KeyPad Outdoor Jeweller user manual

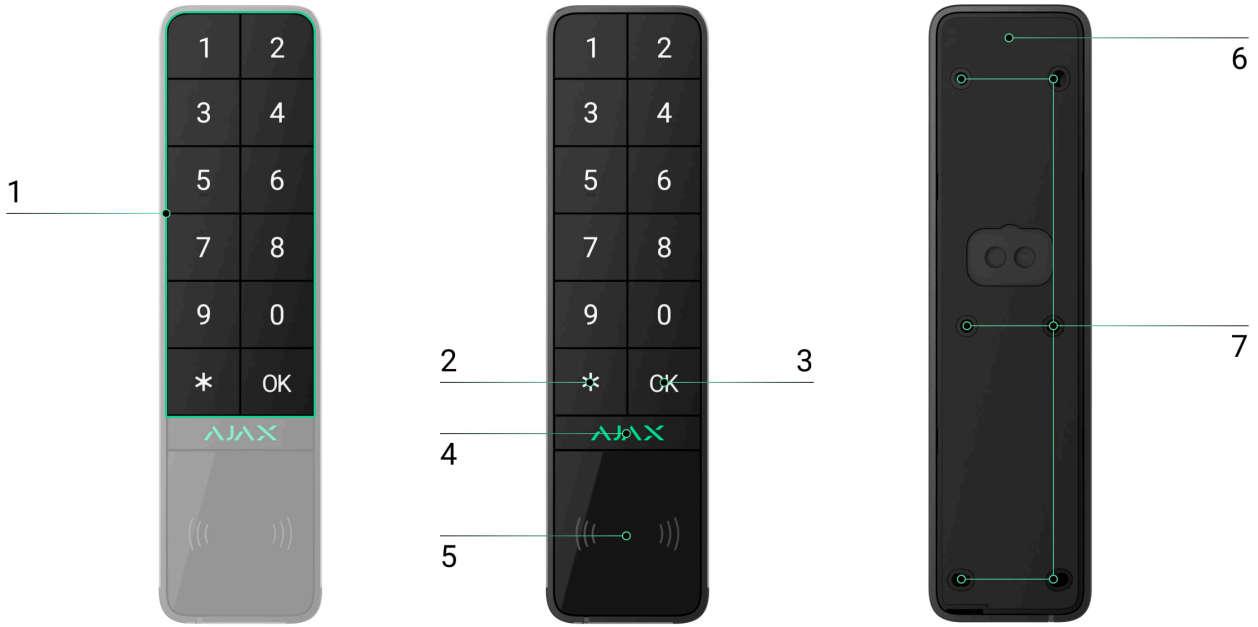
Updated September 19, 2025

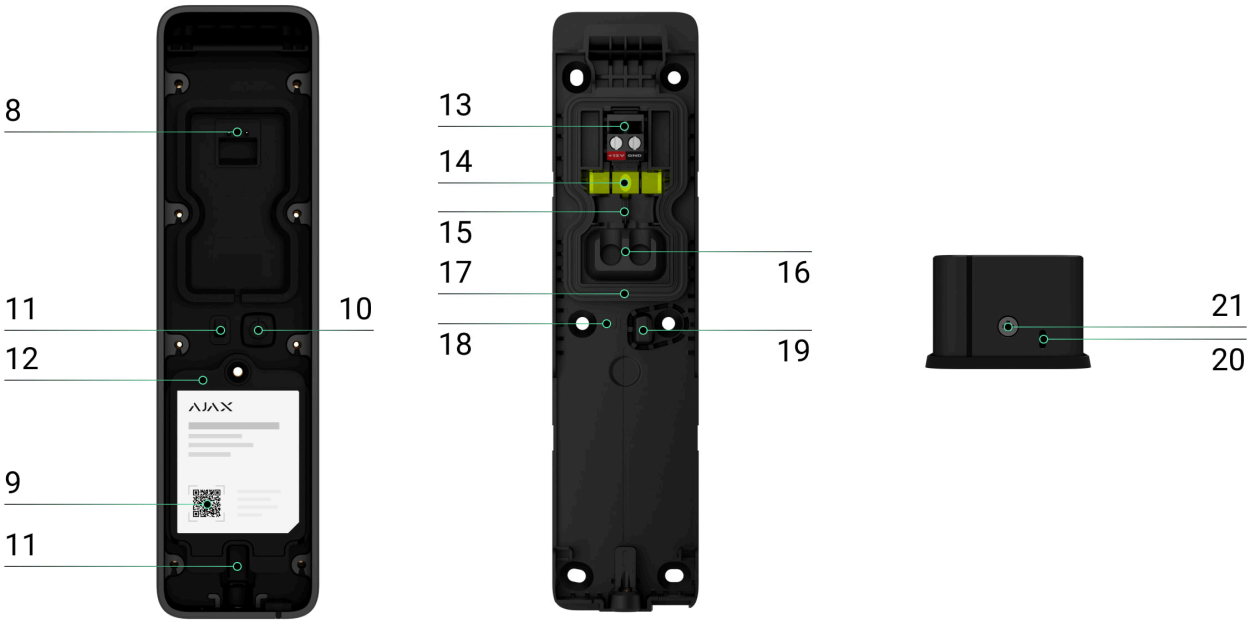
KeyPad Outdoor Jeweller is a wireless keypad designed to manage Ajax systems. Users can authenticate using smartphones, **Tag** key fobs, **Pass** cards, and codes. The device is intended for both outdoor and indoor use.

The keypad operates in the Ajax system and exchanges data with the hub using the secure Jeweller radio communication protocol.

Buy KeyPad Outdoor Jeweller

Functional elements





1. Numpad.
2. **Function** button.
3. **OK** button with an LED indicator.
4. Ajax logo with an LED indicator.
5. Card/key fob/Bluetooth reader.
6. SmartBracket mounting panel. To remove the panel, unscrew the holding screw.
7. Holes to attach SmartBracket to the surface.
8. Pins for connecting the device to the SmartBracket terminals.

9. QR code with the device ID. It is used to add the device to the hub.
10. Power button.
11. **Tamper buttons**.
12. Lid of the battery compartment.
13. Terminals for connecting an external power supply.
14. Bubble level to check the inclination angle of the mount during installation.
15. Tie slot to fix the cables.
16. Rubber sealing plug for routing cables from the back of the device.
17. Rectangular rubber sealing ring. Protects the device against water. Do not remove it.
18. **UP** key, which indicates the top of the keypad.
19. Perforated part of the mounting panel. Triggers a tamper alarm in case of any attempt to detach the device from the surface. Do not break it off.
20. Sound hole for the built-in buzzer.
21. Holding screw to secure the keypad on SmartBracket.

Compatible hubs

An Ajax hub with the firmware **OS Malevich 2.33** and later is required for the keypad to operate.

Check device compatibility

Operating principle

KeyPad Outdoor Jeweller features large mechanical buttons, a reader for contactless authorization, a built-in buzzer, and LED indicators. The keypad is used to control security modes and automation devices and to notify of system events via sound and LED indication.

KeyPad Outdoor Jeweller features **primary** and **secondary** operating modes. You can set up one keypad function for each mode and switch between modes with a long press of the **OK** button.

Learn more

The lower part of the keypad front side features a reader for contactless authorization so that you can present Tag, Pass, or a smartphone.

Depending on the settings, the KeyPad Outdoor Jeweller built-in buzzer notifies of the following:

- alarms;
- security mode changes;
- entry/exit delays;
- triggering of opening detectors;
- malfunctions.

Keypad operating modes and functions

KeyPad Outdoor Jeweller features two operating modes: **primary** and **secondary**. You can configure each mode independently in the keypad **settings** in Ajax apps. For each operating mode, you can set only one keypad function and switch between modes with a long press of the **OK** button on the keypad.

Also, you can disable the secondary operating mode if you do not need it.

There are three keypad functions that can be set up for each keypad operating mode:

- **Switch armed mode**. With this function, users can arm/disarm the entire site or specific groups or activate **Night mode**.
- **Manage automation devices**. With this function, users can create a scenario with one or multiple automation devices that can be controlled directly from the

keypad.

- Start entry delay. With this function, users can use KeyPad Outdoor Jeweller as a **bypass keypad** to activate an entry delay so they can disarm the site using the main keypad.

> Only one primary function and one secondary function can be set at once.

