

KeyPad S Plus Jeweller user manual

Soon to be: Superior KeyPad Plus Jeweller

Updated September 3, 2024



KeyPad S Plus Jeweller is a wireless touch keypad. It allows you to manage the Ajax system using encrypted contactless cards and key fobs. The keypad also supports a “silent alarm” feature that activates by entering the duress code. The LED light indicates the current security mode.

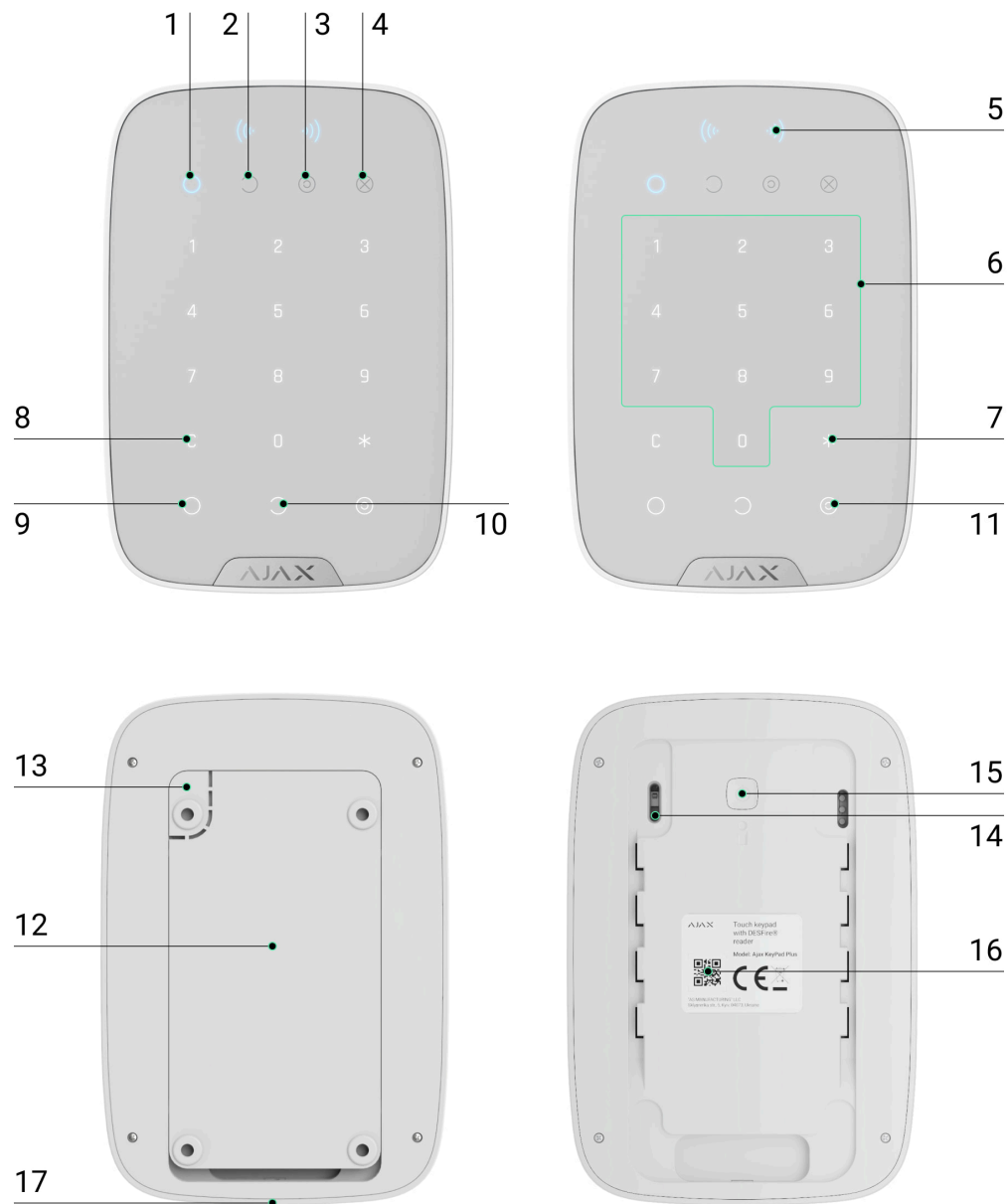
KeyPad S Plus operates within the Ajax system, connected to the hub via the protected Jeweller protocol. The communication range in an open space is up to 1,700 meters. **KeyPad S Plus** operates for up to 4,5 years from pre-installed batteries. The device is designed for indoor use only.






This product line is developed for projects. Only accredited Ajax Systems partners can sell, install and administer **Superior** products.

