Superior MotionProtect G3 Jeweller user manual

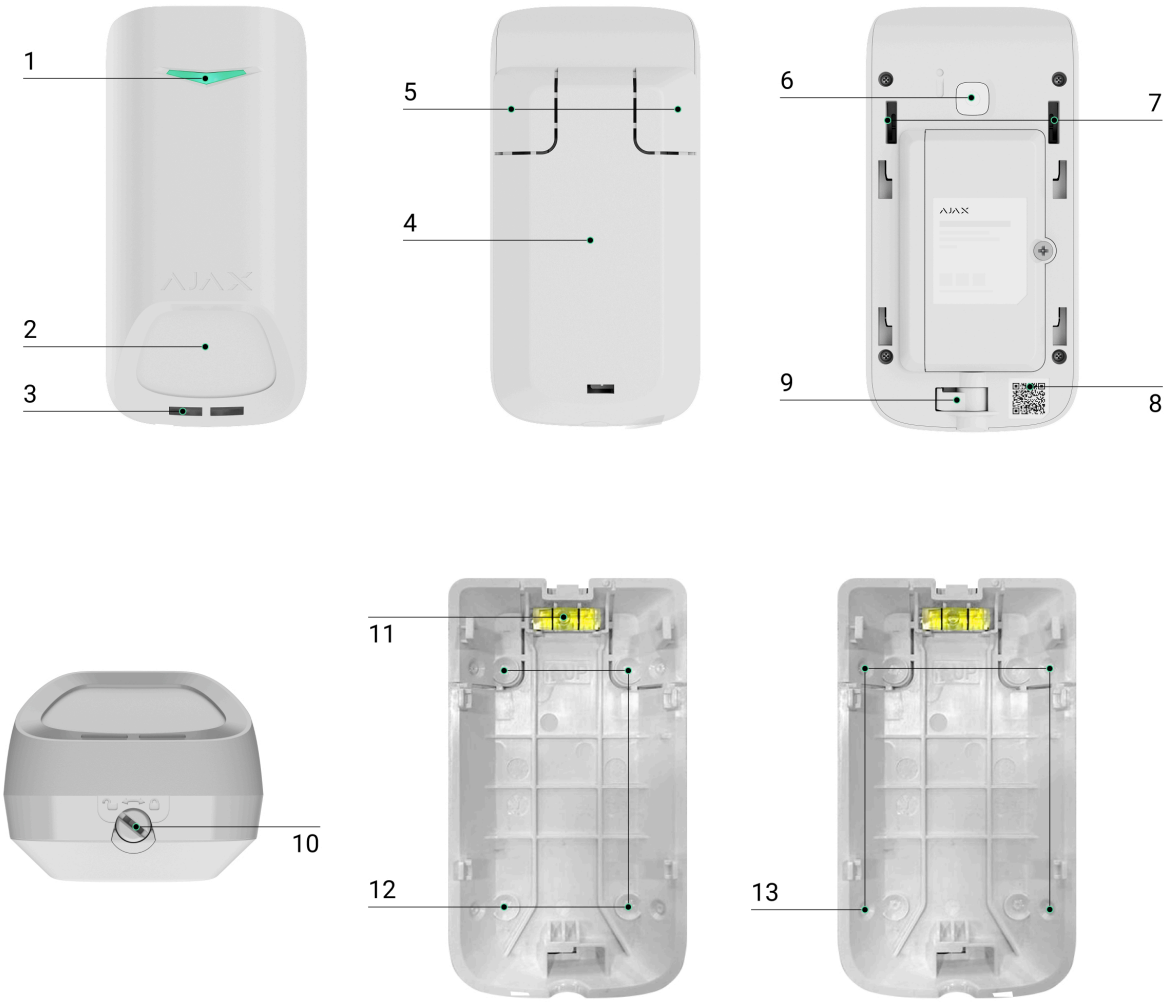
Updated January 21, 2026

Superior MotionProtect G3 Jeweller is a wireless motion detector. It detects motion at a distance of up to 15 m and features an anti-masking system that detects attempts to block the detector's field of view. The device is designed for indoor use only and complies with EN 50131 (Grade 3) requirements.

Superior MotionProtect G3 Jeweller communicates with the hub using two secure protocols: **Jeweller** to transmit alarms and events, and **Wings** to update the firmware. The communication range in open space is up to 3,000 m.

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

Functional elements



1. LED indicator.

2. Sensitive area of the detector’s IR motion sensor.

3. Masking sensor.

4. SmartBracket mounting panel. To remove the panel, slide it down.

5. Perforated parts of the mounting panel. They are necessary for a tamper button to trigger in case of any attempt to detach the detector from the

surface. Do not break them off.

