Mehr erfahren

- Alarme;
- Änderungen des Sicherheitsmodus;
- Ein-/Ausgangsverzögerungen;
- Auslösung der Öffnungsmelder;
- Störungen.

Für jeden Betriebsmodus kann eine der folgenden drei Funktionen eingestellt werden:

- **Scharf-/Unscharfschalten**. Mit dieser Funktion kann der Benutzer das gesamte Objekt oder bestimmte Gruppen scharf/unscharf schalten oder den **Nachtmodus** aktivieren.
- **Automatisierungsgeräte steuern**. Mit dieser Funktion kann der Benutzer ein Szenario mit einem oder mehreren Automatisierungsgeräten erstellen, die direkt über das Bedienteil gesteuert werden können.
- **Eingangsverzögerung aktivieren**. Mit dieser Funktion können Benutzer KeyPad Outdoor Jeweller als **Bypass-Bedienteil** verwenden, um eine Eingangsverzögerung zu aktivieren, damit sie die Anlage über das Hauptbedienteil unscharf schalten können.

> ⚠ Es kann jeweils nur eine primäre und eine sekundäre Funktion eingestellt werden.

KeyPad Outdoor Jeweller zeigt mit LEDs an, welcher Modus gerade aktiv ist, je nach konfigurierter Funktion:

- **Scharf-/Unscharfschalten**: Das Ajax Logo leuchtet rot oder grün, je nach Sicherheitszustand des Systems. Die **OK**-Taste leuchtet weiß, genau wie der Ziffernblock.
- **Automatisierungsgeräte steuern**: Die **OK**-Taste leuchtet je nach Zustand des Automatisierungsgeräts rot oder grün. Die Ajax Logo-LED ist aus. Wenn das Bedienteil ein Szenario mit mehreren Automationsgeräten steuert, ist der Zustand des Szenarios auf dem Bedienteil nicht verfügbar.
- **Eingangsverzögerung aktivieren**: Das Ajax Logo leuchtet rot auf, wenn das Objekt aktiviert ist, und blinkt gleichzeitig mit dem Piepton rot, wenn die Eingangsverzögerung gestartet wird. Die **OK**-Taste leuchtet weiß, genau wie der Ziffernblock.

Mehr erfahren

Sicherheitskontrolle

KeyPad Outdoor Jeweller ermöglicht das Scharf- und Unscharfschalten des gesamten Objekts oder bestimmter Gruppen sowie die Aktivierung des **Nachtmodus**. Benutzer können die Sicherheit über KeyPad Outdoor Jeweller kontrollieren:

1. **Karten oder Handsender**. KeyPad Outdoor Jeweller nutzt die DESFire®-Technologie, um Benutzer schnell und sicher zu identifizieren. DESFire® basiert auf dem internationalen Standard ISO 14443 und bietet 128-Bit-Verschlüsselung sowie Kopierschutz. Tag und Pass unterstützen diese Technologie und sind mit KeyPad Outdoor Jeweller kompatibel.
2. **Smartphones**. Mit installierter App Ajax Security System und Unterstützung für Bluetooth Low Energy (BLE). Smartphones können anstelle von Tag oder Pass für die Benutzerautorisierung verwendet werden. BLE ist ein Funkprotokoll mit geringem Stromverbrauch. Das Bedienteil unterstützt Android- und iOS-Smartphones mit BLE 4.2 und höher.
3. **Codes**. KeyPad Outdoor Jeweller unterstützt allgemeine Codes, persönliche Codes und Codes für nicht registrierte Benutzer.

Zugangscodes

- **Bedienteil-Code** ist ein allgemeiner Code für das Bedienteil. Wenn diese Option verwendet wird, werden alle Ereignisse im Namen des Bedienteils an Ajax Apps gesendet.
- **Benutzercode** ist ein persönlicher Code, der für die an die Hub-Zentrale angeschlossenen Benutzer eingerichtet wird. Wenn diese Option verwendet wird, werden alle Ereignisse im Namen des Benutzers an Ajax Apps gesendet.
- **Bedienteil-Zugangscode** ist ein Code, der für eine Person eingerichtet wird, die nicht im System registriert ist. Wenn diese Option verwendet

wird, werden Ereignisse an Ajax Apps mit einem mit diesem Code verbundenen Namen gesendet.

- Der **Einsatzteam-Code** ist ein Zugangscode für das Einsatzteam, der nach dem Alarm aktiviert wird und für einen bestimmten Zeitraum gilt. Wenn der Code aktiviert und verwendet wird, werden Ereignisse an die Ajax App mit einem mit dem Code verknüpften Titel gesendet.

> Die Anzahl der persönlichen Codes, der Bedienteil-Codes und der Einsatzteam-Codes hängt vom Modell der Hub-Zentrale ab.
>
> Gerätekompatibilität prüfen

Zugriffsrechte und Codes können in Ajax Apps geändert werden. Wenn der Code kompromittiert ist, kann er per Fernzugriff geändert werden, sodass kein Installateur vor Ort sein muss. Wenn ein Benutzer seinen Pass, Tag oder sein Smartphone verliert, kann ein Administrator oder ein PRO-Benutzer mit Systemkonfigurationsrechten das Gerät in der App sofort sperren. In der Zwischenzeit kann ein Benutzer einen persönlichen Code verwenden, um das System zu steuern.

Sicherheitskontrolle der Gruppen

KeyPad Outdoor Jeweller ermöglicht die Sicherheitskontrolle von Gruppen (wenn der **Gruppenmodus** aktiviert ist). Ein Administrator oder PRO-Benutzer mit Systemkonfigurationsrechten kann auch die **Einstellungen** für das Bedienteil anpassen, um festzulegen, welche Gruppen gemeinsam genutzt werden (Bedienteilgruppen). Weitere Informationen zur Sicherheitskontrolle der Gruppen finden Sie in diesem **Abschnitt**.

Funktionstaste

KeyPad Outdoor Jeweller verfügt über eine **Funktionstaste** (*), die in einem von drei Modi arbeitet:

- **Keine** — die **Funktionstaste** ist deaktiviert, und es passiert nichts, wenn der Benutzer diese Taste kurz drückt.
- **Panik**: Wenn die **Funktionstaste** gedrückt wird, sendet das System einen Alarm an die Leitstelle des Überwachungsunternehmens und an alle Benutzer.
- **Feueralarm stummschalten**: Wenn die **Funktionstaste** gedrückt wird, schaltet das System ausgelöste Ajax Brandmelder stumm. Nur verfügbar, wenn die Funktion **Alarm vernetzter Brandmelder** aktiviert ist (Hub-Zentrale → Einstellungen ⚙ → Service → Brandmelder-Einstellungen).

Außerdem können falsch eingegebene Codes mit einem langen Drücken auf die **Funktionstaste** gelöscht werden, wenn keine andere Aktion für ein langes Drücken eingerichtet ist.

Bedrohungscode

KeyPad Outdoor Jeweller unterstützt einen **Bedrohungscode**, mit dem der Benutzer eine Alarmdeaktivierung simulieren kann. In diesem Fall werden weder die **Ajax App** noch die in der Einrichtung installierten **Sirenen** Ihre Aktivität aufdecken. Dennoch werden das Sicherheitsunternehmen und andere Nutzer des Sicherheitssystems über den Vorfall informiert.

Mehr erfahren

Eingangsverzögerung aktivieren (Bypass-Bedienteil)

Die Funktion **Eingangsverzögerung** aktivieren (d. h. ein Bypass-Bedienteil) dient dazu, eine Eingangsverzögerung zu aktivieren, bevor das System über das Hauptbedienteil unscharf geschaltet wird.

Die Bypass-Technologie ermöglicht die vorübergehende Deaktivierung von Sicherheitsmeldern, wie z. B. **Öffnungsmeldern** und anderen. Dies ermöglicht es den Benutzern, mehr Zeit zu gewinnen, von dem Moment an, in dem sie einen Bereich betreten, bis sie das Gelände mit dem

Hauptsteuergerät (z. B. **KeyPad TouchScreen Jeweller**) unscharf schalten können.

Mehr erfahren

Auto-Sperre beim unbefugten Zugriff

Wenn innerhalb einer Minute dreimal hintereinander ein falscher Code oder ein nicht verifizierter Transponder verwendet wird, wird das Bedienteil für die in den **Einstellungen** festgelegte Zeit gesperrt. Während dieser Zeit ignoriert die Hub-Zentrale alle Codes und Transponder und informiert die Benutzer des Sicherheitssystems über den unberechtigten Zutrittsversuch.

Ein PRO oder ein Benutzer mit Systemkonfigurationsrechten kann das Bedienteil über die App entsperren, bevor die angegebene Sperrzeit abläuft.

Zweistufige Scharfschaltung

KeyPad Outdoor Jeweller kann für die zweistufige Scharfschaltung verwendet werden, jedoch nicht als Gerät der zweiten Stufe. Die zweistufige Scharfschaltung mit Tag, Pass oder Smartphone funktioniert ähnlich wie die Eingabe eines persönlichen oder allgemeinen Codes am Bedienteil.

Mehr erfahren

Verwaltung von Automatisierungsgeräten und Szenarien

KeyPad Outdoor Jeweller verfügt über die Funktion **Automatisierungsgeräte steuern**, mit der ein oder mehrere Automatisierungsgeräte gesteuert werden können. So kann ein Benutzer beispielsweise Garagentore öffnen oder alle intelligenten Lichtschalter am Standort ausschalten.

Wenn das Bedienteil ein Automatisierungsgerät steuert, zeigt es den Status des Geräts mit der LED-Anzeige der **OK**-Tatste an. Wenn die **OK**-Taste grün leuchtet, ist ein Automatisierungsgerät aktiv; wenn sie rot leuchtet, ist ein Automatisierungsgerät inaktiv.

Wenn das Bedienteil ein Szenario mit mehreren Automatisierungsgeräten steuert, kann das Bedienteil nicht den Status des Geräts oder des Szenarios anzeigen. Stattdessen zeigt es an, ob die eingestellte Aktion abgeschlossen ist oder nicht.

> KeyPad Outdoor Jeweller kann nur ein Szenario verwalten.

Die Verwaltung von Automatisierungsgeräten ist nur nach Autorisierung über das Bedienteil möglich.

Anzeige des Sicherheitsmodus und des Zustands der Automatisierungsgeräte

KeyPad Outdoor Jeweller informiert den Benutzer über den Sicherheitsmodus des Systems und den Zustand der Automatisierungsgeräte durch:

- das Logo mit LED-Anzeige;
- die **OK**-Taste mit LED-Anzeige;
- akustische Anzeige.

Wenn sich das Bedienteil im Modus **Scharf-/Unscharfschalten** befindet, leuchtet das Ajax Logo grün oder rot, um den Zustand des Sicherheitsmodus des Systems anzuzeigen.

Wenn sich das Bedienteil im Modus **Automationsgeräte steuern** befindet, leuchtet die **OK**-Taste grün oder rot, um den Zustand des Automatisierungsgeräts anzuzeigen. Wenn das Bedienteil jedoch ein

Szenario mit mehreren Automatisierungsgeräten verwaltet, kann es den Zustand des Szenarios nicht anzeigen.

Der eingebaute Summer meldet Alarme, Türöffnungen sowie Ein-/Ausgangsverzögerungen.

Weitere Informationen finden Sie im Abschnitt **LED-Beleuchtung**.

Stummschaltung des Feueralarms

KeyPad Outdoor Jeweller kann vernetzte Brandmelder durch Drücken der **Funktionstaste** stumm schalten (wenn die erforderliche Einstellung aktiviert ist). Die Reaktion des Systems auf das Drücken der Taste hängt von den Einstellungen und dem Systemzustand ab:

- **Alarm vernetzter Brandmelder hat sich bereits ausgebreitet** – beim ersten Tastendruck werden alle Sirenen aller Brandmelder außer denen, die den Alarm registriert haben, stumm geschaltet. Die übrigen Melder können durch erneutes Drücken der Taste stummgeschaltet werden.
- **Die Auslöseverzögerung für vernetzte Brandmelder läuft** — durch Drücken der **Funktionstaste** werden die Sirenen der ausgelösten Brandmelder stumm geschaltet.

Beachten Sie, dass diese Option nur verfügbar ist, wenn der **Alarm vernetzter Brandmelder** aktiviert ist.

Mehr erfahren

Datenübertragungsprotokolle Jeweller

Jeweller ist ein Funk-Datenübertragungsprotokoll, das eine schnelle und zuverlässige Zwei-Wege-Kommunikation zwischen Hub-Zentralen und Geräten ermöglicht. Das Gerät verwendet **Jeweller**, um Befehle, Alarme und Ereignisse zu übertragen.

Mehr erfahren

Übermittlung von Ereignissen an die Leitstelle

Das Ajax System kann Alarme über **SurGard (Contact ID), SIA (DC-09), ADEMCO 685** und andere Protokolle an die Überwachungs-App Ajax PRO Desktop sowie an eine Notruf- und Serviceleitstelle (NSL) übertragen.

