

# KeyPad Benutzerhandbuch

Aktualisiert April 23, 2021



**KeyPad** ist eine drahtlose Touch-Tastatur für den Innenbereich zur Verwaltung des Ajax-Sicherheitssystems. Verwendung in Innenräumen. Mit diesem Gerät kann der Benutzer das System scharf- und unscharf- schalten sowie den Systemzustand einsehen. KeyPad ist geschützt gegen Versuche den Paascode zu erraten. Außerdem kann KeyPad einen stillen Alarm auslösen, wenn der Bedrohungscode eingegeben wird.

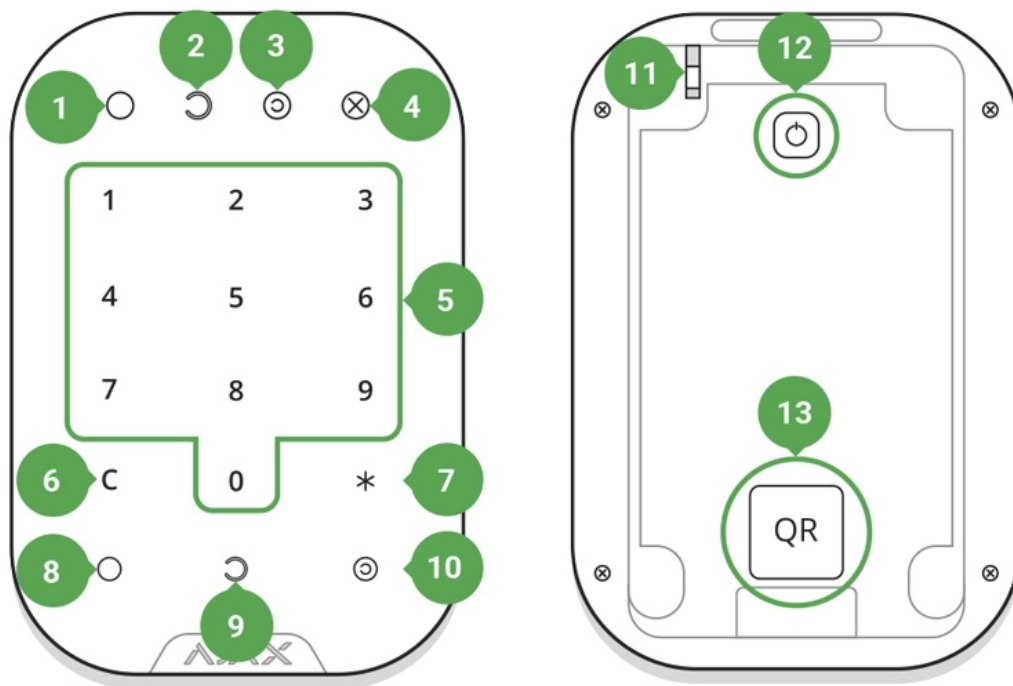
Das KeyPad ist über ein gesichertes Jeweller-Funkprotokoll mit dem Ajax-Sicherheitssystem verbunden und kommuniziert mit der Hub-Zentrale in einer Entfernung von bis zu 1.700 m in Sichtlinie.



KeyPad arbeitet nur mit Ajax-Hub-Zentralen und unterstützt keine Verbindung über ocBridge Plus or uartBridge-Integrationsmodule.

Das Gerät wird über die Ajax-Apps für iOS, Android, macOS und Windows eingerichtet.

# Funktionselemente



1. LED-Anzeige für scharf gestellt
2. LED-Anzeige für unscharf gestellt
3. LED-Anzeige für Nachtmodus
4. LED-Anzeige für Störungen
5. Touch-Oberfläche
6. Taste „Löschen“
7. Taste „Funktion“
8. Taste „Scharfschalten“
9. Taste „Unscharfschalten“
10. Taste „Nachtmodus“
11. Manipulationstaste
12. Taste „Ein-/Ausschalten“
13. QR-Code

Um die SmartBracket-Platte zu entfernen, schieben Sie sie nach unten (ein

# Funktionsprinzip

KeyPad ist ein stationäres Steuergerät für Innenräume. Zu seinen Funktionen gehören das Scharf-/Unscharfschalten des Systems mit einer Zahlenkombination (oder einfach durch Drücken der Taste), die Aktivierung des Nachtmodus, die Anzeige des Sicherheitsmodus, das Sperren, wenn jemand versucht, den Passcode zu erraten sowie das Auslösen eines stillen Alarms, wenn jemand den Benutzer zwingt, das System unscharf zu stellen.

