

Hub 2 Benutzerhandbuch

Aktualisiert February 19, 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.



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. Der Ajax Cloud-Dienst wird von Amazon Web Services (AWS) angeboten. 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.

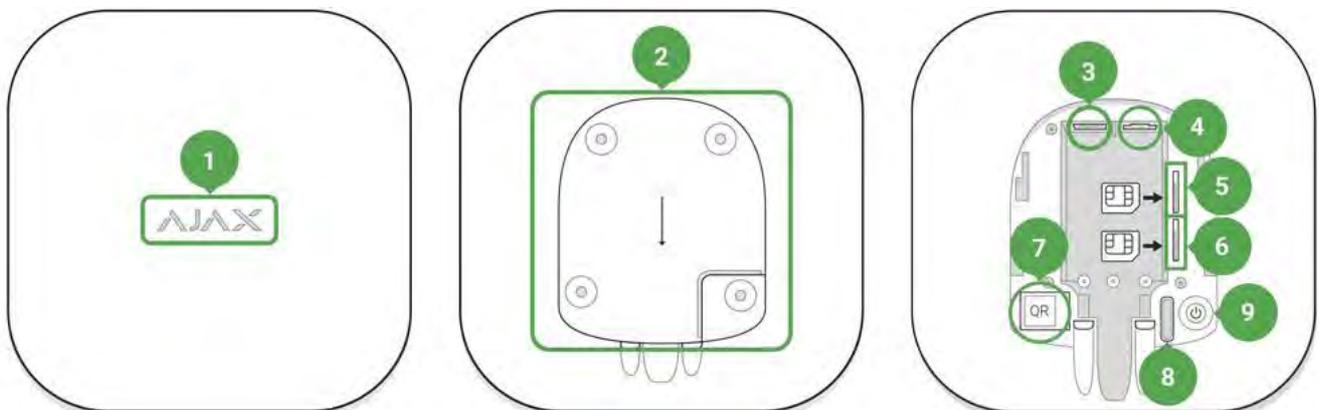
Benutzer können das Sicherheitssystem verwalten und umgehend auf Alarme und Benachrichtigungen mit den für iPhone und Smartphones mit Android, MacOS und Windows entwickelten Apps reagieren. Das System meldet Alarme und andere Ereignisse mithilfe von Push-Benachrichtigungen, SMS und Telefonanrufen.

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



Ajax-Logo mit Leuchtanzeige

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!)

Netzkabelanschluss

Ethernet-Kabelanschluss

Steckplatz 2: SIM-Karte (Typ micro-SIM)

Steckplatz 1: SIM-Karte (Typ micro-SIM)

QR-Code

Manipulationstaste

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.

[Alle Geräte von Ajax](#)

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.

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

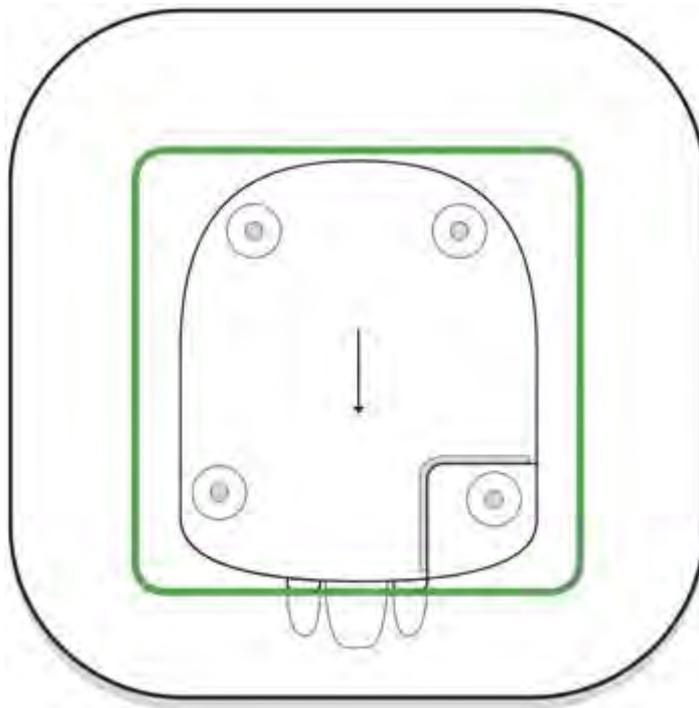
Sicherheitsanforderungen

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.