6. Power button.
7. **Tamper buttons**.
8. QR code with the device ID. It is used to add the device to the hub.
9. Latch with the tamper button on the SmartBracket's lock.
10. SmartBracket's lock. It is used to fix the device on the SmartBracket mounting panel.
11. Bubble level for checking the inclination angle of the mount during installation.
12. Places for drilling holes to mount the device on the surface.
13. Places for drilling holes to mount the device on the corner.

Compatible hubs and range extenders

The device requires an Ajax hub with **OS Malevich 2.35** or later.

☞ **Check devices compatibility**

Operating principle

Superior MotionProtect G3 Jeweller is a wireless IR motion detector with an anti-masking system. It identifies intrusions by detecting moving objects with temperatures close to that of the human body.

In case of an alarm, it instantly sends an alarm to the hub, activating the sirens connected to the system, triggering **scenarios**, and notifying users and the security company. All Superior MotionProtect G3 Jeweller alarms and events are recorded in the event feed of the Ajax apps.

Users and the monitoring company know exactly where motion is detected. The notifications contain the name of a **space** (the name of a guarded facility), the device name, and the **virtual room** to which the device is assigned.

The detector does not switch to armed mode instantly. The switching time depends on the delay when leaving (specified in the **device settings**) and the hub–detector polling interval. The polling interval specified in the Jeweller settings is **36 seconds** by default. In the first case, the delay is set by a user or a PRO with admin rights. In the second case, the delay occurs because the hub takes one polling interval to notify the detector about the security mode change.

How Ajax notifies users of alarms

More about Ajax motion detectors

Protection against false alarms

Superior MotionProtect G3 Jeweller uses the **SmartDetect algorithm** to protect against false alarms. This algorithm allows the detector to analyze the thermal diagram read by the sensor: the intensity of infrared radiation, size of the heat spot, time spent in the detection area, and other parameters.

Temperature compensation

Due to temperature compensation, the detector responds to movements, even if the temperature at the facility is close to the human body temperature. Read more about temperature compensation in **the article**.

Anti-masking system

Masking is an attempt to block the view of the detector. Superior MotionProtect G3 Jeweller detects the following types of masking:

- An obstacle in front of the detector's motion sensor sensitive area.
- Painting over the detector's motion sensor sensitive area.
- Taping the detector's motion sensor sensitive area.

The system notifies users and the security company's monitoring station about masking. The maximum masking detection time is up to 120 s (depending on the obstacle type and the distance to it).

If the **Anti-masking** feature is enabled, it is always active and works regardless of the security mode.

 Learn more

Superior Jeweller data transfer protocols

Superior Jeweller is an upgraded radio protocol for Superior devices, ensuring compliance with EN 50131 (Grade 3). 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 operates via the regular Jeweller protocol, the system will be limited to Grade 2: encryption remains, but frequency hopping is disabled. Superior devices can also operate using the regular Jeweller protocol, depending on the hub.

 Learn more

Advanced encrypted communication

Communication between Superior MotionProtect 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 verify 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 the hub, as well as reliable system and data protection.

Frequency hopping

To comply with the Grade 3 requirements, Superior MotionProtect 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 **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 MotionProtect G3 Jeweller can transmit the following events:

1. Motion alarm.
2. Masking alarm.
3. IR sensor malfunction/recovery.
4. Masking sensor malfunction/recovery.

5. Tamper alarm. Tamper recovery.
6. Low battery alarm/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 **PRO Desktop** or the CMS, the type of the device, its name, security group, and virtual room. The list of transmitted parameters may differ depending on the type of CMS and the selected communication protocol.

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

Selecting the installation site

When choosing where to place Superior MotionProtect G3 Jeweller, consider the parameters that affect its operation:

- **Jeweller and Wings signal strength**.
- The distance between the device and the hub.
- **Detection zone**.
- The presence of objects or structures that can obstruct the detector's view.

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**.

Signal strength

The signal strength is the ratio of undelivered or corrupted data packages to those expected over a specific 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; stable operation is not guaranteed.

Note that if the signal strength is excellent, the device can automatically adjust the radio transmission power to reduce power consumption and radio interference.

Run the Jeweller and Wings signal strength test before final installation. The test checks the signal strength at the device's maximum transmission power. If the test shows the signal strength of one or zero bars, we do not guarantee the device will operate stably. Consider relocating it, as adjusting its position even by 20 cm or rotating it relative to the hub 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 the Jeweller and Wings signal strength tests.