KeyPad Outdoor Jeweller kann folgende Ereignisse übertragen:

1. Scharf-/Unscharfschalten des Systems.
2. Eingabe des Bedrohungscodes.
3. Betätigung der Paniktaste.
4. Sperrung des Bedienteils nach einem unbefugten Zugriffsversuch.
5. Erfolgloser Versuch, das Sicherheitssystem scharf zu schalten (bei aktivierter Systemintegritätsprüfung).
6. Sabotagealarm. Wiederherstellung des Sabotagekontakts.
7. Verlust/Wiederherstellung der Verbindung zur Hub-Zentrale.
8. Dauerhafte Deaktivierung/Aktivierung des Geräts.
9. Einmalige Deaktivierung/Aktivierung des Geräts.

Sobald ein Alarm eingeht, weiß der Betreiber in der Leitstelle des Sicherheitsunternehmens, was passiert ist und wohin er das Einsatzteam schicken muss. Die Adressierbarkeit der Ajax Geräte ermöglicht das Senden von Ereignissen an **Ajax PRO Desktop** oder die NSL unter Angabe des Gerätetyps, seines Namens, seiner Sicherheitsgruppe und seines virtuellen Raums. Die Liste der zu übertragenden Informationen kann je nach NSL-Typ und dem gewählten Kommunikationsprotokoll variieren.

> Die Geräte-ID und die Nummer der Schleife (Zone) finden Sie in den Gerätezuständen.

Auswahl des Installationsortes

Bei der Wahl des Installationsortes für KeyPad Outdoor Jeweller sind die Parameter zu berücksichtigen, die seinen Betrieb beeinflussen:

- **Jeweller Signalstärke**

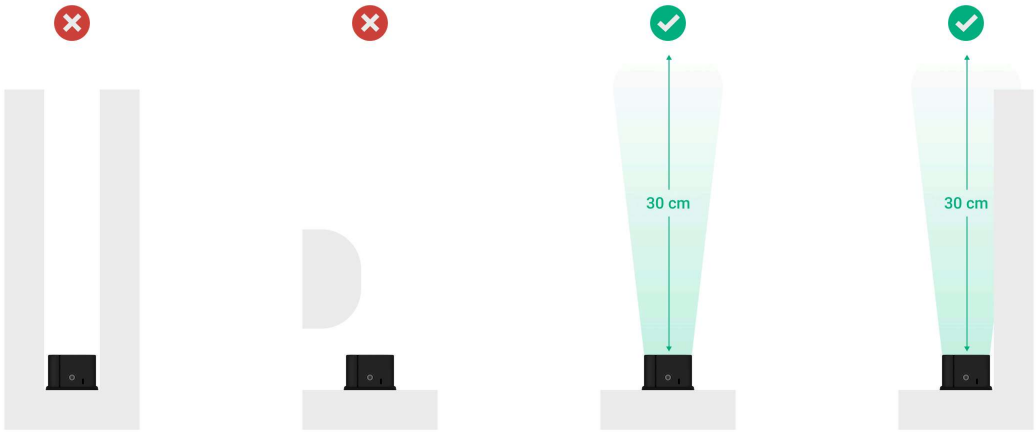
Berücksichtigen Sie die Empfehlungen für die Platzierung bei der Entwicklung eines Projekts für das System der Einrichtung. Das Ajax System muss von Fachleuten geplant und installiert werden. Eine Liste der empfohlenen Partner finden **Sie hier**.

KeyPad Outdoor Jeweller wird vorzugsweise im Außen- oder Innenbereich in der Nähe des Eingangs angebracht. Dadurch kann der Benutzer das System vor dem Betreten des Objekts oder bis zum Ablauf der Eingangsverzögerung deaktivieren. Die Benutzer können den Standort auch beim Verlassen des Objekts schnell aktivieren.

KeyPad Outdoor Jeweller verfügt über ein geschütztes Gehäuse, sodass das Bedienteil an öffentlichen Orten wie Restaurants, Krankenhäusern, Büros oder in Produktionsstätten unter schwierigen Bedingungen installiert werden kann.

Die empfohlene Montagehöhe beträgt 1,3–1,5 m über dem Boden. Installieren Sie das Bedienteil auf einer flachen, vertikalen Oberfläche. Dies stellt sicher, dass KeyPad Outdoor Jeweller sicher an der Oberfläche befestigt ist und hilft, falsche Sabotagealarme zu vermeiden.

Das Bedienteil soll am Installationsort nicht von zwei Wänden auf beiden Seiten umschlossen sein und auch nicht von etwas davor blockiert werden. Für den ordnungsgemäßen Betrieb des Karten-/Handsender-/Bluetooth-Lesers muss ein freier Bereich von 30 cm vor dem Bedienteil vorhanden sein.



Signalstärke

Die Signalstärke wird durch die Anzahl der nicht zugestellten oder beschädigten Datenpakete in einem bestimmten Zeitraum bestimmt. Das Symbol ıı| auf der Registerkarte **Geräte** in Ajax Apps zeigt die Signalstärke an:

- **drei Balken** – ausgezeichnete Signalstärke;
- **zwei Balken** – gute Signalstärke;
- **ein Balken –** geringe Signalstärke, stabiler Betrieb ist nicht garantiert;
- **durchgestrichenes Symbol** – kein Signal.

> Prüfen Sie die Signalstärke von Jeweller vor der endgültigen Installation. Bei einer Signalstärke von einem oder null Balken können wir nicht garantieren, dass das Gerät stabil funktioniert. Versuchen Sie in diesem Fall, das Gerät an einem anderen Ort zu platzieren, da eine Verschiebung um 20 cm die Signalstärke erheblich verbessern kann. Wenn das Signal nach dem Standortwechsel immer noch schwach oder instabil ist, ist ein Funk-Signalverstärker zu verwenden.

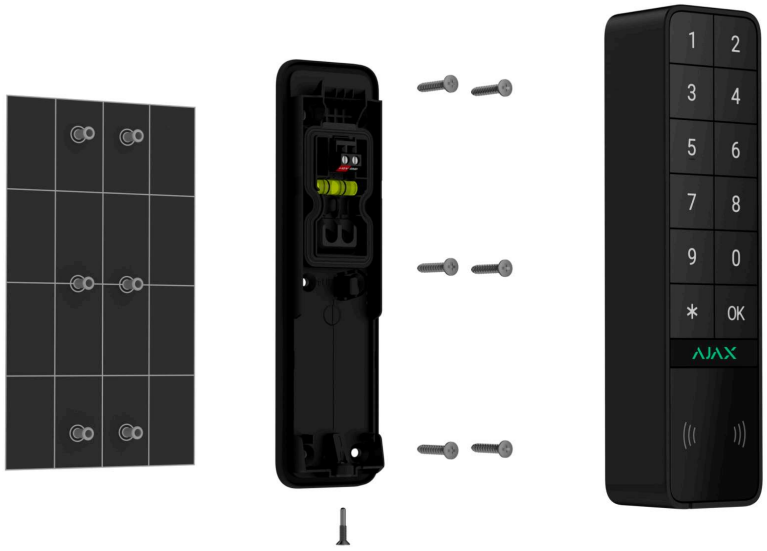
Im Abschnitt **Funktionsprüfung** erfahren Sie, wie Sie den Jeweller Signalstärketest durchführen können.

Was ist der Jeweller Signalstärketest

Hier darf das Bedienteil nicht installiert werden

1. An Orten, an denen Strom- oder Ethernetkabel, Dekorationsgegenstände oder andere Objekte das Bedienteil verdecken können. Für den ordnungsgemäßen Betrieb des Karten-/Handsender-/Bluetooth-Lesers muss ein freier Bereich von 30 cm vor dem Bedienteil vorhanden sein.
2. An Orten, an denen Temperatur und Luftfeuchtigkeit außerhalb der zulässigen Grenzen liegen. Dadurch kann das Gerät beschädigt werden.
3. An Orten, an denen das akustische Signal gedämpft wird (in Möbeln, hinter dicken Vorhängen usw.).
4. In der Nähe von Glasbruchmeldern. Der Ton des eingebauten Summers kann einen Alarm auslösen.
5. An Orten mit geringer oder instabiler Jeweller Signalstärke.

Installation



Bevor Sie KeyPad Outdoor Jeweller installieren, vergewissern Sie sich, dass Sie den optimalen Installationsort gewählt haben, der den Anforderungen dieses Benutzerhandbuchs entspricht.

So installieren Sie das Gerät:

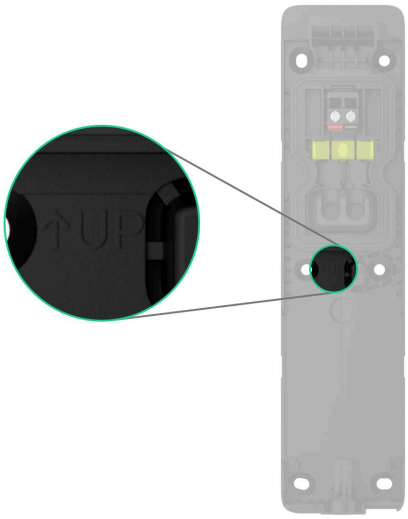
1. Lösen Sie die Befestigungsschraube an der Unterseite des Geräts und entfernen Sie die SmartBracket-Montageplatte vom Bedienteil.

   Wenn Sie die externe Stromversorgung anschließen möchten, lesen Sie den Abschnitt Externe Stromversorgung anschließen für weitere Informationen.

2. **Fügen Sie das Gerät dem System hinzu**.
3. Befestigen Sie die SmartBracket-Platte vorübergehend mit doppelseitigem Klebeband oder anderen temporären Befestigungsmitteln.

   Doppelseitiges Klebeband darf nur für eine temporäre Befestigung verwendet werden. Das mit dem Klebeband befestigte Gerät kann sich jederzeit von der Oberfläche lösen. Solange das Gerät mit Klebeband befestigt ist, wird der Sabotagealarm nicht ausgelöst, wenn das Gerät von der Oberfläche abgenommen wird.

   Das Symbol **UP** auf dem SmartBracket zeigt den oberen Teil des Bedienteils an. Berücksichtigen Sie dies bei der Installation des Geräts.



4. Setzen Sie das Bedienteil auf die SmartBracket-Montageplatte. Die LED-Anzeige des Geräts startet zu blinken. Dies ist ein Signal dafür, dass das Gehäuse des Geräts geschlossen ist.

5. Führen Sie die **Funktionsprüfung** durch.

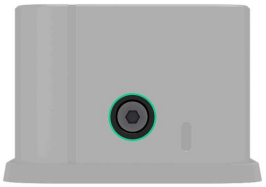
6. Wenn die Tests erfolgreich verlaufen sind, entfernen Sie das Bedienteil aus dem SmartBracket.

7. Befestigen Sie die SmartBracket-Montageplatte mit den mitgelieferten Schrauben. Verwenden Sie alle Befestigungspunkte.

> Wenn Sie andere Befestigungsmittel verwenden, achten Sie darauf, dass sie die Platte nicht beschädigen oder verformen.

8. Setzen Sie das Bedienteil auf die SmartBracket-Montageplatte.

9. Ziehen Sie die Befestigungsschraube an der Unterseite des Gehäuses des Bedienteils mit einem Drehmoment von **1—1.1 N·m** fest. Die Schraube sorgt für eine sicherere Befestigung und schützt das Bedienteil vor einer schnellen Demontage. Außerdem ist die Schraube mit einem Sabotagekontakt versehen, der reagiert, wenn jemand versucht, die Befestigungsschraube zu lösen. Das System sendet einen Sabotagealarm an Ajax Apps und die NSL.



Anschluss einer externen Stromversorgung

Beim Anschluss und Betrieb des KeyPad Outdoor Jeweller an eine externe Stromversorgung sind die allgemeinen Sicherheitsvorschriften für den Umgang mit elektrischen Geräten sowie die Vorschriften und Bestimmungen zur elektrischen Sicherheit zu beachten.

KeyPad Outdoor Jeweller ist mit Klemmen für den Anschluss eines 10,5–14 V⎓ Netzteils ausgestattet.

Beim Anschluss an eine externe Stromversorgung dienen die eingebauten Akkus als Notstromquelle. Sie dürfen nicht entfernt werden, wenn ein Netzteil angeschlossen ist.

Verwenden Sie zum Anschluss eines externen Netzteils ein Kabel, das die folgenden Anforderungen erfüllt:

- maximale Kabellänge: **100 m**
- Mindestquerschnittsfläche des Kabels: **0,5 mm² (20 AWG)**
- Leitermaterial: **Kupfer**
- maximaler elektrischer Widerstand (ρ): **0,02 Ω-mm²/m**

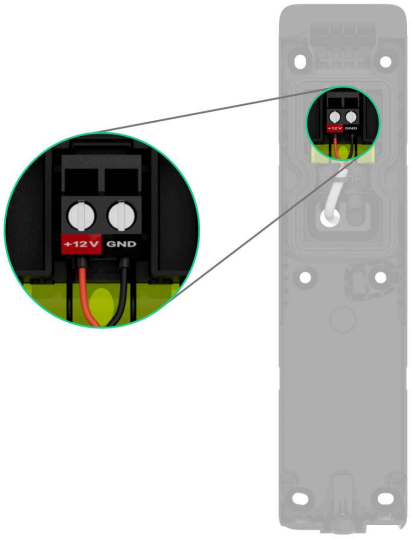
Die Verwendung eines Kabels, das diesen Parametern nicht entspricht, kann zu einem instabilen Betrieb des Geräts oder zu Fehlfunktionen führen.