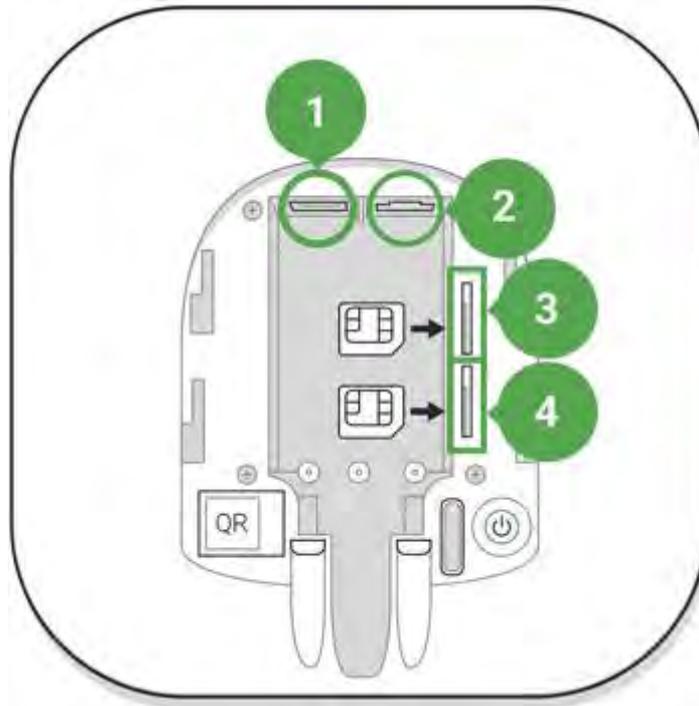
Es ist strengstens untersagt, das an die Stromversorgung angeschlossene Gerät zu zerlegen! Des Weiteren darf das Gerät nicht mit einem beschädigten Netzkabel betrieben werden.

Hub-Anschluss

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!



Netzkabel und Ethernet-Kabel mit den entsprechenden Anschlüssen verbinden.



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

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.

- i** 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.

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

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](#).

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.

Geben Sie dem Hub einen Namen und scannen Sie den QR-Code unter dem Deckel, oder geben Sie ihn manuell ein.

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.

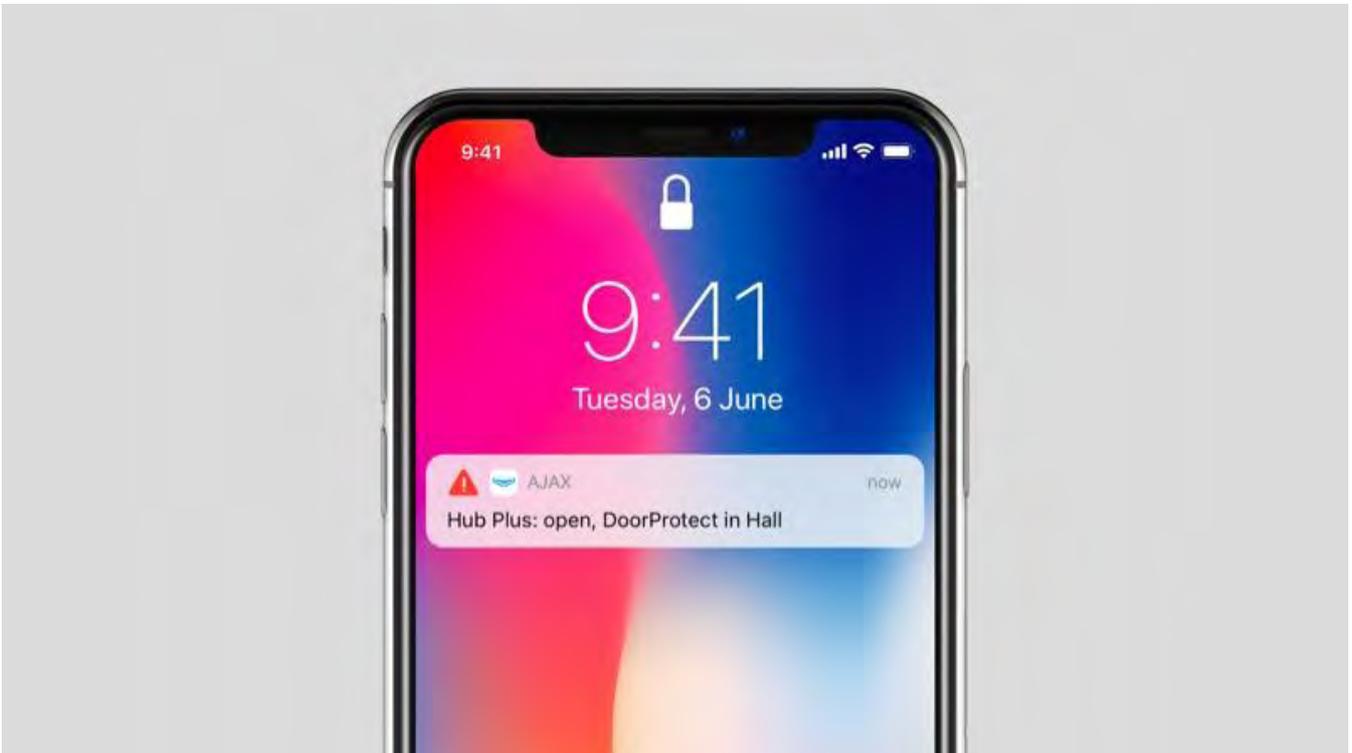
Wenn der Administrator des Sicherheitssystems geändert oder aus der Hub-Liste gelöscht wird, werden die damit verknüpften Geräte nicht zurückgesetzt.

