KeyPad TouchScreen Fibra user manual

Soon to be: Superior KeyPad TouchScreen Fibra

Updated September 25, 2024

KeyPad TouchScreen Fibra is a wired keypad with a touch screen designed for managing the Ajax system. Users can authenticate using smartphones, **Tag** key fobs, **Pass** cards, and codes. The device is intended for indoor use.
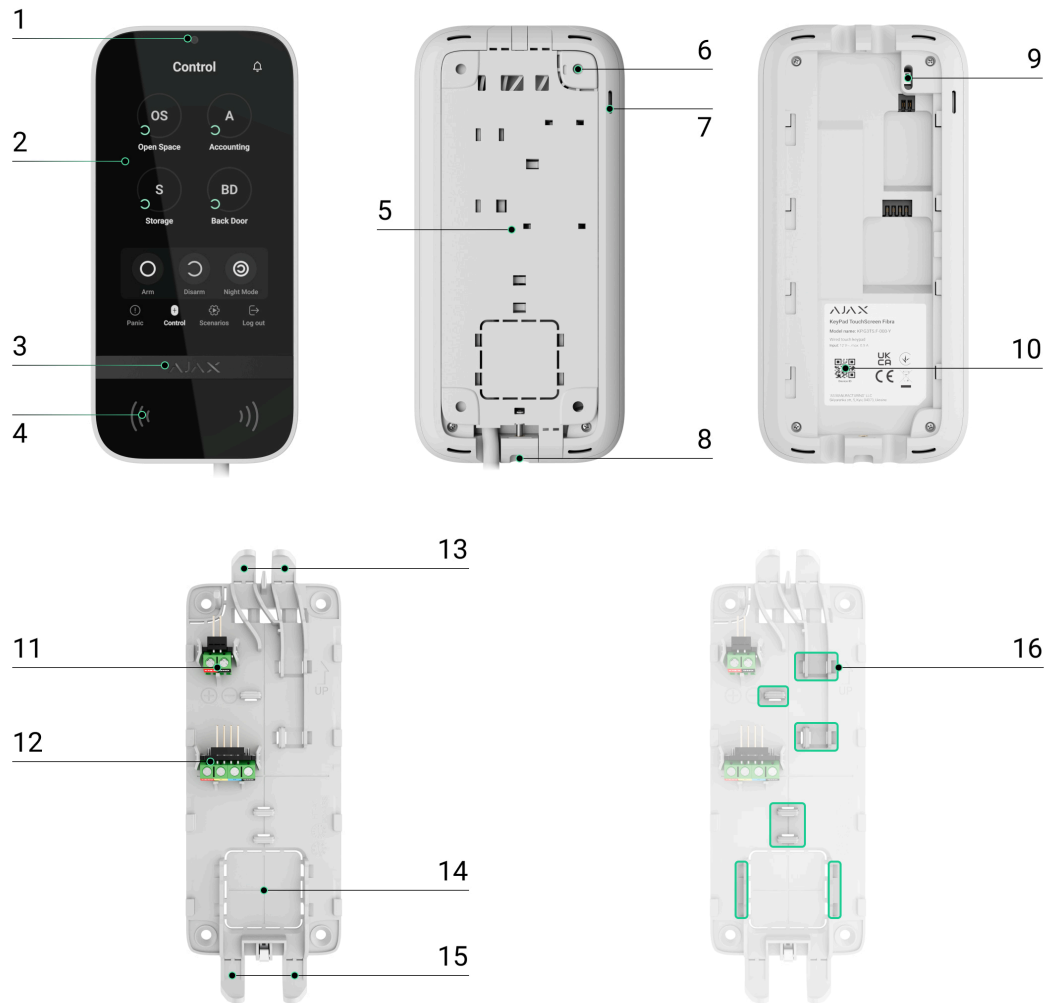
The keypad operates in the Ajax system and exchanges data with the hub using the secure Fibra wired communication protocol.

Learn more

KeyPad TouchScreen Fibra is part of the Fibra product line of wired devices. Only accredited Ajax Systems partners can install, sell, and administer these devices.

Buy KeyPad TouchScreen Fibra

Functional elements

1. Ambient light sensor for automatically adjusting the backlight brightness.

2. IPS touchscreen display with a 5-inch diagonal.

3. Ajax logo with an LED indicator.

4. Cards/key fobs/Bluetooth reader.

5. The SmartBracket mounting panel. To remove the panel, slide it down.

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

7. Built-in buzzer.

8. The hole for attaching the SmartBracket mounting panel with a holding screw.

9. **Tamper button**.

10. QR code with the device ID for adding the keypad to the Ajax system.

11. Terminals for connecting an external power supply unit (not included). The terminals can be removed from the holders when necessary.

12. Input terminals for connecting the Fibra line to KeyPad TouchScreen Fibra.

13. Perforated part of the mounting panel for routing cables from the top.

14. Perforated part of the mounting panel for routing cables through the wall.

15. Perforated part of the mounting panel for routing cables from the bottom.

16. Fasteners to fix the cables with ties.

Compatible hubs

Hub Hybrid (2G) or **Hub Hybrid (4G)** with the firmware **OS Malevich 2.21** and higher is required for the keypad to operate.

Operating principle

KeyPad TouchScreen features a built-in buzzer, a touchscreen display, and a reader for contactless authorization. The keypad can be used to control security modes and automation devices and to notify about system events.

The keypad can automatically adjust the backlight brightness and wakes up upon approach. Sensitivity is **adjustable** in the app. KeyPad TouchScreen interface is inherited from Ajax Security System app. There are dark and light interface appearances to choose from. A 5-inch diagonal touchscreen display provides access to the security mode of an object or any group and control over automation scenarios. The display

also indicates system malfunctions, if present (when **system integrity check** is enabled).

Depending on the settings, the KeyPad TouchScreen built-in buzzer notifies about:

- alarms;

- security mode changes;

- entry/exit delays;

- triggering of the opening detectors.

The keypad is powered by the control panel and has a backup power source – pre-installed rechargeable batteries. KeyPad TouchScreen can also be powered by a third-party power supply unit with a voltage range of 10.5–14 V⎓ and an operating current from 0.5 A.

Security control
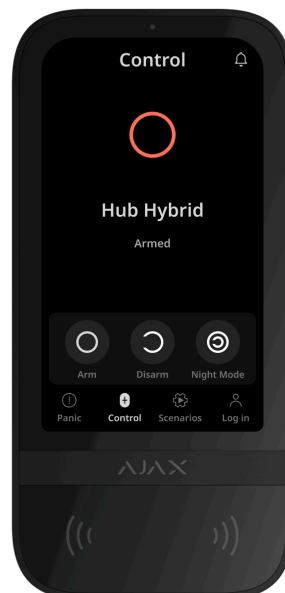
KeyPad TouchScreen can arm and disarm the entire object or specific groups, and activate **Night Mode**. Use the **Control** ⊕ tab to change the security mode. Users can control the security using KeyPad TouchScreen through:

1. **Smartphones**. With the installed **Ajax Security System** 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 higher.

2. **Cards or key fobs**. To quickly and securely identify users, KeyPad TouchScreen uses the DESFire® technology. DESFire® is based on the ISO 14443 international standard and combines 128-bit encryption and copy protection.

3. **Codes**. KeyPad TouchScreen supports general, 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 Both Hub Hybrid (2G) and Hub Hybrid (4G) support up to 50 personal, keypad access, and RRU codes.

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 object. If a user loses their Pass, Tag, or 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
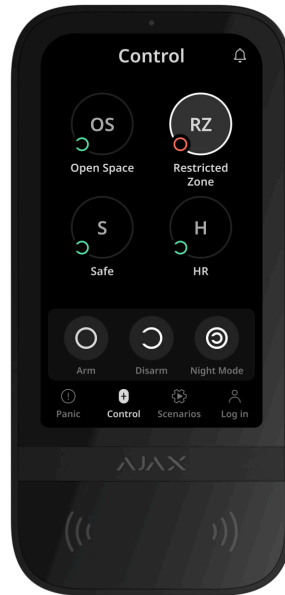
KeyPad TouchScreen allows controlling the groups' security (if **Group Mode** is enabled). An admin or PRO with the rights to configure the system can also adjust the keypad **settings** to determine which groups will be shared (keypad groups). By default, all groups are visible on the keypad display in the **Control** ⊕ tab. You can learn more about group security management in **this section**.

