KeyPad Benutzerhandbuch

Aktualisiert September 8, 2022



KeyPad ist eine kabellose Touch-Tastatur für den Innenbereich, die das Ajax-Sicherheitssystem verwaltet. 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 Code zu erraten. Außerdem kann KeyPad einen stillen Alarm auslösen, wenn der Bedrohungscode eingegeben wird.

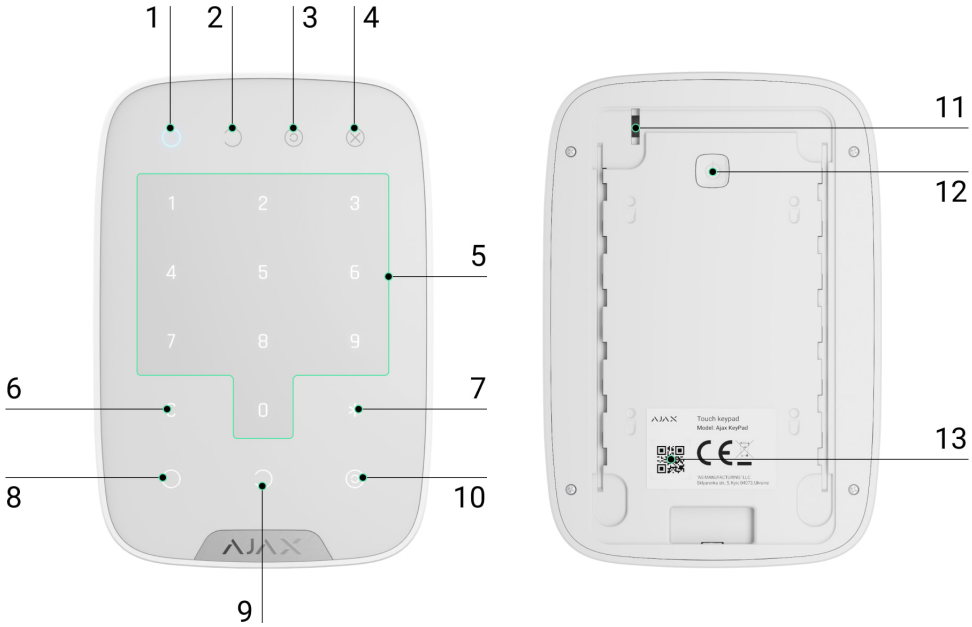
Das KeyPad ist über ein gesichertes **Jeweller**-Funkprotokoll mit dem Ajax-Sicherheitssystem verbunden und kommuniziert mit der **Hub-Zentrale** in einer Entfernung von bis zu 1.700 m in Sichtlinie.

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.

Tastatur KeyPad kaufen

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 perforiertes Teil ist erforderlich, um den Manipulationsschutz zu betätigen, falls

ein Versuch unternommen wird, das Gerät von der Oberfläche abzureißen).

Funktionsprinzip

KeyPad ist eine Touch-Tastatur zur Verwaltung des Ajax-Sicherheitssystems. Sie steuert die Sicherheitsmodi des gesamten Objekts oder einzelner Gruppen und ermöglicht die Aktivierung des **Nachtmodus**. Die Tastatur unterstützt die Funktion „Stiller Alarm“ – der Benutzer informiert das Sicherheitsunternehmen darüber, dass er gezwungen ist, das Sicherheitssystem zu deaktivieren, wobei Sirenentöne oder Signaltöne in den Ajax-Apps nicht ausgelöst werden.

Sie können die Sicherheitsmodi mit KeyPad mithilfe von Codes steuern. Bevor Sie den Code eingeben, sollten Sie die Tastatur durch Berühren aktivieren („aufwecken“). Wenn sie aktiviert ist, wird die Hintergrundbeleuchtung der Tasten eingeschaltet und die Tastatur piept.

