

Hub Plus Benutzerhandbuch

Aktualisiert July 3, 2020



Hub Plus ist ein zentrales Gerät des Ajax-Sicherheitssystems, das die angeschlossenen Geräte koordiniert und mit dem Benutzer und dem Sicherheitsunternehmen interagiert.

Hub Plus benötigt einen Internetzugang, um mit dem Cloud Server Ajax Cloud zu kommunizieren – für die Konfiguration und Steuerung von jedem Punkt der Welt aus, die Übertragung von Ereignisbenachrichtigungen und die Aktualisierung der Software. Die persönlichen Daten und Systembetriebsprotokolle werden unter mehrstufigem Schutz gespeichert, und der Informationsaustausch mit Hub Plus erfolgt über einen verschlüsselten Kanal auf einer 24-Stunden-Basis.

Bei der Kommunikation mit der Ajax Cloud kann das System die Ethernet-Verbindung, Wi-Fi und das GSM-Netz nutzen.



Bitte nutzen Sie all diese Kommunikationskanäle, um eine zuverlässigere Kommunikation zwischen der Hub-Zentrale und der Ajax Cloud zu gewährleisten.

Hub Plus kann über die [App](#) für iOS, Android, macOS oder Windows gesteuert werden. Die App ermöglicht es, auf alle Benachrichtigungen des Sicherheitssystems umgehend zu reagieren.

Folgen Sie dem Link, um die Anwendung für Ihr Betriebssystem herunterzuladen:

[Android](#)

[iOS](#)

Der Benutzer kann die Benachrichtigungen in den Einstellungen der Hub-Zentrale anpassen. Wählen Sie, was für Sie bequemer ist: Push-Benachrichtigungen, SMS oder Anrufe. Wenn das Ajax-System mit der zentralen Überwachungsstation verbunden ist, wird das Alarmsignal unter Umgehung der Ajax Cloud direkt an diese gesendet.

[Intelligente Alarmzentrale Hub Plus kaufen](#)

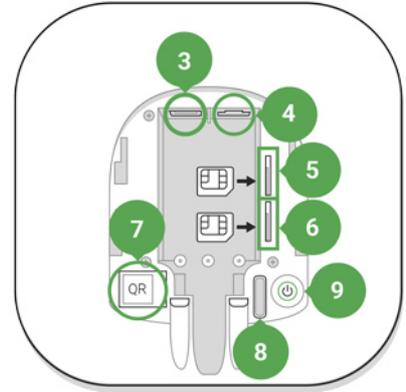
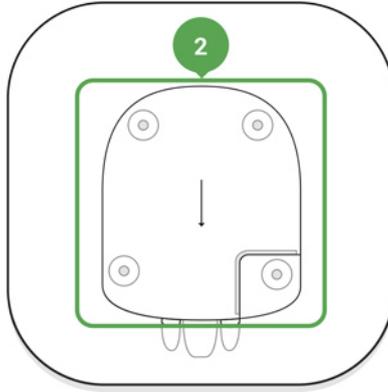
Hub Plus unterstützt bis zu 150 angeschlossene Ajax-Geräte. Das geschützte [Jeweller-Funkprotokoll](#) gewährleistet eine zuverlässige Kommunikation zwischen den Geräten in einer Entfernung von bis zu 2 km in der Sichtlinie.

[Liste der Ajax-Geräte](#)

Verwenden Sie Szenarien, um das Sicherheitssystem zu automatisieren und die Anzahl der Routineaktionen zu verringern. Passen Sie den Sicherheitszeitplan an, programmieren Sie Aktionen von Automatisierungsgeräten ([Relay](#), [WallSwitch](#) oder [Socket](#)) als Reaktion auf einen Alarm, durch Drücken der [Button](#) oder nach Zeitplan. Ein Szenario kann in der Ajax-Anwendung remote erstellt werden.

[So erstellen und konfigurieren Sie ein Szenario im Ajax Sicherheitssystem](#)

Steckdosen und Anzeige



1. LED-Logo zur Anzeige des Status der Hub-Zentrale
2. SmartBracket-Befestigungsplatte (ein perforiertes Teil ist erforderlich, um den Manipulationsschutz im Falle eines Versuchs, die Hub-Zentrale zu demontieren, zu betätigen)
3. Buchse für das Stromversorgungskabel
4. Buchse für das Ethernet-Kabel
5. Steckplatz für die Mikro-SIM
6. Steckplatz für die Mikro-SIM
7. QR-Code
8. Manipulationstaste
9. „Ein“-Taste

Logo-Anzeige



Wenn Sie auf den Netzschalter klicken, leuchtet das Ajax-Logo für eine Sekunde grün auf. Gleich danach ändert das Logo seine Farbe in rot und zeigt damit an, dass die Hub-Zentrale geladen wird. Wenn das Laden abgeschlossen ist, hängt die Farbe des Logos von der Verbindung mit der Ajax Cloud ab.

Wenn die Hub-Zentrale nicht an die Stromversorgung angeschlossen ist, leuchtet das Logo 3 Minuten lang auf und blinkt dann alle 20 Sekunden.

