KeyPad Plus User Manual

Updated April 30, 2021

KeyPad Plus is a wireless touch keypad for managing the Ajax security system with encrypted contactless cards and key fobs. Designed for indoor installation. Supports “silent alarm” when entering the duress code. Indicates the current security mode with a LED light.

Manages security modes using passwords and cards or key fobs. Indicates the current security mode with a LED light.

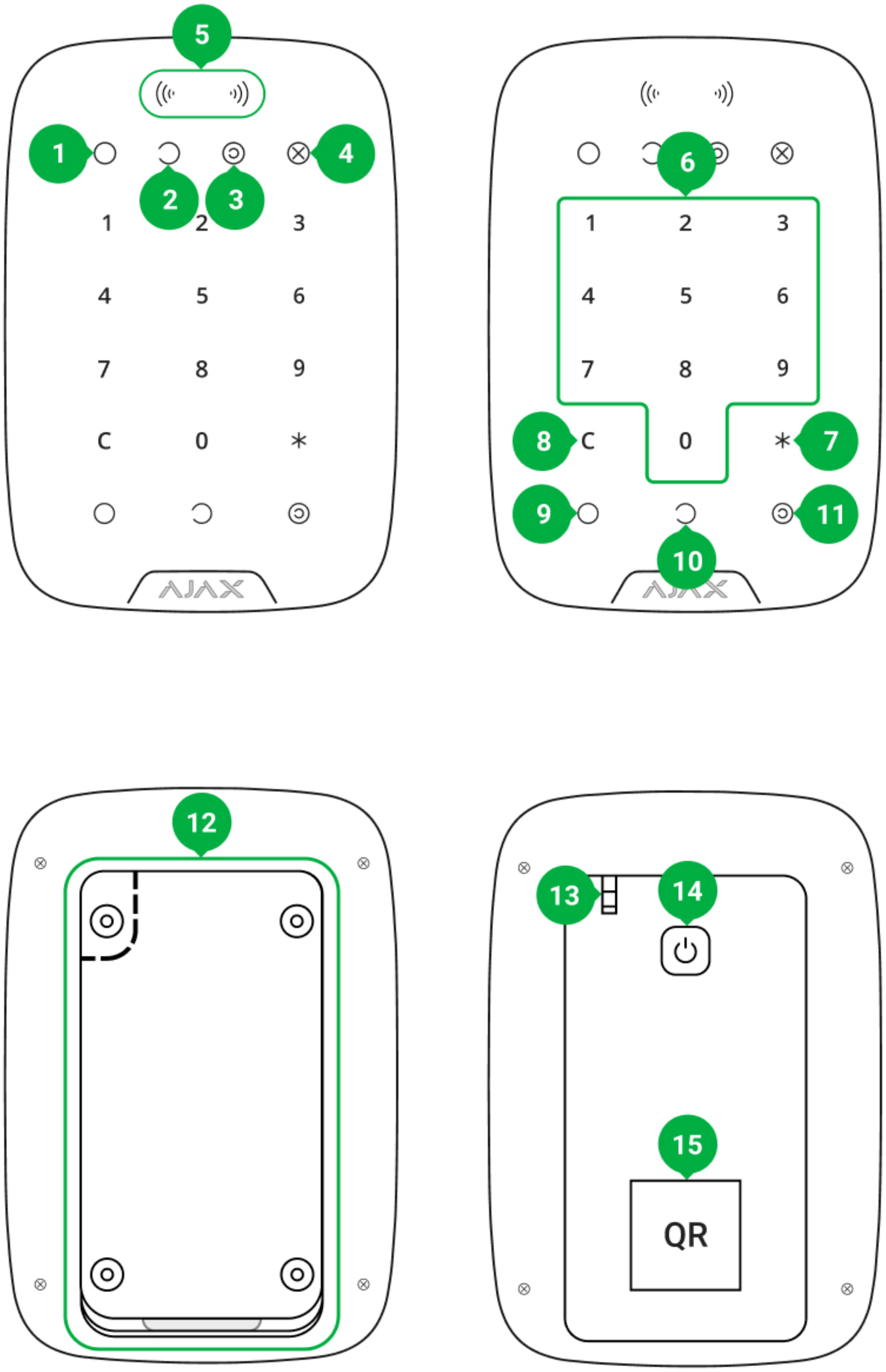
The keypad only works with Hub Plus, Hub 2 и Hub 2 Plus running OS Malevich 2.11 and higher. Connection to Hub and the ocBridge Plus and uartBridge integration modules is not supported!