Emergency buttons
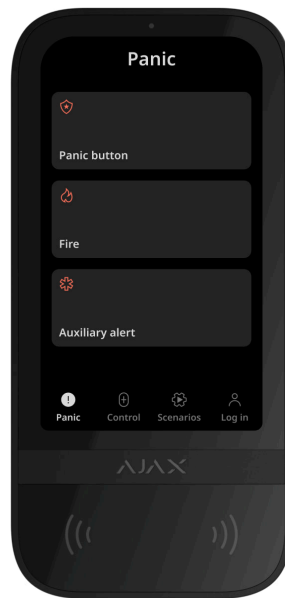
For emergencies, the keypad features the **Panic** ⓘ tab with three buttons:

- Panic button;

- Fire;

- Auxiliary alarm.

In Ajax app, an admin or a PRO with the rights to configure the system can select the number of buttons displayed in the **Panic** ⓘ tab. There are two options available in the KeyPad TouchScreen settings: only **Panic button** (by default) or all three buttons. The text of notifications in apps and event codes transmitted to the Central Monitoring Station (CMS) depend on the selected button type.

You can also activate accidental press protection. In this case, the user confirms alarm transmission by pressing the **Send** button on the keypad display. The confirmation screen appears after pressing any panic button.

> ⓘ Pressing emergency buttons can trigger Alarm scenarios in Ajax system.

Scenarios management
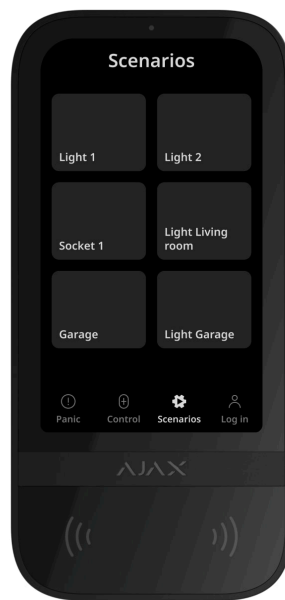
The separate keypad tab holds up to six buttons that control one **automation device** or a group of devices. Group scenarios provide more convenient control over multiple switches, relays, or sockets simultaneously.

Create automation scenarios in the **keypad settings** and manage them using KeyPad TouchScreen.

Learn more

Indication of malfunctions and security mode

KeyPad TouchScreen informs users about system malfunctions and security mode through:

- display;

- logo;

- sound indication.

Depending on the settings, the logo lights up red continuously or when the system or group is armed. KeyPad TouchScreen indication is shown on the display only when it is active. The built-in buzzer notifies about alarms, door openings, and entry/exit delays.
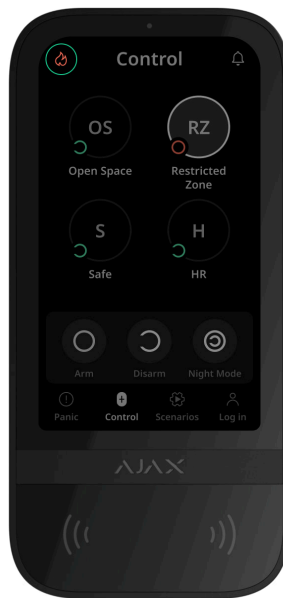
Fire alarm muting
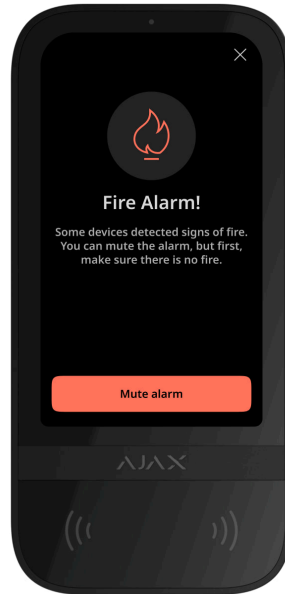
In case of a fire alarm in the system, users can mute it using KeyPad TouchScreen.

> ⓘ Pressing the **Fire** emergency button in the Panic tab doesn't activate Interconnected Fire Detectors Alarm (if enabled). When sending an emergency signal from the keypad, an appropriate notification will be transmitted to the app and the CMS.

The screen with information about the fire alarm and the button to mute it will appear on all KeyPad TouchScreen with the **Mute Fire Alarm** feature enabled. If the mute button has already been pressed on the other keypad, a corresponding notification appears on the remaining KeyPad TouchScreen displays. Users can close the fire alarm muting screen and use other keypad features. To reopen the muting screen, press the icon 🔥 on the KeyPad TouchScreen display.

> ℹ️ To instantly display the fire alarm muting screen on the KeyPad TouchScreen, enable the **Always Active Display** toggle in the keypad settings. Also, connect the third-party power supply.
>
> Otherwise, the muting screen will only be displayed when the keypad wakes up.

Duress code

KeyPad TouchScreen 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

User pre-authorization

Pre-authorization feature is essential to prevent unauthorized access to the control panel and the current system state. The feature can be activated separately for the **Control** ⊕ and **Scenarios** 🎛️ tabs in the keypad settings.

The screen for entering the code is displayed on the tabs for which pre-authorization is activated. The user should authenticate first, either by entering a code or presenting a personal access device to the keypad. The exception is the **Alarm** ⓘ tab, which allows unauthorized users to send an emergency signal.

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. KeyPad TouchScreen will turn off the reader and block access to all tabs. The keypad's display will show an appropriate notification.

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

Two-Stage Arming

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

Learn more

Fibra data transfer protocol

The keypad uses Fibra technology to transmit alarms and events and to update the firmware. It is a wired data transfer protocol for fast and 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 both PRO Desktop monitoring app and the central monitoring station (CMS) in the formats of **SurGard (Contact ID), SIA (DC-09), ADEMCO 685**, and other protocols.

KeyPad TouchScreen can transmit the following events:

1. Entry of the duress code.

2. Pressing the panic button. Each button has its own event code.

3. Keypad locking due to an unauthorized access attempt.

4. Tamper alarm and recovery.

5. Connection loss/restoration between KeyPad TouchScreen and the hub.

6. Arming/disarming the system.

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

8. Permanent deactivation/activation of the keypad.

9. One-time deactivation/activation of the keypad.

10. Low voltage detection on the Fibra line and voltage restoration to normal values.

11. Low backup battery charge and battery charge restoration.

12. Backup battery malfunction/restoration.

13. Malfunction detection; the keypad cannot charge the backup battery.

When an alarm is received, the operator at the security company's monitoring station knows what happened and precisely where to dispatch a rapid response team. The addressability of Ajax devices allows sending events to PRO Desktop or the CMS, including the device type, its name, security group, and virtual room. Note that the list of transmitted parameters may vary depending on the CMS type and the selected communication protocol for the monitoring station.

> **i** The ID and device number can be found in its states in the Ajax app.

Adding to the system

> ⚠️ **KeyPad TouchScreen Fibra** is compatible only with Hub Hybrid (2G) and Hub Hybrid (4G). Only accredited partners can add and configure Fibra devices in Ajax PRO apps.

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.

What is a space

How to create a space

> **i** The **space** functionality is available for apps of such versions or later:
>
> - Ajax Security System 3.0 for iOS;
>
> - Ajax Security System 3.0 for Android;
>
> - Ajax PRO: Tool for Engineers 2.0 for iOS;
>
> - Ajax PRO: Tool for Engineers 2.0 for Android;
>
> - Ajax PRO Desktop 4.0 for macOS;
>
> - Ajax PRO Desktop 4.0 for Windows.

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, Wi-Fi, 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

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

Automatically   **Manually**

To add a device automatically:

1. Open the **Ajax PRO app** and select the hub to which you want to add KeyPad TouchScreen.

2. Go to the **Devices** ⊟ tab and click **Add device**.

3. Select **Add all Fibra devices**. The hub will scan the Fibra lines. After scanning, all devices connected to the hub that have not been added to the system will be displayed.