KeyPad Outdoor Jeweller shows which mode is currently active by LED indication depending on the configured function:

- **Switch armed mode** — the Ajax logo lights up red or green, depending on the system security state. The **OK** button lights up white, as do the number buttons.
- **Manage automation devices** — the **OK** button lights up red or green, depending on the automation device state. The Ajax logo LED is off. If the keypad controls a scenario with multiple automation devices, the scenario's state is unavailable on the keypad.
- **Start entry delay** — the Ajax logo lights up red when the site is armed and flashes red simultaneously with beep when the entry delay is started. The **OK** button lights up white, as do the number buttons.

Learn more

Security control

KeyPad Outdoor Jeweller can arm and disarm the entire site or specific groups and activate **Night mode**. Users can control the security using KeyPad Outdoor Jeweller through:

1. **Cards or key fobs**. To quickly and securely identify users, KeyPad Outdoor Jeweller uses the DESFire® technology. DESFire® is based on the ISO 14443 international standard and combines 128-bit encryption and copy protection. **Tag** and **Pass** support this technology and are compatible with KeyPad Outdoor Jeweller.
2. **Smartphones**. With the installed **Ajax Security System** app and Bluetooth Low Energy (BLE) support. Smartphones can be used instead of Tag or Pass for user authorization. BLE is a low-power consumption radio protocol. The keypad supports Android and iOS smartphones with BLE 4.2 and later.
3. **Codes**. KeyPad Outdoor Jeweller supports general codes, personal codes, and codes for unregistered users.

Access codes

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

Check device compatibility

Access rights and codes can be adjusted in Ajax apps. If the code is compromised, it can be changed remotely, so there is no need to call an installer to the site. If a user loses their Pass, Tag, or a smartphone, an admin or a PRO with system configuration rights can instantly block the device in the app. Meanwhile, a user can use a personal code to control the system.

Security control of the groups

KeyPad Outdoor Jeweller allows controlling the groups' security (if **Group mode** is enabled). An admin or PRO with the rights to configure the system can also adjust the keypad **settings** to determine which groups will be shared (keypad groups). You can learn more about group security management in **this section**.

Function button

KeyPad Outdoor Jeweller has the **Function** button (✳) that operates in one of three modes:

- **None** — the **Function** button is disabled, and nothing happens when the user presses this button shortly.
- **Panic** — after the **Function** button is pressed, the system sends an alarm to the security company monitoring station and all users.
- **Mute fire alarm** — after the **Function** button is pressed, the system mutes the alarm of Ajax fire detectors. Available only if an **Interconnected fire detectors alarm** feature is enabled (Hub → Settings ⚙ → Service → Fire detectors settings).

Also, incorrectly entered codes can be cleared with a long press of the **Function** button if no other action is set up for a long press.

Duress code

KeyPad Outdoor Jeweller supports a **duress code** that allows a user to simulate alarm deactivation. In this case, neither the **Ajax app** nor the **sirens** installed at the facility will reveal your actions. Still, the security company and other security system users will be alerted about the incident.

Learn more

Start entry delay (a bypass keypad)

The **Start entry delay** feature (i.e., a bypass keypad) is designed to activate an entry delay before the site is disarmed using the main keypad.

Bypass technology provides temporary deactivation of security detectors, such as **opening detectors** and others. This allows users to get more time from the moment they enter an area until they can disarm the site with the main control device (e.g., **KeyPad TouchScreen Jeweller**).

Learn more

Unauthorized access auto-lock

If an incorrect code is entered or a non-verified access device is used three times in a row within 1 minute, the keypad will lock for the time specified in its **settings**. During this time, the hub will ignore all codes and access devices while informing the security system users about attempted unauthorized access.

PRO or a user with system configuration rights can unlock the keypad through the app before the specified locking time expires.

Two-stage arming

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

Learn more

Automation devices and scenarios management

KeyPad Outdoor Jeweller has the **Manage automation devices** feature designed to control one or multiple automation devices. For example, a user can open garage doors or turn off all smart light switches at the site.

When the keypad controls one automation device, it shows the device's state with LED indication of the **OK** button. When the **OK** button is green, an automation device is active; when it is red, an automation device is inactive.

When the keypad controls a scenario with multiple automation devices, the keypad cannot show the state of the device or scenario. Instead, it indicates whether the set action is completed or not.

KeyPad Outdoor Jeweller can manage only one scenario.

Managing automation devices is available only after authorization on the keypad.

Indication of security mode and automation devices state

KeyPad Outdoor Jeweller informs users about system security mode and automation device state by means of:

- the logo with LED indication;
- the **OK** button with LED indication;
- sound indication.

If the keypad is in **Switch armed mode**, the Ajax logo lights up green or red to notify of the system's security mode state.

If the keypad is in the **Manage automation devices** mode, the **OK** button lights up green or red to notify of the automation device's state. But when the keypad manages a scenario with multiple automation devices, it cannot notify of the scenario's state.

The built-in buzzer notifies of alarms, door openings, and entry/exit delays.

Refer to the **Indication** section for more information.

Fire alarm muting

KeyPad Outdoor 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 the 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

Jeweller data transfer protocols

Jeweller is a wireless data transfer protocol that provides fast and reliable two-way communication between the hub and devices. The device uses **Jeweller** to transmit commands, alarms, and events.

Learn more

Sending events to the monitoring station

The Ajax system can transmit alarms to the **Ajax 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 Outdoor Jeweller can transmit the following events:

1. Arming/disarming the system.

2. Entry of the duress code.
3. Pressing the panic button.
4. Keypad locking due to an unauthorized access attempt.
5. Unsuccessful attempt to arm the security system (with the **system integrity check** enabled).
6. Tamper alarm. Tamper button recovery.
7. Loss and restoration of connection with the hub.
8. Permanent deactivation/activation of the device.
9. One-time deactivation/activation of the device.

When an alarm is received, the operator of the security company monitoring station knows what happened and precisely where to send a fast response team. The addressability of Ajax devices allows sending events to the **Ajax PRO Desktop** or the CMS the type of the device, its name, security group, and virtual room. The list of transmitted parameters may differ depending on the type of CMS and the selected communication protocol.

You can find the device ID and loop (zone) number in the device states.

Selecting the installation site

When choosing where to place KeyPad Outdoor Jeweller, consider the parameters that affect its operation:

- **Jeweller signal strength**

Consider the recommendations for placement when developing a project for the system of the facility. The Ajax system must be designed and installed by specialists. A list of recommended partners is **available here**.

KeyPad Outdoor Jeweller is best placed outdoors or indoors near the entrance. This allows users to disarm the site before entering the premises or until the entry delays expire. Users can also quickly arm the site when leaving the premises.

KeyPad Outdoor Jeweller has a protected enclosure, so the keypad can be installed in public places, such as restaurants, hospitals, offices, or at production plants in severe conditions.

The recommended installation height is 1.3–1.5 meters above the floor. Install the keypad on a flat, vertical surface. This ensures KeyPad Outdoor Jeweller is securely attached to the surface and helps avoid false tamper alarms.

At the installation site, the keypad should not be surrounded by two walls on both sides or obstructed by anything in front of it. A clear 30 cm zone in front of the keypad is required for proper card/key fob/Bluetooth reader operation.

Signal strength

The signal strength is determined by the number of undelivered or corrupted data packages over a certain period of time. The icon in the **Devices** tab in Ajax apps 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** — no signal.

> Check the Jeweller signal strength before final installation. With a signal strength of one or zero bars, we do not guarantee the device will operate stable. Consider relocating the device, as adjusting its position even by 20 cm can significantly improve the signal strength. If the signal remains poor or unstable after relocation, consider using a radio signal range extender.

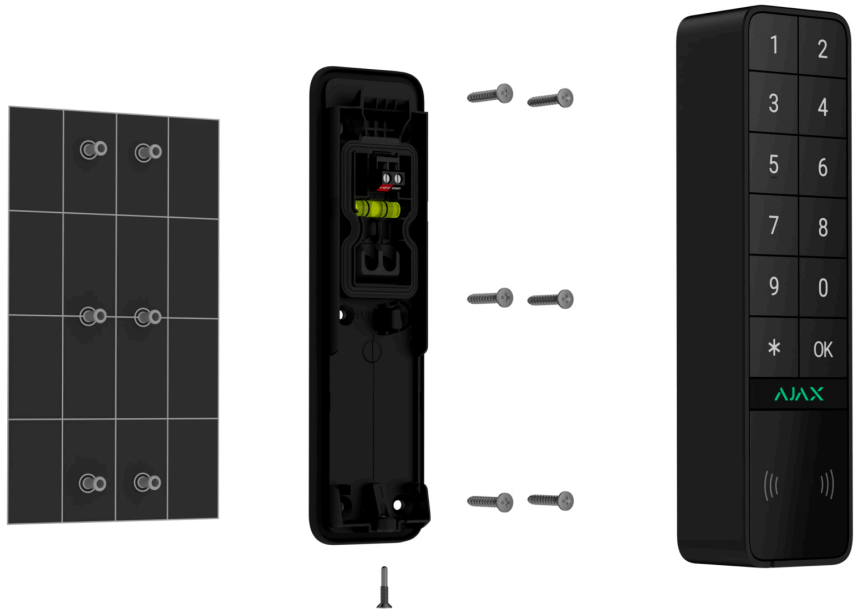
Refer to the **Functionality testing** section to learn how to run Jeweller signal strength test.