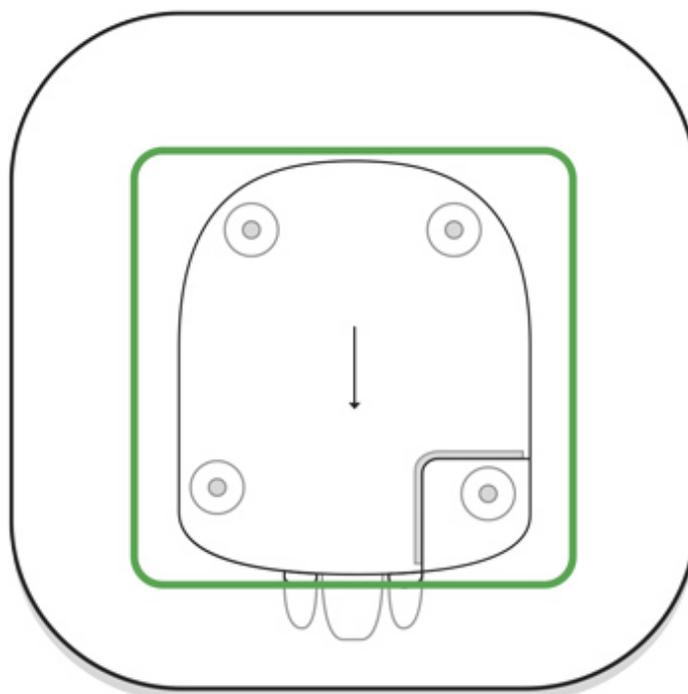
Kommunikation mit der Ajax Cloud

Anzeigefarbe informiert über die Kommunikation mit der Ajax Cloud

Anzeige	Ereignis
Leuchtet weiß	Mindestens zwei Kommunikationskanäle sind miteinander verbunden (Ethernet, Wi-Fi, GSM)
Leuchtet hellgrün	Ein Kommunikationskanal ist angeschlossen
Leuchtet rot	Hub Plus ist nicht mit dem Internet verbunden oder es besteht keine Kommunikation zum Server

Anschluss an das Netzwerk

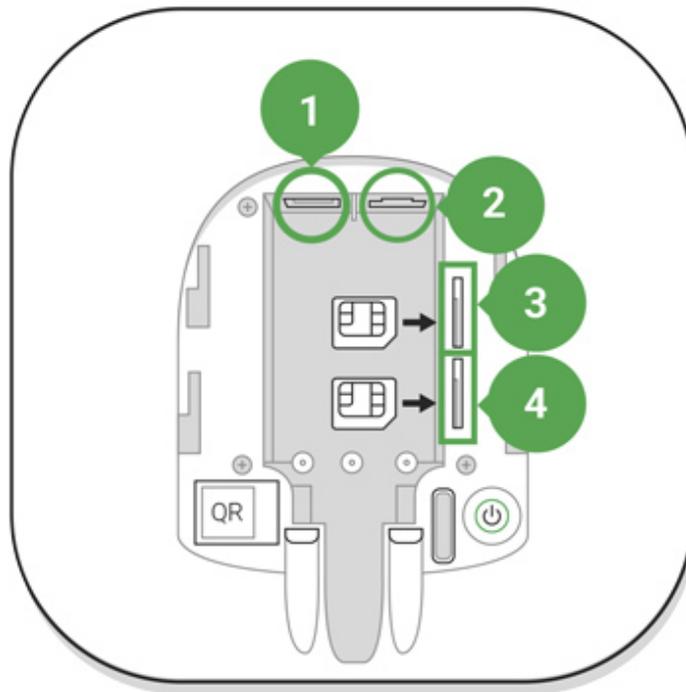
1. Öffnen Sie den Decker der Hub-Zentrale, indem Sie ihn mit Kraft nach unten schieben.





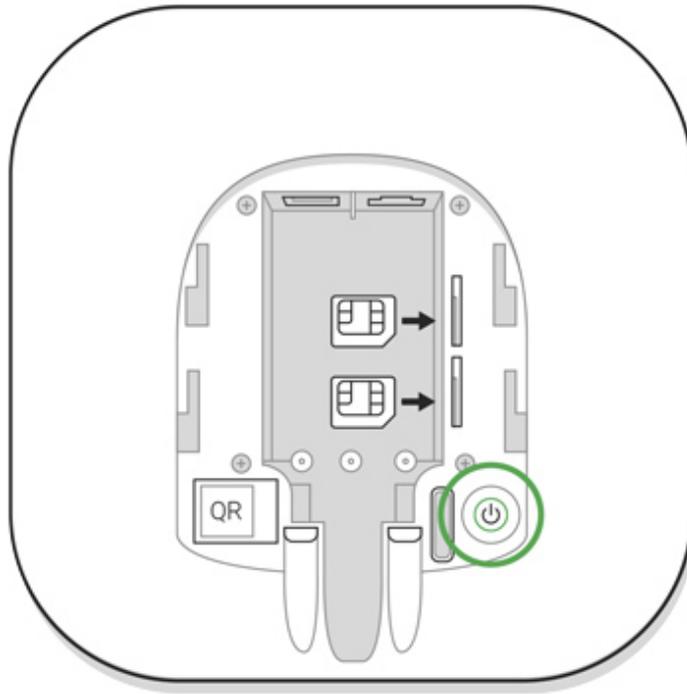
Seien Sie vorsichtig und beschädigen Sie nicht den Manipulationsschutz, der die Hub-Zentrale vor der Demontage schützt!

