

Superior KeyPad TouchScreen G3 Jeweller user manual

Updated March 9, 2026



Superior KeyPad TouchScreen G3 Jeweller is a wireless keypad with a touch screen designed for managing Ajax systems. Users can authenticate using smartphones, Tag key fobs, Pass cards, and codes. The device is intended for indoor use only.

Superior KeyPad TouchScreen G3 Jeweller communicates with a hub over two secure radio protocols. The keypad uses the **Jeweller** protocol to transmit alarms and events, and the **Wings** protocol to update firmware, transmit the list of groups, rooms, and other additional information. The communication range in an open space is up to 2,500 meters. The maximum range depends on the hub model.

[Learn more](#)

Buy Superior KeyPad TouchScreen G3 Jeweller



Superior products are available exclusively to accredited Ajax Systems partners for sales, installation, and maintenance, creating a protected, high-value revenue channel.

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

Functional elements



1. Ambient light sensor for automatically adjusting the backlight brightness.
2. IPS touch display with a 5-inch diagonal.
3. Ajax logo with an LED indicator.
4. Card/key fob/Bluetooth reader.
5. SmartBracket mounting panel. To remove the panel, slide it down.

6. Perforated part of the mounting panel for triggering the tamper in case of any attempt to detach the keypad from the surface. Do not break it off.
7. Perforated part of the mounting panel for routing cables through the wall.
8. Built-in buzzer.
9. Tamper button.
10. QR code with the device ID for adding the keypad to the Ajax system.
11. Power button.
12. Terminals for connecting an external power supply unit (not included). The terminals can be removed from the holders when necessary.
13. Cable channel for routing the cable from the third-party power supply unit.
14. Perforated part of the mounting panel for routing cables from the bottom.
15. The hole for attaching the SmartBracket mounting panel with a holding screw.

Compatible hubs and range extenders

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

Check devices compatibility

Operating principle

Superior KeyPad TouchScreen G3 Jeweller features a built-in buzzer, a touch display, and a reader for contactless authorization. The keypad can be used to change security modes and control automation devices, as well as to notify alert users to system alarms.

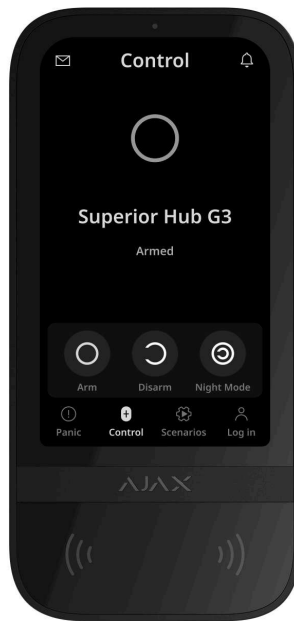
The keypad automatically adjusts the backlight brightness and wakes up upon approach. Sensitivity is adjustable in the app. The Superior KeyPad TouchScreen G3 Jeweller interface resembles that of the Ajax Security System app. There are dark and light appearances to choose from. The 5-inch touch screen enables quick access to security modes of the entire system or specific groups, as well as to automation scenario control. The display also indicates system malfunctions when the system integrity check option is enabled.


The built-in buzzer of Superior KeyPad TouchScreen G3 Jeweller provides audio alerts based on system settings, notifying users about:

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

The keypad operates on pre-installed batteries and can also be powered by a third-party power supply unit within a 10.5–14 V_{DC} voltage range and a minimum operating current of 0.5 A. When external power is connected, the pre-installed batteries serve as a backup power source.

Security control



Superior KeyPad TouchScreen G3 Jeweller can be used to arm and disarm the entire system or specific groups and activate **Night Mode**. Use the **Control**  tab to change the security mode. Users can authenticate into Superior KeyPad TouchScreen G3 Jeweller via:

- 1. Smartphones.** Authentication is possible via the [Ajax Security System](#) app on smartphones that support Bluetooth Low Energy (BLE). BLE is a low-power radio protocol that enables smartphones to function as an alternative to Tag or Pass for user authentication. The keypad supports Android and iOS smartphones with BLE version 4.2 and later.
- 2. Cards or key fobs.** To quickly and securely identify users, Superior KeyPad TouchScreen G3 Jeweller uses the DESFire® technology. DESFire® is based on the ISO 14443 international standard and combines 128-bit encryption and copy protection.
- 3. Codes.** Superior KeyPad TouchScreen G3 Jeweller supports general keypad codes, personal user codes, and codes for unregistered users.

Access codes

- **Keypad code** is a general code assigned to the keypad. When used, all events appear in Ajax apps under the keypad's name.

- **User code** is a personal code set up for users connected to the hub. When used, all events appear in Ajax apps under the respective user's name.
- **Keypad access code** is a code created for an unregistered person. When used, events appear in Ajax apps under the name associated with this code.
- **RRU code** is a temporary access code for rapid response units (RRU), activated after the alarm for a specified duration. When the code is activated and used, events appear in Ajax apps under the title associated with this code.



The supported number of user codes, keypad access codes, and RRU codes depends on the [hub model](#).

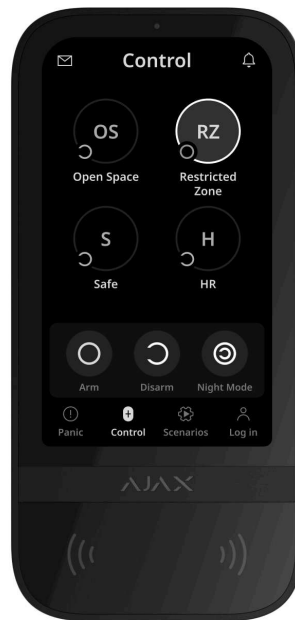
Access rights and codes can be managed directly in Ajax apps. If a code is compromised, it can be changed remotely without requiring an installer's visit. If a user loses their Pass, Tag, or, smartphone, an admin or a PRO with system configuration rights can instantly block the lost device in an Ajax app. Meanwhile, the user can still control the system via a personal code.

Duress code

Superior KeyPad TouchScreen G3 Jeweller supports a **duress code** that allows users to discreetly send an alarm while appearing to disarm the system. When the duress code is entered, the system does not activate sirens or display any visible alerts in Ajax apps. However, a silent alarm is immediately transmitted to the security company and other security system users, notifying them of the emergency.

[Learn more](#)

Security control of the groups





Superior KeyPad TouchScreen G3 Jeweller allows controlling the groups' security when **Group Mode** is enabled. In the keypad **settings**, you can specify which groups will be displayed (keypad groups). By default, all groups are visible on the keypad display in the **Control** **+** tab. You can learn more about group security management in [this section](#).



If the **Followed group** feature is configured for groups, their security mode will automatically change depending on their settings and initiators' states.

User pre-authorization

The **pre-authorization** feature is essential to prevent unauthorized access to the control panel and the current system state. The feature can be activated separately for the **Control** **+** and **Scenarios**  tabs in the keypad **settings**.

When pre-authorization is activated for designated tabs, a code entry screen appears on them. Users must authenticate either by entering a code or presenting an access device to the keypad before performing any actions. An exception applies to the **Alarm**  tab, which remains accessible to all users, allowing them to send an emergency signal without authentication.

Unauthorized access auto-lock

If an incorrect code is entered or an unverified access device is used three times within one minute, the keypad will lock for the duration specified in its settings. During this period, the hub ignores all code entries and access devices, while informing the security system users about the attempted unauthorized access. Superior KeyPad TouchScreen G3 Jeweller turns off the reader and blocks access to all tabs. The keypad's display shows a corresponding notification.

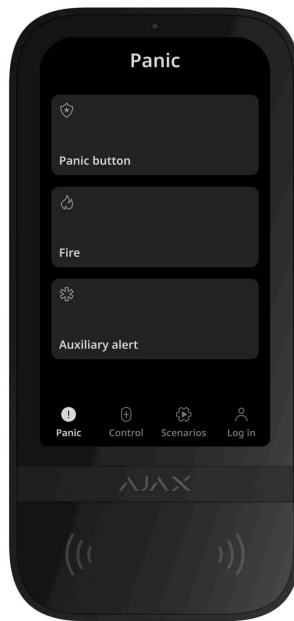
A PRO or a user with system configuration rights can unlock the keypad via the app before the specified lock time expires.

Two-stage arming

Superior KeyPad TouchScreen G3 Jeweller supports two-stage arming and can be used to initiate the process, but it cannot serve as a second-stage device. The two-stage arming procedure using Tag, Pass, or a smartphone works similarly to arming with a personal or general code entered on the keypad.


[Learn more](#)

Emergency buttons



For emergencies, the keypad features the **Panic**  tab with three buttons:

- Panic button;
- Fire;
- Auxiliary alert.

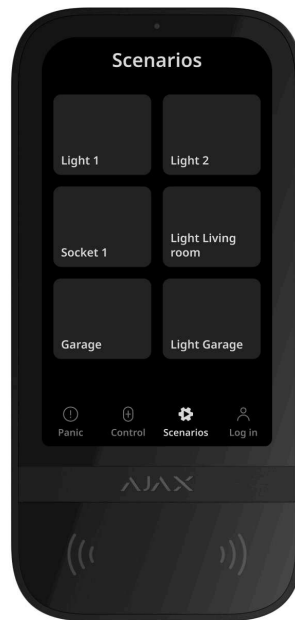
In an Ajax app, an admin or a PRO with system configuration rights can customize which buttons appear in the **Panic**  tab. There are two available options in the Superior KeyPad TouchScreen G3 Jeweller settings: only the **Panic button** (by default) or all three buttons. The text of in-app notifications and event codes transmitted to the Central Monitoring Station (CMS) depend on the selected button type.

You can also enable accidental press protection to prevent false alarms. When activated, the user must confirm the alarm transmission by pressing the **Send** button on the keypad display. The confirmation screen appears after any emergency button is pressed.



Pressing emergency buttons can trigger Alarm scenarios within an Ajax system.

