KeyPad Plus Jeweller user manual

Updated September 1, 2025

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

The keypad 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 (4G) Jeweller, Hub Plus Jeweller, Hub 2 Jeweller, Superior Hub Hybrid and Hub 2 Plus Jeweller running OS Malevich 2.11 and higher. Connection to Hub (2G) Jeweller and the ocBridge Plus* and uartBridge* integration modules is not supported.

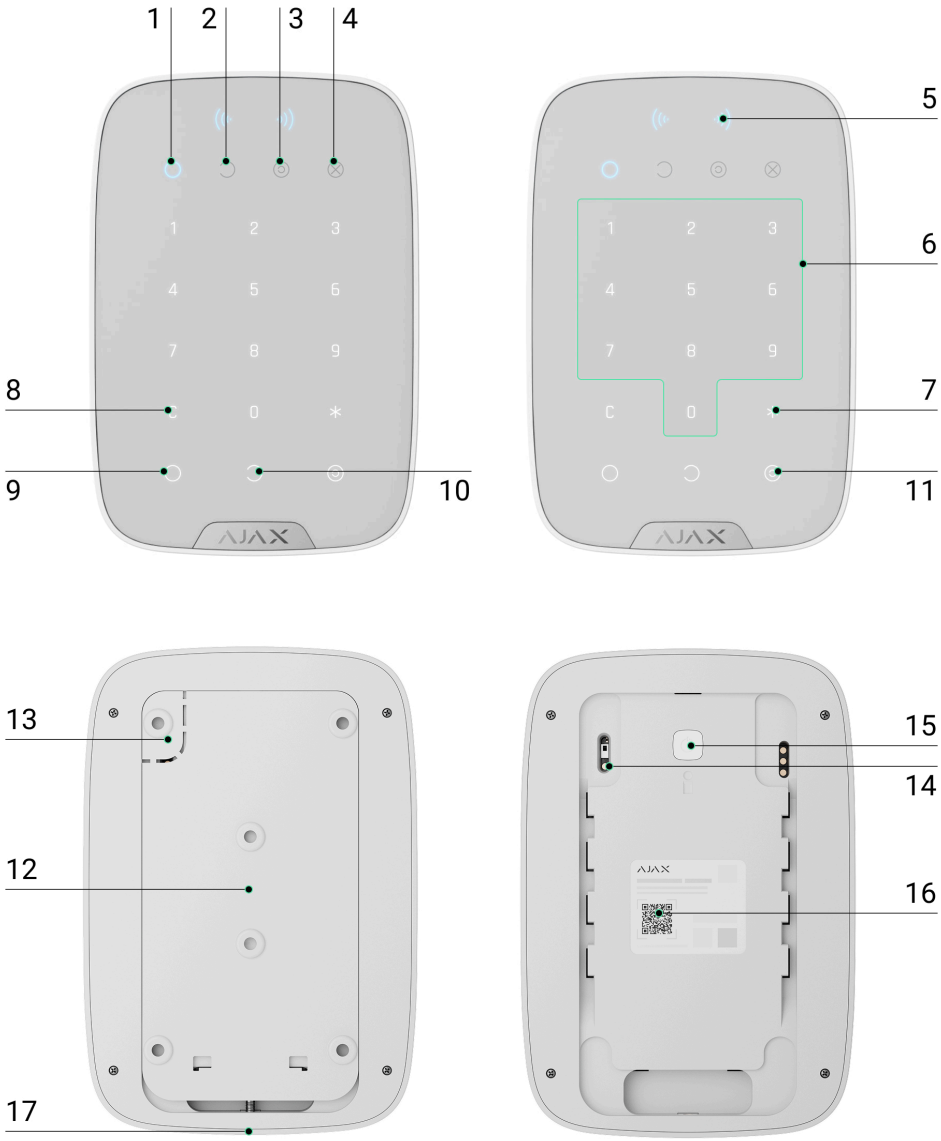
** Not evaluated by UL.*

The keypad operates as part of the Ajax 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 3.5 years.

