

# Hub 2 Benutzerhandbuch

Aktualisiert November 15, 2020



**Ajax** ist ein funkgestütztes Sicherheitssystem für den Schutz vor Einbruch, Brand und Überschwemmung, das den Benutzern die Steuerung elektrischer Geräte über eine mobile App ermöglicht. Das System reagiert sofort auf Bedrohungen und informiert Sie und den Sicherheitsdienst über alle Vorfälle. Verwendung in Innenräumen.



**Hub 2** ist eine intelligente Zentrale für Sicherheitssysteme, die Melder mit Fotoverifizierung bei Einbrüchen unterstützt. Als zentrales Element des

Sicherheitssystems steuert es den Betrieb von Ajax-Geräten und übermittelt im Falle einer Bedrohung die Alarmsignale, um den Eigentümer und die zentrale Überwachungsstation unverzüglich über die Vorfälle zu informieren.

Für Hub 2 ist eine Internetverbindung erforderlich, um von jedem Ort der Welt über Ajax-Anwendungen auf den Ajax Cloud-Dienst zugreifen, die Übertragung von Alarmen und Ereignissen verfolgen und die Firmware OS Malevich aktualisieren zu können. Alle Daten werden in einem mehrstufig gesichertem System gespeichert und der Informationsaustausch mit dem Hub erfolgt über einen verschlüsselten Kanal.

Zur Kommunikation mit dem Ajax Cloud-Dienst verwendet der Hub eine kabelgebundene Internetverbindung (Ethernet) und zwei 2G-SIM-Karten. Es wird empfohlen, alle Kommunikationskanäle zu verwenden, um eine zuverlässigere Verbindung mit dem Ajax Cloud-Dienst sicherzustellen und sich gegen den Ausfall eines der Dienstanbieter zu schützen.

Benutzer können das Sicherheitssystem verwalten und umgehend auf Alarme und Benachrichtigungen mit den für iPhone und Smartphones mit Android, MacOS und Windows entwickelten Apps reagieren. Das System meldet Alarme und andere Ereignisse mithilfe von Push-Benachrichtigungen, SMS und Telefonanrufen.

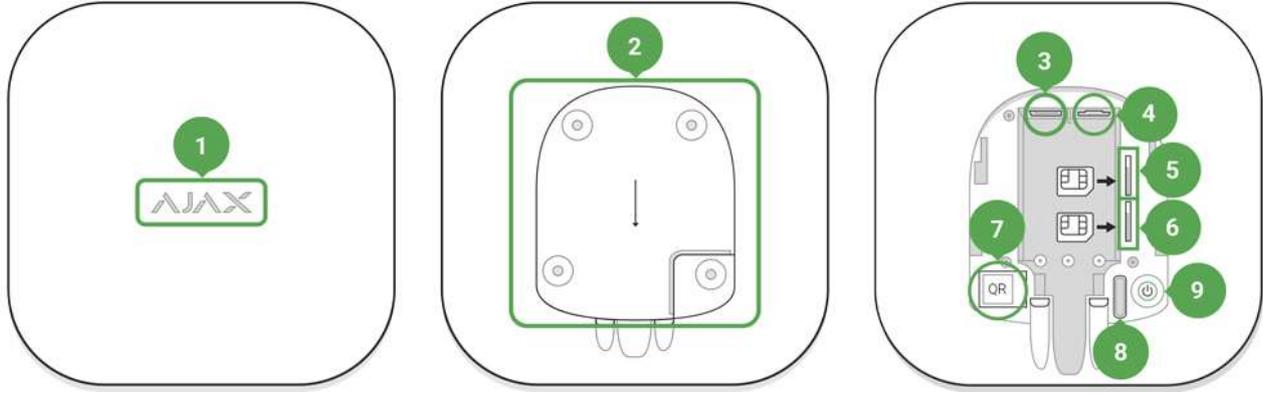
Mithilfe von Szenarien können Sie Abläufe im Rahmen des Sicherheitssystems automatisieren und wiederkehrende Vorgänge auf ein Minimum reduzieren. Passen Sie den Sicherheitszeitplan an und programmieren Sie das Verhalten der Automatisierungsgeräte (Relay, WallSwitch oder Socket) bei Auslösung des Alarms, bei Betätigung des Button oder nach Zeitplan. Ein Szenario kann auch mobil in der Ajax App angelegt werden.

### So erstellen und konfigurieren Sie ein Szenario im Ajax Sicherheitssystem



[Intelligente Alarmzentrale Hub 2 kaufen](#)

## Funktionselemente



1. Ajax-Logo mit Leuchtanzeige
2. SmartBracket-Montageplatte (zum Öffnen kräftig nach unten schieben; der perforierte Abschnitt ist für die Auslösung des Manipulationsalarm erforderlich, wenn versucht wird, den Hub von der Oberfläche abzureißen. Nicht abbrechen!)
3. Netzkabelanschluss
4. Ethernet-Kabelanschluss
5. Steckplatz 2: SIM-Karte (Typ micro-SIM)
6. Steckplatz 1: SIM-Karte (Typ micro-SIM)
7. QR-Code
8. Manipulationstaste
9. Ein/Aus-Taste

## Funktionsweise Hub 2

Der Hub sammelt in verschlüsselter Form Informationen über den Betrieb der angeschlossenen Geräte, analysiert die Daten und informiert im Alarmfall den Anlagenbetreiber in weniger als einer Sekunde über die Gefahr und übermittelt den Alarm direkt an die Überwachungszentrale des Sicherheitsdienstes.

Für den Datenaustausch mit den Geräten, die Überwachung ihres Betriebs und die zeitnahe Reaktion auf Bedrohungen nutzt Hub 2 die Jeweller-Funktechnik. Für die Übertragung von Bild- und Videodaten nutzt Hub 2 das Funkprotokoll Ajax Wings. Dabei handelt es sich um ein Hochgeschwindigkeitsprotokoll auf der Grundlage der Jeweller-Technologie. Die Kanalzuverlässigkeit wird bei Wings über eine gesonderte Antenne weiter optimiert.



## Hub-LED-Anzeige



Das Logo mit Leuchtanzeige kann je nach Gerätestatus rot, weiß oder grün leuchten.

Ereignis	Leuchtanzeige
Ethernet und mindestens eine SIM-Karte sind verbunden	Leuchtet weiß
Ein einzelner Kommunikationskanal ist verbunden	Leuchtet grün
Der Hub ist nicht mit dem Internet verbunden oder es besteht keine Verbindung zum Ajax Cloud-Dienst	Leuchtet rot
Kein Strom	Leuchtet 3 Minuten durchgehend und blinkt dann alle 20 Sekunden. Die Farbe der Anzeige hängt von der Anzahl der verbundenen Übertragungskanäle ab.

