the current security mode by LED indication.

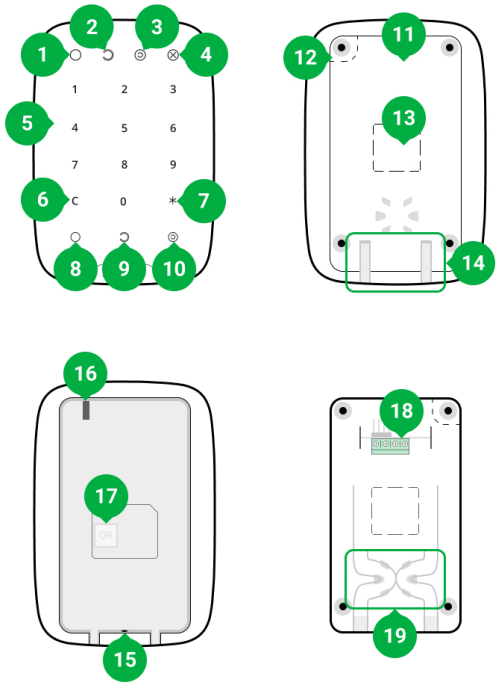
The keypad is compatible with Hub Hybrid (2G) and Hub Hybrid (4G). Connection to other hubs, radio signal range extenders, ocBridge Plus, and uartBridge is not supported. Integration with other security systems is not provided

KeyPad Fibra only works as a part of the Ajax security system, communicating with the hub via the secure Fibra protocol. The wired connection range is up to 2000 meters when connected via the twisted pair U/UTP cat.5.

KeyPad Fibra is the device of the new Fibra wired product line. Such devices can only be purchased, installed and administered 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 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 part for wire output.
14. Holes for wire output.

15. The hole for attaching the SmartBracket mounting panel with a screw.
16. **Tamper button**. Triggers when an attempt is made to detach the keypad from the surface or remove the mounting panel.
17. QR code of the device. Used to connect the keypad to the Ajax security system.
18. Terminal block for connecting the keypad.
19. A hole for fixing the wires with ties.

Operating principle

KeyPad Fibra is a touch keypad for controlling the Ajax security system. It controls the security modes of the entire facility or individual groups and allows activating the **Night mode**. Supports the “silent alarm” function, i.e. the ability to inform the security company about the compulsion to disarm the security system without exposing the user by sirens.

You can control the security modes with KeyPad Fibra using general or personal codes. Before entering the code, you should activate (“wake up”) KeyPad Fibra by touching it. When the keypad is activated, the button’s backlight turns on, and the built-in speaker beeps.

The backlight brightness and the keypad volume are adjusted in **keypad settings**. 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!

KeyPad Fibra supports 4 to 6 digit codes. Entering the code should be confirmed by pressing one of the buttons: ○ (arm), ◌ (disarm), and ⟲ (Night mode). Incorrectly entered numbers are cleared by C ("Reset") button.

KeyPad Fibra also supports control of security modes without entering a code, if the "Arm without code" function is enabled in the settings. This function is disabled by default.

Function button

KeyPad Fibra has a Function button that operates in 3 modes:

- **Off** — the button is disabled and nothing happens after it is pressed.
- **Alarm** — after the Function button is pressed, the system sends an alarm to the monitoring station of the security company, to users, and activates the **sirens** connected to the system.
- **Mute Interconnected Fire Alarm** — after the Function button is pressed, the system disables the fire alarm of FireProtect/FireProtect Plus detectors. The option works only if **Interconnected FireProtect Alarms** is enabled (Hub → Settings ⚙ → Service → Fire detectors settings).

Duress code

KeyPad Fibra supports **duress code**. It allows you to simulate alarm deactivation. Unlike the panic button, if this code is entered, the user will not be compromised by the **siren** sounding, and the keypad and **Ajax app** will inform about the successful disarming of the system. At the same time, the security company will receive an alarm.

The keypad supports both general and personal duress codes. You can set a personal code in the user settings. Each user sets this code individually.