> Only Hub 2 Plus Jeweller and Hub 2 (4G) Jeweller are certified according to UL/ULC standards.

Buy KeyPad Plus Jeweller 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. Power button
14. Tamper button
15. Keypad QR Code

Operating principle

0:00 / 0:04

KeyPad Plus Jeweller 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 Jeweller using:

1. **Codes**. The keypad supports general and personal codes, as well as arming without entering a code.
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 Jeweller uses the DESFire® technology. DESFire® is based on the ISO 14443 international standard and combines 128-bit encryption and copy protection.

KeyPad Plus Jeweller supports code types as follows:

- **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** — 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.

Access codes are not supported by the Hub (2G) Jeweller control panel.

Before entering a code or using Tag/Pass, you should activate (“wake up”) the KeyPad Plus Jeweller 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.

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 Plus Jeweller with firmware version 6.60.0.6 or higher and hubs with OS Malevich 2.19 or higher.

The KeyPad Plus Jeweller 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 Jeweller 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 Jeweller 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 Jeweller 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 detectors alarm** — after the **Function** button is pressed, the system mutes the alarm of the **Ajax fire detectors***. Available only if an **Interconnected Fire Detectors Alarm** is enabled (Hub → Settings → Service → Fire detectors settings)** Only FireProtect 2 RB (Heat/Smoke/CO) UL Jeweller and FireProtect 2 RB (Heat/Smoke) UL Jeweller are certified according to UL/ULC standards.*

Learn more

Duress code

KeyPad Plus Jeweller 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

Two-stage arming

KeyPad Plus Jeweller 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 arming using a personal or general code on the keypad.

Learn more

Event transmission to the monitoring station

The Ajax system can connect to the CMS and transmit events and alarms to the monitoring station of the security company in **SurGard (Contact ID), ADEMCO 685, 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 Jeweller is incompatible with Hub (2G) Jeweller, third-party security central units, and ocBridge Plus* and uartBridge* integration modules.

** Not evaluated by UL.*

Before starting connection

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.

1. Install the Ajax app and **create an account**. Add a hub and create at least one room.

> Only Hub 2 Plus Jeweller and Hub 2 (4G) Jeweller are certified according to UL/ULC standards.

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.

> Only a user or PRO with full admin rights can add a device to the hub.

To connect KeyPad Plus Jeweller

1. Open the Ajax app. If your account has access to multiple hubs, select the one to which you want to connect KeyPad Plus Jeweller.
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 Jeweller 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 Jeweller is not removed from the device list of the old hub. This must be done manually through the Ajax app.

KeyPad Plus Jeweller 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 Jeweller states. You can see them in the **Devices** tab in the Ajax app.

Icon	Value
	Jeweller signal strength — Displays the signal strength between the hub or radio signal range extender and KeyPad Plus Jeweller
	Battery charge level of KeyPad Plus Jeweller
	KeyPad Plus Jeweller works via a **radio signal range extender**
	The device is in the signal attenuation test mode. **Learn more**
	KeyPad Plus Jeweller body status notifications are disabled **Learn more**

	KeyPad Plus Jeweller is deactivated Learn more
	Pass/Tag reading is enabled in KeyPad Plus Jeweller settings
	Pass/Tag reading is disabled in KeyPad Plus Jeweller settings
	The device has lost connection with the hub or the hub has lost connection with the Ajax Cloud server.
	The device has not been transferred to the new hub. Learn more

States

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

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

Parameter	Value
Data import	Displays the error when transferring data to the new hub: • **Failed** — the device has not been transferred to the new hub. Learn more
Malfunction	Pressing ⓘ opens the KeyPad Plus Jeweller malfunctions list.

