MotionCam Outdoor HighMount (PhOD) Jeweller user manual

Updated September 1, 2025



MotionCam Outdoor HighMount (PhOD) Jeweller is a wireless motion detector supporting **Photo by alarm**, **Photo on demand**, **Photo by scenario**, **Photo by schedule**, and **Photo by arming/disarming** features.

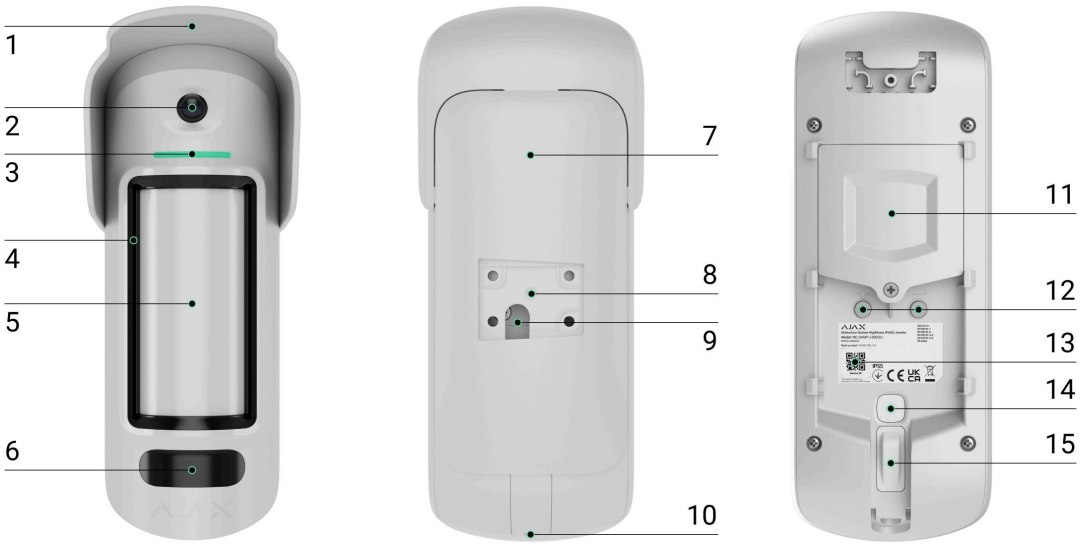
It detects movement at a distance of up to 15 m. The device is equipped with a PIR sensor and uses radio frequency scanning with a K-band microwave sensor to filter out infrared interference. Also, it features an anti-masking system that detects attempts to block the detector's field of view. The device is designed for outdoor and indoor use.

MotionCam Outdoor HighMount (PhOD) Jeweller communicates with a hub via two secure radio protocols. The detector uses **Jeweller** to transmit alarms or events and **Wings** to transmit photos and update firmware. The communication range in an open space is up to 1,700 m.

Buy MotionCam Outdoor HighMount (PhOD) Jeweller

Functional elements

Detector



1. Hood for protecting the camera and anti-masking sensors from rain and snow.
2. Camera.
3. LED indicator.
4. Masking sensor.
5. Motion sensor lens.
6. Infrared (IR) illumination. It is used to take photos in dark and low-light conditions.
7. SmartBracket mounting panel. To remove the panel, slide it down.
8. Recess for mounting SmartBracket to the swivel mount.
9. Hole for routing an external power supply cable.
10. Holding screw. It is used to fix the device on the SmartBracket mounting panel.
11. Lid of the battery compartment.

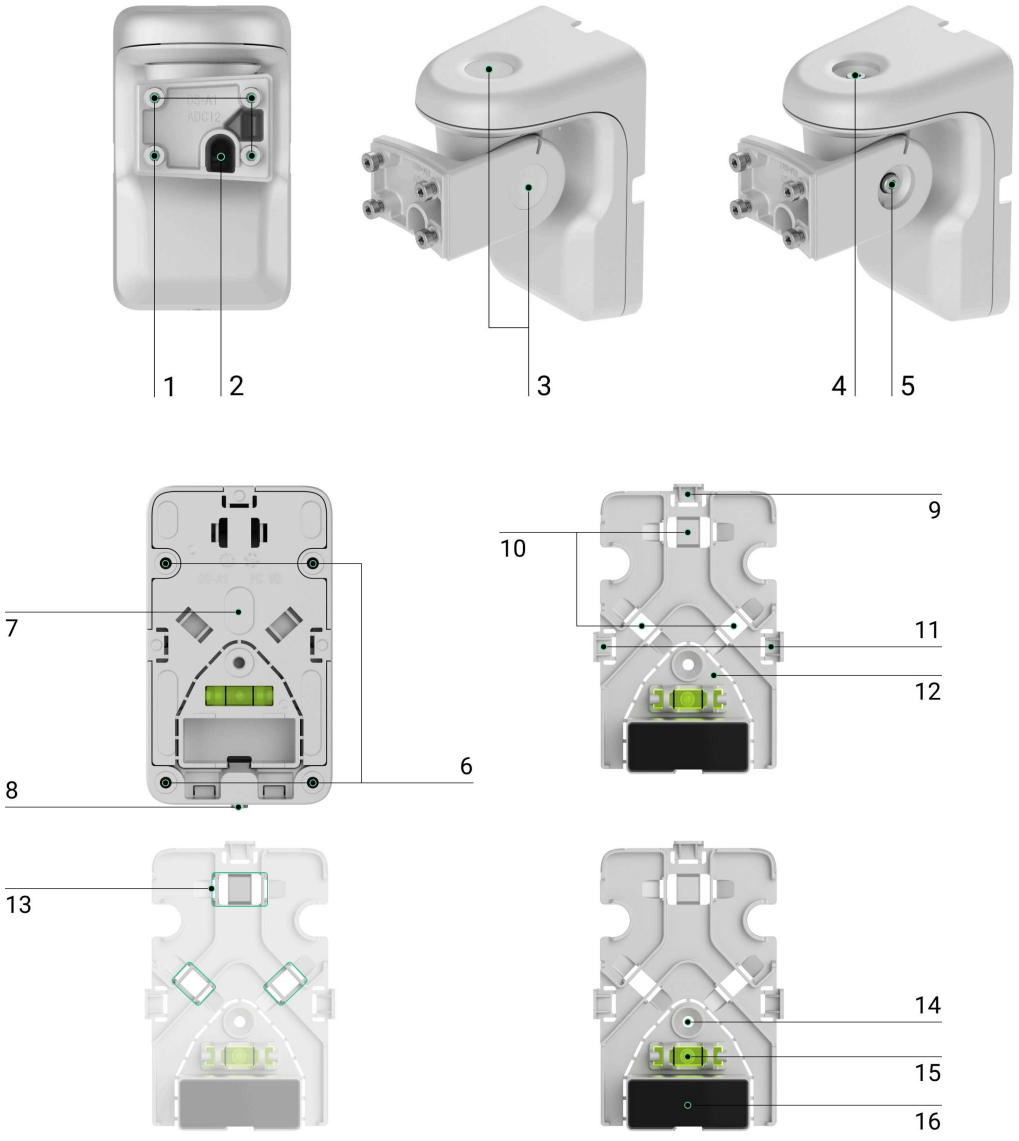
12. Terminals for the external power supply connection.

13. QR code with the device ID. It is used to add the device to the hub.

14. Power button.

15. Tamper button.

Swivel mount



1. Fixing points to attach the SmartBracket mounting panel to the swivel mount with screws.

2. Conduit to route an external power supply cable through the swivel mount.

3. Rubber sealing plugs to protect screws that adjust the positioning angles of the detector.
4. Top screw to adjust and fix the horizontal position of the detector.
5. Side screw to adjust and fix the tilt angle of the detector.
6. Holes to attach the swivel mount to the surface.
7. Plastic panel of the swivel mount. It has a bubble level, a magnet, and elements for cable management.
8. Holding screw. It is used to fix the elements of the swivel mount.
9. Perforated part of the plastic panel to route the cable from the top of the swivel mount.
10. Spots to route the cable through the wall.
11. Perforated parts of the plastic panel to route the cable from the sides of the swivel mount.
12. Perforated part with a magnet of the plastic panel. It is used to trigger the device magnetometer in case of any attempts to tilt or shift the detector or detach it from the surface. Do not break it off.
13. Fasteners to fix the cables with ties.
14. Hole to attach the plastic panel on the surface.
15. Bubble level to check the inclination angle of the mount during installation.
16. Magnet. It is used to trigger the device magnetometer in case of any attempts to tilt or shift the detector or detach it from the surface.