Das KeyPad zeigt den Status der Kommunikation mit der Hub-Zentrale und Systemfehler an. Die Tasten leuchten auf, sobald Sie die Tastatur berühren, sodass Sie den Passcode ohne externe Beleuchtung eingeben können. KeyPad verwendet auch einen Signalton bei der Eingabe.





Um KeyPad zu aktivieren, berühren Sie die Tastatur: die Hintergrundbeleuchtung schaltet sich ein, und der Signalton zeigt an, dass das KeyPad aktiviert ist.

Wenn die Batterie schwach ist, schaltet sich die Hintergrundbeleuchtung unabhängig von den Einstellungen auf einem minimalen Niveau ein.

Wenn Sie die Tastatur 4 Sekunden lang nicht berühren, dimmt KeyPad die Hintergrundbeleuchtung ab, und nach weiteren 12 Sekunden schaltet das Gerät in den Schlafmodus.




Beim Wechsel in den Schlafmodus löscht KeyPad die eingegebenen Befehle!

KeyPad unterstützt Passcodes mit 4-6 Ziffern. Der eingegebene Passcode wird nach dem Drücken der Schaltfläche an die Hub-Zentrale gesendet:  (Scharfschalten),  (Unscharfschalten) oder  (Nachtmodus). Falsche Befehle können mit der  -Taste (Reset) zurückgesetzt werden.

Wenn innerhalb von 30 Minuten dreimal ein falscher Passcode eingegeben wird, wird das KeyPad für die vom Administrator-Benutzer voreingestellte Zeit gesperrt. Sobald KeyPad gesperrt ist, ignoriert die Hub-Zentrale alle Befehle und benachrichtigt gleichzeitig die Benutzer des Sicherheitssystems über den

automatisch entsperrt.


KeyPad ermöglicht die Scharfschaltung des Systems ohne Passcode: durch Drücken der Taste  (Scharfschalten). Diese Funktion ist standardmäßig deaktiviert.

Wenn die Funktionstaste (\*) gedrückt wird, ohne den Passcode einzugeben, führt die Hub-Zentrale den dieser Taste in der App zugeordneten Befehl aus.

KeyPad kann ein Wachschutzunternehmen bei der Bedrohungscodeeingabe benachrichtigen. Der **Bedrohungscode** aktiviert – im Gegensatz zur Paniktaste – keine Sirenen. KeyPad und die App melden die erfolgreiche Unscharfschaltung des Systems, aber der Wachschutzunternehmen erhält einen Alarm.

## Anzeige

Wenn Sie KeyPad berühren, wacht es auf, wobei die Tastatur beleuchtet und der Sicherheitsmodus angezeigt wird: Scharfgeschaltet, Unscharfgeschaltet oder Nachtmodus. Der Sicherheitsmodus ist immer aktuell, unabhängig von dem Steuergerät, mit dem er geändert wurde (Funkfernbedienung oder App).

Ereignis	Anzeige
Störungsanzeige  blinkt	Die Anzeige signalisiert den Kommunikationsverlust mit der Hub-Zentrale oder das Öffnen der Tastenfeldabdeckung
Taste der Tastatur gedrückt	Ein kurzer Piepton, die LED-Anzeige für den aktuellen Scharfschaltungsstatus blinkt einmal auf
Das System ist scharfgeschaltet	Kurzes Tonsignal, LED-Anzeige für Scharfschalten/Nachtmodus leuchtet
Das System ist unscharf geschaltet	Zwei kurze Tonsignale, die LED-Anzeige leuchtet für unscharf geschaltet
Falscher Passcode	Langes Tonsignal, die Hintergrundbeleuchtung der Tastatur blinkt 3 Mal
Eine Störung wird beim Scharfschalten erkannt (z. B. wenn die Verbindung mit dem Melder verloren wurde)	Ein langer Piepton, die LED-Anzeige für den aktuellen Scharfschaltungsstatus des Systems blinkt dreimal auf

