Superior KeyPad Outdoor Fibra user manual

Updated March 16, 2025

Superior KeyPad Outdoor Fibra is a wired keypad designed to manage the Ajax system. Users can authenticate using smartphones, Tag key fobs, Pass cards, and codes. The device is intended for outdoor and indoor use and complies with EN 50131 (Grade 3) requirements.
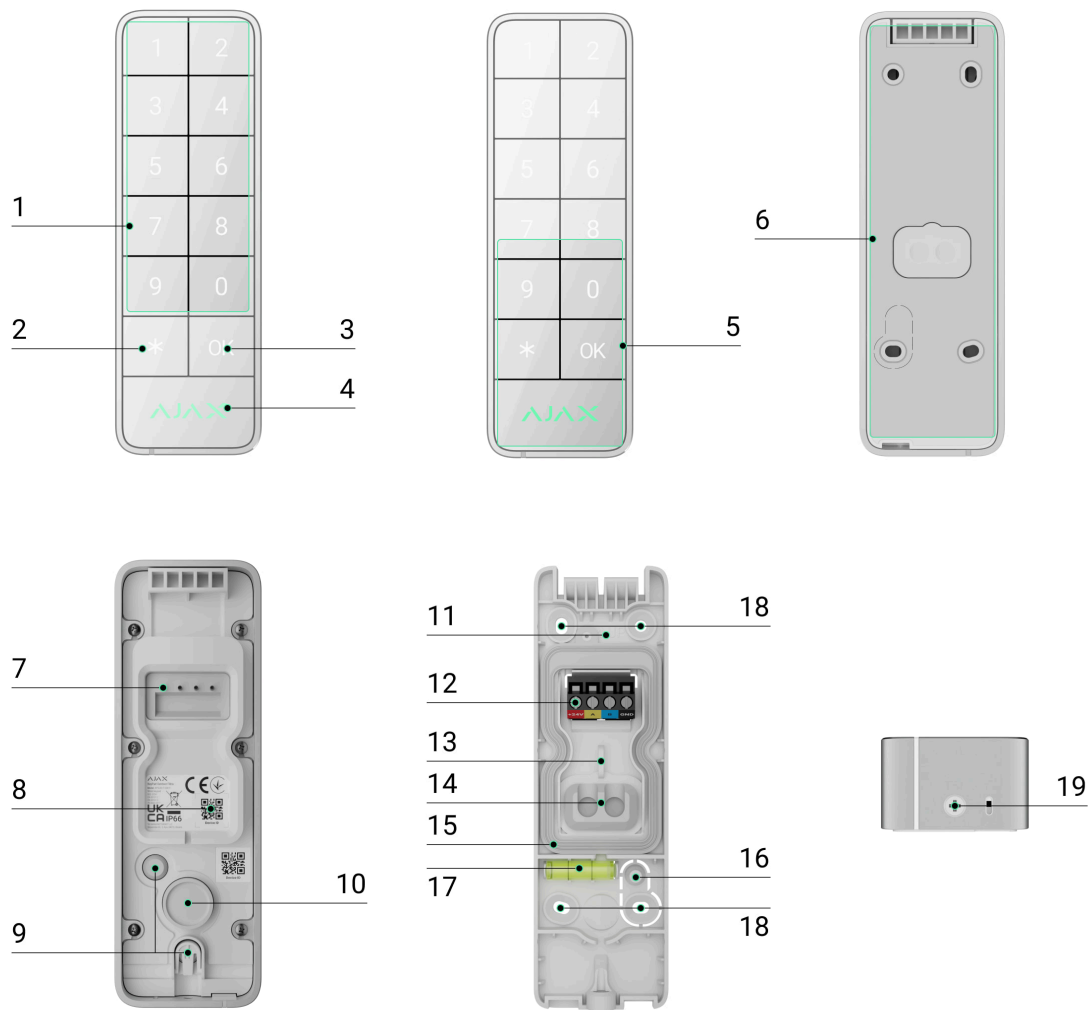
The keypad operates in the Ajax system and exchanges data with the hub using the secure Fibra wired communication protocol.

Learn more

Superior KeyPad Outdoor Fibra is a part of the Superior product line. Only accredited Ajax Systems partners can sell, install, and administer Superior products.

Buy Superior KeyPad Outdoor Fibra

Functional elements

1. Numpad.

2. Function button.

3. OK button with an LED indicator.

4. Ajax logo with an LED indicator.

5. Cards/key fobs/Bluetooth reader.

6. SmartBracket mounting panel. To remove the panel, unscrew the holding screw.

7. Pins for connecting the device to the input terminals on SmartBracket.

8. QR code with the device ID. It is used to add the device to the hub.

9. Tamper buttons.

10. Built-in buzzer.

11. **UP** key, which indicates the top of the keypad.

12. Input terminals for connecting the Fibra line to Superior KeyPad Outdoor Fibra.

13. Fastener to fix the cables with ties.

14. Rubber sealing plug for routing cables from the back of the device.

15. Rectangular rubber sealing ring. Protects the device against water. Do not remove it.

16. Perforated part of the mounting panel. Triggers a tamper in case of any attempt to detach the device from the surface. Do not break it off.

17. Bubble level to check the inclination angle of the mount during installation.

18. Holes to attach SmartBracket to the surface.

19. Holding screw to secure the keypad on SmartBracket.

Compatible hubs

An Ajax hub with the firmware **OS Malevich 2.28** and later is required for the keypad to operate.

Check device compatibility

Operating principle

Superior KeyPad Outdoor Fibra features large mechanical buttons, a reader for contactless authorization, a built-in buzzer, and LED indicators. The keypad is used to control security modes and automation devices and to notify of system events via sound and LED indication.

Superior KeyPad Outdoor Fibra features **primary** and **secondary** operating modes. You can set up one keypad function for each mode and switch between modes with a long press of the **OK** button.

The lower part of the keypad front side features a reader for contactless authorization so that you can present Tag, Pass, or a smartphone directly to the Ajax logo or buttons.

Depending on the settings, the Superior KeyPad Outdoor Fibra built-in buzzer notifies of the following:

- alarms;

- security mode changes;

- entry/exit delays;

- triggering of opening detectors;

- malfunctions.

Keypad operating modes and functions

Superior KeyPad Outdoor Fibra features two operating modes: **primary** and **secondary**. You can configure each mode independently in the keypad **settings** in Ajax apps. For each operating mode, you can set only one keypad function and switch between modes with a long press of the **OK** button on the keypad.

Also, you can disable the secondary operating mode if you do not need it.

There are three keypad functions that can be set up for each keypad operating mode:

- **Switch armed mode**. With this function, users can arm/disarm the entire site or specific groups or activate **Night mode**.

- **Manage automation devices**. With this function, users can create a scenario with one or multiple automation devices that can be controlled directly from the keypad.

- **Start entry delay**. With this function, users can use Superior KeyPad Outdoor Fibra as a **bypass keypad** to activate an entry delay so they can disarm the site using the main keypad.

> ⚠️ Only one primary function and one secondary function can be set at once.

Superior KeyPad Outdoor Fibra shows which mode is currently active by LED indication depending on the configured function:

- **Switch armed mode** — the Ajax logo lights up red or green, depending on the system security state. The **OK** button lights up white, as do the number buttons.

- **Manage automation devices** — the **OK** button lights up red or green, depending on the automation device state. The Ajax logo LED is off. If the keypad controls a scenario with multiple automation devices, the scenario's state is unavailable on the keypad.

- **Start entry delay** — the Ajax logo lights up red when the site is armed and flashes red simultaneously with beep when the entry delay is started. The **OK** button lights up white, as do the number buttons.

Learn more

Security control

Superior KeyPad Outdoor Fibra can arm and disarm the entire site or specific groups and activate **Night mode**. Users can control the security using Superior KeyPad Outdoor Fibra through:

1. **Cards or key fobs**. To quickly and securely identify users, Superior KeyPad Outdoor Fibra uses the DESFire® technology. DESFire® is based on the ISO 14443 international standard and combines 128-bit encryption and copy protection. Tag and Pass support this technology and are compatible with Superior KeyPad Outdoor Fibra.

2. **Smartphones**. With the installed <u>Ajax Security System</u> app and Bluetooth Low Energy (BLE) support. Smartphones can be used instead of Tag or Pass for user authorization. BLE is a low-power consumption radio protocol. The keypad supports Android and iOS smartphones with BLE 4.2 and later.

3. **Codes**. Superior KeyPad Outdoor Fibra supports general codes, personal codes, and codes for unregistered users.

Access codes

- **Keypad code** is a general code set up for the keypad. When used, all events are sent to Ajax apps on behalf of the keypad.

- **User code** is a personal code set up for users connected to the hub. When used, all events are sent to Ajax apps on behalf of the user.

- **Keypad access code** is a code set up for a person who is not registered in the system. When used, events are sent to Ajax apps with a name associated with this code.