KeyPad unterstützt die folgenden Codetypen:

- **Tastaturcode** – ein allgemeiner Code, der für die Tastatur festgelegt wird. Bei dessen Verwendung werden alle Ereignisse im Auftrag von Tastatur an Ajax-Apps übermittelt.
- **Benutzercode** – ein persönlicher Code, der für Benutzer eingerichtet wird, die ein Konto im System haben. Bei dessen Verwendung werden alle Ereignisse im Namen des Benutzers an Ajax-Apps übermittelt.
- **Tastatur-Zugangscode** wird für eine Person festgelegt, die im System nicht registriert ist. Bei dessen Verwendung werden Ereignisse mit einem diesem Code zugeordneten Namen an Ajax-Apps übermittelt.

> Die Anzahl der persönlichen Codes und Zugangscodes hängt vom Modell der Hub-Zentrale ab.

Die Helligkeit der Hintergrundbeleuchtung und die Lautstärke der Tastatur werden in ihren **Einstellungen** angepasst. Bei entladenen Batterien schaltet sich die Hintergrundbeleuchtung unabhängig von den Einstellungen auf der niedrigsten Stufe ein.

Wenn die Tastatur 4 Sekunden lang nicht berührt wird, reduziert KeyPad die Helligkeit der Hintergrundbeleuchtung, 8 Sekunden später aktiviert den Energiesparmodus und schaltet das Display aus. Wenn die Tastatur in den Energiesparmodus wechselt, werden die eingegebenen Befehle zurückgesetzt!

KeyPad unterstützt 4-6-stellige Codes. Die Eingabe des Codes muss durch Drücken einer der Tasten bestätigt werden: ◯ (Scharfschalten), ◯ (Unscharfschalten) und ◎ (Nachtmodus). Versehentlich eingegebene Zeichen werden mit der Taste C („Löschen“) zurückgesetzt.

KeyPad unterstützt die Steuerung von Sicherheitsmodi auch ohne Eingabe eines Codes, wenn die Funktion „Scharfschaltung ohne Passcode“ in den Einstellungen aktiviert ist. Diese Funktion ist standardmäßig deaktiviert.

Funktionstaste

Die KeyPad-Tastatur verfügt über eine Funktionstaste, die in 3 verschiedenen Modi verwendet werden kann:

- **Aus** — die Funktionstaste ist deaktiviert und führt bei Betätigung keine Befehle aus.
- **Alarm** — das System sendet einen Alarm an die Leitstelle und an alle Benutzer, wenn die Funktionstaste gedrückt wird.
- **Gekoppelten Rauchmelder Alarm stummschalten** — nach Drücken der Funktionstaste schaltet das System die Sirenen von Ajax-Feuermeldern stumm. Die Option funktioniert nur, wenn der Gekoppelte Rauchmelder Alarm aktiviert ist (Hub → Einstellungen → Service → Feuermelder Einstellungen).

Bedrohungscode

Mit einem Bedrohungscode kann man eine Unscharfschaltung simulieren. Im Gegensatz zur Paniktaste wird der Benutzer bei Eingabe dieses Codes aufgrund von Sirenensignal nicht gefährdet: Die Tastatur und die Ajax-App informieren über die erfolgreiche Unscharfschaltung des Systems. Gleichzeitig erhält das Sicherheitsunternehmen einen Alarm.

Verfügbare Arten von Bedrohungscodes:

- **Tastaturcode** — ein allgemeiner Bedrohungscode. Bei dessen Verwendung werden alle Ereignisse im Auftrag von Tastatur an Ajax-Apps übermittelt.
- **Benutzerbedrohungscode** — ein persönlicher Bedrohungscode, der für jeden Benutzer mit einem Konto im System eingerichtet wird. Bei dessen Verwendung werden alle Ereignisse im Namen des Benutzers an Ajax-Apps übermittelt.
- **Tastatur-Zugriffscode** — ein Bedrohungscode, der für eine Person eingerichtet wird, die im System nicht registriert ist. Bei dessen Verwendung werden Ereignisse mit einem diesem Code zugeordneten Namen an Ajax-Apps übermittelt.