[Berechtigungen für Nutzer des Ajax-Sicherheitssystems](#)

Hub-Einstellungen

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 **Zimmer**  und klicken Sie auf **Zimmer 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:

Öffnen Sie in der Ajax-Anwendung den Raum und wählen Sie **Gerät hinzufügen**.

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).

Klicken Sie auf Hinzufügen und der Countdown der verbleibenden Zeit für das Hinzufügen eines Geräts beginnt.

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.

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 Videüberwachungsgeräte an das System angeschlossen werden.

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

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

[Eine Kamera eines Drittanbieters hinzufügen](#)

Hub-Einstellungen

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

Anpassbare Parameter:

Benutzer

Ethernet

Mobilfunk

Geofence

Gruppen

Sicherheitszeitplan

Test Erfassungszone

Jeweller

Dienst

Leitstelle

PRO

Sicherheitsdienste

Benutzerhandbuch

Benutzer — Sicherheitssystemeinstellungen 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](#)

Test Erfassungsbereich — 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.

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:

$$\text{Abfrageintervall} * (\text{Anzahl der nicht zugestellten Pakete} + 1 \text{ Korrekturpaket})$$

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 — Eine Gruppe von Hub-Dienst-Einstellungen.

Verbindungseinstellungen für den Hub und den Ajax Cloud-Dienst:

Server-Ping-Intervall. Die Häufigkeit der Abfrage des Ajax Cloud-Dienstes durch den Hub, einstellbar von 10 bis 300 Sekunden. Der empfohlene und voreingestellte Wert ist 60 s.

Verzögerung bei Verbindungsfehler. Um das Risiko eines Fehlalarms bei Verbindungsverlust mit dem Ajax Cloud-Dienst zu reduzieren, ist eine Verzögerung erforderlich. Sie wird nach 3 erfolglosen Hub-Server-Abfragen aktiviert. Die Verzögerung kann im Bereich von 30 bis 600 Sekunden eingestellt werden. Der empfohlene und voreingestellte Wert beträgt 300 s.

Die Zeit bis zum Senden einer Meldung über den Kommunikationsverlusts zwischen Hub und Ajax Cloud-Dienst wird mit folgender Formel berechnet:

*(Abfrageintervall * 4) + Zeitfilter*

Bei Standardeinstellung meldet der Ajax Cloud-Dienst nach 9 Minuten einen Hub-Verlust:

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

Zeit bis zum Erkennen des Verbindungsverlust zwischen Hub und Ajax Cloud-Dienst

LED-Helligkeit. Anpassen der Helligkeit der LEDs im Logo des Hubs. Stellen Sie die Helligkeit zwischen 1 und 10 ein (Standard: 10).

Systemprüfung. Bei aktivierter Funktion überprüft der Hub vor der Scharfschaltung den Status aller Geräte: Batterieladung, Manipulationsalarm, Verbindung. Sollte bei der Scharfschaltung ein Problem erkannt werden, aktiviert der Hub den Scharfschaltungsmodus nicht und gibt eine Warnung aus.

Scharfschaltberechtigung (Die Option wird erst aktiv, nachdem die **Systemprüfung** aktiviert wurde). Bei aktivierter Funktion kann das Sicherheitssystem auch bei einer Störung scharfgeschaltet werden.

So aktivieren Sie das fehlerhafte Sicherheitssystem über die Ajax-Anwendung:

Scharfschaltungsmodus aktivieren — Es wird eine Meldung mit einer Liste der Störungen angezeigt.

Bestätigen Sie die Scharfschaltung des Sicherheitssystems durch Drücken von **Scharfschalten**.

Aktivierung des Scharfschaltungsmodus trotz Fehler(n) im Sicherheitssystem über eine KeyPad-Tastatur oder eine SpaceControl-Funkfernbedienung:

Aktivieren Sie den Scharfschaltungsmodus — Sie erhalten eine Ablehnung.

Bestätigen Sie die Scharfschaltung des Systems durch erneute Aktivierung des Scharfschaltungsmodus innerhalb von 30 Sekunden.

So funktioniert eine Systemintegritätsprüfung?