Superior, Fibra and Baseline product lines are mutually compatible. This opens up numerous possibilities for building systems of any configuration.

Functional elements



1. **Armed** indicator.
2. **Disarmed** indicator.
3. **Night Mode** indicator.
4. **Malfunction** indicator.
5. **Pass/Tag** reader.

6. Numpad.
7. **Function** button.
8. **Reset** button.
9. **Arm** button .
10. **Disarm** button .
11. **Night Mode** button .
12. SmartBracket mounting panel (to remove the plate, slide it down).
13. A perforated part is required for actuating the tamper in case of any attempt to dismantle the device.
14. Tamper button.
15. Power button.
16. QR code.
17. Holding screw.

Compatible hubs and range extenders

An Ajax hub with the firmware OS Malevich 2.16 and higher is required for the detector to operate.

[Check devices compatibility](#)

Operating principle

00:00

00:04

1. Codes. The keypad supports general and personal codes and arming without entering a code.

2. Cards or key fobs. You can connect Tag key fobs and Pass cards to the system.

KeyPad S Plus supports the following code types:

- **Keypad code** — general code set up for the keypad. When used, all events are delivered to Ajax apps on behalf of the keypad.
- **User code** — personal code set up for a user connected to the hub. When used, all events are delivered to Ajax apps on behalf of the user.
- **Keypad access code** — a code set up for a person who is not registered in the system. When used, events are delivered 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.



The number of personal, access, and RRU codes depends on the hub model.

Before entering a code or using Tag/Pass, you should activate (“wake up”) KeyPad S Plus by sliding a hand over the touch panel from top to bottom. The button backlight is enabled when activated, and the keypad beeps.



Auto-wake on Delay when Entering function allows automatically activating the keypad when Delay When Entering is set up. This function is supported by KeyPad S Plus Jeweller with firmware version 5.60.6.3 or higher and hubs with OS Malevich 2.18 and higher.

KeyPad S Plus has LED indicators showing 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).



KeyPad S Plus can be used in low-light conditions as it has a backlight. Pressing the buttons is accompanied by a sound signal. The backlight brightness and keypad volume are adjustable in the settings. If the keypad is not touched for 4 seconds, KeyPad S Plus reduces the backlight brightness. After 8 seconds of inactivity, it enters 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 S Plus has the **Function** button that operates in one of 3 modes:

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

[Learn more](#)

Duress code

KeyPad S Plus supports **duress code**. It allows you to simulate alarm deactivation. In this case, the Ajax app and the sirens installed at the facility will not give away your actions. Still, the security company and other security system users will be alerted about the incident.

[Learn more](#)

Unauthorized access auto-lock

If a wrong code is entered three times within 1 minute, the keypad will be locked for the time specified in its settings. During this time, the hub will ignore all codes while simultaneously informing the users of the security system about an attempt to guess the code.

A user or PRO with administrator rights can unlock the keypad through the app. Also, unlocking occurs automatically after the lock time specified in the settings expires.

Mute interconnected fire detectors alarms function

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

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

Remember that the option is available only if **Interconnected Fire Detectors Alarm** is enabled.

[Learn more](#)



With the [OS Malevich 2.12](#) update, users can mute fire alarms in their groups without affecting detectors in the groups they do not have access to.

[Learn more](#)

Two-stage arming

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

[Learn more](#)

Sending events to the monitoring station

The Ajax system can transmit alarms to the [PRO Desktop](#) monitoring app as well as the central monitoring station (CMS) in the formats of **SurGard (Contact ID)**, **SIA (DC-09)**, **ADEMCO 685**, and [other protocols](#).

KeyPad S Plus can transmit the following events:

1. The duress code is entered.
2. The panic button is pressed (if the **Function** button works in the panic button mode).
3. The keypad is locked due to an attempt to guess a code.
4. Tamper alarm/recovery.
5. Loss/recovery of connection between KeyPad S Plus and the hub.
6. Temporary activation/deactivation of KeyPad S Plus.

When an alarm is received, the operator of the security company monitoring station knows what happened and where to send the fast response team. The addressability of each Ajax device allows you to send events and the type of the device, the name assigned to it, and the room to the PRO Desktop or the CMS. The list of transmitted parameters may differ depending on the type of CMS and the selected communication protocol.



The ID and number of the device can be found in its [States](#) in the Ajax app.

Adding to the system



KeyPad S Plus is incompatible with [Hub](#) and third-party security control panels.

To connect **KeyPad S Plus** to the hub, the device must be located at the same secured facility as the system (within the range of the hub radio network). For the

device to work via [ReX](#) or [ReX 2](#) radio signal range extender, you must first add the device to the hub, then connect it to **ReX** or **ReX 2** in the settings of the range extender.



