KeyPad User Manual

KeyPad is a wireless touch-sensitive keypad controlling the Ajax security system. It arms and disarms a room from the guard mode, informs of the system status, is protected against code guessing and supports "silent alarm" if the code is entered by force.

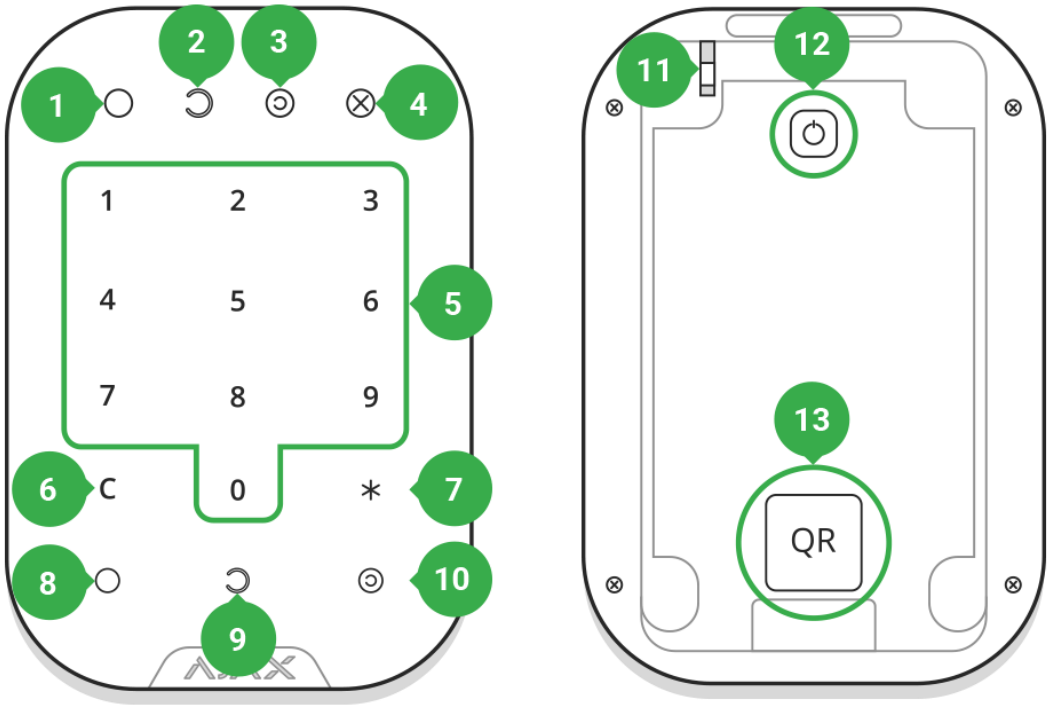
Keypad operates only with the Ajax security system (it may not be used in any third-party security systems), by connecting via the protected Jeweller protocol to the Hub. Communication range - up to 1,700 meters, absent any obstacles.

Device works only with hub, and is not compatible with the Ajax uartBridge or Ajax ocBridge Plus

The keypad is set up via a mobile application for iOS and Android-based smartphones.

☞ **Buy keypad KeyPad**

Functional elements



1. Armed mode indicator
2. Disarmed mode indicator
3. Night mode indicator
4. Malfunction indicator
5. The numeric block of touch buttons
6. Clear button
7. Function button
8. Arming button
9. Disarming button
10. Night mode button
11. Tamper button
12. On/Off button
13. QR code