Compatible hubs and range extenders

An Ajax hub with **OS Malevich 2.26** and later versions is required for the device to operate.

Check device compatibility

Operating principle

MotionCam Outdoor HighMount (PhOD) Jeweller is a wireless motion detector supporting photo verification. It is equipped with two IR sensors, an additional K-band microwave sensor, a camera, and an anti-masking system.

The device detects movement with IR sensors by capturing moving objects with temperatures close to that of the human body. After detecting movement using IR sensors, the detector starts an additional RF scanning of the detection zone with the built-in K-band microwave sensor to filter out false alarms.

When the movement is detected, MotionCam Outdoor HighMount (PhOD) Jeweller takes a series of images, which allows for assessing the situation at the site in dynamics. This saves users from unnecessary anxiety and security companies from false patrol despatches.

> **Learn more about photo verification**

In case of an alarm, the detector instantly sends an alarm to the hub, activating the sirens connected to the system, triggering **scenarios**, and notifying users and the security company. All MotionCam Outdoor HighMount (PhOD) Jeweller alarms and events are recorded in the event feed of Ajax apps.

Users and the monitoring company know exactly where movement 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.

> **How Ajax notifies users of alarms**

> **Learn more about Ajax motion detectors**

Protection against false alarms

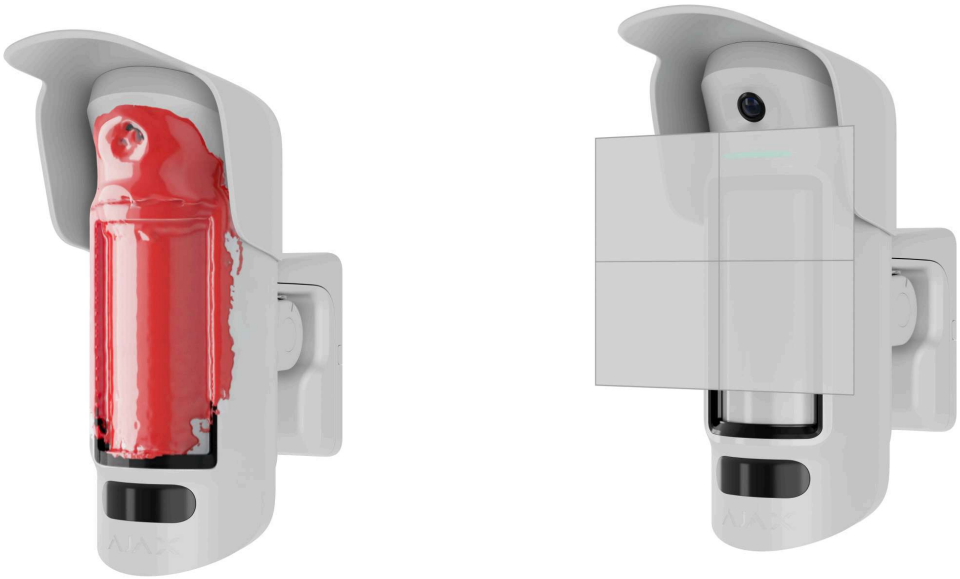
MotionCam Outdoor HighMount (PhOD) Jeweller uses the **SmartDetect algorithm** to prevent false alarms. This algorithm allows the detector to analyze the thermal diagram read by the sensor, including the intensity of infrared radiation, size of the heat spot, time spent in the detection area, and other parameters.

After this stage, the detector performs additional RF scanning of the detection zone with a built-in K-band microwave sensor to eliminate false alarms due to IR interference, such as air flows, heated curtains and blinds, fans, fireplaces, air conditioners, etc. Depending on the result, the alarm will be activated or not.

Temperature compensation

Due to temperature compensation, the detector responds to movement, 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. MotionCam Outdoor HighMount (PhOD) Jeweller detects the following types of masking:

- Placing 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 of masking. The maximum masking detection time is up to 180 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

Jeweller and Wings data transfer protocols

Jeweller and Wings are wireless data transfer protocols that provide fast and reliable two-way communication between the hub and devices. The detector uses **Jeweller** to transmit alarms and events and **Wings** to transmit photos and update the firmware.

Learn more

Firmware update

If a new firmware version for MotionCam Outdoor HighMount (PhOD) Jeweller is available, the icon appears in **Ajax apps** in the **Devices** tab. An admin or a PRO with access to the system settings can run an update via device **states** or **settings**. The on-screen instructions help to update the firmware successfully.

Sending events to the monitoring station

The Ajax system can transmit alarms to the **PRO Desktop** monitoring app and the central monitoring station (CMS) in the formats of **SurGard (Contact ID), SIA (DC-09), ADEMCO 685**, and other protocols.

MotionCam Outdoor HighMount (PhOD) Jeweller can transmit the following events:

1. Motion alarm.
2. Masking alarm.
3. Alarm that the device has been moved: the magnetometer has detected attempts to tilt or shift the detector or detach it from the surface.
4. Tamper alarm. Tamper recovery.
5. Loss and restoration of connection with the hub.
6. Permanent deactivation/activation of the device.
7. 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 rapid response unit. 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.



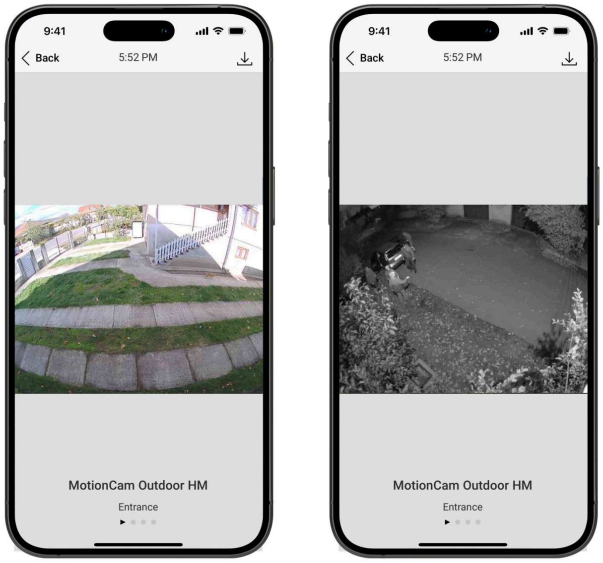
You can find the device ID and loop (zone) number in the device states.

Photo verification

Photo verification allows you to assess what is happening at the secured site with a built-in camera. The device can take from 1 to 5 images with a resolution of 320 × 240 pixels and up to 3 images with a resolution of 640 × 480 pixels.

With photo verification, you can receive visual confirmations of alarms from MotionCam Outdoor HighMount (PhOD) Jeweller and other Ajax devices. You can also check the situation, such as finding out what the children are doing, checking if your pet is OK, or simply monitoring the situation at home.

The detector has an infrared illumination for shooting in the dark that turns on in case of low light. MotionCam Outdoor HighMount (PhOD) Jeweller takes black and white photos when shooting in these conditions.

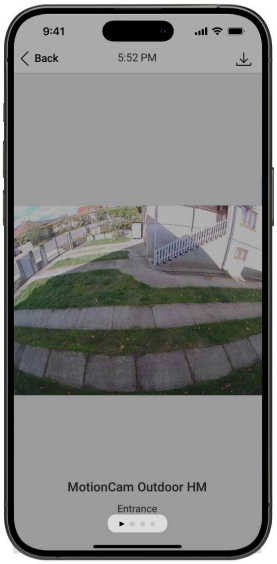


There are several types of photo verification: photo by alarm, photo on demand, photo by scenario, photo by schedule, and photo by arming/disarming.

The photos can be displayed in the app as an image or an animated series (if more than 1 photo is taken). The number of images in the series can be configured in Ajax apps. To view the received photos, tap on the corresponding MotionCam Outdoor HighMount (PhOD) Jeweller notification in the event feed.



Users can view the images from the animated series frame by frame by swiping them left.



You can save the photo verification result as a video or photo by tapping the download icon.