Prüfen Sie vor der Installation des Geräts, ob die Kabelisolierung nicht beschädigt ist. Verwenden Sie nur eine geerdete Stromquelle. Demontieren Sie das Gerät niemals unter Spannung. Verwenden Sie das Gerät nicht, wenn das Netzkabel beschädigt ist.

So schließen Sie die externe Stromversorgung an:

1. Schalten Sie das Stromversorgungskabel spannungsfrei.
2. Demontieren Sie das Gerät, wenn es bereits installiert ist.
3. Machen Sie je nach Anzahl der Kabel ein oder zwei Löcher in den Gummi-Verschlussstopfen in den Aussparungen.

4. Führen Sie das Kabel durch das vorbereitete Loch in das Gehäuse des Bedienteils.
5. Schließen Sie die Drähte gemäß der nachstehenden Abbildung an die Klemmen an. Achten Sie auf die richtige Polarität und Reihenfolge der Kabelanschlüsse. Befestigen Sie das Kabel fest an den Klemmen.



6. Montieren Sie das Bedienteil auf der Oberfläche gemäß den **Schritten 3 bis 9** im Abschnitt **Installation**.

7. Schalten Sie die Stromversorgung ein.

Sobald die externe Stromversorgung angeschlossen ist, ändert sich der Status des Parameters **Stromversorgung** im **Gerätestatus** auf **Verbunden**.

Hinzufügen zum System

> ⚠ Eine Hub-Zentrale und ein Gerät sind nicht kompatibel, wenn sie mit unterschiedlichen Funkfrequenzen arbeiten. Der Funkfrequenzbereich des Geräts kann je nach Region unterschiedlich sein. Es wird empfohlen, die Ajax Geräte in der Region zu kaufen, in der sie verwendet werden sollen. Der Frequenzbereich für den Betrieb kann beim technischen Kundendienst erfragt werden.

Bevor Sie ein Gerät hinzufügen

1. Installieren Sie die **Ajax App**.

2. Melden Sie sich bei Ihrem **Konto** an oder erstellen Sie ein neues Konto.

3. Wählen Sie einen **Space** aus oder erstellen Sie einen neuen.

4. Fügen Sie mindestens einen **virtuellen Raum** hinzu.

5. Fügen Sie dem Space eine **kompatible Hub-Zentrale** hinzu. Stellen Sie sicher, dass die Hub-Zentrale eingeschaltet und über Ethernet, WLAN und/oder Mobilfunknetz mit dem Internet verbunden ist.
6. Überprüfen Sie den Status in der Ajax App, um sicherzustellen, dass der Space deaktiviert ist und die Hub-Zentrale nicht aktualisiert wird.

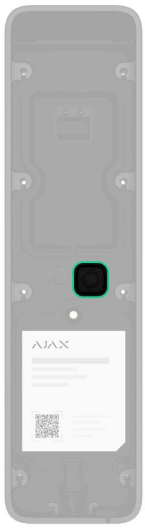
> ⚠ Nur ein PRO-Benutzer oder ein Space-Administrator mit Systemkonfigurationsrechten kann ein Gerät zur Hub-Zentrale hinzufügen.

Kontotypen und ihre Rechte

Hinzufügen zur Hub-Zentrale

1. Öffnen Sie eine **Ajax App**. Wählen Sie den **Space** aus, dem Sie das Gerät hinzufügen möchten.
2. Gehen Sie zum Menü **Geräte** und klicken Sie auf **Gerät hinzufügen**.
3. Geben Sie einen Namen für das Gerät ein.
4. Scannen Sie den QR-Code oder geben Sie die Geräte-ID manuell ein. Der QR-Code mit der Geräte-ID befindet sich auf dem Gehäuse des Geräts. Er ist auch auf der Verpackung des Geräts angegeben.
5. Wählen Sie einen virtuellen Raum und eine Sicherheitsgruppe (wenn der **Gruppenmodus** aktiviert ist).
6. Tippen Sie auf **Hinzufügen**, und der Countdown beginnt.

7. Schalten Sie das Gerät ein, indem Sie die Ein/Aus-Taste 3 Sekunden lang gedrückt halten.



Wenn die Verbindung fehlschlägt, versuchen Sie es in 5 Sekunden erneut. Wenn bereits die maximale Anzahl von Geräten zur Hub-Zentrale hinzugefügt wurde, erhalten Sie eine Fehlermeldung, wenn Sie versuchen, weitere Geräte hinzuzufügen.

KeyPad Outdoor Jeweller hat einen eingebauten Summer, der Alarme und bestimmte Systemzustände signalisieren kann, aber keine Sirene ist. Sie können bis zu 50 Bedienteile mit eingebautem Summer zur Hub-Zentralen hinzufügen. Berücksichtigen Sie dies bei der Planung Ihres Sicherheitssystems.

Sobald das Gerät zur Hub-Zentrale hinzugefügt wurde, erscheint es in der Liste der Geräte in der Ajax App. Das Update-Intervall für die Gerätezustände in der Liste hängt von den **Jeweller** oder **Jeweller/Fibra** Einstellungen ab und beträgt standardmäßig 36 Sekunden.

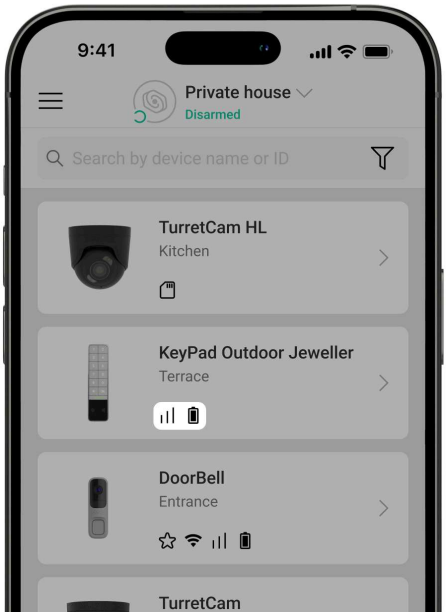
> KeyPad Outdoor Jeweller arbeitet mit nur einer Hub-Zentrale. Wenn es mit einer neuen Hub-Zentrale gekoppelt wird, sendet es keine Ereignisse mehr an die alte Hub-Zentrale. Nach dem Hinzufügen zu einer neuen Hub-Zentrale wird das Bedienteil nicht automatisch aus der Geräteliste der alten Hub-Zentrale entfernt. Dies muss über die Ajax App erfolgen.

Funktionsprüfung

Ein Ajax System bietet mehrere Testarten, die bei der Auswahl des richtigen Installationsortes für die Geräte helfen. Für KeyPad Outdoor Jeweller sind die folgenden Tests verfügbar:

- **Jeweller Signalstärketest** – zur Bestimmung der Signalstärke und -stabilität zwischen der Hub-Zentrale (oder dem Funk-Signalverstärker) und dem Gerät über das Jeweller Funk-Datenübertragungsprotokoll am Installationsort des Geräts.
- **Signaldämpfungs-Prüfung** – um die Leistung des Funksenders zu verringern oder zu erhöhen; um die Stabilität der Kommunikation zwischen dem Gerät und der Hub-Zentrale zu überprüfen, wird die sich ändernde Umgebung am Installationsort simuliert.

Symbole

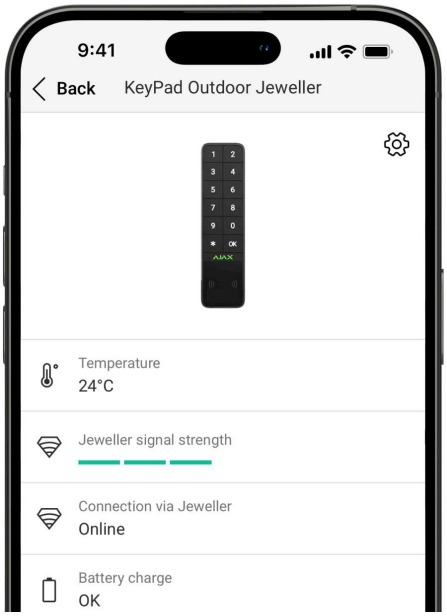


Die Symbole in der Ajax App zeigen einige der Zustände des KeyPad Outdoor Jeweller an. Die Symbole können auf der Registerkarte **Geräte** überprüft werden.

Symbol	Bedeutung
	Jeweller Signalstärke. Zeigt die Signalstärke zwischen der Hub-Zentrale und dem Gerät an. Der empfohlene Wert liegt bei 2 bis 3 Balken. Mehr erfahren
	Akkuladestand des Geräts. Mehr erfahren
RE	Das Gerät arbeitet über den Funk-Signalverstärker. Mehr erfahren
	Der **Karten-/Anhängerleser** ist in den Einstellungen des Bedienteils aktiviert.
	Bluetooth ist in den Einstellungen des Bedienteils aktiviert.
	Die Bluetooth-Einrichtung ist unvollständig. Die Beschreibung ist in den Bedienteilzuständen verfügbar.

	Die Funktion **Glockenton beim Öffnen** ist in den Einstellungen des Bedienteils aktiviert.
	Das Gerät befindet sich im Modus der Signaldämpfungsprüfung. Mehr erfahren
	Die Montageplatte ist entriegelt.
	Das Gerät ist dauerhaft deaktiviert. Mehr erfahren
	Benachrichtigungen über Sabotagealarme sind dauerhaft deaktiviert. Mehr erfahren
	Das Gerät ist bis zur nächsten Unscharfschaltung des Systems deaktiviert. Mehr erfahren
	Benachrichtigungen über Sabotagealarm sind deaktiviert, bis das Objekt zum ersten Mal unscharf geschaltet wird. Mehr erfahren
Offline	Das Gerät hat die Verbindung zur Hub-Zentrale verloren oder die Hub-Zentrale hat die Verbindung zum Ajax Cloud Server verloren.
Not transferred	Das Gerät wurde nicht auf die neue Hub-Zentrale übertragen. Mehr erfahren

Zustände



Die Zustände enthalten Informationen über das Gerät und seine Betriebsparameter. Die Zustände des KeyPad Outdoor Jeweller sind in der Ajax App verfügbar:

1. Gehen Sie auf die Registerkarte **Geräte** .
2. Wählen Sie **KeyPad Outdoor Jeweller** in der Liste aus.

Parameter	Bedeutung
Datenimport	Zeigt den Fehler bei der Übertragung von Daten auf die neue Hub-Zentrale an: • **Fehlgeschlagen** — das Gerät wurde nicht auf die neue Hub-Zentrale übertragen. Mehr erfahren
Störung	Durch Tippen auf ⓘ wird die Liste der Gerätestörungen geöffnet. Das Feld wird nur angezeigt, wenn eine Störung erkannt wird.
Warnung ⚠	Durch Tippen auf ⓘ wird die Liste der Einstellungen und Berechtigungen geöffnet, die der App für den korrekten Betrieb des Bedienteils gewährt werden müssen.

Temperatur	Gerätetemperatur. Sie wird vom Prozessor gemessen und verändert sich abhängig von der Umgebungstemperatur. Sie können ein Szenario nach Temperatur erstellen, um Automatisierungsgeräte zu steuern. **Mehr erfahren**
Jeweller Signalstärke	Jeweller Signalstärke zwischen dem Gerät und der Hub-Zentrale (oder dem Funk-Signalverstärker). Der empfohlene Wert liegt bei 2 bis 3 Balken. Jeweller ist ein Protokoll zur Übertragung von Ereignissen und Alarmen.
Verbindung über Jeweller	Verbindungsstatus über den Jeweller Kanal zwischen dem Gerät und der Hub-Zentrale (oder dem Funk-Signalverstärker): • **Online** — das Gerät ist mit der Hub-Zentrale (oder dem Funk-Signalverstärker verbunden). Normaler Zustand. • **Offline** — das Gerät ist nicht mit der Hub-Zentrale (oder dem Funk-Signalverstärker verbunden). Überprüfen Sie die Geräteverbindung.
Akkuladung	Ladezustand des Akkus des Geräts. Es sind zwei Zustände verfügbar: • **OK**. • **Niedriger Batteriestand**. Bei niedrigem Akkustand werden entsprechende Meldungen an den Benutzer und an das Sicherheitsunternehmen gesendet. **Mehr erfahren**