- **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.

> ℹ️ The number of personal codes, keypad access codes, and RRU codes depends on the hub model.
>
> <u>Check device compatibility</u>

Access rights and codes can be adjusted in Ajax apps. If the code is compromised, it can be changed remotely, so there is no need to call an installer to the site. If a user loses their Pass, Tag, or a smartphone, an admin or a PRO with system configuration rights can instantly block the device in the app. Meanwhile, a user can use a personal code to control the system.

Security control of the groups

Superior KeyPad Outdoor Fibra allows controlling the groups' security (if **Group mode** is enabled). An admin or PRO with the rights to configure the system can also adjust the keypad **settings** to determine which groups will be shared (keypad groups). You can learn more about group security management in **this section**.

Function button

Superior KeyPad Outdoor Fibra has the **Function** button (✳) that operates in one of three modes:

- **None** — the **Function** button is disabled, and nothing happens when the user presses this button shortly.

- **Panic** — after the **Function** button is pressed, the system sends an alarm to the security company monitoring station and all users.

- **Mute fire alarm** — after the **Function** button is pressed, the system mutes the alarm of Ajax fire detectors. Available only if an **Interconnected fire detectors** alarm feature is enabled (Hub → Settings ⚙ → Service → Fire detectors settings).

Also, incorrectly entered codes can be cleared with a long press of the **Function** button if no other action is set up for a long press.

Duress code

Superior KeyPad Outdoor Fibra supports a **duress code** that allows a user to simulate alarm deactivation. In this case, neither the **Ajax app** nor the **sirens** installed at the facility will reveal your actions. Still, the security company and other security system users will be alerted about the incident.

Learn more

Start entry delay (a bypass keypad)

The **Start entry delay** feature (i.e., a bypass keypad) is designed to activate an entry delay before the site is disarmed using the main keypad.

Bypass technology provides temporary deactivation of security detectors, such as opening detectors and others. This allows users to get more time from the moment they enter an area until they can disarm the site with the main control device (e.g., **Superior KeyPad TouchScreen Fibra**).

Learn more

Unauthorized access auto-lock

If an incorrect code is entered or a non-verified access device is used three times in a row within 1 minute, the keypad will lock for the time specified in its settings. During this time, the hub will ignore all codes and access devices while informing the security system users about attempted unauthorized access.

PRO or a user with system configuration rights can unlock the keypad through the app before the specified locking time expires.

Two-stage arming

Superior KeyPad Outdoor Fibra can participate in two-stage arming but cannot be used as a second-stage device. The two-stage arming process using Tag, Pass, or a smartphone is similar to using a personal or general code on the keypad.

Learn more

Automation devices and scenarios management

Superior KeyPad Outdoor Fibra has the **Manage automation devices** feature designed to control one or multiple automation devices. For

example, a user can open garage doors or turn off all smart light switches at the site.

When the keypad controls one automation device, it shows the device's state with LED indication of the **OK** button. When the **OK** button is green, an automation device is active; when it is red, an automation device is inactive.

When the keypad controls a scenario with multiple automation devices, the keypad cannot show the state of the device or scenario. Instead, it indicates whether the set action is completed or not.

> **i** Superior KeyPad Outdoor Fibra can manage only one scenario.

Managing automation devices is available only after authorization on the keypad.

Indication of security mode and automation devices state

Superior KeyPad Outdoor Fibra informs users about system security mode and automation device state by means of:

- the logo with LED indication;

- the **OK** button with LED indication;

- sound indication.

If the keypad is in **Switch armed mode**, the Ajax logo lights up green or red to notify of the system's security mode state.

If the keypad is in the **Manage automation devices** mode, the **OK** button lights up green or red to notify of the automation device's state. But when the keypad manages a scenario with multiple automation devices, it cannot notify of the scenario's state.

The built-in buzzer notifies of alarms, door openings, and entry/exit delays.

Refer to the **Indication** section for more information.

Fire alarm muting

Superior KeyPad Outdoor Fibra can mute an interconnected fire alarm by pressing the **Function** button (if the required setting is enabled). The reaction of the system to pressing the button depends on the settings and the state of the system:

- **Interconnected fire detectors alarm have already propagated** — by the first press of the button, all sirens of the fire detectors are muted, except for those that registered the alarm. Pressing the button again mutes the remaining detectors.

- **Interconnected alarms delay time lasts** — by pressing the **Function** button, the siren of the triggered Ajax fire detectors is muted.

Remember that the option is available only if **Interconnected fire detectors alarm** is enabled.

Learn more

Fibra data transfer protocol

The device uses Fibra technology to transmit alarms and events. It is a wired data transfer protocol for fast, reliable two-way communication between the hub and connected devices.

Learn more

Sending events to the monitoring station

The Ajax system can transmit alarms to the PRO Desktop monitoring app as well as the central monitoring station (CMS) in the formats of **SurGard**

(Contact ID), SIA (DC-09), ADEMCO 685, and **other protocols**.

Superior KeyPad Outdoor Fibra can transmit the following events:

1. Arming/disarming the system.

2. Entry of the duress code.

3. Pressing the panic button.

4. Keypad locking due to an unauthorized access attempt.

5. Unsuccessful attempt to arm the security system (with the **system integrity check** enabled).

6. Tamper alarm. Tamper recovery.

7. Low supply voltage on the Fibra line and voltage return to normal values.

8. Loss and restoration of connection with the hub.

9. Permanent deactivation/activation of the device.

10. One-time deactivation/activation of the device.

When an alarm is received, the operator of the security company monitoring station knows what happened and precisely where to send a fast response team. The addressability of Ajax devices allows sending events to the **PRO Desktop** or the CMS the type of the device, its name, security group, and virtual room. The list of transmitted parameters may differ depending on the type of CMS and the selected communication protocol.

> (i) You can find the device ID, loop (zone) number, and line number in the device states.

Selecting the installation site

When choosing where to place Superior KeyPad Outdoor Fibra, consider the parameters that affect its operation:

- **Fibra signal strength**.

- **The length of the cable** for connecting the keypad.

Consider the recommendations for placement when developing a project for the system of the facility. The Ajax system must be designed and installed by specialists. A list of recommended partners is **available here**.

Superior KeyPad Outdoor Fibra is best placed outdoors or indoors near the entrance. This allows users to disarm the site before entering the premises or until the entry delays expire. Users can also quickly arm the site when leaving the premises.

Superior KeyPad Outdoor Fibra has a protected enclosure, so the keypad can be installed in public places, such as restaurants, hospitals, offices, or at production plants in severe conditions.

The recommended installation height is 1.3–1.5 meters above the floor. Install the keypad on a flat, vertical surface. This ensures Superior KeyPad Outdoor Fibra is securely attached to the surface and helps avoid false tamper alarms.

Fibra signal strength

Fibra signal strength is the ratio of undelivered or corrupted data packages to those expected over a specific time. The icon ıl 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.

    What is Fibra signal strength test

Lines power test

The test simulates the maximum energy consumption of devices connected to the hub. If the system passes the test successfully, all its devices have enough power in any situation. After the test, the app displays a notification with the status of each line:

- Test passed.

- Test passed with malfunctions.

- Test failed.

What is Lines power test

Do not install the keypad

1. In places where power or Ethernet cables, decor items, or other things may obstruct the keypad.

2. In places with temperature and humidity outside the permissible limits. This could damage the device.

3. In places where the acoustic signal can be attenuated (inside furniture, behind thick curtains, etc.).

4. Near the glass break detectors. The built-in buzzer sound may trigger an alarm.

5. In places with low or unstable Fibra signal strength.

Designing and preparing

It is crucial to properly design the system project to install and configure the devices correctly. The project must consider the number and types of devices at the site, their exact location and installation height, the length of wired Fibra lines, the cable type, and other parameters.

Tips for designing the Fibra system project

Cable length and type

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

Recommended cable types for connecting Superior KeyPad Outdoor Fibra to the hub:

- U/UTP cat.5, 4 × 2 × 0.51 mm (24 AWG), copper conductor.

- Signal cable 4 × 0.22 mm², copper conductor.

> ⓘ The wired connection range may vary if you use a different cable type. No other types of cables have been tested.

Verification using a calculator

Use the **Fibra power supply calculator** to ensure that the project is designed correctly and the system will work in practice. It helps to check the communication quality and cable length for wired Fibra devices when designing the system project.

Preparing for installation

Cable arrangement

When preparing to lay cables, check the electrical and fire safety regulations in your region. Strictly follow these standards and regulations. Tips for cable arrangement are available in **the article**.

Cable routing

We recommend you carefully read the **Selecting the installation site** section before installation. Do not deviate from the system project. Violating the basic Superior KeyPad Outdoor Fibra installation rules and the recommendations of this manual may lead to incorrect operation and loss of connection with the device. Tips for cable routing are available in **the article**.