Learn more

Unauthorized access auto-lock

If a wrong code is entered three times within 1 minute, the keypad will be locked for the time specified in the **settings**. During this time, the hub will ignore all codes, while simultaneously informing users of the security system about an attempt to guess the code.

An user or PRO with admin 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 can participate in two-stage arming. This process is similar to arming with a personal or general code on a keypad. The process must be completed either by re-arming using the SpaceControl second-stage device or by restoring the second-stage detector (returning to its original position).

KeyPad Fibra cannot act as a second-stage 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 two-way wired data transfer protocol that provides fast and reliable communication between the hub and the rest of the devices. Using the bus connection method, Fibra delivers alarms and events instantly, even if 100 detectors are connected to the system.

Fibra supports floating key block encryption and verifies each communication session with devices to prevent sabotage and forgery. 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 real time in the Ajax apps.

More about Fibra protocol (in progress)

Sending events to the monitoring station

The Ajax security system can transmit alarms to the **Ajax PRO Desktop** monitoring app as well as the central monitoring station (CMS) in the formats of the **Sur-Gard protocol (Contact ID)**, **SIA (DC-09)**, and other proprietary protocols. A complete list of supported protocols is **available here**.

Which CMSs can the Ajax security system be connected to

KeyPad Fibra can transmit the following events:

1. 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 / restoration of connection to the hub.
6. Temporary deactivation / activation of the device.
7. Unsuccessful attempt to arm the security system (with **Integrity Check** enabled).

When an alarm is received, the operator of the security company monitoring station knows exactly what happened and precisely where to send a fast response team on the site. Addressability of each Ajax device allows you to send not only events to the PRO Desktop or to the CMS but also the type of the device, the name of the device, and the virtual room to which the detector is assigned. Note that the list of transmitted parameters may differ depending on

the type of CMS and the selected protocol for communication with the monitoring station.

The device ID, the loop (zone) number, and the bus number can be found in its states in the Ajax app.

Detector placement

When choosing the place to install KeyPad Fibra, take into account the parameters that affect the correct operation of the keypad: Fibra signal strength and connection cable length.

Consider the placement recommendations when designing your facility's security system. Design and installation of the security system should be carried out by professionals. A list of authorized official Ajax partners is **available here**.

KeyPad Fibra is best placed indoors near the entrance. This allows disarming the system before the entry delay has expired, as well as quickly arming the system when leaving the premises.

When holding KeyPad Fibra in your hands or using it on a table, we cannot guarantee that the touch buttons will work properly.

It is a good practice to install the keypad **1.3–1.5 meters above the floor** for convenience. Install the device on a flat, vertical surface. For example, on the wall. This allows KeyPad Fibra to be firmly attached to the surface and to avoid false tamper triggering.

Design and preparation

For the system to work correctly, it is important to properly design the project and install all devices correctly. Failure to follow the basic installation rules and recommendations of this manual may result in detector malfunction, false alarms, or loss of connection with already installed devices.

When designing the layout scheme of the detectors, consider the wiring diagram of the power cables laid on the site. Signal cables must be laid at a distance of at least 50 cm from the power cables when lying parallel, and, if they intersect, it must be at a 90° angle. Note that, if you connect multiple devices on the same bus, detectors are connected in sequence.

The maximum number of connectable devices for the Hub Hybrid is 100 at the default settings.

How to calculate the number of connectable detectors (in progress)

For facilities that are under construction or renovation, cables are laid after the main wiring of the facility. Use protective tubes to route system cables to organize and secure the wires; ties, clips, and staples can be used to secure them.

When laying wires externally (without mounting them inside the walls), use an electric channel raceway. Raceways should be no more than half-filled with cables. Do not allow cables and wires to sag. The raceway should be hidden from view if possible — for example, behind furniture.

We recommend laying 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.

When selecting a cable, consider the length of the connection lines and the number of detectors to be connected; these parameters affect the signal strength. We recommend using shielded copper cables with a high-quality insulation layer.

When installing, observe the bend radius that the manufacturer specifies in the cable specs. Otherwise, you risk damaging or breaking the conductor.

Be sure to check all cables for bends and physical damage before installation. Perform the installation in a way that minimizes the possibility of damage to the cables from the outside.