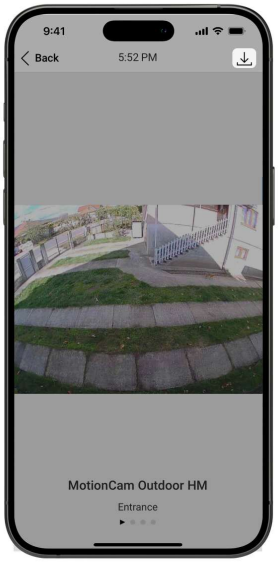


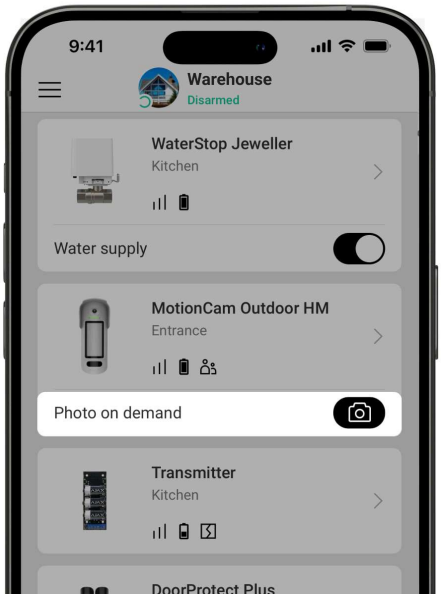
Photo by alarm

The detector takes **photos by alarm** only if the movement is detected and only when armed mode is on. By default, the **Photo by alarm** feature is enabled for all detectors. The number of images and their resolution can be changed in the **device settings**. Photos by alarm are available to all users with access to the event feed.

> 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 is specified in the **Jeweller** or **Jeweller/Fibra** settings; its default value is **36 seconds**. 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 of the security mode change.

Features of alarm photo verification

Photo on demand



The **Photo on demand** feature allows users to take photos using the built-in cameras of detectors that support photo verification. With this feature, you can check the situation at the site: find out what the children are doing, check if your pet is OK, or simply monitor the situation at home. Depending on the settings, photos can be taken at any time or when MotionCam Outdoor HighMount (PhOD) Jeweller is armed.

By default, the **Photo on demand** feature is disabled for all users. Users with the right to manage privacy settings (space settings, the **Privacy** section) determine who can take and view photos on demand and which detectors that support photo verification can take pictures. PRO users cannot manage privacy settings, but they can take photos on demand if they have been granted such permission.

Privacy settings do not apply to photos taken by detectors triggered in case of an alarm. All system users who have access to the event feed can view the photos taken in case of an alarm.

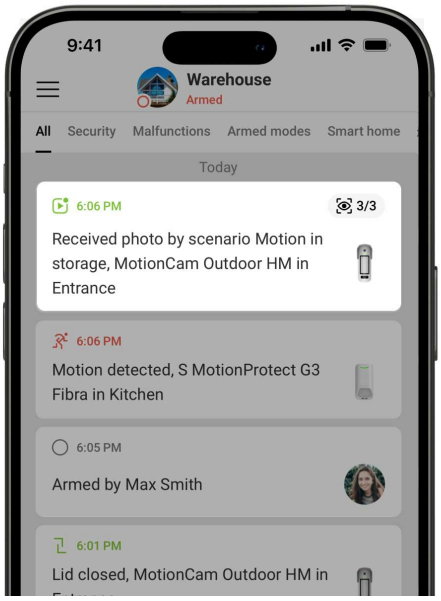
Photos on demand are not sent to the security company monitoring station.

PRO Desktop users can take and view photos on demand only from their personal account if an admin has granted them the appropriate access rights. Taking and viewing photos on demand is not available for the security company profile in the PRO Desktop app.

More about the Photo on demand feature

How to set Photo on demand

Photo by scenario



The **Photo by scenario** feature allows you to create a scenario for motion detectors supporting photo verification. These detectors will take pictures in case of alarms from specified Ajax devices.

By default, the **Allow photos by scenarios** option is disabled for all detectors. An admin or a user with access to privacy settings can enable it.

In the system settings, you can also set exactly when a detector supporting photo verification can take photos according to a scenario: always or when the device is armed.

Photos by scenario are available to all system users who have access to the event feed. The event of taking a photo after the alarm from specified devices is sent to the security company monitoring station via SIA DC-09 (SIA-DCS) and other proprietary protocols. The event code is 730.

If the CMS software supports photo verification, photos by scenario are available to the CMS engineers. Photos by scenario are also available in the **PRO Desktop** app.



Photos by scenario will not be sent to the CMS if only a direct connection with the monitoring station is used.

More about the Photo by scenario feature

How to set up Photo by scenario

Photo by schedule

The **Photo by schedule** feature allows you to create a scenario for motion detectors supporting photo verification. These detectors will take pictures by schedule.

Before creating a scheduled scenario, enable the **Allow photos by scenarios** option. An admin or a user with access to privacy settings can enable this option.

You can precisely set when a detector supporting photo verification can take pictures according to a scheduled scenario: always or when it is armed.

Photos taken by schedule are available to all system users who have access to the event feed. The event of taking a photo is sent to the CMS via **SIA DC-09 (SIA-DCS)** and other proprietary protocols. The event code is 731.

If the CMS software supports photo verification, photos by schedule are available to the CMS engineers. These photos are also available in the **PRO Desktop** app.

Photos taken by schedule are not sent to the CMS if only a direct connection with the monitoring station is used.

How to set up Photo by schedule

Photo by arming/disarming

The **Photo by arming/disarming** feature allows users to receive photos from a built-in camera when the security state changes. With this feature, you can check the situation at the facility when the system is armed, disarmed, or switched to **Night mode**.

Before creating an arming/disarming scenario, enable the **Allow photos by scenarios** option. A space admin or a user with access to privacy settings can enable this option.

The **Photo by arming/disarming** scenario is available in the hub's settings with **OS Malevich 2.29** and later. The feature allows you to configure conditions under which the selected detectors take photos: when arming, when disarming, when **Night mode** is enabled, or when **Night mode** is disabled. Also, you can set up whether to consider or ignore entry/exit delays.

Photos by arming/disarming are available to all system users with access to the event feed. The event of taking a photo is sent to the CMS via **SIA DC-09 (SIA-DCS)** and other proprietary protocols. The event code is 732.

If the CMS software supports photo verification, the CMS engineers can access photos by arming/disarming. These photos are also available in **PRO Desktop**.

Photos by arming/disarming will not be sent to the CMS if only a direct connection with the monitoring station is used.

How to set up Photo by arming/disarming

Selecting the installation site



MotionCam Outdoor HighMount (PhOD) Jeweller is suitable for securing the territory of the protected facility, such as private houses, parking lots, construction areas, unheated premises, etc. The device is suitable for installation both outdoors and indoors.

The device is designed for installation at a height of 2–4 m. The device should be mounted on a flat, stable surface, such as the wall of a house or a solid fence. Installing the device on a shaky (unstable) surface will result in false alarms.

Depending on the installation height, the tilt angle and horizontal position of the device must be adjusted using the swivel mount. This is necessary to ensure that detector's motion sensors and camera have the correct fields of view. The direction of the detector sensors should be perpendicular to an alleged intrusion path to the site.

When choosing where to place MotionCam Outdoor HighMount (PhOD) Jeweller, consider the parameters that affect its operation:

- Jeweller and Wings signal strength.

- Motion detection area.
- Distance between MotionCam Outdoor HighMount (PhOD) Jeweller and another detector with a K-band microwave sensor should be at least 20 cm.
- The presence of objects or structures that can obstruct the detector's view.

Consider the placement recommendations when developing a system project. Only specialists should design and install Ajax systems. A list of recommended partners is **available here**.

Signal strength

The signal strength is determined by the number of undelivered or corrupted data packages over a certain period of time. The icon in the **Devices** tab in Ajax apps indicates the signal strength:

- **three bars** — excellent signal strength;
- **two bars** — good signal strength;
- **one bar** — low signal strength, stable operation is not guaranteed;
- **crossed-out icon** — no signal.

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

Refer to the **Functionality testing** section to learn how to run Jeweller and Wings signal strength tests.

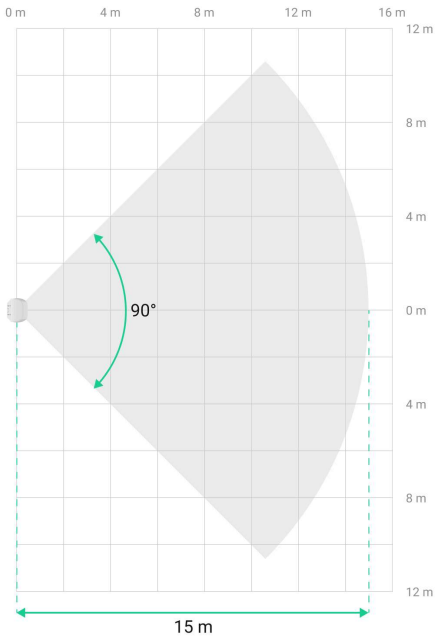
What is Jeweller signal strength test

What is Wings signal strength test

Motion detection zone

The detector location 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 and camera, viewing angles, and the presence of obstacles to the detector's view.