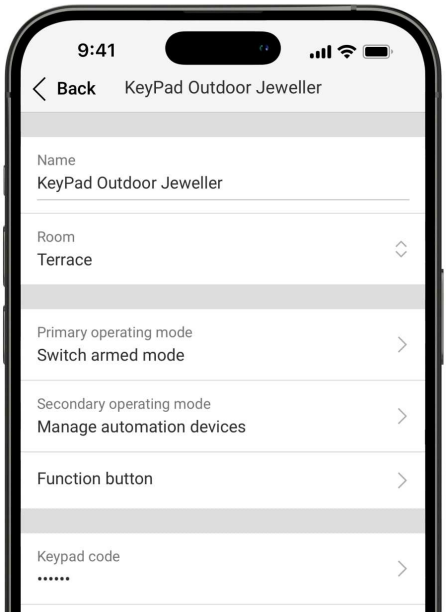
Sendeleistung	Zeigt die gewählte Leistung des Transmitters an. Der Parameter wird angezeigt, wenn im Menü **Signaldämpfungsprüfung** die Option **Max** oder **Dämpfung** gewählt wird. Mehr erfahren
<Name des Funk-Repeaters>	Status der Verbindung zwischen dem Gerät und dem Funk-Signalverstärker. • **Online** — das Gerät ist mit dem Funk-Signalverstärker verbunden. • **Offline** — das Gerät ist nicht mit dem Funk-Signalverstärker verbunden. Dieses Feld wird angezeigt, wenn das Gerät über einen Funk-Signalverstärker betrieben wird.
Deckel	Der Status des Sabotagekontakts des Geräts, der auf das Abnehmen oder Öffnen des Gerätegehäuses reagiert: • **Geöffnet** — das Gerät wurde von der SmartBracket-Montageplatte entfernt oder seine Integrität ist beeinträchtigt. Überprüfen Sie die Montage des Geräts. • **Geschlossen** — das Gerät ist an der SmartBracket-Montageplatte installiert. Die Integrität des Gerätegehäuses und der Montageplatte ist nicht beeinträchtigt. Normaler Zustand. Mehr erfahren
Montageplatte	Der Status des Sabotagekontakts des Geräts, der auf die Entriegelung der SmartBracket-Montageplatte reagiert: • **Entriegelt** – die Befestigungsschraube für SmartBracket ist abgeschraubt oder

	die Montageplatte ist beschädigt. Überprüfen Sie die Befestigungsschraube und die Befestigung des Geräts. • **Verriegelt** – die Befestigungsschraube für SmartBracket ist fest angezogen. Die Integrität des Gerätegehäuses und der Montageplatte ist nicht beeinträchtigt. Normaler Zustand. Mehr erfahren
Externe Stromversorgung	Zustand der externen Stromversorgung: • **Verbunden** – die Stromversorgung ist an den Melder angeschlossen. • **Getrennt** – die Stromversorgung ist getrennt oder nicht angeschlossen.
Akustische Alarmsignalisierung	Zeigt den Status der Einstellung **Bedienteil-Summer aktivieren, wenn im System ein Alarm ausgelöst wird**.
Alarmdauer	Dauer des Tonsignals im Alarmfall. Die Einstellung erfolgt in Schritten von 3 Sekunden. Wird angezeigt, wenn die Funktion **Bedienteil-Summer aktivieren, wenn ein Alarm im System ausgelöst wird** aktiviert ist.
Karten-/Anhängerleser	Zeigt an, ob der Karten- und Anhängerleser aktiviert ist.
Bluetooth	Zeigt an, ob das Bluetooth-Modul des Bedienteils zur Steuerung des Systems mit einem Smartphone aktiviert ist.
Piepton-Einstellungen	

Scharfschaltung/Unscharfschaltung	Wenn aktiviert, signalisiert das Bedienteil das Scharf- und Unscharfschalten durch einen kurzen Piepton.
Aktivierung/Deaktivierung des Nachtmodus	Wenn diese Funktion aktiviert ist, signalisiert das Bedienteil das Ein- und Ausschalten des **Nachtmodus** durch einen kurzen Piepton.
Eingangsverzögerungen	Wenn diese Funktion aktiviert ist, piept das Bedienteil bei **Eingangsverzögerungen**.
Ausgangsverzögerungen	Wenn diese Funktion aktiviert ist, piept das Bedienteil bei **Ausgangsverzögerungen**.
Eingangsverzögerungen im Nachtmodus	Wenn diese Funktion aktiviert ist, piept das Bedienteil bei **Eingangsverzögerungen** im **Nachtmodus**.
Ausgangsverzögerungen im Nachtmodus	Wenn diese Funktion aktiviert ist, piept das Bedienteil bei **Ausgangsverzögerungen** im **Nachtmodus**.
Glockenton beim Öffnen	Wenn diese Funktion aktiviert ist, signalisiert das Bedienteil das Auslösen des Öffnungsmelders im Systemmodus **Unscharf**. **Mehr erfahren**
Piepton-Lautstärke	Wird angezeigt, wenn die Signalisierung von Scharf-/Unscharfschaltung, Ein-/Ausgangsverzögerung und Öffnen aktiviert ist. Zeigt die Lautstärke des Summers für Benachrichtigungen an.
Dauerhafte Deaktivierung	Der Status der Funktion zur permanenten Deaktivierung des Geräts: • **Nein –** das Gerät arbeitet im normalen Modus und meldet alle Ereignisse. • **Vollständig —** der Administrator der Hub-Zentrale hat das Gerät vollständig vom Systembetrieb ausgeschlossen.

	Das Gerät führt keine Systembefehle aus und meldet keine Alarme oder andere Ereignisse. • **Nur Gehäuse** — Benachrichtigungen über das Auslösen des Sabotagealarms wurden vom Administrator der Hub-Zentrale deaktiviert. Mehr erfahren
Einmalige Deaktivierung	Zeigt den Status der Einstellung für die einmalige Deaktivierung des Geräts an: • **Nein** — das Gerät arbeitet im normalen Modus. • **Vollständig** — das Gerät ist für die Zeit, in der der Scharfschaltmodus aktiv ist, vollständig vom Betrieb des Systems ausgeschlossen. Das Gerät führt keine Systembefehle aus und meldet keine Alarme oder andere Ereignisse. • **Nur Gehäuse** — Benachrichtigungen über die Auslösung des Sabotagealarms sind für die Zeit, in der der Scharfmodus aktiv ist, deaktiviert. Mehr erfahren
Firmware	Firmware-Version des Geräts.
Geräte-ID	Geräte-ID. Auch über den QR-Code auf dem Gehäuse und der Verpackung des Geräts verfügbar.
Geräte-Nr.	Gerätenummer. Diese Nummer wird im Alarmfall oder bei anderen Ereignissen an die NSL übermittelt.

Einstellungen



So ändern Sie die Einstellungen von KeyPad Outdoor Jeweller in den Ajax Apps:

1. Gehen Sie auf die Registerkarte **Geräte** .
2. Wählen Sie **KeyPad Outdoor Jeweller** in der Liste aus.
3. Gehen Sie zu den **Einstellungen** .
4. Nehmen Sie die erforderlichen Einstellungen vor.
5. Klicken Sie auf **Zurück**, um die neuen Einstellungen zu speichern.

Einstellungen	Bedeutung
Name	Gerätename. Wird in der Geräteliste der Hub-Zentrale, im SMS-Text sowie in den Benachrichtigungen im Ereignisprotokoll angezeigt. Um den Namen des Geräts zu ändern, tippen Sie auf das Textfeld. Der Name kann bis zu 24 lateinische oder bis zu 12 kyrillische Zeichen enthalten.
Raum	Auswahl des virtuellen Raums, dem KeyPad Outdoor Jeweller zugeordnet ist.

	Der Raumname wird im SMS-Text und in den Benachrichtigungen des Ereignisprotokolls angezeigt.
Primärer Betriebsmodus	Öffnet das Menü mit den Einstellungen für den **primären Betriebsmodus**.
Sekundärer Betriebsmodus	Öffnet das Menü mit den Einstellungen für den **sekundären Betriebsmodus**.
Funktionstaste	Auswahl der Funktion der * Taste (**Funktionstaste**): • **Keine** — die Funktionstaste ist deaktiviert und führt keine Befehle aus, wenn sie gedrückt wird. • **Panik** — nach Drücken der Funktionstaste sendet das System einen Alarm an die NSL und alle Benutzer. • **Feueralarm stummschalten** — wenn die Funktionstaste gedrückt wird, schaltet das System ausgelöste Ajax Brandmelder stumm. Nur verfügbar, wenn die Funktion **Alarm vernetzter Brandmelder** aktiviert ist. Mehr erfahren
Bedienteil-Code	Auswahl eines allgemeinen Codes für die Sicherheitskontrolle. Enthält 4 bis 6 Ziffern.
Bedrohungscode	Auswahl eines allgemeinen Bedrohungscodes für den stillen Alarm. Enthält 4 bis 6 Ziffern. Mehr erfahren
Auto-Sperre beim unbefugten Zugriff	Wenn diese Funktion aktiviert ist, wird das Bedienteil für eine voreingestellte Zeit gesperrt, wenn innerhalb einer Minute mehr als dreimal hintereinander ein falscher Code eingegeben wird oder ein nicht verifiziertes Zutrittsgerät verwendet wird.

	Ein PRO-Benutzer oder ein Benutzer mit Systemkonfigurationsrechten kann das Bedienteil über die App entsperren, bevor die angegebene Sperrzeit abläuft.
Auto-Sperrzeit	Auswahl des Zeitraums für die Bedienteilsperre nach unberechtigten Zugriffsversuchen: • 3 Minuten • 5 Minuten • 10 Minuten • 20 Minuten • 30 Minuten • 60 Minuten • 90 Minuten • 180 Minuten Verfügbar, wenn die Funktion **Sperre bei unbefugtem Zugriff** aktiviert ist.
Karten-/Anhängerleser	Wenn aktiviert, kann der Sicherheitsmodus mit den Zugriffsgeräten **Pass** und **Tag** gesteuert werden.
Bluetooth	Wenn aktiviert, kann der Sicherheitsmodus mit einem Smartphone gesteuert werden.
Bluetooth-Empfindlichkeit	Einstellung der Empfindlichkeit des Bluetooth-Moduls des Bedienteils: • Minimal • Niedrig • Normal (standardmäßig) • Hoch • Max

	Verfügbar, wenn der **Bluetooth-Schalter** aktiviert ist.
Hintergrundbeleuchtung und Anzeige	Öffnet das Menü mit den Einstellungen für **Hintergrundbeleuchtung und Anzeige**.
Akustische Signalisierung	Öffnet das Menü mit den Einstellungen für die **akustische Signalisierung**.
Jeweller Signalstärketest	Schaltet das Gerät in den Jeweller Signalstärketestmodus. Der Test ermöglicht es, die Signalstärke zwischen der Hub-Zentrale (oder dem Funk-Signalverstärker) und dem Gerät über das kabellose Datenübertragungsprotokoll Jeweller zu überprüfen, um den optimalen Installationsort auszuwählen. **Mehr erfahren**
Signaldämpfungsprüfung	Umschalten des Geräts in den Modus für die Signaldämpfungsprüfung. **Mehr erfahren**
Karte/Anhänger zurücksetzen	Ermöglicht das Löschen aller mit Tag oder Pass verbundenen Hub-Zentralen aus dem Gerätespeicher. **Mehr erfahren**
Benutzerhandbuch	Öffnet das Benutzerhandbuch zu KeyPad Outdoor Jeweller in der Ajax App.
Dauerhafte Deaktivierung	Ermöglicht es dem Benutzer, die Ereignisse des Geräts zu deaktivieren, ohne es aus dem System zu entfernen. Es stehen drei Optionen zur Verfügung: • **Nein** — das Gerät arbeitet im normalen Modus und überträgt alle Ereignisse. • **Vollständig** — das Gerät führt keine Systembefehle aus und nimmt nicht an

	Automatisierungsszenarien teil; das System ignoriert Gerätealarme und andere Benachrichtigungen. • **Nur Deckel** — das System ignoriert nur Benachrichtigungen über die Auslösung des Sabotagealarms des Geräts. Mehr erfahren
Einmalige Deaktivierung	Ermöglicht es dem Benutzer, Ereignisse des Geräts bis zur ersten Unscharfschaltung zu deaktivieren. Es stehen drei Optionen zur Verfügung: • **Nein** — das Gerät arbeitet im normalen Modus und überträgt alle Ereignisse. • **Vollständig** — das Gerät ist bis zur ersten Unscharfschaltung vollständig vom Betrieb des Systems ausgeschlossen. Das Gerät führt keine Systembefehle aus und meldet keine Alarme oder andere Ereignisse. • **Nur Gehäuse** — Benachrichtigungen über die Auslösung des Sabotagealarms sind bis zur nächsten Unscharfschaltung deaktiviert. Mehr erfahren
Gerät löschen	Entkoppelt das Gerät, trennt es von der Hub-Zentrale und löscht seine Einstellungen.

Primärer und sekundärer Betriebsmodus

KeyPad Outdoor Jeweller verfügt über zwei Betriebsmodi: primär und sekundär. Für jeden Betriebsmodus kann eine der drei Funktionen des Bedienteils konfiguriert werden: **Scharf-/Unscharfschalten**, **Automatisierungsgeräte steuern** oder **Eingangsverzögerung** aktivieren.

Es kann nur eine primäre und eine sekundäre Bedienteilfunktion gleichzeitig eingestellt werden. Um zwischen den Funktionen zu wechseln, halten Sie die **OK**-Taste auf dem Bedienteil gedrückt.