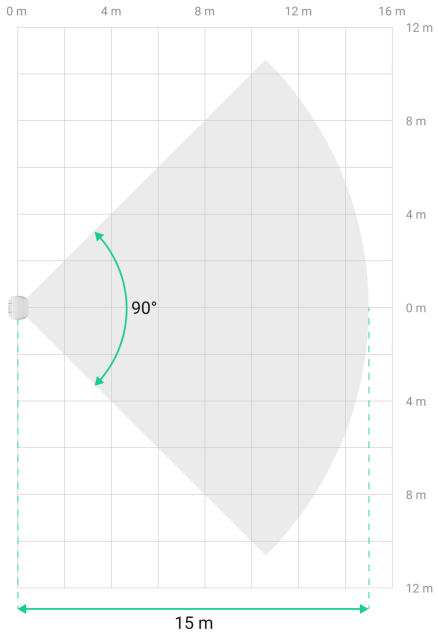
What is Jeweller signal strength test

What is Wings signal strength test

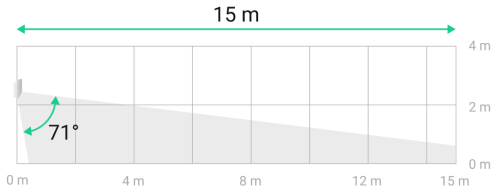
Motion detector detection area

The location of the detector determines the area to be monitored and the effectiveness of the security system. When selecting the installation place, consider the direction of the detector sensors, viewing angles, and the presence of obstacles to the detector's view.

The detector can recognize motion at a distance of up to 15 m. The direction of the detector sensors should be perpendicular to the intended entry path into the premises. Ensure that furniture, house plants, vases, and decorative or glass elements do not obstruct the view of the detector.



Horizontal characteristics of the motion detection area



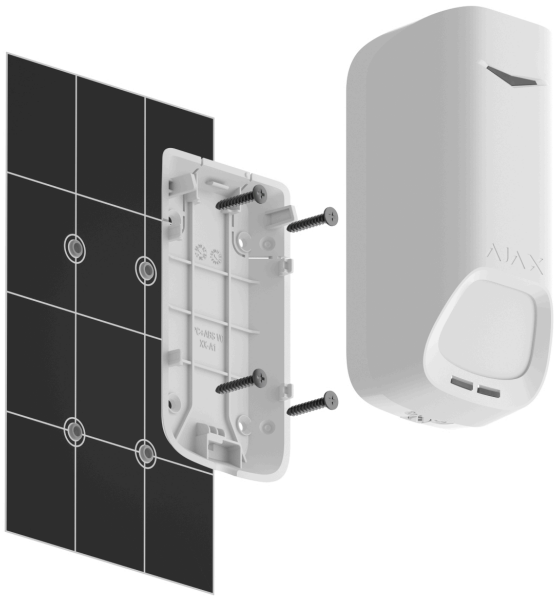
Vertical characteristics of the motion detection area

When installing the detector, perform the **Detection zone test**. This allows you to check the operation of the device and accurately determine the sector in which the detector registers motion.

Where not to install the device

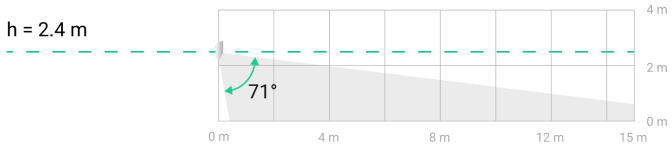
1. Outdoors. This could damage the device.
2. In places where objects and structures may obstruct the detector's view. For example, behind a flower or a column.
3. In places where glass structures may obstruct the detector's view; it doesn't register movement behind glass.
4. Inside premises with temperature and humidity outside the **permissible limits**. This could damage the device.
5. In places with low or unstable Jeweller signal strength.
6. Closer than 1 m to the hub or radio signal range extender.

Installation

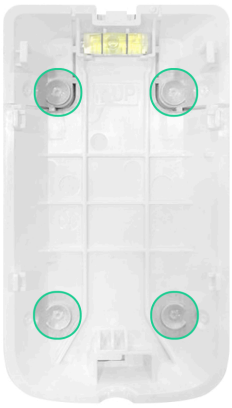


Before installing Superior MotionProtect G3 Jeweller, ensure that you have chosen the optimal location that complies with the requirements of this manual.

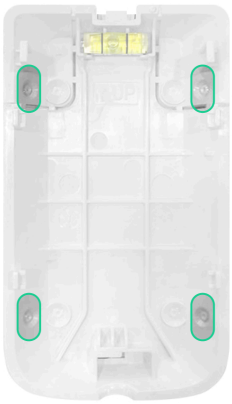
1. Remove the SmartBracket mounting panel from the detector.
2. Temporarily secure the SmartBracket panel to a vertical surface or corner using double-sided adhesive tape or other temporary fasteners. This is necessary for testing the detector. The installation height is 2.4 m.