Mehr erfahren

Sperre bei unbefugtem Zugriff

Wenn innerhalb von 1 Minute dreimal ein falscher Code eingegeben wird, wird die Tastatur für die in den Einstellungen festgelegte Zeit gesperrt. Während dieser Zeit ignoriert die Hub-Zentrale alle Codes und benachrichtigt die Benutzer des Sicherheitssystems und die Notruf- und Serviceleitstelle (NSL) über einen Versuch, den Code zu erraten.

Wenn die voreingestellte Sperrzeit abgelaufen ist, wird KeyPad automatisch entsperrt. Benutzer oder PRO-Benutzer mit Administratorrechten können die Tastatur jedoch über die Ajax-App entsperren.

Zweistufige Scharfschaltung

Das KeyPad kann zur zweistufigen Scharfschaltung verwendet werden. Wenn diese Funktion aktiviert ist, wird das System nur scharfgeschaltet, nachdem es mit SpaceControl erneut scharfgeschaltet wurde oder nachdem ein Zweitphasen-Melder in seinen Ausgangszustand zurückgekehrt hat (z. B. durch Schließen der Eingangstür, an der DoorProtect installiert ist).

Mehr erfahren

Jeweller-Datenübertragungsprotokoll

Die Tastatur verwendet das Jeweller-Funkprotokoll, um Ereignisse und Alarme zu übertragen. Dies ist ein kabelloses Zweiwege-Protokoll zur Datenübertragung, das eine schnelle und zuverlässige Kommunikation zwischen der Hub-Zentrale und den angeschlossenen Geräten ermöglicht.

Jeweller unterstützt die Blockverschlüsselung mit einem Floating-Key und die Authentifizierung von Geräten bei jeder Kommunikationssitzung, um Sabotage und Spoofing von Geräten zu verhindern. Das Protokoll umfasst regelmäßige Abfragen von Geräten in Intervallen von 12 bis 300 Sekunden (in der Ajax-App eingestellt) durch die Hub-Zentrale, um die Kommunikation mit allen Geräten zu überwachen und ihren Status in den Ajax-Apps anzuzeigen.

Mehr über Jeweller erfahren

Übertragung von Ereignissen an die Leitstelle

Das Ajax-Sicherheitssystem kann Alarme an die PRO Desktop-Überwachungs-App sowie an die Notruf- und Serviceleitstellen (NSL) über SurGard (Contact ID), SIA (DC-09), ADEMCO 685 und **andere proprietäre Protokolle** übertragen. Eine vollständige Liste der Notruf- und Serviceleitstellen, mit denen das Ajax-Sicherheitssystem verbindet werden kann, finden **Sie hier**.

KeyPad kann die folgenden Ereignisse übertragen:

- Bedrohungscode wird eingegeben.
- Die Paniktaste wird gedrückt (wenn die Funktionstaste als Paniktaste funktioniert).
- Die Tastatur ist wegen eines Versuchs, einen Code zu erraten, gesperrt.
- Sabotagealarm/Wiederherstellung.
- Verlust/Wiederherstellung der Hub-Zentrale-Verbindung.
- Die Tastatur wird vorübergehend aus-/eingeschaltet.
- Erfolgloser Versuch, das Sicherheitssystem scharf zu schalten (bei aktivierter Integritätsprüfung).

Wenn ein Alarm eingeht, versteht der Bediener der Überwachungsstation im Sicherheitsunternehmen, was passiert ist und wohin er das schnelle

Einsatzteam schicken muss. Die Adressierbarkeit jedes Ajax-Geräts ermöglicht es, nicht nur Ereignisse, sondern auch den Typ des Geräts, die Sicherheitsgruppe, den ihm zugewiesenen Namen und den Raum an die PRO Desktop-App oder an die NSL zu senden. Die Liste der übertragenen Parameter kann je nach NSL-Typ und gewähltem Kommunikationsprotokoll unterschiedlich sein.

Die Geräte-ID und die Schleifennummer (Zone) finden Sie unter der Geräte-Option Zustände in der Ajax-App.