Parameter	Bedeutung
Primärer Betriebsmodus	
Funktion des Bedienteils	Auswahl der Bedienteilfunktion für den primären Betriebsmodus: • Scharf-/Unscharfschalten • Automatisierungsgeräte steuern • Eingangsverzögerung aktivieren Es kann jeweils nur eine primäre und eine sekundäre Funktion eingestellt werden.
Sekundärer Betriebsmodus	
Funktion des Bedienteils	Auswahl der Bedienteilfunktion für den sekundären Betriebsmodus: • Keine • Scharf-/Unscharfschalten • Automatisierungsgeräte steuern • Eingangsverzögerung aktivieren Es kann jeweils nur eine primäre und eine sekundäre Funktion eingestellt werden.
Scharf-/Unscharfschalten	
Sicherheitsobjekte	Auswahl der vom Gerät kontrollierten Sicherheitsobjekte. Sie können den gesamten Space, alle oder bestimmte Gruppen oder den **Nachtmodus** auswählen.

	Die Auswahl von Gruppen ist möglich, wenn der **Gruppenmodus** aktiviert ist.
Zugriffseinstellungen	Auswahl der Methode zum Scharf-/Unscharfschalten: • Nur Bedienteil-Codes. • Nur Benutzercodes. • Bedienteil- und Benutzercodes. Um die **Bedienteil-Zugangscodes** zu aktivieren, die für Personen eingerichtet wurden, die nicht im System registriert sind, wählen Sie die Optionen auf dem Bedienteil: **Nur Bedienteil-Codes** oder **Bedienteil- und Benutzercodes**.
Vorabautorisierung	Wenn diese Option aktiviert ist, muss der Benutzer für die Benutzung des Bedienteils authentifiziert werden: Geben Sie einen Code ein oder halten Sie ein persönliches Zugangsgerät an das Bedienteil.
Autorisierung mit Code bestätigen	Wenn diese Funktion aktiviert ist, können Benutzer das System nur dann scharf oder unscharf schalten, wenn sie mit zwei Arten der Identifizierung erfolgreich autorisiert wurden, d. h. mit Pass, Tag oder einem Smartphone und Eingabe des entsprechenden Passcodes. **Mehr erfahren**
Einfacher Wechsel des Scharfschaltmodus	Wenn diese Funktion aktiviert ist, müssen Benutzer nach der Eingabe eines Passcodes oder dem Lesen eines Zugangsgeräts nicht die **OK**-Taste drücken.
Scharfschaltung ohne Code	Wenn diese Funktion aktiviert ist, kann der Benutzer das Objekt scharf schalten, ohne einen Code einzugeben oder das persönliche Zugangsgerät vorzuzeigen. Wenn diese Funktion deaktiviert ist, geben Sie einen Code ein oder zeigen Sie das

	Zugangsgerät vor, um das System zu aktivieren. Verfügbar, wenn der Schalter für die **Vorabautorisierung** deaktiviert ist.
Automatischer Wechsel in den Sekundärmodus	Nur für die Option **Sekundärer Betriebsmodus** verfügbar. Mit dieser Option kann der Benutzer einstellen, wann das Bedienteil automatisch in den sekundären Modus wechselt, ohne dass die **OK**-Taste lange gedrückt werden muss: • Aus. • Wenn das System deaktiviert ist. • Wenn das System aktiviert ist.
Automatisierungsgeräte steuern	
Automatisierungsszenarien	Erstellt und konfiguriert ein Szenario zur Verwaltung von Automatisierungsgeräten mit einem Bedienteil. Sie können ein Szenario erstellen, das **bei einer vordefinierten Aktion** oder **bei Änderung des Zustands** eines oder mehrerer Automatisierungsgeräte ausgeführt wird. Das Bedienteil kann nur ein Szenario verwalten.
Zugriffseinstellungen	Auswahl der Methode zum Scharf-/Unscharfschalten: • Nur Bedienteil-Codes. • Nur Benutzercodes.

	• Bedienteil- und Benutzercodes. Um die **Bedienteil-Zugangscodes** zu aktivieren, die für nicht im System registrierte Personen eingerichtet wurden, wählen Sie die Option **Nur Bedienteil-Codes** oder **Bedienteil- oder Benutzercodes**.
Vorabautorisierung	Wenn diese Option aktiviert ist, muss der Benutzer für die Benutzung des Bedienteils authentifiziert werden: Geben Sie einen Code ein oder halten Sie ein persönliches Zugangsgerät an das Bedienteil.
Einfache Gerätesteuerung	Wenn diese Funktion aktiviert ist, müssen Benutzer nach der Eingabe eines Passcodes oder dem Lesen eines Zugangsgeräts nicht die **OK**-Taste drücken.
Gerätesteuerung einschränken	Mit dieser Option kann der Benutzer festlegen, wann die Steuerung des Automatisierungsgeräts über das Bedienteil gesperrt werden soll: • Aus. • Wenn das System deaktiviert ist. • Wenn das System aktiviert ist.
Automatischer Wechsel in den Sekundärmodus	Nur für die Option **Sekundärer Betriebsmodus** verfügbar. Mit dieser Option kann der Benutzer einstellen, wann das Bedienteil automatisch in den sekundären Modus wechselt, ohne dass die **OK**-Taste lange gedrückt werden muss: • Aus. • Wenn das System deaktiviert ist.

	• Wenn das System aktiviert ist.
Eingangsverzögerung aktivieren	
Eingangsverzögerung	Auswahl der Eingangsverzögerungszeit: 5 bis 255 Sekunden. Die Eingangsverzögerung (Alarmaktivierungsverzögerung) ist die Zeit, die der Benutzer benötigt, um das System über das Hauptbedienteil zu deaktivieren.
Zugriffseinstellungen	Auswahl der Methode zum Scharf-/Unscharfschalten: • Nur Bedienteil-Codes. • Nur Benutzercodes. • Bedienteil- und Benutzercodes. Um die **Bedienteil-Zugangscodes** zu aktivieren, die für nicht im System registrierte Personen eingerichtet wurden, wählen Sie die Option **Nur Bedienteil-Codes** oder **Bedienteil- oder Benutzercodes**.
Autorisierung mit Code bestätigen	Wenn diese Funktion aktiviert ist, können Benutzer das System nur dann scharf oder unscharf schalten, wenn sie mit zwei Arten der Identifizierung erfolgreich autorisiert wurden, d. h. mit Pass, Tag oder einem Smartphone und Eingabe des entsprechenden Passcodes. Mehr erfahren
Einfacher Verzögerungsbeginn	Wenn diese Funktion aktiviert ist, müssen Benutzer nach der Eingabe eines Passcodes oder dem Lesen eines Zugangsgeräts nicht die **OK**-Taste drücken.

Automatischer Wechsel in den Sekundärmodus	Nur für die Option **Sekundärer Betriebsmodus** verfügbar. Mit dieser Option kann der Benutzer einstellen, wann das Bedienteil automatisch in den sekundären Modus wechselt, ohne dass die OK-Taste lange gedrückt werden muss: • Aus. • Wenn das System deaktiviert ist. • Wenn das System aktiviert ist.

Hintergrundbeleuchtung und Anzeige

Einstellungen	Bedeutung
Helligkeit	Helligkeit der Hintergrundbeleuchtung des Bedienteils einstellen.
Hintergrundbeleuchtung immer aktiv	Wenn diese Funktion aktiviert ist, bleibt die Hintergrundbeleuchtung des Bedienteils immer aktiv.
Anzeige des Scharfschaltungsmodus	Mit dieser Option kann der Benutzer festlegen, wann der Sicherheitsstatus des Systems auf dem Bedienteil angezeigt werden soll: • **Niemals** — keine LED-Anzeige des Sicherheitszustands. • **Nur bei Scharfschaltung** — das Logo leuchtet rot, wenn das System aktiviert, teilweise aktiviert oder im **Nachtmodus** ist.

	• **Immer** — das Logo leuchtet rot, wenn das System aktiviert ist, grün, wenn es deaktiviert ist, und gelb, wenn die Scharfschaltung nicht abgeschlossen ist.

Akustische Signalisierung

KeyPad Outdoor Jeweller verfügt über einen eingebauten Summer, der je nach Einstellung Folgendes signalisieren kann:

1. Alarme.
2. Ein-/Ausgangsverzögerungen.
3. Glockenton beim Öffnen.
4. Ausführung von Befehlen (z. B. Scharfschaltung, Unscharfschaltung).
5. Drücken der Tasten auf dem Bedienfeld.

> Wir raten davon ab, das KeyPad Outdoor Jeweller anstelle der Sirene zu verwenden. Der Summer des Bedienteils ist nur für zusätzliche Benachrichtigungen gedacht. Ajax Sirenen sollen Eindringlinge abschrecken und Aufmerksamkeit erregen. Eine korrekt installierte Sirene ist aufgrund der höheren Montageposition schwieriger zu demontieren als ein Bedienteil auf Augenhöhe.

Parameter	Bedeutung
Piepton-Einstellungen	Öffnet das Menü für die **Piepton-Einstellungen**.
Piepton bei Wechsel des Scharfschaltungsmodus	
Scharfschaltung/Unscharfschaltung	**Wenn aktiviert**: Es wird eine akustische Benachrichtigung gesendet, wenn der Sicherheitsmodus über das Bedienteil, ein anderes Gerät oder die App geändert wird. **Wenn deaktiviert**: Es wird eine akustische Benachrichtigung gesendet, wenn der

	Sicherheitsmodus nur über das Bedienteil geändert wird. Die Lautstärke des Pieptons hängt von der Lautstärke der konfigurierten Tasten ab.
Aktivierung/Deaktivierung des Nachtmodus	**Wenn aktiviert**: Es wird eine akustische Benachrichtigung gesendet, wenn der **Nachtmodus** über das Bedienteil, ein anderes Gerät oder die App aktiviert/deaktiviert wird. **Wenn deaktiviert**: Es wird eine akustische Benachrichtigung gesendet, wenn der **Nachtmodus** nur über das Bedienteil aktiviert/deaktiviert wird. Mehr erfahren Die Lautstärke des Pieptons hängt von der Lautstärke der konfigurierten Tasten ab.
Piepton bei Verzögerungen	
Eingangsverzögerungen	Wenn diese Funktion aktiviert ist,signalisiert der eingebaute Summer über die Eingabeverzögerung. Mehr erfahren
Ausgangsverzögerungen	Wenn diese Funktion aktiviert ist, signalisiert der eingebaute Summer über die Ausgangsverzögerung. Mehr erfahren
Eingangsverzögerungen im Nachtmodus	Wenn diese Funktion aktiviert ist, signalisiert der eingebaute Summer über die Eingangsverzögerung im Nachtmodus. Mehr erfahren
Ausgangsverzögerungen im Nachtmodus	Wenn diese Funktion aktiviert ist, signalisiert der eingebaute Summer über die

	Ausgangsverzögerung im Nachtmodus. Mehr erfahren
Schneller Signalton bei Verzögerungen	
Schnelles Signal bei Ablauf der Eingangsverzögerung	Signalisiert dem Benutzer, dass die **Eingangsverzögerung** abläuft. Sie können eine von vier Optionen wählen, wann der schnelle Piepton beginnen soll: • Niemals • Letzte 5 Sekunden • Letzte 10 Sekunden • Letzte 15 Sekunden Diese Option ist verfügbar, wenn **Piepton bei Eingangsverzögerungen** aktiviert ist.
Schnelles Signal bei Ablauf der Ausgangsverzögerung	Benachrichtigt den Benutzer, dass die **Ausgangsverzögerung** abläuft. Sie können eine von vier Optionen wählen, wann der schnelle Piepton beginnen soll: • Niemals • Letzte 5 Sekunden • Letzte 10 Sekunden • Letzte 15 Sekunden Diese Option ist verfügbar, wenn **Piepton bei Ausgangsverzögerungen** aktiviert ist.
Piepton bei Unscharfschaltung	
Glockenton beim Öffnen	Wenn aktiviert, informiert der eingebaute Summer den Benutzer mit einem kurzen Piepton darüber, dass die Öffnungsmelder

	im Systemmodus **Unscharf** ausgelöst wurden. Mehr erfahren
Piepton-Lautstärke	Auswahl der Lautstärke des eingebauten Summers für Benachrichtigungen über Scharf-/Unscharfschaltung, Eingangs-/Ausgangsverzögerung und Öffnen: • **Leise.** • **Laut.** • **Sehr laut.**
Buttons	
Lautstärke	Einstellung der Lautstärke des Summers bei Interaktion mit dem Bedienteil.
Reaktionen auf Alarme	
Akustisches Alarmsignal	Einstellung des Modus, wenn der eingebaute Summer einen Alarm auslöst: • **Immer** — ein akustischer Alarm wird unabhängig vom Sicherheitszustand des Systems ausgelöst. • **Nur bei Scharfschaltung** — ein akustischer Alarm wird ausgelöst, wenn das System oder die Gruppe, dem/der das Bedienteil zugeordnet ist, scharf geschaltet ist.
Aktiviert den Bedienteilsummer, wenn ein Alarm im System erkannt wird	Wenn aktiviert, signalisiert der eingebaute Summer einen Alarm im System.
Alarme im Gruppenmodus	Auswahl der Gruppe (aus den gemeinsamen Gruppen), über die das Bedienteil einen Alarm melden soll. Die Standardeinstellung ist **Alle gemeinsamen Gruppen**.