4. Select the desired device from the list. When selected, the LED indicator will flash to identify this device, and an appropriate notification will appear on the keypad display.

5. Name the device, and select the room and security group if **Group Mode** is enabled. Click **Save**.

If the connection attempt fails, verify that the wired connection is correctly set up before trying again. If the maximum number of devices (100 for Hub Hybrid) has already been added to the hub, you will receive an error notification while adding.

⚠️ KeyPad TouchScreen 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.

ℹ️ **KeyPad TouchScreen** 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.

Malfunctions

When a KeyPad TouchScreen malfunction is detected, the Ajax app displays a malfunction counter on the device icon. All malfunctions are indicated in the keypad's states. Fields with malfunctions will be highlighted in red.

A malfunction is displayed if:

- the keypad enclosure is open (tamper is triggered);

- there is no connection with the hub;

- the keypad backup battery is low;

- the backup battery is not installed;

- the backup battery is malfunctioned;

- KeyPad TouchScreen has a malfunction and cannot charge the backup battery;

- low voltage on the Fibra line;

- the keypad temperature is outside acceptable limits.

Icons

Icons in the app

The icons in the app display some keypad states. To access them:

1. Sign in to the **Ajax app**.

2. Select the hub.

3. Go to the **Devices** ➖ tab.

Icon	Meaning
ııl	Fibra signal strength. Displays the signal strength between the hub and the device. The recommended value is 2–3 bars. **Learn more**
🔋	The keypad backup battery charge level is OK, or the battery is charging.
🔋	The keypad backup battery charge level is low.
🔋	The keypad backup battery is malfunctioned or not installed.
✳	Displayed when the keypad Bluetooth module is enabled.
⚠	Bluetooth setup is not complete. The description is available in the keypad states.
🔄	A firmware update is available. Go to the keypad states or settings to find the description and launch an update. ⓘ The icon is not available in the Ajax Security System app with version 3.0 and higher for iOS and Android. **Learn more**
(( ))	**Pass/Tag reading** is enabled in KeyPad TouchScreen settings.

🔔	**Chime on opening** is enabled in KeyPad TouchScreen settings.
⚙️	Device is permanently deactivated. **Learn more**
⊔	Tamper alarm notifications are permanently deactivated. **Learn more**
⚙️①	Device is deactivated until the first disarming of the system. **Learn more**
⊔①	Tamper alarm notifications are deactivated until the first disarming of the system. **Learn more**
→]	The device was not transferred to the new hub. **Learn more**

Icons on the display

Icons appear on top of the display and inform about specific system states or events.

Icon	Meaning
⊙!	System restoration is required after an alarm. The user can either send a request or restore the system depending on their **account type**. To do so, click the icon and select the required button on the screen. **Learn more**

🔥	Mute fire alarm. It appears after closing the **fire alarm muting screen**. Users can click the icon anytime and mute the fire alarm, including the interconnected fire alarm. **Learn more**
🔔	**Chime on opening** is disabled. Click the icon to enable. Appears on the display when the required **settings are adjusted**.
🔔	**Chime on opening** is enabled. Click the icon to disable. Appears on the display when the required **settings are adjusted**.

States

The states provide information about the device and its operating parameters. The states of KeyPad TouchScreen can be found in Ajax apps:

1. Go to the **Devices** ➖ tab.

2. Select **KeyPad TouchScreen** from the list.

Parameter	Value
Malfunction	Clicking on ⓘ opens the list of the KeyPad TouchScreen malfunctions. The field is displayed only if a malfunction is detected.
New firmware version available ↻	Clicking on ⓘ opens the instructions for updating the keypad's firmware. The field is displayed if a **new firmware version** is available.

	ⓘ The state is not displayed in the Ajax Security System app with version 3.0 and higher for iOS and Android.
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.
Fibra Signal Strength	Fibra signal strength between the device and the hub. The recommended value is 2–3 bars. Fibra is a protocol for transmitting KeyPad TouchScreen events and alarms.
Connection via Fibra	Connection status on the Fibra channel between the device and the hub: • **Online** — the device is connected to the hub. Normal status. • **Offline** — the device is not connected to the hub. Check the device connection.
Line Voltage	The voltage value on the Fibra line that the keypad is connected to.
Battery Charge	The device backup battery statuses: • **OK.** • **Low.** • **Charging.** • **Error.** • **Battery not installed.** The indication of the backup battery charge on the Fibra line is displayed with the 🗋

	icon.
Lid	The status of the keypad tamper that responds to detachment or opening of the device enclosure: • **Open** — the keypad was removed from the SmartBracket or its integrity was compromised. Check the device. • **Closed** — the keypad is installed on the SmartBracket mounting panel. The integrity of the device enclosure and the mounting panel is not compromised. Normal state. **Learn more**
External Power	Keypad external power supply connection status: • **Connected** — external power supply is connected to the device. • **Disconnected** — the external power is disconnected. The device runs on batteries. **Learn more**
Always Active Display	Displayed when the **Always Active Display** toggle is enabled in the keypad settings and external power supply is connected.
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 you 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	Shows the status of the keypad permanent deactivation setting: • **No** — the keypad operates in the normal mode. • **Lid only** — the hub administrator has disabled notifications about triggering of the keypad tamper.

	Entirely — the keypad is entirely excluded from the operation of the system. The device does not execute system commands and does not report alarms or other events. **Learn more**
One-Time Deactivation	Shows the status of the keypad one-time deactivation setting: • **No** — the keypad operates in the normal mode. • **Lid only** — notifications on the keypad tamper triggering are disabled until the first disarm. • **Entirely** — the keypad is entirely excluded from the operation of the system until the first disarm. The device does not execute system commands and does not report alarms or other events. **Learn more**
Firmware	Keypad firmware version.
ID	Keypad ID. Also available on the QR code on the device enclosure and its package box.
Device No.	Number of the device loop (zone).
Line No.	The number of the Fibra line that KeyPad TouchScreen is connected to.

Settings

To change the KeyPad TouchScreen settings in the Ajax app:

1. Go to the **Devices** ➖ tab.

2. Select **KeyPad TouchScreen** from the list.

3. Go to **Settings** by clicking on the ⚙ icon.

4. Set the required parameters.

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

Setting	Value
Name	Name of the keypad. Displayed in the list of hub devices, text of SMS and notifications in the events feed. To change the name of the device, click on the text field. The name can contain up to 12 Cyrillic characters or up to 24 Latin characters.
Room	Selecting the virtual room to which KeyPad TouchScreen is assigned. The room name is displayed in the text of SMS and notifications in the events feed.
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**.
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.

Screen Detection Range	Configuring a distance at which the keypad reacts to approaching and turns on a display: • Minimum. • Low. • Normal (by default). • High. • Max. Select the optimal sensitivity the keypad will respond to approaching as you prefer.
Mute Fire Alarm	When enabled, users can mute **Ajax fire detectors** alarm (even **Interconnected**) with a keypad. Learn more
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 sensitivity of the keypad's Bluetooth module: • Minimum. • Low. • Normal (by default). • High. • Max.

	Available if the **Bluetooth** toggle is enabled.
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, min	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.
Chime managing with keypad	When enabled, the user can activate/deactivate from the keypad display notifications about triggering the opening detectors. Enable additionally **Chime on opening** at keypad's settings and for at least one bistable detector. **Learn more**
Firmware Update	Switches the device to the firmware updating mode.

Fibra Signal Strength Test	Switches the device to the Fibra signal strength testing mode.
Pass/Tag Reset	Allows deleting all hubs associated with Tag or Pass from device memory.
User Guide	Opens the KeyPad TouchScreen user manual in the Ajax app.
Permanent Deactivation	Allows the user to disable 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 does not execute system commands and does not participate in automation scenarios, and the system ignores alarms and other device notifications. - **Lid only** — the system ignores the device tamper triggering notifications.
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. - **Lid only** — notifications on the device tamper triggering are disabled while the armed mode is active.

	• **Entirely** — the device is completely excluded from the operation of the system while the armed mode is active. The device does not execute system commands and does not report alarms or other events. **Learn more**
Delete Device	Unpairs the device, disconnects it from the hub, and deletes its settings.