The keypad operates as part of the Ajax security system by connecting via the Jeweller secure radio communication protocol to the hub. The communication range without obstacles is up to 1700 meters. The pre-installed battery life is up to

4.5 years.

Buy KeyPad Plus keypad

Functional elements



1. **Armed** indicator

2. **Disarmed** indicator
3. **Night mode** indicator
4. **Malfunction** indicator
5. **Pass/Tag Reader**
6. Numeric touch button box
7. **Function** button
8. **Reset** button
9. **Arm** button ○
10. **Disarm** button ◌
11. **Night mode** button ◎
12. SmartBracket mounting plate (to remove the plate, slide it down)

> ⚠ Do not tear off the perforated part of the mount. It is required for actuating the tamper in case of any attempt to dismantle the keypad.

13. Tamper button
14. Power button
15. Keypad QR Code

Operating principle

KeyPad Plus arms and disarms the security of the entire facility or separate groups as well as allows activating the **Night mode**. You can control the security modes with KeyPad Plus using:

1. **Passwords.** The keypad supports common and personal passwords, as well as arming without entering a password.
2. **Cards or key fobs**. You can connect **Tag key fobs** and **Pass cards** to the system. To quickly and securely identify users, KeyPad Plus uses the DESFire® technology. DESFire® is based on the ISO 14443 international standard and combines 128-bit encryption and copy protection.

Before entering a password or using Tag/Pass, you should activate ("wake up") the KeyPad Plus by sliding your hand over the touch panel from top to bottom. When it is activated, the button backlight is enabled, and the keypad beeps.

The KeyPad Plus is equipped with LED indicators that show the current security mode and keypad malfunctions (if any). The security status is displayed only when the keypad is active (the device backlight is on).

You can use the KeyPad Plus without ambient lighting as the keypad has a backlight. The pressing of the buttons is accompanied by a sound signal. The backlight brightness and keypad volume are adjustable in the settings. If you do not touch the keypad for 4 seconds, KeyPad Plus reduces the backlight brightness, and 8 seconds later goes into power-saving mode and turns off the display.

> If the batteries are discharged, the backlight turns on at the minimum level regardless of the settings.

Function button

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

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

Learn more

Duress code

KeyPad Plus supports **duress code**. It allows you to simulate alarm deactivation. The Ajax app and sirens installed at the facility will not give you away in this case, but the security company and other users of the security system will be warned about the incident.

Learn more

stage device. The two-stage arming process using Tag or Pass is similar to arming using personal or common password on the keypad.

Learn more

Event transmission to the monitoring station

The Ajax security system can connect to the CMS and transmit events and alarms to the monitoring station of the security company in **Sur-Gard** (**ContactID**), SIA DC-09, and other proprietary protocol formats. A complete list of supported protocols is available **here**. The device ID and the number of the loop (zone) can be found in **its states**.

Connection

> ⚠ KeyPad Plus is incompatible with Hub, third-party security central units, and ocBridge Plus and uartBridge integration modules.

Before starting connection

1. Install the Ajax app and **create an account**. Add a hub and create at least one room.
2. Ensure that the hub is on and has Internet access (via Ethernet cable, Wi-Fi, and/or mobile network). This can be done by opening the Ajax app or by looking at the hub logo on the faceplate — it lights white or green if the hub is connected to the network.
3. Make sure that the hub is not in armed mode and does not start updates by checking its status in the app.

To connect KeyPad Plus

1. Open the Ajax app. If your account has access to multiple hubs, select the one to which you want to connect KeyPad Plus.
2. Go to the **Devices** menu and click **Add Device**.
3. Name the keypad, scan or enter the QR code (located on the package and under the SmartBracket mount), and select a room.
4. Click **Add**; the countdown will begin.
5. Turn on the keypad by holding the power button for 3 seconds. Once connected, KeyPad Plus will appear in the hub device list in the app. To connect, locate the keypad at the same protected facility as the system (within the coverage area of the hub radio network range). If the connection fails, try again in 10 seconds.

> The keypad only works with one hub. When connected to a new hub, the device stops sending commands to the old hub. Once added to a new hub, KeyPad Plus is not removed from the device list of the old hub. This must be done manually through the Ajax app.

KeyPad Plus turns off automatically 6 seconds after being turned on if the keypad fails to connect to the hub. Therefore, you do not need to turn off the device to retry the connection.

