



# AJAX WH System Keypad Wireless Touch Keyboard User Manual

[Home](#) » [ajax](#) » AJAX WH System Keypad Wireless Touch Keyboard User Manual 

## Contents

- [1 AJAX WH System Keypad Wireless Touch Keyboard](#)
- [2 Product Information](#)
- [3 Product Usage Instructions](#)
- [4 Functional elements](#)
- [5 Operating Principle](#)
- [6 Function button](#)
- [7 Sending events to the monitoring station](#)
- [8 Indication](#)
- [9 Connecting](#)
- [10 Selecting the Location](#)
- [11 Settings](#)
- [12 Configuring codes](#)
- [13 Controlling security via codes](#)
- [14 Using Duress Code](#)
- [15 Functionality Testing](#)
- [16 Installation](#)
- [17 KeyPad Maintenance and Battery Replacement](#)
- [18 Technical Specifications](#)
- [19 Warranty](#)
- [20 Documents / Resources](#)
  - [20.1 References](#)



**AJAX WH System Keypad Wireless Touch Keyboard**



## Product Information

The KeyPad is a wireless indoor touch-sensitive keyboard designed for managing the Ajax security system. It allows users to arm and disarm the system and view its security status. The device is protected against code guessing and can raise a silent alarm when the code is entered under duress. It connects to the Ajax security system via a secured Jeweller radio protocol and has a communication range of up to 1,700 m in line of sight. The KeyPad operates only with Ajax hubs and does not support connecting via ocBridge Plus or cartridge integration modules. It can be set up using the Ajax apps available for iOS, Android, macOS, and Windows.

## 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. The perforated part is required for actuating the tamper in case of any attempt to tear off the device from the surface.

## Operating Principle

The KeyPad is a touch keypad that controls the security modes of the Ajax security system. It allows users to manage the security modes of the entire object or individual groups and activate the Night mode. The keyboard

supports the silent alarm function, which enables the user to inform the security company about being forced to disarm the security system without triggering the siren sounds or Ajax app notifications.

The KeyPad can be used to control security modes using different types of codes:

- **Keypad Code:** A general code set up for the keypad. All events are delivered to Ajax apps on behalf of the keypad.
- **User Code:** A personal code set up for users connected to the hub. 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. Events associated with this code are delivered to Ajax apps with a specific name.

The number of personal codes and access codes depends on the hub model. The brightness of the backlight and the volume of the keypad can be adjusted in its settings. If the batteries are discharged, the backlight turns on at the minimum level regardless of the settings. If the keypad is not touched for 4 seconds, it reduces the brightness of the backlight. After 8 seconds of inactivity, it goes into power-saving mode and turns off the display. Please note that entering commands will be reset as the keypad goes into power-saving mode. The KeyPad supports 4 to 6 digit codes. To confirm the entered code, press one of the following buttons: (arm), (disarm), or (Night mode). Any characters typed by mistake can be reset using the (Reset) button. The KeyPad also supports control of security modes without entering a code if the Arming without Code function is enabled in the settings. By default, this function is disabled.