Security Management

Setting	Value
Control Screen	Activates/deactivates security control from the keypad. When disabled, the **Control** ⊕ tab is hidden from the keypad display. The user cannot control the security mode of the system and groups from the keypad.
Shared Groups	Selecting which groups will be shared and available for management by all authorized users. All system groups and groups created after adding KeyPad TouchScreen to the hub are shared by default. **Available if Group Mode is enabled.**
Pre-authorization	When enabled, to have access to the control panel and current system state, the user should authenticate first: enter a code or present a personal access device.
Arming without Code	When enabled, the user can arm the object without entering a code or presenting the

	personal access device.

If disabled, enter a code or present the access device to arm the system. The screen for entering code appears after pressing **Arm** ◯ button.

Available if the Pre-authorization toggle is disabled. |
| Easy Armed Mode Change/Assigned Group Easy Management | When enabled, users can switch the armed mode of the system (or group) using access devices without confirmation with keypad buttons.

Available if Group Mode is disabled or only 1 group is enabled in the **Shared Groups** menu. |
| Show malfunctions list on a screen | When enabled, the list of malfunctions preventing arming will appear on the keypad display. Enable system integrity check for this. |

Automation Scenarios

Setting	Value
Scenarios Management	Activates/deactivates scenarios management from the keypad.

When disabled, the **Scenarios** ⧼▷⧽ tab is hidden from the keypad display. The user cannot control the automation scenarios from the keypad. |
| Keypad Scenarios | The menu allows you to create up to six scenarios to control one automation device or a group of devices. |

	When the settings are saved, buttons for managing scenarios appear on the keypad display (**Scenarios** 🔆 tab).
	A user or PRO with rights to configure the system can add or delete and turn on/off scenarios. Disabled scenarios don't appear on the **Scenarios** 🔆 tab of the keypad display.
Pre-authorization	When enabled, to have access to manage scenarios, the user should authenticate first: enter a code or present a personal access device.

Emergency Signals

Setting	Value
On-Screen Emergency Buttons	When enabled, the user can send an emergency signal or call for help from the keypad **Panic** ⓘ tab. When disabled, the **Panic** ⓘ tab is hidden from the keypad display.
Button type	Selecting the number of buttons to display on the **Panic** ⓘ tab. Two options are available: • Only the **Panic button** (by default). • Three buttons: **Panic button**, **Fire**, **Auxiliary alarm**.
Accidental Press Protection	When enabled, sending an alarm requires additional confirmation from the user.
Alert with a siren	
If panic button is pressed	When enabled, the sirens added to the system are activated when the **Panic button**

	is pressed.
If fire alarm button is pressed	When enabled, the sirens added to the system are activated when the **Fire** button is pressed. The toggle is displayed if an option with three buttons is enabled in the **Button type** menu.
If auxiliary request button is pressed	When enabled, the sirens added to the system are activated when the **Auxiliary alarm** button is pressed. The toggle is displayed if an option with three buttons is enabled in the **Button type** menu.

Display Settings

Setting	Value
Auto Adjust	The toggle is enabled by default. The display backlight brightness is automatically adjusted depending on the ambient light level.
Manual brightness adjustment	Selecting the display backlight level: from 0 to 100% (0 — the backlight is minimal, 100 — the backlight is maximum). Sets in increments of 10%. The backlight is on when the display is active only. Manual adjustment is available when the **Auto Adjust** toggle is disabled.
Appearance	Interface appearance adjustment: • **Dark** (by default).

	• **Light**.
Always Active Display	The keypad display always remains enabled when the toggle is enabled and the external power supply is connected. The toggle is disabled by default. In this case, the keypad sleeps after a certain time from the last interaction with the display.
Armed Mode Indication	Setting the LED indication of the keypad: • **Off** (by default) — the LED indication is off. • **Only when armed** — the LED indication turns on when the system is armed, and the keypad goes into sleep mode (the display turns off). • **Always** — the LED indication is switched on regardless of the security mode. It is activated when the keypad enters sleep mode. **Learn more**
Language	Configuring the keypad interface language. English is set by default. To change the language, select the required one and click **Save**.

Sound Indication Settings

KeyPad TouchScreen has a built-in buzzer that performs the following functions depending on the settings:

1. Indicates the security status and also the **Entry/Exit delays**.

2. Chimes on opening.

3. Informs about alarms.

> ℹ️ We do not recommend using KeyPad TouchScreen 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.

Setting	Value
Beeps Settings. 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
Beep when disarmed	
Chime on opening	When enabled, the built-in buzzer informs you 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 display.
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.
Alarm in Group Mode	Selecting the group (from the shared) which alarm the keypad will notify. 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. The connection of external power supply to the keypad is recommended for an audible signal duration of more than 30 seconds.

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

Learn more

Setting the keypad response to device alarms

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

> **i** 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 the device **Settings** by clicking on the ⚙ icon.

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.

Setting the keypad response to tamper alarm

KeyPad TouchScreen 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. Click **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.

Setting the keypad response to pressing the panic button in the Ajax apps

You can configure the keypad response to alarm when the panic button is pressed in the 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. Click **Back** to save the new settings.

Setting the keypad after-alarm indication

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 KeyPad TouchScreen after-alarm indication does not work for always active detectors, if the detector was triggered when the system was disarmed.

To enable the KeyPad TouchScreen after-alarm indication, in Ajax PRO app**:**

1. Go to hub settings:

   - Hub → Settings ⚙ → Service → LED Indication.

2. Specify which events KeyPad TouchScreen 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 KeyPad TouchScreen in the **Devices** menu. Click **Back** to save the parameters.

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

How to set Chime

If **Chime on opening** is enabled, KeyPad TouchScreen notify you 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 KeyPad TouchScreen 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. Click **Back** to save the settings.

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

To set the chime control from the keypad display:

1. Open the Ajax app.

2. Go to the **Devices** ➖ tab.

3. Select KeyPad TouchScreen and go to its **Settings** ⚙.

4. Enable the **Chime managing with keypad** toggle.

If the settings are made correctly, a **bell icon** appears in the **Control** ⊕ tab on the keypad display. Click it to activate/deactivate chime on opening.

Codes setting

Keypad access codes ⌄

User access codes ⌄

Unregistered user codes ⌄

RRU Code ⌄

Cards and key fobs adding

KeyPad TouchScreen can work with **Tag key fobs**, **Pass cards**, and third-party devices that support DESFire® technology.
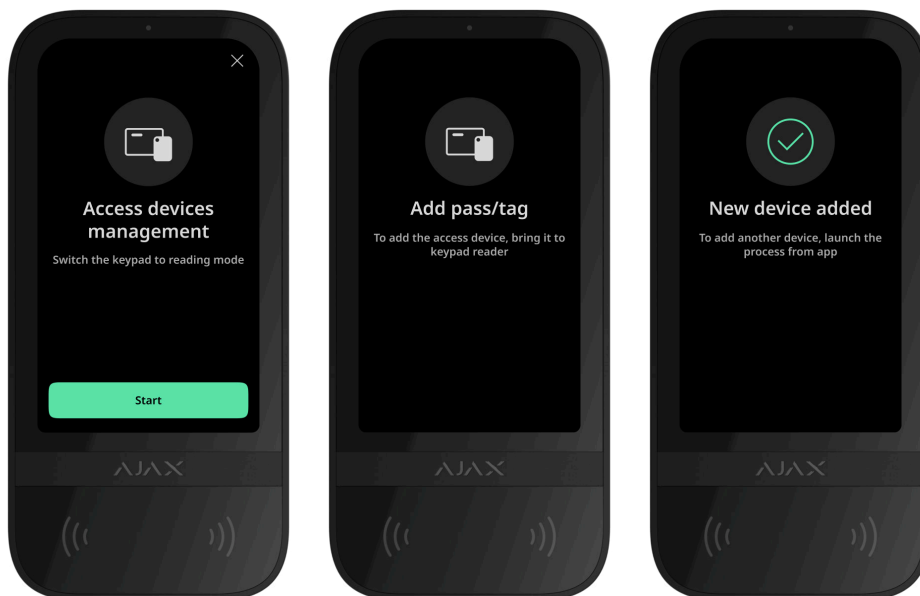
The maximum number of connected Passes and Tags is 50 for **Hub Hybrid (2G)** and **Hub Hybrid (4G)**. The connected Passes and Tags do not affect the total device limit on the hub.