	Wenn das Bedienteil nur eine gemeinsame Gruppe hat und diese gelöscht wird, kehrt die Einstellung zu ihrem ursprünglichen Wert zurück. Wird angezeigt, wenn der **Gruppenmodus** aktiviert ist.
Alarmdauer	Dauer des Tonsignals im Falle eines Alarms: von 3 Sekunden bis 3 Minuten.

Stellen Sie die Ein-/Ausgangsverzögerungen in den Einstellungen des jeweiligen Melders ein, nicht in den Einstellungen des Bedienteils.

Mehr erfahren

Reaktion des Bedienteils auf Gerätealarme

KeyPad Outdoor Jeweller kann auf Alarme von jedem Gerät im System mit einem eingebauten Summer reagieren. Die Funktion ist nützlich, wenn der Benutzer den Summer für den Alarm eines bestimmten Geräts nicht aktivieren muss. Dies kann z. B. bei der Auslösung des Überschwemmungsmelders **LeaksProtect Jeweller** der Fall sein.

Standardmäßig ist die Bedienteilantwort für Alarme aller Geräte im System aktiviert.

So stellen Sie die Reaktion des Bedienteils auf einen Gerätealarm ein:

1. Öffnen Sie die Ajax App.
2. Gehen Sie auf die Registerkarte **Geräte** .
3. Wählen Sie in der Liste das Gerät aus, für das Sie die Reaktion des Bedienteils konfigurieren möchten.

4. Gehen Sie zu den **Einstellungen** ⚙.
5. Suchen Sie die Option **Alarmierung durch Sirene** und wählen Sie in welchen Fällen die Sirene ausgelöst wird. Aktivieren oder deaktivieren Sie die Funktion.
6. Wiederholen Sie die Schritte 3 bis 5 für die anderen Geräte im System.

Reaktion des Bedienteils auf Sabotagealarme

Das KeyPad Outdoor Jeweller kann auf Gehäusealarme von jedem Systemgerät mit einem eingebauten Summer reagieren. Wenn diese Funktion aktiviert ist, gibt der eingebaute Summer ein akustisches Signal ab, wenn der **Sabotagekontakt** des Geräts ausgelöst wird.

So stellen Sie die Reaktion des Bedienteils auf einen Sabotagealarm ein:

1. Öffnen Sie die Ajax App.
2. Gehen Sie auf die Registerkarte **Geräte** ▪.
3. Wählen Sie eine Hub-Zentrale aus und gehen Sie zu deren **Einstellungen** ⚙.
4. Wählen Sie das Menü **Service**.
5. Gehen Sie zum Menü **Töne und Warnungen**.
6. Aktivieren Sie den Schalter **Wenn ein Gehäuse geöffnet ist (Hub-Zentrale oder Melder)**.
7. Klicken Sie auf **Zurück**, um die neuen Einstellungen zu speichern.

> ℹ Der Sabotagekontakt reagiert auf das Öffnen und Schließen des Gehäuses, unabhängig vom Scharfschaltmodus des Geräts oder Systems.

Reaktion des Bedienteils bei Betätigung der Paniktaste in Ajax Apps

Ein Administrator oder PRO mit Systemkonfigurationsrechten kann die Reaktion des Bedienteils bei Betätigung der Paniktaste in Ajax Apps einstellen. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie die Ajax App.
2. Gehen Sie auf die Registerkarte **Geräte** .
3. Wählen Sie eine Hub-Zentrale aus und gehen Sie zu deren **Einstellungen** .
4. Wählen Sie das Menü **Service**.
5. Gehen Sie zum Menü **Töne und Warnungen**.
6. Aktivieren Sie die Funktion **Wenn die Paniktaste in der App gedrückt wird**.
7. Klicken Sie auf **Zurück**, um die neuen Einstellungen zu speichern.

Anzeige des Bedienteils nach Alarmauslösung

0:00 / 0:03

Das Bedienteil kann durch eine LED-Anzeige über die Auslösung im scharfgeschalteten System informieren.

Die Option funktioniert wie folgt:

1. Das System registriert einen Alarm.

2. Das Bedienteil gibt ein Alarmsignal aus (falls aktiviert). Die Dauer und Lautstärke des Signals hängt von den **Geräteeinstellungen** ab.
3. Die LED des Bedienteils blinkt zweimal (einmal alle 3 Sekunden), bis das System unscharf geschaltet wird.

Dank dieser Funktion können die Benutzer des Systems und die Patrouillen der Sicherheitsfirma verstehen, dass der Alarm aufgetreten ist.

> Die Anzeige nach Alarmauslösung durch das KeyPad Outdoor Jeweller funktioniert nicht für immer aktive Melder, wenn der Melder ausgelöst wurde, als das System unscharf geschaltet war.

So aktivieren Sie die Anzeige nach Alarmauslösung für KeyPad Outdoor Jeweller in Ajax PRO App:

1. Gehen Sie zu den Einstellungen der Hub-Zentrale:
   - Hub-Zentrale → Einstellungen ⚙ → Service → LED-Anzeige.
2. Legen Sie fest, welche Ereignisse durch zweimaliges Blinken der LED am KeyPad Outdoor Jeweller angezeigt werden sollen, bevor das System unscharf geschaltet wird:
   - Bestätigter Einbruch-/Notfallalarm.
   - Einzelner Einbruch-/Notfallalarm.
   - Deckelöffnung.
3. Wählen Sie das gewünschte KeyPad Outdoor Jeweller im Menü **Geräte** aus. Tippen Sie auf **Zurück**, um die Parameter zu speichern.
4. Tippen Sie auf **Zurück**. Es werden alle Werte übernommen.

Glockenton beim Öffnen

Wenn der **Glockenton beim Öffnen** aktiviert ist, benachrichtigt KeyPad Outdoor Jeweller den Benutzer mit einem kurzen Piepton, wenn die Öffnungsmelder beim Unscharfschalten des Systems ausgelöst werden. Diese Funktion wird z. B. in Geschäften verwendet, um Mitarbeiter zu benachrichtigen, dass jemand das Gebäude betreten hat.

Die Konfiguration der Benachrichtigungen erfolgt in zwei Schritten: Einrichten des Bedienteils und Einrichten der Öffnungsmelder. **Dieser Artikel** enthält weitere Informationen über **Türglocke** und die Einrichtung von Meldern.

So stellen Sie die Reaktion des Bedienteils:

1. Öffnen Sie die Ajax App.
2. Gehen Sie auf die Registerkarte **Geräte**.
3. Wählen Sie KeyPad Outdoor Jeweller und gehen Sie zu den **Einstellungen**.
4. Gehen Sie zum Menü **Akustische Signalisierung** → **Piepton-Einstellungen**.
5. Aktivieren Sie den Schalter **Glockenton beim Öffnen** in der Kategorie **Piepton bei Unscharfschaltung**.
6. Stellen Sie die gewünschte Lautstärke der Benachrichtigungen ein.
7. Tippen Sie auf **Zurück**, um die Einstellungen zu speichern.

Wenn die Einstellungen korrekt vorgenommen wurden, erscheint ein **Glockensymbol** auf der Registerkarte **Kontrolle** in der Ajax App. Tippen Sie darauf, um die Türglocke zu aktivieren oder zu deaktivieren.

Einstellung der Codes

In Ajax PRO Apps können Sie in den Einstellungen der Hub-Zentrale die Anforderungen an die Länge der Passcodes festlegen, die für die Benutzerautorisierung und den Zugriff auf das System verwendet werden. Sie können die Option **Flexibel (4 bis 6 Symbole)** wählen oder eine feste Codelänge festlegen: **4 Symbole**, **5 Symbole** oder **6 Symbole**.

Die Einstellung einer festen Codelänge setzt alle zuvor konfigurierten Zugangscodes zurück.

Die feste Codelänge ist für die Funktion **Einfache Scharf-/Unscharfschaltung** benötigt, mit der das System nach Eingabe eines Codes oder nach Verwendung eines Zugriffsgeräts ohne Drücken der **OK**-Taste am Bedienfeld deaktiviert werden kann.

Bedienteil-Zugangscodes

So stellen Sie Bedienteil-Codes und Bedrohungscodes ein:

1. Gehen Sie in der Ajax App auf die Registerkarte **Geräte** .
2. Wählen Sie das Bedienteil aus, für das Sie einen Zugangscode einrichten möchten.
3. Gehen Sie zu den **Einstellungen** .
4. Wählen Sie im Menü **Zugriffsoptionen** die Option **Nur Bedienteil-Codes** oder **Bedienteil- oder Benutzercodes**.
5. Öffnen Sie das Menü **Bedienteil-Code**.
6. Stellen Sie den Bedienteil-Code ein. Enthält 4 bis 6 Ziffern.
7. Tippen Sie auf **Fertig**.
8. Öffnen Sie das Menü **Bedrohungscode**.
9. Legen Sie den Bedienteil-Bedrohungscode fest. Enthält 4 bis 6 Ziffern.
10. Tippen Sie auf **Fertig**.

Zugangscodes für Benutzer

So stellen Sie einen persönlichen Code und einen persönlichen Bedrohungscode ein:

1. Wählen Sie den Space in der Ajax App.
2. Gehen Sie zum Menü **Einstellungen** .

3. Öffnen Sie das Menü **Benutzer**.
4. Suchen Sie Ihr Konto in der Liste und tippen Sie es an.
5. Gehen Sie zum Menü **Zugangscode-Einstellungen**.
6. Stellen Sie den **Benutzercode** ein. Enthält 4 bis 6 Ziffern.
7. Tippen Sie auf **Speichern**.
8. Stellen Sie den **Bedrohungscode** ein. Enthält 4 bis 6 Ziffern.
9. Tippen Sie auf **Speichern**.
10. Tippen Sie auf **Zurück**, um die Einstellungen zu speichern.

Codes für nicht registrierte Benutzer

So stellen Sie einen Zugangscode für einen Benutzer ohne Konto ein:

1. Wählen Sie eine Hub-Zentrale in der Ajax App aus.
2. Gehen Sie zum Menü **Einstellungen** ⚙.
3. Gehen Sie zum Menü **Bedienteil-Zugangscodes**.
4. Klicken Sie auf **Code hinzufügen**. Geben Sie einen **Namen** und einen **Zugangscode** ein. Enthält 4 bis 6 Ziffern.
5. Klicken Sie auf **Hinzufügen**, um die Daten zu speichern.

So stellen Sie einen Bedrohungscode für einen Benutzer ohne Konto ein:

1. Wählen Sie in den Einstellungen der Hub-Zentrale das Menü **Bedienteil-Zugangscodes**.
2. Wählen Sie den gewünschten, nicht registrierten Benutzer aus.
3. Klicken Sie auf **Bedrohungscode hinzufügen**. Stellen Sie den Code ein. Enthält 4 bis 6 Ziffern.
4. Tippen Sie auf **Fertig**.

Für nicht registrierte Benutzer kann ein Administrator oder ein PRO-Benutzer mit Systemkonfigurationsrechten den Zugang zur Sicherheitsverwaltung anpassen. Aktivieren Sie zuerst den Gruppenmodus. Wählen Sie das Menü **Bedienteil-Zugangscodes** in den Einstellungen der Hub-Zentrale, suchen Sie den gewünschten Benutzer und stellen Sie im Menü **Sicherheitsverwaltung** die entsprechenden Parameter ein.

Einsatzteam-Code

Nur ein PRO-Benutzer mit Systemkonfigurationsrechten kann in den **Ajax PRO Apps** Einsatzteam-Codes erstellen und konfigurieren. Weitere Informationen zur Konfiguration dieser Funktion finden Sie in **diesem Artikel**.

Karten und Handsender

KeyPad Outdoor Jeweller kann mit **Tag**-Handsendern, **Pass**-Karten und Zugriffsgeräten anderer Hersteller verwendet werden, welche die DESFire®-Technologie unterstützen.

Bevor Sie Zugriffsgeräte von Drittanbietern hinzufügen, die DESFire® unterstützen, stellen Sie bitte sicher, dass diese über genügend freien Speicherplatz verfügen, um das neue Bedienteil zu unterstützen. Vorzugsweise sollte das Zugriffsgerät eines Drittanbieters vorformatiert werden.

Wie Sie **Tag** oder **Pass** zurücksetzen können, erfahren Sie in diesem Artikel.

Die maximale Anzahl der hinzugefügten Pass- und Tag-Geräte hängt vom Modell der Hub-Zentrale ab. Die hinzugefügten Pass- und Tag-Geräte haben keinen Einfluss auf das Gesamtgerätelimit der Hub-Zentrale.

Gerätekompatibilität prüfen

Tag oder Pass hinzufügen

1. Öffnen Sie die Ajax App.
2. Wählen Sie den Space mit der Hub-Zentrale aus, der Sie einen Tag oder Pass hinzufügen möchten.
3. Gehen Sie auf die Registerkarte **Geräte** .

> Stellen Sie sicher, dass die Funktion **Karten-/Anhängerleser** in den Einstellungen mindestens eines Bedienteils aktiviert ist.