	The field is displayed only if a malfunction is detected.
Temperature	Keypad temperature. It is 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 control automation devices. Learn more
Jeweller Signal Strength	Jeweller signal strength between the hub / radio signal range extender and the keypad. Recommended values — 2–3 bars.
Connection via Jeweller	Connection status between the hub or range extender and the keypad: • **Online** — the keypad is online. • **Offline** — no connection to the keypad.
Transmitter power	Displays the selected power of the transmitter. The parameter appears when the **Max** or **Attenuation** option is selected in the **Signal attenuation test** menu. Learn more
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 Jeweller range extender use. **The field is not displayed if the keypad works directly with the hub**.
Pass/Tag Reading	Displays if card and keyfob reader is enabled.
Assigned Group Easy Management	Displays whether or not the security mode can be switched with Pass or Tag and without confirmation by the control buttons , , .
Easy Armed Mode Change	This setting replaces **Assigned Group Easy Management** on KeyPad Plus Jeweller with firmware version 5.60.6.3 or higher, operating with hubs with OS Malevich 2.19 or higher. Shows the configuration for the **Easy Armed Mode Change** feature:

	• **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 by pressing 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.
Permanent Deactivation	Shows the status of the device: • **No** — the device operates normally and transmits all events. • **Lid only** — the hub admin has disabled notifications about the body opening. • **Entirely** — the hub admin 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
One-Time Deactivation	Shows the status of the keypad one-time deactivation setting: • **No** — the keypad operates in normal mode.

	• **Lid only** — notifications on the keypad tamper triggering are disabled until the first disarm. • **Entirely** — the keypad is entirely excluded from the operation of the system until the first disarm. The device does not execute system commands and does not report alarms or other events. Learn more
Firmware	KeyPad Plus Jeweller firmware version.
Device ID	Device identifier.
Device No.	Number of the device loop (zone).

Settings

KeyPad Plus Jeweller is configured in the Ajax app:

1. Go to the **Devices** tab.
2. Select **KeyPad Plus Jeweller** 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
Name	Device name. Displayed in the list of hub devices, SMS text, and notifications in the event feed.

	To change the device name, click on the pencil icon . The name can contain up to 12 Cyrillic characters or up to 24 Latin characters.
Room	Selecting the virtual room to which KeyPad Plus Jeweller 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**. If the Followed group feature is configured for groups, their security state can automatically change depending on their settings and initiators' states. .
Access Settings	Selecting the method of arming/disarming: • Keypad codes only. • User codes only. • Keypad and user codes.

	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** .
Keypad Code	Selection of a general code for security control. Contains 4 to 6 digits.
Duress Code	Selecting a general 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. • **Panic** — 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. Learn more
Accidental press protection	Available with OS Malevich 2.31 or later.

	When enabled, the **Function** button should be pressed twice to send a panic alarm. This setting is available if **Function button** is set to **Panic**.
Unauthorized Access Auto-Lock	If active, the keypad is locked for the pre-set time if an incorrect code 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 code 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.

Buttons Volume	Selecting the keypad buttons volume level when pressed.
Pass/Tag Reading	When enabled, the security mode can be controlled with Pass and Tag access devices.
Authorization confirmation with a passcode	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. This setting is supported when KeyPad Plus Jeweller is connected to hubs with firmware version OS Malevich 2.20 or higher.
Time for confirmation	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. This setting is supported when KeyPad Plus Jeweller is connected to hubs with firmware version OS Malevich 2.21 or higher.
Assigned Group Easy Management	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.The option is available if **Pass/Tag Reading** is enabled in the keypad settings. 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. Learn more
Easy Armed Mode Change	This setting replaces **Assigned Group Easy Management** on

	KeyPad Plus Jeweller with firmware version 5.60.6.3 or higher, operating with hubs with OS Malevich 2.19 or higher. Allows users to arm/disarm the system without confirmation by pressing keypad buttons. Three options are available: • **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	The option allows you to arm the system without entering a code. To do so, just click on the **Arm** or **Night Mode** button.

Auto-wake on Delay when Entering	The feature is available on KeyPad Plus Jeweller with firmware version 6.60.0.6 or higher, operating with hubs with OS Malevich 2.19 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**	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**
Signal Attenuation Test	Switches the device to the signal attenuation test mode. **Learn more**
Pass/Tag Reset	Allows deleting all hubs associated with Tag or Pass from device memory. **Learn more**
User Guide	Opens KeyPad Plus Jeweller user manual in the Ajax app.
Permanent Deactivation	Allows the user to disable the device without removing it from the system.