How to add a Tag or Pass to the system

1. Open the Ajax app.

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

3. Go to the **Devices** ▬ tab.

ⓘ 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), colour, device name, and user (if necessary).

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

8. Go to any compatible keypad with **Pass/Tag Reading** enabled and activate it.

   After activation, KeyPad TouchScreen will display a screen for switching the keypad to the access devices registration mode. Click the **Start** button.

> ⓘ   A screen updates automatically if the external power supply is connected and the **Always Active Display** toggle is enabled in the keypad settings.

   The screen for switching the keypad to the registration mode will appear on all KeyPad TouchScreen of the system. When an admin or PRO with rights to configure the system starts registering Tag/Pass at one keypad, the rest will switch to their initial state.

9. Present Pass or Tag with the wide side to the keypad reader for a few seconds. It is marked with wave ⁽⁽·⁾⁾ icons on the body. Upon successful addition, you will receive a notification in the Ajax app and on the keypad display.

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.

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

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

How to delete a Tag or Pass from the hub

> ⚠️ 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 hub.

3. Go to the **Devices** ⬛ tab.

4. Select a compatible keypad from the device list.

> ℹ️ Make sure the **Pass/Tag Reading** feature is enabled in the keypad settings.

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

6. Click **Pass/Tag Reset** menu.

7. Click **Continue**.

8. Go to any compatible keypad with **Pass/Tag Reading** enabled and activate it.

   After activation, KeyPad TouchScreen will display a screen for switching the keypad to the access devices resetting mode. Click the **Start** button.

> ℹ️ A screen updates automatically if the external power supply is connected and the **Always Active Display** toggle is enabled in the keypad settings.

The screen for switching the keypad to the resetting mode will appear on all KeyPad TouchScreen of the system. When an admin or PRO with rights to configure the system starts resetting Tag/Pass at one keypad, the rest will switch to the initial state.

9. Put Pass or Tag with the wide side to the keypad reader for a few seconds. It is marked with wave $^{((\cdot))}$ icons on the body. Upon successful formatting, you will receive a notification in the Ajax app and on the keypad display. If the formatting fails, try again.

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

Bluetooth Setting

KeyPad TouchScreen supports security modes control by presenting 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. Connect KeyPad TouchScreen to the hub.

2. Enable the keypad Bluetooth sensor:

   Devices ➖ → **KeyPad Touchscreen** → **Settings** ⚙️ → Enable the **Bluetooth** toggle.

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

To set up Bluetooth authentication

1. Open the Ajax Security System app and select the hub to which the KeyPad TouchScreen 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 KeyPad TouchScreen **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.
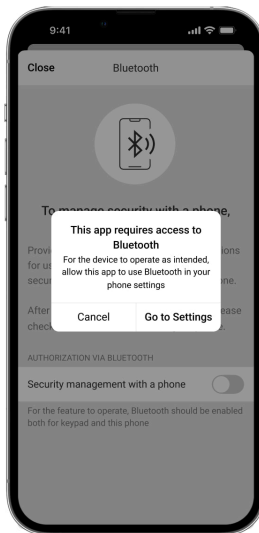
Also, the **Security management with a phone** toggle can be enabled in the app settings:

- Click the ≡ icon in the upper left corner of the screen, select the **App Settings** menu.

- Open menu **System Settings** and enable **Security management with a phone** toggle.
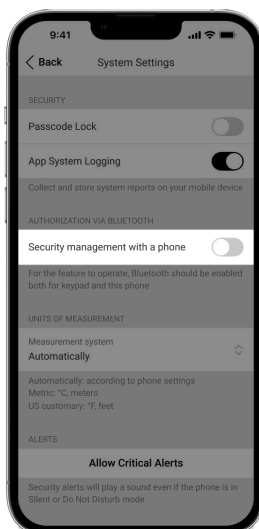
3. We recommend configuring **Geofence** for the stable performance of Bluetooth authentication. The warning ⚠ appears at KeyPad TouchScreen **States** if **Geofence** is disabled and the app is not allowed to use the smartphone location. Pressing the ⓘ symbol opens the window with explanations of what to do.
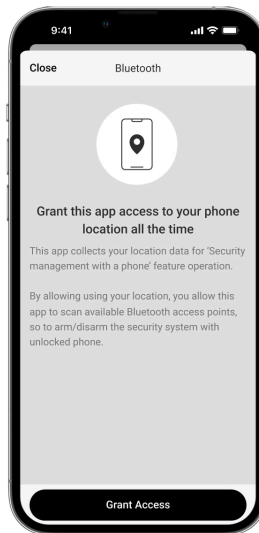
> ℹ️ Bluetooth authentication can be unstable if **Geofence** function is disabled. You will need to launch and minimize the app if the system switches it to the sleep mode.
>
> You can control the system faster via Bluetooth, when the **Geofence** function is activated and configured. All you need is 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**.

Pre-authorization

When the feature is enabled, access to the control panel and current system state is blocked. To unblock it, the user should authenticate: enter an **appropriate code** or present a personal access device to the keypad.

> **i** If pre-authorization is enabled, the **Arming without Code** feature is unavailable in the keypad settings.

You can authenticate in two ways:

1. In the **Control** ⊕ tab. After login, the user will see the shared groups of the system (if Group Mode is activated). They are specified in the keypad settings: **Security Management** → **Shared Groups**. By default, all the system groups are shared.
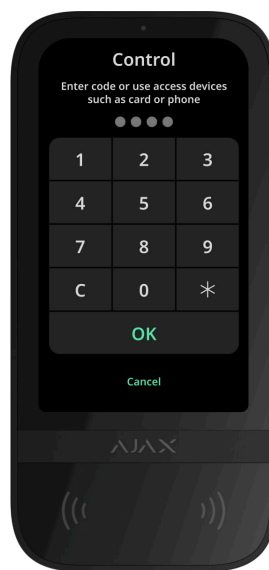
2. In the **Log in** ⌃ tab. After login, the user will see available groups that were hidden from the shared group list.
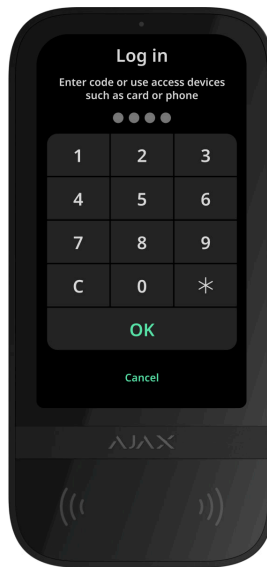
> ℹ️ The keypad display switches to the initial screen after 10 seconds from the last interaction with it. Enter the code or present a personal access device again to control the system with KeyPad TouchScreen.

Pre-authorization with a keypad code ⌄

Pre-authorization with a personal code ⌄

Pre-authorization with an access code ⌄

Pre-authorization with a RRU code ⌄

Pre-authorization with Tag or Pass ⌄

Pre-authorization with a smartphone ⌄

Controlling security

Using codes, Tag/Pass, or a smartphone, you can control the **Night Mode** and the security of the entire object 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.

> ℹ️ KeyPad TouchScreen 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 KeyPad TouchScreen in the Ajax app.

If **Group Mode** is disabled, an appropriate icon on the keypad display indicates the current security mode:

- ○ — Armed.

- ◡ — Disarmed.