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

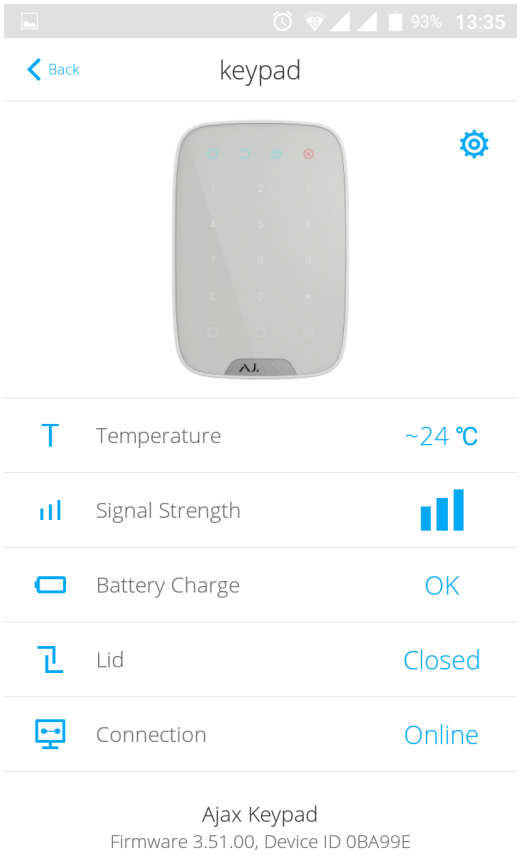
Keypad Operating Principle

Keypad is a touch-sensitive keypad panel controlling the security system.

The keypad is a stationary keypad and is located inside a room. It allows to set the system in the armed mode with a digital code or by pressing one button, switch on the night mode, disarm the room, notify the private security company of the forcing to switch off the security system (by no means disclosing the user).

Keypad is furnished with light indicators signaling about the security system status, about any problems with the detectors or interruption of the communication with the hub. Big touch-sensitive buttons are highlighted, if the device is activated by touch - the code may be entered without external lighting. Service life from pre-installed batteries - up to 2 years.