## Product Usage Instructions

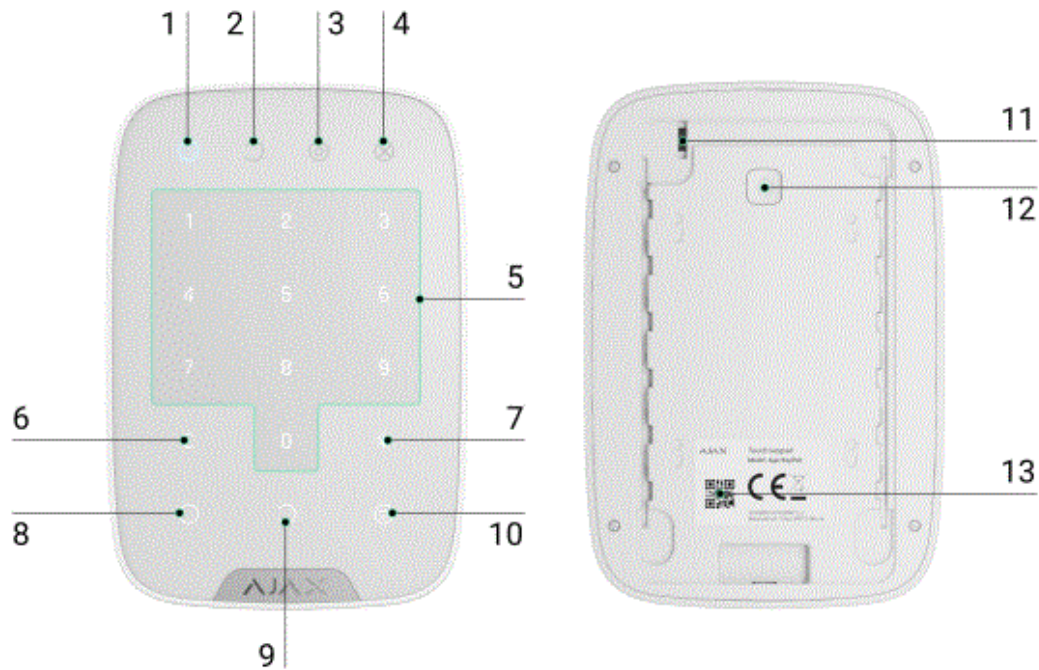
1. Ensure that the KeyPad is within the communication range of the Ajax security system hub.
  2. Set up the KeyPad using the Ajax apps for iOS, Android, macOS, or Windows.
  3. Use the numerical buttons on the keypad to enter the desired code.
  4. To activate the KeyPad, touch it to enable the button backlight and keypad beeps.
  5. Confirm the entered code by pressing one of the following buttons: (arm), (disarm), or (Night mode).
  6. If you make a mistake while entering the code, press the (Reset) button to reset the characters.
  7. To control security modes without entering a code, ensure that the Arming without Code function is enabled in the settings.
  8. If the keypad is not touched for 4 seconds, it will reduce the brightness of the backlight. After 8 seconds of inactivity, it will go into power-saving mode and turn off the display. Please note that entering commands will be reset when the keypad goes into power-saving mode.
  9. Adjust the brightness of the backlight and volume of the keypad in its settings as per your preference.
  10. If the batteries are discharged, the backlight will turn on at the minimum level regardless of the settings.
- KeyPad is a wireless indoor touch-sensitive keyboard managing the Ajax security system. Designed for indoor use. With this device, the user can arm and disarm the system and see its security status. KeyPad is protected against attempts to guess the code and can raise a silent alarm when the code 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.

### **note**

KeyPad operates with Ajax hubs only and does not support connecting via ocBridge Plus or cartridge integration modules.

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

## 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 (a 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 touch keypad for managing the Ajax security system. It controls the security modes of the entire object or individual groups and allows activating the Night mode. The keyboard supports the “silent alarm” function — the user informs the security company about being forced to disarm the security system and is not exposed by the siren sounds or Ajax apps. You can control the security modes with KeyPad using codes. Before entering the code, you should activate (“wake up”) the keypad by touching it. When it is activated, the button backlight is enabled, and the keypad beeps.

### KeyPad supports code types as follows:





- Keypad Code — general code that is set up for the keypad. When used, all events are delivered to Ajax apps

on behalf of the keypad.

- User Code — personal code that is set up for users connected to the hub. When used, all events are delivered to Ajax apps on behalf of the user.
- Keypad Access 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.

#### **note**

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

- The brightness of the backlight and the volume of the keypad are adjusted in its settings. With the batteries discharged, the backlight turns on at the minimum level regardless of the settings.
- If you do not touch the keypad for 4 seconds, KeyPad reduces the brightness of the backlight, and 8 seconds later goes into power-saving mode and turns off the display. As the keypad goes into power saving mode, it resets the commands entered!
- KeyPad supports 4 to 6-digit codes. Entering the code should be confirmed by pressing one of the buttons:   
(arm),  (disarm)  (Night mode). Any characters typed by mistake are reset with a button  ("Reset").  
KeyPad also supports control of security modes without entering a code, if the "Arming without Code" function is enabled in the settings. This function is disabled by default.

#### **Function button**

KeyPad has a Function button that operates in 3 modes:

- Off — the button is disabled. Nothing happens after clicking.
- Alarm — after the Function button is pressed, the system sends an alarm to the monitoring station of the security company, users, and activates the sirens connected to the system.
- Mute Interconnected Fire Detectors Alarms — after the Function button is pressed, the system disables the sirens of Ajax re-detectors. The option works only if Interconnected FireProtect Alarms is enabled (Hub → Settings Service → Fire detectors settings).

