Hub 2 Plus Benutzerhandbuch

Aktualisiert November 15, 2020

Hub 2 Plus ist eine Alarmzentrale im Ajax Sicherheitssystem, die den Betrieb aller angebundenen Geräte steuert und mit Benutzern und Sicherheitsdiensten interagiert.

Die Hub-Zentrale meldet das Öffnen von Türen, das Zerbrechen von Fenstern, die Gefahr durch Feuer oder Überschwemmung und automatisiert wiederkehrende Vorgänge mithilfe von Szenarien. Wenn Eindringlinge den gesicherten Raum betreten, sendet Hub 2 Plus Fotos von **MotionCam**-Bewegungsmeldern und benachrichtigt den Sicherheitsdienst zwecks Entsendung von Sicherheitskräften.

Die Hub 2 Plus-Zentraleinheit darf nur im Innenbereich installiert werden.

Hub 2 Plus benötigt einen Internetzugang für die Verbindung mit der Ajax Cloud. Die Zentraleinheit ist über Ethernet, WLAN und zwei SIM-Karten (2G/3G/4G) mit dem Internet verbunden.

Die Verbindung zur Ajax Cloud ist notwendig für die Konfiguration und Verwaltung des Systems über Ajax Apps, die Übertragung von Alarm- und Ereignismeldungen sowie die Aktualisierung des **OS Malevich**. Der Ajax Cloud-Dienst wird von den Amazon Web Services (AWS) gehostet. Alle Daten in der Ajax Cloud werden mit mehrstufigem Schutz gespeichert und die Informationen werden über einen verschlüsselten Kanal mit der Hub-Zentrale ausgetauscht.

> Nutzen Sie alle Kommunikationskanäle, um eine zuverlässigere Verbindung mit der Ajax Cloud zu gewährleisten und sich gegen Unterbrechungen der Telekommunikationsdienste der jeweiligen Anbieter abzusichern.

Über **Apps** für iOS und Android sowie Anwendungen für MacOS und Windows können Sie das Sicherheitssystem verwalten und schnell auf Alarme und Benachrichtigungen reagieren. Das System ermöglicht Ihnen die Auswahl der zu meldenden Ereignisse und die Art der Benachrichtigung: durch Push-Nachrichten, SMS oder Anrufe.

- **Einrichten von Push-Benachrichtigungen unter iOS**
- **Einrichten von Push-Benachrichtigungen unter Android**

Ist das System an einen Sicherheitsdienst angeschlossen, werden Ereignisse und Alarme an die Überwachungszentrale übertragen — **direkt und/oder über die Ajax Cloud**.

☞ **Zentraleinheit Hub 2 Plus kaufen**

Funktionselemente

1. Ajax Logo mit LED-Anzeige
2. SmartBracket-Montageplatte. Zum Öffnen kräftig nach unten schieben

Das perforierte Teil ist erforderlich, um den Manipulationsschutz im Falle eines Versuchs, die Hub-Zentrale zu demontieren, zu betätigen. Nicht abbrechen!

3. Netzkabel-Buchse
4. Ethernet-Kabelbuchse
5. Steckplatz für Mikro-SIM 2
6. Steckplatz für Mikro-SIM 1
7. QR-Code
8. Manipulationsschutztaste
9. Ein/Aus-Taste

Funktionsprinzip

Die Hub-Zentrale überwacht den Betrieb des Sicherheitssystems, indem sie mit den angeschlossenen Geräten über das **verschlüsselte Jeweller-Protokoll** kommuniziert. Die Funkreichweite beträgt bis zu 2000 m (Freifeld, also ohne Hindernisse wie Wände, Türen, Deckenkonstruktionen). Bei Ansprechen des Melders löst das System innerhalb von 0,15 Sekunden Alarm aus, aktiviert die Sirenen und benachrichtigt die Überwachungszentrale des Sicherheitsdienstes und die Benutzer.

Bei Störungen auf den Betriebsfrequenzen oder bei Störungsversuchen schaltet Ajax auf eine freie/ungestörte Funkfrequenz um und sendet Benachrichtigungen an die Überwachungszentrale des Sicherheitsdienstes und an die Systembenutzer.