Scenario management



The keypad features a dedicated **Scenarios** tab, which can hold up to six buttons that control one automation device or a group of devices. Group scenarios provide more convenient simultaneous control over multiple switches, relays, or sockets.

Create automation scenarios directly in the keypad settings and manage them using Superior KeyPad TouchScreen G3 Jeweller.

Starting with **OS Malevich 2.38** after authorization on the keypad the system records which user initiated an automation scenario from the keypad. This information is displayed in the hub event feed.

[Learn more](#)

Indication of malfunctions and security mode

Superior KeyPad TouchScreen G3 Jeweller informs users about system malfunctions and the current security mode via:

- **Display** – shows system status when active;
- **Logo** – lights up red continuously or only when the system or a group is armed, depending on the settings;
- **Sound indication** – the built-in buzzed signals alarms, opening doors, and entry/exit delays.



Acknowledgment of the latest events

Superior KeyPad TouchScreen G3 Jeweller displays up to 100 latest system events since the last check. Events are grouped and sorted by the date of their occurrence.



An event contains the following information:

- device name;
- action;
- room;
- actual time (HH:MM).

To enable the view of the latest events on the keypad:

1. Open an Ajax app. Select a space with the added device.
2. Go to the **Devices**  tab.
3. Select Superior KeyPad TouchScreen G3 Jeweller and go to its **Settings** by tapping on the gear icon .
4. Select the **Keypad notification center** section.
5. Enable the **Event acknowledgement section** toggle.
6. Tap **Back** to save the new settings.

To view the latest events on the keypad display:

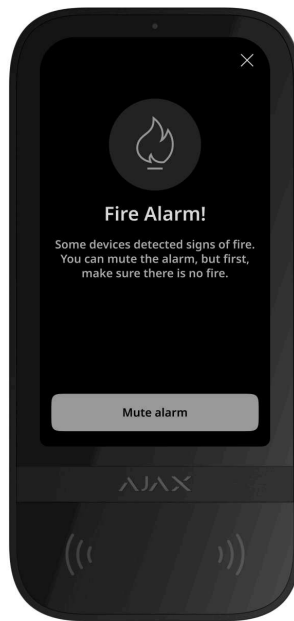
1. Go to the **Control**  tab.
2. Tap the  icon to view a list of the latest events. The icon will have a red badge in the upper right corner if there are new events.
3. Tap the **Mark all as read** button to clear the list of the latest events. Events will remain in the event feed in Ajax apps.



Marking all events as read clears the list of the latest events on the keypad currently in use. Other keypads added to the same hub will still display the latest events.

0:00 / 0:11


Fire alarm muting



In case of a fire alarm in the system, you can mute it using Superior KeyPad TouchScreen G3 Jeweller.

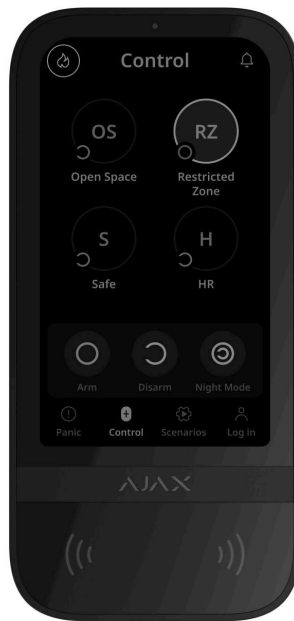


Pressing the **Fire** emergency button in the Panic tab does not activate Interconnected Fire Detectors Alarm (if enabled). Instead, when an emergency signal is sent via the keypad, a corresponding notification is transmitted to Ajax apps and the CMS.

When the **Mute fire alarm** feature is enabled, all Superior KeyPad TouchScreen G3 Jeweller devices in the system will display a screen with fire alarm information and a mute button. If the mute button has already been pressed on another keypad, a corresponding notification appears on the remaining Superior KeyPad TouchScreen G3 Jeweller displays. Users can close the fire alarm muting screen and continue using other keypad features. To reopen the muting screen, simply tap the  icon on the Superior KeyPad TouchScreen G3 Jeweller display.



If the fire alarm is triggered by ManualCallPoint Jeweller, and CO or smoke levels are critical, the alarm cannot be muted via the keypad.



To instantly display the fire alarm muting screen on Superior KeyPad TouchScreen G3 Jeweller, enable the **Always active display** toggle in the **Display settings** and connect an external power supply.

Otherwise, the muting screen will only be displayed when the keypad wakes up.

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.

Wings data transfer protocol

Wings is a proprietary wireless communication technology for transmitting large data packets. The device uses Wings to transmit photos and upload firmware updates.

[Learn more](#)

Advanced encrypted communication

The communication between Superior KeyPad TouchScreen 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 TouchScreen 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

Ajax systems can transmit alarms to both [Ajax PRO Desktop](#) monitoring app and the central monitoring station (CMS) using **SurGard (Contact ID)**, **SIA (DC-09)**, **ADEMCO 685**, and other [supported protocols](#).

Superior KeyPad TouchScreen G3 Jeweller can transmit the following events:

1. Entry of the duress code.
2. Pressing the panic button. Each button has its own event code.
3. Keypad lock due to an unauthorized access attempt.
4. Tamper alarm/recovery.
5. Loss/restoration of connection with the hub or radio signal range extender.
6. Arming/disarming the system.
7. Unsuccessful arming attempt (if the [system integrity check](#) is enabled).
8. Permanent deactivation/activation of the keypad.
9. One-time deactivation/activation of the keypad.

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.



The device ID and number can be found in its [states](#) in an Ajax app.

Adding to the system



Superior KeyPad TouchScreen G3 Jeweller is not compatible with [Hub \(2G\) Jeweller](#), [Hub \(4G\) Jeweller](#), [Hub Plus Jeweller](#), and third-party security control panels.

To connect Superior KeyPad TouchScreen G3 Jeweller to the hub, the keypad must be located at the same secured facility as the system – within the range of the hub’s radio network. For the keypad to operate via the [ReX 2 Jeweller](#) radio signal range extender, you must first add the keypad to the hub and then connect it to **ReX 2 Jeweller** in the range extender’s settings.



The hub and the device must operate on the same radio frequency to be compatible. The device’s radio frequency range might vary depending on the region. We recommend purchasing and using Ajax devices within the same region. To confirm the supported frequency range, contact our [technical support service](#).

Before adding a device

1. Install the [Ajax app](#).
2. Log in to your [account](#) or create a new one.

3. Select a space or create a new one.

What is a space

How to create a space



The **space** functionality is available for apps of the following and later versions:

- Ajax Security System 3.0 for iOS;
- Ajax Security System 3.0 for Android;
- Ajax PRO: Tool for Engineers 2.0 for iOS;
- Ajax PRO: Tool for Engineers 2.0 for Android;
- Ajax PRO Desktop 4.0 for macOS;
- Ajax PRO Desktop 4.0 for Windows.

4. Add at least one virtual room.

5. Add a compatible hub to the space. Ensure the hub is switched on and has internet access via Ethernet, Wi-Fi, and/or a cellular network.


6. Ensure the space is disarmed and the hub is not updating by checking their states in an Ajax app.



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

Types of accounts and their rights

Connecting to the hub

1. Open the Ajax app. Select the hub where you want to add the keypad.
2. Go to the **Devices**  tab. Click **Add Device**.
3. Enter a name for the device, then scan or manually input the QR code (found on the keypad and the package box). Select a room and a group (if Group Mode is enabled).
4. Press **Add**.
5. Turn on the keypad by holding the power button for 3 seconds.

If the connection fails, turn off the keypad and try again after 5 seconds.

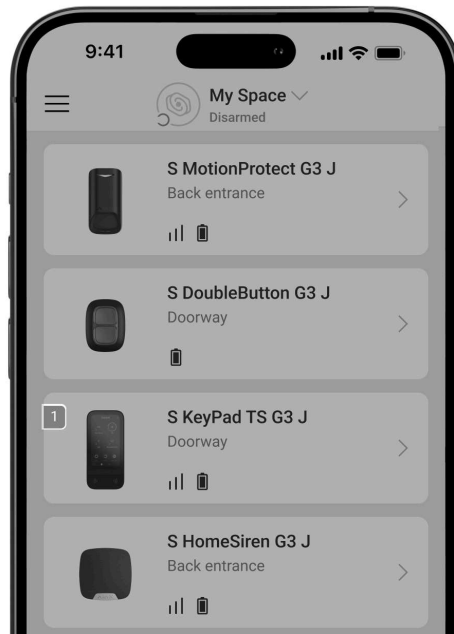
Please note that if the maximum number of devices has been added to the hub (depending on the hub model), you will be notified when attempting to add a new device.

Once connected to the hub, the keypad appears in the list of hub devices in Ajax apps. The update frequency for device states depends on the **Jeweller** or **Jeweller/Fibra** settings, with a default interval of 36 seconds.



Superior KeyPad TouchScreen G3 Jeweller can only operate with one hub at a time. When connected to a new hub, it stops communicating with the previous one. However, adding the keypad to a new hub does not automatically remove it from the device list of the old hub – this must be done manually via an Ajax app.

Malfunctions

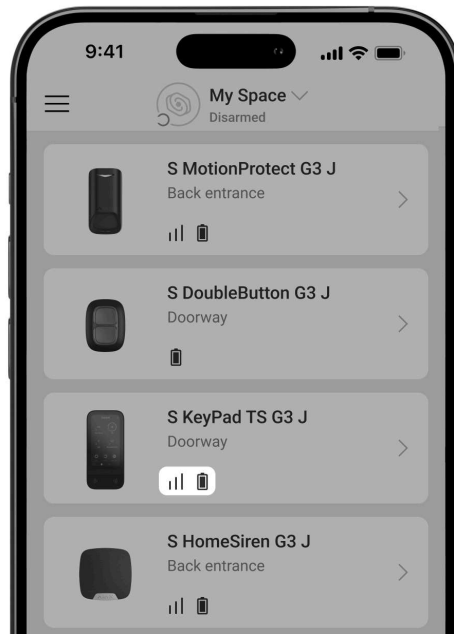


When a Superior KeyPad TouchScreen G3 Jeweller malfunction is detected, Ajax apps display a counter on the device icon. All malfunctions are indicated in the keypad's states, with affected fields highlighted in red.