MotionCam Outdoor HighMount (PhOD) Jeweller detects movement at a distance of up to 15 m. The direction of the detector sensors should be perpendicular to the intended entry path to the site. Ensure that no structures or objects block the detector's view.



Horizontal characteristics of the motion detection area

When installing the detector, take a test photo of the motion detection zone and perform the **Detection zone test**. This allows you to check the device operation and accurately determine the sector in which the device detects movement. Refer to the **Functionality testing** section to learn how to run the tests.

Do not install the detector

1. In places where objects or structures can block the detector’s view. For example, behind a tree or a column.
2. In places where glass structures can block the detector’s view; the device does not detect movement behind glass.
3. In front of water reservoirs or pools if they are located in the detection zone of the detector.
4. Near any magnetic field sources like electric motors for automatic gates, magnetic locks, power cables, etc. Such sources may trigger the device magnetometer and lead to false alarms that the device has been moved.
5. Near other detectors with K-band microwave sensors. The minimum distance between devices should be **at least 20 cm**. Otherwise, detection quality can be decreased, or false alarms can be activated because of wave interference of K-band microwave sensors.
6. In places with low or unstable Jeweller or Wings signal strength.
7. Closer than 1 m to the hub or radio signal range extender.

Installation



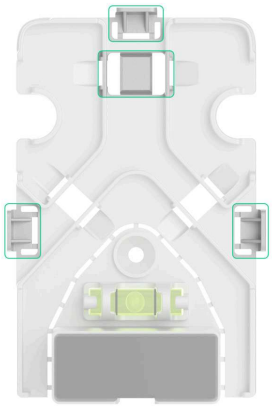
Before installing MotionCam Outdoor HighMount (PhOD) Jeweller, ensure that you have chosen the optimal location that complies with the requirements of this manual.

Do not install the device near any magnetic field sources. If any magnetic source is nearby, adjust the **Magnetic sensor sensitivity** in the device settings or change the device installation place. Otherwise, it can lead to false alarms that the device position has been changed.

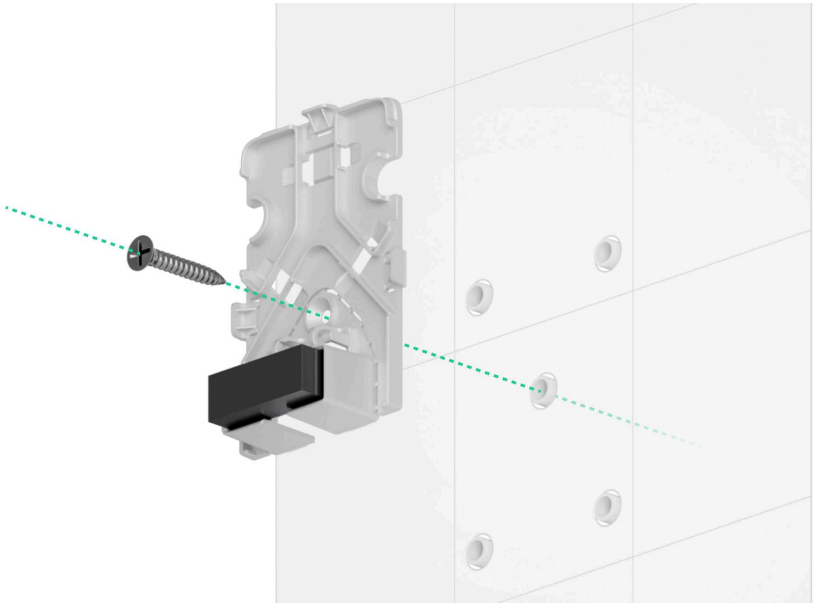
MotionCam Outdoor HighMount (PhOD) Jeweller is designed to be installed using a swivel mount only. Installing the device on a swivel mount allows adjusting the tilt angle and horizontal position of the detector and ensures advanced sabotage protection with a built-in magnetometer.

To install the device:

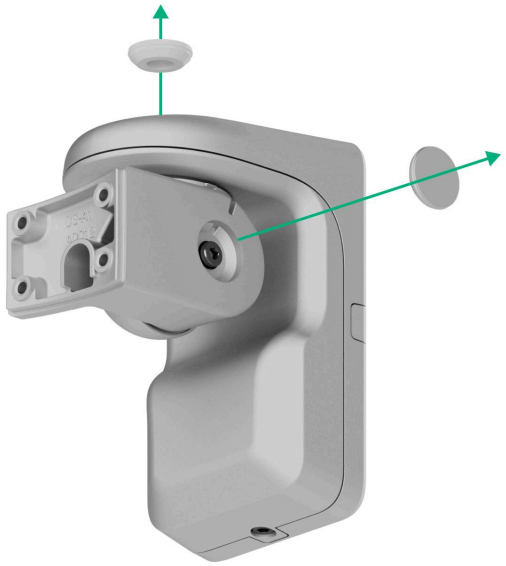
1. Remove the plastic panel from the swivel mount. If you are going to connect the external power supply, carefully break out the corresponding perforated part to run the cable from the top, back, or sides. Also, refer to the **Connecting an external power supply** section for more information.



2. Attach the plastic panel to the surface using a bundled screw.



3. Remove the rubber sealing plugs that protect the top and side screws of the swivel mount. Do not use sharp or spike tools to prevent damaging the sealing plugs.

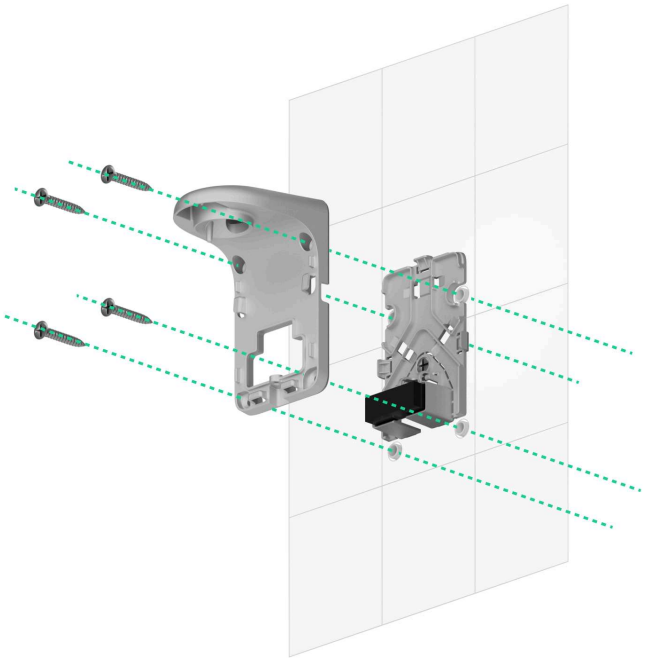


4. Unscrew the top screw and the holding screw at the bottom of the swivel mount. Disassemble the rear part of the swivel mount by sliding it up.



If you are connecting an external power supply, refer to the Connecting an external power supply section to learn how to route the cable through the swivel mount.

5. Place the rear part of the swivel mount over the plastic panel and fix it on the surface with bundled screws. Use all fixing points.



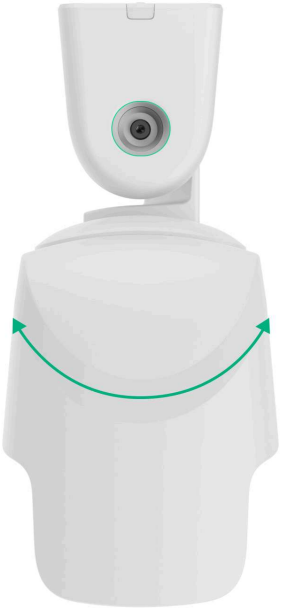
6. Attach the front part of the swivel mount to the rear part and tighten the top screw and the holding screw at the bottom.
7. Remove the SmartBracket mounting panel from the detector. Unscrew the holding screw first and slide the panel down.
8. Attach the SmartBracket mounting panel to the swivel mount and secure it with bundled screws. Use all fixing points.