- ◎ — Night Mode.
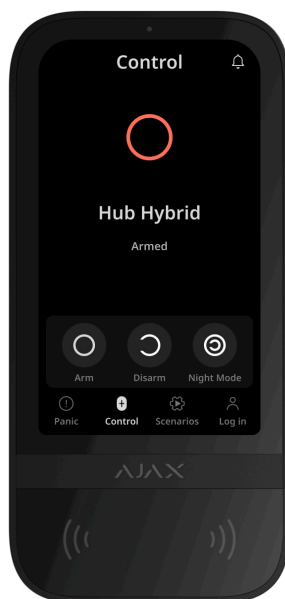
If Group Mode is enabled, users see the security mode of each group separately. The group is armed if its button outline is white and it is

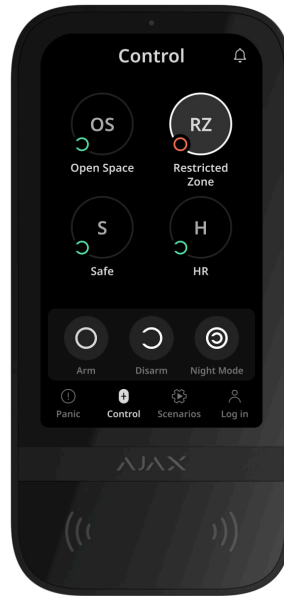marked with ◯ icon. The group is disarmed if its button outline is grey and it is marked with ◡ icon.

The buttons of the groups in the **Night Mode** are framed in a white square on the keypad display.
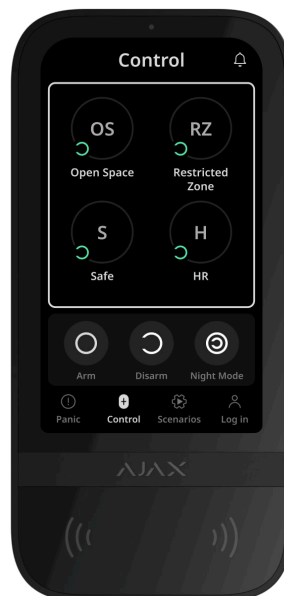
If a personal or access code, Tag/Pass, or smartphone is used, the name of the user who changed the security mode is displayed in the hub event feed and in the notifications list. If a general code is used, the name of the keypad from which the security mode was changed is displayed.

The step sequence to change the security mode with the keypad depends on whether user pre-authorization is enabled in the KeyPad TouchScreen settings.

If pre-authorization is enabled

Security control of the object ⌄

Security control of the group ⌄

Using a duress code ⌄

If pre-authorization is disabled

Security control of the object ⌄

Security control of the group ⌄

Using a duress code ⌄

Example of entering codes

Code	Example	Note
Keypad code Keypad duress code	1234 → OK	Incorrectly entered numbers can be cleared with the **C** button.

User code User duress code	2 → ✳ → 1234 → OK	Enter the **user ID** first, press the ✳ button, and then enter a personal code. Incorrectly entered numbers can be cleared with the C button.
Code of unregistered user Duress code of unregistered user	1234 → OK	Incorrectly entered numbers can be cleared with the C button.
RRU Code	1234 → OK	Incorrectly entered numbers can be cleared with the C button.

Easy armed mode change

Easy armed mode change feature allows you to change the security mode to the opposite using Tag/Pass or smartphone, without confirmation with the Arm ⭕ or Disarm ◝ buttons. Go to the **keypad settings** to enable the feature.

To change the security mode to the opposite

1. Activate the keypad by approaching it or holding your hand in front of the sensor. Perform **pre-authorization** if necessary.

2. Present Tag/Pass or smartphone.

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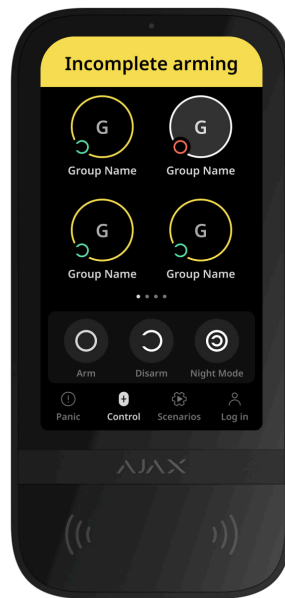
KeyPad TouchScreen can participate in two-stage arming but cannot be used as a second-stage device. The two-stage arming process using Tag, Pass or smartphone is similar to using a personal or general code on the keypad.

Learn more

The system users can see whether the arming is started or incomplete on the keypad display. If Group Mode is activated, the colour of the group buttons depends on the current state:

- **Grey** — disarmed, arming process not started.

- **Green** — arming process started.

- **Yellow** — arming is incomplete.

- **White** — armed.

Managing scenarios with the keypad

KeyPad TouchScreen allows you to create up to six scenarios to control one or a group of automation devices.

To create a scenario:

1. Open the **Ajax app**. Select the hub with at least one KeyPad TouchScreen and **automation device**. Add one if necessary.

2. Go to the **Devices** ➖ tab.

3. Select KeyPad TouchScreen from the list and go to the **Settings** ⚙ menu.

4. Go to the **Automation Scenarios** menu. Enable the **Scenarios Management** toggle.

5. Open the **Keypad Scenarios** menu.

6. Press **Add Scenario**.

7. Select one or more automation devices. Press **Next**.

8. Enter the scenario name in the **Name** field.

9. Select device action during the scenario performance.

10. Press **Save**.

11. Press **Back** to return to the **Automation Scenarios** menu.

12. If necessary, activate the **Pre-authorization** toggle.

Created scenarios are displayed in the app: **KeyPad TouchScreen →
Settings** ⚙ **→ Automation Scenarios → Keypad Scenarios**. You can turn
them off, adjust settings, or delete them at any time.

To remove a scenario:

1. Go to the **Settings** ⚙ of KeyPad TouchScreen.

2. Open **Automation Scenarios → Keypad Scenarios** menu.

3. Select the scenario you want to remove.

4. Press **Next**.

5. Press **Delete Scenario**.

The user can see and manage automation scenarios after authentication
when the **Pre-authorization** feature is enabled. Go to the **Scenarios** ⚙ tab,

enter the code or present a personal access device to the keypad.

To perform a scenario, press an appropriate button in the **Scenarios** ⚙ tab.

> ℹ The KeyPad TouchScreen display shows only activated scenarios in the keypad settings.

Fire alarm muting

Chapter in progress

Indication

KeyPad TouchScreen informs users about alarms, entry/exit delays, current security mode, malfunctions, and other system states with:

- display;

- logo with an LED indicator;

- built-in buzzer.

KeyPad TouchScreen indication is shown on the display only when it is active. Icons that indicate some system or keypad states are displayed in the upper part of the **Control** ⊕ tab. For example, they can indicate a fire alarm, system restoration after an alarm, and chime on opening. Information about the security mode will be updated even if it is changed by another device: key fob, another keypad, or in the app.

Event	Indication	Note
Alarm.	The built-in buzzer emits an acoustic signal.	If **Activate keypad buzzer if alarm in the system is detected** toggle is enabled.

		The duration of the acoustic signal depends on the keypad settings.
An alarm was detected in the armed system.	The LED indicator flashes twice approximately every 3 seconds until the system is disarmed.	To activate, enable the **after-alarm indication** in the hub settings. Also, specify KeyPad TouchScreen as a device for informing about other devices' alarms. The indication turns on after the built-in buzzer has completed playing the alarm signal.
Switching on the device/Loading the updated system configuration to the keypad.	An appropriate notification is shown on the display while the data is loading.	
Switching off the device.	The LED indicator lights up for 1 second, then flashes three times.	
The system or the group is armed.	The built-in buzzer emits a short beep.	If notifications for **Arming/Disarming** are enabled.
The system or the group is switched to the **Night Mode**.	The built-in buzzer emits a short beep.	If notifications for **Night Mode Activation/Deactivation** are enabled.
The system is disarmed.	The built-in buzzer emits two short beeps.	If notifications for **Arming/Disarming** are enabled.
System in the armed mode.	The LED indicator lights up red for a short time every 3 seconds if the external power is not connected. The LED indicator constantly lights up red if the external power is connected.	If **Armed Mode Indication** is enabled. The indication turns on when the keypad switches to sleep mode (the display goes out).