Passcode zu erraten, gesperrt	blinken gleichzeitig
Schwache Batterie	<p>Nach dem Scharf-/Unscharfschalten des Systems blinkt die Störungsanzeige sanft. Die Tastatur ist gesperrt, während die Anzeige blinkt.</p> <p>Wenn KeyPad mit schwachen Batterien aktiviert wird, ertönt ein langer Signalton, die Störungsanzeige leuchtet sanft auf und schaltet sich dann aus</p>

## Verbindung

### Bevor Sie das Gerät anschließen:

1. Schalten Sie die Hub-Zentrale ein und überprüfen Sie seine Internetverbindung (das Logo leuchtet weiß oder grün).
2. Installieren Sie die [Ajax-Anwendung](#). Erstellen Sie das Konto, fügen Sie die Hub-Zentrale zur App hinzu und erstellen Sie mindestens einen Raum.
3. Stellen Sie sicher, dass die Hub-Zentrale deaktiviert ist und nicht aktualisiert wird, indem Sie den Status in der Ajax-App überprüfen.



Nur Benutzer mit Administratorrechten können der App ein Gerät hinzufügen

### Wie Sie KeyPad an die Hub-Zentrale anschließen:

1. Wählen Sie die Option **Gerät hinzufügen** in der Ajax-App.
2. Benennen Sie das Gerät, scannen/schreiben Sie manuell den **QR-Code** (befindet sich auf dem Körper und der Verpackung) und wählen Sie den Aufstellungsraum aus.
3. Wählen Sie **Hinzufügen** — der Countdown beginnt.

innerhalb der Abdeckung des drahtlosen Netzwerks der Hub-Zentrale befinden (am gleichen geschützten Objekt).

Eine Anfrage für eine Verbindung zur Hub-Zentrale wird im Moment des Einschaltens des Geräts für eine kurze Zeit übertragen.

Wenn KeyPad nicht an die Hub-Zentrale angeschlossen werden konnte, schalten Sie es für 5 Sekunden aus und versuchen Sie es erneut.

Das angeschlossene Gerät wird in der Geräteliste der App angezeigt. Die Aktualisierung der Gerätestatus in der Liste hängt vom Melder-Ping-Intervall in den Hub-Zentrale-Einstellungen ab (der Standardwert beträgt 36 Sekunden).



KeyPad hat keine voreingestellten Passcodes. Bevor Sie die Tastatur nutzen, stellen Sie sicher, dass die erforderlichen Passcodes erstellt wurden: allgemeine, persönliche und Bedrohungscode.

## Auswählen des standorts

Der Standort des Geräts hängt von seiner Entfernung zur Hub-Zentrale und von Hindernissen ab, die die Übertragung des Funksignals behindern: Wände, Böden, große Gegenstände im Raum.



Gerät ist nur für die Innenraummontage vorgesehen.

### Installieren Sie KeyPad nicht:




1. In der Nähe der Funkübertragungsausrüstung, einschließlich derer, die in 2G/3G/4G-Mobilfunknetzen arbeitet, Wi-Fi-Router, Transceiver, Funkstationen sowie einer Ajax-Hub-Zentrale (verwendet ein GSM-Netz).
2. In der Nähe von elektrischen Leitungen.

außerhalb des zulässigen Bereichs liegen.

6. Näher als 1 m von der Hub-Zentrale entfernt.



Prüfen Sie die Jeweller-Signalstärke am Installationsort

Während des Tests wird der Signalpegel in der App und auf der Tastatur mit den LED-Anzeigen  (scharf gestellt),  (unscharf gestellt),  (Nachtmodus) und der LED-Anzeige **X** für Störungen angezeigt.

Wenn der Signalpegel niedrig ist (ein Balken), können wir den stabilen Betrieb des Geräts nicht garantieren. Ergreifen Sie alle möglichen Maßnahmen zur Verbesserung der Signalqualität. Bewegen Sie zumindest das Gerät: Schon eine Verschiebung um 20 cm kann die Qualität des Signalempfangs deutlich verbessern.