The hub and the device operating at different radio frequencies are incompatible. The radio-frequency range of the device may vary by region. We recommend purchasing and using Ajax devices in the same region. You can check the range of operating radio frequencies with the [technical support service](#).

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](#)



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.



This product line is developed for projects. Only accredited Ajax Systems partners can install and administer Superior products.

Connecting to the hub

1. Open an Ajax PRO app. Select the hub where you want to add the device.
2. Go to the **Devices**  tab and click **Add Device**.
3. Name the keypad, scan, or type in the QR code (located on the package and under the SmartBracket mount), and select a room and a group (if Group mode is enabled).
4. Click **Add**; the countdown will begin.
5. Turn on the keypad by holding the power button for 3 seconds. Once connected, KeyPad S 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.




KeyPad S Plus 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 S Plus is not removed from the device list of the old hub. This must be done manually through the Ajax app.







KeyPad S 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 display some **KeyPad S Plus** states. To access them:

1. Sign in to the [Ajax app](#).
2. Select the hub.
3. Go to the **Devices**  tab.


Icon	Meaning
	Jeweller signal strength. Displays the signal strength between the hub and the device. The recommended value is 2–3 bars. Learn more
	The device battery charge level is OK, or it is charging. Learn more
	The device has a malfunction. The list of malfunctions is available in the device states. Learn more
	Displayed when the device is operating via a radio signal range extender .
	The device is permanently deactivated. Learn more
	The device has been deactivated due to exceeding the preset number of alarms. Learn more


	<p>The device has tamper triggering events permanently deactivated.</p> <p>Learn more</p>
	<p>The device is deactivated until the first disarm.</p> <p>Learn more</p>
	<p>The device has tamper triggering events deactivated. Until the first disarm.</p> <p>Learn more</p>
	<p>Pass/Tag reading is enabled in KeyPad S Plus settings.</p>
	<p>Pass/Tag reading is disabled in KeyPad S Plus settings.</p>
	<p>The device was not transferred to the new hub.</p> <p>Learn more</p>


States


The **States** menu includes information about the device and its operating parameters. The states of **KeyPad S Plus Jeweller** can be found in Ajax apps:

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

Parameter	Value
Malfunction	<p>Clicking on  opens the list of the device's malfunctions.</p> <p>The field is displayed only if a malfunction is detected.</p>

Temperature	<p>Keypad temperature. The acceptable error between the value in the app and the room temperature – 2 °C.</p> <p>The value is updated as soon as the device identifies a temperature change of at least 1 °C.</p> <p>You can configure a scenario by temperature to control automation devices.</p> <p>Learn more</p>
Jeweller signal strength	<p>Signal strength between the hub/range extender and the keypad.</p> <p>We recommend installing the device in places the signal strength is 2–3 bars.</p>
Connection via Jeweller	<p>Connection status between the hub or range extender and the keypad:</p> <ul style="list-style-type: none"> • Online — the keypad is online. • Offline — no connection to the keypad.
ReX	<p>Displays the status of using a radio signal range extender.</p> <div>  <p>The field is not displayed if the keypad works directly with the hub.</p> </div>
Battery Charge	<p>The battery charge level of the device. Two states are available:</p> <ul style="list-style-type: none"> • OK. • Battery low. <p>When the batteries are discharged, the Ajax apps and the security company will receive appropriate</p>



	<p>notifications.</p> <p>After sending a low battery notification, the keypad can work for up to 2 months.</p> <p><u>How battery charge is displayed in Ajax apps</u></p>
Lid	<p>Tamper is triggered if someone tries to detach the device from the surface or damage the enclosure. There are two states:</p> <ul style="list-style-type: none"> • Open. • Closed. <p><u>Learn more</u></p>
Pass/Tag Reading	Displays if card and key fob reader is enabled.
Assigned group easy management	Displays whether the security mode can be switched with Pass or Tag and without confirmation by the control buttons.
Easy Armed Mode Change	<div data-bbox="834 1213 1450 1518">  <p>This setting replaces Assigned Group Easy Management on KeyPad S Plus Jeweller with firmware version 6.60.0.6 or higher, operating with hubs with <u>OS Malevich 2.19</u> or higher.</p> </div> <p>Shows the configuration for the Easy Armed Mode Change feature:</p> <ul style="list-style-type: none"> • Off — each arming or disarming attempt should be confirmed by entering the passcode or presenting the access device. • Arm/disarm using access device without confirming action by buttons — allows users to switch security modes of the system using