2. Schließen Sie Stromversorgungs- und Ethernet-Kabel an die Steckdosen an.



- 1 – Steckdose
- 2 – Ethernet-Buchse
- 3, 4 – Steckplätze für SIM-Karten

3. Halten Sie den Netzschalter 2 Sekunden lang gedrückt, bis das Logo aufleuchtet.



Die Hub-Zentrale benötigt etwa 2 Minuten, um die verfügbaren Kommunikationskanäle zu identifizieren.



Das hellgrüne bzw. weiße Logo zeigt an, dass die Hub-Zentrale mit der Ajax Cloud verbunden ist.

Wenn die Ethernet-Verbindung nicht automatisch erfolgt, deaktivieren Sie den Proxy, die Filterung nach MAC-Adressen und aktivieren Sie das DHCP in den Routereinstellungen: die Hub-Zentrale erhält eine IP-Adresse. Bei der nächsten Einrichtung in der Web- oder Mobilanwendung können Sie eine statische IP-Adresse festlegen.

Um die Hub-Zentrale mit dem GSM-Netz zu verbinden, benötigen Sie eine Micro-SIM-Karte mit einer deaktivierten PIN-Code-Anforderung (Sie können sie mit dem Mobiltelefon deaktivieren) und einen ausreichenden Betrag auf dem Konto, um für die GPRS- und SMS-Dienste und Anrufe zu bezahlen.



In einigen Regionen wird Hub Plus zusammen mit einer SIM-Karte verkauft.

Wenn die Hub-Zentrale keine Verbindung zur Ajax Cloud über GSM herstellt, verwenden Sie Ethernet, um die Netzwerkparameter in der Anwendung einzurichten. Für die korrekte Einstellung des Zugangspunktes, des

Benutzernamens und des Passworts wenden Sie sich bitte an den Support-Service des Betreibers.

Um die Wi-Fi-Verbindung zu verwenden, gehen Sie zu den Einstellungen der Hub-Zentrale (dem Wi-Fi-Menü), wählen Sie den Zugangspunkt aus und geben Sie das Netzwerkpasswort ein.

Ajax-Account

Der Benutzer mit Administratorrechten kann das Ajax-Sicherheitssystem über die App konfigurieren. Das Administratorkonto mit den Informationen über die hinzugefügten Hubs wird verschlüsselt und in die Ajax Cloud gestellt.

Alle vom Benutzer eingestellten Parameter des Ajax-Sicherheitssystems und der angeschlossenen Geräte werden lokal auf der Hub-Zentrale gespeichert. Diese Parameter sind untrennbar mit der Hub-Zentrale verbunden: Ein Wechsel des Hub-Administrators hat keinen Einfluss auf die Einstellungen der angeschlossenen Geräte.



Eine Telefonnummer darf nur zur Erstellung eines einzigen Ajax-Accounts verwendet werden.

Erstellen Sie das Ajax-Account in der App gemäß der Schritt-für-Schritt-Anleitung. Als Teil des Prozesses müssen Sie Ihre E-Mail und Telefonnummer bestätigen.

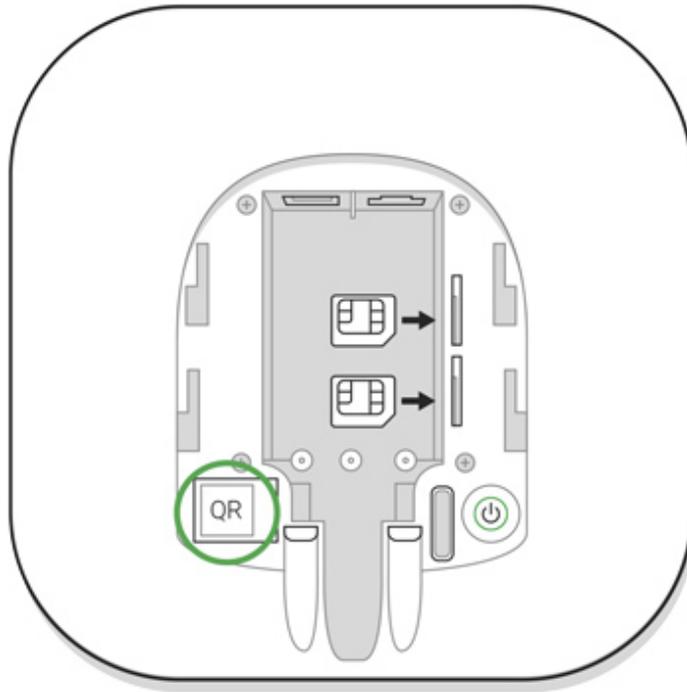
Das Ajax-Account erlaubt es, die Rollen zu kombinieren: Sie können sowohl der Administrator einer Hub-Zentrale als auch der Benutzer einer anderen Hub-Zentrale sein.