Automatische Softwareupdates. Konfigurieren automatischer Firmware-Updates für das OS Malevich. Wenn der Hub eingeschaltet wird, aktualisiert er automatisch seine Firmware, wenn eine neue Version verfügbar ist.

So aktualisiert sich OS Malevich

Konfiguration der Brandmelder FireProtect und FireProtect Plus

Gekoppelte Rauchmelder Alarme. Die Funktion aktiviert die eingebauten Sirenen aller Brandmelder, wenn mindestens einer von ihnen eine Bedrohung erkennt.

Der vernetzte FireProtect-Alarm?

Ersten Alarm ignorieren Schlummerfunktion für Alarme zur Überprüfung auf Rauch.

Die Option funktioniert wie folgt:

Ein Melder erfasst Rauch und gibt einen Alarm aus.

Ein im Melder integrierter 30-Sekunden-Timer wird aktiviert.

Wenn der Melder nach 30 s immer noch eine Bedrohung erfasst, wird ein Alarm an den Hub gesendet.

Diese Einstellung wird für Bereiche empfohlen, in denen potenzielle Ursachen für Fehlalarme vorliegen, z. B. wenn der Melder an einem Ort installiert ist, an dem Zugluft wahrscheinlich ist.

Die Einstellungen zum Sammeln und Speichern von Ajax-Sicherheitssystemberichten.

Hub-Systemspeicher. Sie können Protokolle deaktivieren oder einen Übertragungskanal auswählen:

Ethernet

AUS (WLAN, nur in Hub Plus)

Nein — Protokollierung ist deaktiviert

 Es wird nicht empfohlen, Protokolle zu deaktivieren, da diese Informationen bei Fehlern im Betrieb des Systems hilfreich sein können!

Einstellungen für die Sirenenaktivierung

Wenn das Hub- oder das Meldergehäuse offen ist. Wenn die Funktion aktiv ist, aktiviert der Hub die angeschlossenen Sirenen, wenn das Gehäuse des Hubs, des Melders oder eines anderen Ajax-Geräts geöffnet ist.

Wenn in der App eine Alarmtaste gedrückt wird. Wenn die Funktion aktiv ist, aktiviert der Hub die angeschlossenen Sirenen beim Drücken der Paniktaste in der Ajax-App.

-  Deaktivieren Sie die Aktivierung der Sirene, indem Sie in den Einstellungen der Funkfernbedienung (**Geräte**  **SpaceControl**  **Einstellungen** ) die Paniktaste an der SpaceControl-Funkfernbedienung drücken.

Leitstelle — 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.

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

Benutzerhandbuch — öffnet das Hub 2-Benutzerhandbuch.

Hub entkuppeln — Entfernt Ihren Account vom Hub. Ansonsten bleiben alle Einstellungen und verknüpften Melder gespeichert.

Zurücksetzen der Hub-Einstellungen

Setzen Sie den Hub auf die Werkseinstellungen zurück:

Schalten Sie den Hub ein, wenn er ausgeschaltet ist.

Entfernen Sie alle Benutzer und Installateure vom Hub.

Halten Sie den Ein/Aus-Taster für 30 Sekunden gedrückt – das Ajax-Logo auf dem Hub beginnt rot zu blinken.

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	Verbindungsverlust zwischen Gerät und Hub	Push-Nachrichten SMS

	Funkstörung (Jamming) Niedrige Batterieladung im Gerät oder Hub Abdeckung Manipulieren des Meldergehäuses	
Alarm	Einbruch Brand Überschwemmung Der Hub hat die Verbindung zum Ajax Cloud-Dienst verloren	Anrufe Push-Nachrichten SMS
Ereignisse	Ein-/Ausschalten von <u>WallSwitch</u> , <u>Relay</u> , <u>Socket</u>	Push-Nachrichten SMS
Scharf-/Unscharfschaltung	Scharf-/Unscharfschaltung ganzer Bereiche/Objekte oder Gruppen Nachtmodus aktivieren	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.

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:

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.

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.

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

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 starken Funkstörungen.

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.

[Wie wechselt man die Batterie des Hubs](#)

Paketinhalt

Hub 2

Netzkabel

Ethernet-Kabel

Montagesatz

GSM-Startup-Kit – nicht in allen Ländern verfügbar

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
Stromversorgung	110 V~ bis 240 V~, 50/60 Hz
Eingebauter Akku	Li-Ion 2 Ah (bis zu 16 Stunden Akkulaufzeit bei deaktivierter Ethernet-Verbindung)
Stromverbrauch	10 Wh
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
Funksignalreichweite	Bis zu 2,000 m (Freifeld)
Kommunikationskanäle	2 SIM-Karten (GSM 850/900/1800/1900 MHz GPRS) Ethernet
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