A malfunction is displayed if:


- the keypad enclosure is open (tamper triggered);
- there is no connection with the hub or range extender via Jeweller;
- there is no connection with the hub or range extender via Wings;
- the keypad's battery is low;
- the keypad's temperature is outside the acceptable range.




Icons















Icons in the app

The icons in the app display some keypad states. To access them:

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



Icon	Meaning
	Jeweller signal strength. Displays the signal strength between the hub and the device. The recommended value is 2–3 bars. Learn more
	The keypad battery level is OK. Learn more
	The keypad has a malfunction. The list of malfunctions is available in the keypad states.




	<u>Learn more</u>
	Displayed when the keypad Bluetooth module is enabled.
	Bluetooth setup is not complete. The description is available in the keypad states.
	<p>A firmware update is available. Go to the keypad states or settings to find the description and launch an update.</p> <div data-bbox="456 560 1403 705" style="border: 1px solid black; border-radius: 10px; padding: 10px; margin: 10px 0;">  The icon is not available in the Ajax Security System app with version 3.0 and later for iOS and Android. </div> <p>To update the firmware, <u>CONNECT</u> the external power supply to Superior KeyPad TouchScreen G3 Jeweller.</p> <p><u>Learn more</u></p>
	Displayed when the keypad is operating via a <u>radio signal range extender</u> .
	Pass/Tag reading is enabled in the keypad settings.
	Chime on opening is enabled in the keypad settings.
	The device is in the signal attenuation test mode. <u>Learn more</u>
	Device is permanently deactivated. <u>Learn more</u>
	Tamper alarm notifications are permanently deactivated. <u>Learn more</u>

	<p>Device is deactivated until the first disarming of the system.</p> <p><u>Learn more</u></p>
	<p>Tamper alarm notifications are deactivated until the first disarming of the system.</p> <p><u>Learn more</u></p>
<p>Offline</p>	<p>The device has lost connection with the hub or the hub has lost connection with the Ajax Cloud server.</p>
<p>Not transferred</p>	<p>The device has not been transferred to the new hub.</p> <p><u>Learn more</u></p>

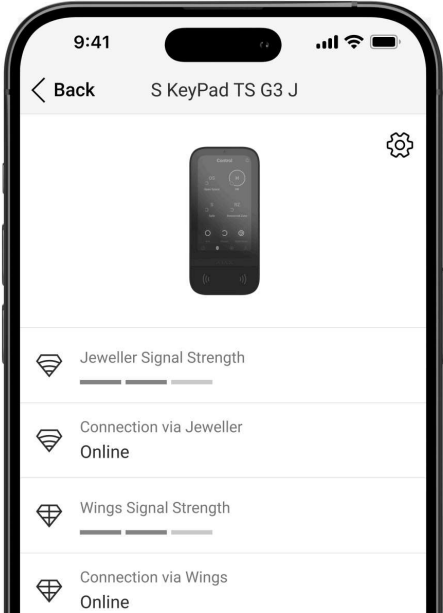
Icons on the display

Icons appear on top of the display and inform about specific system states or events.

Icon	Meaning
	<p>System restoration is required after an alarm. The user can either send a request or restore the system depending on their <u>account type</u>. To do so, click the icon and select the required button on the screen.</p> <p><u>Learn more</u></p>
	<p>Mute fire alarm. It appears after closing the <u>fire alarm muting screen</u>. Users can click the icon anytime and mute the fire alarm, including the interconnected fire alarm.</p>





	<div style="border: 1px solid black; padding: 10px; margin-bottom: 10px;">  <p>If the fire alarm is triggered by <u>ManualCallPoint Jeweller</u>, and CO or smoke levels are critical, the alarm cannot be muted via the keypad.</p> </div> <p><u>Learn more</u></p>
	<p>Chime on opening is disabled. Click the icon to enable.</p> <p>Appears on the display when the required <u>settings are adjusted</u>.</p>
	<p>Chime on opening is enabled. Click the icon to disable.</p> <p>Appears on the display when the required <u>settings are adjusted</u>.</p>



States



States provide information about the device and its operating parameters. The Superior KeyPad TouchScreen G3 Jeweller states can be found in an Ajax app:

1. Go to the **Devices**  tab.
2. Select **Superior KeyPad TouchScreen G3 Jeweller** from the list.

Parameter	Value
Data import	<p>Displays the error when transferring data to the new hub:</p> <ul style="list-style-type: none"> • Failed – the device has not been transferred to the new hub. <p><u>Learn more</u></p>
Malfunction	<p>Clicking on  opens the list of Superior KeyPad TouchScreen G3 Jeweller malfunctions.</p> <p>The field is displayed only if a malfunction is detected.</p>
New firmware version available 	<p>Clicking on  opens the instructions for updating the keypad's firmware.</p> <p>The field is displayed if a <u>new firmware version</u> is available.</p> <div style="border: 1px solid black; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> The state is not displayed in the Ajax Security System app with version 3.0 and later for iOS and Android.</p> </div>

	<p>To update the firmware, CONNECT an external power supply to Superior KeyPad TouchScreen G3 Jeweller.</p>
<p>Warning </p>	<p>Clicking on  opens the list of the settings and permissions that the app needs to be granted for the correct operation of the keypad.</p>
<p>Jeweller signal strength</p>	<p>Signal strength between the hub or range extender and the device on the Jeweller channel. The recommended value is 2–3 bars.</p> <p>Jeweller is a protocol for transmitting Superior KeyPad TouchScreen G3 Jeweller events and alarms.</p>
<p>Connection via Jeweller</p>	<p>Connection status on the Jeweller channel between the device and the hub (or the range extender):</p> <ul style="list-style-type: none"> • Online – the device is connected to the hub or the range extender. • Offline – the device is not connected to the hub or the range extender. Check the keypad connection.
<p>Wings signal strength</p>	<p>Signal strength between the hub or the range extender and the device on the Wings channel. The recommended value is 2–3 bars.</p> <p>Wings is a protocol for updating a firmware and transmitting the list of the groups, rooms, and other additional information.</p>
<p>Connection via Wings</p>	<p>Connection status on the Wings channel between the hub or the range extender and the device:</p>

	<ul style="list-style-type: none">• Online – the device is connected to the hub or the range extender.• Offline – the device is not connected to the hub or the range extender. Check the keypad connection.
Transmitter power	<p>Displays the selected power of the transmitter.</p> <p>The parameter appears when the Max or Attenuation option is selected in the Signal attenuation test menu.</p> <p><u>Learn more</u></p>
Battery charge	<p>The battery level of the device:</p> <ul style="list-style-type: none">• OK• Battery low <p>When the batteries are low, the Ajax apps and the security company will receive appropriate notifications.</p> <p>After sending a low battery notification, the keypad can work for up to 2 weeks.</p>
Lid	<p>The status of the keypad tamper that responds to detachment or opening of the device enclosure:</p> <ul style="list-style-type: none">• Open – the keypad was removed from the SmartBracket or its integrity was compromised. Check the device.• Closed – the keypad is installed on the SmartBracket mounting panel. The integrity of the device enclosure and the mounting panel is not compromised. Normal state.

	<p><u>Learn more</u></p>
External power	<p>Keypad external power supply connection status:</p> <ul style="list-style-type: none"> • Connected – external power supply is connected to the device. • Disconnected – the external power is disconnected. The device runs on batteries. <p><u>Learn more</u></p>
Always active display	<p>Displayed when the Always active display toggle is enabled in the keypad settings and external power supply is connected.</p>
Alarms sound indication	<p>Shows the status of the Activate keypad buzzer if alarm in the system is detected setting.</p>
Alarm duration	<p>Duration of sound signal in case of alarm.</p> <p>Sets in increments of 3 seconds.</p> <p>Displayed when the Activate keypad buzzer if alarm in the system is detected toggle is enabled.</p>
Pass/Tag reading	<p>Displays if the reader for cards and key fobs is enabled.</p>
Bluetooth	<p>Displays if the keypad’s Bluetooth module is enabled for controlling the system with a smartphone.</p>
Easy armed mode change	<p>Shows the configuration for the Easy armed mode change feature:</p> <ul style="list-style-type: none"> • Off – when this option is selected, each armed mode change must be confirmed by entering a passcode or presenting an access device.

- **Arm/disarm using access device without confirming action by buttons** – allows switching security state using access devices without confirmation with keypad buttons.



Option available when **Pass/tag reading** or **Bluetooth** is enabled and the keypad is assigned to one group only for security management.

- **Disarm without disarming button** – allows for arming or disarming without keypad confirmation for the whole system or groups. Available if Codes length restrictions are enabled in hub's settings.

Advanced encryption

The state of the communication with advanced encryption between the device and the hub or radio signal range extender:

- **Active** – the device communication is protected by advanced encryption.
- **Inactive** – the device communication operates without advanced encryption.

Learn more

Beep settings

Arming/disarming

When enabled, the keypad notifies about arming and disarming with a short beep.

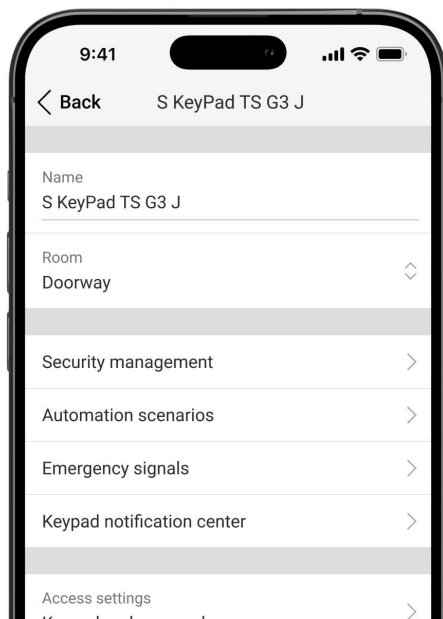
Night mode activation/deactivation

When enabled, the keypad notifies you when the **Night Mode** is switched on/off by making a short beep.