#### **Duress Code**

Duress Code allows you to simulate alarm deactivation. Unlike the panic button, if this code is entered, the user will not be compromised by the siren sounding, and the keypad and Ajax app will inform about the successful disarming of the system. At the same time, the security company will receive an alarm.

#### **The following types of duress codes are available:**

- Keypad Code — general duress code. When used, events are delivered to Ajax apps on behalf of the keypad.
- User Duress Code — personal duress code, set up for each user connected to the hub. When used, events are delivered to Ajax apps on behalf of the user.
- Keypad Access Code — duress 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.

[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 the settings. During this time, the hub will ignore all codes and inform the users of the security system and the CMS about an attempt to guess the code.
- The keypad will automatically unlock after the lock time defined in the settings expires. However, a user or PRO with admin rights can unlock the keypad through the Ajax app.

## Two-stage arming

- KeyPad participates in arming in two stages. When this feature is enabled, the system will only arm after being re-armed with SpaceControl or after a second-stage detector is restored (for example, by closing the front door on which DoorProtect is installed).

[Learn more](#)

## Jeweller data transfer protocol

- The keypad uses the Jeweller radio protocol to transmit events and alarms. This is a two-way wireless data transfer protocol that provides fast and reliable communication between the hub and the connected devices.
- Jeweller supports block encryption with an operating key and authentication of devices at each communication session to prevent sabotage and device spoofing. The protocol involves regular polling of devices by the hub at intervals of 12 to 300 seconds (set in the Ajax app) to monitor communication with all devices and display their statuses in the Ajax apps.

## More about Jeweller

## Sending events to the monitoring station

The Ajax security system can transmit alarms to the PRO Desktop monitoring app as well as the central monitoring station (CMS) via SurGard (Contact ID), SIA (DC-09), ADEMCO 685, and other proprietary protocols. See the list of CMSs to which you can connect the Ajax security system [here](#)

## KeyPad can transmit the following events:

- The duress code is entered.
- The panic button is pressed (if the Function button works in the panic button mode).
- The keypad is locked due to an attempt to guess a code.
- Tamper alarm/recovery.
- Hub connection loss/restoration.
- The keypad is temporarily turned off/on.
- Unsuccessful attempt to arm the security system (with Integrity Check enabled).

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 not only events but also the type of the device, the security group, the name assigned to it, and the room to the PRO Desktop or to the CMS. The list of transmitted parameters may differ depending on the type of the CMS and the selected

communication protocol.

**note**

The device ID and the number of the loop (zone) can be found in its states in the Ajax app.

**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 <b>X</b> blinks	Indicator notifies about lack of communication with hub or keypad lid opening. You can check <a href="#">the reason for malfunction in the Ajax Security System app</a>
KeyPad button pressed	A short beep, the system's current arming state LED blinks once
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
A malfunction is detected when arming (e.g., the detector is lost)	A long beep, the system's current arming state LED 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	<p>After arming/disarming the system, the malfunction indicator blinks smoothly. The keyboard is locked while the indicator blinks.</p> <p>When activating KeyPad with low batteries, it will beep with a long sound signal, the malfunction indicator smoothly lights up and then switches off</p>

## 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.

### note

Only users with admin 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 the 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 fails to connect to the hub, switch it off for 5 seconds and retry. The connected device will appear in the app device list. The update of the device statuses in the list depends on the detector ping interval in the hub settings (the default value is 36 seconds).

### note

There are no pre-set codes for KeyPad. Before using KeyPad, set all necessary codes: keypad code (general code), personal user codes, and duress codes (general and personal).

## Selecting the Location



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

### note

The device was developed only for indoor use.




## 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.

**note**

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 after moving the device still has a low or unstable signal strength, use a radio signal range extender.
- KeyPad is designed for operation when Flxed to the vertical surface. When using KeyPad in hands, we cannot guarantee successful operation of the sensor keyboard.