What is Jeweller signal strength test

Where not to install the keypad

1. In places where power or Ethernet cables, decor items, or other things may obstruct the keypad. A clear 30 cm zone in front of the keypad is required for proper card/key fob/Bluetooth reader operation.
2. In places with temperature and humidity outside the permissible limits. This could damage the device.
3. In places where the acoustic signal can be attenuated (inside furniture, behind thick curtains, etc.).
4. Near the glass break detectors. The built-in buzzer sound may trigger an alarm.
5. In places with low or unstable Jeweller signal strength.

Installation



Before installing KeyPad Outdoor Jeweller, ensure that you have chosen the optimal location that complies with the requirements of this manual.

To install the device:

1. Unscrew the holding screw at the bottom of the device and remove the SmartBracket mounting panel from the keypad.

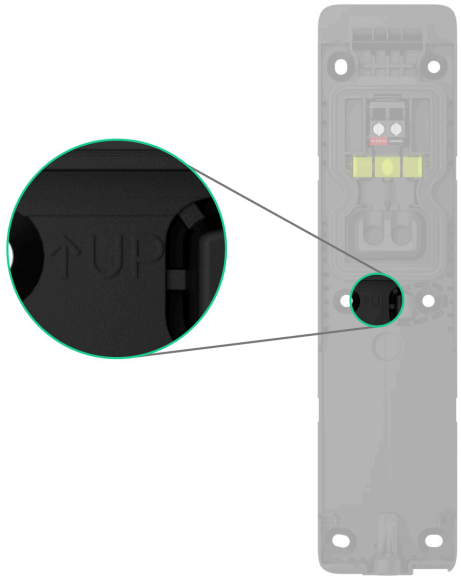
If you are going to connect the external power supply refer to the Connecting an external power supply section for more information.

2. Add the device to the system.

3. Temporarily secure the SmartBracket panel using double-sided adhesive tape or other temporary fasteners.

> Double-sided adhesive tape can only be used for temporary installation. The device attached by the tape may come unstuck from the surface at any time. As long as the device is taped, the tamper alarm will not be triggered when the device is detached from the surface.

SmartBracket has the **UP** key that indicates the top of the keypad. Consider it when installing the device.



4. Place the keypad on the SmartBracket mounting panel. The device LED indicator will flash. It is a signal indicating that the enclosure of the device is closed.

5. Run the **functionality testing**.

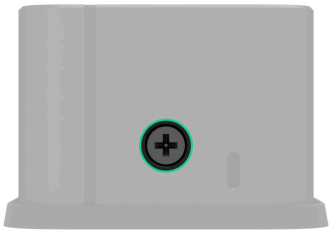
6. If the tests are passed successfully, remove the keypad from SmartBracket.

7. Fix the SmartBracket panel on the surface with bundled screws. Use all fixing points.

> When using other fasteners, ensure they do not damage or deform the panel.

8. Place the keypad on the SmartBracket mounting panel.

9. Tighten the holding screw on the bottom of the keypad's enclosure with a torque of **1—1.1 N·m**. The screw is needed for more reliable fastening and protection of the keypad from quick dismantling. Also, the screw has a tamper button that responds if someone tries to unscrew the holding screw. The system will send a notification of tamper alarm triggering to Ajax apps and the CMS.



Connecting an external power supply

When connecting an external power supply and using KeyPad Outdoor Jeweller follow the general electrical safety regulations for using electrical appliances, as well as the requirements of regulatory legal acts on electrical safety.

KeyPad Outdoor Jeweller is equipped with terminals for connecting a 10.5–14 V⎓ power supply.

When external power is connected, the pre-installed batteries serve as a backup power source. Do not remove them while connecting the power supply.

Use a cable that meets the following requirements to connect an external power supply:

- maximum cable length: **100 m**
- minimum wire cross-section area: **0.5 mm² (20 AWG)**
- conductor material: **copper**

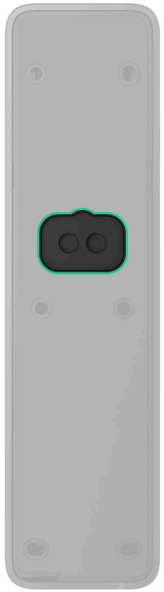
- maximum electrical resistivity (ρ): **0.02 Ω·mm²/m**

Using a cable that does not comply with these parameters may lead to unstable device operation or malfunction.

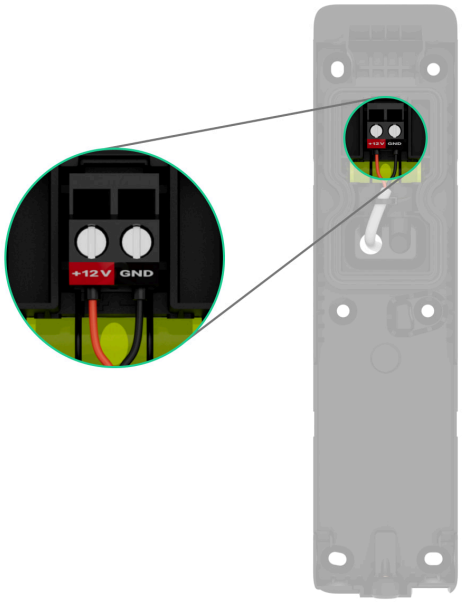
Before installing the device, check the wires for any damage to the insulation. Use only a grounded power source. Do not disassemble the device while it's under voltage. Do not use the device with a damaged power cable.

To connect an external power supply:

1. De-energize the external power supply cable.
2. Dismount the device if it has already been installed.
3. Make one or two holes in the rubber sealing plug in the recesses, considering the number of cables.



4. Run the cable into the keypad enclosure through the hole that was made.
5. Connect the wires to the terminals according to the figure below. Ensure the correct polarity and order of the wire connections. Firmly secure the cable to the terminals.



6. Install the keypad on the surface according to **steps 3–9** described in the **Installation** section.
7. Switch on the external power.

Once the external power supply is connected, the **External power** parameter in the device **states** changes its status to **Connected**.

Adding to the system

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 app**.
2. Log in to your **account** or create a new one.
3. Select a **space** or create a new one.
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. Check the states in the Ajax app to ensure the space is disarmed and the hub is not starting an update.

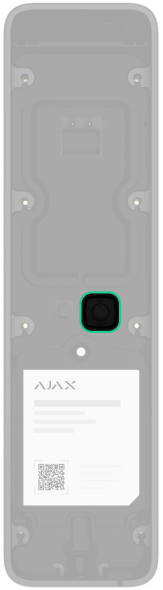
Only a PRO or a space admin with the rights to configure the system can add a device to the hub.

Types of accounts and their rights

Adding to the hub

1. Open an **Ajax app**. Select a **space** to which you want to add the device.
2. Go to the **Devices** tab and tap **Add device**.
3. Assign a name to the device.
4. Scan the QR code or enter the device ID manually. A QR code with ID is placed on the device enclosure. Also, it is duplicated on the device packaging.
5. Select a virtual room and a security group (if **Group mode** is enabled).
6. Tap **Add**, and the countdown will begin.

7. Switch on the device by holding the power button for 3 seconds.



If the connection fails, try again in 5 seconds. If the maximum number of devices has already been added to the hub, you will receive an error notification when you try to add more.

KeyPad Outdoor Jeweller features a built-in buzzer that can notify of alarms and specific system states, but it is not a siren. You can add up to 50 keypads with a built-in buzzer to the hub. Consider this when planning your security system.

Once added to the hub, the device will appear in the list of hub devices in the Ajax app. The update frequency for device statuses in the list depends on the **Jeweller** or **Jeweller/Fibra** settings and is 36 seconds by default.