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 **X** 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 geshaltet
Falscher Code	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
Die Hub-Zentrale reagiert nicht auf den Befehl — keine Verbindung	Langes Tonsignal, die LED-Anzeige für Störungen leuchtet
KeyPad wird nach 3 erfolglosen Versuchen, den Code zu erraten, gesperrt	Langes Tonsignal, Sicherheitsmodus-Anzeigen blinken gleichzeitig
Schwache Batterie	Nach dem Scharf-/Unscharfschalten des Systems blinkt die Störungsanzeige sanft. Die Tastatur ist gesperrt, während die Anzeige blinkt. Wenn KeyPad mit schwachen Batterien aktiviert wird, ertönt ein langer Signalton, die Störungsanzeige leuchtet sanft auf und schaltet sich dann aus

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.
4. Schalten Sie KeyPad ein, indem Sie die Netztaste 3 Sekunden lang gedrückt halten — es blinkt einmal mit der Hintergrundbeleuchtung der Tastatur.

Damit die Erkennung und das Verbinden erfolgen kann, sollte sich KeyPad 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.

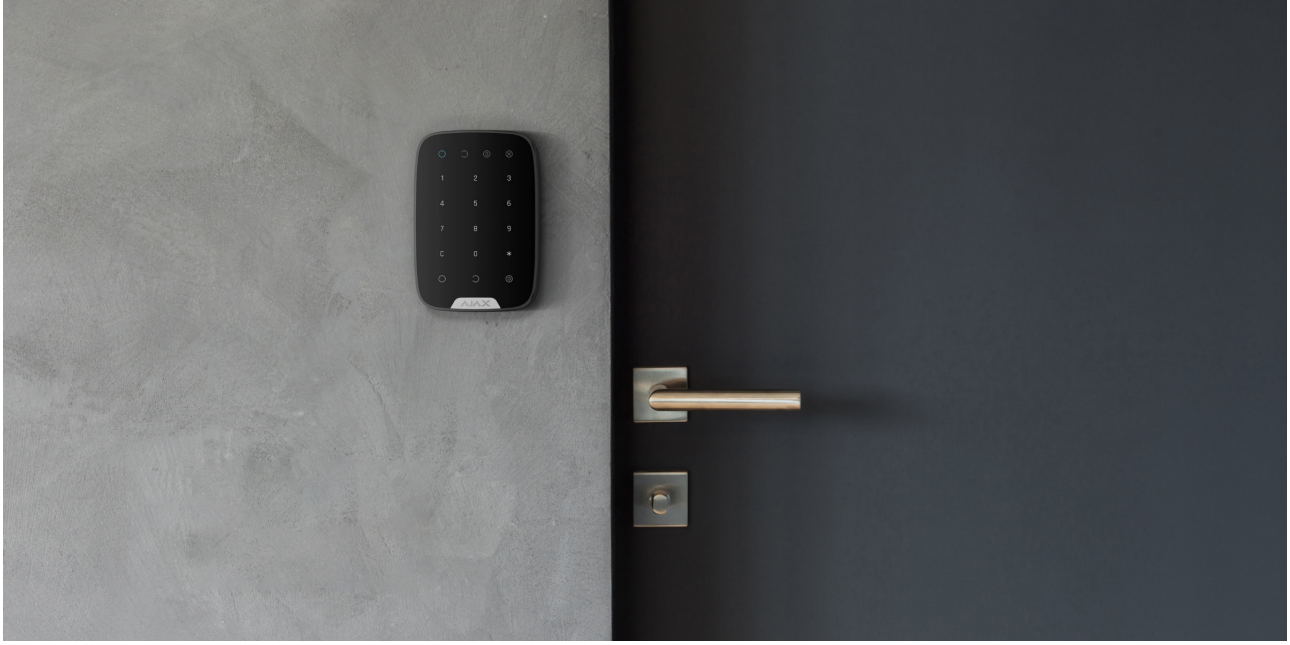
Wenn KeyPad nicht an die Hub-Zentrale angeschlossen werden konnte, schalten Sie es für 5 Sekunden aus und versuchen Sie es erneut.