Wenn das Gerät auch nach einer Bewegung eine geringe oder instabile Signalstärke hat, verwenden Sie einen [ReX Funk-Repeater](#).

KeyPad ist für den Betrieb bei Befestigung an der vertikalen Oberfläche vorgesehen. Wenn Sie bei der Benutzung KeyPad in den Händen halten, können wir nicht garantieren, dass die Sensortastatur erfolgreich funktioniert.

Status



1. Geräte 

2. KeyPad

Parameter	Wert
Temperatur	Temperatur des Gerätes. Gemessen am Prozessor, und ändert sich allmählich

Akku-Ladung	<div> <div>zwei Zustände.</div> <ul style="list-style-type: none"> <li>• OK</li> <li>• Batterieladung niedrig</li> </ul> </div> <div> <b>Anzeige der Batterieladung in Ajax-Apps</b> </div>
Gehäusedeckel	Der Manipulationsmodus des Geräts, der auf Ablösung oder Beschädigung des Gehäuses reagiert
ReX	Zeigt den Status der Verwendung des ReX Funk-Repeater
Vorübergehende Deaktivierung	Zeigt den Status des Geräts an: aktiv, vom Benutzer vollständig deaktiviert, oder nur Benachrichtigungen über das Auslösen der Manipulationsschutz Taste des Geräts deaktiviert
Firmware	Firmware-Version des Melders
Geräte-ID	Geräteerkennung

## Einstellungen

1. Geräte 
2. KeyPad
3. Einstellungen 

Einstellung	Wert
Erstes Feld	Gerätename, kann bearbeitet werden
Raum	Auswählen des virtuellen Raums, dem das Gerät zugewiesen wird
Berechtigung Scharf-/Unscharschaltung	Auswählen der Sicherheitsgruppe, der KeyPad




Passcode	Setzen eines Passcode für das Scharf-/Unscharfschalten
Bedrohungscode	Einstellen eines <u>Nötigungscode</u> s für <u>stillen Alarm</u>
Funktionstaste	<p>Funktionswahl der Taste *</p> <ul style="list-style-type: none"> <li>● <b>AUS</b> – Die Funktionstaste ist deaktiviert und führt beim Betätigen keine Befehle aus</li> <li>● <b>Alarm</b> – das System sendet einen Alarm an die Leitstelle und alle Benutzer, wenn die Funktionstaste gedrückt wird</li> <li>● <b>Gekoppelten Feuersalarm stummschalten</b> – bei Betätigung, wird der Brandalarm der FireProtect/FireProtect Plus Melder stummgeschaltet. Die Option funktioniert nur, wenn der gekoppelte Rauchmelder Alarm aktiviert ist</li> </ul> <p><u>Erfahren Sie mehr</u></p>
Scharfschalten ohne Passcode	Wenn das System aktiv ist, kann es durch Drücken der Taste „Scharfschalten“ ohne Passcode scharf geschaltet werden
Auto-Sperre nach falschen Passwort Eingaben	Wenn die Funktion aktiv ist, wird die Tastatur nach dreimaliger Falscheingabe des Passwortes in Folge (innerhalb von 30 Minuten) für die voreingestellte Zeit gesperrt. Während dieser Zeit kann das System nicht über KeyPad unscharf geschaltet werden
Zeit Auto-Sperre (min)	Sperrzeit nach mehrmaliger Eingabe des falschen Passcodes
Helligkeit	Helligkeit der Tastatur-Hintergrundbeleuchtung
Lautstärke	Lautstärke des Signaltons
	Diese Einstellung erscheint dann, wenn für die

Dämpfungsprüfung	Schaltet die Tastatur in den Signalabschwächungs-Testmodus (verfügbar bei Geräten mit <b>Firmware-Version 3.50 und höher</b> )
Vorübergehende Deaktivierung	<p>Erlaubt dem Benutzer, das Gerät zu trennen, ohne es ganz aus dem System zu entfernen.</p> <p>Es stehen zwei Optionen zur Verfügung:</p> <ul style="list-style-type: none"> <li>● <b>Vollständig</b> – das Gerät führt keine Systembefehle aus, kann nicht über Automatisierungsszenarien angesteuert werden und das System ignoriert Alarme und andere Benachrichtigungen dieses Geräts</li> <li>● <b>Nur Deckel</b> – das System ignoriert nur Benachrichtigungen über das Auslösen der Manipulationsschutz Taste (Abnehmen des Gerätedeckels)</li> </ul> <p><b><u>Mehr über vorübergehende Deaktivierung erfahren</u></b></p>
Benutzerhandbuch	Öffnet das Benutzerhandbuch der Tastatur
Gerät entkoppeln	Trennt das Gerät von der Hub-Zentrale und löscht seine Einstellungen

KeyPad ermöglicht es, sowohl allgemeine als auch persönliche Passcodes für jeden Benutzer festzulegen.