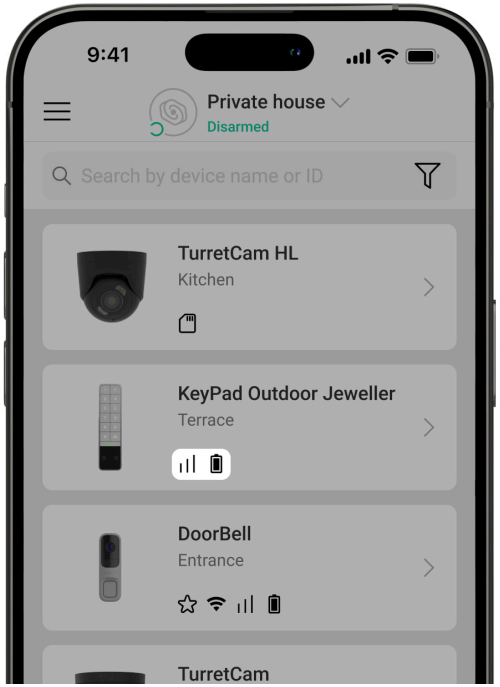
> KeyPad Outdoor Jeweller works with only one hub. When paired with a new hub, it stops sending events to the old one. Adding the keypad to a new hub does not automatically remove it from the device list of the old hub. This must be done through the Ajax app.

Functionality testing

An Ajax system provides several types of tests to help select the correct installation place for the devices. For KeyPad Outdoor Jeweller, the following tests are available:

- **Jeweller signal strength test** — to determine the signal strength and stability between the hub (or the radio signal range extender) and the device via the wireless Jeweller data transfer protocol at the device installation site.
- **Signal attenuation test** — to decrease or increase the power of the radio transmitter; to check the stability of communication between the device and the hub, the changing environment at the site is simulated.

Icons



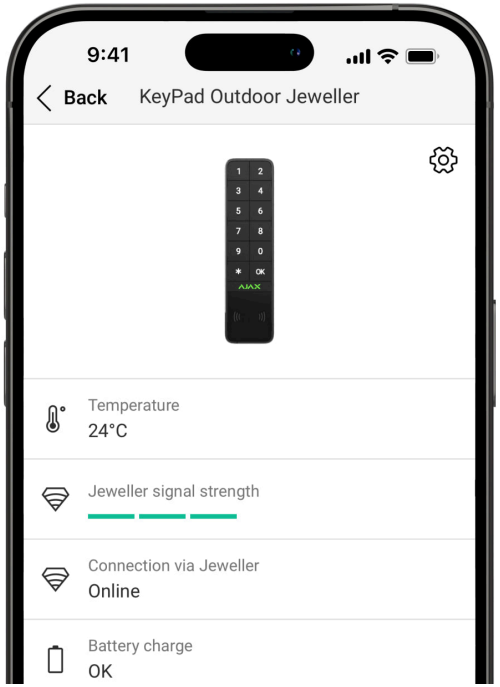
Icons in the Ajax app display some of KeyPad Outdoor Jeweller states. Icons can be checked in the **Devices** tab.

Icon	Meaning

	Jeweller signal strength. It displays the signal strength between the hub and the device. The recommended value is 2–3 bars. **Learn more**
	Battery charge level of the device. **Learn more**
	The device operates through the radio signal range extender. **Learn more**
	**Pass/Tag reading** is enabled in keypad settings.
	**Bluetooth** is enabled in keypad settings.
	Bluetooth setup is not complete. The description is available in the keypad states.
	**Chime on opening** is enabled in keypad settings.
	The device is in the signal attenuation test mode. **Learn more**
	The mounting panel is unlocked.

	The device is permanently deactivated. **Learn more**
	Tamper alarm notifications are permanently deactivated. **Learn more**
	The device is deactivated until until the first disarming of the system. **Learn more**
	Tamper alarm notifications are deactivated until the site is disarmed for the first time. **Learn more**
Offline	The device has lost connection with the hub or the hub has lost connection with the Ajax Cloud server.
Not transferred	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 Outdoor Jeweller can be found in Ajax apps:

1. Go to the **Devices** tab.
2. Select **KeyPad Outdoor Jeweller** in the list.

Parameter	Meaning
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	Tapping on ⓘ opens the list of device malfunctions. The field is displayed only if a malfunction is detected.
Warning ⚠	Tapping on ⓘ opens the list of the settings and permissions that the app needs to be granted for the correct operation of the keypad.
Temperature	Device temperature. It is measured by the processor and changes depending on the ambient temperature. You can create a scenario by temperature to control automation devices. **Learn more**
Jeweller signal strength	Jeweller signal strength between the device and the hub (or the radio signal range extender). The recommended value is 2–3 bars. Jeweller is a protocol for transmitting events and alarms.

Connection via Jeweller	Connection status via Jeweller channel between the device and the hub (or the range extender): • **Online** — the device is connected to the hub (or the range extender). Normal state. • **Offline** — the device is not connected to the hub (or the range extender). Check the device connection.
Battery charge	The battery charge level of the device. Two states are available: • **OK**. • **Battery low**. When the batteries need to be replaced, users and the security company will receive appropriate notifications. Learn more
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

<Range extender name>	Status of device connection to the **radio signal range extender**. • **Online** — the device is connected to the range extender. • **Offline** — the device is not connected to the range extender. The field is displayed if the device operates via the radio signal range extender.
Lid	The status of the device tamper button that responds to detachment or opening of the device enclosure: • **Open** — the device is removed from the SmartBracket mounting panel, or its integrity is compromised. Check the mounting of the device. • **Closed** — the device is installed on the SmartBracket mounting panel. The integrity of the device enclosure and the mounting panel is not compromised. Normal state. **Learn more**
Mounting panel	The status of the device tamper button that responds to unlocking the SmartBracket mounting panel:

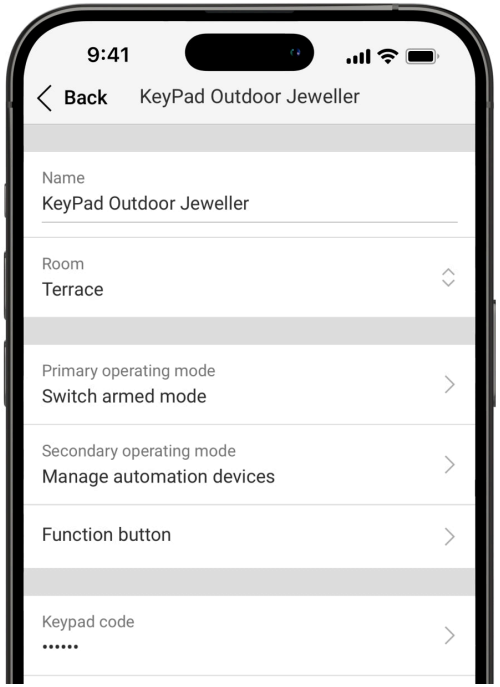
	• **Unlocked** — the holding screw for SmartBracket is unscrewed, or its integrity is compromised. Check the holding screw and mounting of the device. • **Locked** — the holding screw for SmartBracket is screwed. The integrity of the device enclosure and the mounting panel is not compromised. Normal state. Learn more
External power	External power state: • **Connected** — the external power is connected to the detector. • **Disconnected** — the external power is disconnected or not connected.
Alarms sound Indication	Shows the status of the **Activate keypad buzzer if an alarm in the system is detected** setting.
Alarm duration	Duration of sound signal in case of alarm. Sets in increments of 3 seconds. Displayed when the **Activate keypad buzzer if alarm in the system is detected** toggle is enabled.

Pass/Tag reading	Displays if the reader for cards and key fobs is enabled.
Bluetooth	Displays if the keypad's Bluetooth module is enabled for controlling the system with a smartphone.
Beeps settings	
Arming/disarming	When enabled, the keypad notifies about arming and disarming with a short beep.
Night mode activation/deactivation	When enabled, the keypad notifies users when the **Night mode** is switched on/off by making a short beep.
Entry delays	When enabled, the keypad beeps about **Entry delays**.
Exit delays	When enabled, the keypad beeps about **Exit delays**.
Entry delays in Night mode	When enabled, the keypad beeps about **Entry delays** in **Night mode**.
Exit delays in Night mode	When enabled, the keypad beeps about **Exit delays** in **Night mode**.
Chime on opening	When enabled, the keypad notifies about opening detectors triggering in the **Disarmed** system mode.