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 Codes. Bevor Sie KeyPadnutzen, stellen Sie alleerforderlichen Codes fest: Tastaturcode (allgemeiner Passcode), persönliche Benutzercodes und Bedrohungscodes (allgemeine und persönliche).

Auswählen des Installationsortes



Der Installationsort 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.
3. In der Nähe von Metallobjekten und Spiegeln, die eine Dämpfung oder Schwächung des Funksignals verursachen können.
4. Außerhalb der Räumlichkeiten (im Freien).
5. Innerhalb von Räumen, in denen die Temperatur und die Luftfeuchtigkeit 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 am anderen Ort eine geringe oder instabile Signalstärke aufweist, verwenden Sie einen **signalverstärkenden 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	Bedeutung
Temperatur	Temperatur des Gerätes. Gemessen am Prozessor, und ändert sich allmählich
Jeweller-Signalstärke	Signalstärke zwischen der Hub-Zentrale und KeyPad
Akku-Ladung	Ladezustand der Batterie das Gerät. Es gibt zwei Zustände: • OK • Batterieladung niedrig **Anzeige der Batterieladung in Ajax-Apps**
Gehäusedeckel	Der Manipulationsmodus des Geräts, der auf Ablösung oder Beschädigung des Gehäuses reagiert

Verbindung	Verbindungsstatus zwischen der Hub-Zentrale und dem KeyPad
ReX	Zeigt an, ob ein **signalverstärkender Funk-Repeater** genutzt wird
Vorübergehende Deaktivierung	Zeigt den Status des Geräts an: aktiv, vom Benutzer vollständig deaktiviert, oder nur Benachrichtigungen über das Auslösen der Manipulationsschutztaste des Geräts deaktiviert
Firmware	Firmware-Version des Melders
Geräte-ID	Gerätekennung

Einstellungen

1. Geräte
2. KeyPad
3. Einstellungen

Einstellung	Bedeutung
Erstes Feld	Gerätename, kann bearbeitet werden
Raum	Auswählen des virtuellen Raums, dem das Gerät zugewiesen wird
Gruppenverwaltung	Auswählen der Sicherheitsgruppe, der KeyPad zugeordnet ist
Zugriffsoptionen	Auswahl der Verifizierungsart für Scharf-/Unscharfschalten • Nur Tastaturcodes • Nur Benutzerodes • Tastatur- und Benutzercodes Um das Einrichten von **Zugangscodes** für die im System nicht registrierten Personen zu aktivieren, wählen Sie die

	Optionen auf der Tastatur: **Nur Tastaturcodes** oder **Tastatur- und Benutzercodes**
Tastatur Passcode	Setzen eines Codes für das Scharf-/Unscharfschalten
Bedrohungscode	Einstellen eines **Nötigungscodes für stillen Alarm**
Funktionstaste	Funktionswahl der Taste * • **AUS** — Die Funktionstaste ist deaktiviert und führt beim Betätigen keine Befehle aus • **Alarm** — das System sendet einen Alarm an die Leitstelle und alle Benutzer, wenn die Funktionstaste gedrückt wird • **Gekoppelte Rauchmelder Alarm stummschalten** — bei Betätigung, wird der Brandalarm der FireProtect/FireProtect Plus Melder stummgeschaltet. Die Option funktioniert nur, wenn der Gekoppelte Rauchmelder Alarm aktiviert ist **Mehr erfahren**
Scharfschaltung ohne Passcode	Wenn das System aktiv ist, kann es durch Drücken der Taste „Scharfschalten“ ohne Code scharf geschaltet werden
Sperre bei unbefugtem Zugriff	Wenn die Funktion aktiv ist, wird die Tastatur nach dreimaliger Falscheingabe des Codes 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 Codes
Helligkeit	Helligkeit der Tastatur-Hintergrundbeleuchtung
Lautstärke bei Betätigung	Lautstärke des Signaltons
Alarmierung durch Sirene Wenn der Panikknopf gedrückt wird	Diese Einstellung erscheint dann, wenn für die **Funktionstaste** der Betriebsmodus **Alarm** ausgewählt ist.