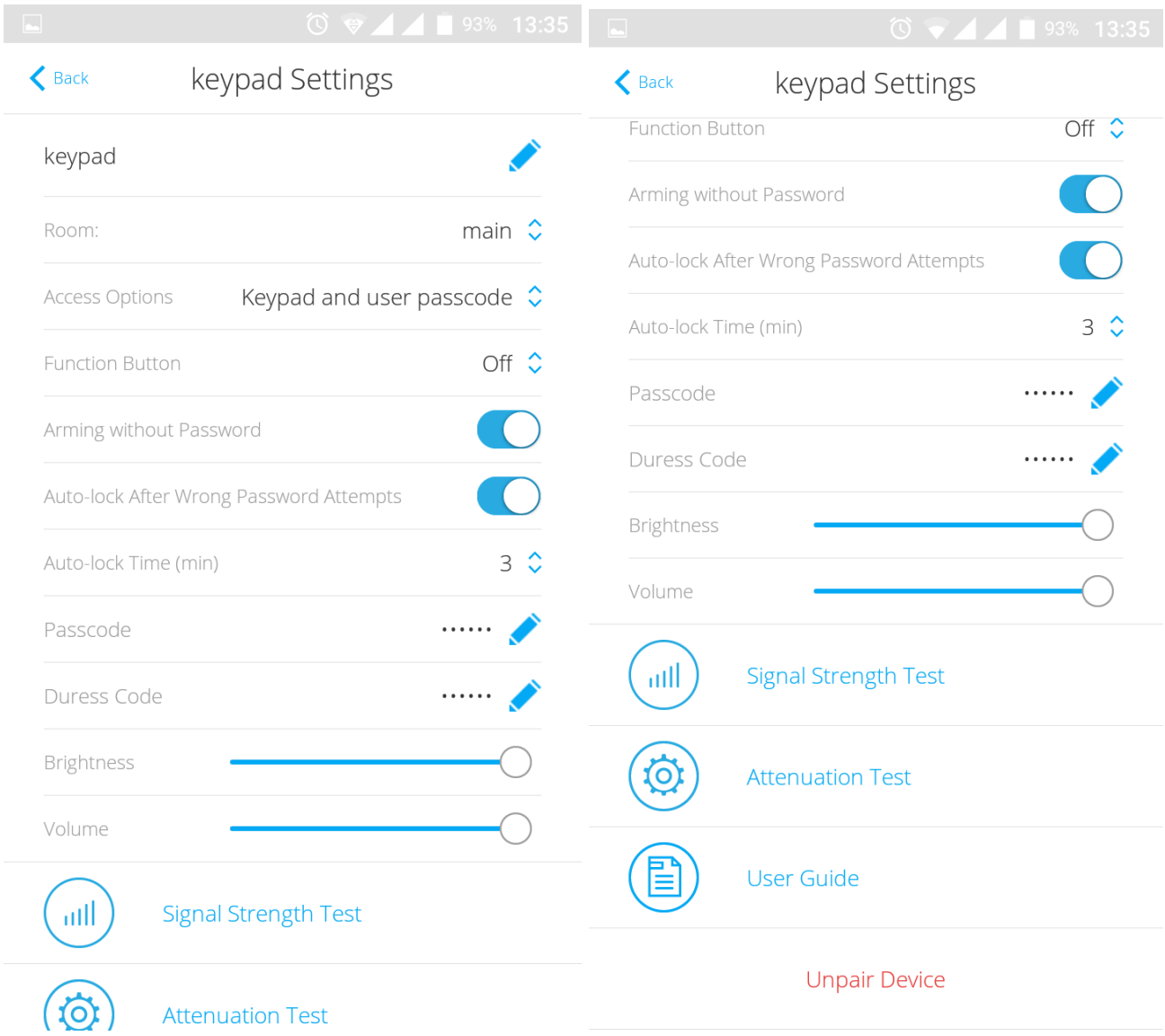
States



Parameter	Value
Temperature	Temperature of the device. Measured on the processor and changes gradually
Signal Strength	Signal strength 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
Connection	Connection status between the Hub and the keypad
Firmware	Detector firmware version

Device ID	Device identifier

Settings



Setting	Value
First field	Device name, can be edited
Room	Selecting the virtual room to which the device is assigned

Access option	Selecting type of passcodes for arming/disarming • Keypad passcode only • User passcode only • Keypad and User passcode
Function Button	Selecting functionality of the function button • Off • Send panic alarm • Silence fire alarm
Arming without password	Allows to arm the system without password by pressing arm button
Auto-lock after wrong password attempts	If active, in case if three incorrect passwords are entered, the keyboard is locked for the time set in the settings. At this time, you can not disarm the system by keypad.
Auto-lock time (min)	Lock period after wrong password attempts
Passcode	Keypad password for arming/disarming
Duress code	Selection a duress code (silent alarm)
Brightness	Brightness of the keypad
Volume	Volume of the keypad
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 keypad from the Hub and deletes its settings

Either a shared or personal password can be set on the keypad for each user.

In order to install a personal password:

- Go to profile settings **(Hub → User settings → Your profile settings)**
- Click Access Code Settings **(in this menu you can also see the user identifier)**
- Set the User Code and Duress Code

Each user sets his own personal password individually!

To control the system using the personal password:

- Enter User identifier * personal password →Arming/disarming button

To control a specific group:

- Enter User identifier * personal password * group identifier →Arming/disarming button

Keypad operation indication

When the keypad wakes up, the LED lights, corresponding to the operating mode of the security system.

Indicators display the current status of the system: in armed mode / disarmed mode / night mode.

Information is up to date even if the status was changed by any other control device - application, fob. The status is updated if the device is waked up by touch.

Event	Indication
LED blinks (X)	Indicator notifies of a fault in the Ajax security system, as well as lights up, if the keypad cannot connect to the hub. You may check the nature of the fault in the Ajax Security System application
Pressing a touch-sensitive button	Short sound signal
The system is set in the armed mode	Short sound signal, LED lights up: "Armed mode" / "Night mode"
The system is disarmed	Two short sound signals, LED lights up: "Removed from the armed mode"
The incorrect master code is entered	Long sound signal, the highlight of the digital block blinks 3 times during the signal sound
The hub refuses to set the system in the armed mode (e.g., a window is opened)	Long sound signal, the current status indicator blinks 3 times during the signal sound
A problem is detected when setting in the armed mode (e.g., the detector is lost)	Long sound signal, the "Fault" indicator blinks 3 times during the signal sound
The hub does not respond to the command - no connection	Long sound signal, the "Fault" indicator lights during the signal sound
The keypad is interlocked due to the password guessing	Long sound signal, the indicators of armed / disarmed /night mode blink simultaneously

Battery low	After successful entering a code and setting the security system in the armed/disarmed mode, the keypad will smoothly blink with the "Fault" indicator. The touch-sensitive buttons will be locked for the time of activity of the indicator. When trying to switch the keypad with the discharged batteries, it will emit a long sound signal, smoothly switch on and off the "Fault" indicator and then the keypad will switch off.

Connecting the Keypad to the Ajax Security System

Before starting connection:

- Following the Hub instruction recommendations, install the Ajax application on your smartphone. Create an account, add the Hub to the application, and create at least one room.
- Go to the Ajax application.
- Switch on the hub and check the internet connection (via Ethernet cable and/or GSM network).
- Ensure that the hub is disarmed and does not start updates by checking its status in the mobile application.