Signal strength and wire length

The Fibra signal level is determined by the number of undelivered or corrupted data packages over a certain period. The icon on the **Devices** tab 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.

The signal strength is influenced by the following factors: the number of devices connected to one bus, the length and type of cable, and the proper connection of the wires to terminals.

Check the Fibra signal strength before final installation of the keypad. If the signal strength is as low as one or zero bars, we cannot guarantee stable operation of the device.

The maximum permissible cable length depends on its type, its material, and the method of connecting the devices. When connected using the **Star connection method** with a twisted pair U/UTP cat.5 (4×2×0.51), the wired connection length can be up to 2,000 meters.

When devices are connected using the **Ring connection method**, the maximum cable length is 500 meters when using a twisted pair.

How to calculate the wire connection length (in progress)

Connecting devices using the Ring connection method will be available with future OS Malevich updates. Hardware update of Hub Hybrid won't be required.

How OS Malevich updates

Do not install KeyPad

1. In places where parts of clothing (for example, next to the hanger), power cables, or Ethernet wire may obstruct the keypad. This can lead to the false triggering of the device.
2. Inside premises with temperature and humidity outside the permissible limits. This could damage the keypad.
3. In places where KeyPad Fibra has an unstable or low signal strength.
4. Outdoors. This could damage the keypad.

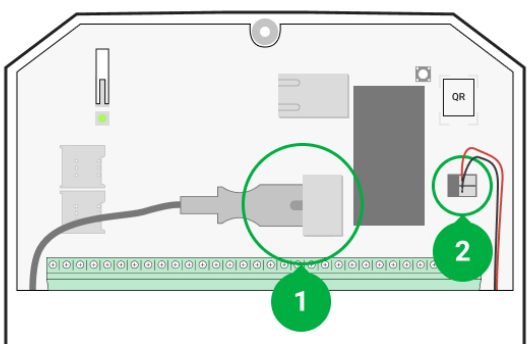
Installation and connection

> Before installing KeyPad Fibra, make sure that you have selected the optimal location and that it meets the requirements of this manual. Wires must be hidden from view and located in a place that is difficult for burglars to access to reduce the likelihood of sabotage. Ideally, the wires should be embedded in the walls, floor, or ceiling. Perform the Fibra signal strength test before final installation.

When connecting, do not twist the wires together; solder them. The ends of the wires that will be inserted into the keypad terminals should be tinned or crimped with special tips. This will ensure a reliable connection. **Follow safety procedures and regulations for electrical installation work**.

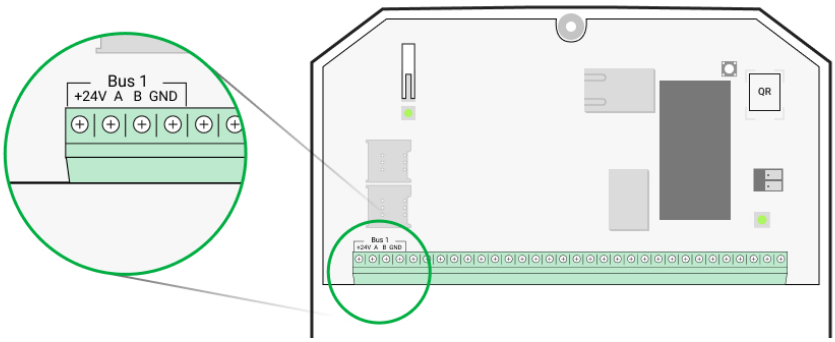
In order to install the keypad:

1. Disconnect the external power and the hub's backup battery.



1 — External power supply
2 — Backup battery

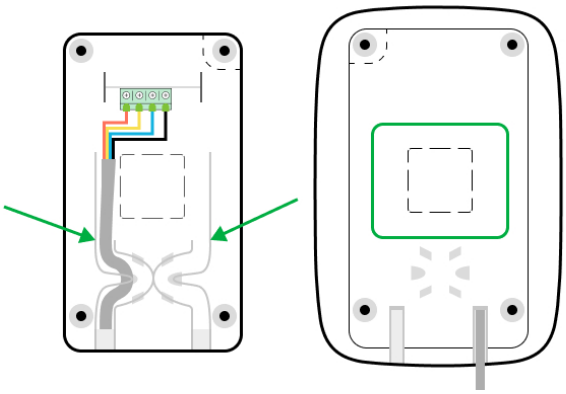
2. Plug the cable into the hub and connect the wires to the bus terminals.