☞ **Stören/Sabotage eines drahtlosen Sicherheitssystems und wie man sich davor schützen kann**

Hub 2 Plus unterstützt bis zu 200 angeschlossene Ajax Geräte, die vor Eindringen, Feuer und Überschwemmung schützen und steuert elektrische (Haushalts-)Geräte automatisch mittels Szenarien oder manuell über eine App.

Für das Senden von Fotos vom **MotionCam**-Bewegungsmelder werden ein gesondertes Wings-Funkprotokoll und eine speziell dafür vorgesehene Antenne

verwendet. So wird die Durchführung einer visuellen Alarmverifizierung auch bei schwankender Signalstärke und Kommunikationsunterbrechungen gewährleistet.

☞ **Alle Ajax-Geräte**

Hub 2 Plus läuft auf dem Echtzeitbetriebssystem OS Malevich. Ähnliche Betriebssysteme kommen in Steuerungssystemen für Raumfahrzeuge, ballistische Raketen und Autobremsen zum Einsatz. Das OS Malevich erweitert die Fähigkeiten des Sicherheitssystems und wird ohne Benutzereingriff über die Luft- bzw. Funkschnittstelle **automatisch aktualisiert**.

Nutzen Sie Szenarien zur Automatisierung des Sicherheitssystems und reduzieren Sie wiederkehrende Vorgänge auf ein Minimum. Richten Sie den Sicherheitszeitplan ein und programmieren Sie Aktionen von Automatisierungsgeräten (**Relay**, **WallSwitch** oder **Socket**) als Reaktion auf einen Alarm, das Betätigen von **Button** oder nach Zeitplan. Ein Szenario kann auch mobil in der Ajax App angelegt werden.

☞ **Erstellen und Konfigurieren eines Szenarios im Ajax Sicherheitssystem**

LED-Anzeige

Das Ajax Logo auf der Vorderseite der Hub-Zentrale leuchtet rot, weiß oder grün – je nach Status der Stromversorgung und der Internetverbindung.

Ereignis	LED-Anzeige
Mindestens zwei Kommunikationskanäle — WLAN, Ethernet oder SIM-Karte — sind verbunden	Leuchtet weiß
Nur ein Kommunikationskanal ist verbunden	Leuchtet grün

Die Hub-Zentrale ist nicht mit dem Internet verbunden oder es besteht keine Verbindung zum Ajax Cloud-Server	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 Apps** konfiguriert und gesteuert. Ajax Anwendungen sind für Fachanwender und Benutzer für iOS, Android, MacOS und Windows verfügbar.

Die Einstellungen der Benutzer des Ajax Sicherheitssystems und die Parameter der angebundenen Geräte werden lokal auf der Hub-Zentrale gespeichert und sind untrennbar mit ihr verbunden. Bei einem Wechsel des Administrators der Hub-Zentrale werden die Einstellungen der angeschlossenen Geräte nicht zurückgesetzt.

Zur Konfiguration des Systems installieren Sie die Ajax Anwendung und **erstellen einen Account**. Die Telefonnummer und E-Mail-Adresse darf bei der Erstellung nur einem einzigen Ajax Account zugeordnet werden! Es muss nicht für jede Hub-Zentrale ein neues Konto erstellt werden — über ein Konto können mehrere Hub-Zentralen verwaltet werden.

Ihr Konto kann zwei Rollen kombinieren: die des Administrators einer Hub-Zentrale und die des Benutzers einer anderen Hub-Zentrale.

Sicherheitsanforderungen

Befolgen Sie bei der Installation und beim Betrieb des Hub 2 Plus genau die allgemeinen Sicherheitsbestimmungen für den Betrieb von elektrischen Geräten und die Anforderungen der gesetzlichen Bestimmungen zur elektrischen Sicherheit.

Es ist strengstens verboten, das unter Spannung stehende Gerät auseinanderzubauen! Verwenden Sie das Gerät auch nicht mit einem

beschädigten Netzkabel.

Verbinden mit dem Netzwerk

1. Entfernen Sie die SmartBracket-Montageplatte, indem Sie sie mit Kraft nach unten schieben. Vermeiden Sie eine Beschädigung des perforierten Teils — es ist für die Aktivierung des Manipulationsschutzes bei der Demontage der Hub-Zentrale unerlässlich!

2. Schließen Sie die Kabel für Stromversorgung und Ethernet an die entsprechenden Buchsen an und installieren Sie die SIM-Karten.