	<p>access devices without confirmation by pressing keypad buttons.</p> <ul style="list-style-type: none">• Disarm without disarming button – the system or its groups, the security of which is managed with a passcode or access devices, will be disarmed without confirmation by pressing keypad buttons. <div><p>A fixed passcode length should be set in the hub settings in the Ajax PRO app.</p></div>
Permanent Deactivation	<p>Shows the status of the device permanent deactivation setting:</p> <ul style="list-style-type: none">• No – the device operates in normal mode.• Lid only – the hub administrator has disabled notifications about triggering of the device tamper.• Entirely – the device is entirely excluded from the operation of the system. The device does not execute system commands and does not report alarms or other events. <p>Learn more</p>
One-Time Deactivation	<p>Shows the status of the device one-time deactivation setting:</p> <ul style="list-style-type: none">• No – the device operates in normal mode.• Entirely – the device is entirely excluded from the operation of the system for a time the armed mode is active. The device does not execute system commands and does not report alarms or other events.• Lid only – notifications on the tamper triggering are disabled for a time the armed mode is active.


	Learn more
Firmware	Device firmware version.
Device ID	Device ID. Also, available on the QR code on the device enclosure and its package box.
Device No.	Number of the device loop (zone).

Settings

To change KeyPad S Plus settings in the Ajax apps:


1. Go to the **Devices**  tab.
2. Select **KeyPad S Plus** from the list.
3. Go to **Settings** by clicking on the gear icon .
4. Set the required parameters.
5. Click **Back** to save the new settings.

Parameter	Value
Name	<p>Name of the device. Displayed in the list of hub devices, text of SMS and notifications in the events feed.</p> <p>To change the name of the keypad, click on the text field.</p> <p>The name can contain up to 12 Cyrillic characters or up to 24 Latin characters.</p>

Room	<p>Selecting the virtual room to which KeyPad S Plus is assigned.</p> <p>The name of the room is displayed in the text of SMS and notifications in the event feed.</p>
Group Management	<p>Selecting the security group controlled by the device. You can select all groups or just one.</p> <p>The field is displayed when the <u>Group mode</u> is enabled.</p>
Access Settings	<p>Selecting the method of arming/disarming:</p> <ul style="list-style-type: none"> • Keypad codes only. • User codes only. • Keypad and user codes. <div>  <p>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.</p> </div>
Keypad Code	<p>Selection of a general code for security control. Contains 4 to 6 digits.</p>
Duress Code	<p>Selecting a general duress code for silent alarm. Contains 4 to 6 digits.</p> <p><u>Learn more</u></p>
Function Button	<p>Selecting the function of the * button (Function button):</p> <ul style="list-style-type: none"> • Off — the Function button is disabled and does not execute any commands when pressed.

	<ul style="list-style-type: none">• Alarm — after the Function button is pressed, the system sends an alarm to the CMS and to all users.• Mute Interconnected Fire Detectors Alarm — when pressed, mutes the alarm of Ajax fire detectors. Available only if an Interconnected Fire Detectors Alarm is enabled. <p><u>Learn more</u></p>
Arming without Code*	<p>The option allows you to arm the system without entering a code. To do this, click on the Arm or Night Mode button.</p> <p>* When enabled, makes your system not compliant with EN 50131 Grade 2, 3.</p>
Unauthorized Access Auto-Lock	<p>If enabled, the keypad will be locked for a pre-set duration if an incorrect code is entered or unverified passes/tags are used more than 3 times consecutively within a 1-minute timeframe.</p> <p>During this time, it is not possible to disarm the system using the keypad. However, you can unlock the keypad through the Ajax app.</p>

Auto-lock Time, min	<p>Selecting the keypad lock period after wrong code attempts:</p> <ul style="list-style-type: none"> • 3 minutes. • 5 minutes. • 10 minutes. • 20 minutes. • 30 minutes. • 60 minutes. • 90 minutes. • 180 minutes.
Brightness	<p>Adjusting the brightness of the keypad buttons backlight. The backlight functions only when the keypad is active.</p> <p>This option does not affect the brightness level of pass/tag reader and security modes indicators.</p>
Buttons Volume	<p>Selecting the keypad buttons volume level when pressed.</p>
Pass/Tag Reading	<p>When enabled, the security mode can be controlled with Pass and Tag access devices.</p>
Authorization confirmation with a passcode	<p>When enabled, system authorization using access devices requires confirmation of the action with the user or keypad code. Available if the Pass/Tag Reading toggle is enabled.</p> <p>This setting is supported when KeyPad Plus Jeweller is connected to hubs with firmware version <u>OS Malevich 2.20</u> or higher.</p>
Time for confirmation	<p>Selecting the maximum time to confirm authorization with a password after access devices' confirmation. Available if the Authorization confirmation with a passcode toggle is enabled.</p>