9. Add the detector to the system.
10. Attach the hood to the detector.

11. Place the detector on the SmartBracket mounting panel.

12. Lose the top screw of the swivel mount, adjust the horizontal position of the detector field of view, then tighten the top screw up.



13. Lose the side screw of the swivel mount, adjust the detector’s tilt angle, then tighten the side screw up.



The tilt angle depends on the detector installation height. To adjust the proper detector field of view, we recommend setting the following tilt angle relative to the detector installation height:

Installation height	Tilt angle
2.0 m	15.0°
2.2 m	15.9°
2.4 m	16.8°
2.6 m	17.7°
2.8 m	18.6°
3.0 m	20.0°
3.2 m	20.4°
3.4 m	21.3°
3.6 m	22.2°
3.8 m	23.1°
4.0 m	24.0°

14. Run the **functionality testing**.

15. If the tests are successful, ensure the firm tightening of the top and side screws of the swivel mount and install the rubber sealing plugs that protect these screws.

16. Remove the detector from the SmartBracket mounting panel and install it again to initiate the calibration of the magnetometer and masking sensors. For proper calibration, ensure that there are no obstacles in front of the detector and that it is not moved.

> Calibration starts automatically after the detector is installed on the SmartBracket mounting panel.

17. Tighten the holding screw on the bottom of the detector enclosure. The screw is needed for more reliable fastening and protection of the

device from quick dismantling.



Connecting an external power supply

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

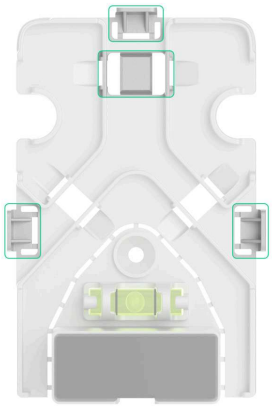
MotionCam Outdoor HighMount (PhOD) Jeweller is equipped with terminals for connecting a 12–24 V⎓ power supply.

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

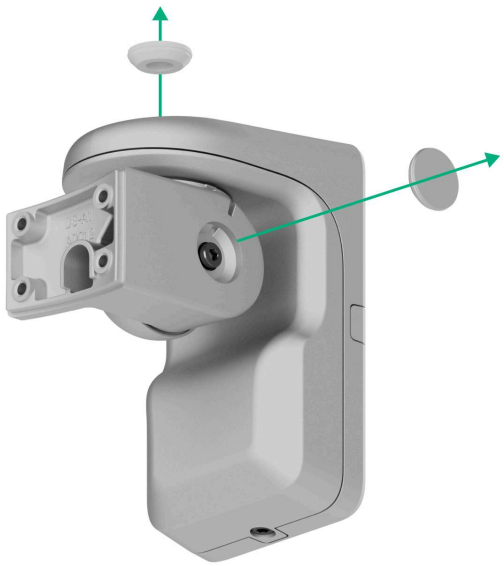
Before installing the device, check the wires for any damage to the insulation. Use only a grounded power source. Do not disassemble the device while it's under voltage. Do not use the device with a damaged power cable.

To connect an external power supply:

1. De-energize the external power supply cable.
2. Dismount the detector and swivel mount if they have already been installed.
3. Remove the plastic panel from the swivel mount. Carefully break out the corresponding perforated part to run the cable from the top, back, or sides.



4. Remove the rubber sealing plugs that protect the top and side screws of the swivel mount. Do not use sharp or spike tools to prevent damaging the sealing plugs.



5. Unscrew the top screw and the holding screw at the bottom of the swivel mount. Disassemble the rear part of the swivel mount by sliding it up.



6. Route the cable inside the detector through the following elements:
    1. The plastic panel of the swivel mount
    2. The rear part of the swivel mount
    3. The front part of the swivel mount
    4. The SmartBracket mounting panel

0:00 / 0:20

7. Connect the cable to the terminals by observing polarity (marked on the plastic). Firmly secure the wires to the terminals.

8. Install the swivel mount and the detector on the surface according to **steps 5–16** described in **Installation** section.
9. Switch on the external power.

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

Adding to the system

The hub and the device operating at different radio frequencies are incompatible. The radio-frequency range of the device may vary by region. We recommend purchasing and using Ajax devices in the same region. You can check the range of operating radio frequencies with the technical support service.

Before adding a device

1. Install an **Ajax app**.
2. Log in to your **account** or create a new one.
3. Select a **space** or create a new one.
4. Add at least one **virtual room**.
5. Add a **compatible hub** to the space. Ensure the hub is switched on and has internet access via Ethernet, Wi-Fi, and/or mobile network.
6. Check the states in the Ajax app to ensure the space is disarmed and the hub is not starting an update.

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

Types of accounts and their rights

Adding to the hub

1. Open an **Ajax app**. Select a **space** to which you want to add the device.
2. Go to the **Devices** tab and tap **Add device**.
3. Assign a name to the device.
4. Scan the QR code or enter the device ID manually. A QR code with ID is placed on the device enclosure. Also, it is duplicated on the device packaging.



5. Select a virtual room and a security group (if **Group mode** is enabled).
6. Tap **Add**, and the countdown will begin.
7. Switch on the device by holding the power button for 3 seconds.



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

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.

> MotionCam Outdoor HighMount (PhOD) Jeweller works with only one hub. When paired with a new hub, it stops sending events to the old one. After the device is added to a new hub, it will not be automatically removed from the device list of the old hub. This must be done through the Ajax app.

Functionality testing

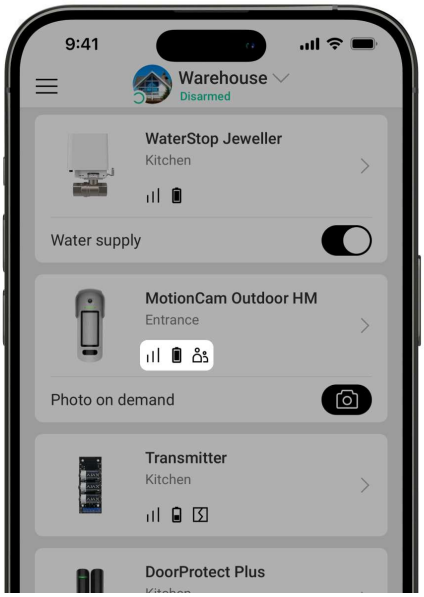
An Ajax system provides several types of tests to help select the correct installation place for the devices. For MotionCam Outdoor HighMount (PhOD) Jeweller, the following tests are available:

- **Motion detection area test** — to take a test photo to check the detector's field of view. The photo helps to adjust the detector's tilt angle and horizontal position correctly.
- **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.

- **Wings 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 Wings data transfer protocol at the device installation site.
- **Detection zone test** — to check how the detector responds to **movement** and **masking** at the installation site.
- **Signal attenuation test** — to decrease or increase the power of the radio transmitter; to check the stability of communication between the device and the hub, the changing environment at the site is simulated.

Icons



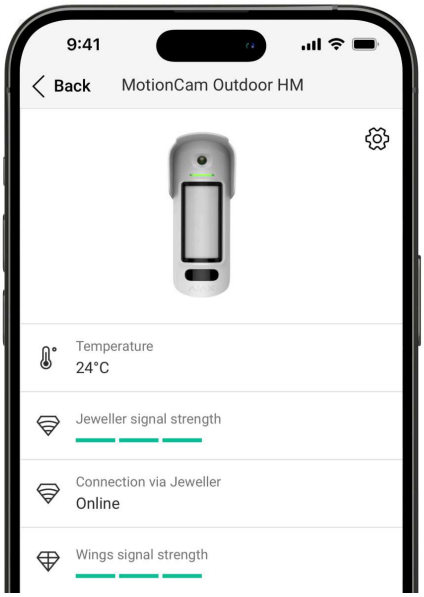
Icons in an Ajax app display some of MotionCam Outdoor HighMount (PhOD) Jeweller states. You can check the icons in the **Devices** tab.

Icon	Meaning

	Jeweller signal strength. It displays the signal strength between the hub and the device. The recommended value is 2–3 bars. Learn more
	Battery charge level of the device. Learn more
	A firmware update is available. Go to the device states or settings to find the description and launch an update.
	Other users have access to the **Photo on demand** feature. Learn more
	The device operates in **Always active** mode. Learn more
	The device operates through the radio signal range extender. Learn more
	Delay when entering and/or leaving is enabled. Learn more
	The device operates in **Night mode**. Learn more
	Masking is detected.
	The device is in the signal attenuation test mode. Learn more
	The device is automatically disabled because the number of alarms has been exceeded.