3. **Add the detector to the system**.
4. Place the detector on the SmartBracket mounting panel and lock it.
5. Run the **functionality testing**.
6. If the detector passes the tests, fix the SmartBracket mounting panel to a vertical surface with bundled screws. Use at least two fixing points (one is in the perforated part of the mount above the tamper). The tamper reacts if someone tries to break or open the lid of the enclosure — the notification about this is sent to Ajax apps.



To fix SmartBracket on the corner, screw the bundled fasteners to the side recesses. Use at least two fixing points (one is in the perforated part of the mount above the tamper).



When using other mounts, make sure they do not damage or deform the mounting panel.

Double-sided adhesive tape can be used for temporary fastening as the device can come unglued from the surface at any time. As long as the device is taped, the tamper will not be triggered when the detector is detached from the surface.

7. Put the detector on the SmartBracket mounting panel and lock it. The lock for SmartBracket has a tamper and is needed to securely fix the detector and protect it from quick dismantling. The tamper responds if

someone tries to unlock the lock for SmartBracket, and the notification about this is sent to Ajax apps.

Adding to the system

Check the device compatibility before the detector 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 a QR code or enter the device ID manually. The QR code with the device 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.

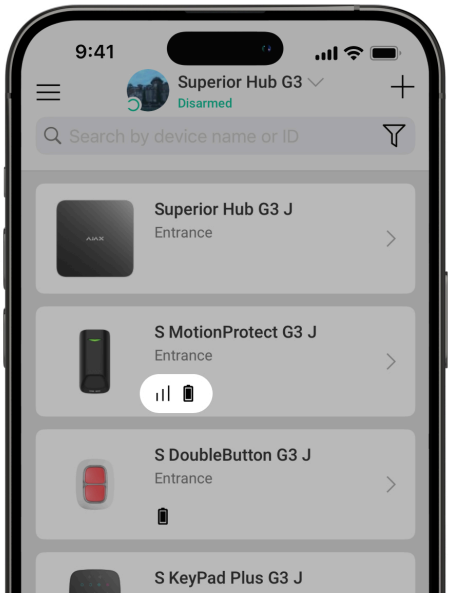
Superior MotionProtect G3 Jeweller works with only one hub. When paired with a new hub, it stops sending events to the old one. Adding the detector to a new hub does not automatically remove it from the device list of the old hub. This must be done through the Ajax app.

Functionality testing

The Ajax system offers several types of tests to help select the correct installation place for the devices. Available for Superior MotionProtect G3 Jeweller:

- **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.
- **Detection zone test** — to check how the detector responds to **motion** and **masking** at the device installation site.
- **Calibration of masking sensor** — to register the detector's field of view characteristics at the installation site. These characteristics will be used as a reference for masking detection.
- **Device self-test** — to check if all detector's built-in sensors operate properly.

Icons



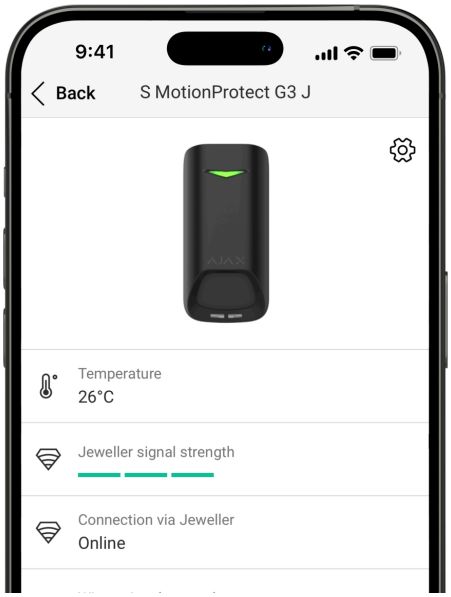
Icons in the Ajax app display some of Superior MotionProtect G3 Jeweller states. The icons can be checked in the **Devices** tab.