Hinzufügen der Hub-Zentrale zur Ajax-App



Die Gewährung des Zugangs zu allen Systemfunktionen (insbesondere zur Anzeige von Benachrichtigungen) ist eine zwingende Voraussetzung für die Steuerung des Ajax-Sicherheitssystems über das Smartphone/Tablet.

1. Loggen Sie sich in Ihr Konto ein.
2. Öffnen Sie das Menü **Hub-Zentrale hinzufügen**, und wählen Sie die Art der Registrierung: manuell oder Schritt-für-Schritt-Anleitung.
3. Geben Sie in der Registrierungsphase den Namen der Hub-Zentrale ein und scannen Sie den QR-Code, der sich unter dem Deckel befindet (oder geben Sie einen Registrierungsschlüssel manuell ein)..



4. Warten Sie, bis die Hub-Zentrale registriert und auf dem Anwendungs-Desktop angezeigt wird.

Installation

Vergewissern Sie sich vor der Installation der Hub-Zentrale, dass Sie den optimalen Standort gewählt haben: Die SIM-Karte weist einen konsistenten Empfang auf, alle Geräte wurden für die Funkkommunikation getestet, und die Hub-Zentrale ist vor direkten Blicken verborgen.

Die Hub-Zentrale sollte zuverlässig an der Oberfläche (vertikal oder horizontal) befestigt sein. Wir empfehlen nicht die Verwendung von doppelseitigem Klebeband: es kann keine sichere Befestigung garantieren und erleichtert die Entfernung des Geräts.

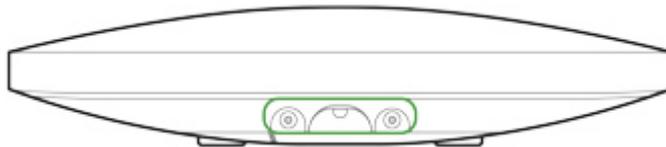
Platzieren Sie die Hub-Zentrale nicht an folgenden Orten:

- außerhalb der Räumlichkeiten (im Freien);

- in der Nähe oder im Inneren von Metallgegenständen oder Spiegeln, die eine Dämpfung und Abschirmung des Signals verursachen;
- an Orten mit niedrigem GSM-Signal;
- in der Nähe von Funkstörungen: weniger als 1 Meter vom Router und den Stromkabeln entfernt;
- in jedem Raum, in dem Temperatur und Luftfeuchtigkeit außerhalb des zulässigen Bereichs liegen.

Installieren der Hub-Zentrale:

1. Befestigen Sie den Decker der Hub-Zentrale mit den mitgelieferten Schrauben auf der Oberfläche. Wenn Sie anderes Befestigungszubehör verwenden, achten Sie darauf, dass der Deckel der Hub-Zentrale nicht beschädigt oder verformt wird.
2. Setzen Sie die Hub-Zentrale auf den Deckel und befestigen Sie sie mit den mitgelieferten Schrauben.



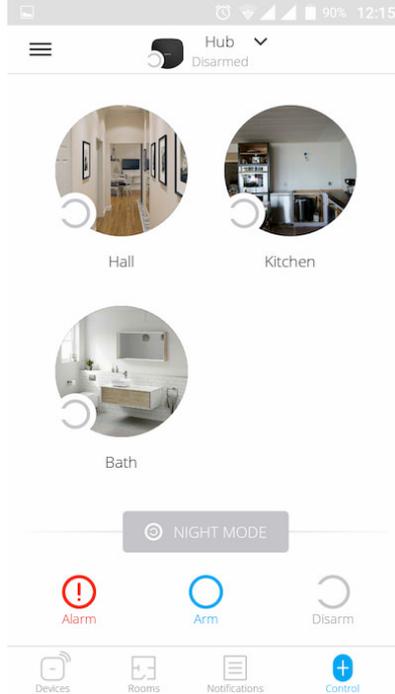
Drehen Sie die Hub-Zentrale nicht um, wenn er vertikal installiert wird (z. B. an einer Wand). Bei korrekter Montage wird das Ajax-Logo horizontal angezeigt.



Die Befestigung der Hub-Zentrale am Deckel mit Schrauben verhindert ein versehentliches Verschieben der Hub-Zentrale und minimiert das Risiko eines Gerätediebstahls.

Wenn die Hub-Zentrale sicher befestigt ist, löst die Demontage ihres Körpers von der Oberfläche den Manipulationsalarm aus, und das System benachrichtigt Sie darüber.

Räume in der Ajax-App



Die virtuellen Räume dienen zur Gruppierung der angeschlossenen Geräte. Der Benutzer kann bis zu 50 Räume erstellen, wobei sich jedes Gerät nur in einem Raum befindet.