## Ajax-Account

Das Sicherheitssystem wird über Ajax-Anwendungen konfiguriert und verwaltet, die für iPhone und Android-Smartphones, macOS und Windows entwickelt

wurden.

Für die Systemkonfiguration muss die [Ajax App](#) installiert und ein Account eingerichtet sein. Wir empfehlen für die Verwaltung eines oder mehrerer Hubs die App "Ajax Security System". Für die Verwaltung von mehr als hundert Hubs empfehlen wir die App [Ajax PRO: Tools für Ingenieure](#) (für iPhone und Android-Smartphones) oder [Ajax PRO Desktop](#) (für PCs und Laptops mit Windows und MacOS). Bei der Einrichtung müssen E-Mail-Adresse und Telefonnummer bestätigt werden. Bitte beachten, dass die Telefonnummer und E-Mail-Adresse zum Erstellen nur eines Ajax-Accounts verwendet werden können! Es muss nicht für jeden Hub ein neuer Account erstellt werden – es können mehrere Hubs zu einem Account hinzugefügt werden.



Ein Account mit Informationen zu den hinzugefügten Hubs wird in verschlüsselter Form in den Ajax Cloud-Dienst hochgeladen.

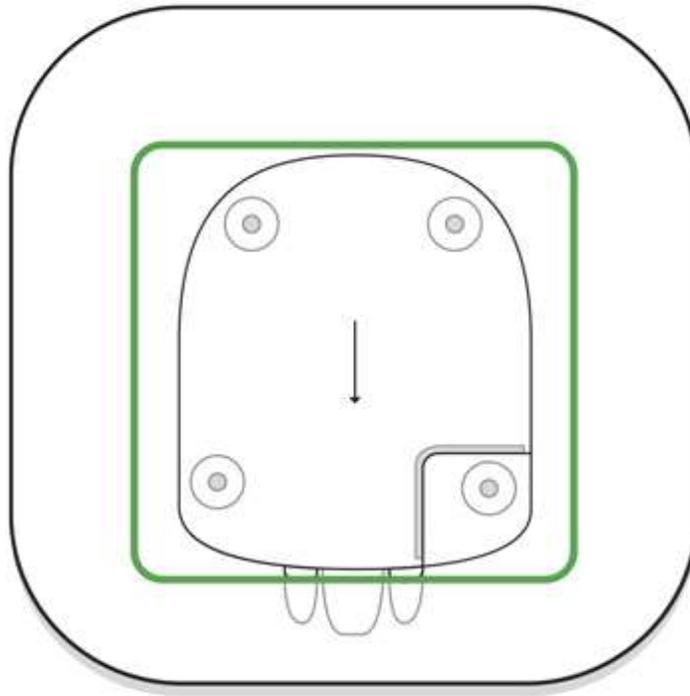
## Sicherheitsanforderungen

Bei Installation und Betrieb des Hub 2 sind die allgemeinen Sicherheitsbestimmungen für den Betrieb von elektrischen Geräten und die Anforderungen der gesetzlichen Bestimmungen zur elektrischen Sicherheit zu beachten.

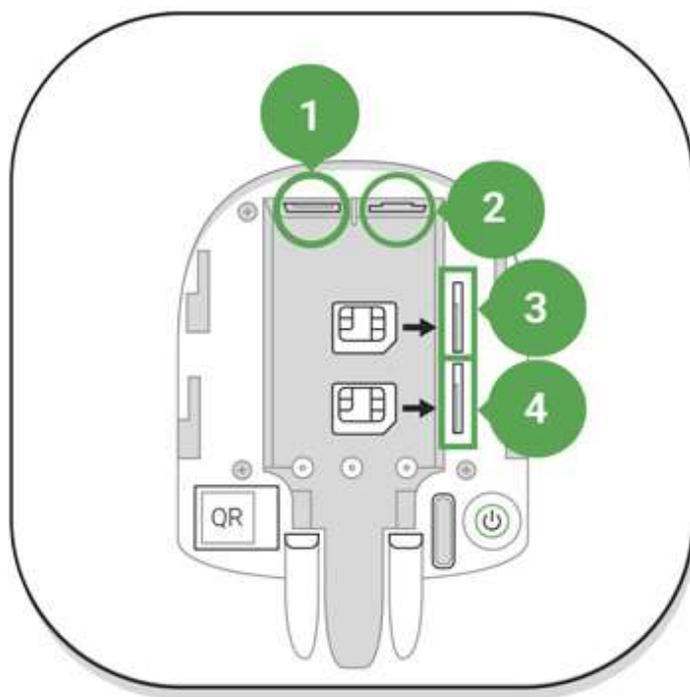
Es ist strengstens untersagt, das an die Stromversorgung angeschlossene Gerät zu zerlegen! Des Weiteren darf das Gerät nicht mit einem beschädigten Netzkabel betrieben werden.

## Hub-Anschluss

1. Deckel des Hubs kräftig nach unten schieben und abnehmen. Den perforierten Teil nicht beschädigen, da er zum Auslösen des Manipulationsalarms bei einem Hacking-Versuch am Hub erforderlich ist!



2. Netzkabel und Ethernet-Kabel mit den entsprechenden Anschlüssen verbinden.



- 1 – Netzkabelanschluss
- 2 – Ethernet-Anschluss
- 3, 4 – micro-SIM-Kartensteckplätze

3. Ein/Aus-Taster 3 Sekunden lang gedrückt halten, bis das Ajax-Logo aufleuchtet. Der Hub benötigt bis zu 2 Minuten, um auf die neueste Firmware-Version zu aktualisieren und auf das Internet zuzugreifen. Das

grüne oder weiße Logo zeigt an, dass der Hub in Betrieb und mit dem Ajax Cloud-Dienst verbunden ist.



Wenn die Ethernet-Verbindung nicht automatisch hergestellt wird, bitte die Proxy- und MAC-Adressfilterung deaktivieren und DHCP in den Router-Einstellungen aktivieren. Der Hub erhält jetzt automatisch eine IP-Adresse. Danach kann dem Hub in der Ajax-Anwendung eine statische IP-Adresse zugewiesen werden.