### So installieren Sie einen persönlichen Passcode:

1. Gehen Sie zu den Profileinstellungen (**Hub-Zentrale** → **Einstellungen**  → **Benutzer** → **Ihre Profileinstellungen**)
2. Klicken Sie auf **Zugangscodes-Einstellungen** (in diesem Menü können Sie auch die


# Passcodebasierte Sicherheitsverwaltung

Sie können die Sicherheit eines ganzen Objekts oder einzelner Gruppen mit gemeinsamen oder persönlichen Passcodes (in der App einstellbar) verwalten.




Sollte ein persönlicher Passcode verwendet werden, wird der Name des Benutzers, der das System unscharf oder scharf geschaltet hat, in den Hub-Ereignissen und in den Benachrichtigungen angezeigt. Sollte ein gemeinsamer Passcode verwendet werden, wird der Name des Benutzers, der den Sicherheitszustand geändert hat, nicht angezeigt.


## Sicherheitsverwaltung eines ganzen Objekts mit gemeinsamen Passcode

Geben Sie einen **gemeinsamen Passcode** ein und berühren Sie die Taste: **Scharfschalten**  / **Unscharfschalten**  / **Nachtmodus** .

Beispiel: 1234 → 

## Sicherheitsverwaltung einzelner Gruppen mit gemeinsamen Passcode

Geben Sie einen **gemeinsamen Passcode** ein, drücken Sie **\***, geben Sie eine **Gruppen-ID** ein und berühren Sie die Taste: **Scharfschalten**  / **Unscharfschalten**  / **Nachtmodus** .

Beispiel: 1234 → \* → 2 → 




### Was ist eine Gruppen-ID?


Sollte eine bestimmte Gruppe dem KeyPad zugeordnet sein (das Feld

Passcode verwalten (sofern der Benutzer die entsprechenden Rechte hat).

## Benutzerrechte im Ajax Sicherheitssystem




### Sicherheitsverwaltung eines ganzen Objekts mit gemeinsamen Passcode


Geben Sie Ihre **Benutzer-ID** ein, drücken Sie **\***, geben Sie Ihren **persönlichen Passcode** ein und berühren Sie die Taste: **Scharfschalten**  / **Unscharfschalten**  / **Nachtmodus** .

Beispiel: 2 → **\*** → 1234 → 

#### Was ist eine Benutzer-ID?

### Sicherheitsverwaltung einzelner Gruppe mit persönlichen Passcode

Geben Sie die **Benutzer-ID** ein, drücken Sie **\***, geben Sie Ihren **persönlichen Passcode** ein, drücken Sie **\***, geben Sie die **Gruppen-ID** ein und berühren Sie die Taste: **Scharfschalten**  / **Unscharfschalten**  / **Nachtmodus** .

Beispiel: 2 → **\*** → 1234 → **\*** → 5 → 

#### Was ist eine Gruppen-ID?

#### Was ist eine Benutzer-ID?

Sollte eine bestimmte Gruppe dem KeyPad zugeordnet sein (das Feld „**Berechtigung Scharf- / Unscharfschalten**“ in den KeyPadeinstellungen)

**persönlichen**, als auch **gemeinsamen** Bedrohungscode verwenden.


## Was ist ein Bedrohungscode und wie benutze ich diesen?




Szenarien und Sirenen reagieren auf Unscharfschaltung unter Bedrohung genauso, wie auf normale Unscharfschaltungen.


### **Für die Verwendung eines Bedrohungscode:**

Geben Sie den **Bedrohungscode** ein und drücken Sie die Taste **Unscharfschaltung** .