1 — Stromanschluss
2 — Ethernet-Anschluss
3, 4 — Steckplätze für Mikro-SIM-Karten

3. Ein/Aus-Taster 3 Sekunden lang gedrückt halten, bis das Ajax Logo aufleuchtet. Es dauert etwa 2 Minuten, bis die Hub-Zentrale auf die neueste Firmware aktualisiert und mit dem Internet verbunden ist. Ein grünes bzw. weißes Logo zeigt an, dass die Hub-Zentrale in Betrieb und mit der Ajax Cloud verbunden ist.

Wenn die Ethernet-Verbindung nicht automatisch hergestellt wird, deaktivieren Sie den Proxy- und MAC-Adressenfilter und aktivieren Sie DHCP in den

Routereinstellungen. Der Hub-Zentrale wird automatisch eine IP-Adresse zugewiesen. Danach können Sie in der Ajax App eine statische IP-Adresse der Hub-Zentrale einrichten.

4. Für die Verbindung mit dem Mobilfunknetz benötigen Sie eine Mikro-SIM-Karte mit deaktivierter PIN-Code-Abfrage (Sie können sie mit einem Mobiltelefon deaktivieren) und ein ausreichendes Guthaben auf Ihrem Konto, um die Dienste zu den Tarifen Ihres Betreibers zu bezahlen. Sollte die Hub-Zentrale keine Verbindung zum Mobilfunknetz herstellen können, konfigurieren Sie die Netzwerkparameter über Ethernet: Roaming, APN-Zugangspunkt, Benutzername und Passwort. Wenden Sie sich an Ihren Telekommunikationsanbieter, um Unterstützung bei der Auswahl dieser Optionen zu erhalten.

Hinzufügen einer Hub-Zentrale zur Ajax App

1. Schalten Sie die Hub-Zentrale ein und warten Sie, bis das Logo grün oder weiß aufleuchtet.
2. Öffnen Sie die Ajax App. Erlauben Sie den Zugriff auf die angeforderten Systemfunktionen, um die Möglichkeiten der Ajax App voll auszuschöpfen und **keine Meldungen über Alarme oder Ereignisse zu verpassen**.
   - Einrichten von Benachrichtigungen unter iOS
   - Einrichten von Benachrichtigungen unter Android
3. Öffnen Sie das Menü **Hub-Zentrale hinzufügen**, und wählen Sie die Art der Registrierung: manuell oder menügeführte Schritt-für-Schritt-Anleitung. Wenn Sie das System zum ersten Mal einrichten, verwenden Sie eine Schritt-für-Schritt-Anleitung.
4. Geben Sie den Namen der Hub-Zentrale ein und scannen Sie den QR-Code unterhalb der SmartBracket-Montageplatte ein, oder geben Sie ihn manuell ein.
5. Warten Sie, bis die Hub-Zentrale hinzugefügt wurde. Die verbundene Hub-Zentrale wird in der Registerkarte **Geräte** angezeigt .

Nach dem Hinzufügen einer Hub-Zentrale zu Ihrem Konto sind Sie der Administrator des Geräts. Administratoren können andere Benutzer in das Sicherheitssystem einladen und deren Berechtigungen festlegen. Die Zentraleinheit Hub 2 Plus kann von bis zu 200 Benutzern genutzt werden.

Beim Wechseln oder Löschen des Administrators werden die Einstellungen der Hub-Zentrale oder der angebundenen Geräte nicht zurückgesetzt.

Benutzerberechtigungen im Ajax Sicherheitssystem

Hub-Zentralen-Status

Symbole

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

Symbole	Wert
	2G verbunden
	3G verbunden
	LTE verbunden
	SIM-Karte nicht installiert
	Die SIM-Karte ist defekt oder hat einen PIN-Code
	Akku/Batterie-Ladezustand von Hub 2 Plus. Anzeige in 5-%-Schritten
	Hub 2 Plus-Fehlfunktion wird erkannt. Die Liste wird in der Statusliste der Hub-Zentrale angezeigt
	Die Hub-Zentrale ist direkt mit der Überwachungszentrale des Sicherheitsdienstes verbunden
	Die Hub-Zentrale ist nicht mehr direkt mit der Überwachungszentrale des Sicherheitsdienstes verbunden

Status

Status sind in der Ajax App aufgeführt:

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

Parameter	Bedeutung
Störung	Öffnen Sie mit einem Klick auf die Liste der Fehlfunktionen des Hub 2 Plus.