	Learn more
	The device is permanently deactivated. Learn more
	Tamper alarm notifications are permanently deactivated. Learn more
	The device is deactivated until the system is disarmed for the first time. Learn more
	Tamper alarm notifications are deactivated until the system is disarmed for the first time. Learn more
Offline	The device has lost connection with the hub or the hub has lost connection with the Ajax Cloud server.
Not transferred	The device has not been transferred to the new hub. Learn more

States



The states include information about the device and its operating parameters. The states of MotionCam Outdoor HighMount (PhOD) Jeweller can be found in Ajax apps:

1. Go to the **Devices** tab.
2. Select **MotionCam Outdoor HighMount (PhOD) Jeweller** in the list.

Parameter	Meaning
Data import	Displays the error when transferring data to the new hub: • **Failed** — the device has not been transferred to the new hub. Learn more
Malfunction	Tapping on ⓘ opens the list of device malfunctions. The field is only displayed if a malfunction is detected.
New firmware version available	Tapping on ⓘ opens the instructions for updating the device's firmware.

	The field is displayed if a new firmware version is available.
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** MotionCam Outdoor HighMount (PhOD) Jeweller is an outdoor detector, and its temperature is not considered when calculating the average temperature in the room to which the detector is assigned. **Learn more**
Jeweller signal strength	Jeweller signal strength between the device and the hub (or the radio signal range extender). The recommended value is 2–3 bars. Jeweller is a protocol for transmitting events and alarms.
Connection via Jeweller	Connection status via Jeweller channel between the device and the hub (or the range extender): • **Online** — the device is connected to the hub (or the range extender). Normal state. • **Offline** — the device is not connected to the hub (or the range extender). Check the device connection.

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 photo verification of alarms and updating the device firmware.
Connection via Wings	Connection status via 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.
Transmitter power	Displays the selected power of the transmitter. The parameter appears when the **Max** or **Attenuation** option is selected in the **Signal attenuation test** menu. Learn more
<Range extender name>	Status of device connection to the radio signal range extender. • **Online** — the device is connected to the range extender. • **Offline** — the device is not connected to the range extender. The field is displayed if the device operates via the radio signal range extender.
Battery charge	The battery charge level of the device. Two states are available: • **OK.**

	• **Battery low.** When the batteries need to be replaced, users and the security company will receive appropriate notifications. Learn more
Lid	The state of the device 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 device installation. • **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
External power	External power state: • **Connected** — the external power is connected to the detector. • **Disconnected** — the external power is disconnected or not connected.
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
Sensitivity	Sensitivity level of the motion detector: • **Low**

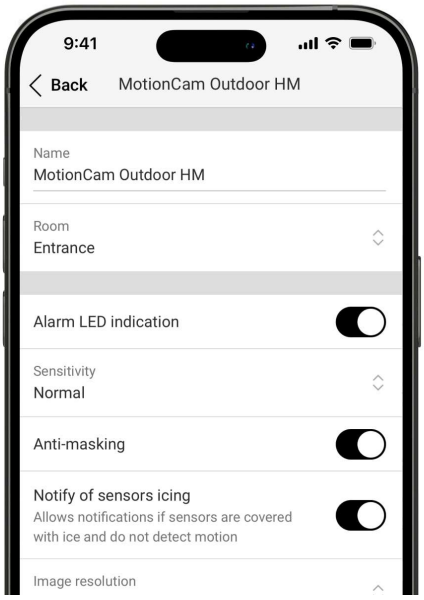
	• **Normal** • **High** Select the sensitivity depending on the results of the **detection zone test**.
Anti-masking	The state of the masking sensor: • **Alarm** — masking is detected. • **On** — the anti-masking system is enabled. Masking is not detected. • **Off** — the anti-masking system is disabled. Masking will not be detected. **Learn more**
Always active	When this option is enabled, the detector is constantly armed, detects movement, and raises alarms. **Learn more**
Alert if moved	The state of the **Alert if moved** setting. When this option is enabled, the built-in magnetometer detects attempts to tilt, shift, or detach the device from the surface. • **Yes** — the magnetometer is enabled. • **No** — the magnetometer is disabled.
Permanent deactivation	The state of the device's permanent deactivation setting: • **No** — the device operates in 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 of 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 the Ajax PRO app. Learn more
One-time deactivation	Shows the state of the device's one-time deactivation setting: • **No** — the device operates in normal mode. • **Entirely** — the device is entirely excluded from the operation of the system for a time armed mode is active. The device does not execute system commands and does not report alarms or other events. • **Lid only** — notifications of tamper triggering are disabled for a time armed mode is active. Learn more
Photo on demand access	Displayed if **Allow photos on demand** is enabled in the space settings in the **Privacy** section.
Alarm reaction	
Operating mode	Shows 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 the countdown and does not raise an alarm even if it is triggered before the countdown is completed. • **Follower** — the detector inherits the delays from Entry/Exit detectors. However, when the Follower is triggered individually, it immediately raises an alarm.
Delay when entering	Delay when entering (alarm activation delay) is the time the user has to disarm the security system after entering the premises. Learn more
Delay when leaving	Delay when leaving (arming delay) is the time the user has to leave the premises after the system is armed. Learn more
Arm in Night mode	If this option is enabled, the device will enter armed mode when the system is set to **Night mode**. Learn more
Night mode delay when entering	Delay when entering in **Night mode**. Delay when entering (alarm activation delay) is the time the user has to disarm the security system after entering the premises. Learn more
Night mode delay when leaving	Delay when leaving in **Night mode**. Night mode delay when leaving (arming delay) is the time the user has to leave the premises after **Night mode** is enabled. Learn more

Night mode delay	Delay when entering in **Night mode** when the device is set to the **Follower** operating mode. It is the time the user has to disable **Night mode** (alarm activation delay) after the Entry/Exit detector is triggered. Learn more
Firmware	Device firmware version.
Device ID	Device ID. It is also available on the QR code on the device enclosure and its package box.
Device No.	Device number. This number is transmitted to the CMS in case of an alarm or event.

Settings



To change MotionCam Outdoor HighMount (PhOD) Jeweller settings in Ajax apps:

1. Go to the **Devices** tab.
2. Select **MotionCam Outdoor HighMount (PhOD) Jeweller** in the list.
3. Go to **Settings** .

4. Set the required settings.

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

Settings	Meaning
Name	Device name. It is 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 MotionCam Outdoor HighMount (PhOD) Jeweller is assigned. The room name is displayed in the text of SMS and notifications in the events feed.
Alarm LED indication	When this option is disabled, the LED indicator does not notify users of alarms and tamper triggering.

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.
Magnetic sensor sensitivity	Allows you to adjust the sensitivity level of the magnetic sensor. It is intended for cases when the specifics of the device installation can lead to frequent false alarms that the device position has been changed (e.g., in cases when the device is installed on a metal surface): • **Low** — allows you to reduce false alarms that the device has been moved. • **Normal** (by default) — is suitable for most installations when the device does not send false alarms that it has been moved.
Camera activation threshold	Allows you to adjust the threshold level of the camera activation. It is intended for cases when the device detects many movements, but they are filtered out as unconfirmed alarms. Each movement activates the camera, which leads to fast battery discharge. A high threshold reduces the number of camera activations in places with many movements and saves the battery life.