	Three options are available: • **No** — the device operates in normal mode and transmits all events. • **Entirely** — the device does not execute system commands and does not participate in automation scenarios, and the system ignores alarms and other device notifications. • **Lid only** — the system ignores the device tamper triggering notifications. Learn more
One-Time Deactivation	Allows the user to disable events of the device until the first disarm. Three options are available: • **No** — the device operates in normal mode. • **Lid only** — notifications on the device tamper triggering are disabled while the armed mode is active. • **Entirely** — the device is completely excluded from the operation of the system while the armed mode is active. The device does not execute system commands and does not report alarms or other events. Learn more
Delete Device	Disconnects KeyPad Plus Jeweller 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

** Only FireProtect 2 RB (Heat/Smoke/CO) UL Jeweller and FireProtect 2 RB (Heat/Smoke) UL Jeweller detectors are certified according to UL/ULC standards.*
*** In compliance with UL 636, the audible alarm should be disabled for triggering the panic button.*

Configuring codes

Ajax 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 added to the hub. This is convenient, for example, to provide a cleaning company with access to security management.

With the **OS Malevich 2.17** update, codes for the rapid response units are available. The RRU codes are activated after the alarm and are valid for a specified period. See how to set up and use each type of code below.

To set 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 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 code individually. The admin cannot set a code for all users.

To set up an access code for a person who is not registered in the system

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

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

> PRO or a user with admin 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 (2G) Jeweller control panel.

To set up the RRU code

Only a PRO with the rights to configure the system can create and configure the RRU codes in the **Ajax PRO apps**. More information about configuring this feature you can find in **this article**.

The RRU codes are supported by hubs (except the Hub (2G) Jeweller model) with OS Malevich 2.17 and higher.

Adding passes and tags

KeyPad Plus Jeweller 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®, make sure they have enough free memory to handle the new keypad. Preferably, 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 (4G) Jeweller	50
Hub Plus Jeweller	99
Hub 2 Jeweller	50
Hub 2 Plus Jeweller	200
Superior Hub Hybrid	50

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

Controlling security via codes

You can control **Night Mode**, security of the entire facility or separate groups using general, personal, RRU, and access codes (configured by PRO or a user

with admin rights). The keypad allows you to use 4 to 6 digit codes. Incorrectly entered numbers can be cleared with the C button.

Code Length Restrictions for the keypad

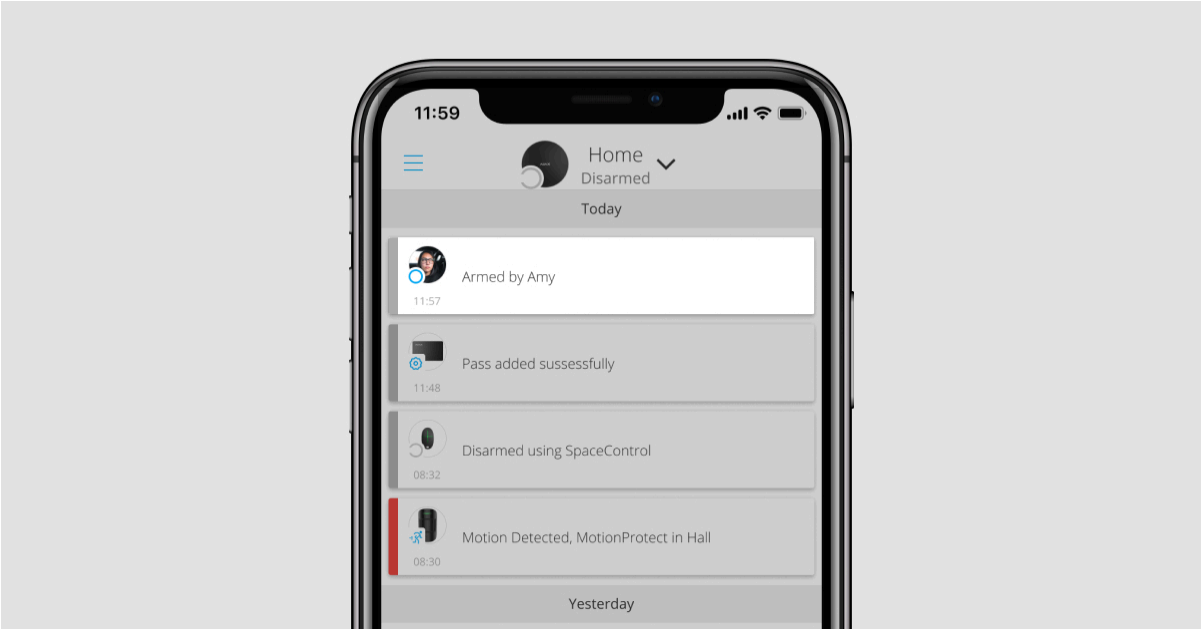
If a personal code or access code is used, the name of the user who armed or disarmed the system is displayed in the hub event feed and in the notifications list. If a general code is used, the name of the user who changed the security mode is not displayed.