	Wenn die Option aktiviert ist, werden durch Drücken der Funktionstaste die in der Einrichtung installierten Sirenen aktiviert
Jeweller Signalstärketest	Schaltet das Gerät in den Signalstärketestmodus
Signaldämpfungs-Prüfung	Schaltet die Tastatur in den Signalabschwächungs-Testmodus (verfügbar bei Geräten mit **Firmware-Version 3.50 und neuer**)
Vorübergehende Deaktivierung	Erlaubt dem Benutzer, das Gerät zu trennen, ohne es ganz aus dem System zu entfernen. Es stehen zwei Optionen zur Verfügung: • **Vollständig** — das Gerät führt keine Systembefehle aus, kann nicht über Automatisierungsszenarien angesteuert werden und das System ignoriert Alarme und andere Benachrichtigungen dieses Geräts • **Nur Deckel** — das System ignoriert nur Benachrichtigungen über das Auslösen der Manipulationsschutztaste (Abnehmen des Gerätedeckels) **Mehr über vorübergehende Deaktivierung erfahren**
Benutzerhandbuch	Öffnet das Benutzerhandbuch der Tastatur
Gerät entkoppeln	Trennt das Gerät von der Hub-Zentrale und löscht seine Einstellungen

Konfiguration der Codes

Mit dem Ajax-Sicherheitssystem können Sie einen Tastaturcode sowie persönliche Codes für Benutzer mit einem Konto im System einrichten.

Mit dem Update **OS Malevich 2.13.1** haben wir auch die Möglichkeit implementiert, einen Zugangscode für Benutzer zu erstellen, die kein Konto beim Ajax-Sicherheitssystem haben. Dies ist beispielsweise praktisch, um einem Reinigungsdienst Zugriff auf die Sicherheitsverwaltung zu ermöglichen. Weiter

unten finden Sie Informationen, wie man jeden Codetyp festlegen und verwenden kann.

So legen Sie einen Tastaturcode fest

1. Gehen Sie zu den Tastatur-Einstellungen.
2. Klicken Sie auf **Tastatur Passcode**.
3. Richten Sie gewünschten Tastaturcode ein.

So legen Sie einen Tastatur-Bedrohungscode fest

1. Gehen Sie zu den Tastatur-Einstellungen.
2. Klicken Sie auf **Bedrohungscode**.
3. Richten Sie gewünschten Tastatur-Bedrohungscode ein.

So legen Sie einen persönlichen Code für einen registrierten Benutzer fest

1. Gehen Sie zu den Profileinstellungen: **Hub-Zentrale** → **Einstellungen** → **Benutzer** → **Ihre Benutzereinstellungen**. In diesem Menü finden Sie auch die Benutzer-ID.
2. Klicken Sie auf **Passcode-Einstellungen**.
3. Richten Sie **Benutzercode** und **Benutzer-Bedrohungscode** ein.

Jeder Benutzer stellt einen persönlichen Code individuell ein.

So legen Sie eine Zugangscode für eine im System nicht registrierte Person fest

1. Gehen Sie zu den Hub-Zentrale-Einstellungen: **Hub-Zentrale** → **Einstellungen**.
2. Klicken Sie auf **Tastatur-Zugangscodes**.
3. Richten Sie **Name** und **Zugangscode** ein.

Um einen Bedrohungscode festzulegen, Einstellungen für den Zugriff auf Gruppen, Nachtmodus oder Code-ID zu ändern, den Code vorübergehend zu deaktivieren oder zu löschen, wählen Sie den gewünschten Code in der Liste aus und nehmen Sie Änderungen vor.

PRO-Benutzer oder ein Benutzer mit Administratorrechten kann einen Zugangscode einrichten oder seine Einstellungen ändern. Diese Funktion wird von den Hub-Zentralen mit OS Malevich 2.13.1 und neuer unterstützt. Das Modell Hub unterstützt Zugangscodes nicht.

