Superior KeyPad Plus G3 Jeweller user manual

Updated January 22, 2026

Superior KeyPad Plus G3 Jeweller is a wireless keypad designed to manage Ajax systems. Users can authenticate using **Tag** key fobs, **Pass** cards, and codes. The device is intended for indoor use only.

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

Superior KeyPad Plus G3 Jeweller is a device of the **Superior product line**. Only accredited Ajax Systems partners can sell, install, and maintain Superior products.

Buy Superior KeyPad Plus G3 Jeweller

Functional elements

1. **Armed** indicator.

2. **Disarmed** indicator.

3. **Night mode** indicator.

4. **Malfunction** indicator.

5. Pass/Tag reader.

6. Numpad.

7. ✳ **Function** button.

8. **Reset** button.
9. **Arm** button.
10. **Disarm** button.
11. **Night Mode** button.
12. SmartBracket mounting panel. To remove the panel, unscrew the holding screw and slide the panel down.
13. Perforated part of the mounting panel. It is required for a tamper button to trigger in case of any attempt to detach the device from the surface. Do not break it off.
14. **Tamper button**.
15. Power button.
16. QR code with the device ID. It is used to add the device to the hub.
17. Holding screw to secure the keypad to SmartBracket.

Compatible hubs

An Ajax hub with **OS Malevich 2.35** and later is required for the keypad to operate.

☞ **Check device compatibility**

Operating principle

Superior KeyPad Plus G3 Jeweller features large touch-sensitive buttons, a reader for contactless authorization, and LED indicators. The keypad is used to control security modes, send a panic alarm, or mute the fire alarm.

Superior KeyPad Plus G3 Jeweller has LED indicators showing the current security mode and keypad malfunctions (if any). The security state is displayed only when the keypad is active (the device backlight is on).

Superior KeyPad Plus G3 Jeweller can be used in low-light conditions thanks to its backlight. Pressing the buttons is accompanied by a sound signal. The backlight brightness and keypad volume are adjustable in the settings. If the

keypad is not touched for 4 seconds, Superior KeyPad Plus G3 Jeweller reduces the backlight brightness. After 8 seconds of inactivity, it enters power-saving mode and turns off the display.

If the battery charge is low, the backlight turns on at the minimum level, regardless of the settings.

Security control

Superior KeyPad Plus G3 Jeweller can arm and disarm the entire site or specific groups and activate **Night mode**. Users can control the security using Superior KeyPad Plus G3 Jeweller through:

1. **Cards or key fobs**. To quickly and securely identify users, Superior KeyPad Plus G3 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 Superior KeyPad Plus G3 Jeweller.
2. **Codes**. Superior KeyPad Plus G3 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 or Tag, 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

Superior KeyPad Plus G3 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

Superior KeyPad Plus G3 Jeweller has the ✳ **Function** button that operates in one of three modes:

- **Off** — the **Function** button is disabled, and nothing happens when the user presses this button.

- **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 detector alarm** feature is enabled (Hub → Settings → Service → Fire detectors settings).

Duress code

Superior KeyPad Plus G3 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

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

Superior KeyPad Plus G3 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 using a personal or general code on the keypad.

 Learn more

Fire alarm muting

Superior KeyPad Plus G3 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 detector 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 detector alarm** is enabled.

 Learn more

Superior Jeweller data transfer protocol

Superior Jeweller is an upgraded radio protocol for Superior devices, ensuring compliance with **Grade 3** (EN 50131). It features advanced **encryption** and **frequency hopping**. Full frequency hopping is available only when all devices in the system use Superior Jeweller. If at least one device runs on the regular Jeweller protocol, the system will be limited to **Grade 2**: encryption remains, but hopping is disabled. Superior devices can also operate on the regular Jeweller protocol, depending on the hub.

 Learn more

Advanced encrypted communication

The communication between Superior KeyPad Plus G3 Jeweller and the hub is protected by an advanced encryption scheme that ensures data confidentiality and integrity. This means that all sensitive data in the message is encrypted, and each message includes a unique authentication tag allowing the system to check that the data has not been modified during transmission. The system can reliably detect tampering and reject forged or altered messages, providing robust protection against both passive and active attacks. This ensures secure communication between the device and hub, as well as reliable system and data protection.

Frequency hopping

To comply with the Grade 3 requirements, Superior KeyPad Plus G3 Jeweller uses **frequency hopping** for radio communication with the hub (or the radio signal range extender). With this method, the hub and devices added to it change their operating frequency according to a defined pattern. The hopping sequence covers a defined set of channels within the operating bands, and devices switch frequencies synchronously with the hub. Even if some channels are affected by jamming, messages can be transmitted successfully via other channels. Frequency hopping improves the system's reliability and performance and ensures its resistance to intentional interference and jamming attempts.