	Available threshold options: • **Normal** (by default) — is suitable when the device does not detect many movements that activate the camera. • **High** — allows you to reduce the number of camera activations when the device detects many movements that trigger the camera and reduce the battery life.
Anti-masking	When this option is enabled, the device detects masking.
Notify of sensors icing	When this option is enabled, the device notifies users if sensors are covered with ice and do not detect movement. The setting is displayed if the **Anti-masking** option is enabled.
Image resolution	The resolution of photos taken by the device camera: • **320 × 240** (by default) • **640 × 480** The higher the resolution, the more detailed the image is. It takes longer to transfer photos with higher resolution. The selected resolution is set for **Photo by alarm**, **Photo by scenario**, **Photo on demand**, **Photo by schedule**, and **Photo by arming/disarming**.
Photos by alarm	The number of photos taken by the device camera: • **No photo** • **1 photo** • **Series of 2**

	• **Series of 3** (by default) • **Series of 4** (only for 320 × 240 px image resolution) • **Series of 5** (only for 320 × 240 px image resolution) The selected number of photos is set for **Photo by alarm** and **Photo by scenario**.
Alarms with photo verification	The number of alarms accompanied by photos. You can choose whether the photo will be transmitted each time the device is triggered or specify the exact number of alarms: 1 to 10. An alarm counter with photo verification is reset when the security system is disarmed and rearmed. The setting is available if the **Always active** option is disabled. When the detector is in the **Always active** mode, it will transmit a photo every time it is triggered.
Photos on demand	The number of photos on demand: • **1 photo** • **Series of 2** • **Series of 3** • **Series of 4** (only for 320 × 240 px image resolution) • **Series of 5** (only for 320 × 240 px image resolution) It is displayed if the **Allow photos on demand** feature is enabled in the space settings in the **Privacy** section.

Always active	When this option is enabled, the detector is always in armed mode and detects movement. Learn more
Alert if moved	When this option is enabled, the device detects attempts to tilt, shift, or detach it from the surface.
Notify on risk of fast battery discharge	When this option is enabled, the user is notified when incorrect installation affects the device's battery life because the detector is often triggered without an actual intrusion.
Alert with a siren	
If motion detected	When this option is enabled, sirens are activated when the device detects the movement.
If masking detected	When this option is enabled, sirens are activated when the device detects masking. The parameter is displayed if the **Anti-masking** option is enabled.
If device was moved	When this option is enabled, the sirens are activated when the device detects attempts to tilt, shift, or detach it from the surface. The setting is displayed if the **Alert if moved** option is enabled.
Alarm reaction	
Operating mode	Specify how this device 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 the countdown and does not raise an alarm even if it is

	triggered before the countdown is completed. • **Follower** — the detector inherits the delays from Entry/Exit detectors. However, when the Follower is triggered individually, it immediately raises an alarm.
Delay when entering	Delay when entering: 5 to 255 seconds. Delay when entering (alarm activation delay) is the time the user has to disarm the security system after entering the premises. Learn more
Delay when leaving	Delay when leaving: 5 to 255 seconds. Delay when leaving (arming delay) is the time the user has to leave the premises after the system is armed. Learn more
Arm in Night mode	When this option is enabled, the detector will enter the armed mode if the system is set to **Night mode**. Learn more
Night mode delay when entering	Delay when entering in **Night mode**: 5 to 255 seconds. Night mode delay when entering (alarm activation delay) is the time the user has to disable **Night mode** after entering the premises. Learn more
Night mode delay when leaving	Delay when leaving in **Night mode**: 5 to 255 seconds.

	Night mode delay when leaving (arming delay) is the time the user has to leave the premises after enabling **Night mode**. Learn more
Night mode delay	Delay time in **Night mode**: 5 to 255 seconds. It is the time the 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
Scenarios	Opens the menu for creating and setting scenarios for the device. The menu allows you to create a scenario according to which the detector takes photos when specified Ajax devices are triggered or by schedule. Learn more
Firmware update	Switches the device to the firmware updating mode if a new version is available.
Motion detection area	Opens the menu for checking the motion detection area. You can take a photo to check the camera field of view and maximum detection zone. The photo helps to adjust the detector's tilt angle and horizontal position correctly. Learn more
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 device 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**
User guide	Opens the MotionCam Outdoor HighMount (PhOD) Jeweller user manual in an Ajax app.
Permanent deactivation	Allows a user to disable events of the device without removing it from the system. Three options are available: • **No** — the device operates in normal mode and transmits all events. • **Entirely** — the device does not execute system commands and does not

	participate in automation scenarios; the system ignores device alarms and other notifications. • **Lid only** — the system ignores only notifications that the device tamper is triggered. Learn more The system can also automatically deactivate devices when the set number of alarms is exceeded. Learn more
One-time deactivation	Allows a user to disable events of the device until the system is disarmed for the first time. Three options are available: • **No** — the device operates in normal mode and transmits all events. • **Entirely** — the device is entirely excluded from the system operation until the system is disarmed for the first time. The device does not execute system commands and does not report alarms or other events. • **Lid only** — notifications of the tamper triggering are disabled until the system is disarmed for the first time. Learn more
Delete device	Unpairs the device, disconnects it from the hub, and deletes its settings.

Configuring the motion detection area

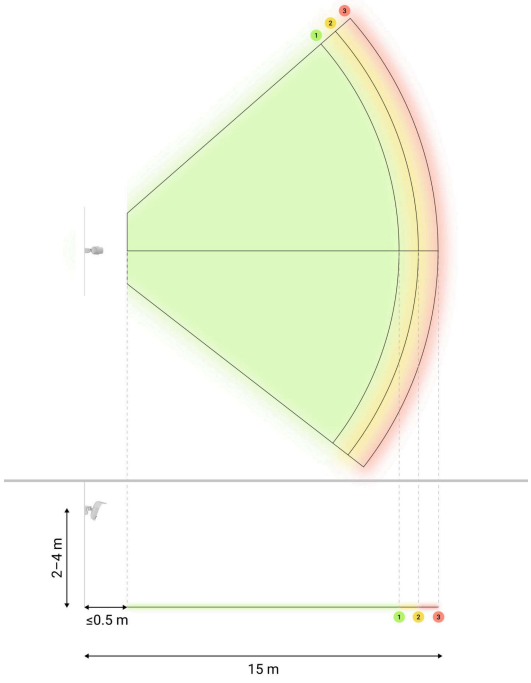
The **Motion detection area** feature allows taking a test photo to check the camera's field of view and the sensors' detection zones and ranges. The test photo helps adjust the detector's tilt angle and horizontal position. The proper device installation ensures efficient movement detection and prevents false alarms.

It is recommended that you check the motion detection area once the device is installed or if the installation place has been changed.

The tilt angle depends on the detector installation height. To set the proper tilt angle relative to the installation height, refer to the table below or the **Installation** section.

Tilt angle relative to the detector installation height

If the device tilt angle is correct, the ground distance from the point of device installation to the lower horizontal line of the motion detection area on the test photo **should not exceed 0.5 m**.



Before taking a test photo, ensure the user with admin rights has enabled the **Photo on demand** feature and provided your account permission to **Always** take

and view photos for this device in the Privacy settings. Otherwise, you will receive a message about a lack of permissions.

Configuring the Photo on demand feature

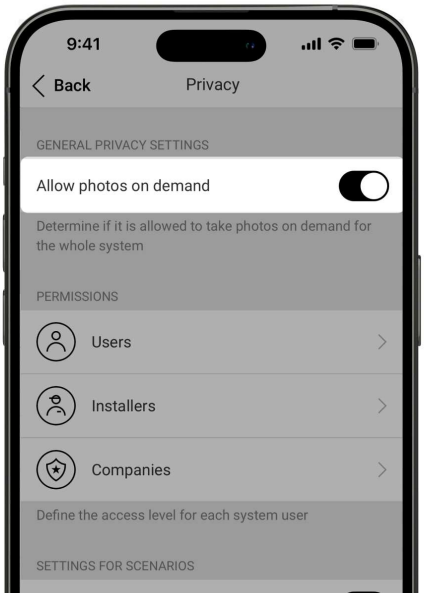
To take a test photo of the motion detection area, in an Ajax app:

1. Go to the **Devices** tab.
2. Select **MotionCam Outdoor HighMount (PhOD) Jeweller** from the list.
3. Go to **Settings**.
4. Go to the **Motion detection area** menu.
5. Tap **Take photo**.
6. The detector is installed correctly if:
    1. the photo shows the proper motion detection area;
    2. the ground distance from the point of device installation to the lower horizontal line of the motion detection area on the test photo does not exceed 0.5 m.

    If not, adjust the tilt angle and horizontal position of the detector and tap **Retake photo**.
7. Tap **Back** to close the photo.

You can download the test photo with sectors of the sensors' detection zones and ranges. The last test photo taken is also available in the **Motion detection area** menu, along with the date and time it was taken.