	<p>This setting is supported when KeyPad Plus Jeweller is connected to hubs with firmware version <u>OS Malevich 2.21</u> or higher.</p>
Assigned group easy management	<p>When enabled, changing the security mode with Tag and Pass does not require confirmation by pressing the arm, disarm, or Night Mode button. The security mode is switched automatically.</p> <p>The option is available if Pass/Tag Reading is enabled in the keypad settings.</p> <p>If the group mode is activated, the option is available when the keypad is assigned to a particular group — the Group Management field in the keypad settings.</p> <p><u>Learn more</u></p>
Easy Armed Mode Change	<div> This setting replaces Assigned Group Easy Management on KeyPad S Plus Jeweller with firmware version 6.60.0.6 or higher, operating with hubs with <u>OS Malevich 2.19</u> or higher.</div> <p>Allows users to arm/disarm the system without confirmation by pressing keypad buttons.</p> <p>Three options are available:</p> <ul style="list-style-type: none">• Off — each arming or disarming attempt should be confirmed by entering the passcode or presenting the access device.• Arm/disarm using access device without confirming action by buttons — allows users to switch security modes of the system using access devices without confirmation with keypad buttons.


- **Disarm without disarming button** – the system or its groups, the security of which is managed with a passcode or access devices, will be disarmed without confirmation by pressing keypad buttons.



A fixed passcode length should be set in the hub settings in the Ajax PRO app.

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 the code appears after pressing the **Arm**  button.

Auto-wake on Delay when Entering



The feature is available on KeyPad S Plus Jeweller with firmware version 5.60.6.3 or higher, operating with hubs with OS Malevich 2.18 or higher.

Activates the keypad after Delay When Entering is started by any security device.

The auto-wake feature may also reduce the keypad battery life.

Alert with a siren if the panic button is pressed	<p>The field is displayed if the Alarm option is selected for the Function button.</p> <p>When the option is enabled, the sirens connected to the security system give an alert when the * button (Function button) is pressed.</p>
Jeweller Signal Strength Test	<p>Switches the keypad to the Jeweller signal strength test mode. The recommended value is 2–3 bars.</p> <p>Learn more</p>
Signal Attenuation Test	<p>Switches the keypad to the signal attenuation test mode.</p> <p>Learn more</p>
Pass/Tag Reset	<p>Allows deleting all hubs associated with Tag or Pass from device memory.</p> <p>Learn more</p>
User Guide	<p>Opens KeyPad S Plus user manual in the Ajax app.</p>
Permanent Deactivation	<p>Allows the user to disable the device without removing it from the system.</p> <p>Three options are available:</p> <ul style="list-style-type: none"> • No — the device operates normally and transmits all events. • Entirely — the device will not execute system commands or participate in automation scenarios, and the system will ignore device alarms and other notifications. • Lid only — the system will only ignore notifications about the triggering of the device tamper button. <p>Learn more</p>

	<p>The system can also automatically deactivate devices when the preset number of alarms is exceeded or when the recovery timer expires.</p> <p>Learn more</p>
One-Time Deactivation	<p>Allows the user to disable events of the device until the first disarm.</p> <p>Three options are available:</p> <ul style="list-style-type: none"> • No – the device operates in normal mode. • Lid only – notifications on the tamper triggering are disabled for a time the armed mode is active. • Entirely – the device is entirely excluded from the system's operation when the armed mode is active. The device does not execute system commands or alarms or other events. <p>Learn more</p>
Delete Device	<p>Disconnects KeyPad S Plus from the hub and deletes its settings.</p>



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



[What is Delay When Entering/Leaving](#)

Codes setting

Ajax system allows you to set up a keypad code, as well as personal codes for users added to the hub. This is convenient, for example, to provide a cleaning company with access to security management.

Keypad access code

To generate a keypad access code, in apps:

- 1. Go to the **Devices**  menu.
- 2. Select the keypad for which you want to set up an access code.
- 3. Go to **Settings** by clicking on the gear icon .
- 4. Find the **Keypad Code** item and click it.
- 5. Set the keypad code. Contains from 4 to 6 digits.
- 6. Press **Done** to save the data.

User access code

Registered user access code

▼

Access code for a user without an account

▼

Duress code

Keypad duress code

▼

Registered user duress code

▼

Duress code for a user without an account

▼

RRU code

▼

Adding passes and tags

KeyPad S Plus can work with Tag key fobs, Pass cards, and third-party cards and key fobs that use DESFire® technology.






