KeyPad User Manual

KeyPad is a wireless indoor touch-sensitive keyboard for managing the Ajax security system. With this device, the user can arm and disarm the system and see its security status. KeyPad is protected against attempts to guess the passcode and can raise a silent alarm when the passcode is entered under duress.

Connecting to the Ajax security system via a secured **Jeweller** radio protocol, KeyPad communicates with the **hub** at a distance of up to 1,700 m in line of sight.

> ⚠️ KeyPad operates with Ajax hubs only and does not support connecting via **ocBridge Plus** or **uartBridge** integration modules.

The device is set up via the **Ajax apps** for iOS, Android, macOS, and Windows.

☞ **Buy keypad KeyPad**

Functional elements
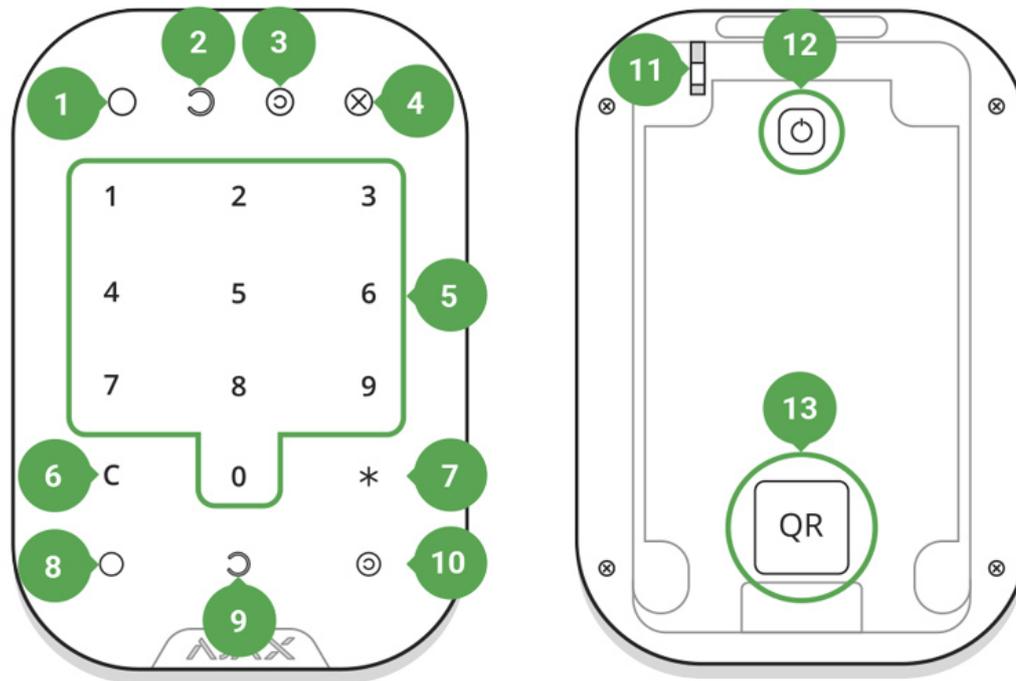
1. Armed mode indicator

2. Disarmed mode indicator

3. Night mode indicator

4. Malfunction indicator

5. The block of numerical buttons

6. "Clear" button

7. "Function" button

8. "Arm" button

9. "Disarm" button

10. "Night mode" button

11. Tamper button

12. On/Off button

13. QR code

To remove the SmartBracket panel, slide it down (perforated part is required for actuating the tamper in case of any attempt to tear off the device from the surface).

Operating Principle

KeyPad is a stationary control device located indoors. Its functions include arming/disarming the system with a numerical combination (or just by pressing the button), activating Night Mode, indicating the security mode, blocking when someone tries to guess the passcode and raising the silent alarm when someone forces the user to disarm the system.

KeyPad indicates the state of communication with the hub and system malfunctions. Buttons are highlighted once the user touches the keyboard so you can enter the passcode without external lighting. KeyPad also uses a beeper sound for indication.

To activate KeyPad, touch the keyboard: the backlight will switch on, and the beeper sound will indicate that KeyPad has woken up.

If the battery is low, the backlight switches on at a minimum level, regardless of the settings.