4. Klicken Sie auf **Gerät hinzufügen**.
5. Wählen Sie **Karte/Anhänger hinzufügen**.
6. Geben Sie den Typ (Tag oder Pass), die Farbe, den Gerätenamen und den Benutzer (falls nötig) an.
7. Tippen Sie auf **Weiter**. Danach schaltet die Hub-Zentrale in den Geräteregistrierungs-Modus.
8. Wählen Sie ein kompatibles Bedienteil mit aktiviertem **Karten-/Anhängerleser**. Drücken Sie die **OK**-Taste, um das Tastenfeld in den Protokollierungsmodus des Zugangsgeräts zu schalten.
9. Halten Sie Pass oder Tag mit der breiten Seite für einige Sekunden an das Bedienteil. Nach erfolgreichem Hinzufügen erhalten Sie eine Benachrichtigung in der Ajax App.

Wenn die Verbindung fehlschlägt, versuchen Sie es nach 5 Sekunden erneut. Bitte beachten Sie, dass Sie beim Hinzufügen eines neuen Geräts eine entsprechende Benachrichtigung in der Ajax App erhalten, wenn die maximale Anzahl von Tag- oder Pass-Geräten bereits zur Hub-Zentrale hinzugefügt wurde.

Tag und Pass können mit mehreren Hub-Zentralen gleichzeitig arbeiten. Die maximale Anzahl von Hub-Zentralen beträgt 13. Wenn Sie versuchen, einen Tag oder Pass zu einer Hub-Zentrale hinzuzufügen, der bereits das Gerätelimit erreicht hat, erhalten Sie eine entsprechende Benachrichtigung. Um solche Zugriffsgeräte mit einer neuen Hub-Zentrale zu verknüpfen, müssen sie zurückgesetzt werden.

Wenn Sie einen weiteren Tag oder Pass hinzufügen möchten, klicken Sie in der App auf **Weitere Karte/Anhänger hinzufügen**. Wiederholen Sie die Schritte 6 bis 9.

Tag oder Pass löschen (zurücksetzen)

Beim Zurücksetzen werden alle Einstellungen und Verbindungen von Handsendern und Karten gelöscht. In diesem Fall werden die zurückgesetzten Tag- und Pass-Geräte nur von der Hub-Zentrale gelöscht, von der aus die Zurücksetzung durchgeführt wurde. Bei anderen Hub-Zentralen wird Tag oder Pass weiterhin in der App angezeigt, kann aber nicht zur Steuerung der Sicherheitsmodi verwendet werden. Diese Geräte müssen manuell gelöscht werden.

1. Öffnen Sie die Ajax App.
2. Wählen Sie einen Space aus.
3. Gehen Sie auf die Registerkarte **Geräte** .
4. Wählen Sie ein kompatibles Bedienteil aus der Geräteliste aus.

Stellen Sie sicher, dass die **Karten-/Anhängerleser** in den Bedienteileinstellungen aktiviert ist.

5. Gehen Sie zu den Einstellungen des Bedienteils, indem Sie auf das Symbol klicken.
6. Klicken Sie auf **Karte/Anhänger zurücksetzen**.

7. Klicken Sie auf **Weiter**.

8. Wählen Sie ein kompatibles Bedienteil mit aktiviertem **Karten-/Anhängerleser**. Drücken Sie die **OK**-Taste, um das Bedienteil in den Modus zum Zurücksetzen des Zugangsgeräts zu schalten.

9. Halten Sie Pass oder Tag mit der breiten Seite für einige Sekunden an das Bedienteil. Wenn die Formatierung erfolgreich war, erhalten Sie eine Benachrichtigung in der Ajax App. Wenn das Zurücksetzen fehlschlägt, versuchen Sie es erneut.

Wenn Sie einen weiteren Tag oder Pass zurücksetzen müssen, klicken Sie in der App auf **Weiteres Gerät zurücksetzen**. Wiederholen Sie Schritt 9.

Bluetooth-Einstellung

KeyPad Outdoor Jeweller unterstützt die Steuerung von Sicherheitsmodi, indem ein Smartphone an den Sensor gehalten wird. Die Sicherheitssteuerung erfolgt über einen Bluetooth-Kommunikationskanal. Diese Methode ist praktisch, sicher und schnell, da kein Kennwort eingegeben, kein Telefon zum Bedienteil hinzugefügt und kein Tag oder Pass verwendet werden muss, der verloren gehen könnte.

> ⚠ Die Bluetooth-Authentifizierung ist nur für Benutzer des Ajax Security System verfügbar.

So aktivieren Sie die Bluetooth-Authentifizierung in der App

1. Fügen Sie KeyPad Outdoor Jeweller zum System hinzu.

2. Aktivieren Sie den Bluetooth-Sensor des Bedienteils:

   - **Geräte** → **KeyPad Outdoor Jeweller** → **Einstellungen** ⚙ → Aktivieren Sie den **Bluetooth**-Schalter.

3. Tippen Sie auf **Zurück**, um die Einstellungen zu speichern.

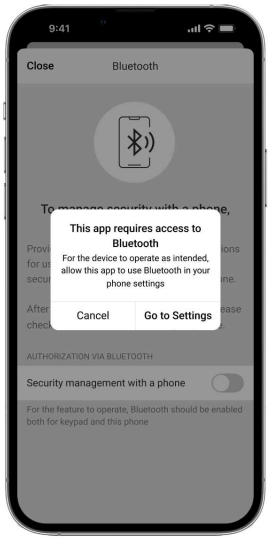
So konfigurieren Sie die Bluetooth-Authentifizierung

1. Öffnen Sie die Ajax Security System App und wählen Sie den Space aus, zu dem das KeyPad Outdoor Jeweller mit aktivierter Bluetooth-Authentifizierung hinzugefügt wird. Standardmäßig ist die Authentifizierung mit Bluetooth für alle Benutzer eines solchen Systems verfügbar.

> So verbieten Sie die Bluetooth-Authentifizierung für bestimmte Benutzer:
>
> 1. Wählen Sie auf der Registerkarte **Geräte** die Hub-Zentrale aus und gehen Sie zu deren Einstellungen .
> 2. Öffnen Sie das Menü **Benutzer** und wählen Sie den gewünschten Benutzer aus der Liste aus.
> 3. Deaktivieren Sie im Menü **Berechtigungen** die Funktion **Sicherheitsmanagement über Bluetooth**.

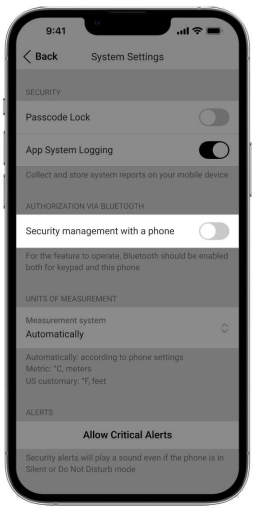
2. Erlauben Sie der Ajax Security System App, Bluetooth zu verwenden, wenn dies nicht bereits zuvor erlaubt wurde. In diesem Fall erscheint eine Warnung ⚠ in den **Zuständen** von KeyPad Outdoor Jeweller. Wenn Sie auf das Symbol ⓘ drücken, öffnet sich ein Fenster mit Erläuterungen zum weiteren Vorgehen. Aktivieren Sie das **Scharf-/Unscharfschalten mit Smartphone** im unteren Bereich des geöffneten Fensters.

Erlauben Sie der App, Geräte in der Nähe zu finden und sich mit ihnen zu verbinden. Das Popup-Fenster für Android- und iOS-Smartphones kann unterschiedlich aussehen.



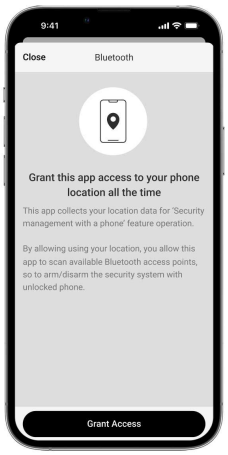
Das **Scharf-/Unscharfschalten mit Smartphone** kann auch in den Einstellungen der App aktiviert werden:

- Klicken Sie auf das Symbol ☰ in der oberen linken Ecke des Bildschirms und wählen Sie das Menü **App Einstellungen**.
- Öffnen Sie das Menü **Systemeinstellungen** und aktivieren Sie den Schalter **Scharf-/Unscharfschalten mit Smartphone**.



3. Es wird empfohlen, **Geofence** einzurichten, um einen stabilen Betrieb der Bluetooth-Authentifizierung zu gewährleisten. Die Warnung ⚠ erscheint bei den Zuständen von KeyPad Outdoor Jeweller, wenn **Geofence** deaktiviert ist und die App den Smartphone-Standort nicht verwenden darf. Wenn Sie auf das Symbol ⓘ klicken, öffnet sich ein Fenster mit Erläuterungen zum weiteren Vorgehen.

Die Bluetooth-Authentifizierung kann instabil sein, wenn die Funktion **Geofence** deaktiviert ist. Die Benutzer müssen die App starten und minimieren, sobald das System in den Schlafmodus wechselt.



Benutzer können das System schneller über Bluetooth steuern, wenn die **Geofence-Funktion** aktiviert und konfiguriert ist. Es genügt, das Telefon zu entsperren und es an den Bedienteilsensor zu halten.

Geofence einrichten

4. Aktivieren Sie die Funktion **Hintergrundbetrieb für Steuerung der Sicherheitsmodi über Bluetooth**. Gehen Sie dazu auf **Geräte** ▪ → **Hub-Zentrale** → **Einstellungen** ⚙ → **Geofence**.

5. Stellen Sie sicher, dass Bluetooth auf Ihrem Smartphone aktiviert ist. Wenn Bluetooth deaktiviert ist, erscheint die Warnung ⚠ in den **Zuständen** des Bedienteils. Wenn Sie auf das Symbol ⓘ drücken, öffnet sich ein Fenster mit Erläuterungen zum weiteren Vorgehen.

6. Aktivieren Sie den Schalter **Keepalive-Service** in den App-Einstellungen für Android-Smartphones. Klicken Sie dazu in der linken oberen Bildschirmecke auf ☰ → **App Einstellungen** → **Systemeinstellungen**.

Steuerung der Sicherheit

Mit Codes, Tag/Pass oder einem Smartphone können Sie den **Nachtmodus** und die Sicherheit des gesamten Objekts oder einzelner Gruppen steuern. Der Benutzer oder PRO mit Systemkonfigurationsrechten kann Zugangscodes einrichten. **Dieser Abschnitt** enthält Informationen über das Hinzufügen von Tag oder Pass zur Hub-Zentrale. Für die Steuerung mit einem Smartphone passen Sie die entsprechenden **Bluetooth-Parameter** in den Einstellungen des Bedienteils an. Schalten Sie auf dem Smartphone Bluetooth und die Standortbestimmung ein und entsperren Sie den Bildschirm.

Wenn ein persönlicher oder Zugangscode, Tag/Pass oder ein Smartphone verwendet wird, wird der Name des Benutzers, der den Sicherheitsmodus geändert hat, im Ereignis-Feed der Hub-Zentrale und in der Benachrichtigungsliste angezeigt. Wenn ein allgemeiner Code verwendet wird, wird der Name des Bedienteils angezeigt, von dem aus die Änderung des Sicherheitsmodus vorgenommen wurde.

> ℹ KeyPad Outdoor Jeweller wird für die in den Einstellungen angegebene Zeit gesperrt, wenn innerhalb von 1 Minute dreimal hintereinander ein falscher Code eingegeben oder ein nicht verifiziertes Zutrittsgerät vorgelegt wird. Die entsprechenden Benachrichtigungen werden an die Benutzer und die Leitstelle des Sicherheitsunternehmens gesendet. Ein Benutzer oder ein PRO mit Systemkonfigurationsrechten kann das KeyPad Outdoor Jeweller in der Ajax App freischalten.

Die Schrittfolge zum Ändern des Sicherheitsmodus mit dem Bedienteil hängt davon ab, ob die Optionen **Vorabautorisierung**, **Autorisierung mit Code bestätigen** und **Einfacher Wechsel des Scharfschaltmodus** in den Einstellungen des KeyPad Outdoor Jeweller aktiviert sind.

Mit Tag, Pass oder einem Smartphone

1. Halten Sie Tag, Pass oder ein Smartphone an das Bedienteil.
2. Geben Sie den erforderlichen Code ein, wenn die Funktion **Autorisierung mit Code bestätigen** aktiviert ist.
3. Drücken Sie die **OK**-Taste auf dem Bedienteil, um das System scharf oder unscharf zu schalten.

Wenn die Funktion **Einfache Scharf-/Unscharfschaltung** aktiviert ist, ist es nicht erforderlich, nach der Verwendung des Zugriffsgeräts die **OK**-Taste zu drücken.

Mit Passcodes

> Falsch eingegebene Codes können durch ein langes Drücken auf die Taste gelöscht werden, wenn keine andere Aktion für ein langes Drücken konfiguriert ist.