Ohne einen Raum zu erstellen, können Sie keine Geräte in der Ajax-App hinzufügen!

Anlegen und Einrichten eines Raums

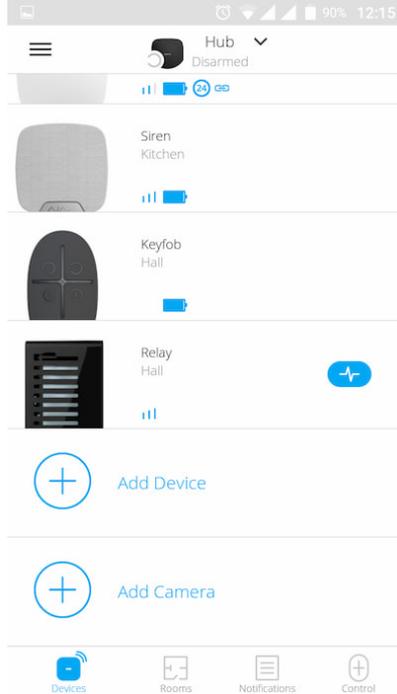
Der Raum wird in der App über das Menü **Raum hinzufügen** angelegt.

Bitte vergeben Sie einen Namen für den Raum und fügen Sie optional ein Foto bei (oder machen Sie ein Foto). Dies hilft, den benötigten Raum in der Liste schnell zu finden.

Durch Drücken der Zahnrad-Schaltfläche gelangen  Sie in das Menü der Raumeinstellungen.

Um den Raum zu löschen, verschieben Sie alle Geräte über das Geräte-Setup-Menü in andere Räume. Durch das Löschen des Raums werden alle seine Einstellungen gelöscht.

Geräte anschließen



Bei der ersten Registrierung der Hub-Zentrale in der App werden Sie aufgefordert, Geräte zur Bewachung des Raums hinzuzufügen. Sie können diesen Schritt jedoch ablehnen und später erneut ausführen.



Der Benutzer kann das Gerät nur hinzufügen, wenn das Sicherheitssystem deaktiviert ist!

1. Öffnen Sie den Raum in der Anwendung und wählen Sie die Option **Gerät hinzufügen**.
2. Benennen Sie das Gerät, scannen Sie den QR-Code (oder geben Sie die ID manuell ein), wählen Sie den Raum aus und gehen Sie zum nächsten Schritt.
3. Wenn die App mit der Suche beginnt und den Countdown startet, schalten Sie das Gerät ein: die LED blinkt einmal. Damit Erkennung und Verbindung erfolgen kann, muss sich das Gerät im Empfangsbereich des drahtlosen Netzwerks der Hub-Zentrale befinden (an einem einzelnen geschützten Objekt).



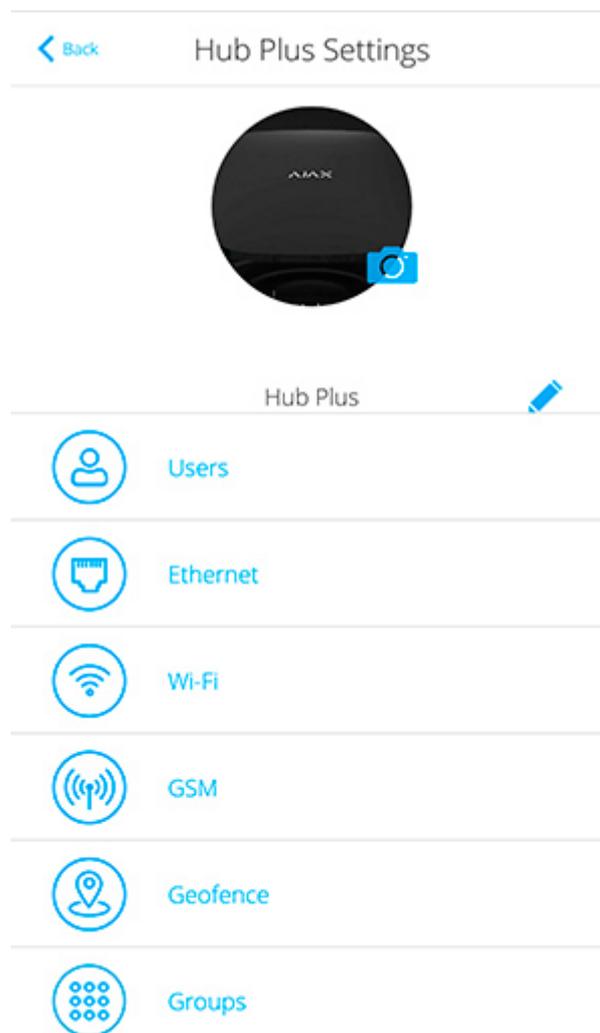
Die Verbindungsanfrage wird im Moment des Einschaltens des Geräts für kurze Zeit übertragen.