Keypad access codes are supported by hubs (except the Hub (2G) Jeweller model) with OS Malevich 2.13.1 and higher.

The **RRU codes** are supported by hubs (except the Hub (2G) Jeweller model) with OS Malevich 2.17 and higher.

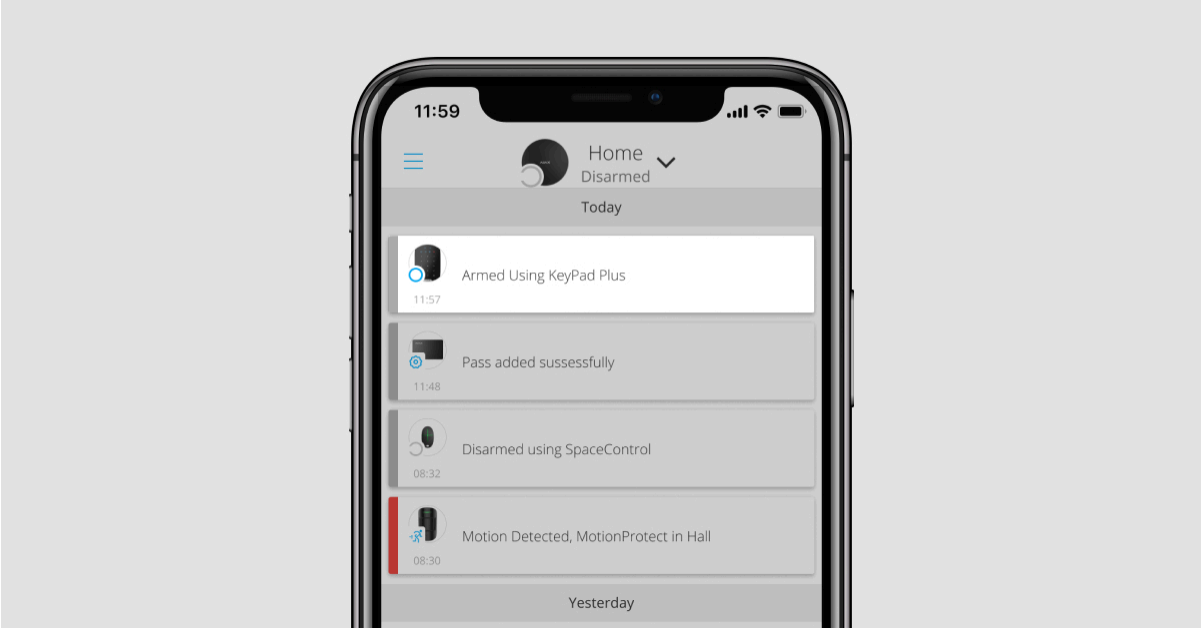
Arming with a personal code

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 Plus Jeweller 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 to the monitoring station of the security company. A user or PRO with administrator rights can unlock the keypad in the Ajax app.