If you do not touch the keyboard for 4 seconds, KeyPad dims the backlight, and after another 12 seconds, the device switches to the sleep mode.

> **i** When switching to sleep mode, KeyPad clears the entered commands!

KeyPad supports passcodes of 4-6 digits. The entered passcode is sent to the hub after pressing the button: ○ (arm), ◡ (disarm) or ◎ (Night mode). Incorrect commands can be reset with the **C** button (Reset).

When incorrect passcode is entered three times during 30 minutes, KeyPad locks for the time preset by the administrator user. Once KeyPad is locked, the hub ignores any commands, simultaneously notifying the security system users of the attempt to guess the passcode. The administrator user can unlock KeyPad in the app. When the pre-set time is up, KeyPad unlocks automatically.

KeyPad allows arming the system without passcode: by pressing the button ○ (Arm). This feature is disabled by default.

When the function button (*) is pressed without entering the passcode, the hub executes the command assigned to this button in the app.

KeyPad can notify a security company of the system being disarmed by force. The **Duress Code** — unlike the panic button — does not activate sirens. KeyPad and the app notify of successful disarming the system, but the security company receives an alarm.

Indication

When touching KeyPad, it wakes up highlighting the keyboard and indicating the security mode: Armed, Disarmed, or Night Mode. The security mode is always actual, regardless of the control device that was used to change it (the key fob or app).

Event	Indication
Malfunction indicator blinks	Indicator notifies about lack of communication with hub or keypad lid opening. You can check the reason for malfunction in the **Ajax Security System app**.
KeyPad button pressed	Short sound signal
The system is armed	Short sound signal, Armed mode / Night mode LED indicator lights up
The system is disarmed	Two short sound signals, LED disarmed LED indicator lights up
Incorrect passcode	Long sound signal, the keyboard backlight blinks 3 times
Failed to arm one or several detectors (e.g., a window is opened)	Long sound signal, the security mode indicator blinks 3 times
A malfunction is detected when arming (e.g., the detector is lost)	Long sound signal, the malfunction indicator blinks 3 times
The hub does not respond to the command — no connection	Long sound signal, the malfunction indicator lights up
KeyPad is locked after 3 unsuccessful attempts to enter the passcode	Long sound signal, security mode indicators blink simultaneously
Low battery	After arming/disarming the system, the malfunction indicator blinks smoothly. The keyboard is locked while the indicator blinks.

	When activating KeyPad with low batteries, it will beep with a long sound signal, the malfunction indicator smoothly lights up and then switches off.

Connecting

Before connecting the device:

1. Switch on the hub and check its Internet connection (the logo glows white or green).

2. Install the **Ajax app**. Create the account, add the hub to the app, and create at least one room.

3. Make sure that the hub is not armed, and it does not update by checking its status in the Ajax app.

> ⚠️ Only users with administrator rights can add a device to the app

How to connect KeyPad to the hub:

1. Select the **Add Device** option in the Ajax app.

2. Name the device, scan/write manually the **QR Code** (located on the body and packaging), and select the location room.

3. Select **Add** — the countdown will begin.

4. Switch on KeyPad by holding power button for 3 seconds — it will blink once with the keyboard backlight.

For detection and pairing to occur, KeyPad should be located within the coverage of the wireless network of the hub (at the same protected object).

A request for connection to the hub is transmitted for a short time at the moment of switching on the device.

If KeyPad failed to connect to the hub, switch it off for 5 seconds and retry.

The connected device will appear in the app device list. Update of the device statuses in the list depends on the detector ping interval in the hub settings (the default value is 36 seconds).

After pairing, the KeyPad default passcode is 123456 and Duress Code is 123457.

Selecting the Location

The location of the device depends on its remoteness from the hub, and obstacles hindering the radio signal transmission: walls, floors, large objects inside the room.

Do not install KeyPad:

1. Near the radio transmission equipment, including that operates in 2G/3G/4G mobile networks, Wi-Fi routers, transceivers, radio stations, as well as an Ajax hub (it uses a GSM network).