Steuerung der Sicherheit über Codes

Sie können die Sicherheit eines ganzen Objekts oder einzelner Gruppen mit allgemeinen oder persönlichen Codes sowie mit Zugangscodes (von PRO-Benutzer oder einem Benutzer mit Administratorrechten konfiguriert) verwalten.

Sollte ein persönlicher Benutzercode 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 allgemeiner Code verwendet werden, wird der Name des Benutzers, der den Sicherheitszustand geändert hat, nicht angezeigt.

Tastatur-Zugangscodes werden von den Hub-Zentralen mit OS Malevich 2.13.1 und neuer unterstützt. Das Modell Hub unterstützt diese Funktion nicht.

Sicherheitsverwaltung eines ganzen Objekts mit einem allgemeinen Code

Geben Sie **den allgemeinen Code** ein und berühren Sie die Taste: **Scharfschalten** ◯ / **Unscharfschalten** ◯ / **Nachtmodus** ◎.

Beispiel: 1234 → ◯

Sicherheitsverwaltung einzelner Gruppen mit einem allgemeinen Code

Geben Sie **den allgemeinen Code** 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 **„Berechtigung Scharf- / Unscharfschalten**“ in den KeyPad-Einstellungen) brauchen Sie die Gruppen-ID nicht einzugeben. Zur Sicherheitsverwaltung dieser Gruppe genügt es, einen allgemeinen Code oder persönlichen Benutzercode einzugeben.

Bitte beachten Sie, dass Sie den **Nachtmodus** nicht mit einem allgemeinen Code verwalten können, wenn dem KeyPad eine Gruppe zugeordnet ist.

In einem solchen Fall können Sie den **Nachtmodus** nur mit einem persönlichen Benutzercode verwalten (sofern der Benutzer die entsprechenden Rechte hat).

Benutzerrechte im Ajax Sicherheitssystem

Sicherheitsverwaltung eines ganzen Objekts mit einem persönlichen Code

Geben Sie **Ihre Benutzer-ID** ein, drücken Sie *, geben Sie **Ihren persönlichen Benutzercode** ein und drücken Sie die Taste: **Scharfschalten** ◯ / **Unscharfschalten** ◯ / **Nachtmodus** ◎.

Beispiel: 2 → * → 1234 → ◯

Was ist eine Benutzer-ID

Sicherheitsverwaltung einzelner Gruppe mit einem persönlichen Code

Geben Sie die Benutzer-ID ein, drücken Sie *, geben Sie Ihren persönlichen Benutzercode ein, drücken Sie *, geben Sie die Gruppen-ID ein und drücken 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 KeyPad-Einstellungen) brauchen Sie die Gruppen-ID nicht einzugeben. Zur Sicherheitsverwaltung dieser Gruppe genügt es, einen persönlichen Benutzer einzugeben.

Sicherheitsverwaltung eines ganzen Objekts mit einem Zugangscode

Geben Sie den Zugangscode ein und drücken Sie die Taste: **Scharfschalten** ◯ / **Unscharfschalten** ◯ / **Nachtmodus** ◎.

Beispiel: 1234 → ◯

Sicherheitsverwaltung einzelner Gruppe mit einem Zugangscode

Geben Sie den Zugangscode ein, drücken Sie *, geben Sie die Gruppen-ID ein und drücken Sie die Taste: **Scharfschalten** ◯ / **Unscharfschalten** ◯ / **Nachtmodus** ◎.

Beispiel: 1234 → * → 2 → ◯

Was ist eine Gruppen-ID

Verwendung eines Bedrohungscodes

Der **Bedrohungscode** ermöglicht die Simulation der Systemunscharfschaltung. Die Ajax App und die am Objekt installierten Sirenen werden nicht ausgelöst, aber das Sicherheitsunternehmen und andere Systembenutzer werden über den Vorfall informiert. Sie können sowohl einen **persönlichen**, als auch **allgemeinen** Bedrohungscode verwenden. Sie können auch einen Bedrohungscodes für Personen einrichten, die nicht im System registriert sind.