4. Für die Verbindung über GSM wird eine von einem Mobilfunkbetreiber ausgegebene Micro-SIM-Karte mit deaktivierter PIN-Abfrage (kann über Mobiltelefon deaktiviert werden) und ein ausreichendes Kontoguthaben benötigt, um die Dienste des Mobilfunkbetreibers zu bezahlen. Wenn der Hub nicht über GSM verbunden ist, müssen die Netzwerkbetreibereinstellungen (Roaming-Einstellungen, APN-Zugangspunkte, Benutzername und Kennwort) über Ethernet konfiguriert werden. Die Einstellungen des Mobilfunkanbieters können über dessen Kundendienst erfragt werden.

## Hinzufügen eines Hubs zur Ajax-App

1. Ajax-App aufrufen. Bitte sicherstellen, dass Zugriff auf alle angeforderten Systemfunktionen gewährt wird, insbesondere Berechtigungen zum Anzeigen von Benachrichtigungen. Für Android-Smartphones empfehlen wir die Verwendung der [Konfigurationsanweisungen für Push-Benachrichtigungen](#).
2. Melden Sie sich bei Ihrem Account an und klicken Sie auf **Hub hinzufügen**. Wählen Sie geeignetes Verfahren: manuell oder schrittweise Anleitung. Wenn Sie das System zum ersten Mal konfigurieren, empfehlen wir die schrittweise Anleitung.
3. Geben Sie dem Hub einen Namen und scannen Sie den QR-Code unter dem Deckel, oder geben Sie ihn manuell ein.
4. Warten Sie, bis das Hinzufügen des Hubs abgeschlossen ist. Nach dem Verknüpfen wird der Hub auf der Registerkarte **Geräte** angezeigt .

## Benutzer des Sicherheitssystems

Wenn Sie Ihrem Account einen Hub hinzufügen, werden Sie Administrator dieses Geräts. Auf einem Hub können bis zu 50 Benutzer/Administratoren angemeldet

sein. Der Administrator lädt Benutzer zur Verwendung des Sicherheitssystems ein und legt deren Berechtigungen fest.

Wenn der Administrator des Sicherheitssystems geändert oder aus der Hub-Liste gelöscht wird, werden die damit verknüpften Geräte nicht zurückgesetzt.



## Berechtigungen für Nutzer des Ajax-Sicherheitssystems

## Hub-Zentralen-Status

### Symbole

Die Symbole zeigen einige der Status von Hub 2 an. Sie können sie in der Ajax App im Menü **Geräte** sehen .

Symbole	Wert
	2G verbunden
	SIM-Karte nicht installiert
	Die SIM-Karte ist defekt oder hat einen PIN-Code
	Akku/Batterie-Ladezustand von Hub 2. Anzeige in 5%-Schritten
	Hub 2-Fehlfunktion wird erkannt. Die Liste wird in der Statusliste der Hub-Zentrale angezeigt
	Die Hub-Zentrale ist direkt mit der Überwachungszentrale des Sicherheitsdienstes verbunden
	Die Hub-Zentrale ist nicht mehr direkt mit der Überwachungszentrale des Sicherheitsdienstes verbunden

### Status

Status sind in der [Ajax App](#) aufgeführt:

1. Öffnen Sie die Registerkarte **Geräte** .
2. Wählen Sie Hub 2 aus der Liste aus.

--	--

Parameter	Bedeutung
Störung	<p>Öffnen Sie mit einem Klick auf  die Liste der Fehlfunktionen des Hub 2.</p> <p>Das Feld erscheint nur bei einer erkannten Störung</p>
Mobilfunk-Signalstärke	<p>Zeigt die Signalstärke des Mobilfunknetzes für die aktive SIM-Karte an. Wir empfehlen, die Hub-Zentrale an Orten mit einer Signalstärke von 2 bis 3 Balken zu installieren. Bei zu geringer Signalstärke kann sich die Hub-Zentrale nicht einwählen bzw. keine SMS zu einem Ereignis oder Alarm senden</p>
Akku-Ladung	<p>Batterie-/Akkuladezustand. Anzeige in 5%-Schritten</p>
Gehäusedeckel	<p>Status des Manipulationsschutzes vor Demontage der Hub-Zentrale:</p> <ul style="list-style-type: none"> <li>• Geschlossen – Gehäusedeckel der Hub-Zentrale ist geschlossen</li> <li>• Geöffnet – die Hub-Zentrale wurde aus der SmartBracket-Halterung entfernt</li> </ul> <p><b><u>Was ist ein Manipulationsschutz?</u></b></p>
Externe Stromversorgung	<p>Status für externen Stromversorgungsanschluss:</p> <ul style="list-style-type: none"> <li>• Verbunden – die Hub-Zentrale ist an eine externe Stromversorgung angeschlossen</li> <li>• Getrennt – keine externe Stromversorgung</li> </ul>
Verbindung	<p>Verbindungsstatus zwischen Hub-Zentrale und Ajax Cloud:</p> <ul style="list-style-type: none"> <li>• Online – Hub-Zentrale ist mit der Ajax Cloud verbunden</li> <li>• Offline – Hub-Zentrale ist nicht mit der Ajax Cloud verbunden</li> </ul>
Mobilfunk	<p>Der Verbindungsstatus der Hub-Zentrale zum Mobilfunknetz:</p>

	<ul style="list-style-type: none"> <li>• Verbunden – die Hub-Zentrale ist über mobiles Internet mit der Ajax Cloud verbunden</li> <li>• Getrennt – die Hub-Zentrale ist nicht über das mobile Internet mit der Ajax Cloud verbunden</li> </ul> <p>Wenn die Hub-Zentrale über genügend Guthaben auf dem Konto oder über Bonus-SMS/Anrufe verfügt, kann sie Anrufe tätigen und SMS-Nachrichten senden, auch wenn der Status <b>Getrennt</b> in diesem Feld angezeigt wird</p>
Aktiv	Zeigt die aktive SIM-Karte an: SIM-Karte 1 oder SIM-Karte 2
SIM 1	Die Nummer der SIM-Karte im ersten Steckplatz. Kopieren Sie die Nummer, indem Sie sie anklicken
SIM 2	Die Nummer der SIM-Karte im zweiten Steckplatz. Kopieren Sie die Nummer, indem Sie sie anklicken
Ethernet	<p>Internetverbindungsstatus der Hub-Zentrale über Ethernet:</p> <ul style="list-style-type: none"> <li>• Verbunden – die Hub-Zentrale ist über Ethernet mit der Ajax Cloud verbunden</li> <li>• Getrennt – die Hub-Zentrale ist nicht über Ethernet mit der Ajax Cloud verbunden</li> </ul>
Mittlerer Rauschpegel (dBm)	<p>Rauschleistungspegel am Installationsort der Hub-Zentrale. Die ersten beiden Werte zeigen den Pegel bei Jeweller- und der dritte den bei Wings-Frequenzen an.</p> <p>Der akzeptable Wert beträgt -80 dBm oder weniger</p>
Überwachungsstation	<p>Der Status der Direktverbindung der Hub-Zentrale zur Überwachungszentrale des Sicherheitsdienstes:</p> <ul style="list-style-type: none"> <li>• Verbunden – die Hub-Zentrale ist direkt mit der Überwachungszentrale des Sicherheitsdienstes verbunden</li> </ul>