Before adding third-party devices that support DESFire®, please ensure they have sufficient available memory to accommodate the new keypad. The third-party device should be pre-formatted.

The maximum number of connected passes/tags depends on the hub model. At the same time, the bound passes and tags do not affect the total limit of devices on the hub.

Hub model	Number of Tag or Pass devices
Hub Plus	99
Hub 2	50
Hub 2 Plus	200
Hub Hybrid (2G)/(4G)	50

The procedure for connecting Tag, Pass, and third-party devices is the same. See the connecting [instructions here](#).

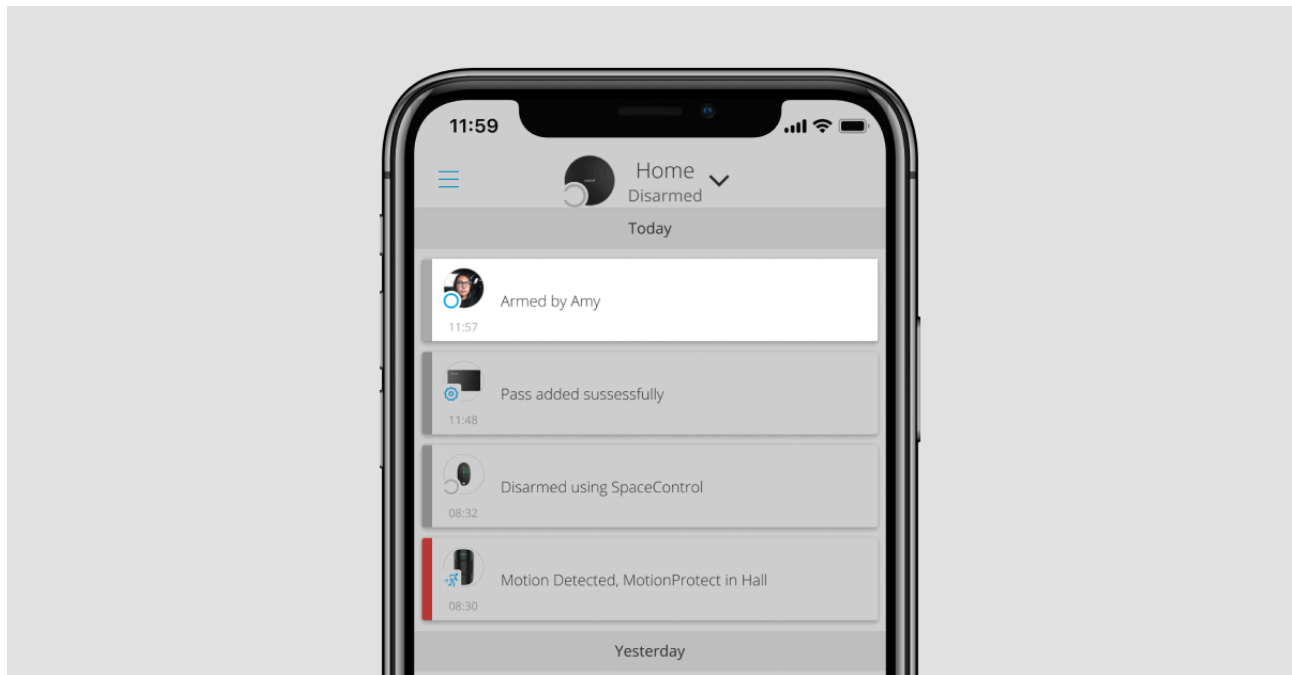
Controlling security with the codes

Using general, personal, or RRU code, you can control the [Night Mode](#) and the security of the entire object or separate groups. Entering the code should be confirmed by pressing one of the buttons  (Arm),  (Disarm) and  (enable [Night Mode](#)). The keypad allows you to use 4 to 6-digit codes. Erroneously entered digits are reset with the button **C**.

If a personal or access code 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 general code is used, the name of the user who changed the security mode is not displayed.