**States**

- 1. Devices 
- 2. KeyPad

Parameter	Meaning
Temperature	Temperature of the device. Measured on the processor and changes gradually.
	Acceptable error between the value in the app and the room temperature — 2°C.  The value is updated as soon as the device identifies a temperature change of at least 2°C.  You can configure a scenario by temperature to contro l automation devices  <a href="#">Learn more</a>
Jeweller Signal Strength	Signal strength between the hub and KeyPad

Battery Charge	<p>Battery level of the device. Two states available:</p> <p>OK</p> <p>Battery discharged</p> <p><a href="#">How battery charge is displayed in Ajax apps</a></p>
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
ReX	<a href="#">Displays the status of using a radio signal range extender</a>
Temporary Deactivation	Shows the status of the device: active, completely disabled by the user, or only notifications about triggering of the device tamper button are disabled
Firmware	Detector firmware version
Device ID	Device identifier

## Settings

1. Devices 
2. KeyPad
3. Settings 

Setting	Meaning
Name	Device name, can be edited
Room	Selecting the virtual room to which the device is assigned

Group management	Selecting the security group to which KeyPad is assigned
Access Settings	<p>Selecting the way of verification for arming/disarming</p> <p>Keypad codes only User codes only Keypad and user codes</p> <p>To activate the <b>Access Codes</b> set up for people who are not registered in the system, select the options on the keypad: <b>Keypad codes only</b> or <b>Keypad and user codes</b></p>
Keypad Code	Setting a code for arming/disarming
Duress Code	Setting <a href="#">a duress code for silent alarm</a>
Function Button	<p>Selection of the button function *</p> <p><b>Off</b> — the Function button is disabled and does not execute any commands when pressed</p> <p><b>Alarm</b> — by pressing the Function button, the system sends an alarm to the monitoring station of the security company and to all users</p> <p><b>Mute Interconnected Fire Detectors Alarm</b> — <a href="#">when pressed, mutes the alarm of Ajax</a></p>

	<p><a href="#">fire detectors. The feature works only if</a> Interconnected Fire Detectors Alarms is <a href="#">enabled</a></p> <p><a href="#">Learn more</a></p>
Arming without Code	If active, the system can be armed by pressing Arm button without a code
Unauthorized Access Auto-lock	If active, the keyboard is locked for the pre-set time after entering incorrect code 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 attempts to enter a code
Brightness	Brightness of the keyboard backlight
Buttons Volume	Volume of the beeper
Alert with a siren if panic button is pressed	<p>The setting appears if the <b>Alarm</b> mode is selected for <b>Function</b> button.</p> <p>If active, the Function button pressing triggers the sirens installed at the object</p>
Jeweller Signal Strength Test	Switches the device to the signal strength test mode
Signal Attenuation Test	Switches the Keypad to the signal fade test mode (available in devices with <b>firmware version 3.50 and later</b> )

Temporary Deactivation	<p>Allows the user to disconnect the device without removing it from the system.</p> <p>Two options are available:</p> <p><b>Entirely</b> — the device will not execute system commands or participate in automation scenarios, and the system will ignore device alarms and other notifications</p> <p><b>Lid only</b> — the system will ignore only notifications about the triggering of the device tamper button</p> <p><a href="#">Learn more about temporary deactivation of devices</a></p>
------------------------	--

User Guide	Opens the Keypad User Manual
Unpair Device	Disconnects the device from the hub and deletes its settings

## Configuring codes

- Ajax security system allows you to set up a keypad code, as well as personal codes for users added to the hub.
- With the OS Malevich 2.13.1 update, we have also added the ability to create access codes for people who are not connected to the hub. This is convenient, for example, to provide a cleaning company with access to security management. See how to set up and use each type of code below.


### To set the keypad code

1. Go to keyboard settings.
2. Select Keypad Code.
3. Set the keypad code you want.

### To set the keypad duress code

1. Go to keypad settings.
2. Select Duress Code.
3. Set the keypad duress code you want.


## To set a personal code for a registered user:

1. Go to profile settings: Hub → Settings  Users → User Settings. In this menu, you can also add the user ID.
2. Click Passcode Settings.
3. Set the User Code and User Duress Code.

### note

Each user sets a personal code individually!

## To set an access code for an unregistered person in the system

1. Go to the hub settings (Hub → Settings  ).
2. Select Keypad Access Codes.
3. Set up Name and Access Code.

If you want to set up a duress code, change settings for access to groups, Night mode, or code ID, temporarily disable or delete this code, select it in the list, and make changes.