	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	Batterie-/Akkuladezustand. Anzeige in 5-%-Schritten
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
Aktiv	Zeigt die aktive SIM-Karte an: SIM-Karte 1 oder SIM-Karte 2
SIM 1	Die Nummer der SIM-Karte im ersten Steckplatz. Kopieren Sie die Nummer, indem Sie sie anklicken
SIM 2	Die Nummer der SIM-Karte im zweiten Steckplatz. Kopieren Sie die Nummer, indem Sie sie anklicken
WLAN	Internetverbindungsstatus der Hub-Zentrale über WLAN. Um die Zuverlässigkeit zu erhöhen, wird empfohlen, die Hub-Zentrale an Orten mit einer Signalstärke von 2 bis 3 Balken zu installieren
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)	Rauschleistungspegel am Installationsort der Hub-Zentrale. Die ersten beiden Werte zeigen den Pegel bei Jeweller- und der dritte den bei Wings-Frequenzen an. Der akzeptable Wert beträgt -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

Räume

Erstellen Sie mindestens einen Raum, bevor Sie einen Melder oder ein Gerät mit einer Hub-Zentrale verknüpfen. Räume werden zur Gruppierung von Meldern und Geräten genutzt und erhöhen den Informationsgehalt von Benachrichtigungen. Der Name des Gerätes und des Raumes wird im Text des Ereignisses oder des Alarms des Sicherheitssystems angezeigt.

Erstellen eines Raums in der Ajax App:

1. Öffnen Sie die Registerkarte **Räume** .
2. Klicken Sie auf **Raum hinzufügen**.

3. Vergeben Sie einen Namen für den Raum und fügen Sie optional ein Foto bei oder machen Sie ein Foto: So können Sie den jeweiligen Raum in der Liste schnell finden.
4. Klicken Sie auf **Speichern**.

Um den Raum zu löschen oder seinen Avatar oder Namen zu ändern, öffnen Sie mit einem Tippen/Klick auf die **Raumeinstellungen**.

Anmelden von Meldern und Geräten

Wenn Sie Ihrem Konto mithilfe der Schritt-für-Schritt-Anleitung eine Hub-Zentrale hinzufügen, werden Sie aufgefordert, Geräte an der Hub-Zentrale anzumelden. Sie können dies jedoch ablehnen und später zu diesem Schritt zurückkehren.

Hinzufügen eines Gerätes zur Hub-Zentrale in der Ajax App:

> 1. Öffnen Sie den Raum und wählen Sie **Gerät hinzufügen**.
> 2. Benennen Sie das Gerät, scannen Sie den QR-Code (oder geben Sie ihn manuell ein) und wählen Sie eine Gruppe aus (falls der Gruppenmodus aktiviert ist).
> 3. Klicken Sie auf **Hinzufügen** — der Countdown zum Hinzufügen eines Geräts beginnt.
> 4. Folgen Sie den Anweisungen in der App, um das Gerät anzumelden.

Bitte beachten: Für die Anmeldung des Geräts an der Hub-Zentrale muss sich dieses innerhalb der Funkreichweite der Hub-Zentrale befinden (am selben Schutzobjekt).

Einstellungen der Hub-Zentrale

Einstellungen können in der Ajax App geändert werden:

1. Öffnen Sie die Registerkarte **Geräte** .
2. Wählen Sie Hub 2 Plus 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

WLAN — Einstellungen für die WLAN-Internetverbindung. Die allgemeine Liste zeigt alle für die Hub-Zentrale verfügbaren Netzwerke an.

- WLAN — ermöglicht die De-/Aktivierung von WLAN auf der Hub-Zentrale. Mit der Taste [i] werden die Netzwerkeinstellungen geöffnet:
  - 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
  - Dieses Netzwerk vergessen — nach dem Antippen löscht die Hub-Zentrale die Netzwerkeinstellungen und verbindet sich nicht mehr mit dem Netzwerk

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 2 — 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: 30 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	Max Anzahl Geräte
12 s	39 Geräte
24 s	79 Geräte
36 s	119 Geräte
48 s	159 Geräte
72 s	200 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
- WLAN
- 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**, **UMTS/LTE** und **WLAN** 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.
- **WLAN** — ermöglicht die Ereignis- und Alarmübertragung über WLAN.
- **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 2 Plus-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

Zurücksetzen der Hub-Zentrale auf Werkseinstellungen:

1. Schalten Sie die Hub-Zentrale ein, falls sie ausgeschaltet ist.
2. Löschen Sie alle Benutzer und Techniker von der Hub-Zentrale.
3. Halten Sie den Ein/Aus-Taster für 30 Sekunden gedrückt — das Ajax Logo auf der Hub-Zentrale beginnt rot zu blinken.
4. Löschen Sie die Hub-Zentrale aus Ihrem Account.