Updating the statuses of devices in the list depends on the Jeweller settings; the default value is 36 seconds.

Icons

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

	Battery charge level of KeyPad Plus
RE	KeyPad Plus works via a ReX radio signal range extender
	KeyPad Plus body status notifications are temporarily disabled Learn more
	KeyPad Plus is temporarily deactivated Learn more
((·))	**Pass/Tag reading** is enabled in KeyPad Plus settings
((·))	**Pass/Tag reading** is disabled in KeyPad Plus settings

States

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

1. Go to the **Devices** tab.
2. Select KeyPad Plus from the list.

Parameter	Value
Malfunction	Pressing ⓘ opens the KeyPad Plus malfunctions list. **The field is displayed only if a malfunction is detected**
Temperature	Keypad temperature. It is measured on the processor and changes gradually.

Connection	Connection status between the hub or range extender and the keypad: - **Online** — the keypad is online - **Offline** — no connection to the keypad
Battery charge	The battery charge level of the device. Two states are available: - OK - Battery low When the batteries are discharged, the Ajax apps and the security company will receive appropriate notifications. After sending a low battery notification, the keypad can work for up to 2 months How battery charge is displayed in Ajax apps
Lid	The status of the device tamper, which reacts to the detachment of or damage to the body: - Opened - Closed What is a tamper
Works via *range extender name*	Displays the status of the ReX range extender use. **The field is not displayed if the keypad works directly with the hub**

Temporary Deactivation	● **No** — the device operates normally and transmits all events ● **Lid only** — the hub administrator has disabled notifications about the body opening ● **Entirely** — the hub administrator has entirely excluded the keypad from the system. The device does not execute system commands and does not report alarms or other events Learn more
Firmware	KeyPad Plus firmware version
ID	Device identifier
Device No.	Number of the device loop (zone)

Settings

KeyPad Plus is configured in the Ajax app:

1. Go to the **Devices** tab.
2. Select KeyPad Plus from the list.
3. Go to **Settings** by clicking on the gear icon ⚙.

To apply the settings after the change, click the **Back** button

Parameter	Value

Room	Selecting the virtual room to which KeyPad Plus is assigned. The name of the room is displayed in the text of SMS and notifications in the event feed
Group Management	Selecting the security group controlled by the device. You can select all groups or just one. **The field is displayed when the Group mode is enabled**
Access Settings	Selecting the method of arming/disarming: ● Keypad code only ● User passcode only ● Keypad and user passcode
Keypad code	Selection of a common password for security control. Contains 4 to 6 digits
Duress code	Selecting a common duress code for silent alarm. Contains 4 to 6 digits Learn more
Function button	Selecting the function of the * button (**Function** button): ● **Off** — the Function button is disabled and does not execute any commands when pressed ● **Alarm** — after the Function button is pressed, the system sends an alarm to the CMS and to all users ● **Mute Interconnected Fire Alarm** — when

Unauthorized Access Auto-Lock	If active, the keypad is locked for the pre-set time if an incorrect password is entered or unverified passes/tags are used more than 3 times in a row within 1 minute. It is not possible to disarm the system via keypad during this time. You can unlock the keypad through the Ajax app
Auto-lock Time (min)	Selecting the keypad lock period after wrong password attempts: ● 3 minutes ● 5 minutes ● 10 minutes ● 20 minutes ● 30 minutes ● 60 minutes ● 90 minutes ● 180 minutes
Brightness	Selecting brightness of the keypad buttons backlight. The backlight works only when the keypad is active. This option does not affect the brightness level of pass/tag reader and security modes indicators
Volume	Selecting the keypad buttons volume level when pressed

	particular group — the **Group Managemen**t field in the keypad settings Learn more
Alert with a siren if the panic button is pressed	The field is displayed if the **Alarm** option is selected for the **Function** button. When the option is enabled, the sirens connected to the security system give an alert when the * button (**Function** button) is pressed
Jeweller Signal Strength Test	Switches the keypad to the Jeweller signal strength test mode Learn more
Attenuation Test	Switches the keypad to the Attenuation test mode Learn more
Pass/Tag Reset	Allows deleting all hubs associated with Tag or Pass from device memory Learn more
	Allows the user to disable the device without removing it from the system. Two options are available: ● **Entirely** — the device will not execute system

Unpair Device	Disconnects KeyPad Plus from the hub and deletes its settings

Entry and exit delays are set in the corresponding detector settings, not in the keypad settings.

