Hub Benutzerhandbuch

Aktualisiert December 7, 2020

Die **Hub-Zentrale** ist ein zentrales Gerät des Ajax-Sicherheitssystems, das die angeschlossenen Geräte koordiniert und mit dem Benutzer und dem Sicherheitsunternehmen interagiert. Verwendung in Innenräumen.

Die Hub-Zentrale 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 der Hub-Zentrale erfolgt über einen verschlüsselten Kanal auf einer 24-Stunden-Basis.

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

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

Die Hub-Zentrale 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 kaufen

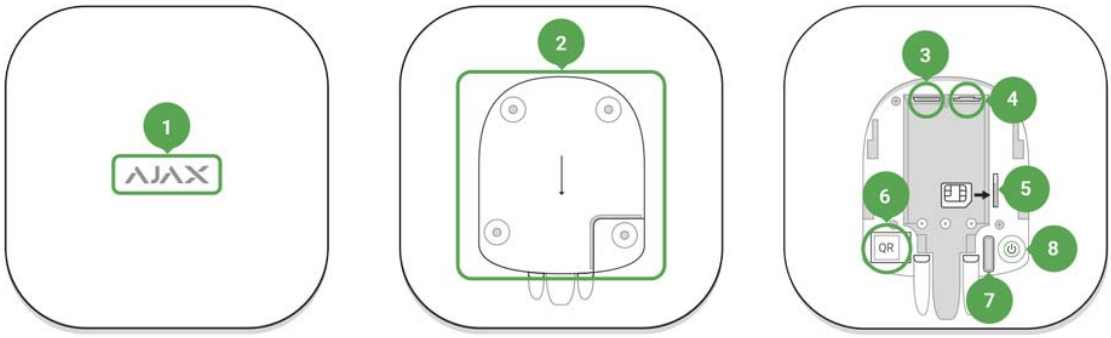
Bis zu 100 Ajax-Geräte können an die Hub-Zentrale angeschlossen werden. Das geschützte Jeweller-Funkprotokoll gewährleistet eine zuverlässige Kommunikation zwischen den Geräten in einer Entfernung von bis zu 2 km in der Sichtlinie.

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. QR-Code
7. Manipulationstaste
8. Netztaste

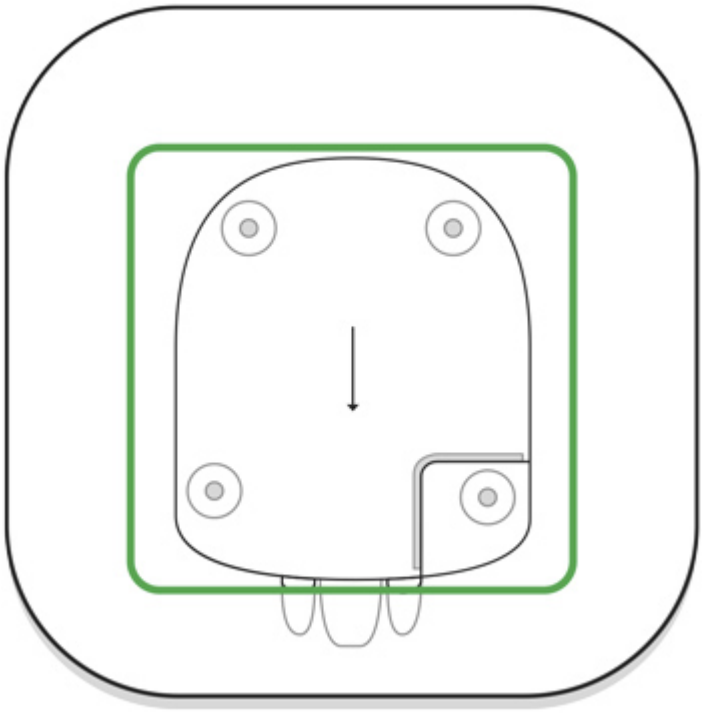
Hub-LED-Anzeige

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.