Frequency hopping does not cause delays or pauses during radio communication and does not reduce the data transfer speed. If **range extenders** are added to the system, the frequency hopping is used for all radio communications: "device ↔ range extender" and "range extender ↔ hub".

The system uses frequency hopping for radio communication only if all wireless devices support this method.

If at least one device added to the system does not support frequency hopping, the hub and all devices switch to the operating frequencies of that device and do not use

frequency hopping for radio communication.

 **Learn more about jamming**

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**.

Superior KeyPad Plus G3 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, including 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 Superior KeyPad Plus G3 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**.

Superior KeyPad Plus G3 Jeweller is best placed 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.

The recommended installation height is 1.3–1.5 meters above the floor. Install the keypad on a flat, vertical surface. This ensures Superior KeyPad

Plus G3 Jeweller is securely attached to the surface and helps avoid false tamper alarms.

When holding Superior KeyPad Plus G3 Jeweller in your hands or using it on a table, we cannot guarantee that the touch buttons will work properly.

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 stably. 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.

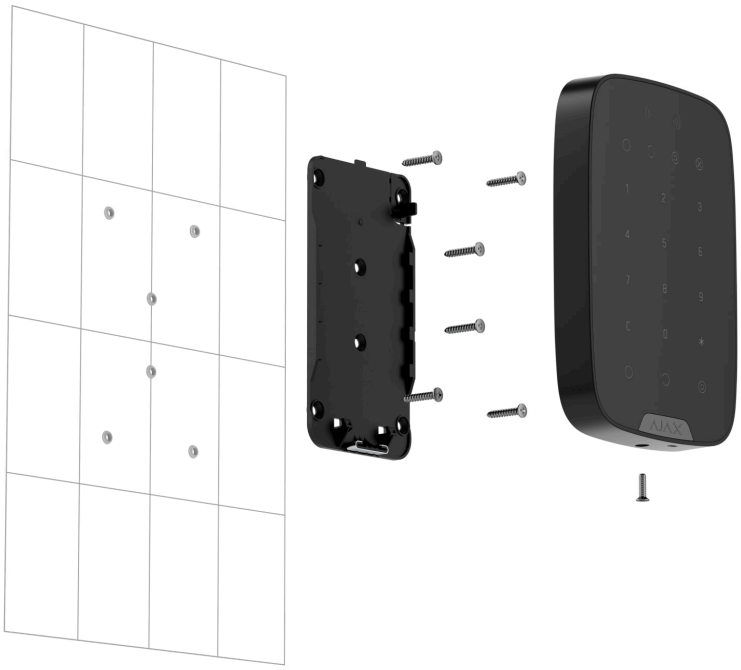
Refer to the **Functionality testing** section to learn how to run Jeweller signal strength test.

What is Jeweller signal strength test

Where not to install the keypad

1. Outdoors. This can lead to device failure.
2. In places where power or Ethernet cables, decor items, or other things may obstruct the keypad.
3. In places with temperature and humidity outside the permissible limits. This could damage the device.
4. Closer than 1 m to the hub or radio signal range extender.
5. In places with low or unstable Jeweller signal strength.

Installation



Before installing Superior KeyPad Plus G3 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.
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 with the tape may come unstuck from the surface at any time. As long as the device is secured with the tape, the tamper alarm will not be activated when the device detaches from the surface.

4. Place the keypad on the SmartBracket mounting panel. The device's **X** LED indicator will flash, showing that the device enclosure is closed.
5. Run **functionality testing**.
6. If the tests are successful, remove the keypad from SmartBracket.
7. Fix the SmartBracket panel on the surface with the provided 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 enclosure. The screw is needed for more reliable fastening and to protect the keypad from quick dismantling.

Adding to the system

The hub and the device operating at different radio frequencies are incompatible. The device's radio frequency range 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.

Check the device compatibility before the device is added to the system. Only verified partners can add and configure Superior devices in Ajax PRO apps

Types of accounts and their rights

Before adding a device

1. Install an **Ajax PRO app**.
2. Log in to a **PRO account** or create a new one.
3. Select a **space** or create a new one.
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.