Controlling security at the object via general code

1. Activate the keypad by swiping your hand over it. Bring Tag or Pass to the keypad pass/tag reader if the **Authorization confirmation with a passcode** feature is activated.
2. Enter the **general code**.
3. Press the **arming** /**disarming** /**Night Mode** key.

For example: 1234 →

Group security management with a general code

1. Activate the keypad by swiping your hand over it. Bring Tag or Pass to the keypad pass/tag reader if the **Authorization confirmation with a passcode** feature is activated.
2. Enter the **general code**.
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 Jeweller (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 general or personal code is sufficient.

If a group is assigned to KeyPad Plus Jeweller, 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 code if the user has the appropriate rights.

Rights in the Ajax security system

Security management of the facility using a personal code

1. Activate the keypad by swiping your hand over it. Bring Tag or Pass to the keypad pass/tag reader if the **Authorization confirmation with a passcode** feature is activated.
2. Enter the **User ID**.
3. Press the * (**Function** button).

4. Enter your **personal code**.
5. Press the **arming** ◯/**disarming** ◯/**Night Mode** ◎ key.

For example: 2 → * → 1234 → ◯

What is User ID

Group security management with a personal code

1. Activate the keypad by swiping your hand over it. Bring Tag or Pass to the keypad pass/tag reader if the **Authorization confirmation with a passcode** feature is activated.
2. Enter the **User ID**.
3. Press the * (**Function** button).
4. Enter your **personal code**.
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 Jeweller (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 code is sufficient.

What is Group ID

What is User ID

Security control of the entire object using an access code

Enter the **access code** and press the **arming** /**disarming** /**Night Mode** button.

For example: 1234 →

Security management of the group using a common code

Enter the **access code**, press the *asterisk icon*, enter the **group ID** and press the **arming** /**disarming** /**Night Mode** button.

For example: 1234 → * → 2 →

What is Group ID

Using a duress code

A duress code allows you to simulate alarm deactivation. The Ajax app and sirens installed at the facility will not give the user away in this case, but the security company and other users will be warned about the incident. You can use both a personal and a general duress code. In **Keypad Access Codes**, you can also set up a duress code for people not registered in the system.

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

Learn more

To use a keypad general duress code

1. Activate the keypad by swiping your hand over it. Bring Tag or Pass to the keypad pass/tag reader if the **Authorization confirmation with a passcode** feature is activated.
2. Enter the **general duress code**.

3. Press the disarming button .

For example: 4321 →

To use a personal duress code of registered user

1. Activate the keypad by swiping your hand over it. Bring Tag or Pass to the keypad pass/tag reader if the **Authorization confirmation with a passcode** feature is activated.
2. Enter the **User ID**.
3. Press the * (**Function** button).
4. Enter the **personal duress code**.
5. Press the disarming button .

For example: 2 → * → 4422 →

To use a duress code of a person who is not registered in the system

Enter the **duress code** set in **Keypad Access Codes** and press the **disarming key** .

For example: 4567 →

Using the RRU code

The RRU code is activated after triggering the alarm during the time configured in the hub settings, and it is valid for a specified period. This ensures that such code will only be used in case of risk, unlike keypad or user codes.

How to configure the RRU code

Security control of the object using the RRU code:

Enter **RRU Code** and press the **arming** / **disarming** / **Night Mode activation** button.

For example: 1234 →

Security control of the group using the RRU code:

Enter **RRU Code**, press *, enter Group ID, and press the **arming** / **disarming** / **Night Mode activation** button.

For example: 1234 → * → 2 →

Security management using Tag or Pass

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

> Note that the keypad can be activated automatically with the **Auto-wake on Delay when Entering** function if Delay When Entering is set up. This function is supported by KeyPad Plus Jeweller with firmware version 6.60.0.6 or higher and hubs with OS Malevich 2.19 or 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 the KeyPad Plus Jeweller 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.

Security control of a single group

Tag or Pass can control the security mode of a single group. This is possible if KeyPad Plus Jeweller is not assigned to any group and Tag or Pass has no group restrictions.