Preparing cables for connection

Remove the insulating layer and strip the cable with a special insulation stripper. The ends of the wires inserted into the device terminals must be tinned or crimped with a sleeve. It ensures a reliable connection and protects the conductor from oxidation. Tips for preparing the cables are available in **the article**.

Installation and connection

> ⚠️ Before installing **Superior KeyPad Outdoor Fibra**, ensure that the optimal keypad location has been selected and meets the requirements of this manual. Cables must be hidden from view and located in a difficult place for intruders to access to reduce the likelihood of sabotage. Ideally, mount them in the walls, floor, or ceiling. Before final installation, run the Fibra signal strength test.

To mount a keypad:

1. Turn off the power of lines in the **Ajax PRO app**:

   - Hub → Settings ⚙ → Lines → Lines power supply

2. Route the cable to connect Superior KeyPad Outdoor Fibra to the hub casing. Connect the wires to the required hub line.
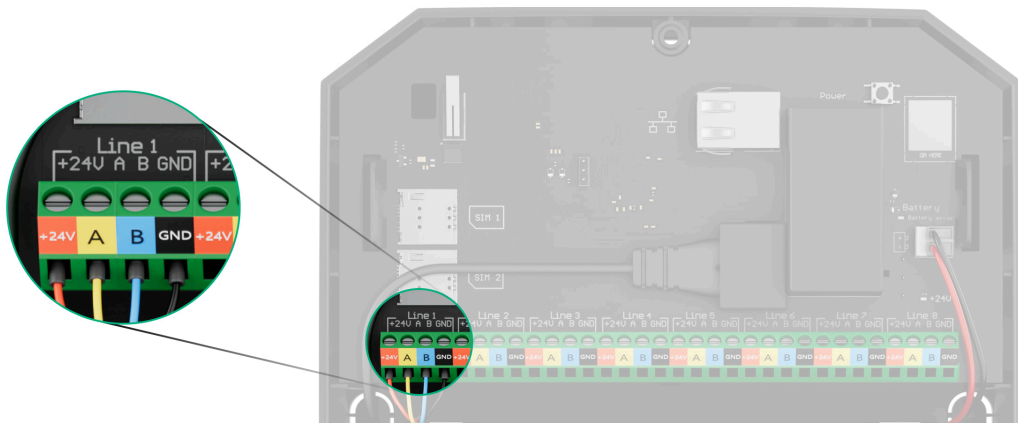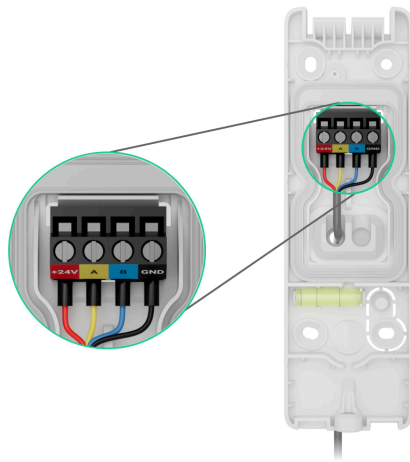
+24V — 24 V⎓ power terminal.

A, B — signal terminals.

GND — ground.

3. Unscrew the holding screw at the bottom of the device and remove the SmartBracket mounting panel from the keypad.

4. Make one or two holes in the rubber sealing plug in the recesses, considering the number of cables.
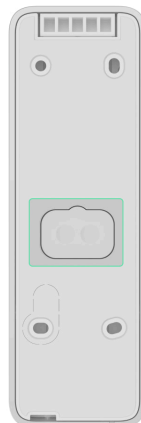
5. Run the cable from the hub into the keypad enclosure through the hole that was made.

6. Connect the wires to the terminals according to the figure below. Ensure the correct polarity and order of the wire connections. Firmly secure the cable to the terminals.

+24V — 24 V⎓ power terminal.
A, B — signal terminals.
GND — ground.

1. If the device is not the last one 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.
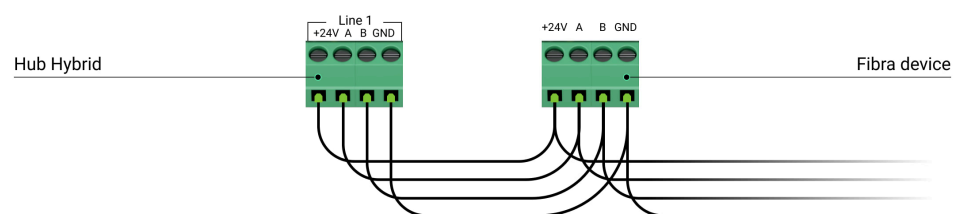
2. If Superior KeyPad Outdoor Fibra is the last device on the line and you are using the **Beam (Radial) connection**, install a terminating resistor on the two contacts by connecting it to the signal terminals of the device. Terminating resistor (120 Ohm) is included in the hub complete set. When the **Ring connection** is used, a terminating resistor is not needed.

| Hub Hybrid | Line 1
+24V A B GND | +24V A B GND | Fibra device |

Terminating resistor
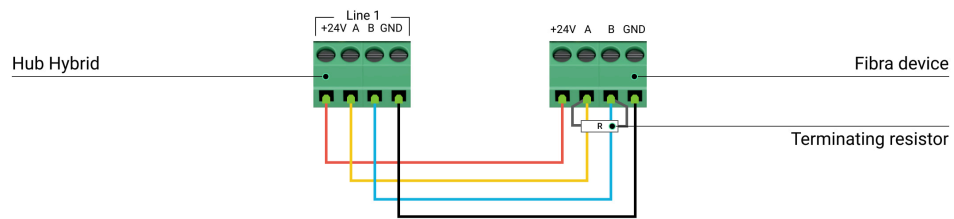
> ℹ️ We recommend using the **Ring connection** method (hub–device–hub). If the ring is broken, not a single device will be disabled. In this case, two beams are formed, which will continue to operate normally and transmit events to the hub. If the ring is broken, the users and the security company receive a notification.

7. Temporarily secure the SmartBracket panel using double-sided adhesive tape or other temporary fasteners.

> ⚠️ Double-sided adhesive 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.

SmartBracket has the **UP** key that indicates the top of the keypad. Consider it when installing the device.
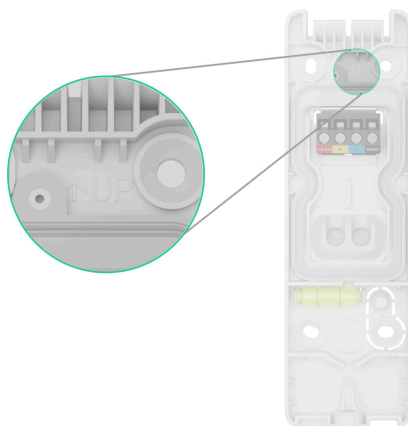
8. Place the keypad on the SmartBracket mounting panel.

9. Turn on the power supply of lines in the **Ajax PRO app**:

- Hub → Settings ⚙ → Lines → Lines power supply

10. The device LED indicator will flash. It is a signal indicating that the enclosure of the keypad is closed.

> ⚠️ If the LED indicator doesn't light up during placing on SmartBracket, check the tamper status in the Ajax app, the integrity of the fastening, and the tightness of the keypad fixation on the panel.

11. **Add the keypad to the system**.

12. Run the **functionality testing**.

13. If the tests are passed successfully, remove the keypad from SmartBracket.

14. Fix the SmartBracket panel on the surface with bundled screws. Use all fixing points.

> ℹ️ When using other fasteners, ensure they do not damage or deform the panel.

15. Place the keypad on the SmartBracket mounting panel.

16. Tighten the holding screw on the bottom of the keypad's enclosure. The screw is needed for more reliable fastening and protection of the keypad from quick dismantling. Also, the screw has a tamper that responds if someone tries to unscrew the holding screw. The system will send a notification of tamper triggering to Ajax apps and the CMS.
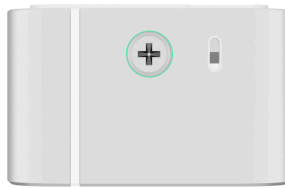
Adding to the system

> ⚠️ **Check the device compatibility** before the keypad is added to the system. Only verified partners can add and configure Superior devices in **Ajax PRO apps**.
>
> **Types of accounts and their rights**

Before adding a device

1. Install an **Ajax PRO app**.

2. Log in to a **PRO account** or create a new one.

3. Select a **space** or create a new one.

4. Add at least one **virtual room**.

5. Add a **compatible hub** to the space. Ensure the hub is switched on and has internet access via Ethernet and/or mobile network.

6. Ensure the space is disarmed, and the hub is not starting an update by checking statuses in the Ajax app.

Adding to the hub

Two ways to add devices are available in the **Ajax PRO app**: automatically and manually.

Automatically   Manually

To add a device automatically:

1. Open the <u>Ajax PRO app</u>. Select the hub to which you want to add Superior KeyPad Outdoor Fibra.

2. Go to the **Devices** ⬛ tab and tap **Add device**.

3. Select **Add all Fibra devices**. The hub will scan the Fibra lines. After scanning, all devices connected to the hub that still need to be added to the system will be shown.