Learn more about entry and exit delays

Adding a personal password

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

To set a personal password in the Ajax app:

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

Each user sets a personal password individually. The administrator cannot set a password for all users.

Hub 2	50
Hub 2 Plus	200

The procedure for connecting Tag, Pass, and third-party devices is the same. See the connecting instructions **here**.

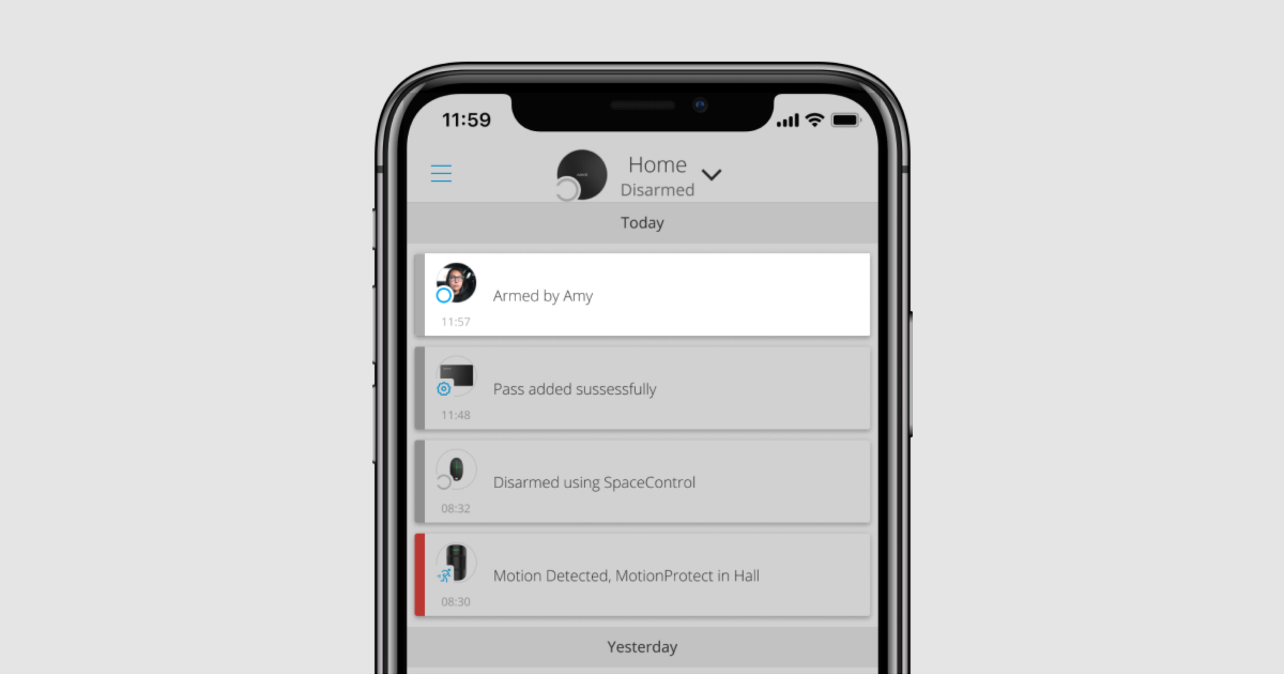
Security management by passwords

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

If a personal password is used, the name of the user who armed or disarmed the system is displayed in the hub event feed and in the notifications list. If a common password is used, the name of the user who changed the security mode is not displayed.