Adding to the hub

1. Open an **Ajax PRO 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.

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

Superior KeyPad Plus G3 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

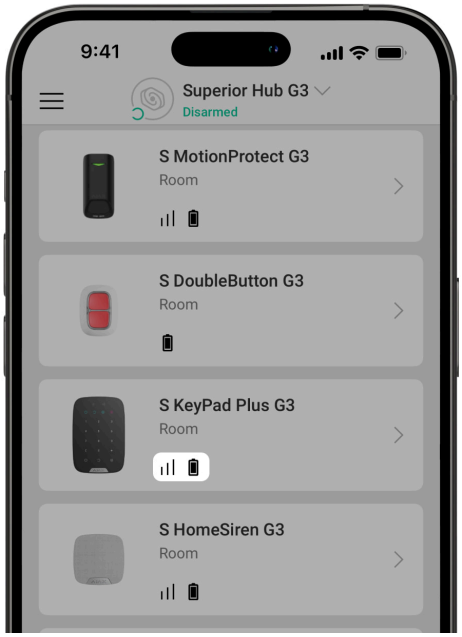
An Ajax system provides several types of tests to help select the correct installation place for the devices. For Superior KeyPad Plus G3 Jeweller, the following tests are available:

- **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

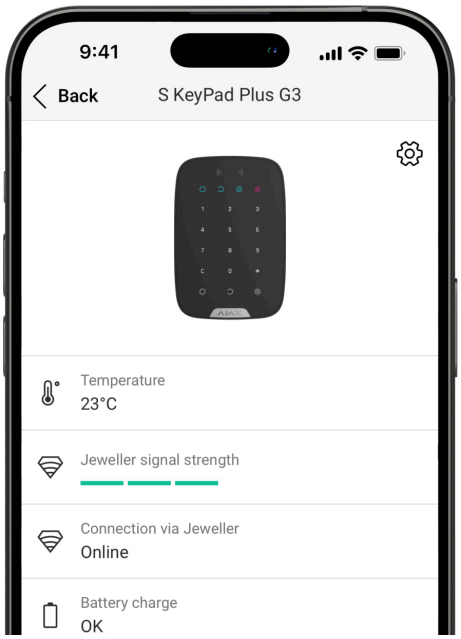


Icons in the Ajax app display some of Superior KeyPad Plus G3 Jeweller states. Icons can be checked in the **Devices** tab.

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.
	The device is in the signal attenuation test mode. **Learn more**
	The device is permanently deactivated. **Learn more**
	Tamper alarm notifications are permanently deactivated. **Learn more**
	The device is deactivated 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**
	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 Superior KeyPad Plus G3 Jeweller can be found in Ajax apps:

1. Go to the **Devices** tab.
2. Select **Superior KeyPad Plus G3 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 (i) opens the list of device malfunctions.

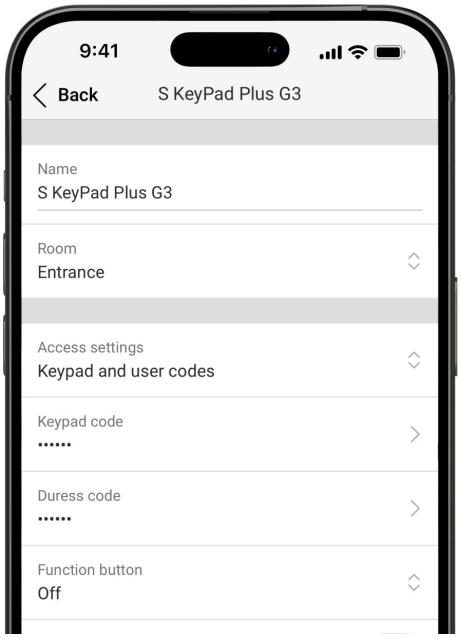
	The field is displayed only if a malfunction is detected.
Temperature	Device temperature. It is measured by the processor and changes depending on the ambient temperature. You can create a scenario by temperature to control automation devices. Learn more
Jeweller signal strength	Jeweller signal strength 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 state 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.
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>	State 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.
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**
Lid	The state 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**

Pass/Tag reading	Displays if the reader for cards and key fobs is enabled.
Easy armed mode change	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	The state 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 state of the device's one-time deactivation setting: • **No** — the device operates in the normal mode. • **Entirely** — the device is entirely excluded from the system operation while 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 while 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 Superior KeyPad Plus G3 Jeweller settings in the Ajax apps:

1. Go to the **Devices** tab.
2. Select **Superior KeyPad Plus G3 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 Superior KeyPad Plus G3 Jeweller is assigned. The room name is displayed in the text of SMS and notifications in the events 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 a 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 all users. • **Mute fire alarm** — when pressed, the system mutes the alarm of Ajax fire detectors. Available only if the **Interconnected fire detector alarm** feature is enabled. **Learn more**
Accidental press protection	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	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, min	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.
Brightness	Adjusting the brightness of the keypad button backlight. The backlight functions only when the keypad is active. This option does not affect the brightness level of the Pass/Tag reader and security modes indicators.
Buttons volume	Selecting the keypad button volume 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, 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 or Tag and entering the appropriate passcode. Learn more
Time for confirmation	Selecting the maximum time to confirm authorization with a password after access device confirmation. Available if the **Authorization confirmation with a passcode** toggle is enabled.