- Getrennt – die Hub-Zentrale ist nicht direkt mit der Überwachungszentrale des Sicherheitsdienstes verbunden

Wenn dieses Feld angezeigt wird, nutzt der Sicherheitsdienst eine Direktverbindung für den Empfang von Ereignissen und Alarmen des Sicherheitssystems.

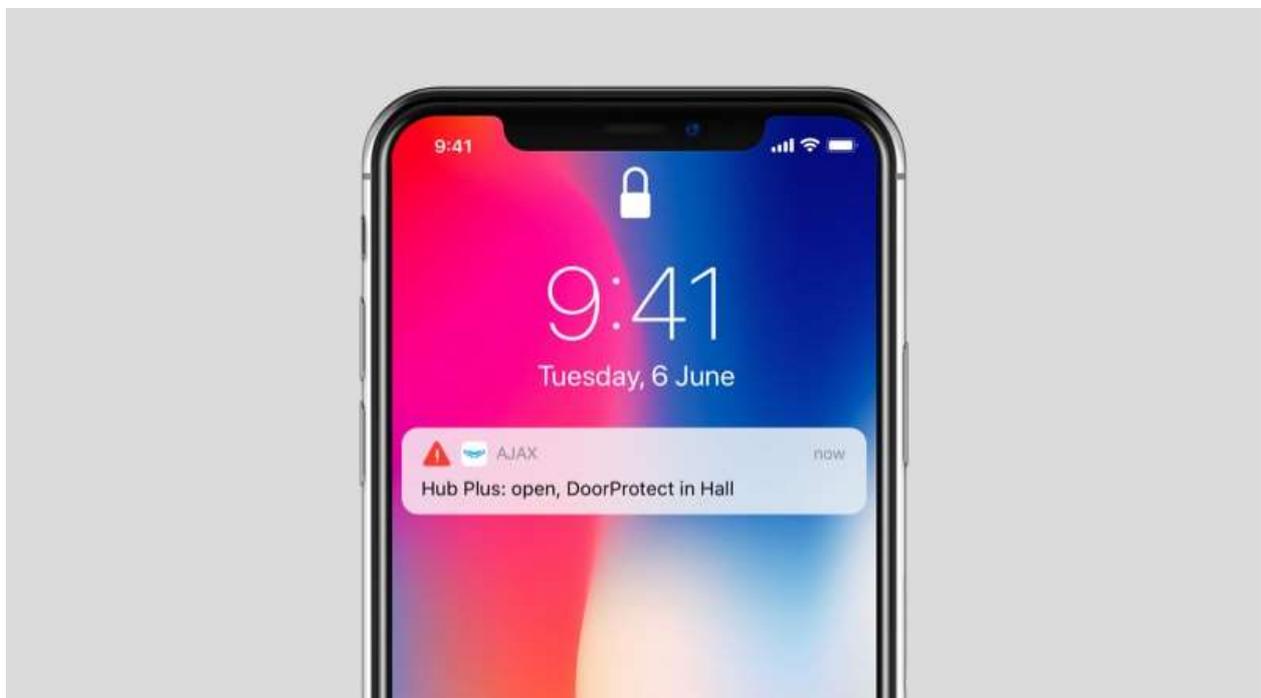
### Was ist eine Direktverbindung?

Hub-Modell	Hub-Modellname
Hardwareversion	Hardwareversion. Aktualisierung nicht möglich
Firmware	Firmwareversion. Kann mobil aktualisiert werden
ID	ID/Seriennummer. Befindet sich auch auf der Gerätebox, auf der Geräteplatine und auf dem QR-Code unter der SmartBracket-Montageplatte

## Erstellung eines Raumes

Vor dem Verknüpfen des Geräts mit dem Hub muss mindestens ein Raum erstellt werden.

In der Geräteereignisbeschreibung wird der Raum angegeben, in dem sich das Gerät befindet:



Um einen Raum zu erstellen, gehen Sie zur Registerkarte **Raum**  und klicken Sie auf **Raum hinzufügen**. Weisen Sie ihm einen Namen zu und hängen Sie gegebenenfalls ein Foto an (oder erstellen Sie ein Foto) – dadurch wird es einfacher, einen Raum in der Liste zu finden.

Um einen Raum zu löschen bzw. seinen Avatar oder Namen zu ändern, gehen Sie zu den Raumeinstellungen (klicken Sie auf das Zahnradsymbol .

## Anschluss von Meldern und Geräten

Wenn Sie einen Hub mithilfe einer schrittweisen Anleitung hinzufügen, werden Sie aufgefordert, Geräte für den Schutz der Bereiche Räumlichkeiten hinzuzufügen. Sie können dies jedoch ablehnen und diesen Schritt später erneut ausführen.

### So fügen Sie dem Hub ein Gerät hinzu:

1. Öffnen Sie in der Ajax-Anwendung den Raum und wählen Sie **Gerät hinzufügen**.
2. Benennen Sie das Gerät, scannen Sie den QR-Code (oder geben Sie ihn manuell ein) und wählen Sie eine Gruppe aus (falls der Gruppenmodus aktiviert ist).
3. Klicken Sie auf Hinzufügen und der Countdown der verbleibenden Zeit für das Hinzufügen eines Geräts beginnt.
4. Schalten Sie das Gerät während des Countdowns ein und dessen LED leuchtet einmal auf. Für die Verknüpfung eines Geräts mit dem Hub muss sich dieses innerhalb der Funkreichweite des Hubs befinden (am selben gesicherten Bereich).

Wenn die Verbindung fehlschlägt, schalten Sie das Gerät für 5 Sekunden aus und versuchen es erneut.