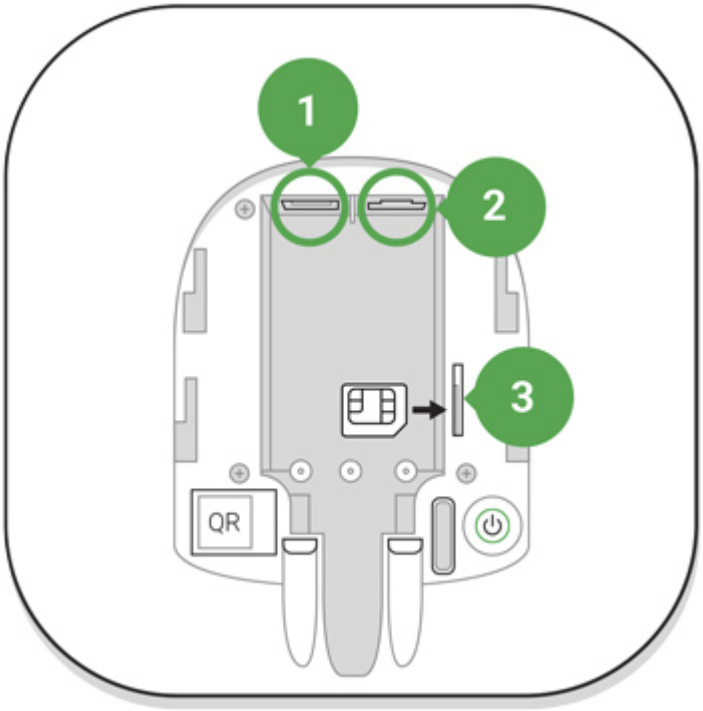
Anschluss an das Netzwerk

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



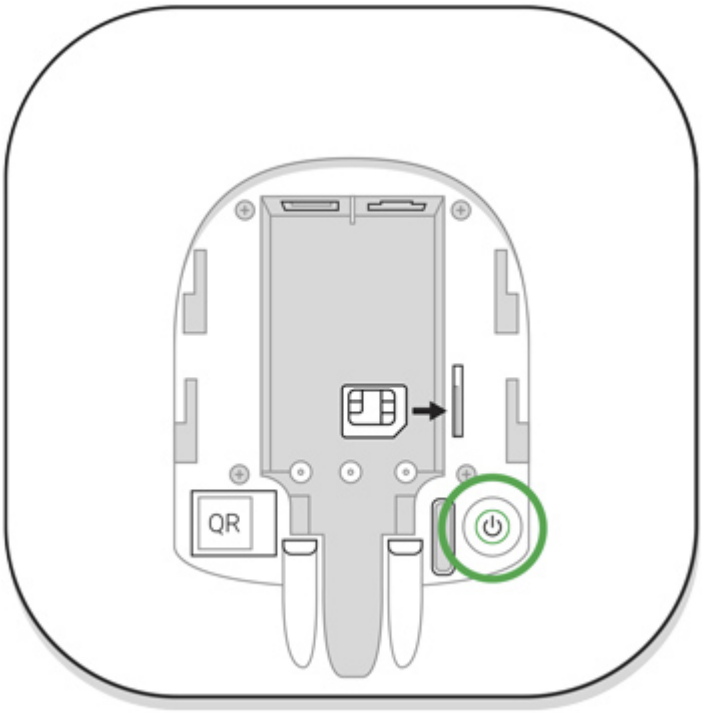
Seien Sie vorsichtig und beschädigen Sie nicht den Manipulationsschutz, der die Hub-Zentrale vor der Demontage schützt!

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



1 — Steckdose
2 — Ethernet-Buchse
3 — 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 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 die Hub-Zentrale 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.

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.

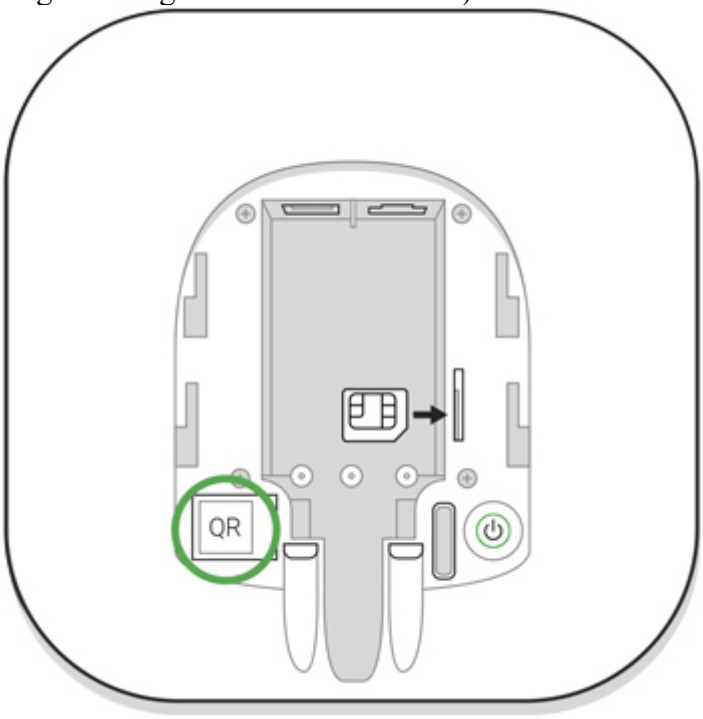
Das Ajax-Account erlaubt es, die Rollen zu kombinieren: Sie können sowohl der Administrator einer Hub-Zentrale als auch der Benutzer einer anderen Hub-Zentrale sein.

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.

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 Desktop der App 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.

Gerät ist nur für die Innenraummontage vorgesehen.

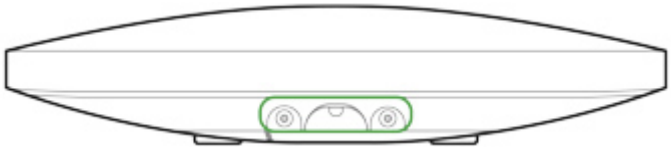
Die Hub-Zentrale sollte zuverlässig an der Oberfläche (vertikal oder horizontal) befestigt sein. Wir empfehlen nicht die Verwendung von doppelseitigem Klebeband: es kann keine sichere Befestigung garantieren und erleichtert die Entfernung des Geräts.