Arming with a personal password

The **username** is displayed in the notifications and events feed



11:59

Home
Disarmed

Today

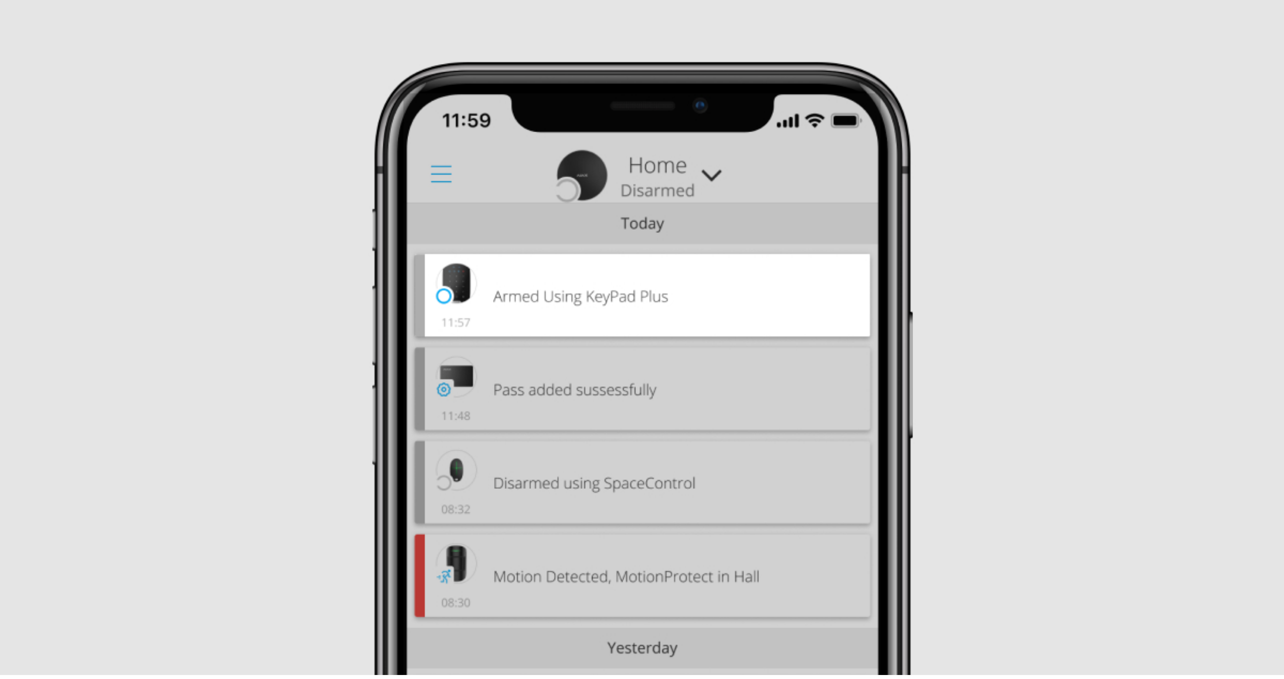
Armed by Amy
11:57

Pass added sussessfully
11:48

Disarmed using SpaceControl
08:32

Motion Detected, MotionProtect in Hall
08:30

Yesterday



11:59

Home
Disarmed

Today

Armed Using KeyPad Plus
11:57

Pass added sussessfully
11:48

Disarmed using SpaceControl
08:32

Motion Detected, MotionProtect in Hall
08:30

Yesterday

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

Security management of the facility using a common password

3. Press the * (Function button).

4. Enter the **Group ID**.

5. Press the arming ○/disarming ◌/Night mode ◎ key.

For example: 1234 → * → 2 → ◌

What is Group ID

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

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

Rights in the Ajax security system

Security management of the facility using a personal password

1. Activate the keypad by swiping your hand over it.

1. Activate the keypad by swiping your hand over it.

2. Enter the **User ID**.

3. Press the * (Function button).

4. Enter your **personal password**.

5. Press the * (Function button).

6. Enter the **Group ID**.

7. Press the arming ○/disarming ◌/Night mode ◎ key.

For example: 2 → * → 1234 → * → 5 → ◌

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

What is Group ID

What is User ID

Using a duress code

2. Enter the **common duress code**.

3. Press the disarming key ○.

For example: 4321 → ○

To use a personal duress code

1. Activate the keypad by swiping your hand over it.

2. Enter the **User ID**.

3. Press the * (Function button).

4. Enter the **personal duress code**.

5. Press the disarming key ○.

For example: 2 → * → 4422 → ○

Security management using Tag or Pass

1. Activate the keypad by swiping your hand over it. KeyPad Plus will beep (if enabled in the settings) and turn on the backlight.

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

Keep in mind that the option is available only if Interconnected FireProtect Alarm is enabled.

Learn more

Indication

KeyPad Plus can report the current security mode, keystrokes, malfunctions, and its status by LED indication and sound. The current security mode is displayed by the backlight after the keypad is activated. The information about the current security mode is relevant even if the arming mode is changed by another device: a key fob, another keypad, or an app.