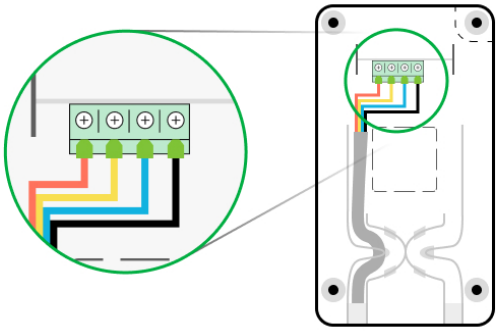
+24V — power supply input
A, B — signal terminals
GND — ground

3. Remove the SmartBracket mounting plate from the keypad.

4. Run the wires from the hub into the keypad body through the special channels on the SmartBracket mounting plate to lead the wire out from the bottom of the keypad. To lead the wire out from the back of the device, carefully break off the perforated part on the SmartBracket mounting plate.



5. 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. Secure the cable with ties.



6. 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.

7. If the detector is the last in the line, install a termination resistor at the end of the connecting line in case the **Star connection method** is in place. With the **Ring connection method**, a termination resistor is not required.

More about connection methods (in progress)

> We recommend connecting devices via the **Ring connection method** (hub – device – hub), because, if the line is broken, the devices will be connected via the **Star connection method** and will continue to transmit events to the hub. Notification about the **Ring** failure will be sent to users and the security company.

8. Temporarily secure the SmartBracket plate to a vertical surface using double-sided tape or other temporary fasteners at the chosen installation place. The recommended installation height is 1.3–1.5 meters above the floor.

9. Turn on the hub to supply the connected keypad with power. An LED of the keypad will notify that the device is turned on.

10. Add KeyPad Fibra to the system.

11. Conduct the Fibra signal strength test. The recommended signal strength value is two or three bars. Otherwise, check the connection and the condition of the wire.

12. Attach the SmartBracket mounting panel with at least two fixation points using bundled screws. Use one of them on the perforated part of the mount above the tamper. When using other fasteners, make sure they do not damage or deform the mounting panel.

Double-sided tape can only be used for temporary installation. The device attached by the tape may come unstuck from the surface at any time. As long as the device is taped, the tamper will not be triggered when the device is detached from the surface.

13. Place the keypad on the SmartBracket mounting plate and fix it with a screw.

Adding to the system

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

Types of accounts and their rights

Before adding a device

1. Install the **PRO version of the app**. Log in to a PRO **account** or create a new one if you don't have it yet. Add a hub compatible with the device to the app, make the necessary settings, and create at least one **virtual room**.
2. Make sure that the hub is turned 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.
3. Make sure the hub is disarmed and does not start updates by checking its status in the Ajax app.
4. Make sure the device is physically connected to the hub.

How to add KeyPad Fibra

There are two ways to add devices: manually and automatically.

To add a device manually:

1. Open the **PRO version of the app**. Select the hub you want to add KeyPad Fibra to.
2. Go to the **Devices** tab and click **Add Device**.
3. Name the keypad, scan or type in the QR code (placed on the device body and the packaging), select a room and a group (if the **group mode** is enabled).
4. Click **Add**.

To add the device automatically:

1. Open the **PRO version of the app**. Select the hub you want to add KeyPad Fibra to.
2. Go to the **Devices** tab and click **Add Device**.
3. Select **Add Bus Devices**. After scanning, a list of all devices physically connected to the hub, which have not yet been added to the system, will be displayed on the screen. The devices are sorted by the buses they are physically connected to.

To add a device:

1. Click on the device in the list.
2. Create a name.
3. Specify the room and the security group (if enabled).
4. Click **Save**.

If the device adds to the hub successfully, it will disappear from the list of available devices.

Device status updating depends on the Fibra settings; the default value is 36 seconds.