### note

PRO or a user with administrator rights can set up an access code or change its settings. This function is supported by hubs with OS Malevich 2.13.1 and higher. Access codes are not supported by the Hub control panel.

## Controlling security via codes

You can control the security of the entire facility or separate groups using general or personal codes, as well as using access codes (configured by PRO or a user with admin rights).

If a personal user code is used, the name of the user who armed/disarmed the system is displayed in notifications and in the hub event feed. If a general code is used, the name of the user who changed the security mode is not displayed.




### note


Keypad Access Codes support hubs with OS Malevich 2.13.1 and higher. The Hub control panel does not support this function.

## Security management of the entire facility using a general code

- Enter the general code and press the arming/disarming / Night mode activation key.
- For example: 1234 →

## Group security management with a general code





- Enter the general code, press the \*, enter the group ID, and press the arming  /disarming  / Night mode activation key  .

For example: 1234 → \* → 2 → 

## What is Group ID





- If a group is assigned to the Keypad (Arming / Disarming permission field in the keypad settings), you do not need to enter the group ID. To manage the arming mode of this group, entering a general or personal user code is sufficient.
- Please note that if a group is assigned to the Keypad, you will not be able to manage Night mode using a general code.
- In this case, Night mode can only be managed using a personal user code (if the user has the appropriate rights).
- Rights in the Ajax security system

## Security management of the entire facility using a personal code

- Enter your user ID, press \*, enter your personal user code, and press the arming  /disarming  / Night mode activation  key.
- For example: 2 → \* → 1234 → 

## What is the User ID

### Group security management using a personal code

- Enter user ID, press \*, enter personal user code, press \*, enter group ID, and press the arming  /disarming  / Night mode activation  .
- For example: 2 → \* → 1234 → \* → 5 → 

## What is Group ID




## What is the User ID

- If a group is assigned to the Keypad (Arming / Disarming permission field in the keypad settings), you do not need to enter the group ID. To manage the arming mode of this group, entering a personal user code is sufficient.

## Security control of the entire object using an access code

- Enter the access code and press the arming/disarming / Night mode activation key.
- For example: 1234 →

## Security management of the group using an access code

- Enter the access code, press the \*, enter the group ID, and press the arming  /disarming  / Night mode activation  key.



- For example: 1234 → \* → 2 → 

## What is Group ID







## Using Duress Code

- Duress Code allows you to raise a silent alarm and imitate alarm deactivation. A silent alarm means that the Ajax app and sirens will not shout and expose you. But a security company and other users will be alerted instantly. You can use both personal and general duress codes. You can also set up a duress access code for people not registered in the system.

### note

Scenarios and sirens react to disarming under duress in the same way as to normal disarming.

### To use a general duress code:

- Enter the general duress code and press the disarming key .
- For example: 4321 → 
- To use a personal duress code of a registered user:
- Enter the user ID, press \*, then enter the personal duress code and press the disarming key .
- For example: 2 → \* → 4422 → 
- To use a duress code of a person unregistered in the system:
- Enter the duress code set in Keypad Access Codes and press the disarming key .
- For example: 4567 → 

### How the re-alarm muting function works

Using the Keypad, you can mute the interconnected fire detector alarm by pressing the Function button (if the corresponding setting is enabled). The reaction of the system to pressing a button depends on the state of the system:

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

### Learn more about Interconnected Fire Detectors Alarms

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

### Learn more

## Functionality Testing

- The Ajax security system allows for conducting tests to check 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 starts depending on the settings of the detector scanning period (the paragraph on “Jeweller” settings in hub settings).
  - Jeweller Signal Strength Test
  - Attenuation Test

## Installation

### WARNING

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!