Beispiel: 4321 → 

### **Für die Verwendung eines persönlichen Bedrohungscode:**

Geben Sie die **Benutzer-ID** ein, drücken Sie **\***, geben Sie dann Ihren **persönlichen Bedrohungscode** ein und drücken Sie die Taste **Unscharfschalten** .

Beispiel: 2 → **\*** → 4422 → 

## **Wie funktioniert die Stummschaltung des Feuersalarms?**

Das KeyPad ermöglicht das Stummschalten von gekoppelten Rauchmelder Alarmen durch Betätigung der Funktionstaste (wenn die entsprechende Einstellung ausgewählt wurde). Die Resonanz auf die Betätigung des Buttons hängt von den gewählten Einstellungen des Systems ab:

## Funktionsprüfung

Das Ajax-Sicherheitssystem ermöglicht die Durchführung von Tests zur Überprüfung der Funktionalität angeschlossener Geräte.

Die Tests beginnen nicht sofort, sondern innerhalb von 36 Sekunden bei Verwendung der Standardeinstellungen. Der Start der Testzeit hängt von den Einstellungen der Abtastperiode des Melders ab (der Absatz zu **Jeweller**-Einstellungen in den Hub-Zentrale-Einstellungen).

### Jeweller-Signalstärketest

### Dämpfungsprüfung

## Installation



Stellen Sie vor der Installation des Melders sicher, dass Sie den optimalen Standort ausgewählt haben und die in diesem Handbuch enthaltenen Richtlinien einhalten!



Die Tastatur sollte an der vertikalen Fläche angebracht werden.

1. Befestigen Sie die SmartBracket-Platte mit Hilfe von mitgelieferten

2. Legen Sie KeyPad auf die Befestigungsplatte und ziehen Sie die Befestigungsschraube an der Gehäuseunterseite an.

Sobald das Tastenfeld in SmartBracket befestigt ist, blinkt es mit der Störungsanzeige **X** und signalisiert damit, dass der Manipulationsschutz betätigt wurde.

Wenn die Störungsanzeige **X** nach der Installation in SmartBracket nicht blinkt, überprüfen Sie den Status des Manipulationsschutzes in der Ajax-App und dann die Befestigungsdichte der Platte.

Wenn KeyPad von der Oberfläche abgerissen oder von der Befestigungsplatte entfernt wird, erhalten Sie die Benachrichtigung.

## Wartung von KeyPad und Batteriewechsel

Überprüfen Sie die Funktionsfähigkeit von KeyPad regelmäßig.

Die in der Tastatur installierte Batterie gewährleistet einen autonomen Betrieb von bis zu 2 Jahren (bei einer Abfragehäufigkeit durch die Hub-Zentrale von 3 Minuten). Wenn die Batterie von KeyPad schwach ist, sendet das Sicherheitssystem die entsprechenden Hinweise, und die Störungsanzeige leuchtet sanft auf und erlischt nach jeder erfolgreichen Eingabe des Passwortes.

### Wie lange funktionieren Batterien in Ajax-Geräten und was beeinflusst deren Lebensdauer

#### Batteriewechsel

# Technische Daten

Sensortyp	Kapazitiv
Anti-Manipulationsschalter	Ja
Schutz gegen das Raten von Passwörtern	Ja
Frequenzband	868,0– 868,6 MHz oder 868,7– 869,2 MHz je nach Verkaufsregion
Kompatibilität	Funktioniert nur mit Ajax <u>hubs</u> und <u>Funk-Repeater</u>
Maximale HF-Ausgangsleistung	Bis zu 20 mW
Modulation des Funksignals	GFSK
Funkreichweite	Bis zu 1.700 m (wenn keine Hindernisse vorhanden sind)
Netzteil	4 × AAA-Batterien
Versorgungsspannung	3 V (Batterien sind paarweise installiert)
Lebensdauer der Batterie	Bis zu 2 Jahre
Installationsmethode	In Innenräumen
Betriebstemperaturbereich	Von -10°C bis +40°C
Betriebsfeuchtigkeit	Bis zu 75%
Gesamtabmessungen	150 × 103 × 14 mm
Gewicht	197 g
Lebensdauer	10 Jahre



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**