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

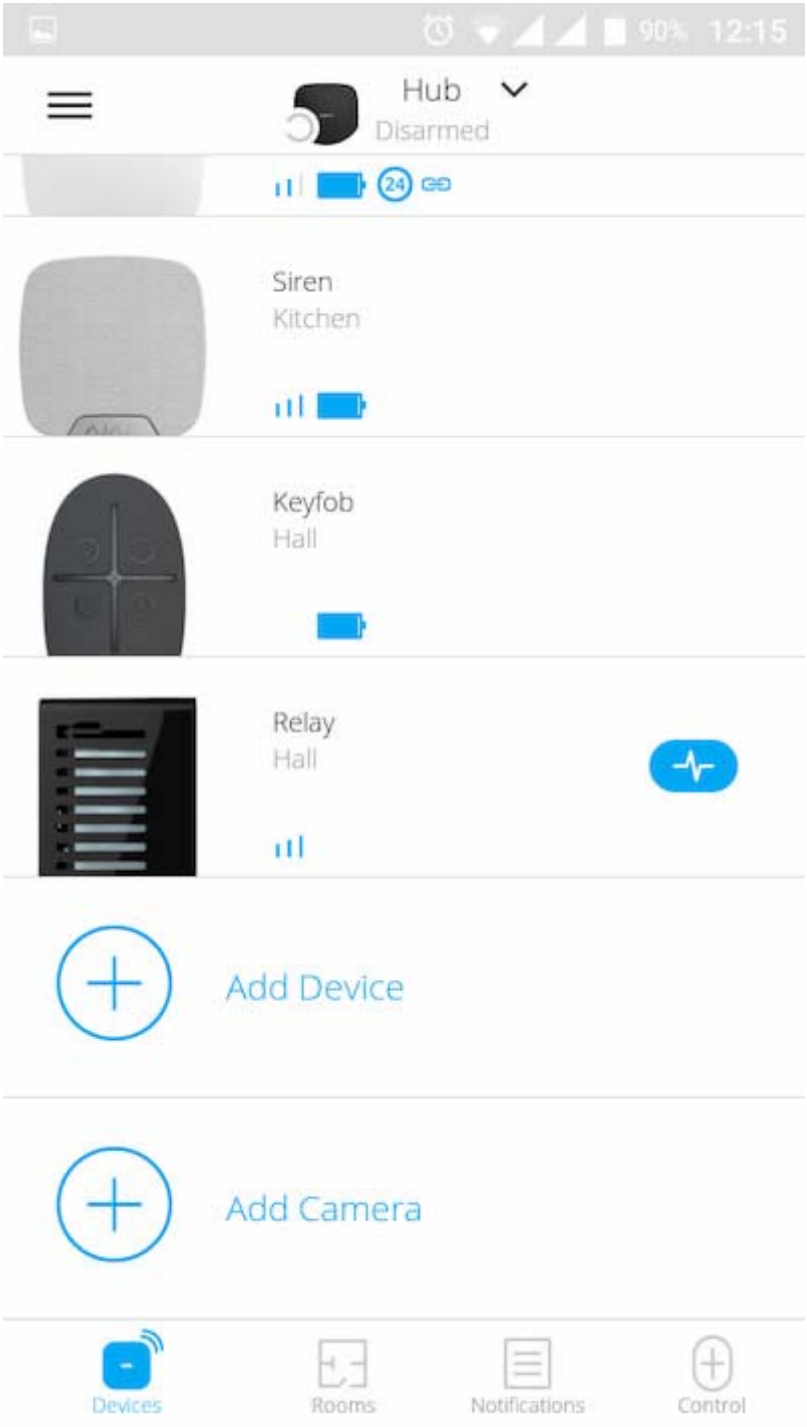
Der Raum wird in der App über das Menü **Raum hinzufügen** angelegt.

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.

Bis zu 10 Kameras oder DVRs, die das RTSP-Protokoll unterstützen, können an die Hub-Zentrale angeschlossen werden.

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

Hub-Zentralen-Status

Symbole

Die Symbole zeigen einige der Status von Hub 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. Anzeige in 5-%-Schritten
	Hub-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 aus der Liste aus.

Parameter	Bedeutung
Störung	Öffnen Sie mit einem Klick auf die Liste der Fehlfunktionen des Hub. Das Feld erscheint nur bei einer erkannten Störung
Mobilfunk-Signalstärke	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
Akku-Ladung	Ladezustand der Batterie das Gerät. Wird in Prozentsatz angezeigt Anzeige der Batterieladung in Ajax-Apps
Gehäusedeckel	Status des Manipulationsschutzes vor Demontage der Hub-Zentrale: • Geschlossen — Gehäusedeckel der Hub-Zentrale ist geschlossen • Geöffnet — die Hub-Zentrale wurde aus der SmartBracket-Halterung entfernt Was ist ein Manipulationsschutz?
Externe Stromversorgung	Status für externen Stromversorgungsanschluss: • Verbunden — die Hub-Zentrale ist an eine externe Stromversorgung angeschlossen • Getrennt — keine externe Stromversorgung

Verbindung	Verbindungsstatus zwischen Hub-Zentrale und Ajax Cloud: • Online — Hub-Zentrale ist mit der Ajax Cloud verbunden • Offline — Hub-Zentrale ist nicht mit der Ajax Cloud verbunden
Mobilfunk	Der Verbindungsstatus der Hub-Zentrale zum Mobilfunknetz: • Verbunden — die Hub-Zentrale ist über mobiles Internet mit der Ajax Cloud verbunden • Getrennt — die Hub-Zentrale ist nicht über das mobile Internet mit der Ajax Cloud verbunden 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 **Getrennt** in diesem Feld angezeigt wird
Ethernet	Internetverbindungsstatus der Hub-Zentrale über Ethernet: • Verbunden — die Hub-Zentrale ist über Ethernet mit der Ajax Cloud verbunden • Getrennt — die Hub-Zentrale ist nicht über Ethernet mit der Ajax Cloud verbunden
Mittlerer Rauschpegel (dBm)	Rauschen im Jeweller-Frequenzbereich. Empfohlene Wert liegt bei -80 dBm oder weniger

Überwachungsstation	Der Status der Direktverbindung der Hub-Zentrale zur Überwachungszentrale des Sicherheitsdienstes: • Verbunden — die Hub-Zentrale ist direkt mit der Überwachungszentrale des Sicherheitsdienstes verbunden • 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

Einstellungen

Einstellungen können in der Ajax App geändert werden:

1. Öffnen Sie die Registerkarte **Geräte** .
2. Wählen Sie Hub aus der Liste aus.
3. Öffnen Sie mit einem Klick auf die **Einstellungen**.

Beachten Sie, dass Sie nach dem Ändern der Einstellungen auf die Schaltfläche **Zurück** klicken sollten, um sie zu speichern.