Configuring the Photo on demand feature



An admin or a user with access to privacy settings can enable and configure the **Photos on demand** feature. To do this, in an Ajax app:

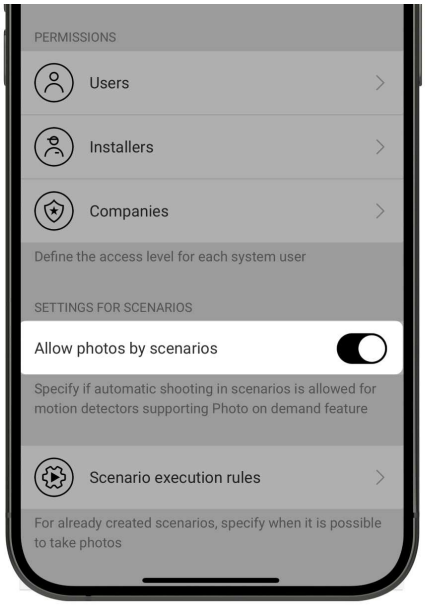
1. Select a space.
2. Go to the **Control** tab.
3. Go to the space **Settings**.
4. Go to the **Privacy** settings.
5. Enable the **Allow photos on demand** option.
6. Select the user category:
    - Users
    - Installers
    - Companies
7. Select a specific user, a PRO, or a company. A list of cameras, DVRs, and detectors supporting photo verification added to the space will open.
8. Select the device to which you want to provide access.
9. Enable the **Take & view photos** option.

10. Specify when the user can take on-demand photos: **Always** or **When device armed**.
11. Tap **Back** to save the settings.
12. Repeat steps 6–11 for any other user and devices to which you want to provide access.

After saving the privacy settings, all users who have access to the event feed will receive a notification of who has received access rights and which user has granted these rights.

Learn more

Configuring the Photo by scenario feature



First, you need to enable the **Photo by scenario** feature in the space **Privacy** settings. After that, it is possible to create scenarios for taking photos in case of alarms from the specified devices.

Enabling the Photo by scenario feature

An admin or a user with access to privacy settings can enable and configure the **Photo by scenario** feature. To do this, in an Ajax app:

1. Select a space.
2. Go to the **Control** tab.
3. Go to the space **Settings**.
4. Go to the **Privacy** settings.
5. Enable the **Allow photos by scenarios** option.
6. Tap **Back** to save the settings.

Learn more

Creating a scenario for taking photos by an alarm of a specified device

An admin or PRO with system configuration rights can create and configure a scenario by alarm. To do this, in an Ajax app:

1. Select a space.
2. Go to the **Devices** tab.
3. Select a detector supporting photo verification from the device list.
4. Go to its **Settings**.
5. Go to Scenarios and tap **Add scenario**.
6. Select the scenario type **By schedule**.
7. Select the devices and type of alarms that will trigger the photo verification.
8. Specify:

- **Name** of the scenario.
- **Devices triggering the scenario**. Select which devices trigger the scenario (available if two or more devices are selected for this scenario):
  - **Any** — the scenario will run if any selected device is triggered.

    - **All selected** — the scenario will run if all selected devices are triggered.

- **Max actuating time for all selected devices**. The time frame within which all selected devices should be triggered to run the scenario. Available only for the **All selected** option.
- **Device action** — only Take photo by default. The number of photos equals the number of **Photos by alarm** specified in the settings.
- **When the detector takes photos**: **Always** or **When armed**. By default, the motion detector takes photos by scenario only when armed.

> Note that only an admin can specify when the detector takes photos.

9. Tap **Save**. The scenario will appear in the list of device scenarios.

Configuring the Photo by schedule feature

An admin or PRO with system configuration rights can create and set up a scenario by schedule. To do this, in an Ajax app:

1. Select a space.
2. Go to the **Devices** tab.
3. Select a detector supporting photo verification from the device list.
4. Go to its **Settings**.
5. Go to **Scenarios** and tap the **Add scenario** button.
6. Select the **By schedule** scenario type.
7. Specify:

    - **Name** of the scenario.

- **Device action** — only **Take photo** by default. The number of photos equals the number of **Photos on demand** specified in the settings.
- **Execution time** — the time of a day when the detector takes photos by schedule.
- **Repeat** — the days of the week when the detector takes photos by schedule.
- **When the detector takes photos**: **Always** or **When armed**. By default, the motion detector takes photos by schedule only when armed.

> ⚠ Note that only an admin can specify when the detector should take photos.

8. Tap **Save**. The scenario will appear in the list of device scenarios.

Indication

The MotionCam Outdoor HighMount (PhOD) Jeweller LED indicator can light up green or red, depending on the device's state.

0:00 / 0:04

Indication upon pressing the power button

Event	Indication
Turning on the device.	Lights up green for about 0.5 s.
Turning on the device that has not been added to the hub.	Lights up green for about 0.5 s, flashes green 6 times, and flashes red 3 times rapidly.
Turning off the device.	Lights up red for about 1 s, then flashes 3 times.

Indication of activated device

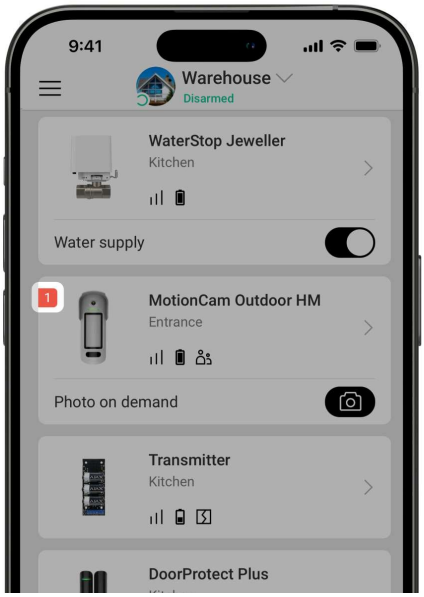
Event	Indication	Note
The device is added to the hub.	Lights up green for about 0.5 s.	
The device is deleted from the hub.	Flashes green six times for 2 s, then flashes red three times rapidly after 0.5 s.	
• Motion alarm. • Tamper alarm. • The device was moved (magnetometer alarm). • Masking is detected / restored to normal state. • Taking photos on demand.	Lights up green for about 0.6 s.	
The detection zone test of the motion sensors is running for the device.	Lights up green constantly and goes out for 0.6 s when movement 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, it lights up red again.	Learn more

Calibration of the masking sensor and magnetometer is in progress.	Lights up green for 0.5 s and goes out for 0.5 s.	Starts automatically when the device is installed on SmartBracket.
The battery charge is low.	Slowly lights up green and slowly goes out when the device is triggered.	The battery needs to be replaced.
The battery is completely discharged.	Flashes green continuously.	The battery needs to be replaced.
There is a device hardware error or sensor malfunction.	Lights up red for about 1 s every 4 s.	The device requires maintenance; contact our **Technical Support**.
Calibration of the masking sensor or magnetometer has failed.	Lights up red for about 1 s every 13 s.	Ensure the device is installed properly and nothing obstructs its field of view. Remove the device from SmartBracket and install it again to restart the calibration. If the indication appears again, contact our **Technical Support**.
Downloading a new firmware version of the device.	Lights up green twice and goes out every 3 s.	
The device firmware is being updated.	Flashes green 2 times every 1 s.	The indication lasts until the firmware update is finished.

Malfunctions

When the device detects a malfunction (for example, there is no connection via the Jeweller protocol), a malfunction counter is displayed in an 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 camera module is faulty. The device detects motion but cannot take photos.
- The device temperature is outside acceptable limits.
- The device lid is open (tamper is triggered).
- The masking sensor could not be adjusted.
- Magnetometer error.
- There is no connection with the hub or radio signal range extender via Jeweller.
- There is no connection with the hub or radio signal range extender via Wings.
- The device battery is low.

Maintenance

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

Do not use substances that contain alcohol, acetone, gasoline, and other active solvents to clean the device. Wipe the lens carefully, as scratches may impair the detector sensitivity.

The pre-installed batteries provide up to 3 years of the detector's battery life at the rate of 1 alarm per day with the standard Jeweller settings (the polling period is 36 seconds). The security system will send an appropriate notification if the detector batteries are nearly depleted. The LED will light up and go out gradually when the device detects any movement or if the tamper is triggered.

MotionCam Outdoor HighMount (PhOD) Jeweller can work up to 2 months after the low battery signal is received. We recommend replacing the batteries immediately upon notification. It is advisable to use lithium batteries, as they have a large capacity and are less affected by temperatures.

How long Ajax devices operate on batteries, and what affects this

Technical specifications

All technical specifications

Compliance with standards

Setup in compliance with EN 50131 requirements

Warranty

The warranty for the products of the "Ajax Systems Manufacturing" Limited Liability Company 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