[Wie man eine IP-Kamera konfiguriert und an das Ajax-Sicherheitssystem anschließt](#)

## Videüberwachung

Sie können Kameras von Drittanbietern an das Sicherheitssystem anschließen: Die nahtlose Integration von IP-Kameras und -Videorecordern von Dahua, Hikvision und Safire wurde vorbereitet, aber es können auch Kameras von weiteren Drittanbietern angeschlossen werden, die das RTSP-Protokoll

unterstützen. Es können bis zu 25 Videoüberwachungsgeräte an das System angeschlossen werden.



[Eine Kamera oder einen Videorecorder von Dahua hinzufügen](#)



[Eine Kamera oder einen Videorecorder von Hikvision/Safire hinzufügen](#)

## Hub-Einstellungen

Um die Hub-Einstellungen vorzunehmen, das Gerät in der Geräteliste auswählen und auf das Zahnradsymbol  klicken.

### Anpassbare Parameter:

**Avatar** – Anpassung des Titelbildes des Ajax-Sicherheitssystems. Dieses wird im Auswahlmenü der Hubs angezeigt und hilft bei der Identifizierung des gewünschten Objekts.

Um den Avatar zu ändern, klicken Sie auf das Kamerasymbol und wählen Sie das gewünschte Bild aus.

**Name des Hubs.** Dieser wird in Push-Benachrichtigungen und SMS angezeigt. Der Name kann bis zu 12 Zeichen im kyrillischen Alphabet oder bis zu 24 Zeichen im lateinischen Alphabet lang sein.

Um den Namen zu ändern, klicken Sie auf das Bleistift-Symbol und geben Sie den gewünschten Hub-Namen ein.

**Benutzer** – Sicherheitseinstellungen für Benutzer. Sie legen fest, welche Benutzer Zugriff auf Ihr Sicherheitssystem haben, welche Berechtigungen gewährt werden und wie das Sicherheitssystem diese Benutzer über Ereignisse benachrichtigt.



[So meldet das Ajax-Sicherheitssystem Alarme](#)



[So fügen Sie dem Hub neue Benutzer hinzu](#)

**Ethernet** – Einstellungen für die kabelgebundene Internetverbindung.

**Mobilfunk** – Aktivieren/Deaktivieren der Mobilfunkverbindung, Einrichten der Verbindung und Überprüfen des Kontoguthabens.

**Geofence** – Konfigurieren von Erinnerungen zum Aktivieren/Deaktivieren des Sicherheitssystems bei Betreten/Verlassen einer bestimmten Zone. Der Standort des Benutzers wird mithilfe des GPS-Moduls des Smartphones ermittelt.



[Was sind Geofences und wie funktionieren sie](#)

**Gruppen** – Konfiguration des Gruppenmodus.

Die Funktionen des Gruppenmodus:

- Verwaltung der Sicherheit einzelner Bereiche oder Gruppen von Meldern.  
Das Büro ist gesichert, während die Reinigungskraft in der Küche arbeitet.
- Differenzierte Berechtigungen für die Administrationstools der Sicherheitsmodi.

Mitarbeiter der Marketingabteilung haben keinen Zugang zur Anwaltskanzlei.



### Hub OS Malevich 2.6: Neue Sicherheitsstufe

**Sicherheitszeitplan** – Scharf-/Unscharfschaltung des Sicherheitssystems nach einem Zeitplan.



### So erstellen und konfigurieren Sie ein Szenario im Ajax Sicherheitssystem

**Erfassungsbereichtstest** – Überprüfung des Erfassungsbereichs der an den Hub angeschlossenen Melder. Bei diesem Test kann die Entfernung festgelegt werden, bei der die Melder einen Alarm melden.



### Was der Test der Erkennungszone ist

**Jeweller** – Einstellen des Abfragezeitraums für den Hub und die angeschlossenen Geräte. Die Einstellungen bestimmen, wie oft der Hub Daten mit den Geräten austauscht und wie schnell der Kommunikationsverlust erkannt wird.



### Mehr erfahren

- **Ping-Intervall des Melders** – die Häufigkeit der Abfrage der angeschlossenen Geräte durch den Hub, einstellbar von 12 bis 300 Sekunden (Standard: 36).

- **Anzahl nicht zugestellte Pakete bis Verbindungsfehler** – ein Zähler für nicht zugestellte Pakete (Standard: 30 Pakete).

**Die Zeit bis zum Senden einer Nachricht bezüglich des Kommunikationsverlusts zwischen Hub und Gerät wird mit folgender Formel berechnet:**

*Abfrageintervall \* (Anzahl der nicht zugestellten Pakete + 1 Korrekturpaket)*

Je kürzer der Abfragezeitraum ist, desto schneller empfängt der Hub Informationen über die Ereignisse von den angeschlossenen Geräten und die Geräte empfangen Hub-Befehle. Dies verringert jedoch die Betriebszeit der Geräte mit den mitgelieferten Batterien. Ansonsten werden die Informationen über einen Alarm oder eine Sabotage sofort übermittelt.

Beachten Sie, dass das Intervall die maximale Anzahl der angeschlossenen Geräte begrenzt:

Intervall	Max. Geräte
12 s	39 Geräte
24 s	79 Geräte
36 s oder mehr	100 Geräte

Unabhängig von den Einstellungen können maximal 10 Sirenen an den Hub angeschlossen werden!

**Service** – die Service-Einstellungen der Hub-Zentrale sind in zwei Gruppen unterteilt: allgemeine Einstellungen und erweiterte Einstellungen.

### **Allgemeine Einstellungen**

#### **Zeitzone**

Festlegen der Zeitzone für die Hub-Zentrale. Diese wird für Szenarien verwendet, welche nach Zeitplan arbeiten. Stellen Sie also die richtige Zeitzone ein, bevor Sie die Szenarien erstellen.



## Erfahren Sie mehr über Szenarien

### LED-Helligkeit

Helligkeitseinstellung der LED-Anzeige des Hub-Logos. Die Helligkeit wird im Bereich von 1 bis 10 angegeben. Der Standardwert liegt bei 10.

## Automatische Software-Aktualisierung

Einrichten eines automatischen Software-Updates von OS Malevich.

- **Falls eingeschaltet**, wird die Software automatisch aktualisiert, wenn eine neue Version verfügbar ist. Die Alarmanlage muss dafür unscharf geschaltet sein und darüber hinaus extern mit Strom versorgt werden.
- **Falls ausgeschaltet**, wird die Software nicht automatisch aktualisiert. Die App informiert Sie darüber, wenn eine neue Software-Version des Betriebssystems OS Malevich verfügbar ist.



## Wie OS Malevich aktualisiert wird

### Systembericht der Hub-Zentrale



Die Logdateien stellen Informationen über die Funktionsweise des Systems zur Verfügung. Sie können dabei helfen, eine Fehlerquelle zu identifizieren und diese zu beheben.