	Learn more
Beep volume	Displayed if the notifications about arming/disarming, entry/exit delay, and opening are activated. Shows the buzzer volume level for notifications.
Permanent deactivation	The status of the device's permanent deactivation setting: • **No** — the device operates in the normal mode and transmits all events. • **Entirely** — the device is completely excluded from the system operation by the hub admin. The device does not execute system commands and does not report alarms or other events. • **Lid only** — the hub admin has disabled notifications about tamper alarm triggering. **Learn more**
One-time deactivation	Shows the status of the device's one-time deactivation setting: • **No** — the device operates in the 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 alarm 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.	Device number. This number is transmitted to the CMS in case of an alarm or event.

Settings



To change KeyPad Outdoor Jeweller settings in the Ajax apps:

1. Go to the **Devices** tab.
2. Select **KeyPad Outdoor Jeweller** in the list.
3. Go to **Settings**.
4. Set the required settings.
5. Tap **Back** to save the new settings.

Settings	Meaning

Name	Device name. Displayed in the list of hub devices, text of SMS and notifications in the events feed. To change the device name, tap on the text field. The name can contain up to 24 Latin characters or up to 12 Cyrillic characters.
Room	Selecting the virtual room to which KeyPad Outdoor Jeweller is assigned. The room name is displayed in the text of SMS and notifications in the events feed.
Primary operating mode	Opens menu with **Primary operating mode** settings.
Secondary operating mode	Opens menu with **Secondary operating mode** settings.
Function button	Selecting the function of the button ✳ (**Function** button): • **None** — 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 all users. • **Mute fire alarm** — when pressed, the system mutes the alarm of Ajax fire detectors.

	Available only if the **Interconnected fire detectors alarm** feature is enabled. **Learn more**
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**
Unauthorized access auto-lock	When enabled, the keypad will be locked for a pre-set time if an incorrect code is entered or unverified access devices are used more than three times in a row within 1 minute. PRO or a user with the rights to configure the system can unlock the keypad through the app before the specified locking time expires.
Auto-lock time	Selecting the keypad lock period after unauthorized access attempts: • 3 minutes • 5 minutes • 10 minutes

	• 20 minutes • 30 minutes • 60 minutes • 90 minutes • 180 minutes Available if the **Unauthorized access auto-lock** toggle is enabled.
Pass/tag reading	When enabled, the security mode can be controlled with **Pass** and **Tag** access devices.
Bluetooth	When enabled, the security mode can be controlled with a smartphone.

Bluetooth sensitivity	Adjusting the sensitivity of the keypad's Bluetooth module: • Minimum • Low • Normal (by default) • High • Max Available if the **Bluetooth** toggle is enabled.
Backlight and indication	Opens menu with **Backlight and indication** settings.
Sound indication	Opens menu with **Sound indication** settings.
Jeweller signal strength test	Switches the device to the Jeweller signal strength test mode. The test allows you to check the signal strength between the hub (or the radio signal range extender) and the device via the wireless Jeweller data transfer protocol to select the optimal installation site. **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 the KeyPad Outdoor Jeweller user manual in the Ajax app.

Permanent deactivation	Allows the user to disable events of 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 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 ignore notifications about the triggering of the device tamper alarm only. 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 and transmits all events. • **Entirely** — the device 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.

	• **Lid only** — notifications on the tamper alarm triggering are disabled until the first disarm. Learn more
Delete device	Unpairs the device, disconnects it from the hub, and deletes its settings.

Primary and secondary operating modes

KeyPad Outdoor Jeweller features two operating modes: **primary** and **secondary**. There are three keypad functions that can be configured for each operating mode: **Switch armed mode**, **Manage automation devices**, or **Start entry delay**.

Only one primary keypad function and one secondary keypad function can be set at once. To switch between functions, press and hold the **OK** button on the keypad.

Parameter	Meaning
Primary operating mode	
Keypad function	Selecting the keypad function for the primary operating mode: • Switch armed mode

	• Manage automation devices • Start entry delay Only one primary function and one secondary function can be set at once.
Secondary operating mode	
Keypad function	Selecting the keypad function for the secondary operating mode: • None • Switch armed mode • Manage automation devices • Start entry delay Only one primary function and one secondary function can be set at once.
Switch armed mode	
Security objects	Selecting the security sites controlled by the device. You can select the entire space, all or particular groups, or **Night mode**.

	Selecting groups is available if **Group mode** is enabled.
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**.
Pre-authorization	When enabled, the user should be authenticated to use the keypad: enter a code or present a personal access device to the keypad.
Authorization confirmation with a passcode	When enabled, users are permitted to arm or disarm the system only when they have been successfully authorized with two forms of identification, i.e., by using Pass, Tag, or a smartphone and entering the appropriate passcode. **Learn more**
Easy armed mode change	When enabled, users do not need to press the **OK** button after a passcode is entered or an access

	device is read.
Arming without code	When enabled, the user can arm the site without entering a code or presenting the personal access device. If disabled, enter a code or present the access device to arm the system. Available if the **Pre-authorization** toggle is disabled.
Auto-switch to secondary mode	Available only for **Secondary operating mode**. With this option, the user can set when the keypad automatically starts to operate in secondary mode without a long press of the **OK** button: • Off. • When system is disarmed. • When system is armed.
Manage automation devices	

Automation scenarios	Creates and configures a scenario to manage automation devices with a keypad. You can create a scenario **on preset action** or **on switching the state** of one or multiple automation devices. The keypad can manage only one scenario.
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**.
Pre-authorization	When enabled, the user should be authenticated to use the keypad: enter a code or present a personal access device to the keypad.
Easy assigned device switch	When enabled, users do not need to press the **OK** button after a passcode is entered or an access device is read.
Restrict device management	With this option, the user can set when the control of the automation device using the keypad should be blocked:

	• Off. • When system is disarmed. • When system is armed.
Auto-switch to secondary mode	Available only for **Secondary operating mode**. With this option, the user can set when the keypad automatically starts to operate in secondary mode without a long press of the **OK** button: • Off. • When system is disarmed. • When system is armed.
Start entry delay	

Delay when entering	Selecting entry delay time: 5 to 255 seconds. Entry delay (alarm activation delay) is the time the user has to disarm the site using the main keypad.
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**.
Authorization confirmation with a passcode	When enabled, users are permitted to arm or disarm the system only when they have been successfully authorized with two forms of identification, i.e., by using Pass, Tag, or a smartphone and entering the appropriate passcode. Learn more
Easy delay start	When enabled, users do not need to press the **OK** button after a passcode is entered or an access device is read.

Auto-switch to secondary mode	Available only for **Secondary operating mode**. With this option, the user can set when the keypad automatically starts to operate in secondary mode without long pressing the **OK** button: • Off. • When system is disarmed. • When system is armed.

Backlight and indication

Settings	Meaning
Brightness	Adjusting the keypad backlight brightness level.
Always-active backlight	When enabled, the keypad backlight always remains active.
Armed mode indication	With this option, the user can set when it is required to show the system security state on the

	keypad: • **Never** — no security state LED indication. • **Only when armed** — the logo is red when the site is armed, partially armed, or in **Night mode**. • **Always** — the logo is red when the site is armed, green when disarmed, and yellow when arming is incomplete.

Sound indication

KeyPad Outdoor Jeweller has a built-in buzzer that, depending on the settings, can notify of the following:

1. Alarms.
2. **Entry/Exit delays**.
3. Chimes on opening.
4. Commands execution (e.g., arming, disarming).
5. Pressing the keypad buttons.

We do not recommend using KeyPad Outdoor Jeweller instead of the siren. The keypad's buzzer is meant for additional notifications only. Ajax sirens are designed to deter intruders and draw attention. A properly installed siren is more difficult to dismantle due to its elevated mounting position compared to a keypad at eye level.

Parameter	Meaning
Beeps settings	Opens the **Beeps settings** menu.
Beep on armed mode change	
Arming/disarming	**When enabled**: an audible notification is sent if the security mode is changed from the keypad, another device, or the app. **When disabled**: an audible notification is sent if the security mode is changed from the keypad only. The volume of the beep depends on the configured buttons' volume.
Night mode activation/deactivation	**When enabled**: an audible notification is sent if the **Night mode** is activated/deactivated from the keypad, another device, or the app. **When disabled**: an audible notification is sent if the **Night mode** is activated/deactivated from the keypad only.