> ℹ️ Scanning is also available in the **Lines** menu:
>
> **Hub → Settings**   **→ Lines → Add all Fibra devices**.

4. Select the device from the list. After pressing, the LED indicator will flash to identify this device.

5. Set the device name, and specify the room and security group if <u>Group mode</u> is enabled.

6. Tap **Save**.

The device connected to the hub will appear in the list of hub devices in the Ajax app.

If the connection fails, check the wired connection's correctness and try again. If the maximum number of devices has already been added to the hub, you will receive an error notification while adding.

> ⚠️ Superior KeyPad Outdoor Fibra features a built-in buzzer that can notify of alarms and specific system states, but it is not a siren. You can add up to 10 such devices (including sirens) to the hub. Consider this when planning your security system.

Once added to the hub, the keypad will appear in the list of hub devices in the Ajax app. The update frequency for device statuses in the list depends on the **Jeweller/Fibra** settings, with the default value of 36 seconds.

> **i** Superior KeyPad Outdoor Fibra works with only one hub. When paired with a new hub, it stops sending events to the old one. Adding the keypad to a new hub does not automatically remove it from the device list of the old hub. This must be done through the Ajax app.

Functionality testing

The Ajax system offers several types of tests to help select the correct installation place for the devices. The **Fibra signal strength test** is available for Superior KeyPad Outdoor Fibra. This test determines the strength and stability of the signal at the device installation site.

To run a test, in the Ajax app:

1. Select the required space.

2. Go to the **Devices** ⬛ tab.

3. Select **Superior KeyPad Outdoor Fibra** in the list.

4. Go to **Settings** ⚙.

5. Run the **Fibra signal strength test**.

Icons
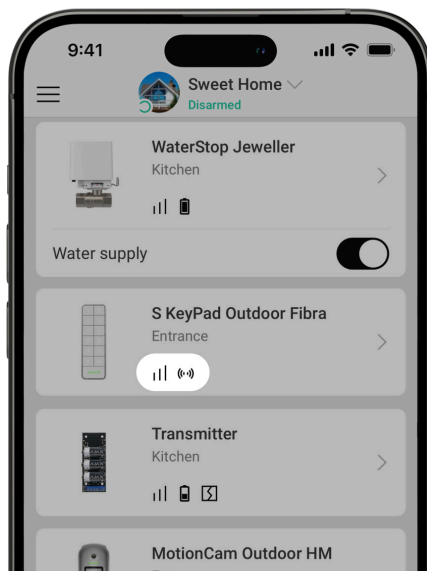
Icons in the Ajax app display some of Superior KeyPad Outdoor Fibra states. Icons can be checked in the **Devices** ⊟ tab.

Icon	Meaning
ılı	Fibra signal strength — displays the signal strength between the hub and the device. Recommended values: 2–3 bars. **Learn more**
(((•)))	**Pass/Tag reading** is enabled in keypad settings.
⚹	**Bluetooth** is enabled in keypad settings.
⚠	Bluetooth setup is not complete. The description is available in the keypad states.
🔔	**Chime on opening** is enabled in keypad settings.
🔓	The mounting panel is unlocked.
⚙	The device is permanently deactivated. **Learn more**

⟳ (icon)	Tamper alarm notifications are permanently deactivated. **Learn more**
⚙ (icon)	The device is deactivated until the site is disarmed for the first time. **Learn more**
⟳① (icon)	Tamper alarm notifications are deactivated until the site is disarmed for the first time. **Learn more**
Offline	The device has lost connection with the hub or the hub has lost connection with the Ajax Cloud server.
Not transferred	The device has not been transferred to the new hub. **Learn more**

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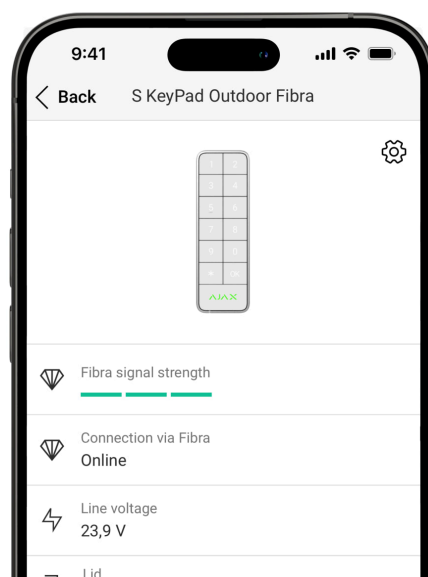
The states include information about the device and its operating parameters. The states of Superior KeyPad Outdoor Fibra can be found in Ajax apps:

1. Go to the **Devices** ⬛ tab.

2. Select **Superior KeyPad Outdoor Fibra** in the list.

| Parameter	Meaning
Data import	Displays the error when transferring data to the new hub: • **Failed** — the device has not been transferred to the new hub. **Learn more**
Malfunction	Tapping on ⓘ opens the list of device malfunctions. The field is displayed only if a malfunction is detected.
Warning ⚠	Clicking on ⓘ opens the list of the settings and permissions that the app needs to be granted for the correct operation of the keypad.
Temperature	Device temperature. It is measured by the processor and changes depending on the ambient temperature. You can create a scenario by temperature to control automation devices. **Learn more**
Fibra signal strength	Signal strength between the hub and Superior KeyPad Outdoor Fibra. Recommended values: 2–3 bars. Fibra is a protocol for transmitting events and alarms.

	Learn more
Connection via Fibra	The status of the connection between the hub and the device: • **Online** — the device is connected to the hub. • **Offline** — the device has lost connection with the hub. Check the device connection to the hub.
Line voltage	The voltage value on the Fibra line to which the device is connected.
Lid	The status of the device tamper that responds to detachment or opening of the device enclosure: • **Open** — the device is removed from the SmartBracket mounting panel, or its integrity is compromised. Check the mounting of the device. • **Closed** — the device is installed on the SmartBracket mounting panel. The integrity of the device enclosure and the mounting panel is not compromised. Normal state. **Learn more**
Mounting panel	The status of the device tamper that responds to unlocking the SmartBracket mounting panel: • **Unlocked** — the holding screw for SmartBracket is unscrewed, or its integrity is compromised. Check the holding screw and mounting of the device. • **Locked** — the holding screw for SmartBracket is screwed. The integrity of the device enclosure and the

	mounting panel is not compromised. Normal state. Learn more
Alarms sound Indication	Shows the status of the **Activate keypad buzzer if an alarm in the system is detected** setting.
Alarm duration	Duration of sound signal in case of alarm. Sets in increments of 3 seconds. Displayed when the **Activate keypad buzzer if alarm in the system is detected** toggle is enabled.
Pass/Tag reading	Displays if the reader for cards and key fobs is enabled.
Bluetooth	Displays if the keypad's Bluetooth module is enabled for controlling the system with a smartphone.
Beeps settings	
Arming/disarming	When enabled, the keypad notifies about arming and disarming with a short beep.
Night mode activation/deactivation	When enabled, the keypad notifies users when the **Night mode** is switched on/off by making a short beep.
Entry delays	When enabled, the keypad beeps about delays when entering.
Exit delays	When enabled, the keypad beeps about delays when leaving.
Entry delays in Night mode	When enabled, the keypad beeps about delays when entering in **Night mode**.
Exit delays in Night mode	When enabled, the keypad beeps about delays when leaving in **Night mode**.
Chime on opening	When enabled, a siren notifies about opening detectors triggering in the **Disarmed** system mode.

	Learn more
Beep volume	Displayed if the notifications about arming/disarming, entry/exit delay, and opening are activated. Shows the buzzer volume level for notifications.
Permanent deactivation	The status of the device's permanent deactivation setting: • **No** — the device operates in the normal mode and transmits all events. • **Entirely** — the device is completely excluded from the system operation by the hub admin. The device does not execute system commands and does not report alarms or other events. • **Lid only** — the hub admin has disabled notifications about tamper triggering. **Learn more**
One-time deactivation	Shows the status of the device's one-time deactivation setting: • **No** — the device operates in the normal mode. • **Entirely** — the device is entirely excluded from the operation of the system for a time the armed mode is active. The device does not execute system commands and does not report alarms or other events. • **Lid only** — notifications on the tamper triggering are disabled for a time the armed mode is active. **Learn more**
Firmware	Device firmware version.

Device ID	Device ID. Also available on the QR code on the device enclosure and its package box.
Device No.	Device number. This number is transmitted to the CMS in case of an alarm or event.
Line No.	The number of the hub's Fibra line to which the device is connected. Displayed in case of **Beam (Radial)** connection.
Ring No.	The number of the hub's Fibra ring to which the device is connected. Displayed in case of **Ring** connection.