Mute the device when code on keypad is being entered	If enabled, the device stops beeping the delays or any other annunciations once the user starts entering the code on keypad
Entry delays	When enabled, the keypad beeps about <u>Entry delays</u> .
Exit delays	When enabled, the keypad beeps about <u>Exit delays</u> .
Entry delays in Night mode	When enabled, the keypad beeps about <u>Entry delays</u> in Night mode .
Exit delays in Night mode	When enabled, the keypad beeps about <u>Exit delays</u> in Night mode .
Chime on opening or doorbell button press	When enabled, a siren notifies about opening detectors triggering in the Disarmed system mode. <u>Learn more</u>
Beep volume	Displayed if the notifications about arming/disarming, entry/exit delay, and opening are activated. Shows the buzzer volume level for notifications.

<p>Permanent deactivation</p>	<p>Shows the status of the keypad permanent deactivation setting:</p> <ul style="list-style-type: none"> • No – the keypad operates in the normal mode. • Lid only – the hub administrator has disabled notifications about triggering of the keypad tamper. • Entirely – the keypad is entirely excluded from the operation of the system. The device does not execute system commands and does not report alarms or other events. <p><u>Learn more</u></p>
<p>One-time deactivation</p>	<p>Shows the status of the keypad one-time deactivation setting:</p> <ul style="list-style-type: none"> • No – the keypad operates in the normal mode. • Lid only – notifications on the keypad tamper triggering are disabled until the first disarm. • Entirely – the keypad is entirely excluded from the operation of the system until the first disarm. The device does not execute system commands and does not report alarms or other events. <p><u>Learn more</u></p>
<p>Firmware</p>	<p>Keypad firmware version.</p>
<p>Device ID</p>	<p>Keypad ID. Also available on the QR code on the device enclosure and its package box.</p>
<p>Device No.</p>	<p>Number of the device loop (zone).</p>

Settings




To change the Superior KeyPad TouchScreen G3 Jeweller settings in an Ajax app:

1. Go to the **Devices**  tab.
2. Select **Superior KeyPad TouchScreen G3 Jeweller** from the list.
3. Go to **Settings** by clicking on the  icon.
4. Set the required parameters.
5. Click **Back** to save the new settings.

Setting	Value
Name	<p>Name of the keypad. Displayed in the list of hub devices, text of SMS and notifications in the events feed.</p> <p>To change the name of the device, click on the text field.</p>

	The name can contain up to 12 Cyrillic characters or up to 24 Latin characters.
Room	<p>Selecting the virtual room to which Superior KeyPad TouchScreen G3 Jeweller is assigned.</p> <p>The room name is displayed in the text of SMS and notifications in the events feed.</p>
Access settings	<p>Selecting the method of arming/disarming:</p> <ul style="list-style-type: none"> • Keypad codes only. • User codes only. • Keypad and user codes. <p>To activate the Keypad Access Codes set up for people who are not registered in the system, select the options on the keypad: Keypad codes only or Keypad and user codes.</p>
Keypad code	Selection of a general code for security control. Contains 4 to 6 digits.
Duress code	<p>Selecting a general duress code for silent alarm. Contains 4 to 6 digits.</p> <p><u>Learn more</u></p>
Screen detection range	<p>Configuring a distance at which the keypad reacts to approaching and turns on a display:</p> <ul style="list-style-type: none"> • Minimum • Low • Normal (by default) • High • Maximum

	Select the optimal sensitivity the keypad will respond to approaching as you prefer.
Mute fire alarm	<p>When enabled, users can mute Ajax fire detectors alarm (even Interconnected) with a keypad.</p> <div data-bbox="834 495 1403 758" style="border: 1px solid black; padding: 10px;"><p>If the fire alarm is triggered by ManualCallPoint Jeweller, and CO or smoke levels are critical, the alarm cannot be muted via the keypad.</p></div> <p><u>Learn more</u></p>
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	<p>Adjusting sensitivity of the keypad's Bluetooth module:</p> <ul style="list-style-type: none">• Minimum• Low• Normal (by default)• High• Maximum <p>Available if the Bluetooth toggle is enabled.</p>
Unauthorized access auto-lock	When enabled, the keypad will be locked for a pre-set time if an incorrect code is entered or



	<p>unverified access devices are used more than three times in a row within 1 minute.</p> <p>PRO or a user with the rights to configure the system can unlock the keypad through the app before the specified locking time expires.</p>
Auto-lock time, min	<p>Selecting the keypad lock period after unauthorized access attempts:</p> <ul style="list-style-type: none">• 3 minutes• 5 minutes• 10 minutes• 20 minutes• 30 minutes• 60 minutes• 90 minutes• 180 minutes <p>Available if the Unauthorized access auto-lock toggle is enabled.</p>
Chime managing with keypad	<p>When enabled, the user can activate/deactivate from the keypad display notifications about triggering the opening detectors. Enable additionally Chime on opening at keypad's settings and for at least one bistable detector.</p> <p><u>Learn more</u></p>
Firmware update	<p>Switches the device to the firmware updating mode.</p> <p>To update the firmware, <u>CONNECT</u> an external power supply to Superior KeyPad</p>

	<p>TouchScreen G3 Jeweller.</p> <p><u>Learn more</u></p>
Jeweller signal strength test	<p>Switches the device to the Jeweller signal strength test mode.</p> <p><u>Learn more</u></p>
Wings signal strength test	<p>Switches the device to the Wings signal strength test mode.</p> <p><u>Learn more</u></p>
Signal attenuation test	<p>Switches the device to the signal attenuation test mode.</p> <p><u>Learn more</u></p>
Pass/Tag reset	<p>Allows deleting all hubs associated with Tag or Pass from device memory.</p> <p><u>Learn more</u></p>
User guide	<p>Opens the Superior KeyPad TouchScreen G3 Jeweller user manual in an Ajax app.</p>
Permanent deactivation	<p>Allows the user to disable the device without removing it from the system.</p> <p>Three options are available:</p> <ul style="list-style-type: none"> • No – the device operates in normal mode and transmits all events. • Entirely – the device does not execute system commands and does not participate in automation scenarios, and the system ignores alarms and other device notifications.

	<ul style="list-style-type: none"> • Lid only – the system ignores the device tamper triggering notifications. <p><u>Learn more</u></p>
One-time deactivation	<p>Allows the user to disable events of the device until the first disarm.</p> <p>Three options are available:</p> <ul style="list-style-type: none"> • No – the device operates in normal mode. • Lid only – notifications on the device tamper triggering are disabled while the armed mode is active. • Entirely – the device is completely excluded from the operation of the system while the armed mode is active. The device does not execute system commands and does not report alarms or other events. <p><u>Learn more</u></p>
Delete device	<p>Unpairs the device, disconnects it from the hub, and deletes its settings.</p>

Security Management

Setting	Value
---------	-------




<p>Control screen</p>	<p>Activates/deactivates security control from the keypad.</p> <p>When disabled, the Control  tab is hidden from the keypad display. The user cannot control the security mode of the system and groups from the keypad.</p>
<p>Shared groups</p>	<p>Selecting which groups will be shared and available for management by all authorized users.</p> <p>All system groups and groups created after adding Superior KeyPad TouchScreen G3 Jeweller to the hub are shared by default.</p> <p>Available if <u>Group Mode</u> is enabled.</p>
<p>Pre-authorization</p>	<p>When enabled, to have access to the control panel and current system state, the user should authenticate first: enter a code or present a personal access device.</p>
<p>Authorization confirmation with a passcode</p>	<p>If enabled, system authorization using access devices requires confirmation of the action with a user code or keypad code.</p> <p>The user can also choose time for action confirmation.</p>
<p>Arming without code*</p>	<p>When enabled, the user can arm the system without entering a code or presenting the personal access device.</p> <p>If disabled, enter a code or present the access device to arm the system. The screen for entering code appears after pressing Arm  button.</p> <p>Available if the Authorization confirmation with a passcode and Pre-authorization toggle is disabled.</p>

<p>Easy armed mode change</p>	<p>When enabled, users can switch the armed mode of the system (or group) using access devices without confirmation with keypad buttons:</p> <ul style="list-style-type: none"> • Off – when every arming or disarming requires confirmation. • Arm/disarm using access device without confirming action by buttons – arming and disarming does not require keypad confirmation. Available if Group Mode is disabled or only 1 group is enabled in the Shared Groups menu. • Disarm without disarming button – allows for arming or disarming without keypad confirmation for the whole system or groups. Available if Codes length restrictions are enabled in hub's settings.
<p>Show malfunctions list on a screen</p>	<p>When enabled, the list of malfunctions preventing arming will appear on the keypad display. Enable system integrity check for this.</p> <p>It may take some time to display the list. This reduces the time of the keypad operation on the pre-installed batteries.</p>




** – when enabled, makes your system non-compliant with EN 50131 (Grade 2 and 3).*

Automation scenarios

Setting	Value
Scenarios management	Activates/deactivates scenarios management from the keypad.


	<p>When disabled, the Scenarios  tab is hidden from the keypad display. The user cannot control the automation scenarios from the keypad.</p>
Keypad scenarios	<p>The menu allows you to create up to six scenarios to control one automation device or a group of devices.</p> <p>When the settings are saved, buttons for managing scenarios appear on the keypad display (Scenarios  tab).</p> <p>A user or PRO with rights to configure the system can add or delete and turn on/off scenarios. Disabled scenarios don't appear on the Scenarios  tab of the keypad display.</p>
Pre-authorization	<p>When enabled, to have access to manage scenarios, the user should authenticate first: enter a code or present a personal access device.</p>

Emergency signals

Setting	Value
On-Screen emergency buttons	<p>When enabled, the user can send an emergency signal or call for help from the keypad Panic  tab.</p> <p>When disabled, the Panic  tab is hidden from the keypad display.</p>
Button type	<p>Selecting the number of buttons to display on the Panic  tab. Two options are available:</p> <ul style="list-style-type: none"> • Only the Panic button (by default).