Easy armed mode change	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	When enabled, the user can arm the object without entering a code or presenting the personal access device. If disabled, enter a code or present the access device to arm the system. The screen for entering the code appears after pressing the ◯ **Arm** button.

Auto-wake on Delay when entering	Activates the keypad after any security device starts **Entry delay**. The auto-wake feature may also reduce the keypad battery life.
Alert with a siren if the panic button is pressed	The setting is displayed if the **Panic** 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 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 Superior KeyPad Plus G3 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.

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 **Disarm** 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

Superior KeyPad Plus G3 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. Tap **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 **Disarm** 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 at least one keypad setting.

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 **Disarm** 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.

Controlling security

Using codes, Tag, or Pass, 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.

If a personal or access code, Tag, or Pass 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.

Superior KeyPad Plus G3 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 Superior KeyPad Plus G3 Jeweller in the Ajax app.

The step sequence for changing the security mode with the keypad depends on whether **Arming without code, Authorization confirmation with a passcode**, and **Easy armed mode change** options are enabled in the Superior KeyPad Plus G3 Jeweller settings.

Using Tag or Pass

1. Activate the keypad by approaching your hand in front of it.
2. Present Tag or Pass to the keypad Pass/Tag reader.
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.

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

Using passcodes

Incorrectly entered codes can be cleared by pressing the C **Reset** button.

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

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

☞ **Learn more about user ID**

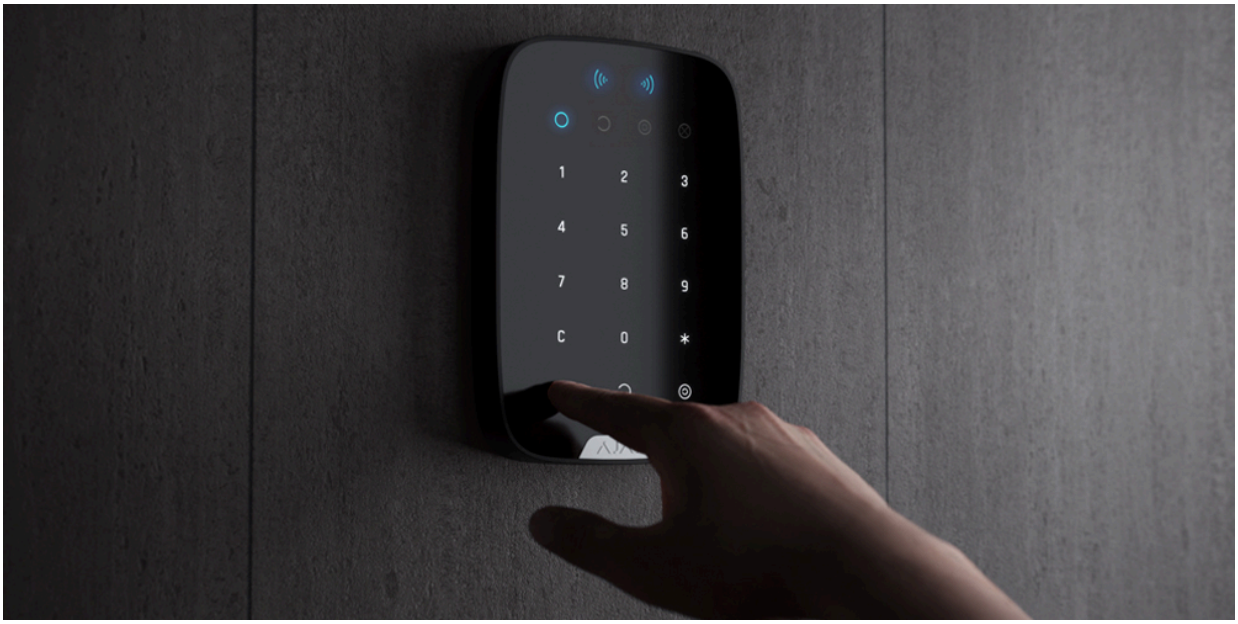
☞ **Learn more about group ID**

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 or Tag) and then enter a passcode to confirm their authorization to the system.