Settings
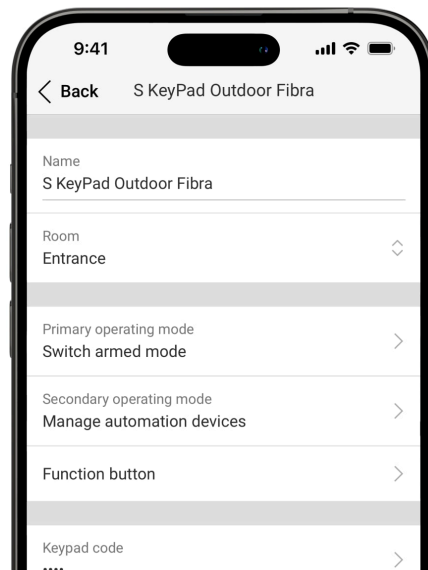
To change Superior KeyPad Outdoor Fibra settings in the Ajax apps:

1. Go to the **Devices** ⬛ tab.

2. Select **Superior KeyPad Outdoor Fibra** in the list.

3. Go to **Settings** ⚙.

4. Set the required settings.

5. Tap **Back** to save the new settings.

Settings	Meaning
Name	Device name. Displayed in the list of hub devices, text of SMS and notifications in the events feed. To change the device name, tap on the text field. The name can contain up to 24 Latin characters or up to 12 Cyrillic characters.
Room	Selecting the virtual room to which Superior KeyPad Outdoor Fibra is assigned. The room name is displayed in the text of SMS and notifications in the events feed.
Primary operating mode	Opens menu with **Primary operating mode** settings.
Secondary operating mode	Opens menu with **Secondary operating mode** settings.
Function button	Selecting the function of the $\ast$ button (**Function** button): • **None** — the function button is disabled and does not execute any commands when pressed. • **Panic** — after the function button is pressed, the system sends an alarm to the CMS and all users. • **Mute fire alarm** — when pressed, the system mutes the alarm of Ajax fire detectors. Available only if the **Interconnected fire detectors alarm** feature is enabled. Learn more
Keypad code	Selection of a general code for security control. Contains 4 to 6 digits.

Duress code	Selecting a general duress code for silent alarm. Contains 4 to 6 digits. **Learn more**
Unauthorized access auto-lock	When enabled, the keypad will be locked for a pre-set time if an incorrect code is entered or unverified access devices are used more than three times in a row within 1 minute. PRO or a user with the rights to configure the system can unlock the keypad through the app before the specified locking time expires.
Auto-lock time	Selecting the keypad lock period after unauthorized access attempts: • 3 minutes. • 5 minutes. • 10 minutes. • 20 minutes. • 30 minutes. • 60 minutes. • 90 minutes. • 180 minutes. Available if the **Unauthorized access auto-lock** toggle is enabled.
Pass/tag reading	When enabled, the security mode can be controlled with **Pass** and **Tag** access devices.
Bluetooth	When enabled, the security mode can be controlled with a smartphone.
Bluetooth sensitivity	Adjusting the sensitivity of the keypad's Bluetooth module:

- Minimum.

- Low.

- Normal (by default).

- High.

- Max.

Available if the **Bluetooth** toggle is enabled.

Backlight and indication	Opens menu with **Backlight and indication** settings.
Sound indication	Opens menu with **Sound indication** settings.
Fibra signal strength test	Switches the device to the Fibra signal strength test mode. The test allows you to check the signal strength between the hub and the device via the wired Fibra data transfer protocol to select the optimal installation site. **Learn more**
Pass/tag reset	Allows deleting all hubs associated with Tag or Pass from device memory. **Learn more**
User guide	Opens the Superior KeyPad Outdoor Fibra user manual in the Ajax app.
Permanent deactivation	Allows the user to disable events of the device without removing it from the system. Three options are available: - **No** — the device operates in normal mode and transmits all events. - **Entirely** — the device will not execute system commands or participate in automation scenarios, and the system

	will ignore device alarms and other notifications. • **Lid only** — the system will ignore notifications about the triggering of the device tamper only. Learn more
One-time deactivation	Allows the user to disable events of the device until the first disarm. Three options are available: • **No** — the device operates in normal mode and transmits all events. • **Entirely** — the device 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. • **Lid only** — notifications on the tamper triggering are disabled until the first disarm. Learn more
Delete device	Unpairs the device, disconnects it from the hub, and deletes its settings.

Primary and secondary operating modes

Superior KeyPad Outdoor Fibra features two operating modes: **primary** and **secondary**. There are three keypad functions that can be configured for each operating mode: **Switch armed mode**, **Manage automation devices**, or **Start entry delay**.

Only one primary keypad function and one secondary keypad function can be set at once. To switch between functions, press and hold the **OK** button

on the keypad.

Parameter	Meaning
Primary operating mode	
Keypad function	Selecting the keypad function for the primary operating mode: • Switch armed mode • Manage automation devices • Start entry delay Only one primary function and one secondary function can be set at once.
Secondary operating mode	
Keypad function	Selecting the keypad function for the secondary operating mode: • None • Switch armed mode • Manage automation devices • Start entry delay Only one primary function and one secondary function can be set at once.
Switch armed mode	
Security objects	Selecting the security sites controlled by the device. You can select the entire space, all or particular groups, or **Night mode**. Selecting groups is available if Group mode is enabled.
Access settings	Selecting the method of arming/disarming:

	- Keypad codes only. - User codes only. - Keypad and user codes. To activate the **Keypad access codes** set up for people who are not registered in the system, select the options on the keypad: **Keypad codes only** or **Keypad and user codes**.
Pre-authorization	When enabled, the user should be authenticated to use the keypad: enter a code or present a personal access device to the keypad.
Authorization confirmation with a passcode	When enabled, users are permitted to arm or disarm the system only when they have been successfully authorized with two forms of identification, i.e., by using Pass, Tag, or a smartphone and entering the appropriate passcode. **Learn more**
Easy armed mode change	When enabled, users do not need to press the **OK** button after a passcode is entered or an access device is read.
Arming without code	When enabled, the user can arm the site without entering a code or presenting the personal access device. If disabled, enter a code or present the access device to arm the system. Available if the **Pre-authorization** toggle is disabled.
Auto-switch to secondary mode	ⓘ Available only for **Secondary operating mode**.

	With this option, the user can set when the keypad automatically starts to operate in secondary mode without a long press of the **OK** button: • Off. • When system is disarmed. • When system is armed.
Manage automation devices	
Automation scenarios	Creates and configures a scenario to manage automation devices with a keypad. You can create a scenario **on preset action** or **on switching the state** of one or multiple automation devices. The keypad can manage only one scenario.
Access settings	Selecting the method of arming/disarming: • Keypad codes only. • User codes only. • Keypad and user codes. To activate the **Keypad Access Codes** set up for people who are not registered in the system, select the options on the keypad: **Keypad codes only** or **Keypad and user codes**.
Pre-authorization	When enabled, the user should be authenticated to use the keypad: enter a code or present a personal access device to the keypad.
Easy assigned device switch	When enabled, users do not need to press the **OK** button after a passcode is entered or an access device is read.
Restrict device management	With this option, the user can set when the control of the automation device using the keypad should be blocked:

	- Off. - When system is disarmed. - When system is armed.
Auto-switch to secondary mode	Available only for **Secondary operating mode**. With this option, the user can set when the keypad automatically starts to operate in secondary mode without a long press of the **OK** button: - Off. - When system is disarmed. - When system is armed.

Start entry delay	
Delay when entering	Selecting entry delay time: 5 to 255 seconds. Entry delay (alarm activation delay) is the time the user has to disarm the site using the main keypad.
Access settings	Selecting the method of arming/disarming: - Keypad codes only. - User codes only. - Keypad and user codes. To activate the **Keypad Access Codes** set up for people who are not registered in the system, select the options on the keypad:

	Keypad codes only or **Keypad and user codes**.
Authorization confirmation with a passcode	When enabled, users are permitted to arm or disarm the system only when they have been successfully authorized with two forms of identification, i.e., by using Pass, Tag, or a smartphone and entering the appropriate passcode. **Learn more**
Easy delay start	When enabled, users do not need to press the **OK** button after a passcode is entered or an access device is read.
Auto-switch to secondary mode	ⓘ Available only for **Secondary operating mode**. With this option, the user can set when the keypad automatically starts to operate in secondary mode without long pressing the **OK** button: • Off. • When system is disarmed. • When system is armed.

Backlight and indication

Settings	Meaning
Brightness	Adjusting the keypad backlight brightness level.

Always-active backlight	When enabled, the keypad backlight always remains active.
Armed mode indication	With this option, the user can set when it is required to show the system security state on the keypad: • **Never** — no security state LED indication. • **Only when armed** — the logo is red when the site is armed, partially armed, or in **Night mode**. • **Always** — the logo is red when the site is armed, green when disarmed, and yellow when arming is incomplete.