Das Zurücksetzen der Hub-Zentrale löscht keine verbundenen Benutzer!

Ereignis- und Alarmbenachrichtigungen

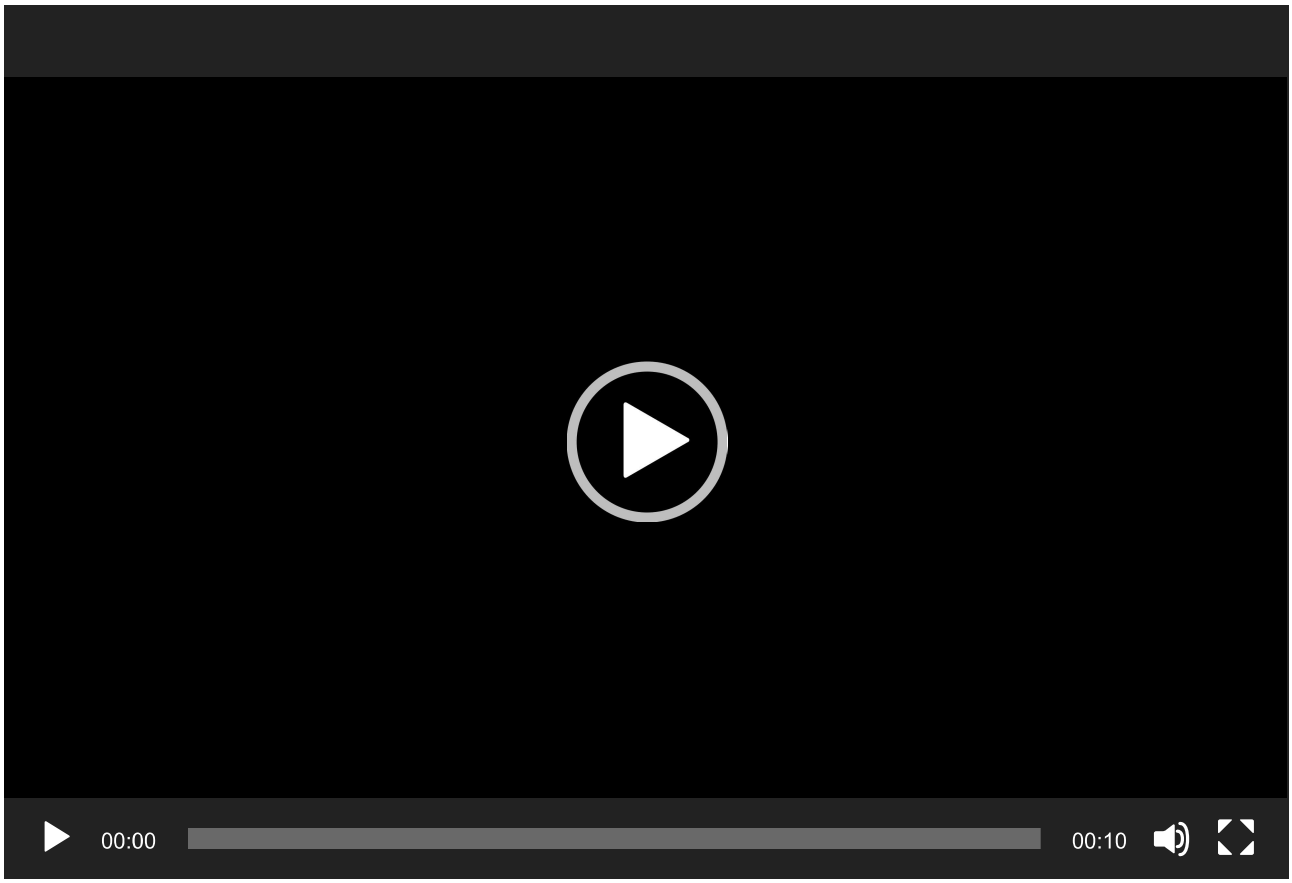
Das Ajax Sicherheitssystem informiert den Benutzer auf drei Arten über Alarme und Ereignisse: Push-Benachrichtigungen, SMS und Telefonanrufe. Die

Benachrichtigungseinstellungen können nur für registrierte Benutzer geändert werden.