If the connection fails, check the accuracy of the wired connection and try again. If hub already has the maximum number of devices added (for Hub Hybrid, the default is 100), you will get an error notification when you add one.

KeyPad Fibra works with one hub only. When connected 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 through the Ajax app.

Malfunctions

When a keypad malfunction is detected (for example, there is no connection via the Fibra protocol), the Ajax app displays a malfunction counter in the upper left corner of the device icon.

All malfunctions can be seen in the keypad states. Fields with malfunctions will be highlighted in red.

Malfunction is displayed if:

- The keypad temperature is out of acceptable limits.
- The keypad body is open (tamper is triggered).
- There is no connection with the hub via the Fibra protocol.

Icons

The icons represent some of KeyPad Fibra states. You can see them in the **Devices** tab in the Ajax app.

Icon	Meaning
	Fibra signal strength — displays the signal strength between the hub and the keypad. Learn more (in progress)
	KeyPad Fibra is temporarily deactivated by a user or PRO with administrator rights. **Learn more**
	KeyPad Fibra has tamper triggering events temporarily deactivated by a user or PRO with administrator rights.

Learn more

States

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

1. Go to the **Devices** tab.
2. Choose KeyPad Fibra from the list.

Parameter	Meaning
Malfunction	Clicking on opens a list of malfunctions of KeyPad Fibra. The field is displayed if a malfunction is detected.
Temperature	Detector temperature — it is measured on the processor and changes gradually. Acceptable measurement error between the value in the app and the room temperature: 2–4°C. The value is updated as soon as the detector identifies a temperature change of at least 1°C.
Fibra signal strength	Signal strength between the hub and KeyPad Fibra. Recommended values — 2–3 bars. Fibra — protocol for transmitting KeyPad Fibra events and alarms Learn more (in progress)
Connection via Fibra	Status of the connection between the hub and the keypad: • **Online** — the keypad is connected to the hub. • **Offline** — the keypad is not connected to the hub. Check the wired connection.

Bus voltage	Bus voltage value.
Lid	The status of the tamper that responds to demount or opening of the body: • **Open** — the keypad is removed from its SmartBracket mounting plate. • **Closed** — the keypad is fixed to the SmartBracket mounting plate. Learn more
Temporary deactivation	Shows the status of the device temporary deactivation function: • **No** — the device operates normally and transmits all events. • **Lid only** — the hub administrator has disabled notifications about triggering on the device tamper. • **Entirely** — the hub administrator has entirely excluded the keypad from the system. The device does not execute system commands and does not report alarms or other events. • **By number of alarms** — the device is automatically disabled when the number of alarms is exceeded (specified in the Devices Auto Deactivation settings). Learn more
Firmware	Keypad firmware version.
ID	Keypad ID. Also available on the keypad body and packaging.
Device №	Keypad loop (zone) number.
Bus №	The number of the hub bus the keypad is connected to.

Settings

To change the keypad settings in the Ajax app:

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

Settings	Meaning
First field	Keypad name. Displayed in the list of hub devices, SMS text, and notifications in the events feed. To change the keypad name, click on the pencil icon. The name can contain up to 12 Cyrillic characters or up to 24 Latin characters.
Room	Selecting the virtual room to which KeyPad Fibra is assigned. The room name is displayed in the text of SMS and notifications in the event feed.
Group security management	Selecting the security group controlled by the keypad. You can select all groups or just one. The field is displayed if the **Group mode** is enabled.
Access Settings	Selecting the method of arming/disarming: • Keypad code only • User passcode only • Keypad and user passcode
Keypad code	Selecting a general code for security control. Contains 4 to 6 digits.
Duress code	Selecting a general duress code (“silent alarm”). Contains 4 to 6 digits.