### NOTE

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 the 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 a 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 light up and go out after each successful code entry.
  - How long do Ajax devices operate on batteries, and what affects this
  - 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 guessing a code	Yes
Radio communication protocol	Jeweller <a href="#">Learn more</a>
Radio frequency band	866.0 – 866.5 MHz 868.0 – 868.6 MHz 868.7 – 869.2 MHz 905.0 – 926.5 MHz 915.85 – 926.5 MHz 921.0 – 922.0 MHz Depends on the region of sale.
Compatibility	<a href="#">Operates only with all Ajax hubs, and radio signal range extenders</a>
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) <a href="#">Learn more</a>
Power supply	4 × AAA batteries
Power supply voltage	3 V (batteries are installed in pairs)
Battery life	Up to 2 years
Installation method	Indoors
Operating temperature range	From -10°C to +40°C
Operating humidity	Up to 75%
Overall dimensions	150 × 103 × 14 mm
Weight	197 g
Service life	10 years
Certification	Security Grade 2, Environmental Class II in conformity with the requirements of EN 50131-1, EN 50131-3, EN 50131-5-3

Compliance with standards

## Warranty

Warranty for the Limited Liability Company “Ajax Systems Manufacturing” 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](mailto:support@ajax.systems)

Subscribe to the newsletter about safe life. No spam

Email
















Subscribe

## Documents / Resources

 <p>KeyPad User manual Version 2.13.1</p> <p>KeyPad is a wireless alarm system component designed for use with Ajax Systems alarm systems. It is a compact, sleek device that can be used to arm and disarm the alarm system. It is also used to receive status information from the alarm system.</p> <p>Connecting to the Ajax security system via a network. KeyPad will connect to the Ajax security system via a network. It will connect to the Ajax security system via a network. It will connect to the Ajax security system via a network.</p> <p>The device is set up via the Ajax app for iOS, Android, macOS, and Windows.</p> <p><input type="checkbox"/> <a href="#">Download PDF</a></p>	<p><a href="#">AJAX WH System Keypad Wireless Touch Keyboard</a> [pdf] User Manual</p> <p>WH System Keypad Wireless Touch Keyboard, WH, System Keypad Wireless Touch Keyboard, Keypad Wireless Touch Keyboard, Wireless Touch Keyboard, Touch Keyboard</p>
--	--

## References

- 📄 [OS Malevich 2.13.1: Access codes for keypads without registering a user | Ajax Systems Blog](#)
- 📄 [Connecting Ajax to CMS](#)
- 📄 [OS Malevich 2.12: Full control over the hub communication and even more features for Ajax sirens | Ajax Systems Blog](#)
- 📄 [End user agreement - Ajax Systems](#)
- 📄 [Jeweller radio technology | Ajax Systems](#)
- 📄 [Fire alarm systems from Ajax Systems](#)
- 📄 [Security system control panels | Ajax Systems](#)
- 📄 [KeyPad - Wireless touch keyboard | Ajax Systems](#)
- 📄 [ocBridge Plus — Module for Ajax devices integration with wired systems](#)
- 📄 [Signal range extenders in the security system | Ajax Systems](#)
- 📄 [uartBridge — Module for Ajax devices integration with third-party wireless alarms systems](#)
- 📄 [What affects the quality of radio communication between Ajax devices](#)
- 📄 [Software | Ajax Systems](#)
- 📄 [Ajax devices standards compliance list](#)
- 📄 [Warranty - Ajax Systems](#)
- 📄 [User account types and rights | Ajax Systems Support](#)

-  [How battery charge is displayed in Ajax apps | Ajax Systems Support](#)
-  [What is the identification \(ID\) of the group? | Ajax Systems Support](#)
-  [What is duress code, and how to use it | Ajax Systems Support](#)
-  [What is the user identifier? | Ajax Systems Support](#)
-  [How long Ajax devices operate on batteries, and what affects this | Ajax Systems Support](#)
-  [How to deactivate a device without removing it from the system | Ajax Systems Support](#)
-  [How to change batteries in the KeyPad | Ajax Systems Support](#)
-  [Which CMSs can Ajax hubs be connected to | Ajax Systems Support](#)
-  [Jeweller radio protocol: technology and capabilities | Ajax Systems Support](#)
-  [How to create and configure a scenario in the Ajax system | Ajax Systems Support](#)
-  [What a residential fire alarm system is and how It works | Ajax Systems Support](#)
-  [How to set up your system according to PD 6662:2017 requirements | Ajax Systems Support](#)
-  [What is Attenuation Test | Ajax Systems Support](#)
-  [What is Interconnected Fire Detectors Alarm and how does it work | Ajax Systems Support](#)
-  [What is Jeweller Signal Strength Test | Ajax Systems Support](#)