Diese Einstellung ermöglicht Ihnen, entweder einen Kanal für die Datenübertragung der Logdateien aus der Hub-Zentrale auszuwählen oder deren Protokollierung zu deaktivieren:

- Ethernet
- Nein – Protokollierung ist deaktiviert



Wir raten davon ab, die Protokolle zu deaktivieren, da diese im Falle von Systemfehlern helfen können!



### Erweiterte Einstellungen

Die Liste der erweiterten Hub-Einstellungen ist von der genutzten App abhängig: Ajax Security System oder PRO: Tool for Engineers.

Ajax Security System	Ajax PRO
Serververbindung Sirenen-Einstellungen Feuermelder-Einstellungen Systemintegritätsprüfung	PD 6662-Einstellungsassistent Serververbindung Sirenen-Einstellungen Feuermelder-Einstellungen Systemintegritätsprüfung Alarmverifizierung Wiederherstellung nach Alarm Vorgang zur Scharf-/Unscharfschaltung Automatische Gerätedeaktivierung

### PD 6662-Einstellungsassistent

Öffnet einen Einstellungsassistenten (Schritt-für-Schritt Anleitung) zur Konfiguration des Systems gemäß britischem PD 6662:2017.



[Erfahren Sie mehr über PD 6662:2017](#)



[Wie man das System gemäß PD 6662:2017 konfiguriert](#)

### Serververbindung

Das Menü enthält Einstellungen für die Verbindung zwischen der Hub-Zentrale und der Ajax-Cloud:

- **Hub-Server Abfrageintervall.** Wie oft die Hub-Zentrale Abfragen der Ajax-Cloud vornimmt. Das Intervall kann im Bereich von 10 bis 300 Sekunden festgelegt werden. Der empfohlene und voreingestellte Wert beträgt 60 Sekunden.
- **Verbindungsausfall-Alarmverzögerung.** Diese gibt eine Verzögerung zur Verringerung des Risikos von Fehlalarmen beim Verbindungsverlust zwischen der Hub-Zentrale und der Ajax-Cloud vor. Sie wird nach drei erfolglosen Abfragen vom Hub-Server aktiviert und kann im Zeitintervall

von 30 bis 600 Sekunden liegen. Der empfohlene und voreingestellte Wert beträgt 300 Sekunden.

Die Zeit, bevor eine Benachrichtigung über den Verbindungsverlust zwischen der Hub-Zentrale und der Ajax-Cloud versendet wird, errechnet sich über folgende Formel:

$$(Sever-Ping-Intervall * 4) + Verbindungsausfall-Alarmverzögerung$$

Bei Standardeinstellungen registriert die Ajax-Cloud den Verbindungsverlust zur Hub-Zentrale nach 9 Minuten:

$$(60 s * 4) + 300 s = 9 \text{ Minuten}$$

- **Alarme über Verbindungsverlust zum Server deaktivieren.** Ajax-Apps können Sie auf zwei verschiedene Arten über einen Verbindungsverlust zwischen der Hub-Zentrale und dem Server benachrichtigen: mit der standardmäßigen Push-Benachrichtigung oder mit einem Alarmton (standardmäßig aktiviert). Wenn diese Option aktiviert ist, kommt die Push-Benachrichtigung mit einem Standardton.

## Sirenen-Einstellungen

Das Menü enthält zwei Einstellmöglichkeiten für Sirenen: Alarmierung durch Sirene und Anzeige nach Alarmauslösung.

## Sirenenaktivierungsparameter

**Wenn ein Gehäuse geöffnet ist (Hub-Zentrale oder Melder).** Bei aktivierter Funktion, schaltet die Hub-Zentrale die Ajax-Sirenen ein, wenn das Gehäuse der Hub-Zentrale, der Melder, oder von einem anderen Gerät geöffnet wird.

**Bei betätigter Paniktaste in der App.** Bei aktivierter Funktion, schaltet die Hub-Zentrale die Ajax-Sirenen ein, wenn die Paniktaste in der Ajax-App betätigt wird.



Sie können die Sirenenauslösung deaktivieren zur Betätigung der Paniktaste auf dem SpaceControl. Dies kann in den Einstellungen von SpaceControl vorgenommen werden (Geräte → SpaceControl → Einstellungen .

## Anzeige nach Alarmauslösung



Diese Funktion ist nur in den [Ajax PRO-Apps](#) verfügbar

Mithilfe der LED-Anzeige kann die Sirene über einen Alarm informieren. Dank dieser Funktion können Systembenutzer und vorbeifahrende Einsatzteams eines Wachunternehmens sehen, dass es im System einen Alarm gab.



[Funktionsweise in HomeSiren](#)



[Funktionsweise in StreetSiren](#)



[Funktionsweise in StreetSiren DoubleDeck](#)

## Feuermelder-Einstellungen

Einstellungsmenü für FireProtect und FireProtect Plus. Ermöglicht Ihnen einen gekoppelten Rauchmelder-Alarm einzurichten.

Diese Funktion wird von den europäischen Brandschutznormen empfohlen. Im Brandfall soll eine Alarmlautstärke von mindestens 85 dB in einem Abstand von 3 Metern zur Lärmquelle erreicht werden. Diese Lautstärke ermöglicht es, auch eine tief schlafende Person während eines Brandes aufzuwecken. Sie können die ausgelösten Brandmelder mit der Ajax-App, dem Button oder dem KeyPad stummschalten.



[Mehr erfahren](#)

## Systemintegritätsprüfung

Die **Systemintegritätsprüfung** ist eine Funktion, die für die Überprüfung des Zustands aller Melder und Geräte verantwortlich ist, bevor diese scharf geschaltet werden. Standardmäßig ist die Prüfung deaktiviert.



[Mehr erfahren](#)

## Alarmverifizierung



Diese Funktion ist nur in den [Ajax PRO-Apps](#) verfügbar

Die **Alarmverifizierung** ist ein spezielles Ereignis, das die Hub-Zentrale an die Leitstelle und die Systembenutzer sendet, wenn mehrere Melder innerhalb eines bestimmten Zeitraumes ausgelöst wurden. Ein überflüssiges Ausrücken von Sicherheitsfirmen und Polizei wird somit durch unsere Alarmverifizierungsfunktion vermieden.