Arten von Ereignissen	Zweck	Arten von Benachrichtigungen
Störungen	• Verbindungsverlust zwischen Gerät und Hub-Zentrale • Funkstörung (Jamming) • Niedrige Batterieladung im Gerät oder der Hub-Zentrale • Abdecken • Manipulationsalarm	Push-Benachrichtigungen SMS
Alarm	• Eindringen • Feuer • Überschwemmung • Verbindungsverlust zwischen Hub-Zentrale und Ajax Cloud-Server	Anrufe Push-Benachrichtigungen SMS
Ereignisse	• Aktivierung von **WallSwitch**, **Relay**, **Socket**	Push-Benachrichtigungen SMS
Scharf-/Unscharfschaltung	• Scharf-/Unscharfschaltung ganzer Objekte oder Gruppen • **Nachtmodus** aktivieren	Push-Benachrichtigungen SMS

 So benachrichtigt Ajax die Nutzer über Meldungen

Videoüberwachung



Sie können Kameras von Drittanbietern an das Sicherheitssystem anschließen: Es wurde eine nahtlose Integration mit IP-Kameras und -Videorekordern von Dahua, Hikvision und Safire implementiert. Sie können auch Kameras von Drittanbietern anschließen, die das RTSP-Protokoll unterstützen. Es können bis zu 100 Videoüberwachungsgeräte an das System angeschlossen werden.

☞ **Hinzufügen einer Kamera zum Ajax Sicherheitssystem**

Verbindung zu einem Sicherheitsdienst herstellen

Die Liste der Unternehmen, die das System mit ihrer Überwachungszentrale verbinden, finden Sie im Menü **Sicherheitsunternehmen** (**Geräte** **Hub-Zentrale** **Einstellungen** **Sicherheitsunternehmen**):

Wählen Sie einen Sicherheitsdienst aus und klicken Sie auf **Überwachungsanfrage senden**. Danach wird sich das Sicherheitsunternehmen mit Ihnen in Verbindung setzen und die Bedingungen für die Verbindung mit Ihrer Anlage besprechen. Oder Sie können sich selbst an einen Sicherheitsdienst wenden (Kontaktdaten in der App verfügbar), um eine Verbindung zu vereinbaren.

Die Anbindung an die Überwachungszentrale (CMS) erfolgt über das Contact ID- oder SIA-Protokoll.

Installation

Vergewissern Sie sich vor der Installation der Hub-Zentrale, dass Sie den optimalen Standort gewählt haben und dieser den Anforderungen dieses Handbuchs entspricht! Die Hub-Zentrale sollte nicht direkt sichtbar sein.

Stellen Sie sicher, dass die Kommunikation zwischen Hub-Zentrale und allen angeschlossenen Geräten stabil ist. Bei zu geringer Signalstärke (ein Balken) können wir einen stabilen Betrieb des Sicherheitssystems nicht garantieren. Setzen Sie alle möglichen Maßnahmen zur Verbesserung der Signalqualität um! Zumindest sollte der Hub-Zentrale neu positioniert werden, da bereits eine Verlagerung um 20 cm den Signalempfang erheblich verbessern kann.

Wenn auch nach der Umsetzung die Signalstärke zu niedrig oder unstabil ist, verwenden Sie den **Funk-Repeater ReX**.

Beachten Sie bei der Installation und Nutzung des Geräts 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 unter Spannung stehende Gerät auseinanderzubauen! Betreiben Sie das Gerät nicht an einem beschädigten Netzkabel.

Installation der Hub-Zentrale:

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

Wir raten von der Verwendung doppelseitigen Klebebands für die Installation ab: es kann dazu führen, dass eine Hub-Zentrale bei Stößen herunterfällt.