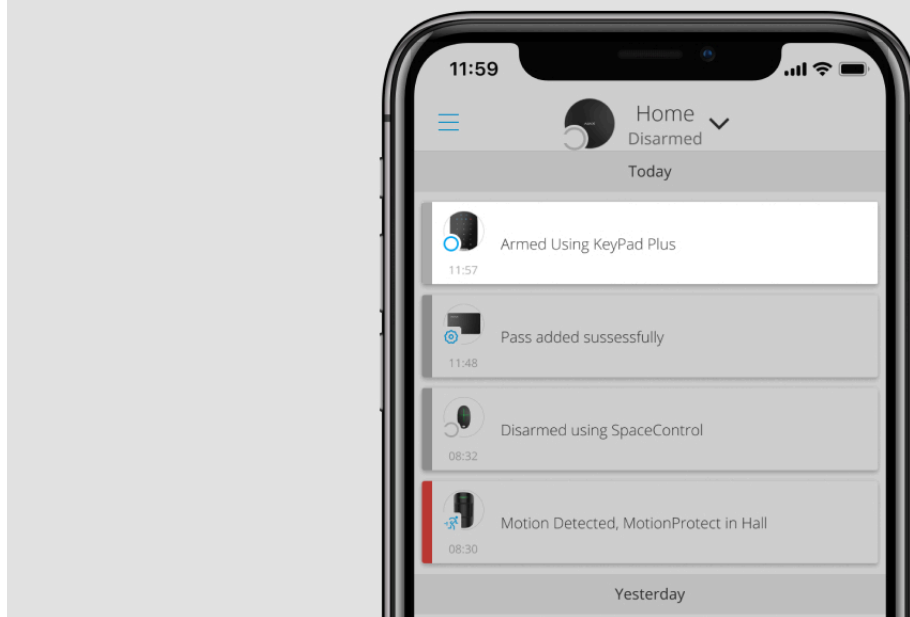
Arming with a personal code

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



Arming with a general code

The **device name** is displayed in the notifications and events feed



KeyPad S Plus is locked for the time specified in the settings if an incorrect code is entered 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 administrator rights can unlock the keypad in the Ajax app.

Controlling the object with a keypad code



Controlling the group with a keypad code



Controlling the object with a personal code



Controlling the group with the personal code



Security control of the entire object using an access code



Controlling the group with a general code



Using a duress code



Using the RRU code



Security management using Tag or Pass

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



Note that the keypad can be activated automatically by Auto-wake on [Delay when Entering](#) function if Delay When Entering is set up. This function is supported by KeyPad S Plus Jeweller with firmware version 5.60.6.3 or higher and hubs with [OS Malevich 2.18](#) and higher.

2. Bring Tag or Pass to the keypad pass/tag reader. It is marked with wave icons.
3. Enter the required code if the **Authorization confirmation with a passcode** feature is activated.
4. Press the **Arm, Disarm, or Night Mode** button on the keypad.



Note that if **Easy armed mode change** is enabled in KeyPad S Plus settings, you do not need to press the **Arm, Disarm, or Night Mode** button. The security mode will change to the opposite after tapping Tag or Pass.

Indication



KeyPad S Plus can report the current security mode, keystrokes, malfunctions, and status by LED indication and sound. The backlight displays the current security mode 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.

You can activate the keypad by swiping your hand over the touch panel from top to bottom. When activated, the backlight on the keypad will turn on, and a beep will sound (if enabled).



Auto-wake on Delay when Entering function allows automatically activating the keypad when Delay When Entering is set up. This function is supported by KeyPad S Plus Jeweller with firmware version 5.60.6.3 or higher and hubs with OS Malevich 2.18 and higher.



Event	Indication
There is no connection to the hub or radio signal range extender	LED X blinks
KeyPad S Plus enclosure 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 code 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 code attempt or attempt to use an unauthorized pass/tag	Long beep, during which the security status LEDs and keypad backlight blink 3 times
The batteries are low	<p>After changing the security mode, the X LED lights up. The touch buttons are locked for this time.</p> <p>When you try to turn on the keypad with discharged batteries, it emits a long beep, the X LED smoothly lights up and goes off, and then the keypad turns off.</p> <p><u>How to replace batteries in KeyPad S Plus</u></p>
The system requires to confirm authorization with a password after access devices' confirmation. Available if the Authorization confirmation with a passcode feature is activated	The current security status LED blinks during the set time for confirmation

Sound notifications of malfunctions

KeyPad S Plus can notify system users with an audible sound if any device is offline or the battery is low. The keyboards' LEDs **X** will blink. Malfunction notifications will be displayed in the events feed, SMS text, or push notifications.

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.



Sound notifications of malfunctions settings are available for all hubs with firmware version **OS Malevich 2.15** or higher.

Sound notifications of malfunctions are supported by KeyPad S Plus with firmware version 5.57.5.0 or higher.

Event	Indication	Note
If any device is offline	Two short sound signals, Malfunction indicator X blinks twice. Beep once per minute until all devices in the system are online.	Users can delay sound indication for 12 hours.
If KeyPad S Plus is offline	Two short sound signals, Malfunction indicator X blinks twice. Beep once per minute until the keyboard in the system is online.	It's impossible to delay sound indication.
If battery of any device is low	Three short sound signals, Malfunction indicator X blinks three times.	Users can delay sound indication for 4 hours.