Icon	Meaning
	Jeweller signal strength — displays the signal strength between the hub and the device. Recommended values: 2–3 bars. Learn more
	Battery charge level of the device. Learn more
	The device is in the signal attenuation test mode. Learn more
24	The device operates in the **Always active** mode. Learn more

	The device operates via the radio signal range extender. **Learn more**
	A firmware update is available. Go to the device states or settings to find the description and launch an update.
Updating	A firmware update is in progress: downloading/installing the latest version.
	New firmware installation has failed.
	The lock for SmartBracket is unlocked.
	Entry/exit delay is enabled. **Learn more**
	The device operates in **Night mode**. **Learn more**
	The masking is detected.
	The device is automatically disabled due to exceeding the number of alarms. **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 first disarming of the system. **Learn more**
Offline	The device has lost connection with the hub, or the hub has lost connection with the Ajax Cloud server.
Not transferred	The device has not been transferred to the new hub. **Learn more**

States



The states include information about the device and its operating parameters. The states of Superior MotionProtect G3 Jeweller can be found in Ajax apps:

1. Go to the **Devices** tab.

2. Select **Superior MotionProtect G3 Jeweller** in the list.

Parameter	Value
New firmware version available	Tap on ⓘ to open instructions for updating the device firmware. The field is displayed if a new firmware version is available.
Sensor calibration failed	Displays the masking sensor calibration error. Tap ⓘ to open additional information about device calibration.
Malfunction	Tapping on ⓘ opens the list of device malfunctions. The field is displayed only if a malfunction is detected.
Data import	Displays the error when the data is being transferred to the new hub: • **Failed** — the device has not been transferred to the new hub. **Learn more**
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	The state of the connection via the 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.
Wings signal strength	Wings signal strength between the device and the hub (or the range extender). The recommended value is 2–3 bars. Wings is a protocol for updating the device firmware.
Connection via Wings	The state of the connection via the Wings 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.
<Range extender name>	The state of the 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.
Transmitter power	Displays the selected power of the transmitter. The parameter appears when the **Max** or **Attenuation** option is selected in the **Signal attenuation test** menu. Learn more
Battery charge	The battery charge level of the device. Displays as a percentage. When the batteries need to be replaced, users and the security company will receive appropriate notifications. Learn more
Lid	The state of the device tampers that respond to detachment or opening of the device enclosure: • **Open** — the device is removed from the SmartBracket mounting panel, or its integrity is compromised. Check the mounting of the device. • **Closed** — the device is installed on the SmartBracket mounting panel. The integrity of the device enclosure and the mounting panel is not compromised. Normal state. Learn more

Mounting panel	The state of the device tamper that responds to unlocking the SmartBracket mounting panel lock: • **Unlocked** — the lock for SmartBracket is unlocked, or its integrity is compromised. Check the lock and mounting of the device. • **Locked** — the lock for SmartBracket is locked. The integrity of the device enclosure and the mounting panel is not compromised. Normal state. Learn more
Sensitivity	Sensitivity level of the motion detector: • **Low** • **Normal** • **High** Select the sensitivity depending on the results of the **detection zone test**.
Anti-masking	The state of the masking sensor: • **Alert** — masking is detected. • **On** — the anti-masking system is enabled. Masking is not detected. • **Off** — the anti-masking system is disabled. Masking will not be detected. Learn more
Always active	When this option is enabled, the detector is constantly armed, detects motion, and raises alarms.

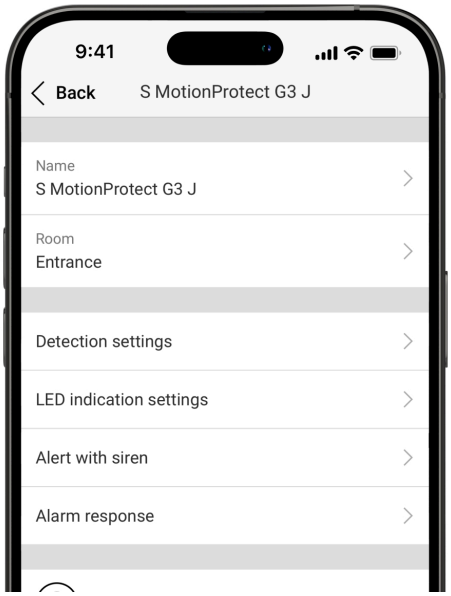
	Learn more
Permanent deactivation	The state of the device permanent deactivation setting: • **No** — the device operates in the normal mode and transmits all events. • **Entirely** — the device is completely excluded from the system operation by the hub admin. The device does not execute system commands and does not report alarms or other events. • **Lid only** — the hub admin has disabled notifications about tamper triggering. • **By number of alarms** — the device is automatically excluded from the system when the number of alarms is exceeded. The number of alarms is specified in the **Devices auto deactivation** hub settings in Ajax PRO-app. Learn more

One-time deactivation	Shows the state of the device one-time deactivation setting: • **No** — the device operates in the normal mode. • **Entirely** — the device is entirely excluded from the operation of the system for a time the armed mode is active. The device does not execute system commands and does not report alarms or other events. • **Lid only** — notifications on the tamper triggering are disabled for a time the armed mode is active. Learn more
Alarm response	
Operating mode	Indicates how the detector responds to alarms: • **Instant alarm** — the armed detector immediately responds to a threat and raises an alarm. • **Entry/Exit** — when a delay is set, the armed device starts counting down and does not raise an alarm even if it is triggered before the countdown ends. • **Follower** — the detector inherits delays from Entry/Exit detectors. However, when the follower is triggered individually, it immediately raises an alarm.