	Learn more The volume of the beep depends on the configured buttons' volume.
Beep on delays	
Entry delays	When enabled, the built-in buzzer beeps about an Entry delay. **Learn more**
Exit delays	When enabled, the built-in buzzer beeps about an Exit delay. **Learn more**
Entry delays in Night mode	When enabled, the built-in buzzer beeps about an Entry delay in the **Night mode**. **Learn more**
Exit delays in Night mode	When enabled, the built-in buzzer beeps about an Exit delay in the **Night mode**. **Learn more**

Fast beep on delays	
Fast beep on Entry delay expiration	Notifies the user that the **Entry delay** time is running out. You can choose one of four options for when the fast beep should start: • Never • Last 5 seconds • Last 10 seconds • Last 15 seconds The option is available when **Beep on entry delays** is enabled.

Fast beep on Exit delay expiration	Notifies the user that the **Exit delay** time is running out. You can choose one of four options for when the fast beep should start: • Never • Last 5 seconds • Last 10 seconds • Last 15 seconds The option is available when **Beep on exit delays** is enabled.
Beep when disarmed	
Chime on opening	When enabled, the built-in buzzer informs users with a short beep that the opening detectors are triggered in the **Disarmed** system mode. Learn more
Beep volume	Selecting the built-in buzzer volume level for notifications about arming/disarming, entry/exit delay, and opening: • **Quiet**. • **Loud**.

	• **Very loud**.
Buttons	
Volume	Adjusting the buzzer notification volume for interactions with the keypad.
Alarms reaction	
Audible alarm	Setting the mode when the built-in buzzer enables an alarm: • **Always** — an audible alarm will be activated regardless of the system security mode. • **Only when armed** — an audible alarm will be activated if the system or the group a keypad is assigned to is armed.
Activate keypad buzzer if alarm in the system is detected	When enabled, the built-in buzzer notifies an alarm in the system.

Alarms in Group mode	Selecting the group (from the shared) which alarm the keypad will notify of. The **All shared groups** option is set by default. If the keypad has only one shared group and it is deleted, the setting will return to its initial value. Displayed if the **Group mode** is enabled.
Alarm duration	Duration of sound signal in case of alarm: from 3 seconds to 3 minutes.

Adjust the entry/exit delays in the appropriate detectors settings, not the keypad settings.

Learn more

Keypad response to device alarms

KeyPad Outdoor Jeweller can respond to alarms from each device in the system with a built-in buzzer. The function is useful when users do not need to activate the buzzer for the alarm of a specific device. For example, this can be applied to the triggering of the **LeaksProtect Jeweller** leakage detector.

By default, the keypad response is enabled for alarms of all devices in the system.

To set the keypad response to a device alarm:

1. Open the Ajax app.
2. Go to the **Devices** tab.
3. Select the device for which you want to configure the keypad response from the list.
4. Go to **Settings**.
5. Find the **Alert with a siren** option and select the toggles which will activate it. Enable or disable the function.
6. Repeat steps 3–5 for the rest of the system devices.

Keypad response to tamper alarms

KeyPad Outdoor Jeweller can respond to enclosure alarms from each system device with a built-in buzzer. When the function is activated, the keypad built-in buzzer will emit a sound signal upon triggering the **tamper button** of the device.

To set the keypad response to a tamper alarm:

1. Open the Ajax app.
2. Go to the **Devices** tab.
3. Select the hub and go to its **Settings**.
4. Select the **Service** menu.
5. Go to the section **Sounds and Alerts**.
6. Enable the **If lid of hub or any detector is open** toggle.
7. Tap **Back** to save the new settings.

Tamper button reacts to opening and closing of the enclosure, regardless of the armed mode of the device or system.

Keypad response to pressing the panic button in the Ajax apps

An admin or PRO with rights to configure the system can set up the keypad response to the alarm when the panic button is pressed in Ajax apps. To do this, follow these steps:

1. Open the Ajax app.
2. Go to the **Devices** tab.

3. Select the hub and go to its **Settings** .

4. Select the **Service** menu.

5. Go to the section **Sounds and Alerts**.

6. Enable the **If in-app panic button is pressed** toggle.

7. Tap **Back** to save the new settings.

Keypad after-alarm indication

0:00 / 0:03

The keypad can inform about triggering in the armed system through LED indication.

The option functions as follows:

1. The system registers the alarm.
2. The keypad plays an alarm signal (if enabled). The duration and volume of the signal depend on the **device settings**.
3. The keypad's LED flashes twice (once every 3 seconds) until the system is disarmed.

Thanks to this feature, system users and security company patrols can understand that the alarm has occurred.

> The KeyPad Outdoor Jeweller after-alarm indication does not work for always active detectors, if the detector was triggered when the system was disarmed.

To enable the KeyPad Outdoor Jeweller after-alarm indication, in the Ajax PRO app:

1. Go to hub settings:
   - Hub → Settings → Service → LED Indication.
2. Specify which events KeyPad Outdoor Jeweller will inform about by double flashing of the LED indicator before the system is disarmed:

- Confirmed intrusion/hold-up alarm.
- Single intrusion/hold-up alarm.
- Lid opening.

3. Select the required KeyPad Outdoor Jeweller in the **Devices** menu. Tap **Back** to save the parameters.
4. Tap **Back**. All values will be applied.

Chime on opening

If **Chime on opening** is enabled, KeyPad Outdoor Jeweller notify a user with a short beep if the opening detectors are triggered when the system is disarmed. The feature is used, for example, in stores to notify employees that someone has entered the building.

Notifications are configured in two stages: setting up the keypad and setting up opening detectors. **This article** provides more information about **Chime** and how to set up detectors.

To set the keypad response:

1. Open the Ajax app.
2. Go to the **Devices** tab.

3. Select KeyPad Outdoor Jeweller and go to its **Settings** ⚙.
4. Go to the **Sound indication** menu → **Beeps settings**.
5. Enable the **Chime on opening** toggle in the **Beep when disarmed** category.
6. Set the required notifications volume.
7. Tap **Back** to save the settings.

If the settings are made correctly, a bell icon appears in the **Control** + tab of the Ajax app. Tap it to activate or deactivate chime.

Codes setting

In Ajax PRO apps, within the hub settings, you can set the requirements for the length of passcodes used for user authorization and access to the system. You can select the **Flexible (4 to 6 symbols)** option or define the fixed code length: **4 symbols**, **5 symbols**, or **6 symbols**.

Setting a fixed code length will reset all previously configured access codes.

The fixed code length is required for the **Easy armed mode change** feature, which allows disarming the system without pressing the **OK** button on the keypad after entering a passcode or using an access device.

Keypad access codes

To set keypad and keypad duress codes:

1. In the Ajax app, go to the **Devices** tab.
2. Select the keypad for which you want to set up an access code.
3. Go to its **Settings**.
4. Select **Keypad codes only** or **Keypad and user codes** option in the **Access settings** menu.
5. Go to the **Keypad code** menu.
6. Set the keypad code. Contains from 4 to 6 digits.
7. Tap **Done**.
8. Go to the **Duress code** menu.
9. Set the keypad duress code. Contains from 4 to 6 digits.
10. Tap **Done**.

User access codes

To set a personal code and a personal duress code:

1. Select the space in the Ajax app.
2. Go to the **Settings** menu.
3. Open the **Users** menu.
4. Find your account in the list and tap on it.
5. Go to the **Passcode settings** menu.
6. Set the **User code**. Contains from 4 to 6 digits.
7. Tap **Save**.
8. Set the **Duress code**. Contains from 4 to 6 digits.
9. Tap **Save**.
10. Tap **Back** to save the settings.

Unregistered user codes

To set an access code for a user without an account:

1. Select the hub in the Ajax app.
2. Go to the **Settings** menu.
3. Go to the **Keypad access codes** menu.

4. Tap **Add code**. Set up **Name** and **Access code**. Contains from 4 to 6 digits.
5. Tap **Add** to save the data.

To set a duress code for a user without an account:

1. Select **Keypad access codes** menu in the hub settings.
2. Select the required unregistered user.
3. Tap **Add duress code**. Set the code. Contains from 4 to 6 digits.
4. Tap **Done**.

For unregistered users, an admin or PRO with the rights to configure the system can adjust the access to security management. First, enable Group mode. Then, select the **Keypad access codes** menu in the hub settings, find the required user, and set the appropriate parameters in the **Security management** menu.

RRU code

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

Cards and key fobs

KeyPad Outdoor Jeweller can work with **Tag** key fobs, **Pass** cards, and third-party devices that support 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.
>
> This article provides information on how to reset **Tag** or **Pass**.