	<ul style="list-style-type: none"> • Three buttons: Panic button, Fire, Auxiliary alert.
Accidental press protection	When enabled, sending an alarm requires additional confirmation from the user.
Alert with siren	
If panic button is pressed	When enabled, the <u>sirens</u> added to the system are activated when the Panic button is pressed.
If fire report button is pressed	<p>When enabled, the <u>sirens</u> added to the system are activated when the Fire button is pressed.</p> <p>The toggle is displayed if an option with three buttons is enabled in the Button type menu.</p>
If auxiliary request button is pressed	<p>When enabled, the <u>sirens</u> added to the system are activated when the Auxiliary alert button is pressed.</p> <p>The toggle is displayed if an option with three buttons is enabled in the Button type menu.</p>

Keypad notification center

Setting	Value
Event acknowledgement section	<p>When enabled the list of the latest event appear on the keypad display.</p> <p>The icon  will have a red badge in the upper right corner if there are new events.</p>

Display settings

Setting	Value
Auto adjust	The toggle is enabled by default. The display backlight brightness is automatically adjusted depending on the ambient light level.
Manual brightness adjustment	<p>Selecting the display backlight level: from 0 to 100% (0 – the backlight is minimal, 100 – the backlight is maximum). Sets in increments of 10%.</p> <p>The backlight is on when the display is active only.</p> <p>Manual adjustment is available when the Auto adjust toggle is disabled.</p>
Appearance	<p>Interface appearance adjustment:</p> <ul style="list-style-type: none">• Dark (by default).• Light
Always active display	<p>The keypad display always remains enabled when the toggle is enabled and the external power supply is connected.</p> <p>The toggle is disabled by default. In this case, the keypad sleeps after a certain time from the last interaction with the display.</p>
Armed mode indication	<p>Setting the LED indication of the keypad:</p> <ul style="list-style-type: none">• Never (by default) – the LED indication is off.• Only when armed – the LED indication turns on when the system is armed, and the keypad goes into sleep mode (the display turns off).

	<ul style="list-style-type: none"> • Always – the LED indication is switched on regardless of the security mode. It is activated when the keypad enters sleep mode. <p><u>Learn more</u></p>
Language	<p>Configuring the keypad interface language. English is set by default.</p> <p>To change the language, select the required one and click Save.</p>

Sound indication

Superior KeyPad TouchScreen G3 Jeweller has a built-in buzzer that performs the following functions depending on the settings:

1. Indicates the security status and also the Entry/Exit delays.
2. Chimes on opening.
3. Informs about alarms.



We do not recommend using Superior KeyPad TouchScreen G3 Jeweller instead of a siren. The keypad's buzzer is intended for additional notifications only. Meanwhile, 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.

Setting	Value
Beep settings	

Beep on armed mode changes	
Arming/disarming	<p>When enabled: an audible notification is sent if the security mode is changed via the keypad, another device, or an app.</p> <p>When disabled: an audible notification is sent if the security mode is changed via the keypad only.</p> <p>The volume of the beep depends on the configured buttons' volume.</p>
Night mode activation/deactivation	<p>When enabled: an audible notification is sent if the Night mode is activated/deactivated via the keypad, another device, or an app.</p> <p>When disabled: an audible notification is sent if the Night mode is activated/deactivated via the keypad only.</p> <p><u>Learn more</u></p> <p>The beep volume depends on the buttons' volume setting.</p>
Mute the device when code on keypad is being entered	<p>When this option is enabled, the keypad stops beeping once the user starts entering the code on it.</p>
Beep on delays	
Entry delays	<p>When enabled, the built-in buzzer beeps about an Entry delay.</p> <p><u>Learn more</u></p>
Exit delays	<p>When enabled, the built-in buzzer beeps about an exit delay.</p> <p><u>Learn more</u></p>

Entry delays in Night mode	<p>When enabled, the built-in buzzer beeps about an Entry delay in <u>Night mode</u>.</p> <p><u>Learn more</u></p>
Exit delays in Night mode	<p>When enabled, the built-in buzzer beeps about an exit delay in <u>Night mode</u>.</p> <p><u>Learn more</u></p>
Fast beep on delays	
Fast beep on Entry delay expiration	<p>Notifies a user that the Entry delay time is running out. There are 4 options to choose from when the fast beep should start:</p> <ul style="list-style-type: none"> • Never • Last 5 seconds • Last 10 seconds • Last 15 seconds
Fast beep on Exit delay expiration	<p>Notifies a user that the Exit delay time is running out. There are 4 options to choose from when the fast beep should start:</p> <ul style="list-style-type: none"> • Never • Last 5 seconds • Last 10 seconds • Last 15 seconds
Beep when disarmed	
Chime on opening or doorbell button press	<p>When enabled, the built-in buzzer informs you with a short beep that the opening detectors are triggered in the Disarmed system mode.</p>

	<u>Learn more</u>
Beep volume	<p>Selecting the built-in buzzer volume level for notifications about arming/disarming, entry/exit delay, and opening:</p> <ul style="list-style-type: none"> • Quiet • Loud • Very loud
Buttons	
Volume	Adjusting the buzzer notification volume for interactions with the keypad display.
Alarms reaction	
Audible alarm	<p>Setting the mode when the built-in buzzer enables an alarm:</p> <ul style="list-style-type: none"> • 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	<p>Selecting the group (from the shared) which alarm the keypad will notify. The All shared groups option is set by default.</p> <p>If the keypad has only one shared group and it is deleted, the setting will return to its initial value.</p> <p>Displayed if the <u>Group mode</u> is enabled.</p>

Alarm duration

Duration of sound signal in case of alarm:
from 3 seconds to 3 minutes.


The connection of external power supply to the keypad is recommended for an audible signal duration of more than 30 seconds.



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

[Learn more](#)

Firmware update

The Superior KeyPad TouchScreen G3 Jeweller firmware update can be installed when a new version is available. You can find out about it in the devices list in Ajax PRO: Tool for Engineers and Ajax PRO Desktop apps. If an update is available, the corresponding keypad will have an icon . An admin or a PRO with access to the system settings can run an update in the Superior KeyPad TouchScreen G3 Jeweller [states](#) or [settings](#). An update takes up to 1 or 2 hours (if the keypad operates via [ReX 2 Jeweller](#)).



To update the firmware, [connect](#) an external power supply unit to Superior KeyPad TouchScreen G3 Jeweller. Without an external power supply, an update won't be started.

If Superior KeyPad TouchScreen G3 Jeweller is not powered from an external power supply at the installation place, you can use a separate SmartBracket mounting panel for Superior KeyPad TouchScreen G3 Jeweller. To do this, remove the keypad from the main mounting panel and install it on a reserve panel connected to an external power supply with a voltage of 10.5–14 V[~] and a current of 0.5 A or more.

The mounting panel can be purchased separately from [authorized Ajax Systems partners](#).



Setting the keypad response to device alarms

Superior KeyPad TouchScreen G3 Jeweller can respond to alarms from each detector in the system with a built-in buzzer. The feature is useful when you do not need to activate the buzzer for the alarm of a specific device. For example, this can be applied to the triggering of 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 an 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 the device **Settings** by clicking on the  icon.
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.

Setting the keypad response to tamper alarm

Superior KeyPad TouchScreen G3 Jeweller can respond to tamper alarms from each system device with a built-in buzzer. When the feature 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 an 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. Click **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.

Setting the keypad response to pressing the panic button in Ajax apps

You can configure the keypad response to alarm when the panic button is pressed in Ajax apps. To do this, follow these steps:

1. Open an 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. Click **Back** to save the new settings.

Setting the keypad after-alarm indication



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 Superior KeyPad TouchScreen G3 Jeweller after-alarm indication does not work for always active detectors, if the detector was triggered when the system was disarmed.

To enable the Superior KeyPad TouchScreen G3 Jeweller after-alarm indication, in Ajax PRO app:

1. Go to hub settings:

- Hub → Settings  → Service → LED Indication.



2. Specify which events Superior KeyPad TouchScreen G3 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 Superior KeyPad TouchScreen G3 Jeweller in the **Devices** menu.
4. Click **Back** to save the parameters.

How to set Chime

If **Chime managing with keypad** is enabled, Superior KeyPad TouchScreen G3 Jeweller notify you 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 an Ajax app.
2. Go to the **Devices**  tab.
3. Select Superior KeyPad TouchScreen G3 Jeweller and go to its **Settings** .
4. Go to the **Sound indication** menu → **Beep settings**.

5. Enable the **Chime on opening or doorbell button press** toggle in the **Beep when disarmed** category.
6. Set the required notifications volume.
7. Click **Back** to save the settings.

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

To set the chime control from the keypad display:

1. Open an Ajax app.
2. Go to the **Devices**  tab.
3. Select Superior KeyPad TouchScreen G3 Jeweller and go to its **Settings** .
4. Enable the **Chime managing with keypad** toggle.

If the settings are made correctly, a bell icon appears in the **Control**  tab on the keypad display. Click it to activate/deactivate chime on opening.



Codes setting

Keypad access codes ▼

User access codes ▼

Unregistered user codes ▼

RRU Code ▼

Cards and key fobs adding

Superior KeyPad TouchScreen 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.