Sound indication

Superior KeyPad Outdoor Fibra has a built-in buzzer that, depending on the settings, can notify of the following:

1. Alarms.

2. Delays when entering/leaving.

3. Chimes on opening.

4. Commands execution (e.g., arming, disarming).

5. Pressing the keypad buttons.

> ℹ️ We do not recommend using Superior KeyPad Outdoor Fibra instead of the siren. The keypad's buzzer is meant for additional notifications only. Ajax sirens are designed to deter intruders and draw attention. A properly installed siren is more difficult to dismantle due to its elevated mounting position compared to a keypad at eye level.

Parameter	Meaning
Beeps settings	Opens the **Beeps settings** menu.
Beep on armed mode change	
Arming/disarming	**When enabled**: an audible notification is sent if the security mode is changed from the keypad, another device, or the app. **When disabled**: an audible notification is sent if the security mode is changed from the keypad only. The volume of the beep depends on the configured buttons' volume.
Night mode activation/deactivation	**When enabled**: an audible notification is sent if the **Night mode** is activated/deactivated from the keypad, another device, or the app. **When disabled**: an audible notification is sent if the **Night mode** is activated/deactivated from the keypad only. **Learn more** The volume of the beep depends on the configured buttons' volume.
Beep on delays	
Entry delays	When enabled, the built-in buzzer beeps about a delay when entering. **Learn more**
Exit delays	When enabled, the built-in buzzer beeps about a delay when leaving. **Learn more**
Entry delays in Night mode	When enabled, the built-in buzzer beeps about a delay when entering in the **Night**

	mode. Learn more
Exit delays in Night mode	When enabled, the built-in buzzer beeps about a delay when leaving in the **Night mode**. Learn more
Fast beep on delays	
Fast beep on Entry delay expiration	Notifies the user that the **Delay when entering** time is running out. You can choose one of four options for when the fast beep should start: • Never • Last 5 seconds • Last 10 seconds • Last 15 seconds The option is available when **Beep on entry delays** is enabled.
Fast beep on Exit delay expiration	Notifies the user that the **Delay when leaving** time is running out. You can choose one of four options for when the fast beep should start: • Never • Last 5 seconds • Last 10 seconds • Last 15 seconds The option is available when **Beep on exit delays** is enabled.

Beep when disarmed	
Chime on opening	When enabled, the built-in buzzer informs users with a short beep that the opening detectors are triggered in the **Disarmed** system mode. **Learn more**
Beep volume	Selecting the built-in buzzer volume level for notifications about arming/disarming, entry/exit delay, and opening: - **Quiet.** - **Loud.** - **Very loud.**
Buttons	
Volume	Adjusting the buzzer notification volume for interactions with the keypad.
Alarms reaction	
Audible alarm	Setting the mode when the built-in buzzer enables an alarm: - **Always** — an audible alarm will be activated regardless of the system security mode. - **Only when armed** — an audible alarm will be activated if the system or the group a keypad is assigned to is armed.
Activate keypad buzzer if alarm in the system is detected	When enabled, the built-in buzzer notifies an alarm in the system.
Alarms in Group mode	Selecting the group (from the shared) which alarm the keypad will notify of. The **All shared groups** option is set by default. If the keypad has only one shared group and it is deleted, the setting will return to its initial value.

	Displayed if the **Group mode** is enabled.
Alarm duration	Duration of sound signal in case of alarm: from 3 seconds to 3 minutes.

> ⚠️ Adjust the entry/exit delays in the appropriate detectors settings, not the keypad settings.
>
> Learn more

Keypad response to device alarms

Superior KeyPad Outdoor Fibra can respond to alarms from each device in the system with a built-in buzzer. The function is useful when users do not need to activate the buzzer for the alarm of a specific device. For example, this can be applied to the triggering of the **LeaksProtect Jeweller** leakage detector.

> ℹ️ By default, the keypad response is enabled for alarms of all devices in the system.

To set the keypad response to a device alarm:

1. Open the Ajax app.

2. Go to the **Devices** ➖ tab.

3. Select the device for which you want to configure the keypad response from the list.

4. Go to **Settings** ⚙️.

5. Find the **Alert with a siren** option and select the toggles which will activate it. Enable or disable the function.

6. Repeat steps 3–5 for the rest of the system devices.

Keypad response to tamper alarms

Superior KeyPad Outdoor Fibra can respond to enclosure alarms from each system device with a built-in buzzer. When the function is activated, the keypad built-in buzzer will emit a sound signal upon triggering the tamper button of the device.

To set the keypad response to a tamper alarm:

1. Open the Ajax app.

2. Go to the **Devices** ⬛ tab.

3. Select the hub and go to its **Settings** ⚙.

4. Select the **Service** menu.

5. Go to the section **Sounds and Alerts**.

6. Enable the **If lid of hub or any detector is open** toggle.

7. Tap **Back** to save the new settings.

> ⓘ   Tamper button reacts to opening and closing of the enclosure, regardless of the armed mode of the device or system.

Keypad response to pressing the panic button in the Ajax apps

An admin or PRO with rights to configure the system can set up the keypad response to the alarm when the panic button is pressed in Ajax apps. To do this, follow these steps:

1. Open the Ajax app.

2. Go to the **Devices** ⬛ tab.

3. Select the hub and go to its **Settings** ⚙.

4. Select the **Service** menu.

5. Go to the section **Sounds and Alerts**.

6. Enable the **If in-app panic button is pressed** toggle.

7. Tap **Back** to save the new settings.

Keypad after-alarm indication

0:00 / 0:07

The keypad can inform about triggering in the armed system through LED indication.

The option functions as follows:

1. The system registers the alarm.

2. The keypad plays an alarm signal (if enabled). The duration and volume of the signal depend on the **device settings**.

3. The keypad's LED flashes twice (once every 3 seconds) until the system is disarmed.

Thanks to this feature, system users and security company patrols can understand that the alarm has occurred.

> **i** The Superior KeyPad Outdoor Fibra after-alarm indication does not work for always active detectors, if the detector was triggered when the system was disarmed.

To enable the Superior KeyPad Outdoor Fibra after-alarm indication, in the Ajax PRO app:

1. Go to hub settings:

   - Hub → Settings ⚙ → Service → LED Indication.

2. Specify which events Superior KeyPad Outdoor Fibra will inform about by double flashing of the LED indicator before the system is disarmed:

   - Confirmed intrusion/hold-up alarm.

   - Single intrusion/hold-up alarm.

   - Lid opening.

3. Select the required Superior KeyPad Outdoor Fibra in the **Devices** ⬛ menu. Tap **Back** to save the parameters.

4. Tap **Back**. All values will be applied.

Chime on opening

If **Chime on opening** is enabled, Superior KeyPad Outdoor Fibra notify a user with a short beep if 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.

Notifications are configured in two stages: setting up the keypad and setting up opening detectors. **This article** provides more information about **Chime** and how to set up detectors.

To set the keypad response:

1. Open the Ajax app.

2. Go to the **Devices** ⊟ tab.

3. Select Superior KeyPad Outdoor Fibra and go to its **Settings** ⚙.

4. Go to the **Sound indication** menu → **Beeps settings**.

5. Enable the **Chime on opening** toggle in the **Beep when disarmed** category.

6. Set the required notifications volume.

7. Tap **Back** to save the settings.

If the settings are made correctly, a **bell icon** appears in the **Control** ⊕ tab of the Ajax app. Tap it to activate or deactivate chime on opening.

Codes setting

> ℹ In Ajax PRO apps, within the hub settings, you can set the requirements for the length of passcodes used for user authorization and access to the system. You can select the **Flexible (4 to 6 symbols)** option or define the fixed code length: **4 symbols**, **5 symbols**, or **6 symbols**.
>
> Setting a fixed code length will reset all previously configured access codes.
>
> The fixed code length is required for the **Easy armed mode change** feature, which allows disarming the system without pressing the **OK** button on the keypad after entering a passcode or using an access device.

Keypad access codes

To set keypad and keypad duress codes:

1. In the Ajax app, go to the **Devices** ⊟ tab.

2. Select the keypad for which you want to set up an access code.

3. Go to its **Settings** ⚙.

4. Select **Keypad codes only** or **Keypad and user codes** option in the **Access settings** menu.

5. Go to the **Keypad code** menu.

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

7. Tap **Done**.

8. Go to the **Duress code** menu.

9. Set the keypad duress code. Contains from 4 to 6 digits.

10. Tap **Done**.

User access codes

To set a personal code and a personal duress code:

1. Select the space in the Ajax app.

2. Go to the **Settings** ⚙ menu.

3. Open the **Users** menu.

4. Find your account in the list and tap on it.

5. Go to the **Passcode settings** menu.

6. Set the **User code**. Contains from 4 to 6 digits.

7. Tap **Save**.

8. Set the **Duress code**. Contains from 4 to 6 digits.

9. Tap **Save**.

10. Tap **Back** to save the settings.

Unregistered user codes

To set an access code for a user without an account:

1. Select the hub in the Ajax app.

2. Go to the **Settings** ⚙ menu.

3. Go to the **Keypad access codes** menu.

4. Tap **Add code**. Set up **Name** and **Access code**. Contains from 4 to 6 digits.

5. Tap **Add** to save the data.

To set a duress code for a user without an account:

1. Select **Keypad access codes** menu in the hub settings.

2. Select the required unregistered user.

3. Tap **Add duress code**. Set the code. Contains from 4 to 6 digits.

4. Tap **Done**.

> ℹ For unregistered users, an admin or PRO with the rights to configure the system can adjust the access to security management. First, enable Group mode. Then, select the **Keypad access codes** menu in the hub settings, find the required user, and set the appropriate parameters in the **Security management** menu.