Was ist ein Bedrohungscode und wie benutze ich diesen

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

So verwenden Sie einen allgemeinen Bedrohungscode:

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

Beispiel: 4321 → ◯

So verwenden Sie einen 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 → ◯

So verwenden Sie einen Bedrohungscode einer im System nicht registrierten Person:

Geben Sie **den Bedrohungscode**, der in **Tastatur-Zugangscodes** festgelegt wurde, ein und drücken Sie die Taste **Unscharfschalten** ◯.

Beispiel: 4567 → ◯

Wie funktioniert die Stummschaltung des Feueralarms

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:

- **Die Funktion „Gekoppelter Rauchmelder Alarm“ ist aktiviert und der Alarm hat sich bereits verbreitet**. Bei der ersten Betätigung der Funktionstaste wird der Alarm aller Brandmelder, bis auf den der ausgelösten Brandmelder,

auf stumm geschaltet. Bei der zweiten Betätigung werden auch die ausgelösten Brandmelder auf stumm geschaltet.

- **Die Ausbreitung des Alarms ist durch die Funktion „Gekoppelter Rauchmelder Alarm“ verzögert**. Beim Betätigen der Funktionstaste wird der Alarm des ausgelösten Melders (FireProtect/FireProtect Plus) auf stumm geschaltet.

Erfahren Sie mehr über den „Gekoppelten Rauchmelder Alarm“ von Brandmeldern

Mit dem Update OS Malevich 2.12 können Benutzer die Feueralarme in ihren Gruppen stummschalten, ohne dabei Melder in Gruppen zu beeinflussen, auf die sie keinen Zugriff haben.

Mehr erfahren

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 Schrauben an der Oberfläche, wobei Sie mindestens zwei Befestigungspunkte (einen davon — über dem Manipulationsschutz) verwenden müssen. Nachdem Sie andere Befestigungselemente ausgewählt haben, stellen Sie sicher, dass sie die Platte nicht beschädigen oder verformen.

   Doppelseitiges Klebeband darf nur zur vorübergehenden Befestigung von KeyPad verwendet werden. Das Band wird im Laufe der Zeit trocken laufen, was zum Herunterfallen der Tastatur und zur Beschädigung des Geräts führen kann.

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 Codes.

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

Batteriewechsel

Komplettsatz

1. KeyPad
2. SmartBracket-Montageplatte
3. Batterien AAA (vorinstalliert) — 4 Stk
4. Einbausatz
5. Schnellstartanleitung

Technische Daten

Sensortyp	Kapazitiv
Anti-Manipulationsschalter	Ja
Schutz gegen Codemanipulationen	Ja
Funkkommunikationsprotokoll	Jeweller **Mehr erfahren**
Funkfrequenzband	866,0 – 866,5 MHz 868,0 – 868,6 MHz 868,7 – 869,2 MHz 905,0 – 926,5 MHz 915,85 – 926,5 MHz 921,0 – 922,0 MHz Abhängig von der Verkaufsregion.
Kompatibilität	Funktioniert nur mit Ajax **hubs** und **Funksignal-Repeater**
Maximale HF-Ausgangsleistung	Bis zu 20 mW
Modulation des Funksignals	GFSK
Funkreichweite	Bis zu 1.700 m (wenn keine Hindernisse vorhanden sind)

	Mehr erfahren
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
Zertifizierung	Sicherheitsstufe 2, Umweltklasse II in Übereinstimmung mit den Anforderungen von EN 50131-1, EN 50131-3, EN 50131-5-3

Einhaltung von Standards

Garantie

Die Garantie für die Produkte der Limited Liability Company “Ajax Systems Manufacturing” gilt 2 Jahre nach dem Kauf und gilt nicht für die vorinstallierte Batterie.

Wenn das Gerät nicht ordnungsgemäß funktioniert, wenden Sie sich zunächst an den Support — in der Hälfte der Fälle können technische Probleme aus der Ferne behoben werden!

Der vollständige Text der Garantie

Abonnieren Sie unsere E-Mails über Sicherheit im Alltag. Ganz ohne Spam

Email

Abonnement