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 — Benutzereinstellungen für ein Sicherheitssystem: welche Berechtigungen den Benutzern gewährt werden und wie das Sicherheitssystem sie über Ereignisse und Alarme benachrichtigt.

Um die Benutzereinstellungen zu ändern, klicken Sie auf gegenüber dem Benutzernamen.

Wie das Ajax Sicherheitssystem Benutzer über Warnungen benachrichtigt
So fügen Sie der Hub-Zentrale neue Benutzer hinzu

Ethernet — Einstellungen für eine kabelgebundene Internetverbindung.

- Ethernet — ermöglicht Ihnen die De-/Aktivierung von Ethernet auf der Hub-Zentrale
- DHCP/Statisch — Auswahl des Typs der zu empfangenden IP-Adresse der Hub-Zentrale: dynamisch oder statisch
- IP-Adresse — IP-Adresse der Hub-Zentrale
- Subnetzmaske — Subnetzmaske, die die Hub-Zentrale verwendet
- Router — von der Hub-Zentrale verwendetes Gateway
- DNS — DNS der Hub-Zentrale

Mobilfunk — Aktivieren/Deaktivieren der Mobilfunk-Kommunikation, Konfigurieren von Verbindungen und Account prüfen.

- Mobilfunk — deaktiviert und aktiviert SIM-Karten auf der Hub-Zentrale
- Roaming — wenn Roaming aktiviert ist, können die in der Hub-Zentrale installierten SIM-Karten Roaming nutzen
- Fehler der Netzwerkregistrierung ignorieren — wenn diese Einstellung aktiviert ist, ignoriert die Hub-Zentrale Fehler beim Versuch, eine Verbindung über eine SIM-Karte herzustellen. Aktivieren Sie diese Option, wenn die SIM-Karte keine Verbindung zum Netzwerk herstellen kann.
- Ping vor dem Verbindungsaufbau deaktivieren — wenn diese Einstellung aktiviert ist, ignoriert die Hub-Zentrale Kommunikationsfehler des Mobilfunkanbieters. Aktivieren Sie diese Option, wenn die SIM-Karte keine Verbindung zum Netzwerk herstellen kann.
- SIM 1 — zeigt die Nummer der installierten SIM-Karte an. Klicken Sie auf das Feld, um zu den Einstellungen der SIM-Karte zu gelangen

SIM-Karten-Einstellungen

Verbindungseinstellungen

- **APN**, **Benutzername** und **Passwort** — Einstellungen für die Verbindung mit dem Internet über eine SIM-Karte. Die Einstellungen des Mobilfunkanbieters können über dessen Kundendienst erfragt werden.

Einrichten und bearbeiten des APN in der Hub-Zentrale

Mobildatennutzung

- **Eingehend** — die Menge der von der Hub-Zentrale empfangenen Daten. Anzeige in KB oder MB.
- **Ausgehend** — die Menge der von der Hub-Zentrale gesendeten Daten. Anzeige in KB oder MB.

Denken Sie daran, dass die Datennutzung von der Hub-Zentrale gemessen wird und von den Statistiken Ihres Anbieters abweichen kann.

Statistik zurücksetzen — setzt die Statistiken über ein- und ausgehenden Datenverkehr zurück.

Guthaben prüfen

- **USSD-Code** — geben Sie in diesem Feld den Code ein, der zur Überprüfung des Guthabens verwendet wird. Zum Beispiel *111#. Klicken Sie danach auf **Guthaben abfragen**, um eine Anfrage zu senden. Das Ergebnis wird unter der Schaltfläche angezeigt.

Geofence — Konfiguration von Erinnerungen zur Scharf-/Unscharfschaltung des Sicherheitssystems beim Durchqueren eines bestimmten Gebiets. Der Standort des Benutzers wird mit dem GPS-Modul des Smartphones bestimmt.

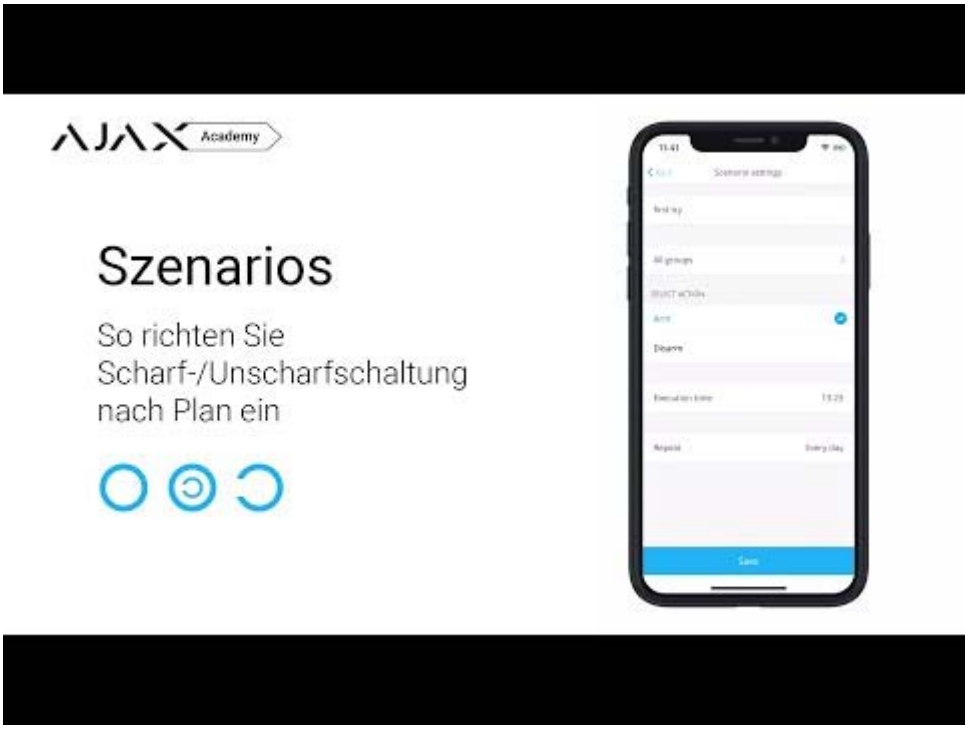
Geofences und deren Funktionsweise

Gruppen — Konfiguration des Gruppenmodus. Dies ermöglicht Ihnen Folgendes:

- Verwalten der Sicherheitsmodi für separate Bereiche oder Gruppen von Meldern.
  Zum Beispiel ist das Büro scharfgeschaltet, während die Reinigungskraft in der Küche arbeitet.
- Abgegrenzter Zugang zur Kontrolle der Sicherheitsmodi.
  Zum Beispiel haben die Mitarbeiter der Marketingabteilung keinen Zugang zur Rechtsabteilung.

OS Malevich 2.6: eine neue Stufe der Sicherheit

Sicherheitszeitplan — Scharf-/Unscharschaltung des Sicherheitssystems nach Zeitplan.



Erstellen und Konfigurieren eines Szenarios im Ajax Sicherheitssystem

Erfassungsbereichstest — Ausführen des Erkennungsbereichstests für die angebundenen Melder. Der Test bestimmt die ausreichende Entfernung für die Registrierung von Alarmen durch die Melder.

Der Erfassungsbereichstest

Jeweller — Konfigurieren des Ping-Intervalls der Hub-Zentrale für den Melder. Die Einstellungen bestimmen, wie häufig die Hub-Zentrale mit Geräten kommuniziert und wie schnell ein Verbindungsverlust erkannt wird.

Mehr erfahren

- **Melder-Ping-Intervall** — die Häufigkeit, mit der die angeschlossenen Geräte von der Hub-Zentrale abgefragt werden, ist im Bereich von 12 bis 300 s (Standard: 36 s) einstellbar
- **Anzahl nicht übermittelter Pakete zur Bestimmung des Verbindungsfehlers** — ein Zähler für nicht übermittelte Pakete (Standard: 8 Pakete).

Die Zeit bis zum Auslösen des Alarms durch den Kommunikationsverlust zwischen Hub-Zentrale und Gerät wird mit der folgenden Formel berechnet:

*Ping-Intervall * (Anzahl der nicht übermittelten Pakete + 1 Korrekturpaket)*

Ein kürzeres Ping-Intervall (in Sekunden) bedeutet zwar eine schnellere Übertragung der Ereignisse zwischen Hub-Zentrale und den angeschlossenen Geräten, aber auch eine geringere Batterielebensdauer. Alarme werden stets unabhängig vom Ping-Intervall sofort übertragen.

Wir raten davon ab, die Standardeinstellungen von Ping-Periode und -Intervall zu verkürzen.

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

Intervall	Verbindungslimit
12 Sekunden	39 Geräte
24 Sekunden	79 Geräte
36 und mehr Sekunden	100 Geräte

Unabhängig von den Einstellungen unterstützt die Hub-Zentrale maximal 10 angeschlossene Sirenen!

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!

Wie man einen Fehlerbericht versendet

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 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 → SpaceContol → 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 Ereignis-Protokoll der Hub-Zentrale gelöscht.

Überwachungszentrale — die Einstellungen für die direkte Verbindung zur Überwachungszentrale des Sicherheitsdienstes. Die Parameter werden vom technischen Personal des Sicherheitsdienstes eingestellt. Denken Sie daran, dass Ereignisse und Alarme auch ohne diese Einstellungen an die Überwachungszentrale des Sicherheitsdienstes gesendet werden können.

Die Registerkarte „Überwachungszentrale“

- **Protokoll** — die Wahl des Protokolls, das von der Hub-Zentrale verwendet wird, um Alarme über eine direkte Verbindung an die Überwachungszentrale des Sicherheitsdienstes zu senden. Verfügbare Protokolle: Ajax Translator (Contact ID) und SIA.
- **Bei Bedarf verbinden**. Aktivieren Sie diese Option, wenn Sie nur bei der Übertragung eines Ereignisses eine Verbindung zur Überwachungszentrale benötigen. Wenn die Option deaktiviert ist, wird die Verbindung kontinuierlich aufrechterhalten. Diese Option ist nur für das SIA-Protokoll verfügbar.
- **Objektnummer** — die Nummer eines Objekts in der Überwachungsstation (Hub-Zentrale).

Primäre IP-Adresse

- **IP-Adresse** und **Port** sind Einstellungen der primären IP-Adresse und des Ports des Servers des Sicherheitsdienstes, an den Ereignisse und Alarme gesendet werden.

Sekundäre IP-Adresse

- **IP-Adresse** und **Port** sind Einstellungen der sekundären IP-Adresse und des Ports des Servers des Sicherheitsdienstes, an den Ereignisse und Alarme gesendet werden.

Alarm-Sendekanäle

In diesem Menü werden Kanäle zum Senden von Alarmen und Ereignissen an die zentrale Überwachungsstation des Sicherheitsdienstes ausgewählt. Hub 2 Plus kann über **Ethernet** und **EDGE** Alarme und Ereignisse an die Überwachungszentrale senden. Wir empfehlen Ihnen, alle Kommunikationskanäle gleichzeitig zu nutzen – das erhöht die Übertragungssicherheit und schützt vor Ausfällen auf der Seite der Telekommunikationsanbieter.