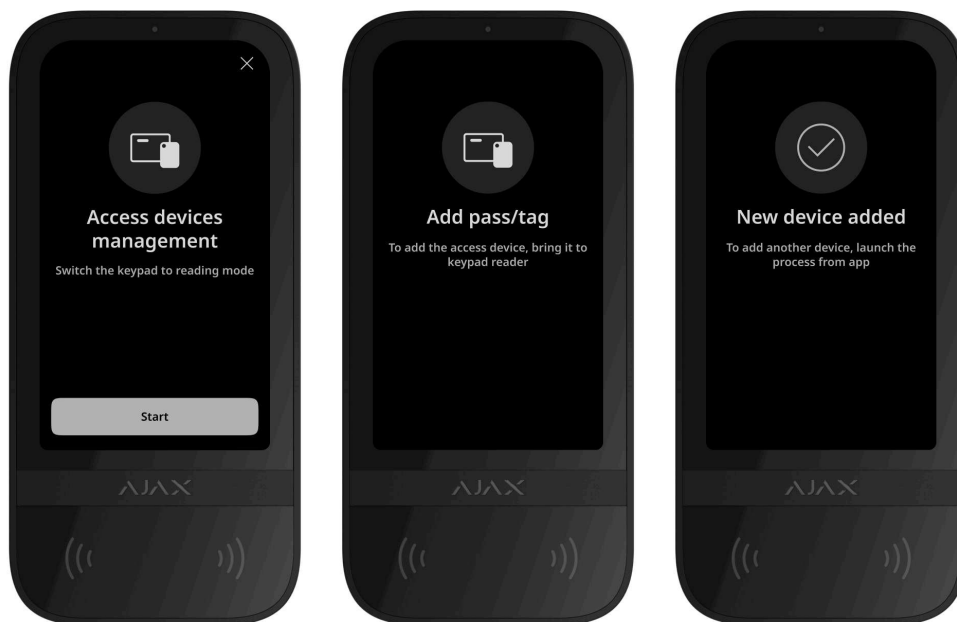
[This article](#) provides information on how to reset **Tag** or **Pass**.


The maximum number of connected Passes and Tags depends on the hub model. The connected Passes and Tags do not affect the total device limit on the hub.

Hub model	Number of Tag or Pass devices
<u>Hub 2 (2G)</u>	50

<u>Hub 2 (4G)</u>	50
<u>Hub 2 Plus</u>	200
<u>Superior Hub Hybrid (2G)</u>	50
<u>Superior Hub Hybrid (4G)</u>	50
<u>Superior Hub G3 Jeweller</u>	200
<u>Superior Hub Hybrid 2</u>	200
<u>Hub BP Jeweller</u>	50

How to add a Tag or Pass to the system



1. Open an Ajax app.
2. Select the hub to which you want to add a 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. Click **Next**. After that, the hub will switch to the device registration mode.
8. Go to any compatible keypad with **Pass/Tag reading** enabled and activate it.

After activation, Superior KeyPad TouchScreen G3 Jeweller will display a screen for switching the keypad to the access devices registration mode. Click the **Start** button.



A screen updates automatically if the external power supply is connected and the **Always active display** toggle is enabled in the keypad settings.

The screen for switching the keypad to the registration mode will appear on all Superior KeyPad TouchScreen G3 Jeweller of the system. When an admin or PRO with rights to configure the system starts registering Tag/Pass at one keypad, the rest will switch to their initial state.

9. Present Pass or Tag with the wide side to the keypad reader for a few seconds. It is marked with wave (☞) icons on the body. Upon successful addition, you will receive a notification in an Ajax app and on the keypad display.

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 an 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 bind a Tag or Pass to a hub that has already reached the hub limit, you will receive a corresponding notification. To bind such a key fob/card to a new hub, you will need to reset it.

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

How to delete a Tag or Pass from the hub




Resetting will delete all settings and bindings 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 an Ajax app.
2. Select the hub.
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. Click **Pass/Tag reset** menu.

7. Click **Continue**.

8. Go to any compatible keypad with **Pass/Tag reading** enabled and activate it.

After activation, Superior KeyPad TouchScreen G3 Jeweller will display a screen for switching the keypad to the access devices resetting mode. Click the **Start** button.



A screen updates automatically if the external power supply is connected and the **Always active display** toggle is enabled in the keypad settings.

The screen for switching the keypad to the resetting mode will appear on all Superior KeyPad TouchScreen G3 Jeweller devices of the system. When an admin or PRO with rights to configure the system starts resetting Tag/Pass at one keypad, the rest will switch to the initial state.

9. Put Pass or Tag with the wide side to the keypad reader for a few seconds. It is marked with wave (☞) icons on the body. Upon successful formatting, you will receive a notification in an Ajax app and on the keypad display. If the formatting fails, try again.

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

Bluetooth Setting


Superior KeyPad TouchScreen G3 Jeweller supports security modes control by presenting 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 passcode, add a phone to the keypad, or use a 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. Connect Superior KeyPad TouchScreen G3 Jeweller to the hub.
2. Enable the keypad Bluetooth sensor:

Devices  → **Superior KeyPad TouchScreen G3 Jeweller** → **Settings** 
→ Enable the **Bluetooth** toggle.

3. Click **Back** to save the settings.



To set up Bluetooth authentication

1. Open the Ajax Security System app and select the hub to which the Superior KeyPad TouchScreen G3 Jeweller with enabled Bluetooth authentication is added. By default, authentication with Bluetooth is available for all users of such a system.

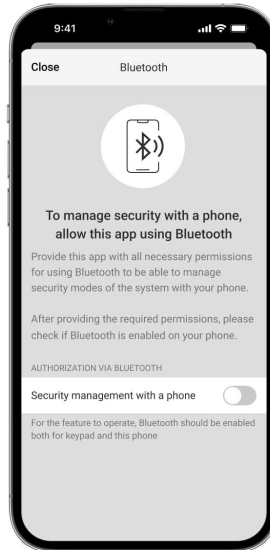


To prohibit Bluetooth authentication for certain users:

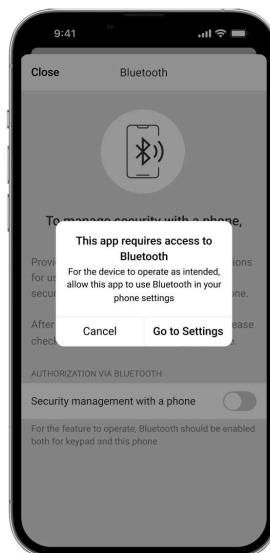
1. In the **Devices** tab, select the hub and go to its settings .
2. Open **Users** menu and the required user from the list.
3. In the **Permissions** section, disable the **Security management via Bluetooth** toggle.

2. Allow the Ajax Security System app to use Bluetooth if it was not previously granted. In this case, the warning  appears at Superior KeyPad TouchScreen G3 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.

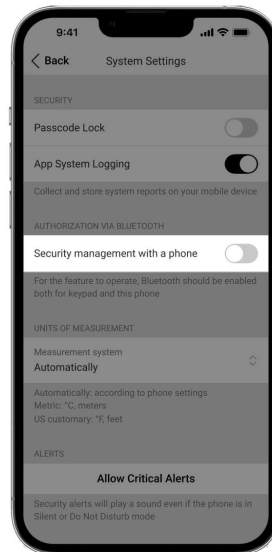


Grant the app permission to find and connect to nearby devices. The popup window for Android and iOS smartphones can differ.

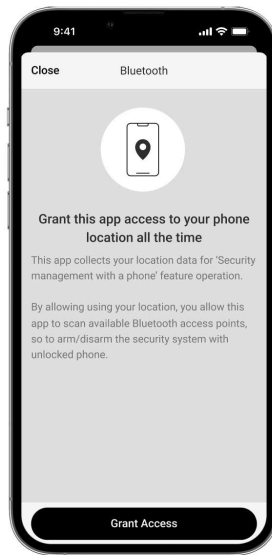


Also, the **Security management with a phone** toggle can be enabled in the app settings:

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








3. We recommend configuring **Geofence** for the stable performance of Bluetooth authentication. The warning ⚠ appears at Superior KeyPad TouchScreen G3 Jeweller **States** if **Geofence** is disabled and the app is not allowed to use the smartphone location. Pressing the ⓘ symbol opens the window with explanations of what to do.



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

You can control the system faster via Bluetooth, when the **Geofence** option is activated and configured. All you need 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**.


Pre-authorization

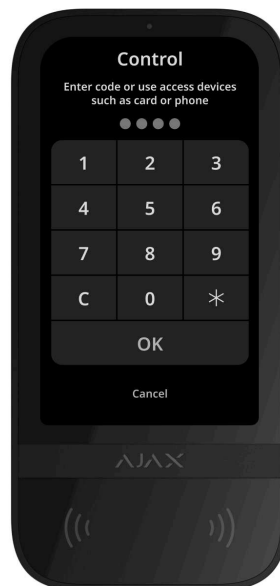
When the feature is enabled, access to the control panel and current system state is blocked. To unblock it, the user should authenticate: enter an appropriate code or present a personal access device to the keypad.




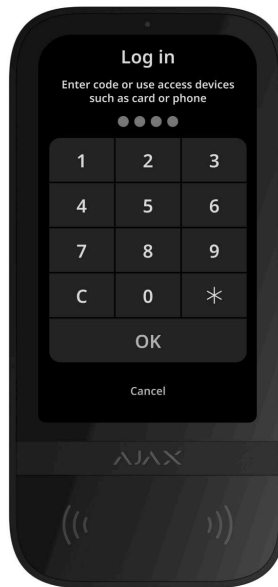
If pre-authorization is enabled, the **Arming without code** feature is unavailable in the keypad settings.

You can authenticate in two ways:

1. In the **Control**  tab. After login, the user will see the shared groups of the system (if Group Mode is activated). They are specified in the keypad settings: **Security management** → **Shared groups**. By default, all the system groups are shared.



2. In the **Log in**  tab. After login, the user will see available groups that were hidden from the shared group list.



The keypad display switches to the initial screen after 10 seconds from the last interaction with it. Enter the code or present a personal access device again to control the system with Superior KeyPad TouchScreen G3 Jeweller.