[Mehr erfahren](#)

## Wiederherstellung nach Alarm



Diese Funktion ist nur in den [Ajax PRO-Apps](#) verfügbar

Die Systemwiederherstellungsfunktion verhindert eine Scharfschaltung des Systems, wenn zuvor ein Alarm verzeichnet wurde. Um das System scharf zu schalten, muss es von einem autorisierten Benutzer oder PRO-Benutzer wiederhergestellt werden. Die verschiedenen Alarmtypen, die eine Wiederherstellung des Systems erfordern, werden bei der Einrichtung definiert.

Diese Funktion verhindert, dass der Benutzer ein System scharf schalten kann, in welchem sich Melder befinden, die Fehlalarme generieren.



[Mehr erfahren](#)

## Vorgang zur Scharf-/Unscharfschaltung



Diese Funktion ist nur in den [Ajax PRO-Apps](#) verfügbar

Über dieses Einstellungsmenü können Sie die zweistufige Scharfschaltung aktivieren sowie eine Alarmübermittlungsverzögerung beim Unscharfschalten des Systems festlegen.



[Was ist der zweistufige Scharfschaltungsprozess und warum wird dieser benötigt](#)



[Was ist die Alarmübermittlungsverzögerung und warum wird diese benötigt](#)

## Automatische Gerätedeaktivierung



Diese Funktion ist nur in den [Ajax PRO-Apps](#) verfügbar

Das Ajax-Sicherheitssystem kann Alarme oder andere Ereignisse der Melder ignorieren, ohne diese aus dem System entfernen zu müssen. Sie können das System so einrichten, dass Benachrichtigungen über Ereignisse von bestimmten Meldern weder an die Benutzer noch an die Leitstelle gesendet werden.

Dafür können Sie die **automatische Gerätedeaktivierung** einrichten: nach Timer und nach Alarmanzahl.



[Was ist die automatische Gerätedeaktivierung](#)

Es besteht ebenfalls die Möglichkeit, ein bestimmtes Gerät manuell zu deaktivieren. Mehr über die manuelle Gerätedeaktivierung erfahren Sie unter folgendem [Link](#).

## Löschen des Hub-Ereignisspeichers

Wenn Sie den Knopf betätigen, werden alle Benachrichtigungen im Ereignisprotokoll der Hub-Zentrale gelöscht.

**Sicherheitsunternehmen** – eine Liste der Sicherheitsdienste in Ihrer Nähe. Das Gebiet wird durch die GPS-Daten oder die regionalen Einstellungen Ihres Smartphones bestimmt.

**Überwachungszentrale** – die Einstellungen für die direkte Verbindung zur Überwachungszentrale des Sicherheitsdienstes.



Die Ereignisse und Alarmer können ohne diese Einstellungen an die zentrale Überwachungsstation des Sicherheitsdienstes übermittelt werden



[Die Überwachungsstation](#)

**PRO** – Einstellungen für PRO-Benutzer (Installateure und Vertreter von Sicherheitsdiensten) des Sicherheitssystems. Sie legen fest, welche Benutzer Zugriff auf Ihr Sicherheitssystem haben, welche Berechtigungen gewährt werden und wie das Sicherheitssystem diese Benutzer über Ereignisse benachrichtigt.

**Benutzerhandbuch** – öffnet das Hub 2-Benutzerhandbuch.

**Datenimport** – Ein Menü zur automatischen Übertragung von Geräten und Einstellungen von einer anderen Hub-Zentrale. **Beachten Sie, dass Sie sich in den Einstellungen derjenigen Hub-Zentrale befinden, in die Sie Daten importieren möchten.**

**Hub entkuppeln** – entfernt Ihr Konto aus der Hub-Zentrale. Hierbei werden alle Einstellungen und mit der Hub-Zentrale verbundene Melder gespeichert.

## Zurücksetzen der Hub-Einstellungen

Setzen Sie den Hub auf die Werkseinstellungen zurück:

1. Schalten Sie den Hub ein, wenn er ausgeschaltet ist.
2. Entfernen Sie alle Benutzer und Installateure vom Hub.
3. Halten Sie den Ein/Aus-Taster für 30 Sekunden gedrückt – das Ajax-Logo auf dem Hub beginnt rot zu blinken.
4. Löschen Sie den Hub aus Ihrem Account.

## Meldungen über Ereignisse und Alarme

Das Ajax-Sicherheitssystem informiert den Benutzer über Meldungen und Ereignisse mithilfe von drei Arten von Benachrichtigungen: Push-Nachrichten, SMS und Telefonanrufe. Die Meldeeinstellungen können nur für angemeldete Benutzer geändert werden.

Arten von Ereignisse	Zweck	Arten von Benachrichtigungen
Störungen	<ul style="list-style-type: none"><li>• Verbindungsverlust zwischen Gerät und Hub</li><li>• Funkstörung (Jamming)</li><li>• Niedrige Batterieladung im Gerät oder Hub</li><li>• Abdeckung</li></ul>	Push-Nachrichten SMS

	<ul style="list-style-type: none"> <li>• Manipulieren des Meldergehäuses</li> </ul>	
Alarm	<ul style="list-style-type: none"> <li>• Einbruch</li> <li>• Brand</li> <li>• Überschwemmung</li> <li>• Der Hub hat die Verbindung zum Ajax Cloud-Dienst verloren</li> </ul>	Anrufe Push-Nachrichten SMS
Ereignisse	<ul style="list-style-type: none"> <li>• Ein-/Ausschalten von <u>WallSwitch</u>, <u>Relay</u>, <u>Socket</u></li> </ul>	Push-Nachrichten SMS
Scharf-/Unscharfschaltung	<ul style="list-style-type: none"> <li>• Scharf-/Unscharfschaltung ganzer Bereiche/Objekte oder Gruppen</li> <li>• Nachtmodus aktivieren</li> </ul>	Push-Nachrichten SMS



## So informiert Ajax die Benutzer über Alarme

## Verbindung zu einem Sicherheitsdienst herstellen

Die Liste der Organisationen, die das System mit den zentralen Überwachungsstationen der Organisationen verbinden, finden Sie im Menü **Sicherheitsdienste (Geräte  > Hub > Einstellungen  > Wachschutzunternehmen):**

Wenden Sie sich an die Vertreter des Unternehmens, das solche Dienstleistungen in Ihrer Nähe erbringt, und veranlassen Sie die Anbindung.

Die Anbindung an die Überwachungszentrale (CMS) wird über die Kontakt-ID oder das SIA-Protokoll hergestellt.

## Montage

Stellen Sie vor der Installation des Hubs sicher, dass Sie den optimalen Standort ausgewählt haben und dass dieser den Anforderungen dieser Anleitung entspricht! Der Hub sollte vor neugierigen Blicken geschützt sein.