RRU code

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

Cards and key fobs

Superior KeyPad Outdoor Fibra can work with **Tag** key fobs, **Pass** cards, and third-party devices that support DESFire® technology.

> ℹ Before adding third-party devices that support DESFire®, make sure they have enough free memory to handle the new keypad. Preferably, the third-party device should be pre-formatted.

provides information on how to reset **Tag** or **Pass**.

The maximum number of added Pass and Tag devices depends on the hub model. The added Pass and Tag devices do not affect the total device limit on the hub.

Check device compatibility

Adding Tag or Pass

1. Open the Ajax app.

2. Select the space with hub to which you want to add Tag or Pass.

3. Go to the **Devices** ➖ tab.

> ℹ️ Make sure the **Pass/Tag reading** feature is enabled in at least one keypad setting.

4. Click **Add device**.

5. Select **Add pass/tag**.

6. Specify the type (Tag or Pass), color, device name, and user (if necessary).

7. Tap **Next**. After that, the hub will switch to the device registration mode.

8. Go to any compatible keypad with **Pass/Tag reading** enabled. Press the **OK** button to switch keypad to the access device logging mode.

9. Present Pass or Tag with the wide side to the keypad for a few seconds. Upon successful addition, you will receive a notification in the Ajax app.

If the connection fails, try again in 5 seconds. Please note that if the maximum number of Tag or Pass devices has already been added to the hub, you will receive a corresponding notification in the Ajax app when adding a new device.

> **i** Both Tag and Pass can work with several hubs at the same time. The maximum number of hubs is 13. If you try to add Tag or Pass to a hub that has already reached the device limit, you will receive a corresponding notification. To add such a key fob/card to a new hub, you will need to reset it.

If you need to add another Tag or Pass, tap **Add another pass/tag** in the app. Repeat steps 6–9.

Deleting (resetting) Tag or Pass

> **!** Resetting will delete all settings and bindings of key fobs and cards. In this case, the reset Tag and Pass are only removed from the hub from which the reset was made. On other hubs, Tag or Pass are still displayed in the app but cannot be used to manage the security modes. These devices should be removed manually.

1. Open the Ajax app.

2. Select the space.

3. Go to the **Devices** ⬛ tab.

4. Select a compatible keypad from the device list.

> **i** Make sure the **Pass/Tag reading** feature is enabled in the keypad settings.

5. Go to the keypad settings by clicking the ⚙ icon.

6. Tap **Pass/Tag reset**.

7. Tap **Continue**.

8. Go to any compatible keypad with **Pass/Tag reading** enabled. Press the **OK** button to switch the keypad to the access device resetting mode.

9. Present Pass or Tag with the wide side to the keypad for a few seconds. Upon successful formatting, you will receive a notification in the Ajax app. If the formatting fails, try again.

If you need to reset another Tag or Pass, tap **Reset another Pass/Tag** in the app. Repeat step 9.

Bluetooth setting

Superior KeyPad Outdoor Fibra supports security modes control by bringing a smartphone to the sensor. Security management is established through a Bluetooth communication channel. This method is convenient, secure, and fast, as there is no need to enter a password, add a phone to the keypad, or use Tag or Pass that could be lost.

> ⚠️ Bluetooth authentication is available only for Ajax Security System users.

To enable Bluetooth authentication in the app

1. Add Superior KeyPad Outdoor Fibra to the system.

2. Enable the keypad Bluetooth sensor:

   - **Devices** ➖ → **Superior KeyPad Outdoor Fibra** → **Settings** ⚙️ → Enable the **Bluetooth** toggle

3. Tap **Back** to save the settings.

To set up Bluetooth authentication

1. Open the Ajax Security System app and select the space to which the Superior KeyPad Outdoor Fibra with enabled Bluetooth authentication is added. By default, authentication with Bluetooth is available for all users of such system.

> ⓘ To prohibit Bluetooth authentication for certain users:
>
> 1. In the **Devices** tab select the hub and go to its settings.
>
> 2. Open **Users** menu and the required user from the list.
>
> 3. In the **Permissions** section, disable the **Security management via Bluetooth** toggle.

2. Allow the Ajax Security System app to use Bluetooth if it was not previously granted. In this case, the warning ⚠ appears at Superior KeyPad Outdoor Fibra **States**. Pressing the ⓘ symbol opens the window with explanations of what to do. Enable the **Security management with a phone** toggle at the bottom of the opened window.
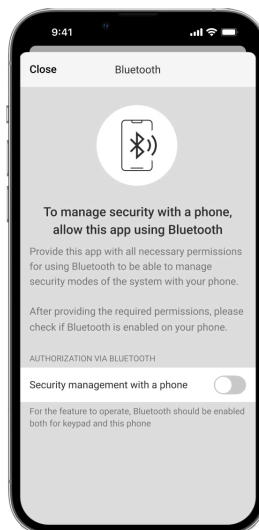

Grant the app permission to find and connect to nearby devices. The popup window for Android and iOS smartphones can differ.
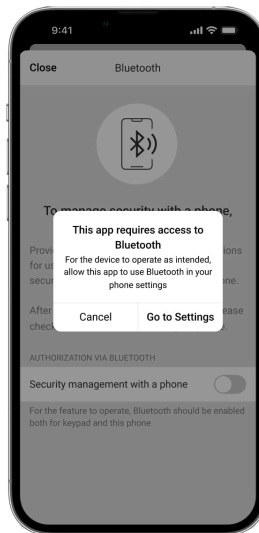
Also, the **Security management with a phone** toggle can be enabled in the app settings:

- Tap the ☰ icon in the upper left corner of the screen and select the **App settings** menu.

- Open the **System settings** menu and enable **Security management with a phone** toggle.
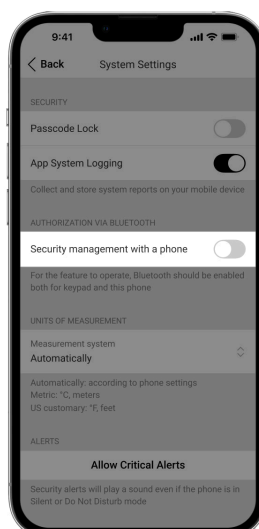
3. We recommend configuring **Geofence** for the stable performance of Bluetooth authentication. The warning ⚠ appears at Superior KeyPad Outdoor Fibra **States** if **Geofence** is disabled and the app is not allowed to use the smartphone location. Tapping the ⓘ symbol opens the window with explanations of what to do.
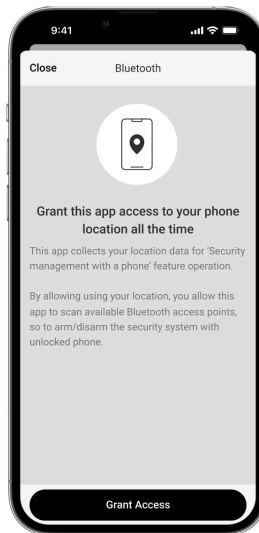
> **i** Bluetooth authentication can be unstable if **Geofence** function is disabled. Users will need to launch and minimize the app if the system switches it to sleep mode.
>
> Users can control the system faster via Bluetooth, when the **Geofence** function is activated and configured. All that is needed is to unlock the phone and present it to the keypad sensor.
>
> How to set up Geofence

4. Enable the **Keep app alive to manage security via Bluetooth** toggle. For this, go to **Devices** ⬛ → **Hub** → **Settings** ⚙ → **Geofence**.

5. Ensure that Bluetooth is enabled on your smartphone. If it is disabled, the warning ⚠ appears in the keypad **States**. Pressing the ⓘ symbol opens the window with explanations of what to do.

6. Enable the **Keep-Alive Service** toggle in the app settings for Android smartphones. For this, in the upper left corner of the screen, click the ☰ → **App settings** → **System settings**.

Controlling security

Using codes, Tag/Pass, or a smartphone, you can control the **Night mode** and the security of the entire site or separate groups. The user or PRO with the rights to configure the system can set up access codes. This chapter provides information on how to add Tag or Pass to the hub. To control with a smartphone, adjust the appropriate Bluetooth parameters in the

keypad settings. Turn on the smartphone Bluetooth, location, and unlock the screen.