Entry delay	Entry delay (alarm activation delay) is the time a user has to disarm the system after entering the premises. **Learn more**
Exit delay	Exit delay (arming delay) is the time a user has to leave the premises after arming the system. **Learn more**
Arm in Night mode	When the option is enabled, the device will be armed when the system is set to **Night mode**. **Learn more**
Entry delay in Night mode	Entry delay time in **Night mode**. Entry delay (alarm activation delay) in **Night mode** is the time a user has to disable **Night mode** after entering the premises. **Learn more**
Exit delay in Night mode	Exit delay time in **Night mode**. Exit delay (arming delay) in **Night mode** is the time a user has to leave the premises after enabling **Night mode**. **Learn more**
Night mode delay	Entry delay time in **Night mode** when the device is set to the **Follower** operating mode. This is the time a user has to disable **Night mode** (alarm activation delay) after the Entry/Exit detector is triggered. **Learn more**
Firmware	Device firmware version.

Device ID	The device identifier. It is also available on the QR code on the device enclosure and its packaging.
Device No.	The device number. This number is transmitted to a monitoring station in case of an alarm or event.

Settings



To change Superior MotionProtect G3 Jeweller settings in the Ajax apps:

1. Go to the **Devices** tab.
2. Select **Superior MotionProtect G3 Jeweller** in the list.
3. Go to **Settings**.
4. Set the required settings.
5. Click **Back** to save the new settings.

Setting	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 MotionProtect G3 Jeweller is assigned. The room name is displayed in the text of SMS and notifications in the events feed.
Detection settings	
Always active	When enabled, the detector is always in the armed mode and detects motion. Learn more
Sensitivity	Sensitivity level of the motion detector. It depends on the type of the facility, the presence of probable sources of false alarms, and the specifics of the protected area: • **Low** — there are likely sources of false alarms in the protected area. • **Normal** (by default) — recommended value suitable for most facilities. Do not change it if the detector operates correctly. • **High** — there are no obstacles in the protected area; the maximum detection distance and the alarm detection speed

	are important. For example, if the detector is installed in a narrow passage.
Anti-masking	When this option is enabled, the device detects the masking.
LED indication settings	
Alarm LED indication	When disabled, the LED indicator doesn't notify about alarms and tamper triggering.
Alert with siren	
If motion detected	When the setting is enabled, the **sirens added to the system** are activated when the device detects motion.
If masking detected	When the option is enabled, the **sirens added to the system** are activated when the device detects masking. The setting is displayed if the **Anti-masking** option is enabled.
Alarm response	

Operating mode	This setting allows a user to specify how the device will respond to alarms: • **Instant alarm** — the armed detector immediately responds to a threat and raises an alarm. • **Entry/Exit** — when a delay is set, the armed device starts counting down and does not raise an alarm even if it is triggered before the countdown ends. • **Follower** — the detector inherits delays from Entry/Exit detectors. However, when the follower is triggered individually, it immediately raises an alarm.
Entry delay	This setting allows a user to select an entry delay time: 5 to 255 seconds. Entry delay (alarm activation delay) is the time a user has to disarm the system after entering the premises. Learn more
Exit delay	This setting allows a user to select an exit delay time: 5 to 255 seconds. Exit delay (arming delay) is the time a user has to leave the premises after arming the system. Learn more
Arm in Night mode	When the setting is enabled, the device will switch to armed mode when the system is set to **Night mode**. Learn more

Entry delay in Night mode	This setting allows a user to select an entry delay time in **Night mode**: 5 to 255 seconds. Entry delay (alarm activation delay) is the time a user has to disable **Night mode** after entering the premises. Learn more
Exit delay in Night mode	This setting allows a user to select an exit delay time in **Night mode**: 5 to 255 seconds. Exit delay (arming delay) is the time a user has to leave the premises after enabling **Night mode**. Learn more
Night mode delay	This setting allows a user to select a delay time in **Night mode**: 5 to 255 seconds. This is the time a user has to disable **Night mode** (alarm activation delay) after the Entry/Exit detector is triggered. The setting is displayed if the device is set to the **Follower** operating mode and the **Arm in Night mode** option is enabled. Learn more
Firmware update	With this setting, the device switches to the firmware update mode if a new version is available.
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
Wings signal strength test	Switches the device to the Wings 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 Wings data transfer protocol to select the optimal installation site. **Learn more**
Detection zone test	Switches the detector to the detection zone test mode. The option allows testing **motion** and **masking** sensors. The test helps to check whether the device is installed correctly to detect all alarms. **Learn more**
Signal attenuation test	Switches the device to the signal attenuation test mode. **Learn more**
Calibration of masking sensor	Runs the calibration of the masking sensor to ensure that the device operates correctly and can instantly detect attempts to block its field of view. **Learn more**
Device self-test	Runs the device self-test to check if the built-in sensors operate properly. The test checks the IR motion sensor and masking sensor. **Learn more**