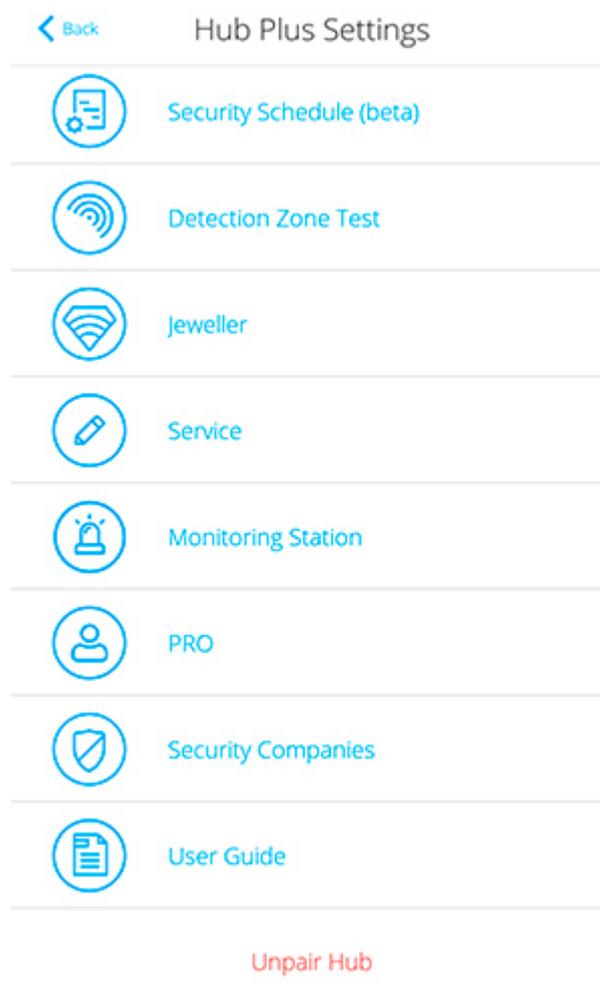
Wenn die Verbindung beim ersten Versuch fehlschlägt, schalten Sie das Gerät für 5 Sekunden aus und versuchen Sie es erneut.

Wie man eine IP-Kamera konfiguriert und an das Ajax-Sicherheitssystem anschließt

Einstellungen

Die Einstellungen der Hub-Zentrale und der angeschlossenen Geräte befinden sich im Menü **Hub Plus Einstellungen** .





Einstellbare Parameter:

- **Benutzern** – legen Sie fest, wer Zugang zu Ihrem Sicherheitssystem hat, welche Rechte ihnen gewährt werden und wie die Hub-Zentrale über Ereignisse informiert.
- **Ethernet** – konfigurieren Sie die Ethernet-Verbindung.
- **WLAN** – konfigurieren Sie die Wi-Fi-Verbindung.
- **GSM** – Ein-/Ausschalten der Mobilfunk-Kommunikation, Konfiguration der Verbindung und Überprüfung des Guthabens.
- **Geofence** – setzen Sie die Erinnerung an das Scharf-/Unscharfschalten des Sicherheitssystems beim Betreten des angegebenen Bereichs.



Der Standort des Benutzers wird auf der Grundlage der Daten der GPS-Antenne oder des iBeacon (nur bei Apple-Geräten) bestimmt.

- **Gruppen** – Einstellungen für den Gruppenmodus öffnen.

- **Sicherheitszeitplan** – legen Sie einen Zeitplan für die automatische Scharf-/Unscharfschaltung des Sicherheitssystems fest.
- **Erkennungsbereichstest** – führen Sie den Erkennungsbereichstest für die angeschlossenen Geräte durch.
- **Jeweller** – konfigurieren Sie das Hub-Melder-Ping-Intervall und die Anzahl nicht zugestellter Pakete, die den Verbindungsabbruch bestimmen.

Das Ping-Intervall bestimmt, wie häufig die Geräte kommunizieren. Das kürzere Intervall (in Sekunden) bedeutet eine schnellere Übertragung der Ereignisse zwischen der Hub-Zentrale und den angeschlossenen Geräten. Alarme werden in jedem Fall sofort übermittelt.

Denken Sie daran, dass das Ping-Intervall die maximale Anzahl der angeschlossenen Geräte reduzieren kann:

Intervall, sek	Verbindungslimit, Geräte
12	39
24	79
36	119
48 und mehr	150

Die Anzahl nicht zugestellter Pakete bestimmt, wie schnell die Hub-Zentrale den Verbindungsverlust mit dem Gerät erkennt.

Berechnung der Zeit für das Auslösen des Alarms (mit den Standardparametern):

$$(8 \text{ Pakete} + 1 \text{ Korrektur}) \times 36 \text{ Sekunden Abfrageintervall} = 5 \text{ Minuten } 24 \text{ Sekunden}$$

- **Service** – öffnet die Service-Einstellungen der Hub-Zentrale.

Verbindungsausfall-Alarmverzögerung – regelt die Alarmbenachrichtigungsverzögerung des Verbindungsverlustes zum Server.

Server-Ping-Intervall – reguliert das Intervall für das Senden von Pings vom Hub zum Server.