- **Ethernet** — ermöglicht die Ereignis- und Alarmübertragung über Ethernet.
- **Mobilfunk** — ermöglicht die Ereignis- und Alarmübertragung über das mobile Internet.
- **Periodischer Testbericht** — wenn aktiviert, sendet die Hub-Zentrale Testberichte mit einem bestimmten Zeitraum an die CMS (Überwachungszentrale) zur zusätzlichen Überwachung der Objektverbindung.
- **Ping-Intervall der Überwachungszentrale** — legt den Zeitraum für das Versenden von Testnachrichten fest: von 1 Minute bis 24 Stunden.

Verschlüsselung

Verschlüsselungseinstellungen für die Ereignisübertragung im SIA-Protokoll. Es wird eine AES 128-Bit-Verschlüsselung verwendet.

- **Verschlüsselung** — wenn aktiviert, werden Ereignisse und Alarme, die im SIA-Format an die zentrale Überwachungsstation übertragen werden, verschlüsselt.
- **Sicherheitsschlüssel** — Verschlüsselungsschlüssel der übertragenen Ereignisse und Alarme. Muss mit dem Wert der Überwachungszentrale übereinstimmen.

Paniktaste Koordinaten

- **Koordinaten senden** — bei aktivierter Funktion werden bei Betätigung der App-Paniktaste die Koordinaten desjenigen Geräts an die Überwachungszentrale gesendet, auf dem die App installiert ist und die Paniktaste gedrückt wurde.

Alarmwiederherstellung an der Leitstelle

Mit dieser Einstellung können Sie wählen, wann das Wiederherstellungsereignis an die Leitstelle übermittelt wird: sofort (standardmäßig) oder bei Unscharfschaltung der Alarmanlage.

Mehr erfahren

PRO — Einstellungen für PRO-Benutzer des Sicherheitssystems (Service-Techniker*innen und Vertreter*innen von Sicherheitsdiensten). Bestimmen, wer Zugriff auf das Sicherheitssystem hat, welche Berechtigungen PRO-Benutzer erhalten und wie das Sicherheitssystem sie über die Ereignisse informiert.

So fügen Sie der Hub-Zentrale das PRO hinzu

Sicherheitsunternehmen — eine Liste der Sicherheitsdienste in Ihrem Bereich. Das Gebiet wird durch die GPS-Daten oder die regionalen Einstellungen Ihres Smartphones bestimmt.

Benutzerhandbuch — öffnet das Hub-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.**

Mehr über Datenimport erfahren

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

Einstellungen zurücksetzen

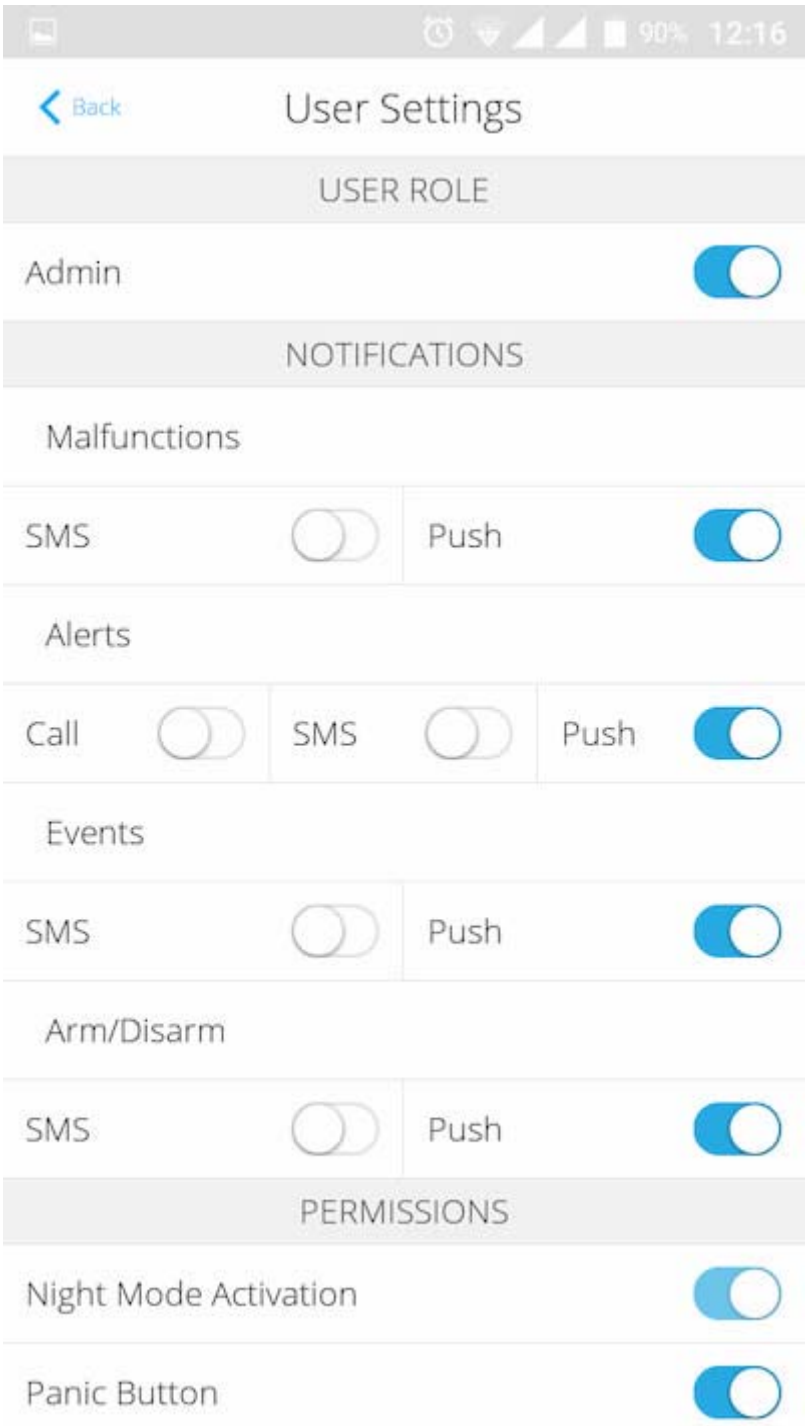
Um die Hub-Zentrale auf die werkseitigen Standardeinstellungen zurückzusetzen, schalten Sie ihn ein und halten Sie dann den Netzschalter 30 Sekunden lang gedrückt (das Logo beginnt rot zu blinken).