Gerät ist nur für die Innenraummontage vorgesehen.

Stellen Sie sicher, dass der Hub bei allen angeschlossenen Geräten eine stabile Signalstärke aufweist. Wenn die Signalstärke niedrig ist (ein einzelner Balken), garantieren wir keinen stabilen Betrieb des Sicherheitssystems. Ergreifen Sie mögliche Maßnahmen zur Verbesserung der Signalqualität! Zumindest sollte der Hub neu positioniert werden, da bereits eine Verlagerung um 20 cm den Signalempfang erheblich verbessern kann.

Wenn nach der Verlegung eine geringe oder instabile Signalstärke gemeldet wird, verwenden Sie einen ReX-Funksignal-Reichweiten Repeater.

Bei Installation und Betrieb des Geräts sind die allgemeinen Sicherheitsbestimmungen für den Betrieb von elektrischen Geräten und die Anforderungen der gesetzlichen Bestimmungen zur elektrischen Sicherheit zu beachten.

### **Hub-Installation:**

1. Befestigen Sie die SmartBracket-Montageplatte mit den mitgelieferten Schrauben. Achten Sie bei Verwendung anderer Befestigungselemente darauf, dass diese die Platte nicht beschädigen oder verformen.



Doppelseitiges Klebeband wird für die Montage nicht empfohlen. Dies kann dazu führen, dass ein Hub herunterfällt und das Gerät aufgrund der Stoßbelastung ausfällt.

2. Befestigen Sie den Hub an der Montageplatte. Überprüfen Sie nach der Installation in der Ajax-App den Status des Sabotagekontakts und anschließend den festen Sitz der Platte.

3. Um eine höhere Zuverlässigkeit zu gewährleisten, befestigen Sie den Hub mit den mitgelieferten Schrauben an der Platte.

Drehen Sie die Hub-Zentrale nicht um, wenn er vertikal installiert wird (z. B. an einer Wand). Bei korrekter Montage wird das Ajax-Logo horizontal angezeigt.

Sie erhalten eine Benachrichtigung, wenn versucht wird, den Hub von der Oberfläche oder von der Montageplatte zu entfernen.



Es ist strengstens untersagt, das an die Stromversorgung angeschlossene Gerät zu zerlegen! Verwenden Sie das Gerät nicht mit einem beschädigten Netzkabel.

Zerlegen oder modifizieren Sie nicht den Hub oder seine Einzelteile – dies kann den normalen Betrieb des Geräts beeinträchtigen oder zu einem Ausfall führen.

### **Platzieren Sie den Hub nicht an folgenden Orten:**

- Außerhalb des Raums (im Freien).
- In der Nähe von metallischen Gegenständen und Spiegeln, die ein Funksignal abschwächen oder abschirmen können.
- An Orten mit einem schwachen GSM-Signal.
- In der Nähe von Funkstörungen: weniger als 1 Meter vom Router und den Stromkabeln entfernt.
- In Räumen mit hoher Luftfeuchtigkeit und Temperaturen außerhalb der zulässigen Grenzen.

## **Ajax-Systemwartung**

**Ajax-Systemwartung** Überprüfen Sie regelmäßig die Funktionsfähigkeit des Ajax-Sicherheitssystems. Reinigen Sie das Gehäuse nach Bedarf von Staub, Spinnweben und anderen Verunreinigungen. Verwenden Sie ein weiches, trockenes Tuch, das für die Pflege der Geräte geeignet ist.

Verwenden Sie keine Mittel, die Alkohol, Aceton, Benzin und andere aktive Lösungsmittel enthalten.



## Paketinhalt

1. Hub 2
2. Netzkabel
3. Ethernet-Kabel
4. Montagesatz
5. GSM-Startup-Kit – nicht in allen Ländern verfügbar
6. Schnellstartanleitung

## Technische Daten

Klassifizierung	Vernetzte Zentraleinheit für Sicherheitssysteme mit Anbindung über Ethernet und zwei SIM-Karten
Maximale Anzahl angeschlossener Geräte	Bis zu 100
Anzahl anschließbarer ReX	Bis zu 5
Sicherheitsgruppen	Bis zu 9
Benutzer des Sicherheitssystems	Bis zu 50
Videoüberwachung	Bis zu 25 Kameras oder DVRs
Räume	Bis zu 50
Anzahl Szenarien	Bis zu 32  (Reaktionen auf die Änderung des Sicherheitsmodus werden im Gesamtlimit der Hub-Szenarien nicht berücksichtigt)
Kommunikationsprotokolle der Überwachungszentrale	Contact ID, SIA  Die Fotobestätigungen von Alarmen werden an das CMS-System Manitou, ABSistemDC(NG), WBB, Horus und SBN
Stromversorgung	110 V~ bis 240 V~, 50/60 Hz

Eingebauter Akku	Li-Ion 2 A·h (bis zu 16 Stunden Akkulaufzeit bei deaktivierter Ethernet-Verbindung)
Stromverbrauch	10 W
Manipulationssicher	Verfügbar, Manipulationsalarm
Betriebsfrequenzband	868,0 MHz bis 868,6 MHz oder 868,7 MHz bis 869,2 MHz, je nach Verkaufsregion
HF-Ausgangsleistung	8.20 dBm / 6.60 mW (Grenzwert 25 mW)
Funksignalmodulation	GFSK
Funksignalleistung	Bis zu 2,000 m (Freifeld)
Kommunikationskanäle	<ul style="list-style-type: none"> <li>• 2 SIM-Karten (GSM 850/900/1800/1900 MHz GPRS)</li> <li>• Ethernet</li> </ul>
Installation	In Innenräumen
Betriebstemperaturbereich	Von -10°C bis +40°C
Betriebsfeuchte	Bis zu 75%
Abmessungen	163 × 163 × 36 mm
Gewicht	362 g

## Garantie

Die Garantie für die Produkte der „AJAX SYSTEMS MANUFACTURING“ LIMITED LIABILITY COMPANY gilt 2 Jahre nach dem Kauf und gilt nicht für den vorinstallierten Akku.

Wenn das Gerät nicht ordnungsgemäß funktioniert, empfehlen wir, dass Sie sich zuerst an den Support wenden, da technische Probleme in der Hälfte der Fälle aus der Ferne behoben werden können!



[Garantie](#)



[Nutzungsvereinbarung](#)

Technischer Kundendienst: [support@ajax.systems](mailto:support@ajax.systems)