Die Zeit für die Generierung der Nachricht über den Verbindungsverlust zwischen dem Server und der Hub-Zentrale wird wie folgt berechnet (**mit den Standardparametern**):

$$(3 \text{ Pings} + 1 \text{ Korrektur}) \times 60 \text{ Sekunden Abfrageintervall} + 300 \text{ Sekunden Zeitfilter} = 9 \text{ Minuten.}$$

Sie können die automatische Hub-Firmware-Aktualisierung deaktivieren (standardmäßig aktiviert).

So schaltet man die automatische Aktualisierung die Hub-Zentrale-Firmware aus

- **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:

1. Scharfschaltungsmodus aktivieren – Es wird eine Meldung mit einer Liste der Störungen angezeigt.
2. 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:

1. Aktivieren Sie den Scharfschaltungsmodus – Sie erhalten eine Ablehnung.
2. 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.



Gekoppelte Alarme werden von Meldern der Baureihen FireProtect und Fireprotect Plus mit Firmware-Version 3.42 und höher unterstützt. Bitte beachten Sie, dass Sie bei Aktivierung von gekoppelten Alarmen das Ping-Intervall des Hub-Zentralen-Melders in den Jeweller Einstellungen auf maximal 48 Sekunden einstellen können.

Der vernetzte FireProtect-Alarm?

- **Ersten Alarm ignorieren** Schlummerfunktion für Alarme zur Überprüfung auf Rauch.

Die Option funktioniert wie folgt:

1. Ein Melder erfasst Rauch und gibt einen Alarm aus.
2. Ein im Melder integrierter 30-Sekunden-Timer wird aktiviert.
3. 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.

- **Überwachungszentrale** – CMS-Verbindungseinstellungen konfigurieren.
- **PRO** – PRO-Konten konfigurieren, die mit der Hub-Zentrale verbunden sind.

- **Sicherheitsunternehmen** – wählen Sie einen Sicherheitsdienst in Ihrer Region aus und verbinden Sie ihn.

Einstellungen zurücksetzen

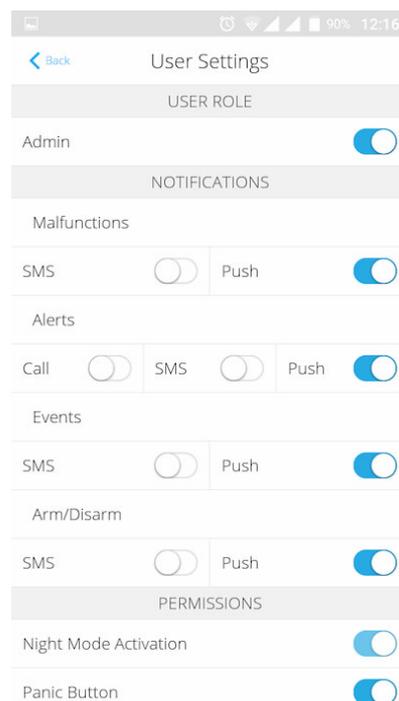
Um die Hub-Zentrale auf die werkseitigen Standardeinstellungen zurückzusetzen, schalten Sie ihn ein und halten Sie dann den Netzschalter 30 Sekunden lang gedrückt (das Logo beginnt rot zu blinken).

Gleichzeitig werden alle angeschlossenen Melder, Raum- und Benutzereinstellungen gelöscht. Die Benutzerprofile bleiben mit dem System verbunden.

Benutzern

Nachdem Sie die Hub-Zentrale zum Konto hinzugefügt haben, werden Sie Administrator dieses Geräts. Eine Hub-Zentrale kann bis zu 99 Benutzer/Administratoren haben. Der Administrator kann Benutzer in das Sicherheitssystem einladen und ihre Rechte festlegen.

Ereignisse und Alarmbenachrichtigungen



Die Hub-Zentrale benachrichtigt die Benutzer auf drei Arten über Ereignisse: Push-Benachrichtigungen, SMS und Anrufe.

Die Benachrichtigungen werden im Menü „Benutzern“ eingestellt:

Ereignistypen	Wofür es verwendet wird	Arten von Benachrichtigungen
Scharfschalten/Unscharfschalten	Benachrichtigungen im Falle von Scharfschalten/Entschärfen	<ul style="list-style-type: none">• SMS• Push-Benachrichtigung
Alarm	Hinweise auf Eindringen, Feuer, Überschwemmung	<ul style="list-style-type: none">• SMS• Push-Benachrichtigung• Anruf
Ereignisse	Mitteilungen über Ereignisse im Zusammenhang mit WallSwitch, Relay	<ul style="list-style-type: none">• SMS• Push-Benachrichtigung
Störungen	Hinweise auf verlorene Kommunikation, Blockieren, niedrige Batterieladung oder Öffnen des Meldergehäuses	<ul style="list-style-type: none">• SMS• Push-Benachrichtigung

- Die **Push-Benachrichtigung** wird von der Ajax Cloud an die Ajax Security System-App gesendet, wenn eine Internetverbindung verfügbar ist.
- Die **SMS** wird an die vom Benutzer bei der Registrierung des Ajax-Kontos angegebene Telefonnummer gesendet.
- Der **Telefonanruf** bedeutet, dass die Hub-Zentrale die im Ajax-Account angegebene Nummer anruft.