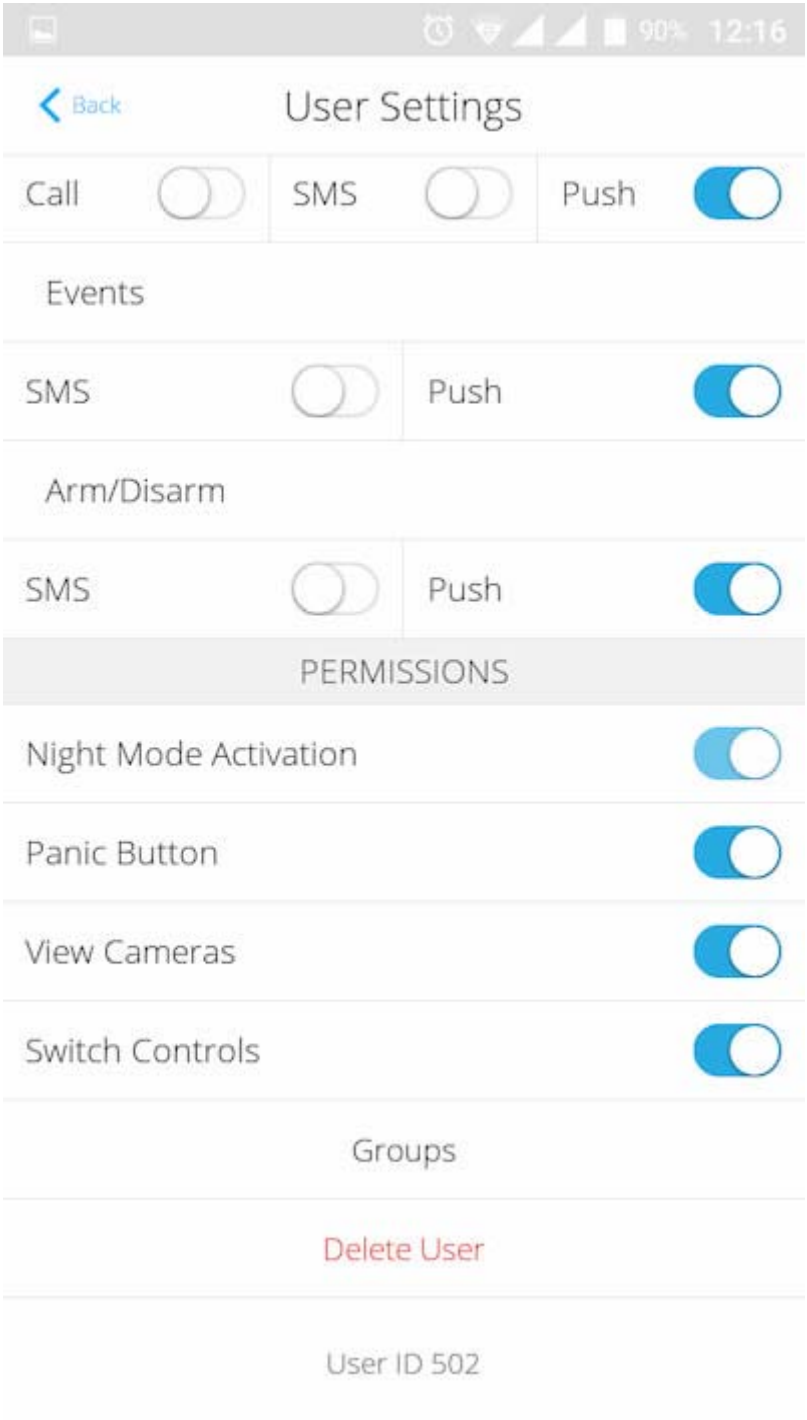
Gleichzeitig werden alle angeschlossenen Melder, Raum- und Benutzereinstellungen gelöscht. Die Benutzerprofile bleiben mit dem System verbunden.

Benutzern

Nachdem Sie die Hub-Zentrale zum Konto hinzugefügt haben, werden Sie Administrator dieses Geräts. Eine Hub-Zentrale kann bis zu 50 Benutzer/Administratoren haben. Der Administrator kann Benutzer in das Sicherheitssystem einladen und ihre Rechte festlegen.

Ereignisse und Alarmbenachrichtigungen


90% 12:16
Back
User Settings
USER ROLE
Admin
NOTIFICATIONS
Malfunctions
SMS
Push
Alerts
Call
SMS
Push
Events
SMS
Push
Arm/Disarm
SMS
Push
PERMISSIONS
Night Mode Activation
Panic Button



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 werden nach dem Scharfschalten/Unscharfschalten empfangen	• SMS • Push-Benachrichtigung

Alarm	Hinweise auf Eindringen, Feuer, Überschwemmung	• SMS • Push-Benachrichtigung • Anruf
Ereignisse	Benachrichtigungen über Ereignisse im Zusammenhang mit Ajax WallSwitch, Relay-Steuerung	• SMS • Push-Benachrichtigung
Störungen	Hinweise auf verlorene Kommunikation, Blockieren, niedrige Batterieladung oder Öffnen des Meldergehäuses	• SMS • Push-Benachrichtigung