2. Close to electrical wiring.

3. Close to metal objects and mirrors that can cause radio signal attenuation or shading.

4. Outside the premises (outdoors).

5. Inside premises with the temperature and humidity beyond the range of permissible limits.

6. Closer than 1 m to the hub.

> ⚠️ Check the Jeweller signal strength at the installation location

During testing, the signal level is displayed in the app and on the keyboard with security mode indicators ◯ (Armed mode), ◠ (Disarmed mode), ◉ (Night mode) and malfunction indicator **X**.

If the signal level is low (one bar), we cannot guarantee the stable operation of the device. Take all possible measures to improve the quality of the signal. At least, move the device: even a 20 cm shift can significantly improve the quality of signal reception.

If the device has low or unstable signal strength even after moving, use a **ReX radio signal range extender**.

KeyPad is designed for operation when fixed to the vertical surface. When using KeyPad in hands, we cannot guarantee successful operation of the sensor keyboard.

States

1. Devices

2. KeyPad
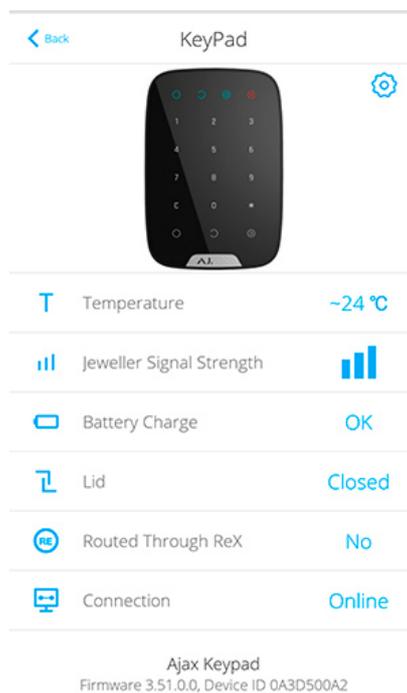
Parameter	Value
Temperature	Temperature of the device. Measured on the processor and changes gradually
Jeweller Signal Strength	Signal strength between the hub and KeyPad
Connection	Connection status between the hub and the KeyPad

Battery Charge	Battery level of the device
Lid	The tamper mode of the device, which reacts to the detachment of or damage to the body
Routed Through ReX	Displays the status of using the ReX range extender
Firmware	Detector firmware version
Device ID	Device identifier

Settings

1. Devices

2. KeyPad

3. Settings ⚙

Access Options   Keypad and user passcode ⌄

Function Button   Off ⌄

Arming without Password

Auto-lock After Wrong Password Attempts

Passcode   ······ ✎

Duress Code   ······ ✎

Brightness

Volume

📶   Jeweller Signal Strength Test

⚙   Attenuation Test

📄   User Guide

Unpair Device
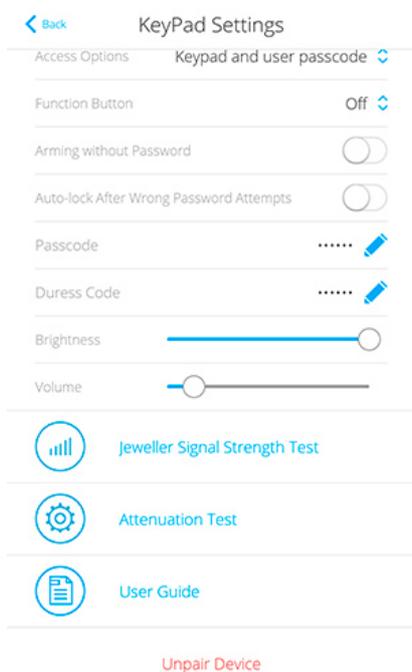
Setting	Value
First field	Device name, can be edited
Room	Selecting the virtual room to which the device is assigned
Arming/Disarming Permissions	Selecting the security group to which KeyPad is assigned
Access option	Selecting the way of verification for arming/disarming • KeyPad passcode only • User passcode only • KeyPad and User passcode
Passcode	Setting a passcode for arming/disarming
Duress code	Setting a duress code for silent alarm
Function Button	Selecting the functionality for the function button • Off • Send panic alarm • Silence fire alarm
Arming without passcode	If active, the system can be armed by pressing Arm button without passcode

Auto-lock after wrong password attempts	If active, the keyboard is locked for the pre-set time after entering incorrect passcode three times in a row (during 30 min). During this time, the system cannot be disarmed via KeyPad.
Auto-lock time (min)	Lock period after wrong passcode attempts
Brightness	Brightness of the keyboard backlight
Volume	Volume of the beeper
Jeweller Signal Strength Test	Switches the device to the signal strength test mode
Attenuation Test	Switches the KeyPad to the signal fade test mode (available in devices with **firmware version 3.50 and later**)
User Manual	Opens the KeyPad User Manual
Unpair Device	Disconnects the device from the hub and deletes its settings

KeyPad allows to set both general and personal passcodes for each user.