An incorrect code was entered.	An appropriate notification is shown on the display. The built-in buzzer emits a short beep (if adjusted).	The beep loudness depends on the configured buttons' volume.
Error when adding a card/key fob.	An appropriate notification is shown on the display. The LED indicator lights up red once. The built-in buzzer emits a long beep.	The beep loudness depends on the configured buttons' volume.
Successfully added card/key fob.	An appropriate notification is shown on the display. The built-in buzzer emits a short beep.	The beep loudness depends on the configured buttons' volume.
Low backup battery.	The LED indicator smoothly lights up and goes out when the tamper is triggered, an alarm is activated, or the system is armed or disarmed (if the indication is activated).	
Tamper triggering.	The LED indicator lights up red for 1 second.	
Fibra Signal Strength Test.	The LED indicator lights up green during the test.	Turns on after launching an appropriate test in the **keypad settings**.
Firmware update.	The LED indicator periodically lights up green while the firmware is updating.	Turns on after launching the firmware update in the keypad **States**.
Muting interconnected fire alarm.	An appropriate notification is shown on the display. The built-in buzzer emits an acoustic signal.	

The keypad is deactivated.	An appropriate notification is shown on the display.	If **Entirely** option is selected for the **Permanent** or **One-Time Deactivation** keypad settings.
System restoration is required.	An appropriate screen to restore or send a request for the system restoration after the alarm appears on the display.	The **Restoration After Alarm feature** has to be adjusted in the system. The screen appears when arming or switching the system to the **Night Mode** if an alarm or malfunction occurred in the system before. Admins or PROs with the rights to configure the system can restore the system. Other users can send a request for restoration.
Intending to arm the system when it is already armed.	An appropriate notification is shown on the display. The built-in buzzer emits a short beep.	After entering the correct code and if notifications for **Arming/Disarming** are enabled.
Intending to disarm the system when it is already disarmed.	An appropriate notification is shown on the display. The built-in buzzer emits two short beeps.	After entering the correct code and if notifications for **Arming/Disarming** are enabled.
Removing the keypad from the hub.	The LED indicator flashes red 6 times, then 3 times, but faster.	
The keypad is locked if the code is entered incorrectly.	An appropriate notification is shown on the display. The built-in buzzer emits a beep.	The beep loudness depends on the configured buttons' volume.

Sound notifications of malfunctions

If any device is offline or the battery is low, KeyPad TouchScreen can notify system users with an audible sound. The keypad's LED indicator will also flash. Malfunction notifications will be displayed in the events feed, SMS, or push notification.

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

1. Click **Devices** ⬛, choose hub and open its settings ⚙:

   Click **Service → Sounds and Alerts**.

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

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

Event	Indication	Note
If any device is offline.	Two short sound signals, LED indicator flashes twice. Beep occurs once per minute until all devices in the system are online.	Users can delay sound indication for 12 hours.
If KeyPad TouchScreen is offline.	Two short sound signals, LED indicator flashes twice. Beep occurs once per minute until the keypad in the system is online.	Sound indication delay is not possible.
If the battery of any device is low.	Three short sound signals, LED indicator flashes three times. Beep occurs once per minute until the battery is	Users can delay sound indication for 4 hours.

| | restored or the device is removed. | |

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

Functionality testing

The Ajax system offers several types of tests to help select the correct installation place for the devices. Tests do not start immediately. However, the waiting time does not exceed the duration of one "hub-device" ping interval. Ping interval can be checked and configured at hub settings (**Hub → Settings** ⚙ **→ Jeweller/Fibra**).

To run a test, in the Ajax app:

1. Select the required hub.

2. Go to the **Devices** ➖ tab.

3. Select **KeyPad TouchScreen** from the list.

4. Go to **Settings** ⚙.

5. Run the Fibra Signal Strength Test.

Device placement

⚠ The device is designed for indoor use only.

When choosing a location for the device, consider the parameters that affect its operation:

- Fibra signal strength.

- Length of the cable used to connect KeyPad TouchScreen.

Follow these recommendations when designing the system project for an object. Only professionals should design and install the Ajax system. The list of authorized Ajax partners is **available here**.

KeyPad TouchScreen is best placed indoors near the entrance. This allows disarming the system before the entry delays have expired and quickly arming the system when leaving the premises.

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

Signal strength

The Fibra signal strength is determined by the number of undelivered or corrupted data packages over a certain period of time. The icon ılıl 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.

> **What is Fibra Signal Strength Test**

Do not install the keypad

1. Outdoors. This can lead to keypad failure.

2. 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 false triggering of the keypad.

3. Inside premises with temperature and humidity outside the permissible limits. This could damage the keypad.

4. In a place with a low signal level. This may result in the loss of the connection with the hub.

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

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

Designing

It is crucial to design the system project properly to ensure the correct installation and configuration of the devices. The design must consider the number and types of devices at the object, their exact locations and installation heights, the length of wired Fibra lines, the type of cable used, and other parameters. Refer to **the article** to learn 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 — 500 meters.

Recommended cable types:

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

- Signal cable 4 × 0.22, copper conductor.

> **i** Please note, the wired connection range might vary if other cable types are used. As of now, no other cable types have been tested.

Verification using a calculator

To ensure that the project is designed correctly and the system functions as intended in practice, we have developed a **Fibra power supply calculator**. It helps to check the communication quality and cable length for wired Fibra devices when designing the system project.

Preparing for installation

Cable arrangement

Before laying cables, check the electrical and fire safety regulations applicable in your region. Strictly follow these standards and regulations. Tips for cable arrangement are available in **this article**.

Cable routing

Before beginning the installation, we strongly advise reviewing the **Device placement** section thoroughly. Stick to the outlined system project without deviation. Violation of the basic KeyPad TouchScreen installation rules and the recommendations of this manual may lead to incorrect operation, as well as loss of connection with the device. Tips for cable routing are available in **this article**.

Preparing cables for connection

First, remove the insulation 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. This ensures a reliable connection and protects the conductor from oxidation. Tips for preparing the cables are available in **this article**.
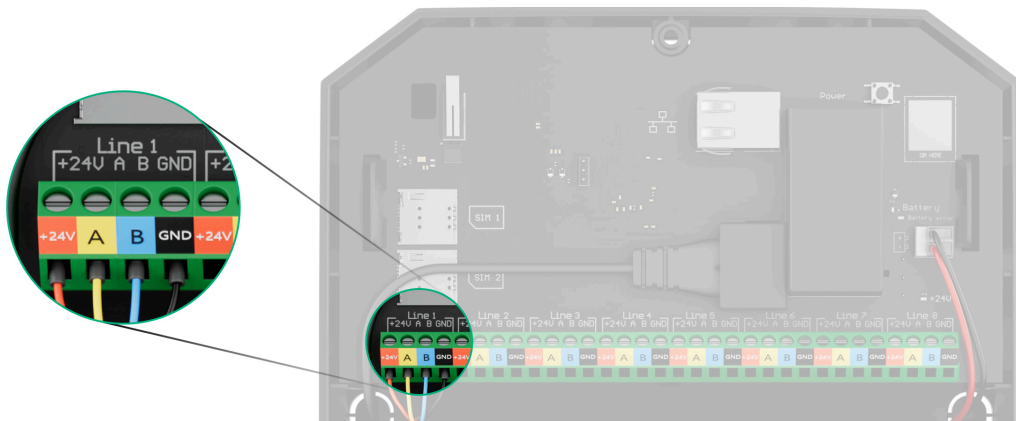
Installation

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 KeyPad TouchScreen to the hub casing. Connect the wires to the required hub line.
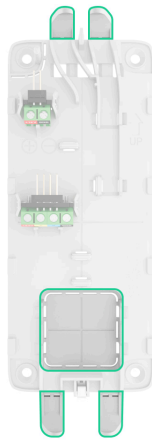

+24V — 24 V⎓ power terminal.
A, B — signal terminals.
GND — ground.

3. Remove the SmartBracket mounting panel from the keypad. Unscrew the holding screw first and slide the panel down.

4. Carefully break out the necessary perforated part to output the cable from the rear side (top, bottom, or through the wall).