Pre-authorization with a keypad code



Pre-authorization with a personal code



Pre-authorization with an access code



Pre-authorization with a RRU code



Pre-authorization with Tag or Pass



Pre-authorization with a smartphone



Controlling security

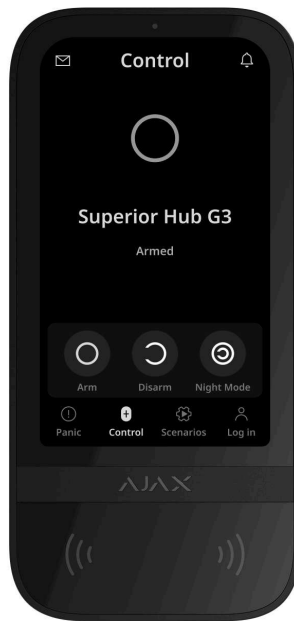
Using codes, Tag/Pass, or a smartphone, you can control the **Night mode** and the security of the entire system or separate groups. The user or PRO with the rights to configure the system can set up access codes. This chapter provides information on how to add Tag or Pass to the hub. To control with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





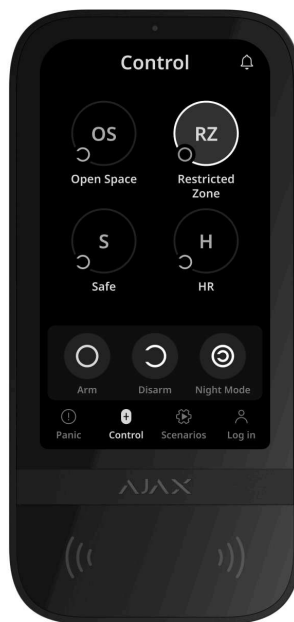
Superior KeyPad TouchScreen G3 Jeweller is locked for the time specified in the settings if an incorrect code is entered, or an unverified access device is presented three times in a row within 1 minute. The corresponding notifications are sent to users and the monitoring station of the security company. A user or PRO with the rights to configure the system can unlock Superior KeyPad TouchScreen G3 Jeweller in Ajax apps.

If Group mode is disabled, an appropriate icon on the keypad display indicates the current security mode:

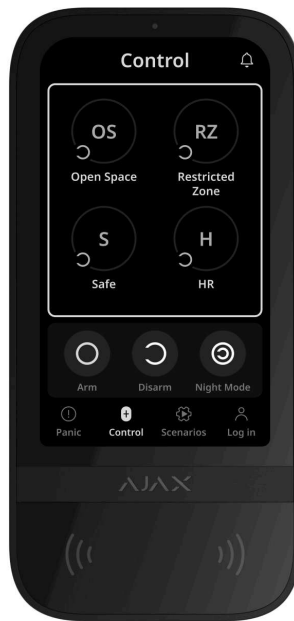
- – Armed.
- – Disarmed.
- – Night Mode.



If **Group mode** is enabled, users see the security mode of each group separately. The group is armed if its button outline is white and marked with the  icon. The group is disarmed if its button outline is grey and marked with the  icon.



The buttons of the groups in the **Night mode** are framed in a white square on the keypad display.



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

The step sequence to change the security mode with the keypad depends on whether user pre-authorization is enabled in the Superior KeyPad TouchScreen G3 Jeweller settings.

If pre-authorization is enabled

Security control of the system



Security control of the group



Using a duress code



If pre-authorization is disabled

Security control of the system



Security control of the group



Using a duress code



Example of entering codes

Code	Example	Note
Keypad code Keypad duress code	1234 → OK	Incorrectly entered numbers can be cleared with the C button.
User code User duress code	2 → * → 1234 → OK	Enter the <u>user ID</u> first, press the * button, and then enter a personal code. Incorrectly entered numbers can be cleared with the C button.
Code of unregistered user Duress code of unregistered user	1234 → OK	Incorrectly entered numbers can be cleared with the C button.
RRU Code	1234 → OK	Incorrectly entered numbers can be cleared with the C button.

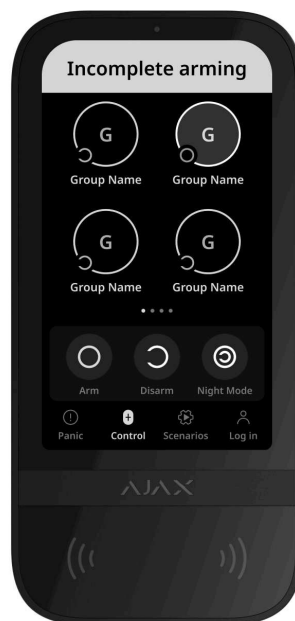
Easy armed mode change

Easy armed mode change feature allows you to change the security mode to the opposite using Tag/Pass or smartphone, without confirmation with the Arm or Disarm buttons. Go to the keypad settings to enable the feature.

To change the security mode to the opposite

1. Activate the keypad by approaching it or holding your hand in front of the sensor. Perform pre-authorization if necessary.
2. Present Tag/Pass or smartphone.

Two-stage arming



Superior KeyPad TouchScreen G3 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 smartphone is similar to using a personal or general code on the keypad.

Learn more

The system users can see whether the arming is started or incomplete on the keypad display. If Group Mode is activated, the color of the group buttons depends on the current state:

- **Grey** – disarmed, arming process not started.
- **Green** – arming process started.
- **Yellow** – arming is incomplete.
- **White** – armed.


Managing scenarios with the keypad


Superior KeyPad TouchScreen G3 Jeweller allows users to create up to six scenarios of two types. The **Scenario with preset action** scenario type enables control of one or more automation devices and Ajax WaterStop Jeweller. The **Device control** scenario type allows users to switch the state of a single automation device or **Ajax WaterStop Jeweller** from the keypad's **Scenarios** tab.


Starting with **OS Malevich 2.38** after authorization on the keypad the system records which user initiated an automation scenario from the keypad. This information is displayed in the hub event feed.

Scenario with preset action Device control


To create a scenario:


1. Open an Ajax app. Select the space with at least one Superior KeyPad TouchScreen G3 Jeweller and automation device. Add one if necessary.
2. Go to the **Devices**  tab.

3. Select Superior KeyPad TouchScreen G3 Jeweller from the list and go to the **Settings**  menu.
4. Go to the **Automation scenarios** menu. Enable the **Scenarios management** toggle.
5. Open the **Keypad scenarios** menu.
6. Press **Add scenario**.
7. Select the **On preset action** scenario type.
8. Select one or more automation devices. Press **Next**.
9. Enter the scenario name in the **Name** field.
10. Select the preferred device action during scenario execution.
11. Press **Save**.
12. Press **Back** to return to the **Automation scenarios** menu.
13. If necessary, activate the **Pre-authorization** toggle.

Created scenarios are displayed in the app: **Superior KeyPad TouchScreen G3 Jeweller** → **Settings**  → **Automation scenarios** → **Keypad scenarios**. You can turn them off, adjust settings, or delete them at any time.

To remove a scenario:

1. Go to the **Settings**  of Superior KeyPad TouchScreen G3 Jeweller.
2. Open **Automation scenarios** → **Keypad scenarios** menu.
3. Select the scenario you want to remove.
4. Press **Next**.
5. Press **Delete scenario**.

The user can see and manage automation scenarios after authentication when the **Pre-authorization** feature is enabled. Go to the **Scenarios**  tab,

enter the code or present a personal access device to the keypad.

To perform a scenario, press an appropriate button in the **Scenarios**  tab.




The Superior KeyPad TouchScreen G3 Jeweller display shows only activated scenarios in the keypad settings.

Indication

Superior KeyPad TouchScreen G3 Jeweller informs users about alarms, entry/exit delays, current security mode, malfunctions, and other system states with:

- display;
- logo with an LED indicator;
- built-in buzzer.

Superior KeyPad TouchScreen G3 Jeweller indication is shown on the display only when it is active. Icons that indicate some system or keypad states are displayed in the upper part of the **Control**  tab. For example, they can indicate a fire alarm, system restoration after an alarm, and chime on opening. Information about the security mode will be updated even if it is changed by another device: key fob, another keypad, or in the app.

Event	Indication	Note
-------	------------	------

Alarm	The built-in buzzer emits an acoustic signal.	<p>If Activate keypad buzzer if alarm in the system is detected toggle is enabled.</p> <p>The duration of the acoustic signal depends on the keypad settings.</p>
An alarm was detected in the armed system	The LED indicator flashes twice approximately every 3 seconds until the system is disarmed.	<p>To activate, enable the <u>after-alarm indication</u> in the hub settings. Also, specify Superior KeyPad TouchScreen G3 Jeweller as a device for informing about other devices' alarms.</p> <p>The indication turns on after the built-in buzzer has completed playing the alarm signal.</p>
Switching on the device>Loading the updated system configuration to the keypad	An appropriate notification is shown on the display while the data is loading.	
Switching off the device	The LED indicator lights up for 1 second, then flashes three times.	
The system or the group is armed	The built-in buzzer emits a short beep.	If notifications for Arming/disarming are enabled.
The system or the group is switched to the Night mode	The built-in buzzer emits a short beep.	If notifications for Night Mode Activation/Deactivation are enabled.

<p>The system is disarmed</p>	<p>The built-in buzzer emits two short beeps.</p> <p>The LED indicator's light is constantly green if the external power is connected.</p>	<p>If notifications for Arming/disarming are enabled.</p>
<p>System in the armed mode</p>	<p>The LED indicator lights up red for a short time every 3 seconds if the external power is not connected.</p> <p>The LED indicator constantly lights up red if the external power is connected.</p>	<p>If Armed mode indication is enabled.</p> <p>The indication turns on when the keypad switches to sleep mode (the display goes out).</p>
<p>An incorrect code was entered</p>	<p>An appropriate notification is shown on the display.</p> <p>The built-in buzzer emits a short beep (if adjusted).</p>	<p>The beep loudness depends on the configured buttons' volume.</p>
<p>Error when adding a card/key fob</p>	<p>An appropriate notification is shown on the display.</p> <p>The LED indicator lights up red once.</p> <p>The built-in buzzer emits a long beep.</p>	<p>The beep loudness depends on the configured buttons' volume.</p>
<p>Successfully added card/key fob</p>	<p>An appropriate notification is shown on the display.</p> <p>The built-in buzzer emits a short beep.</p>	<p>The beep loudness depends on the configured buttons' volume.</p>
<p>Low battery</p>	<p>The LED indicator smoothly lights up and goes out when the tamper is triggered, an alarm is activated, or the system is armed or disarmed</p>	



	(if the indication is activated).	
Tamper triggering	The LED indicator lights up red for 1 second.	
Jeweller/Wings signal strength test	The LED indicator lights up green during the test.	Turns on after launching an appropriate test in the <u>keypad settings</u> .
Firmware update	The LED indicator periodically lights up green while the firmware is updating.	Turns on after launching the firmware update in the keypad <u>States</u> .
Muting interconnected fire alarm	An appropriate notification is shown on the display. The built-in buzzer emits an acoustic signal.	
The keypad is deactivated	An appropriate notification is shown on the display.	If Entirely option is selected for the <u>Permanent</u> or <u>One-Time Deactivation</u> keypad settings.
System restoration is required	An appropriate screen to restore or send a request for the system restoration after the alarm appears on the display.	The <u>Restoration after alarm feature</u> has to be adjusted in the system. The screen appears when arming or switching the system to the Night mode if an alarm or malfunction occurred in the system before. Admins or PROs with the rights to configure the system can restore the system. Other users can send a request for restoration.