	Beep once per minute until the battery is restored or the device is removed.	
--	--	--

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

Malfunctions

When a malfunction is detected, the Ajax app displays a malfunction counter on the device icon. All malfunctions are shown in the device states. Fields with malfunctions will be highlighted in red.


A malfunction is displayed if:

- The device temperature is outside acceptable limits.
- The device enclosure is open (tamper is triggered).
- No connection with the hub or radio signal range extender via Jeweller.
- The device battery is low.

Functionality testing

The Ajax system offers several tests to help select the device installation place. Tests do not start immediately. However, the waiting time does not exceed the duration of one “hub—device” polling interval. The polling interval can be checked and configured at hub settings (**Hub** → **Settings** ⚙️ → **Jeweller** or **Jeweller/Fibra**).

To run a test in the Ajax app:

1. Select the required hub.
2. Go to the **Devices**  tab.
3. Select **KeyPad S Plus** from the list.

4. Go to **Settings** ⚙️.

5. Select a test:

1. Jeweller Signal Strength Test

2. Signal Attenuation Test

6. Run the test.

Device placement



The device is designed for indoor use only.





KeyPad S Plus 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.



When holding KeyPad S Plus in your hands or using it on a table, we cannot guarantee that the touch buttons will work properly.

It is a good practice to install the keypad 1.3 to 1.5 meters above the floor for convenience. Install the keypad on a flat, vertical surface. This allows KeyPad S Plus to be firmly attached to the surface and to avoid false tamper triggering.

Signal strength

The Jeweller signal strength is determined by the number of undelivered or corrupted data packages over a certain period. The icon  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** — signal is missing.



Check the Jeweller signal strength before final installation. With a signal strength of one or zero bars, we do not guarantee stable operation of the device. Consider relocating the device, as repositioning even by 20 cm can significantly improve the signal strength. If there is still poor or unstable signal after the relocation, use a [radio signal range extender](#).

[What affects the radio communication range](#)

How not to install the keypad

1. Outdoors. This can lead to false alarms and device 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 device.
4. In places where KeyPad S Plus has an unstable or poor signal strength with the hub or radio signal range extender.

5. Closer than 1 meter from the hub or radio signal range extender. This can lead to a loss of communication with the device.
6. Close to electrical wiring. This may cause communication interference.
7. Outdoors. This could damage the device.
8. In a place with a low signal level. This may result in the loss of the connection with the hub.

Installation



Before installing KeyPad S Plus, ensure that you have selected the optimal location that complies with the requirements of this manual.

1. Attach the keypad to the surface with double-sided adhesive tape and carry out **signal strength** and **attenuation tests**. If the signal strength is unstable or one bar is displayed, move the keypad or use the radio signal range extender.



Use double-sided tape only for temporary installation. The device attached to the tape may come unstuck from the surface anytime. As long as the device is taped, the tamper will not be triggered when the device is detached from the surface.

2. Check the convenience of code 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 all fixing points. Be sure to fix the perforated corner on the SmartBracket plate so the tamper responds to a detachment attempt.



5. Tighten the holding screw on the bottom of the device's enclosure for more reliable fastening and protection from quick dismantling.
6. As soon as the keypad is fixed on the SmartBracket, it shall blink once with LED **X** — this is a signal that the tamper has been triggered. If the LED does not blink after installation on SmartBracket, check the tamper status in the Ajax app, and then make sure the plate is firmly attached.

Maintenance



Check the functioning of your keypad regularly. This can be done once or twice a week. Clean the device enclosure of dust, cobwebs, and other contaminants as they emerge. Use soft dry wipes suitable for equipment care.

Do not use substances that contain alcohol, acetone, petrol, and other active solvents to clean the device. Wipe the touch keypad gently: scratches can reduce the sensitivity of the keypad.

The batteries installed in the keypad provide up to 4,5 years of autonomous operation at default settings. If the battery is low, the system sends appropriate notifications, and the **X (Malfunction)** indicator smoothly lights up and goes out after each successful code entry.

KeyPad S Plus can work for up to 2 months after the low battery signal. However, we recommend you replace the batteries immediately upon notification. It is advisable to use lithium batteries. They have a large capacity and are less affected by temperatures.

How to replace batteries in KeyPad S Plus

Technical Specifications

All technical specifications of KeyPad S Plus Jeweller

Compliance with standards

Setup in compliance with EN 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:

- [email](#)
- [Telegram](#)

Manufactured by “AS Manufacturing” LLC

Subscribe to the newsletter about safe life. No spam

Subscribe