If a personal or access code, Tag/Pass, or a smartphone is used, the name of the user who changed the security mode is displayed in the hub event feed and in the notifications list. If a general code is used, the name of the keypad from which the security mode was changed is displayed.

> **i** Superior KeyPad Outdoor Fibra is locked for the time specified in the settings if an incorrect code is entered or an unverified access device is presented three times in a row within 1 minute. The corresponding notifications are sent to users and the monitoring station of the security company. A user or PRO with the rights to configure the system can unlock Superior KeyPad Outdoor Fibra in the Ajax app.

The step sequence for changing the security mode with the keypad depends on whether **Pre-authorization**, **Authorization confirmation with a passcode**, and **Easy armed mode change** options are enabled in the Superior KeyPad Outdoor Fibra settings.

Using Tag, Pass, or a smartphone

1. Present Tag, Pass, or a smartphone to the keypad.

2. Enter the required code if the **Authorization confirmation with a passcode** feature is activated.

3. Press the **OK** button on the keypad to change the armed mode.

If the **Easy armed mode change** option is enabled, you do not need to press the **OK** button after the access device is read.

Using passcodes

Code	Example	Note
Managing the site armed modes		
Keypad code Keypad duress code	1234 → OK	
User code User duress code	5 → ✳ → 1234 → OK	**5** is a user ID
Code of unregistered user Duress code of unregistered user	1234 → OK	
RRU code	1234 → OK	
Managing the group armed modes		
Keypad code Keypad duress code	1234 → ✳ → 2 → OK	**2** is a group ID
User code User duress code	5 → ✳ → 1234 → ✳ → 2 → OK	**5** is a user ID **2** is a group ID
Code of unregistered user Duress code of unregistered user	1234 → ✳ → 2 → OK	**2** is a group ID
RRU code	1234 → ✳ → 2 → OK	**2** is a group ID

Learn more about user ID

Learn more about group ID

Authorization confirmation with a passcode

Authorization confirmation with a passcode is a feature that provides the ability to set up two-factor authentication for users when they control the system's security modes. This definition means that users must first use an access device (Pass, Tag, or a smartphone) and then enter a passcode to confirm their authorization to the system.

Learn more about Authorization confirmation with a passcode

Managing automation devices and scenarios

> ⓘ Ensure the **Manage automation devices** feature is configured for the primary or secondary operating mode in the keypad settings in Ajax apps.

To control the automation device or scenario with Superior KeyPad Outdoor Fibra:

1. Present an access control device to the keypad or enter a passcode to authorize on the keypad.

2. Switch the keypad to the **Manage automation devices** mode with a long press of the **OK** button if this mode is not active or set as the main operating mode. The **OK** button should light up green or red depending on the current state of the automation device.

3. Press the **OK** button to change the state of the automation device or execute a scenario:

   - If the keypad manages a scenario **on switching the state**, the **OK** button LED indication should change to correspond to the state of

the automation device.

- If the keypad manages a scenario **on preset action**, the **OK** button LED indication does not show the state of devices. Instead, it indicates whether the set action is completed or not.

The step sequence for managing the automation devices with the keypad depends on whether **Pre-authorization** and **Easy assigned device switch** options are enabled in the Superior KeyPad Outdoor Fibra settings.

Indication

Superior KeyPad Outdoor Fibra informs users about alarms, entry/exit delays, current security mode, malfunctions, and other system states by means of:

- Ajax logo, **OK** button, and backlight with LED indication;

- built-in buzzer.

Event	LED	Buzzer
Short button press		Short beep
The device is activated when it is not added to the hub	The logo lights up red for 0.3 s and goes out for 0.3 s three times.	
To be added to the hub, the device is selected from the list of devices found by scanning Fibra lines	The logo flashes green rapidly.	
The device is deleted from the hub	The logo lights up red for 0.3 s and goes out for 0.3 s six times.	
The keypad is in **Switch armed mode***	The logo is green or red depending on the current security state.	
The keypad is in **Manage automation devices** mode	The **OK** button is green or red depending on the	

	current automation device state. The logo is off.	
The keypad is in **Start entry delay** mode*	The logo is red when the site is armed. The logo flashes red simultaneously with a beep on entry delay.	
Arming or **Night mode** activation	The logo changes from green to red.	Beep for about 0.2 s.
Disarming	The logo changes from red to green.	Double beep for about 0.4 s.
Pressing **Panic** button (✳)		Long beep for about 0.5 s.
Press and hold the function button (✳) to clear the entered code	The backlight flashes simultaneously with a short beep.	Short beep.
Wrong passcode entered	The backlight lights up three times during a long beep.	Long beep for about 0.6 s.
Request is denied due to lack of user permissions or malfunction	The logo lights up yellow three times during a long beep.	Long beep for about 0.6 s.
The keypad is locked	The backlight lights up three times during a long beep.	Long beep for about 0.6 s.
System integrity check fails	The logo lights up green or red (depending on current security state) three times during a long beep.	Long beep for about 0.6 s.
System security state change is forbidden	The logo lights up yellow three times during a long beep.	Long beep for about 0.6 s.
Tamper alarm/restoration	The logo lights up red for 0.7 s.	
Pass/Tag read is successful	The backlight goes out for about 0.3 s.	Beep for about 0.2 s.
Pass/Tag read is failed	The logo lights up yellow, and the backlight goes out during a beep.	Long beep for about 1 s.

|		
Smartphone reading is successful	The backlight goes out for about 0.1 s.	Frequent beeping for about 0.2 s.
Smartphone reading is failed	The logo lights up yellow during a beep.	Long beep for about 1 s.
The keypad is waiting to read Pass/Tag	The backlight lights up for 0.2 s and goes out for 1 s until Pass/Tag is read.	
Adding Pass/Tag is successful		Two short beeps.
1. Adding Pass/Tag is failed. 2. Invalid card is read. 3. Other malfunctions occurred while reading an access device.	The logo lights up yellow for about 0.3 s.	Long beep for about 0.6 s.
Delay on entering/leaving	The logo lights up red simultaneously with beep on entry delay. The logo lights up green simultaneously with beep on exit delay.	Short beep once per 1 s.
System recovery is needed (PD 6662:2017)	The logo lights up yellow for about 0.1 s then a short beep sounds. It is repeated three times.	
Post alarm indication	The logo flashes red twice every 3.4 s.	
Arming incomplete (PD 6662:2017)	The logo lights up yellow constantly.	Three short beeps for about 0.3 s every 1 s.
One device in the system is offline (UL)	The logo flashes yellow two times simultaneously with a short beep two times every 1 minute.	
One device in the system has a low battery (UL)	The logo flashes yellow three times simultaneously with a short beep with a change in tone every 1 minute.	
Delayed arming (initiated by the device) (PD 6662:2017)	The logo lights up green for about 0.8 s every 1 s.	
Delayed arming (initiated by the app)	The logo lights up red for about 0.8 sec every 1 s.	

(PD 6662:2017)		
The hub does not respond	The logo lights up yellow during a long beep.	Long beep for about 0.5 s.

* When the indication is enabled in the keypad settings.

Malfunctions

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

All malfunctions can be seen in the device **states**. Fields with malfunctions will be highlighted in red.
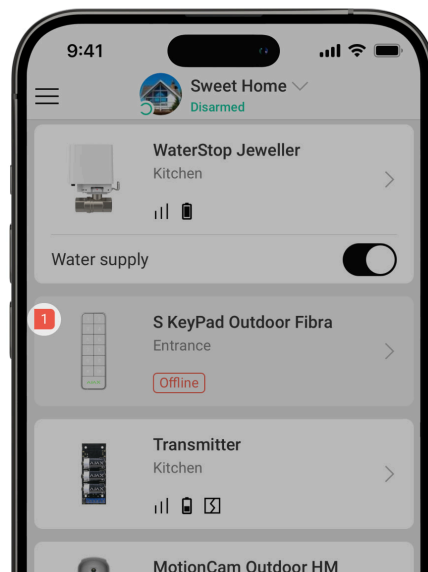
Malfunction is displayed if:

- The device temperature is outside acceptable limits.

- The device lid is open (tamper is triggered).

- There is no signal via Fibra protocol.

Maintenance

Regularly check the functioning of the device. The optimal frequency of checks is once every three months. Clean the device enclosure from dust, cobwebs, and other contaminants as they emerge. Use soft, dry wipes suitable for equipment maintenance.

Do not use substances that contain alcohol, acetone, gasoline, and other active solvents to clean the device.

Technical specifications

All technical specifications

Compliance with standards

Setup in compliance with EN 50131 requirements

Warranty

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

If the device does not operate properly, we recommend contacting support service first, as most technical issues can be resolved remotely.

Warranty obligations

User Agreement

Contact Technical Support:

- email

- Telegram

Manufactured by "AS Manufacturing" LLC