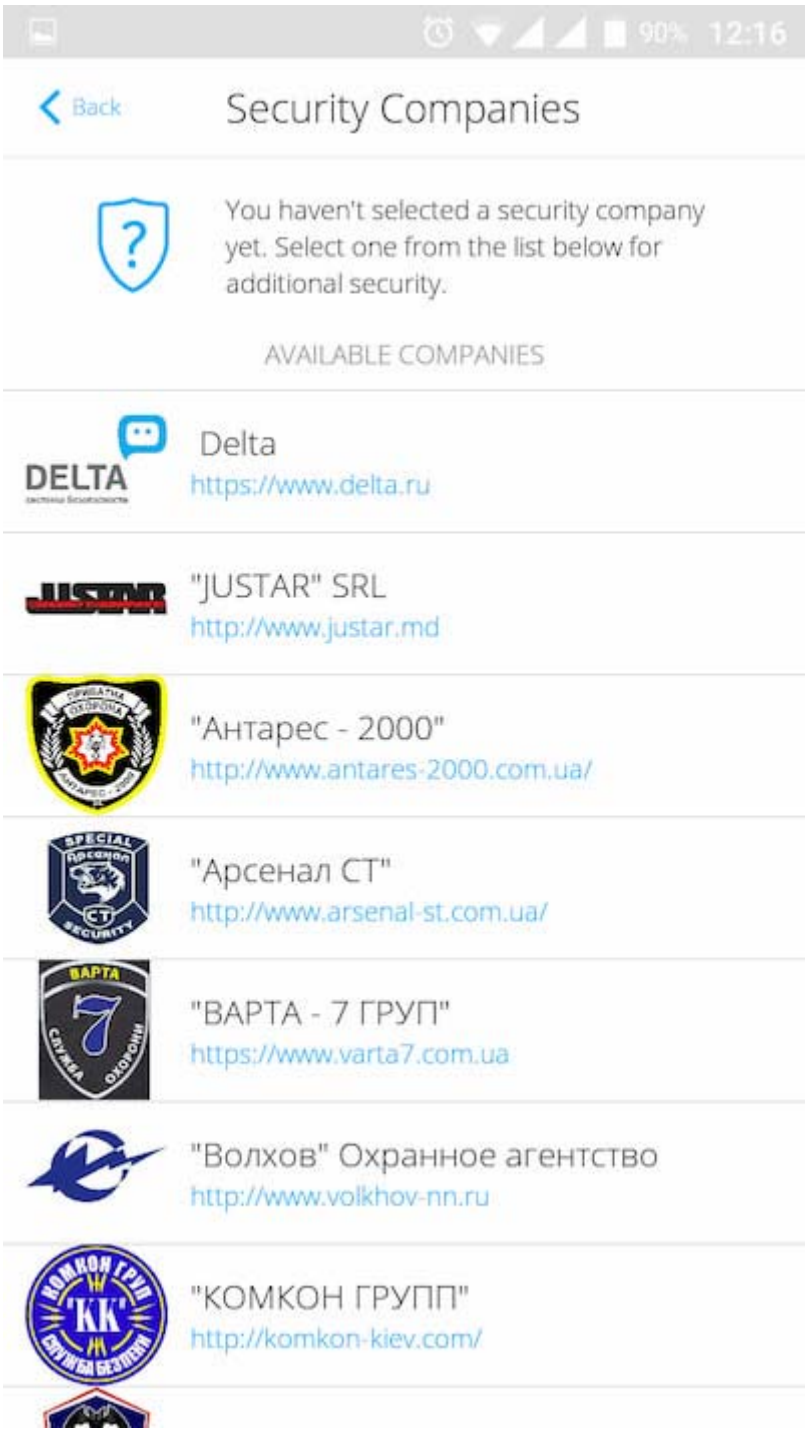
- Die **Push-Benachrichtigung** wird von der Ajax Cloud an die Ajax Security System-App gesendet, wenn eine Internetverbindung verfügbar ist.
- Die **SMS** wird an die vom Benutzer bei der Registrierung des Ajax-Kontos angegebene Telefonnummer gesendet.
- Der **Telefonanruf** bedeutet, dass die Hub-Zentrale 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. Wir empfehlen, 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. Ajax Hub
2. SmartBracket-Montageplatte
3. Netzkabel
4. Ethernetkabel
5. Einbausatz
6. Mikro-SIM (in einigen Ländern nicht enthalten)
7. Schnellstartanleitung

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 100
Gruppen	bis zu 9
Benutzern	bis zu 50
Videoüberwachung	Bis zu 10 Kameras oder DVRs
Räume	bis zu 50
Szenarien	bis zu 5 (Szenarien durch Scharfschalten/Entschärfen sind nicht in der allgemeinen Grenze der Szenarien enthalten)
Angeschlossenes ReX	1
Netzteil	110 – 240 V AC, 50/60 Hz
Akkumulator	Li-Ion 2 A·h (bis zu 15 Stunden autonomer Betrieb bei inaktiver Ethernet-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	GSM 850/900/1800/1900 MHz GPRS, Ethernet
Installation	In Innenräumen
Betriebstemperaturbereich	Von -10°C bis +40°C
Betriebsfeuchtigkeit	Bis zu 75%
Gesamtabmessungen	163 × 163 × 36 mm
Gewicht	350 g
Zertifizierung	Sicherheitsstufe 2, Umweltklasse II SP2 (GSM-SMS), SP5 (LAN) DP3 in Übereinstimmung mit den Anforderungen von EN 50131-1, EN 50131-3, EN 50136-2, EN 50131-10, EN 50136-1, EN 50131-6, EN 50131-5-3

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