The maximum number of added Pass and Tag devices depends on the hub model. The added Pass and Tag devices do not affect the total device limit on the hub.

Check device compatibility

Adding Tag or Pass

1. Open the Ajax app.
2. Select the space with hub to which you want to add Tag or Pass.
3. Go to the **Devices** tab.

Make sure the **Pass/Tag reading** feature is enabled in at least one keypad setting.

4. Click **Add device**.
5. Select **Add pass/tag**.
6. Specify the type (Tag or Pass), color, device name, and user (if necessary).
7. Tap **Next**. After that, the hub will switch to the device registration mode.
8. Go to any compatible keypad with **Pass/Tag reading** enabled. Press the **OK** button to switch keypad to the access device logging mode.
9. Present Pass or Tag with the wide side to the keypad for a few seconds. Upon successful addition, you will receive a notification in the Ajax app.

If the connection fails, try again in 5 seconds. Please note that if the maximum number of Tag or Pass devices has already been added to the hub, you will receive a corresponding notification in the Ajax app when adding a new device.

Both Tag and Pass can work with several hubs at the same time. The maximum number of hubs is 13. If you try to add Tag or Pass to a hub that has already reached the device limit, you will receive a corresponding notification. To add such a key fob/card to a new hub, you will need to reset it.

If you need to add another Tag or Pass, tap **Add another pass/tag** in the app. Repeat steps 6–9.

Deleting (resetting) Tag or Pass

Resetting will delete all settings and linkages of key fobs and cards. In this case, the reset Tag and Pass are only removed from the hub from which the reset was made. On other hubs, Tag or Pass are still displayed in the app but cannot be used to manage the security modes. These devices should be removed manually.

1. Open the Ajax app.
2. Select the space.
3. Go to the **Devices** tab.
4. Select a compatible keypad from the device list.

Make sure the **Pass/Tag reading** feature is enabled in the keypad settings.

5. Go to the keypad settings by clicking the icon.

6. Tap **Pass/Tag reset**.
7. Tap **Continue**.
8. Go to any compatible keypad with **Pass/Tag reading** enabled. Press the **OK** button to switch the keypad to the access device resetting mode.
9. Present Pass or Tag with the wide side to the keypad for a few seconds. Upon successful formatting, you will receive a notification in the Ajax app. If the formatting fails, try again.

If you need to reset another Tag or Pass, tap **Reset another Pass/Tag** in the app. Repeat step 9.

Bluetooth setting

KeyPad Outdoor Jeweller supports security modes control by bringing a smartphone to the sensor. Security management is established through a Bluetooth communication channel. This method is convenient, secure, and fast, as there is no need to enter a password, add a phone to the keypad, or use Tag or Pass that could be lost.

Bluetooth authentication is available only for Ajax Security System users.

To enable Bluetooth authentication in the app

1. Add KeyPad Outdoor Jeweller to the system.
2. Enable the keypad Bluetooth sensor:
   - **Devices** → **KeyPad Outdoor Jeweller** → **Settings** → Enable the **Bluetooth** toggle.
3. Tap **Back** to save the settings.

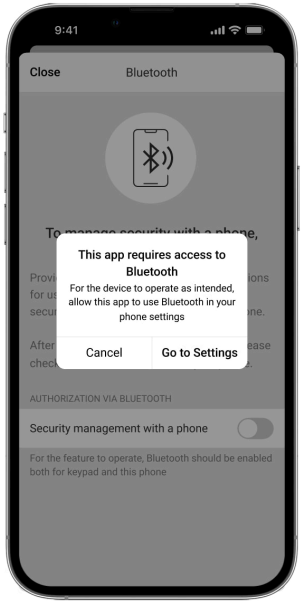
To set up Bluetooth authentication

1. Open the Ajax Security System app and select the space to which the KeyPad Outdoor Jeweller with enabled Bluetooth authentication is added. By default, authentication with Bluetooth is available for all users of such system.

> To prohibit Bluetooth authentication for certain users:
>
> 1. In the **Devices** tab select the hub and go to its settings .
> 2. Open **Users menu** and the required user from the list.
> 3. In the **Permissions** section, disable the **Security management via Bluetooth** toggle.

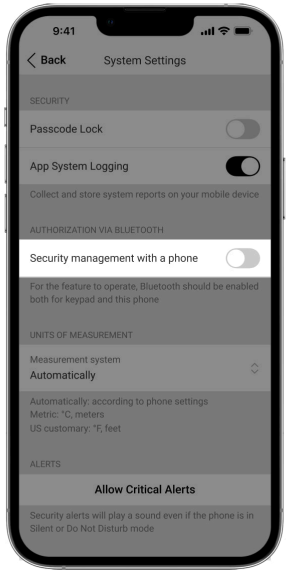
2. Allow the Ajax Security System app to use Bluetooth if it was not previously granted. In this case, the warning ⚠ appears at KeyPad Outdoor Jeweller **States**. Pressing the symbol ⓘ opens the window with explanations of what to do. Enable the Security management with a phone toggle at the bottom of the opened window.

Grant the app permission to find and connect to nearby devices. The popup window for Android and iOS smartphones can differ.



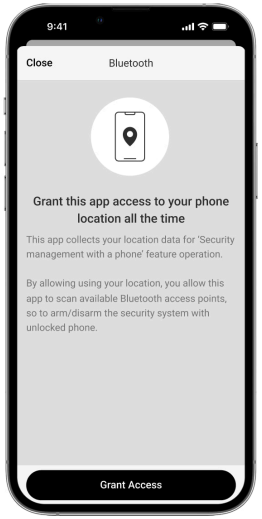
Also, the **Security management with a phone** toggle can be enabled in the app settings:

- Tap the ☰ icon in the upper left corner of the screen and select the **App settings** menu.
- Open the **System settings** menu and enable **Security management with a phone** toggle.



3. We recommend configuring **Geofence** for the stable performance of Bluetooth authentication. The warning ⚠ appears at KeyPad Outdoor Jeweller **States** if **Geofence** is disabled and the app is not allowed to use the smartphone location. Tapping the ⓘ symbol opens the window with explanations of what to do.

> Bluetooth authentication can be unstable if **Geofence** function is disabled. Users will need to launch and minimize the app if the system switches it to sleep mode.



Users can control the system faster via Bluetooth, when the **Geofence** function is activated and configured. All that is needed is to unlock the phone and present it to the keypad sensor.

How to set up Geofence

4. Enable the **Keep app alive to manage security via Bluetooth** toggle. For this, go to **Devices** → **Hub** → **Settings** → **Geofence**.
5. Ensure that Bluetooth is enabled on your smartphone. If it is disabled, the warning ⚠ appears in the keypad **States**. Pressing the ⓘ symbol opens the window with explanations of what to do.
6. Enable the **Keep-Alive Service** toggle in the app settings for Android smartphones. For this, in the upper left corner of the screen, click the ☰ → **App**

settings → System settings.

Controlling security

Using codes, Tag/Pass, or a smartphone, you can control the **Night mode** and the security of the entire site or separate groups. The user or PRO with the rights to configure the system can set up access codes. **This chapter** provides information on how to add Tag or Pass to the hub. To control with a smartphone, adjust the appropriate **Bluetooth parameters** in the keypad settings. Turn on the smartphone Bluetooth, location, and unlock the screen.

If a personal or access code, Tag/Pass, or a smartphone is used, the name of the user who changed the security mode is displayed in the hub event feed and in the notifications list. If a general code is used, the name of the keypad from which the security mode was changed is displayed.

KeyPad Outdoor Jeweller is locked for the time specified in the settings if an incorrect code is entered or an unverified access device is presented 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 the rights to configure the system can unlock KeyPad Outdoor Jeweller in the Ajax app.

The step sequence for changing the security mode with the keypad depends on whether **Pre-authorization**, **Authorization confirmation with a passcode**, and **Easy**

armed mode change options are enabled in the KeyPad Outdoor Jeweller settings.

Using Tag, Pass, or a smartphone

1. Present Tag, Pass, or a smartphone to the keypad.
2. Enter the required code if the **Authorization confirmation with a passcode** feature is activated.
3. Press the **OK** button on the keypad to change the armed mode.

If the **Easy armed mode change** option is enabled, you do not need to press the **OK** button after the access device is read.

Using passcodes

> Incorrectly entered codes can be cleared with a long press of the button if no other action is set up for a long press.