There is no connection to the hub or ReX range extender	LED **X** blinks
KeyPad Plus body is open (SmartBracket mount is removed)	LED **X** blinks briefly once
Touch button pressed	Short beep, the current system security status LED blinks once. The volume depends on the keypad settings
The system is armed	Short beep, **Armed** or **Night mode** LED lights up
The system is disarmed	Two short beeps, the **Disarmed** LED lights up
An incorrect password was entered or there was an attempt to change security mode by an unconnected or deactivated pass/tag	Long beep, digital unit LED backlight blinks 3 times
The security mode cannot be activated (for example, a window is open and the **System integrity check** is enabled)	Long beep, the current security status LED blinks 3 times
The hub does not respond to the command — there is no connection	Long beep, **X** (**Malfunction)** LED lights up
The keypad is locked due to a wrong password attempt or attempt to use an unauthorised pass/tag	Long beep, during which the security status LEDs and keypad backlight blink 3 times

You can change the ping period of devices in the **Jeweller** menu of the hub settings.

Tests are available in the device settings menu (Ajax App → Devices → KeyPad Plus → Settings ⚙)

- Jeweller Signal Strength Test
- Attenuation Test

Choosing a location

⚠ Be sure to check the Jeweller signal strength at the installation site. If the signal strength is low (a single bar), we cannot guarantee a stable operation of the security system! At the very least, relocate the device as repositioning even by 20 cm can significantly improve the signal reception.

If poor or unstable signal strength is still reported after the relocation of the device, use the **ReX radio signal range extender**

Do not install the keypad:

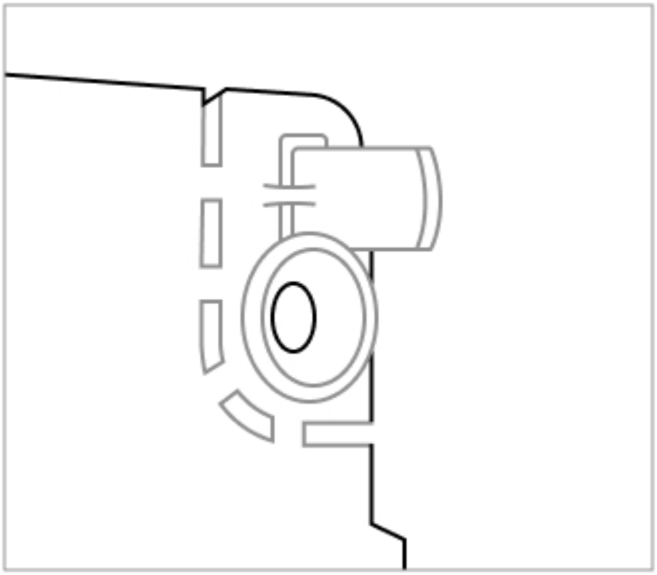
- In places where parts of clothing (for example, next to the hanger), power cables, or Ethernet wire may obstruct the keypad. This can lead to false triggering of the keypad.
- Inside premises with temperature and humidity outside the permissible limits. This could damage the device.
- In places where KeyPad Plus has an unstable or poor signal strength with the hub or ReX range extender.

Double-sided adhesive tape may only be used for temporary attachment of the keypad. The device attached with adhesive tape can at any time be detached from the surface and fall, which may lead to failure. Please note that if the device is attached with adhesive tape, the tamper will not trigger when trying to detach it.

2. Check the convenience for password entry using Tag or Pass to manage security modes. If it is inconvenient to manage the security at the selected location, relocate the keypad.

3. Remove the keypad from the SmartBracket mounting plate.

4. Attach the SmartBracket mounting plate to the surface using the bundled screws. When attaching, use at least two fixing points. Be sure to fix the perforated corner on the SmartBracket plate so that the tamper responds to a detachment attempt.



Check the functioning of your keypad on a regular basis. This can be done once or twice a week. Clean the body from dust, cobwebs, and other contaminants as they emerge. Use a soft dry cloth that is suitable for equipment care.

1. KeyPad Plus

2. SmartBracket mounting plate

3. 4 pre-installed lithium batteries AA (FR6)

4. Installation kit

5. Quick Start Guide

Technical Specifications

Compatibility	Hub Plus, Hub 2, Hub 2 Plus, ReX
Color	Black, White
Installation	Indoor only
Keypad type	Touch-sensitive

Dimensions	165 × 113 × 20 mm
Weight	267 g
Service life	10 years
Warranty	24 months

Compliance with standards

Warranty

The warranty for the AJAX SYSTEMS MANUFACTURING Limited Liability Company products is valid for 2 years after purchase and does not extend to the bundled batteries.

If the device does not function properly, we recommend that you first contact the support service as half of the technical issues can be resolved remotely!