Code	Beispiel	Hinweis
Verwaltung der Scharfschaltmodi des Objekts		
Bedienteil-Code Bedienteil-Bedrohungscode	1234 → OK	
Benutzercode Benutzer-Bedrohungscode	5 → * → 1234 → OK	**5** steht für die Benutzer-ID
Code eines nicht registrierten Benutzers	1234 → OK	

Bedrohungscode eines nicht registrierten Benutzers		
Einsatzteam-Code	1234 → OK	
Керування режимами охорони груп		
Bedienteil-Code Bedienteil-Bedrohungscode	1234 → ✳ → 2 → OK	**2** steht für die Gruppen-ID
Benutzercode Benutzer-Bedrohungscode	5 → ✳ → 1234 → ✳ → 2 → OK	**5** steht für die Benutzer-ID **2** steht für die Gruppen-ID
Code eines nicht registrierten Benutzers Bedrohungscode eines nicht registrierten Benutzers	1234 → ✳ → 2 → OK	**2** steht für die Gruppen-ID
Einsatzteam-Code	1234 → ✳ → 2 → OK	**2** steht für die Gruppen-ID

Erfahren Sie mehr über die Benutzer-ID

Erfahren Sie mehr über die Gruppen-ID

Autorisierung mit Code bestätigen

Die Funktion **Autorisierung mit Code bestätigen** ermöglicht die Einrichtung einer Zwei-Faktor-Authentifizierung für Benutzer beim Aktivieren oder Deaktivieren des Sicherheitssystems oder bestimmter Modi. Diese Definition bedeutet, dass der Benutzer zunächst ein Zugangsgerät (Pass, Tag oder Smartphone) verwenden und dann einen

Passcode eingeben muss, um seine Berechtigung für das System zu bestätigen.

Erfahren Sie mehr über die Funktion Autorisierung mit Code bestätigen

Verwaltung von Automatisierungsgeräten und Szenarien

> Stellen Sie sicher, dass in den Einstellungen des Bedienteils in Ajax Apps die Funktion **Automatisierungsgeräte steuern** für den primären oder sekundären Betriebsmodus konfiguriert ist.

So steuern Sie ein Automatisierungsgerät oder ein Szenario mit KeyPad Outdoor Jeweller:

1. Halten Sie ein Zutrittskontrollgerät an das Bedienteil oder geben Sie einen Passcode ein, um sich auf dem Bedienteil zu autorisieren.
2. Schalten Sie das Bedienteil durch langes Drücken der **OK**-Taste in den Modus **Automatisierungsgeräte steuern**, wenn dieser Modus nicht aktiv oder als Hauptbetriebsmodus eingestellt ist. Die **OK**-Taste leuchtet grün oder rot, je nach dem aktuellen Zustand des Automatisierungsgeräts.
3. Drücken Sie die **OK**-Taste, um den Zustand des Automatisierungsgeräts zu ändern oder ein Szenario auszuführen:
    - Wenn das Bedienteil ein Szenario **zum Umschalten des Zustands** verwaltet, sollte die LED-Anzeige der **OK**-Taste entsprechend dem Zustand des Automatisierungsgeräts wechseln.
    - Wenn das Bedienteil ein Szenario **mit voreingestellter Aktion** verwaltet, zeigt die LED-Anzeige der **OK**-Taste nicht den Zustand der Geräte an. Stattdessen zeigt es an, ob die eingestellte Aktion abgeschlossen ist oder nicht.

Die Schrittfolge für die Verwaltung der Automationsgeräte mit dem Bedienteil hängt davon ab, ob die Optionen **Vorabautorisierung** und **Einfache Gerätesteuerung** in den Einstellungen des KeyPad Outdoor Jeweller aktiviert sind.

Anzeige

KeyPad Outdoor Jeweller informiert den Benutzer über Alarme, Ein- und Ausgangsverzögerungen, den aktuellen Sicherheitsmodus, Störungen und andere Systemzustände mittels:

- des Ajax Logos, **OK**-Taste und Hintergrundbeleuchtung mit LED-Anzeige;
- des eingebauten Summer.

Ereignis	LED	Summer
Einschalten des Geräts	Das Logo leuchtet für ca. 0,5 s grün.	Weckton.
Einschalten des Geräts, das nicht zur Hub-Zentrale hinzugefügt wurde	Das Logo leuchtet zunächst grün auf und blinkt dann sechsmal rot. Anschließend folgen drei schnelle rote Blitze.	
Ausschalten des Geräts	Das Logo leuchtet rot auf und blinkt dreimal schnell rot.	
Das Gerät wird zur Hub-Zentrale hinzugefügt	Das Logo leuchtet für ca. 0,5 s grün.	
Das Gerät wird von der Hub-Zentrale gelöscht	Das Logo leuchtet 0,3 s lang rot auf, erlischt sechsmal für 0,3 s und blinkt dann dreimal schnell rot.	
Kurzer Tastendruck		Kurzer Piepton.
Das Bedienteil befindet sich im Modus **Scharf-/Unscharfschalten***	Das Logo leuchtet je nach Sicherheitsstatus grün oder rot.	
Das Bedienteil befindet sich im Modus **Automatisierungsgeräte steuern**	Die **OK**-Taste leuchtet grün oder rot, je nach Zustand des Automatisierungsgeräts.	

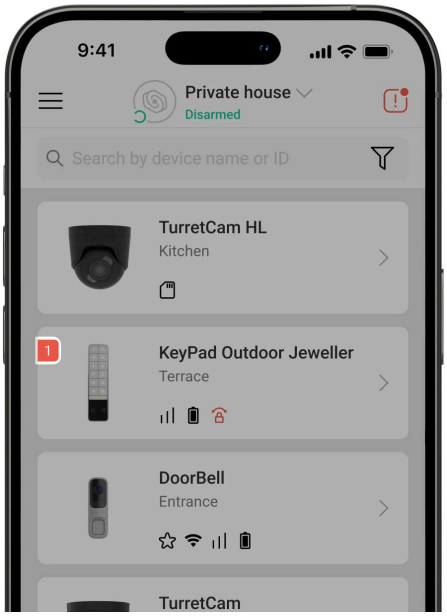
	Das Logo ist aus.	
Das Bedienteil befindet sich im Modus **Eingangsverzögerung aktivieren***	Das Logo leuchtet rot, wenn das System aktiviert ist. Bei einer Eingangsverzögerung blinkt das Logo rot und es ertönt ein Piepton.	
Scharfschaltung oder Aktivierung des **Nachtmodus**	Das Logo wechselt von grün zu rot.	Piepton für ca. 0,2 s.
Unscharschaltung	Das Logo wechselt von rot zu grün.	Doppelter Piepton für ca. 0,4 s.
Die **Paniktaste** (✳) wird gedrückt		Langer Piepton für ca. 0,5 s.
Die Funktionstaste (✳) wird gedrückt, um den eingegebenen Code zu löschen	Die Hintergrundbeleuchtung blinkt gleichzeitig mit einem kurzen Piepton.	Kurzer Piepton.
Falscher Passcode eingegeben	Die Hintergrundbeleuchtung leuchtet dreimal auf, während ein langer Piepton ertönt.	Langer Piepton für ca. 0,6 s.
Anfrage wird aufgrund fehlender Benutzerrechte oder einer Störung abgelehnt	Das Logo leuchtet dreimal gelb auf, während ein langer Signalton ertönt.	Langer Piepton für ca. 0,6 s.
Das Bedienteil ist gesperrt	Die Hintergrundbeleuchtung leuchtet dreimal auf, während ein langer Piepton ertönt.	Langer Piepton für ca. 0,6 s.
Systemintegritätsprüfung fehlgeschlagen	Das Logo leuchtet dreimal grün oder rot auf (je nach aktuellem Sicherheitszustand), während ein langer Piepton ertönt.	Langer Piepton für ca. 0,6 s.
Scharf-/Unscharfschalten ist untersagt	Das Logo leuchtet dreimal gelb auf, während ein langer Signalton ertönt.	Langer Piepton für ca. 0,6 s.
Sabotagealarm/Wiederherstellung	Das Logo leuchtet 0,7 s lang rot.	
Pass/Tag lesen ist erfolgreich	Die Hintergrundbeleuchtung erlischt für ca. 0,3 s.	Piepton für ca. 0,2 s.

Pass/Tag lesen ist fehlgeschlagen	Das Logo leuchtet gelb auf, während die Hintergrundbeleuchtung erlischt und ein langer Piepton ertönt.	Langer Piepton für ca. 1 s.
Authentifizierung per Smartphone ist erfolgreich	Die Hintergrundbeleuchtung erlischt für ca. 0,1 s.	Häufiges Piepen für ca. 0,2 s.
Authentifizierung per Smartphone ist fehlgeschlagen	Das Logo leuchtet gelb auf, während ein Piepton ertönt.	Langer Piepton für ca. 1 s.
Das Bedienteil ist bereit, Pass/Tag zu lesen	Die Hintergrundbeleuchtung leuchtet für 0,2 s auf und erlischt für 1 s, bis Pass/Tag gelesen wird.	
Pass/Tag erfolgreich hinzugefügt		Zwei kurze Pieptöne.
1. Das Hinzufügen von Pass/Tag ist fehlgeschlagen. 2. Ungültige Karte gelesen. 3. Beim Lesen eines Zugriffsgeräts sind andere Störungen aufgetreten.	Das Logo leuchtet für ca. 0,3 s gelb auf.	Langer Piepton für ca. 0,6 s.
Eingangs-/Ausgangsverzögerung	Bei einer Eingangsverzögerung leuchtet das Logo rot auf, und es ertönt ein Piepton. Bei einer Ausgangsverzögerung leuchtet das Logo grün auf, und es ertönt ein Piepton.	Kurzer Signalton einmal pro 1 s.
Systemwiederherstellung erforderlich (PD 6662:2017)	Das Logo leuchtet für ca. 0,1 s gelb auf, dann ertönt ein kurzer Piepton. Er wird dreimal wiederholt.	
Anzeige nach Alarmauslösung	Das Logo blinkt zweimal alle 3,4 s rot.	
Scharfschaltung unvollständig (PD 6662:2017)	Das Logo leuchtet ständig gelb.	Drei kurze Signaltöne für etwa 0,3 s alle 1 s.

Ein Gerät im System ist offline (UL)	Das Logo blinkt zweimal gleichzeitig gelb und es ertönt zweimal alle 1 Minute ein kurzer Piepton.	
Ein Gerät im System hat einen geringen Akkustand (UL)	Das Logo blinkt dreimal gleichzeitig gelb und alle 1 Minute ertönt ein kurzer Piepton mit Tonwechsel.	
Verzögertes Scharfschalten (vom Gerät initiiert) (PD 6662:2017)	Das Logo leuchtet alle 1 s für etwa 0,8 s grün auf.	
Verzögertes Scharfschalten (durch die App initiiert) (PD 6662:2017)	Das Logo leuchtet alle 1 s für ca. 0,8 Sekunden rot auf.	
Die Hub-Zentrale reagiert nicht	Das Logo leuchtet während eines langen Pieptons gelb auf.	Langer Piepton für ca. 0,5 s.
Der Akkustand ist niedrig	Das Logo leuchtet langsam gelb auf und erlischt langsam, nachdem der richtige Zugangscode eingegeben wurde.	
Der Akku ist vollständig entladen	Das Logo leuchtet langsam gelb auf und geht dann langsam aus. Dann schaltet sich das Gerät aus.	Langer Piepton für ca. 2 s.

* Wenn die Anzeige in den Bedienteil-Einstellungen aktiviert ist.

Störungen



Wenn das Gerät eine Störung feststellt (z. B. keine Verbindung über das Jeweller Protokoll), wird in der Ajax App in der linken oberen Ecke des Gerätesymbols ein Störungszähler angezeigt.

Alle Störungen werden unter **Gerätezuständen** angezeigt.. Felder mit Störungen sind rot markiert.

Eine Störung wird in folgenden Fällen angezeigt:

- Die Gerätetemperatur liegt außerhalb des zulässigen Bereichs.
- Der Gerätedeckel ist geöffnet (Sabotagealarm ausgelöst).
- Es besteht keine Verbindung zur Hub-Zentrale oder zum Funk-Signalverstärker über Jeweller.
- Der Akku des Geräts ist schwach.

Wartung

Überprüfen Sie regelmäßig die Funktionsfähigkeit des Gerätes. Das optimale Prüfintervall beträgt drei Monate. Reinigen Sie das Gerätegehäuse von Staub, Spinnweben und anderen Verunreinigungen, sobald diese auftreten. Verwenden Sie ein weiches, trockenes Tuch, das für die Reinigung von Geräten geeignet ist.

Verwenden Sie keine Reinigungsmittel, die Alkohol, Aceton, Benzin oder andere scharfe Lösungsmittel enthalten.

Technische Daten

Alle technischen Daten

Einhaltung von Normen

Einrichtung nach den Anforderungen EN 50131

Garantie

Die Garantie für die Produkte von Limited Liability Company „Ajax Systems Manufacturing“ gilt für 2 Jahre ab dem Kaufdatum.

Wenn das Gerät nicht ordnungsgemäß funktioniert, wenden Sie sich bitte zunächst an den technischen Support von Ajax. In den meisten Fällen können technische Probleme aus der Ferne gelöst werden.

Gewährleistungspflicht

Nutzungsvereinbarung

Technischen Support kontaktieren:

- E-Mail
- Telegram

Hergestellt von „AS Manufacturing“ LLC