To change the security mode of a single group using Tag or Pass:

1. Activate the keypad by swiping your hand over it. Bring Tag or Pass to the keypad pass/tag reader if the **Authorization confirmation with a passcode** feature is activated.
2. Press the ✳ button.
3. Enter the **Group ID**.
4. Press the **arming** / **disarming** / **Night Mode activation** button.

For example: ✳ → 01 →

If the security mode is successfully changed, a short beep will sound, the indicator will change, and a notification with the username will appear in the event log.

Mute Interconnected Fire Detectors Alarms function

KeyPad Plus Jeweller 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 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 **Ajax fire detectors*** is muted.

Keep in mind that the option is available only if **Interconnected Fire Detectors Alarm** is enabled.

** Only FireProtect 2 RB (Heat/Smoke/CO) UL Jeweller and FireProtect 2 RB (Heat/Smoke) UL Jeweller detectors are certified according to UL/ULC standards.*
*** In compliance with UL 636, the audible alarm should be disabled for triggering the panic button.*

Learn more

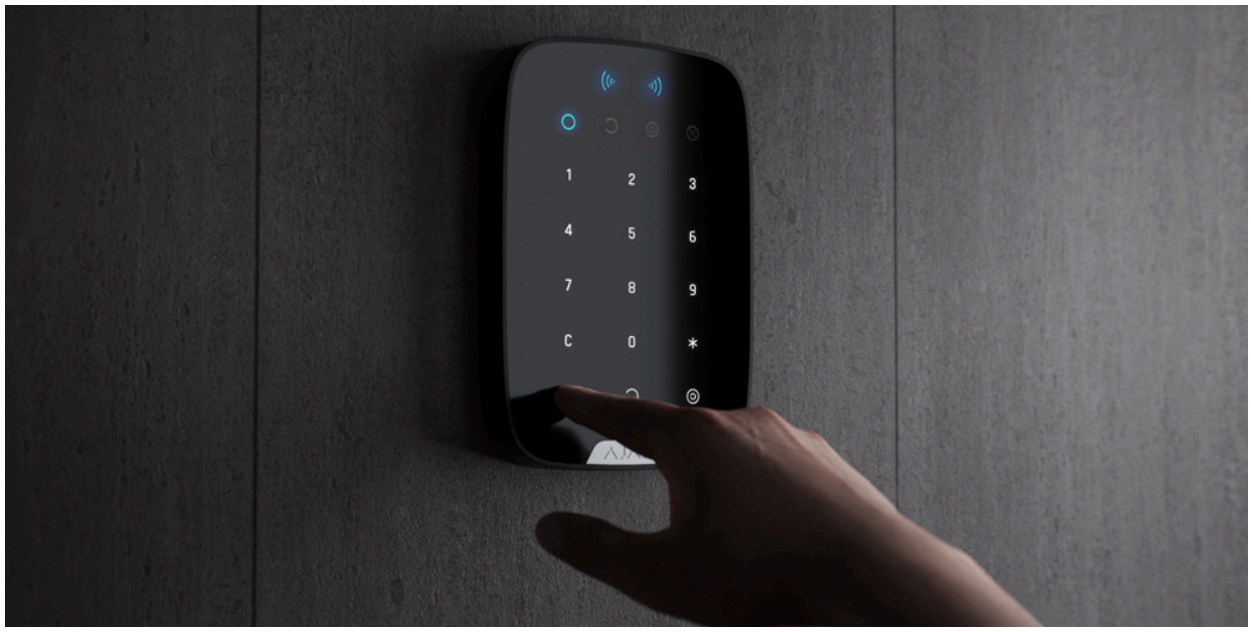
With the OS Malevich 2.12 update, users can mute fire alarms in their groups without affecting detectors in the groups to which they do not have access.

Learn more

Indication

KeyPad Plus Jeweller 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.

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 Plus Jeweller with firmware version 6.60.0.6 or higher and hubs with OS Malevich 2.19 or higher.



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).