2. Befestigen Sie die Hub-Zentrale an der Montageplatte. Überprüfen Sie nach der Installation den Manipulationsschutzstatus in der Ajax App und anschließend die Qualität der Plattenbefestigung. Sie erhalten eine Benachrichtigung, wenn versucht wird, die Hub-Zentrale von der Oberfläche oder von der Montageplatte zu entfernen.
3. Befestigen Sie die Hub-Zentrale mit den mitgelieferten Schrauben auf der SmartBracket-Montageplatte.

Achten Sie auf die lagerichtige Anbringung der Hub-Zentrale (z. B. an einer Wand). Bei korrekter Befestigung kann das Ajax Logo horizontal gelesen werden.

Platzieren Sie die Hub-Zentrale nicht an folgenden Orten:

- Im Außenbereich (im Freien).
- In der Nähe oder im Inneren von metallenen Objekten oder Spiegeln, die eine Dämpfung und Abschirmung des Signals verursachen.
- An Orten mit hohem Funkstörpegel.
- In der Nähe von Funkstörquellen: weniger als 1 Meter vom Router und den Stromkabeln entfernt.

- In jedem Raum, in dem Temperatur und Luftfeuchtigkeit außerhalb des zulässigen Bereichs liegen.

Instandhaltung

Überprüfen Sie die Betriebstüchtigkeit 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 von Geräten geeignet ist.

Verwenden Sie für die Reinigung der Hub-Zentrale keine Mittel, die Alkohol, Aceton, Benzin und andere aktive Lösungsmittel enthalten.

 **Batteriewechsel bei der Hub-Zentrale**

Paketinhalt

1. Hub 2 Plus
2. Montageplatte SmartBracket
3. Stromkabel
4. Ethernet-Kabel
5. Montagesatz
6. Starterpaket — nicht in allen Ländern erhältlich
7. Schnellstartanleitung

Technische Daten

Klassifizierung	Sicherheitssystemzentrale mit Unterstützung für Ethernet, WLAN und zwei SIM-Karten
Unterstützung von Meldern mit Fotoverifizierung von Alarmen	Verfügbar
Anzahl angeschlossener Geräte	Bis zu 200
Anzahl angeschlossener ReX	Bis zu 5

Anzahl von Sicherheitsgruppen	Bis zu 25
Anzahl von Benutzern	Bis zu 200
Videoüberwachung	Bis zu 100 Kameras oder DVRs
Anzahl der Räume	Bis zu 50
Anzahl der Szenarien	Bis zu 64 (Reaktionen durch Scharf- und Unscharfschaltung sind nicht im Gesamtfunktionsumfang der Szenarien der Hub-Zentrale enthalten)
Kommunikationsprotokolle der Überwachungszentrale	Contact ID, SIA Die Fotobestätigungen von Alarmen werden an das CMS-System Manitou, ABsistemDC(NG), WBB, Horus und SBN
Stromversorgung	110 V~ bis 240 V~, 50/60 Hz
Eingebauter Akku	Li-Ion 3 A·h (bis zu 15 Stunden Akkulaufzeit bei deaktivierter Ethernet-Verbindung)
Energieaufnahme aus dem Netz	Bis zu 10 W
Manipulationssicher	Verfügbar, Manipulationsalarm
Betriebsfrequenzband	868,0 MHz bis 868,6 MHz oder 868,7 MHz bis 869,2 MHz, je nach Verkaufsregion
HF-Sendeleistung	10,4 mW (Grenzwert 25 mW)
Funkreichweite	Bis zu 2000 m
Kommunikationskanäle	2 SIM-Karten • 2G (GSM900/DCS1800 (B3/B8)) • 3G (WCDMA 850/900/2100 (B1/B5/B8)) • LTE (FDD B1/B3/B5/B7/B8/B20/B28) WLAN (802.11b/g/n) Ethernet
Betriebstemperaturbereich	Von -10°C bis +40°C
Betriebsfeuchtigkeit	Bis zu 75%

Maße	163 × 163 × 36 mm
Gewicht	367 g

Garantie

Die Gewährleistung für die Produkte der „AJAX SYSTEMS MANUFACTURING“ LIMITED LIABILITY COMPANY gilt für 2 Jahre ab Kaufdatum und umfasst nicht den/die im Lieferumfang enthaltenen Akku/s.

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!

☞ **Gewährleistungspflichten**

☞ **Nutzungsvereinbarung**

Technischer Kundendienst: **support@ajax.systems**