Counting Entry/Exit delays (if Beep on delays is enabled)	The LED indicator and beep sounds turn on simultaneously if the Fast beep on delays feature is enabled.	LED indicator lights up red for Entry delays and green for Exit delays .
--	--	--

Sound notifications of malfunctions

If any device is offline or the battery is low, Superior KeyPad TouchScreen G3 Jeweller can notify system users with an audible sound. The keypad's LED indicator will also flash. Malfunction notifications will be displayed in the events feed, SMS, or push notification.

To enable sound notifications of malfunctions, use Ajax PRO and Ajax PRO Desktop apps:

1. Click **Devices** , choose hub and open its settings :

Click **Service** → **Sounds and alerts**.

2. Enable toggles: **If battery of any device is low** and **If any device is offline**.


3. Click **Back** to save settings.

Event	Indication	Note
If any device is offline	Two short sound signals, LED indicator flashes twice. Beep occurs once per minute until all devices in the system are online.	Users can delay sound indication for 12 hours.
If Superior KeyPad TouchScreen G3 Jeweller is	Two short sound signals, LED indicator flashes twice.	Sound indication delay is not possible.



offline	Beep occurs once per minute until the keypad in the system is online.	
If the battery of any device is low	<p>Three short sound signals, LED indicator flashes three times.</p> <p>Beep occurs once per minute until the battery is restored or the device is removed.</p>	Users can delay sound indication for 4 hours.

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

Functionality testing

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

To run a test, in the Ajax app:

1. Select the required space.
2. Go to the **Devices**  tab.
3. Select **Superior KeyPad TouchScreen G3 Jeweller** from the list.
4. Go to **Settings** .
5. Select a test:
 1. Jeweller signal strength test
 2. Wings signal strength test

3. Signal attenuation test

6. Run the test.

Device placement



The device is designed for indoor use only.

When choosing a location for the device, consider the parameters that affect its operation:



- Jeweller and Wings signal strength.
- Distance between the keypad and the hub or range extender.
- Presence of obstacles for radio signal passage: walls, interfloor ceilings, large objects located in the room.

Consider the recommendations for placement when developing a security system project for your facility. The security system must be designed and installed by specialists. A list of recommended partners is [available here](#).

Superior KeyPad TouchScreen G3 Jeweller is best placed indoors near the entrance. This allows disarming the system before the entry delays have expired and quickly arming the system when leaving the premises.

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

Signal strength

The Jeweller and Wings signal strength is determined by the number of undelivered or corrupted data packages over a certain period of time. The icon  on the **Devices**  tab indicates the signal strength:

- **Three bars** – excellent signal strength.
- **Two bars** – good signal strength.
- **One bar** – low signal strength, stable operation is not guaranteed.
- **Crossed out icon** – no signal.



Check the Jeweller and Wings signal strength before final installation. With a signal strength of one or zero bars, we do not guarantee stable operation of the device. Consider relocating the device as repositioning even by 20 cm can significantly improve the signal strength. If there is still poor or unstable signal after the relocation, use [ReX 2 Jeweller](#) radio signal range extender. **Superior KeyPad TouchScreen G3 Jeweller is not compatible with ReX radio signal range extenders.**

Where the keypad cannot be installed

1. Outdoors. This can lead to keypad failure.
2. In places where parts of clothing (for example, next to the hanger), power cables or Ethernet wire may obstruct the keypad. This can lead to false triggering of the keypad.
3. Nearby any metal objects or mirrors causing attenuation and screening of the signal.
4. Inside premises with temperature and humidity outside the permissible limits. This could damage the keypad.
5. Closer than 1 meter from the hub or radio signal range extender. This can lead to a loss of communication with the keypad.
6. In a place with a low signal level. This may result in the loss of the connection with the hub.

7. Near the glass break detectors. The built-in buzzer sound may trigger an alarm.
8. In places where the acoustic signal can be attenuated (inside furniture, behind thick curtains, etc.).

Installation



Before installing Superior KeyPad TouchScreen G3 Jeweller, ensure that you have selected the optimal location that complies with the requirements of this manual.

To mount a keypad:

1. Remove the SmartBracket mounting panel from the keypad. Unscrew the holding screw first and slide the panel down.
2. Fix the SmartBracket panel using double-sided tape to the selected installation spot.



Double-sided 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 will not be triggered when the device is detached from the surface.



SmartBracket has markings on the inner side for easy installation. The intersection of two lines marks the center of the device (not the attachment panel). Orient them when installing the keypad.



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



If the LED indicator doesn't light up during placing on SmartBracket, check the tamper status in an Ajax app, the integrity of the fastening, and the tightness of the keypad fixation on the panel.

4. Run the Jeweller and Wings signal strength tests. The recommended signal strength is two or three bars. If the signal strength is low (a single bar), we do not guarantee stable operation of the device. Consider relocating the device, as repositioning even by 20 cm can significantly improve the signal strength. If there is still poor or unstable signal after the relocation, use ReX 2 Jeweller radio signal range extender.
5. Run Signal attenuation test. During the test, the signal strength can be reduced and increased to simulate different conditions at the installation location. If the installation spot is chosen correctly, the keypad will have a stable signal strength of 2–3 bars.
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. The screw is needed for more reliable fastening and protection of the keypad from quick dismantling.



Connecting a third-party power supply unit

When connecting a third-party power supply unit and using Superior KeyPad TouchScreen G3 Jeweller, follow the general electrical safety regulations for using electrical appliances, as well as the requirements of regulatory legal acts on electrical safety.

Superior KeyPad TouchScreen G3 Jeweller is equipped with terminals for connecting a 10.5 V–14 V_{DC} power supply unit. Recommended electrical parameters for the power supply unit are: 12 V_{DC} with a current of at least 0.5 A.



We recommend connecting an external power supply when you need to keep a display always active and to avoid rapid battery discharge, for example, when using the keypad in premises with low temperatures. **An external power supply is also required for [updating the keypad firmware](#).**

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

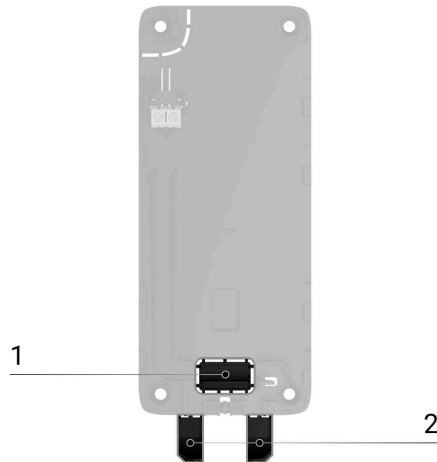
supply.



Before installing the device, make sure to 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 a third-party power supply unit:

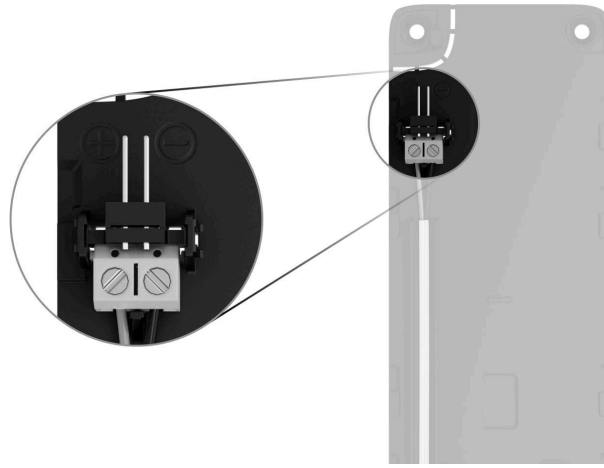
1. Remove the SmartBracket mounting panel. Carefully break out the perforated enclosure part to prepare the holes for the cable:



1 – to output the cable through the wall.

2 – to output the cable from the bottom. It is enough to break out one of the perforated parts.

2. De-energize external power supply cable.
3. Connect the cable to the terminals by observing polarity (marked on the plastic).



4. Route the cable in the cable channel. An example of how to output the cable from the bottom of the keypad:



5. Turn on the keypad and place it on the mounting panel.
6. Check the status of batteries and external power in an Ajax app and the overall operation of the device.



For an INCERT-compliant system, do not connect the third-party power supply unit to Superior KeyPad TouchScreen G3 Jeweller.

Maintenance

Regularly check the functioning of Superior KeyPad TouchScreen G3 Jeweller. The optimal frequency of checks is once every three months. Clean the device enclosure of dust, cobwebs, and other contaminants as they emerge. Use soft, dry wipes suitable for equipment maintenance.

Do not use substances that contain alcohol, acetone, petrol, and other active solvents to clean the device. Gently wipe the touch screen.

The device runs for up to 1.5 years on the pre-installed batteries – a calculated value based on default settings and up to 4 daily interactions with the keypad.

The system will send an early warning when it's time to replace the batteries. When changing the security mode, the LED will slowly light up and go out.

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 the 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