Code	Example	Note
Managing the site armed modes		

Keypad code Keypad duress code	1234 → OK	
User code User duress code	5 → ✳ → 1234 → OK	**5** is a user ID
Code of unregistered user Duress code of unregistered user	1234 → OK	
RRU code	1234 → OK	
Managing the group armed modes		
Keypad code Keypad duress code	1234 → ✳ → 2 → OK	**2** is a group ID

User code User duress code	5 → ✳ → 1234 → ✳ → 2 → OK	**5** is a user ID **2** is a group ID
Code of unregistered user Duress code of unregistered user	1234 → ✳ → 2 → OK	**2** is a group ID
RRU code	1234 → ✳ → 2 → OK	**2** is a group ID

Learn more about user ID

Learn more about group ID

Authorization confirmation with a passcode

Authorization confirmation with a passcode is a feature that provides the ability to set up two-factor authentication for users when they control the system's security modes. This definition means that users must first use an access device (Pass, Tag, or a smartphone) and then enter a passcode to confirm their authorization to the system.

Learn more about Authorization confirmation with a passcode

Managing automation devices and scenarios

> Ensure the **Manage automation devices** feature is configured for the primary or secondary operating mode in the keypad settings in Ajax apps.

To control the automation device or scenario with KeyPad Outdoor Jeweller:

1. Present an access control device to the keypad or enter a passcode to authorize on the keypad.
2. Switch the keypad to the **Manage automation devices** mode with a long press of the **OK** button if this mode is not active or set as the main operating mode. The **OK** button should light up green or red depending on the current state of the automation device.
3. Press the **OK** button to change the state of the automation device or execute a scenario:

    - If the keypad manages a scenario on **switching the state**, the **OK** button LED indication should change to correspond to the state of the automation device.

- If the keypad manages a scenario **on preset action**, the **OK** button LED indication does not show the state of devices. Instead, it indicates whether the set action is completed or not.

The step sequence for managing the automation devices with the keypad depends on whether **Pre-authorization** and **Easy assigned device switch** options are enabled in the KeyPad Outdoor Jeweller settings.

Indication

KeyPad Outdoor Jeweller informs users about alarms, entry/exit delays, current security mode, malfunctions, and other system states by means of:

- Ajax logo, **OK** button, and backlight with LED indication;
- built-in buzzer.

Event	LED	Buzzer
Turning on the device	The logo lights up green for about 0.5 s.	Wake up beep.
Turning on the device not added to hub	The logo lights up green, then flashes red six times, followed by three rapid red flashes.	
Turning off the device	The logo lights up red and flashes red three times rapidly.	

Device is added to the hub	The logo lights up green for about 0.5 s.	
Device is deleted from the hub	The logo lights up red for 0.3 s, goes out for 0.3 s six times, then flashes red three times rapidly.	
Short button press		Short beep.
The keypad is in **Switch armed mode***	The logo is green or red depending on the current security state.	
The keypad is in **Manage automation devices** mode	The **OK** button is green or red depending on the current automation device state. The logo is off.	
The keypad is in **Start entry delay** mode*	The logo is red when the site is armed. The logo flashes red simultaneously with a beep on entry delay.	
Arming or **Night mode** activation	The logo changes from green to red.	Beep for about 0.2 s.
Disarming	The logo changes from red to green.	Double beep for about 0.4 s.
Pressing **Panic** button (✳)		Long beep for about 0.5 s.
Press and hold the function button (✳) to clear the entered code	The backlight flashes simultaneously with a short beep.	Short beep.

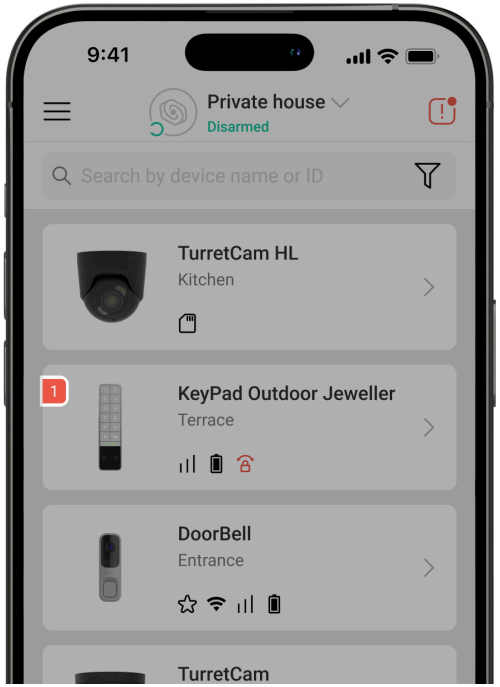
Wrong passcode entered	The backlight lights up three times during a long beep.	Long beep for about 0.6 s.
Request is denied due to lack of user permissions or malfunction	The logo lights up yellow three times during a long beep.	Long beep for about 0.6 s.
The keypad is locked	The backlight lights up three times during a long beep.	Long beep for about 0.6 s.
System integrity check fails	The logo lights up green or red (depending on current security state) three times during a long beep.	Long beep for about 0.6 s.
System security state change is forbidden	The logo lights up yellow three times during a long beep.	Long beep for about 0.6 s.
Tamper alarm/restoration	The logo lights up red for 0.7 s.	
Pass/Tag read is successful	The backlight goes out for about 0.3 s.	Beep for about 0.2 s.
Pass/Tag read is failed	The logo lights up yellow, and the backlight goes out during a beep.	Long beep for about 1 s.
Smartphone reading is successful	The backlight goes out for about 0.1 s.	Frequent beeping for about 0.2 s.
Smartphone reading is failed	The logo lights up yellow during a beep.	Long beep for about 1 s.
The keypad is waiting to read Pass/Tag	The backlight lights up for 0.2 s and goes out for 1 s until Pass/Tag is read.	
Adding Pass/Tag is successful		Two short beeps.

1. Adding Pass/Tag is failed. 2. Invalid card is read. 3. Other malfunctions occurred while reading an access device.	The logo lights up yellow for about 0.3 s.	Long beep for about 0.6 s.
Delay on entering/leaving	The logo lights up red simultaneously with beep on entry delay. The logo lights up green simultaneously with beep on exit delay.	Short beep once per 1 s.
System recovery is needed (PD 6662:2017)	The logo lights up yellow for about 0.1 s then a short beep sounds. It is repeated three times.	
Post alarm indication	The logo flashes red twice every 3.4 s.	
Arming incomplete (PD 6662:2017)	The logo lights up yellow constantly.	Three short beeps for about 0.3 s every 1 s.
One device in the system is offline (UL)	The logo flashes yellow two times simultaneously with a short beep two times every 1 minute.	
One device in the system has a low battery	The logo flashes yellow three times simultaneously with a short beep with a change in tone every 1 minute.	

(UL)		
Delayed arming (initiated by the device) (PD 6662:2017)	The logo lights up green for about 0.8 s every 1 s.	
Delayed arming (initiated by the app) (PD 6662:2017)	The logo lights up red for about 0.8 sec every 1 s.	
The hub does not respond	The logo lights up yellow during a long beep.	Long beep for about 0.5 s.
The battery charge is low	The logo slowly lights up yellow and slowly goes out after the correct passcode is entered.	
The battery is completely discharged	The logo slowly lights up yellow and slowly goes out. Then the device turns off.	Long beep for about 2 s.

* When the indication is enabled in the keypad settings.

Malfunctions



When the device detects a malfunction (for example, there is no connection via the Jeweller protocol), a malfunction counter is displayed in the Ajax app in the upper left corner of the device icon.

All malfunctions can be seen in the device **states**. Fields with malfunctions will be highlighted in red.

Malfunction is displayed if:

- The device temperature is outside acceptable limits.
- The device lid is open (tamper alarm is triggered).

- There is no connection with the hub or radio signal range extender via Jeweller.
- The device battery is low.

Maintenance

Regularly check the functioning of the device. The optimal frequency of checks is once every three months. Clean the device enclosure from dust, cobwebs, and other contaminants as they emerge. Use soft, dry wipes suitable for equipment maintenance.

Do not use substances that contain alcohol, acetone, gasoline, and other active solvents to clean the device.

Technical specifications

All technical specifications

Compliance with standards

Setup in compliance with EN 50131 requirements

Warranty

The warranty for the products of the Limited Liability Company “Ajax Systems Manufacturing” is valid for 2 years after purchase.

If the device does not operate properly, we recommend contacting support service first, as most technical issues can be resolved remotely.

Warranty obligations

User Agreement

Contact Technical Support:

- **email**
- **Telegram**

Manufactured by “AS Manufacturing” LLC