Event	Indication
There is no connection to the hub or radio signal range extender	LED **X** blinks
KeyPad Plus Jeweller 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 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 unauthorised pass/tag	Long beep, during which the security status LEDs and keypad backlight blink 3 times
The batteries are low	After changing the security mode, the **X** LED lights up. The touch buttons are locked for this time. 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, then the keypad turns off **How to replace batteries in KeyPad Plus Jeweller**
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

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

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 (except the Hub model) with firmware version OS Malevich 2.15 or higher.

Sound notifications of malfunctions are supported by KeyPad Plus Jeweller 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 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. Beep once per minute until the battery is restored or the device is removed.	Users can delay sound indication for 4 hours.

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.

Functionality testing

The Ajax system provides several types of tests that help you make sure that installation points of devices are selected correctly.

KeyPad Plus Jeweller functionality tests do not start straight away but after no more than one hub-detector ping period (36 seconds when using the standard hub settings). 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 Jeweller → Settings)

- **Jeweller Signal Strength Test**
- **Signal Attenuation Test**

Choosing a location

KeyPad Plus Jeweller is best placed indoors near the entrance. This allows disarming the system before the entry delays have expired, as well as quickly arming the system when leaving the premises.

When holding KeyPad Plus Jeweller 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 Plus Jeweller to be firmly attached to the surface and to avoid false tamper triggering.

Besides, the placement of the keypad is determined by the distance from the hub or the radio signal range extender, and the presence of obstacles between them that prevent the passage of the radio signal: walls, floors, and other objects.

What affects the radio communication range

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 after moving the device still has a low or unstable signal strength, use a **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 Jeweller has an unstable or poor signal strength with the hub or radio signal range extender.

- Within 1 meter of a hub or radio signal range extender.
- Close to electrical wiring. This may cause communication interferences.
- Outdoors. This could damage the device.

Installing the keypad

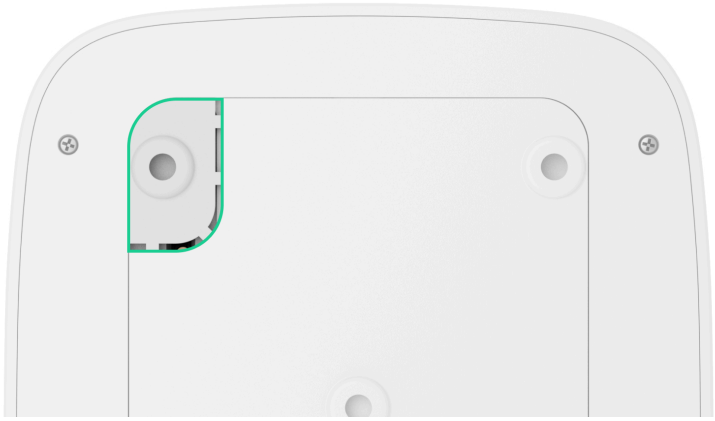
Prior to installing KeyPad Plus Jeweller, be sure to select the optimal location following the requirements of this manual.

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 if one bar is displayed, move the keypad or use the **radio signal 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 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 that the tamper responds to a detachment attempt.



5. Slide KeyPad Plus Jeweller onto the mounting plate and tighten the mounting screw at the bottom of the body. The screw is needed for more reliable fastening and protection of the keypad 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 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.

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

The batteries installed in the keypad provide up to 3.5 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 Plus Jeweller can work 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 long Ajax devices operate on batteries, and what affects this

How to replace batteries in KeyPad Plus Jeweller

Complete set

1. KeyPad Plus Jeweller
2. SmartBracket mounting plate
3. 4 pre-installed lithium batteries AA (FR6)
4. Installation kit
5. Quick Start Guide

Technical specifications

All technical specifications of KeyPad Plus Jeweller

Compliance with standards

UL-compliant installation

Warranty

The warranty for the Limited Liability Company “Ajax Systems Manufacturing” 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.

Warranty obligations

User Agreement

Contact Technical Support:

- **e-mail**
- **Telegram**