⚠ Only users with administrative privileges can add the device to the hub.

The device may only be added if the Ajax security system is disarmed.

1. Open a room in the mobile application or web application and select the option "Add a device".
2. Name the device, scan/write manually the QR Code (located on the body and packaging), and select the location room.
3. When the hub starts searching for a device and launches countdown, switch on the KeyPad by pressing the on/off button for 3 seconds - it will blink once with an LED.

For the detection and interfacing to occur, the detector should be located within the coverage area of the wireless network of the hub (at a single protected object).

Request for connection to the hub is transmitted for a short time at the time of switching on the device. If the connection to the hub failed keypad will switch off after 5 seconds. Repeat the connection attempt.

The keypad will appear in the list of devices of the hub. After adding the keypad to the system, it will have the following default codes: 123456 and Duress Code: 123457

Selection of the Keypad Location

While selecting the Keypad location, take account of the keypad distance from the hub and presence of any obstacles between the devices, hindering radio signal transmission: walls, inserted floors, large-size objects located within the room.

Do not install the KeyPad:

1. **Near radio transmission equipment, including that operated in 2G/3G/4G mobile networks, Wi-Fi routers, transceivers, radio stations, as well as an Ajax Hub (it uses a GSM network).**
2. **In close proximity to electrical wiring.**
3. **Close to metal objects and mirrors that cause radio signal attenuation or shading it.**
4. **Outside the premises (outdoors).**
5. **In rooms with a temperature and humidity exceeding the appropriate levels.**

Check the signal level at the installation location.

During testing, the signal level can be seen in the application and on the keypad panel - blue LEDs O (Armed mode), C (Disarmed mode) and (c) (Night mode), as well as red X (Fault), are used.

If the signal level is one division, we cannot guarantee stable operation of the security system. Take possible measures to improve the quality of the signal! As a minimum, move the device - even 20 cm shift can significantly improve the quality of reception.

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

The touch-sensitive panel of the keypad is designed for operation with the device mounted on the surface. If you use Keypad in your hands, we cannot guarantee successful operation of the touch-sensitive buttons.

Keypad Capabilities

To activate the keypad, touch the touch-sensitive panel - the highlight of the buttons will be activated and a wake-up sound signal will be emitted.

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

If you do not touch the buttons for 4 seconds, Keypad will reduce the highlight brightness, and after another 12 seconds, the device will go to the sleep mode.

When switching over to the sleep mode, the keypad will clear the entered commands!

The keypad allows using codes with the length of 4-6 digits. The entered code will be sent to the Hub after pressing the buttons: O (activate the guard mode), C (deactivate the guard mode) and (c) (night mode). Erroneously entered digits can be cleared using the button C (Reset).

If you enter incorrect code three times during 30 minutes, the keypad will be interlocked for the time preset in the settings. The Hub will ignore any entered codes, simultaneously notifying the security system users of the attempt of guessing the code. The keypad will be unlocked automatically after expiration of the interlock time or manually by the administrator user.

Keypad also supports setting the system in the armed mode without entering a master code, by pressing the button O (activate the armed mode). These features are disabled by default.

If you press the button * (Function) without entering the password, command * will be sent to the hub and the function installed in the hub from the application will be executed.

KeyPad can notify a private security company of the system being removed from the guard mode forcibly - using the Duress code. Unlike the panic button of the fob, if such code is entered, the user will not be compromised by actuation of the siren, and the keypad and message in the application will notify of the successful removal of the system from the guard mode.

Keypad 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!

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 LED X (Fault) of the keypad is not actuated after installation in SmartBracket, check the status of the tamper in the Ajax Security System application and then 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.

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).

- Signal Strength Test
- Attenuation Test

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 [link to the Jeweller set-up clause of the hub manual]) by the hub of 3 minutes). If the Keypad battery is low, the security system will send the relevant notices, and the "Fault" indicator will smoothly lights up and goes out after each successful password entry.

👉 Battery Replacement

Complete Set

1. KeyPad
2. Batteries AAA (pre-installed) - 4 pcs
3. Installation kit
4. Quick Start Guide

Technical Specifications

Sensor type	Capacitive
Protection against passcode guessing	Yes
Tamper protection	Yes
Frequency band	868.0 – 868.6 MHz or 868.7 – 869.2 MHz depending on the region of sale
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 x 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 x 103 x 14 mm
Weight	197 g

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!