5. Run the cable from the hub and optionally an **external power supply** unit into the keypad enclosure.

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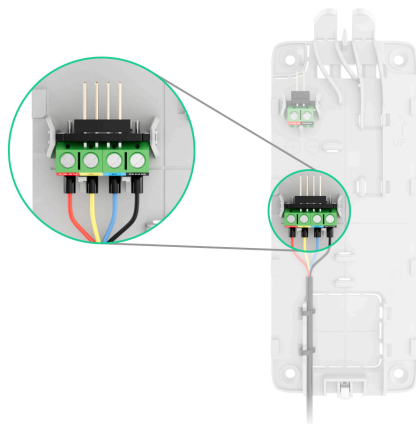

1. If KeyPad TouchScreen is not the last device on the Fibra line, prepare a second cable in advance. Connect the wires to the keypad terminals according to the figure below. The ends of the wires of the first and second cables, which will be inserted into the detector terminals, must be tinned and soldered together, or crimped with a sleeve.
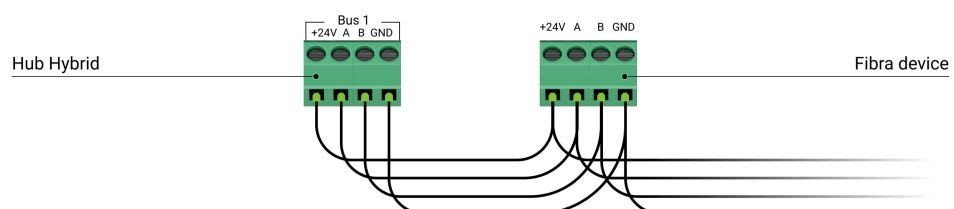
2. If KeyPad TouchScreen is the last device on the line and you are using the **Beam (Radial) connection**, install a terminating resistor on the two contacts by connecting it to the signal terminals of the keypad. A terminating resistor (120 Ohm) is included in the Hub Hybrid complete set.
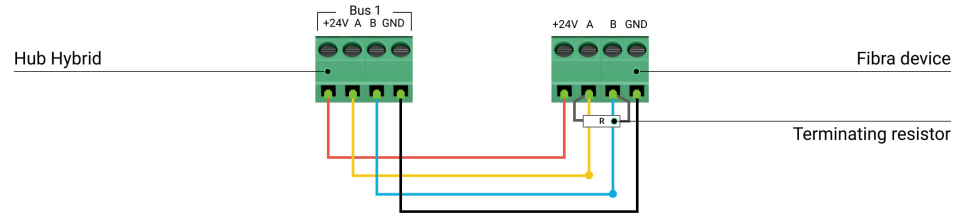
7. Connect the external power supply cable to the corresponding terminals. It is needed for keeping the display always active.
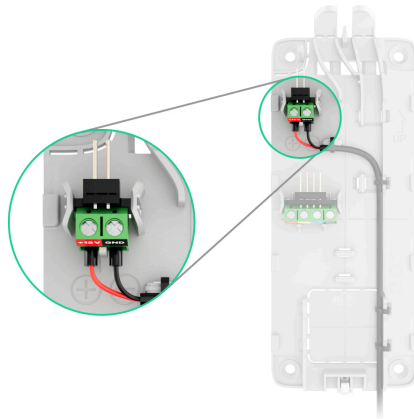
8. Route the cables through the channels and fix them with ties.
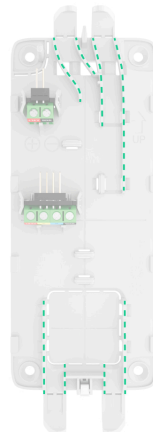
Examples of cable routing:

To the keypad bottom ⌄

To the keypad top ⌄

9. Temporarily fix the SmartBracket mounting panel using double-sided adhesive tape to the selected installation spot.

> ⚠️ 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 markings on the inner side for easy installation. The intersection of two lines marks the center of the device (not the mounting panel). Also, the **UP** key on SmartBracket marks the top of the keypad. Orient these markings when installing the keypad.
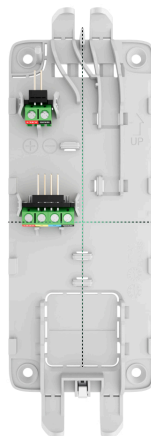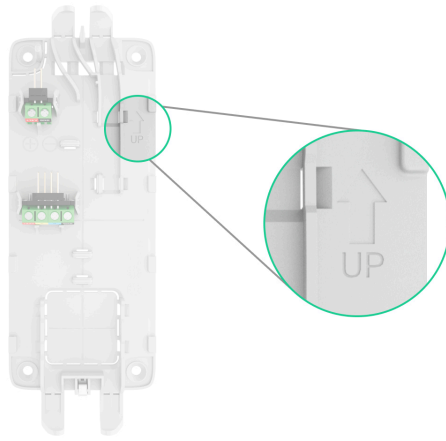
10. Place the keypad on SmartBracket.

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

- **Hub** → **Settings** ⚙ → **Lines** → **Lines Power Supply**.

12. 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.

13. Add the keypad to the hub.

14. Run the keypad functionality testing.

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

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

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

17. Place the keypad on the SmartBracket mounting panel.

18. 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.

Connecting a third-party power supply unit

When connecting a third-party power supply unit and using KeyPad TouchScreen, follow the general electrical safety regulations for using electrical appliances, as well as the requirements of regulatory legal acts on electrical safety.

KeyPad TouchScreen is equipped with terminals for connecting a 10.5–14 V⎓ power supply unit. Recommended electrical parameters for the power supply unit are: 12 V⎓ with a current from 0.5 A.

Do not remove the pre-installed backup batteries while connecting the power supply.

> ⚠️ Before installing the device, make sure to check the wires for any damage to the insulation. Use only a grounded power source. Do not disassemble the device while it's under voltage. Do not use the device with a damaged power cable.

To connect a third-party power supply unit:

1. Remove the SmartBracket mounting panel. Carefully break out the perforated part of the enclosure to prepare the holes for the cable:
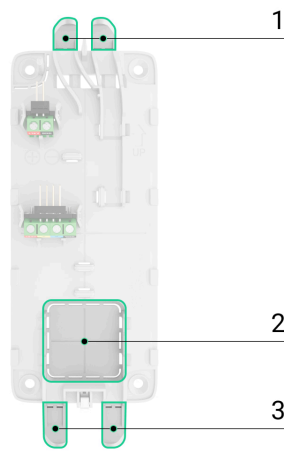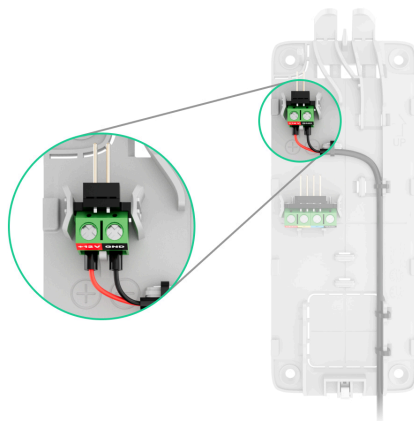
1 — to output the cable from the top; it is enough to break out one of the perforated parts.

2 — to output the cable through the wall.

3 — to output the cable from the bottom; it is enough to break out one of the perforated parts.

2. De-energize external power supply cable.

3. Connect the cable to the terminals, observing the polarity (marked on the plastic).

4. Once the keypad is **installed** and added to the hub, check the status of the backup batteries and external power in the Ajax app, as well as the overall operation of the device.

Firmware update

The KeyPad TouchScreen firmware update can be installed when a new version is available. You can find out about this in the devices list in Ajax PRO: Tool for Engineers and PRO Desktop apps. If an update is available, the corresponding keypad will have an **icon** ↻. An admin or a PRO with access to the system settings can run an update in the KeyPad TouchScreen **states** or **settings**. An update takes up to 1 hour.

How to update KeyPad TouchScreen firmware

Maintenance

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

Do not use substances that contain alcohol, acetone, petrol, and other active solvents to clean the device. Gently wipe the touch screen.

The device runs for up to 1.5 years on the pre-installed batteries — a calculated value based on default settings and up to 4 daily interactions with the keypad.

The system will send an early warning when it's time to replace the batteries. When changing the security mode, the LED will slowly light up and go out.

Technical specifications

All technical specifications of KeyPad TouchScreen Fibra

Compliance with standards

Setup in compliance with EN 50131 requirements

Warranty

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

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

Warranty obligations

User agreement

Contact Technical Support:

- **e-mail**

- **Telegram**

Manufactured by "AS Manufacturing" LLC

Subscribe to the newsletter about safe life. No spam

Email

Subscribe

Subscribe to the newsletter about safe life. No spam