☞ **Learn more about Authorization confirmation with a passcode**

Indication



Superior KeyPad Plus G3 Jeweller can report the current security mode, keystrokes, malfunctions, and state by LED indication and sound. The backlight displays the current security mode after the keypad is activated. The information about the current security mode is relevant even if the arming mode is changed by another device: a key fob, another keypad, or an app.

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

Event	Indication	Note
Turning on the device	All indicators and the numpad backlight light up briefly. Then, a three-tone beep sounds, and the current system security mode LED and the numpad backlight light up. After that, the numpad backlight smoothly goes off, and a double beep sounds	

Turning on the device that has not been added to the hub	All indicators and the numpad backlight light up briefly. After that, the **X** LED flashes 6 times and then flashes 3 times rapidly	The keypad turns off after the indication ends
Turning off the device	The **X** LED lights up for about 1 s and then flashes 3 times	The system sends a notification when the keypad is turned off using the power button
The device is deleted from the hub	The **X** LED flashes 6 times and then flashes 3 times rapidly	The keypad turns off after the indication ends
There is no connection to the hub or radio signal range extender	The **X** LED flashes	
The device lid is open (SmartBracket panel is removed)	The **X** LED flashes briefly once	
Touch button press	Short beep, the current system security state LED flashes 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, the numpad backlight flashes 3 times	
The security mode cannot be activated (**System integrity check** fails)	Long beep, the current security state LED flashes 3 times	
The system requires to confirm authorization with a password after access device confirmation. Available if the Authorization	The current security state LED flashes during the set time for confirmation	

confirmation with a passcode feature is activated		
The keypad is locked due to a wrong code attempt or an attempt to use an unauthorized pass/tag	Long beep, during which the security state LEDs and keypad backlight flash 3 times	
The hub does not respond	Long beep, the **X** LED lights up	
The battery charge is low	After changing the security mode, the **X** LED lights up. The touch buttons are locked during 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, and then the keypad turns off.	How to replace batteries

Sound notifications of malfunctions

Superior KeyPad Plus G3 Jeweller can notify system users with an audible sound if any device is offline or the battery is low. The keypad's LED **X** will flash. Malfunction notifications will be displayed in the events feed, SMS text, or push notifications.

To enable sound notifications of malfunctions, in an Ajax PRO app:

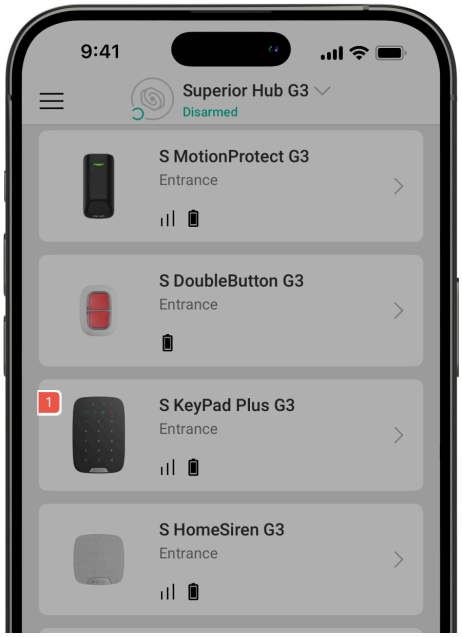
1. Go to the **Devices** tab.
2. Select the hub, and go to its settings.
3. Go to **Service** → **Sounds and alerts**.
4. Enable toggles: **If battery of any device is low and If any device is offline**.

5. Tap **Back** to save settings.

Event	Indication	Note
If any device is offline	Two short sound signals, the **X** LED flashes twice. Beep once per minute until all devices in the system are online.	Users can delay sound indication for 12 hours
If Superior KeyPad Plus G3 Jeweller is offline	Two short sound signals, the **X** LED flashes twice. Beep once per minute until the keypad in the system is online.	It's impossible to delay the sound indication
If the battery of any device is low	Three short sound signals, the **X** LED flashes 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.

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.

If the keypad battery is low, the system sends appropriate notifications, and the **X Malfunction** indicator smoothly lights up and goes out after each successful code entry.

Superior KeyPad Plus G3 Jeweller can work for up to 2 months after the low battery signal. However, we recommend you replace the batteries immediately upon notification. It is advisable to use lithium batteries. They have a large capacity and are less affected by temperatures.

How to replace batteries in Superior KeyPad Plus G3 Jeweller

Technical specifications

All technical specifications of Superior KeyPad Plus G3 Jeweller

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:

- e-mail
- Telegram

Manufactured by “AS Manufacturing” LLC