Monitoring	When enabled, all device event notifications are sent to the monitoring station.
User manual	The setting allows a user to open the Superior MotionProtect G3 Jeweller user manual in an Ajax app.
Permanent deactivation	The setting allows a user to disable device events without removing it from the system. Three options are available: • **No** — the device operates normally 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 tamper alarm notifications only. Learn more The system can also automatically deactivate devices when the set number of alarms is exceeded. Learn more
One-time deactivation	The setting allows a user to disable device events before the system is first disarmed. Three options are available: • **No** — the device operates normally and transmits all events. • **Entirely** — the device is completely excluded from the system operation until the first disarming. The device does not execute system commands and does not report alarms or other events.

	• **Lid only** — tamper alarm notifications are disabled until the system is first disarmed. Learn more
Delete device	The setting allows a user to disconnect the device from the hub and delete its settings.

Masking sensor calibration

Calibration of the masking sensor is important to ensure that the device operates correctly and can instantly detect attempts to block the field of view of its sensors. Calibration starts automatically 10 seconds after the SmartBracket's lock is locked. If the device fails to calibrate the masking sensor, the system sends a notification to users and the monitoring station and displays the corresponding fault in the device **states**.

You can start the calibration of the masking sensor manually, for example, if the automatic calibration fails or the device installation location has been changed.

Before starting the calibration, ensure the device is installed properly and nothing blocks its field of view.

To start calibrating the masking sensor, in the Ajax app:

1. Go to the **Devices** tab.
2. Select **Superior MotionProtect G3 Jeweller** from the list.
3. Go to **Settings**.
4. Go to the **Calibration of masking sensor** menu.

5. Tap **Start**.
6. If the calibration is successful, tap **Close** to return to the settings. If the device fails to calibrate the masking sensor, check if it is installed correctly and nothing blocks its field of view. Then tap **Restart**.

Device self-test

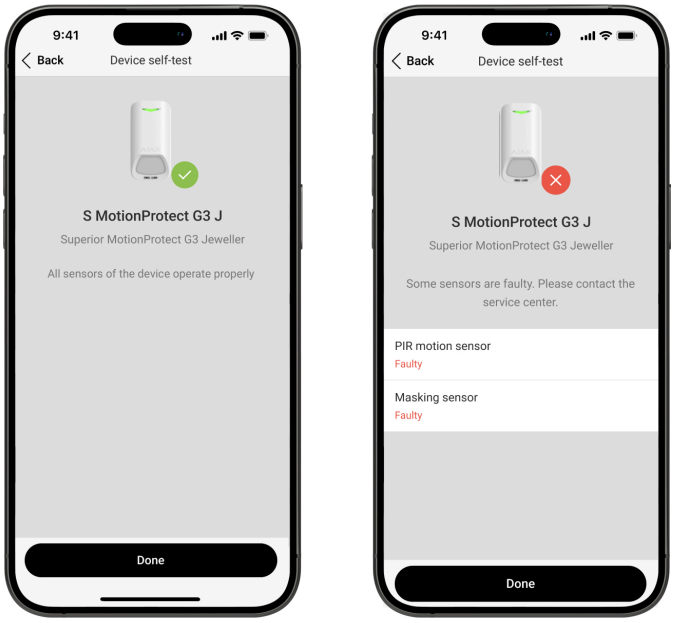
Device self-testing allows users to check if the device's built-in sensors operate properly. During the self-test, the IR motion sensor and masking sensor will be tested. The device runs the self-test of the built-in sensors automatically on a regular basis. If a malfunction is detected, the system notifies users and the CMS.

In addition, the device self-test procedure can be started manually in **Ajax apps**.

Before running the self-test, ensure that the system is disarmed, and another test is not in progress.