	Learn more
Function button	Selecting the function of the * button (Function button): • **Off** — the Function button is disabled and does not execute any commands when pressed. • **Alarm** — operates as a panic button: after the Function button is pressed, the system sends an alarm to the security company monitoring station and to all users. • **Mute Interconnected Fire Alarm** — when pressed, disables the fire alarm of FireProtect / FireProtect Plus detectors. This option functions only if **Interconnected FireProtect Alarms** is enabled. Learn more
Arm without code	The option allows you to arm the system without entering a code. To do this, just click on the **Arm** or **Night mode** button.
Unauthorized Access Auto-lock	When the option is active, the keypad is locked for the pre-set time if an incorrect code is entered more than 3 times in a row within 1 minute. It is not possible to disarm the system using the keypad during this time. You can unlock the keypad through the Ajax app.
Auto-lock Time, min	Selecting the keypad lock period after wrong passcode attempts: • 3 minutes • 5 minutes • 10 minutes • 20 minutes • 30 minutes • 60 minutes • 90 minutes

	• 180 minutes The keypad is locked for a pre-set time if an incorrect code is entered more than 3 times in a row within 1 minute. It is not possible to disarm the system using the keypad during this time. You can unlock the keypad through the Ajax app. The field is displayed when the **Unauthorized Access Auto-lock** option is enabled.
Brightness	Selecting the brightness of the keypad buttons backlight: **from 0 to 5** (0 — backlight is off, 5 — very bright backlight). The backlight is on only when the keypad is active. This option does not affect the brightness level of the security mode indicators.
Buttons Volume	Selecting the volume level of the keypad buttons when pressed: **from 0 to 14** (0 — the sound of pressing is disabled, 14 — very loud sound of pressing).
Alert with a siren if panic button is pressed	The field is displayed if the **Alarm** option is selected for the Function button. When the option is enabled, the **sirens** connected to the security system give an alert when the * button (Function button) is pressed.
Fibra signal strength test	Switches the keypad to the Fibra signal strength test mode. 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. Learn more (in progress)
User Manual	Opens the KeyPad Fibra User Manual in the Ajax app.
Temporary deactivation	Allows to disable the keypad without removing

	it from the system. Two options are available: • **Entirely** — the keypad will not execute commands or participate in automation scenarios. The system will ignore alarms and other notifications from the keypad. • **Lid only** — the system will ignore notifications about the tamper triggering. Learn more
Unpair Device	Unpairs keypad from the hub and deletes its settings.

Adding a personal code

Both general and personal user codes can be set for the keypad. A personal code applies to all Ajax keypads installed at the facility. A general code is set for each keypad individually and can be different or the same as the codes of other keypads.

To set a personal code in the Ajax app:

1. Go to the **User profile settings** (Hub → Settings → Users → Your profile settings).
2. Select **Passcode Settings** (User ID is also visible in this menu).
3. Set **User Code** and **Duress Code**.

Each user sets a personal code for their device individually. The administrator cannot set a code for all users.

Security management by codes

You can manage the **Night mode**, security of the entire facility or separate groups using general or personal codes. The keypad allows you to use 4 to 6 digit codes. Incorrectly entered numbers can be cleared with the button C.

If a personal code is used, the name of the user who armed or disarmed the system is displayed in the hub events feed and in the notifications.

If a general code is used, the name of the user who changed the security mode is not displayed.

Arming with a personal code
In progress
Arming with a general code
In progress

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

Security management of the facility using a general code

1. Activate the keypad by touching any button.
2. Enter the **general code**.
3. Press the Arm / Disarm / Night mode button.

For example: 1234 →

Security management of the group using a general code

1. Activate the keypad by touching any button.
2. Enter the **general code**.
3. Press the * (Function button).
4. Enter the **Group ID**.
5. Press the Arm / Disarm / Night mode button.

For example: 1234 → * → 2 →

What is Group ID

If a security group is assigned to KeyPad Fibra (in the **Group management** field in the keypad settings), you do not need to enter the group ID. To manage the security mode of this group, entering a general or personal code is sufficient.

If a group is assigned to KeyPad Fibra, you will not be able to manage **Night mode** using a general code. In this case, **Night mode** can only be managed using a personal code if the user has the appropriate rights.

Rights in the Ajax security system

Security management of the facility using a personal code

1. Activate the keypad by touching any button.
2. Enter the **User ID**.
3. Press the * (Function button).
4. Enter **your personal code**.
5. Press the Arm / Disarm / Night mode button.