Die Hub-Zentrale ruft nur im Alarmfall an, um Ihre Aufmerksamkeit zu erhalten und die Wahrscheinlichkeit zu verringern, dass Sie einen kritischen Alarm verpassen. Es wird empfohlen, diese Art der Benachrichtigung zu aktivieren. Die Hub-Zentrale ruft nacheinander alle Benutzer, die diese Art

der Benachrichtigung aktiviert haben, in der in den Benutzereinstellungen festgelegten Reihenfolge auf. Wenn der zweite Alarm auftritt, ruft die Hub-Zentrale erneut an, jedoch nicht mehr als einmal in 2 Minuten.



Der Anruf wird automatisch beendet, sobald Sie ihn entgegennehmen. Wir empfehlen Ihnen, die mit die Hub-Zentrale-SIM-Karte verbundene Telefonnummer in Ihrer Kontaktliste zu speichern.

Benachrichtigungseinstellungen können nur für registrierte Benutzer geändert werden.

Verbindung zu einem Sicherheitsdienst herstellen



Die Liste der Organisationen, die das Ajax-System mit der zentralen Überwachungsstation verbinden, finden Sie im Menü **Sicherheitsdienste** der Hub-Zentrale-Einstellungen.

Wenden Sie sich an die Vertreter des Unternehmens, das Dienstleistungen in Ihrer Stadt erbringt, und veranlassen Sie die Verbindung.

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

Instandhaltung

Überprüfen Sie die Betriebsfähigkeit des Ajax-Sicherheitssystems regelmäßig.

Reinigen Sie das Gehäuse der Hub-Zentrale von Staub, Spinnenweben und anderen Verunreinigungen. Verwenden Sie eine weiche, trockene Serviette, die für die Wartung der Geräte geeignet ist.

Verwenden Sie keine Substanzen, die Alkohol, Aceton, Benzin und andere aktive Lösungsmittel enthalten, um die Hub-Zentrale zu reinigen.

Wie man die Batterie der Hub-Zentrale austauscht

Komplettsatz

1. Hub Plus
2. SmartBracket-Montageplatte
3. Netzkabel
4. Ethernetkabel
5. Einbausatz
6. GSM-Startpaket – 2 (nicht in allen Regionen verfügbar)
7. Benutzerhandbuch

Sicherheitsanforderungen

Beachten Sie bei der Installation und Nutzung der Hub-Zentrale die allgemeinen Vorschriften zur elektrischen Sicherheit bei der Verwendung von Elektrogeräten sowie die Anforderungen der gesetzlichen Vorschriften zur elektrischen Sicherheit.

Es ist strengstens verboten, das Gerät unter Spannung zu zerlegen! Verwenden Sie das Gerät nicht mit einem beschädigten Netzkabel.

Technische Daten

Geräte	bis zu 150
Gruppen	bis zu 25
Benutzern	bis zu 99
Videoüberwachung	Bis zu 50 Kameras oder DVRs
Räume	bis zu 50
Szenarien	bis zu 64 (Szenarien durch Scharfschalten/Entschärfen sind nicht in der allgemeinen Grenze der Szenarien enthalten)
Angeschlossenes ReX	bis zu 5
Netzteil	110 – 240 V AC, 50 / 60 Hz
Akkumulator	Li-Ion 2 A·h (bis zu 16 Stunden autonomer Betrieb bei inaktiver Ethernet- und Wi-Fi-Verbindung)
Energieverbrauch aus dem Netz	10 W
Manipulationsschutz	Ja
Frequenzband	868,0 – 868,6 MHz oder 868,7 – 869,2 MHz je nach Verkaufsregion
Effektive Strahlungsleistung	8,20 dBm/6,60 mW (Grenze 25 mW)
Modulation des Funksignals	GFSK
Funkreichweite	Bis zu 2.000 m (ohne Hindernisse)
Kommunikationskanäle	WiFi 2,4 GHz (802.11 b/g/n), Ethernet, 2 Steckplätze Micro-SIM, Netzwerke 2G (GSM900/DCS1800), 3G (WCDMA 900/2100, B8/B1)
Betriebstemperaturbereich	Von -10°C bis +40°C
Betriebsfeuchtigkeit	Bis zu 75%
Gesamtabmessungen	163 × 163 × 36 mm
Gewicht	350 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, wenden Sie sich zunächst an den Support – in der Hälfte der Fälle können technische Probleme aus der Ferne behoben werden!

[Der vollständige Text der Garantie](#)

[Nutzungsbedingungen](#)

Technischer Support: support@ajax.systems



Sie brauchen Hilfe?

Hier finden Sie detaillierte Handbücher und Schulungsvideos zu allen Funktionen von Ajax.

Außerdem stehen wir rund um die Uhr für Sie bereit, falls Sie die Hilfe eines technischen Spezialisten brauchen.

Anfrage senden