To run self-testing, in the Ajax app:

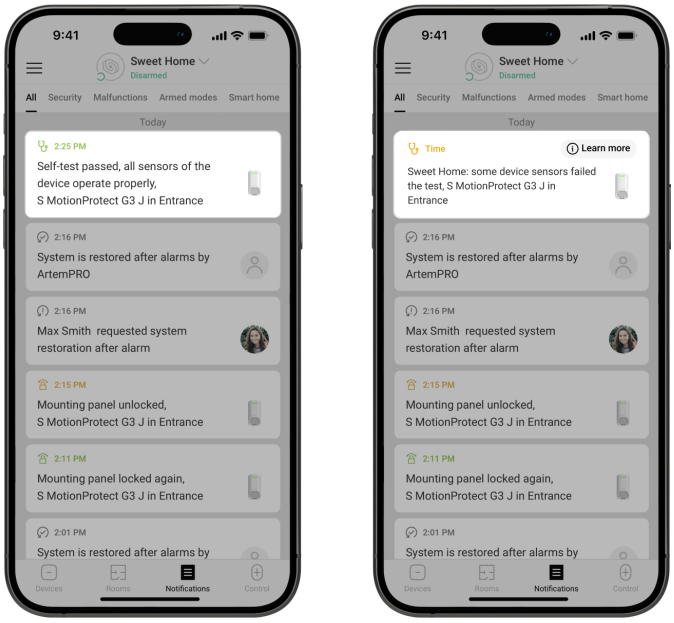
1. Go to the **Devices** tab.
2. Select **Superior MotionProtect G3 Jeweller** from the list.
3. Go to **Settings**.
4. Go to the **Device self-test** menu.
5. Tap **Start**.
6. If self-testing is successful, tap **Done** to return to the settings. If some sensors are faulty, we recommend contacting the service center.



Note that the device self-test checks only the enabled sensors of the device.

If a faulty sensor is disabled, the system will not show the malfunction counter in an Ajax app and will not notify users about the sensor malfunction. However, if a user enables a faulty sensor, the system will send a notification that the sensor is malfunctioning.

Users and the CMS will receive a corresponding notification about the testing result after completion.



Indication

The **Superior MotionProtect G3 Jeweller** LED indicator may light up green or red, depending on the state of the device.

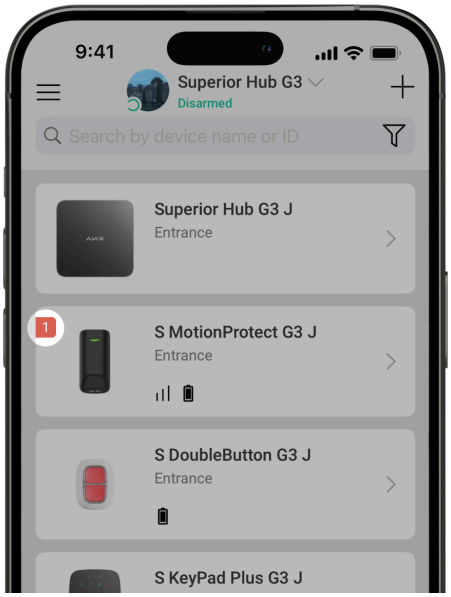
Event	Indication	Note

The device detects an alarm when it is not added to the hub.	Lights up green for 0.3 seconds and goes out for 0.3 seconds three times.	
The device is deleted from the hub.	Lights up green for 0.3 seconds and goes out for 0.3 seconds six times.	
• Motion alarm. • Tamper alarm. • Masking is detected / restored to normal state.	Lights up green for about 0.6 seconds.	
The detection zone test of the motion sensor is running for the device.	Lights up green constantly and goes out for 0.6 seconds when motion is detected.	**Learn more**
The detection zone test of the masking sensor is running for the device.	Lights up red constantly and goes out completely when masking is detected. When the masking is removed, lights up red again.	**Learn more**
Calibration of the masking sensor is in progress.	Lights up green for 0.5 seconds and goes out for 0.5 seconds.	**Learn more**
The device hardware error or its sensors malfunction.	Lights up red for about 1 second every 4 seconds.	The device requires maintenance; contact our **Technical Support**.
Calibration of the masking sensor has failed.	Lights up red for about 1 second every 13 seconds.	Ensure the device is installed properly and nothing blocks its field of view, and then restart the calibration. If the indication repeats, contact our **Technical Support**.

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 mounting panel lock is unlocked (tamper is triggered).
- The device lid is open (tamper is triggered).
- There is no signal via Jeweller protocol.
- There is no signal via Wings protocol.
- The IR sensor is faulty.
- The masking sensor is faulty.

- The calibration of the masking sensor has failed.

Maintenance

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

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

Technical specifications

☞ **All technical specifications of Superior MotionProtect 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:

- email
- Telegram

Manufactured by “AS Manufacturing” LLC