For example: 2 → * → 1234 →

What is User ID

Security management of the group using a personal code

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

6. Enter the **Group ID**.
7. Press the Arm / Disarm / Night mode button.

For example: 2 → * → 1234 → * → 5 →

If a group is assigned to KeyPad Fibra (in the **Group management** field in the keypad settings), you do not need to enter the group ID. To manage the security mode of this group, entering a personal code is sufficient.

What is Group ID

What is User ID

Using a duress code

A duress code allows you to simulate alarm deactivation. The user will not be exposed, since the sirens installed at the facility and the siren in the Ajax app will not raise the alarm, but the security company and other users will be warned of the incident. You can use both a personal and a general duress code.

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

Learn more

To use a general duress code

1. Activate the keypad by touching any button.
2. Enter the **general duress code**.
3. Press the disarming button .

For example: 4321 →

To use a personal duress code

1. Activate the keypad by touching any button.

2. Enter the **User ID**.
3. Press the * (Function button).
4. Enter the **personal duress code**.
5. Press the disarming button .

For example: 2 → * → 4422 →

Mute Fire Alarm function

KeyPad Fibra can disable Interconnected FireProtect alarms by pressing the Function button (if the corresponding setting is enabled). The response of the system to pressing a button depends on the settings and the state of the system:

- **Interconnected FireProtect Alarms have already propagated** — the first press of the Function button mutes all sirens of the fire detectors, except for those that registered the alarm. Pressing the button again mutes the remaining detectors.
- **Interconnected alarms delay time lasts** — pressing the Function button mutes the siren of the triggered FireProtect/FireProtect Plus detector.

Keep in mind that this function works only if Interconnected FireProtect Alarms is enabled in the hub settings.

Learn more

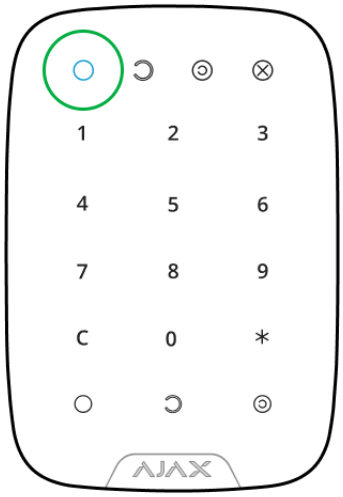
With the OS Malevich 2.12 update, users can mute fire detector alarms in their groups without affecting detectors in the groups to which they do not have access.

Learn more

Indication

KeyPad Fibra can report the current security mode, keystrokes, malfunctions, and its status by LED indication and 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 device (SpaceControl or another KeyPad) or an app.



To activate the keypad, touch any button on the panel. When activated, the keypad turns on the backlight and beeps (if enabled).

Event	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 security 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**) light.	
The keypad is locked due to an attempt to guess a code.	Long beep, security status indicators and keypad backlight blink 3 times.	

Functionality testing

The Ajax security system provides several types of tests that help you make sure that installation points of devices are selected correctly. Tests do not start straight away but begin no later than a single hub-detector ping period (36 seconds under default settings of the hub). You can change the ping period of devices in the **Fibra** menu of the hub settings.

Fibra Signal Strength Test is available for KeyPad Fibra.

To run a test, in the Ajax app:

1. Select the hub if you have several of them or if you are using a PRO app.
2. Go to the **Devices** menu.
3. Select KeyPad Fibra.
4. Go to **Settings**.
5. Select **Fibra Signal Strength Test**.
6. Launch and conduct a test.

Maintenance

Check the functioning of your keypad on a regular basis. This can be done once or twice a week. Clean the body from dust, cobwebs, and other contaminants as they emerge, after turning off the keypad to avoid false alarms due to wrong code attempts. Use a soft dry cloth that is suitable for equipment care.

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

Technical specifications

Learn more

Compliance with standards

Complete set

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

Warranty

Warranty for the AJAX SYSTEMS MANUFACTURING Limited Liability Company 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 of the cases, technical issues can be resolved remotely.

Warranty obligations

User Agreement

Contact Technical Support:

- **e-mail**
- **Telegram**

Subscribe to the newsletter about safe life. No spam

Email

Subscribe