To install a personal passcode:

1. Go to profile settings (**Hub** > **Settings** ⚙ > **Users** > **Your profile settings**)

2. Click **Access Code Settings** (in this menu you can also see the user identifier)

3. Set the **User Code** and **Duress Code**

> ℹ️ Each user sets a personal passcode individually!

To control the system using the personal passcode:

- **Enter**: User identifier * personal passcode > Arm / disarm button

To control a specific group:

- **Enter:** User identifier * personal passcode * group identifier > Arm / disarm button

Functionality Testing

The Ajax security system allows conducting tests for checking the functionality of connected devices.

The tests do not start straight away but within a period of 36 seconds when using the standard settings. The test time start depends on the settings of the detector scanning period (the paragraph on "**Jeweller**" settings in hub settings).

Jeweller Signal Strength Test

Attenuation Test

Installation

> ⚠️ Before installing the detector, make sure that you have selected the optimal location and it is in compliance with the guidelines contained in this manual!

> ℹ️ KeyPad should be attached to the vertical surface.

1. Attach the SmartBracket panel to the surface using bundled screws, using at least two fixing points (one of them — above the tamper). After selecting other attachment hardware, make sure that they do not damage or deform the panel.

> ⚠️ The double-sided adhesive tape may be only used for temporary attachment of KeyPad. The tape will run dry in course of time, which may result in the falling of the KeyPad and damage of the device.

2. Put KeyPad on the attachment panel and tighten the mounting screw on the body underside.

As soon as the KeyPad is fixed in SmartBracket, it will blink with the LED **X** (Fault) — this will be a signal that the tamper has been actuated.

If the malfunction indicator **X** did not blink after installation in SmartBracket, check the status of the tamper in the **Ajax app** and then check the fixing tightness of the panel.

If the KeyPad is torn off from the surface or removed from the attachment panel, you will receive the notification.

KeyPad Maintenance and Battery Replacement

Check the KeyPad operating capability on a regular basis.

The battery installed in the KeyPad ensures up to 2 years of autonomous operation (with the inquiry frequency by the hub of 3 minutes). If the KeyPad battery is low, the security system will send the relevant notices, and the malfunction indicator will smoothly lights up and goes out after each successful passcode entry.

Battery Replacement

Complete Set

1. KeyPad

2. SmartBracket mounting panel

3. Batteries AAA (pre-installed) — 4 pcs

4. Installation kit

5. Quick Start Guide

Technical Specifications

Sensor type	Capacitive
Anti-tamper switch	Yes
Protection against passcode guessing	Yes

Frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz depending on the region of sale
Compatibility	Operates only with **Hub**, **Hub Plus**, **Hub 2** and **ReX**
Maximum RF output power	Up to 20 mW
Modulation of the radio signal	GFSK
Radio signal range	Up to 1,700 m (if there are no obstacles)
Power supply	4 × AAA batteries
Power supply voltage	3 V
Battery life	Up to 2 years
Operating temperature range	From -10°C to +40°C
Operating humidity	Up to 75%
Overall dimensions	150 × 103 × 14 mm
Weight	197 g
Certification	Security Grade 2, Environmental Class II in conformity with the requirements of EN 50131-1, EN 50131-3, EN 50131-5-3

Warranty

Warranty for the "AJAX SYSTEMS MANUFACTURING" LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase and does not apply to the pre-installed battery.

If the device does not work correctly, you should first contact the support service — in half of the cases, technical issues can be solved remotely!

👉 **The full text of the warranty**

👉 **User Agreement**

Technical support: **support@ajax.systems**

Need help?

In this section you'll find detailed manuals and educational videos about all features of Ajax. And in case you need help of a technical specialist, we're available 24/7.

Send request