

Manual de utilizare al tastaturii

La curent8 septembrie 2022



KeyPad este o tastatură de interior sensibilă la atingere fără fir care gestionează sistemul de securitate Ajax. Proiectat pentru utilizare în interior. Cu acest dispozitiv, utilizatorul poate arma și dezarma sistemul și poate vedea starea securității acestuia. Tastatura este protejată împotriva încercărilor de a ghici codul și poate declanșa o alarmă silențioasă atunci când codul este introdus sub presiune.

Conectându-se la sistemul de securitate Ajax printr-un protocol radio securizat Jeweler, KeyPad comunică cu hub-ul la o distanță de până la 1.700 m în linie de vedere.

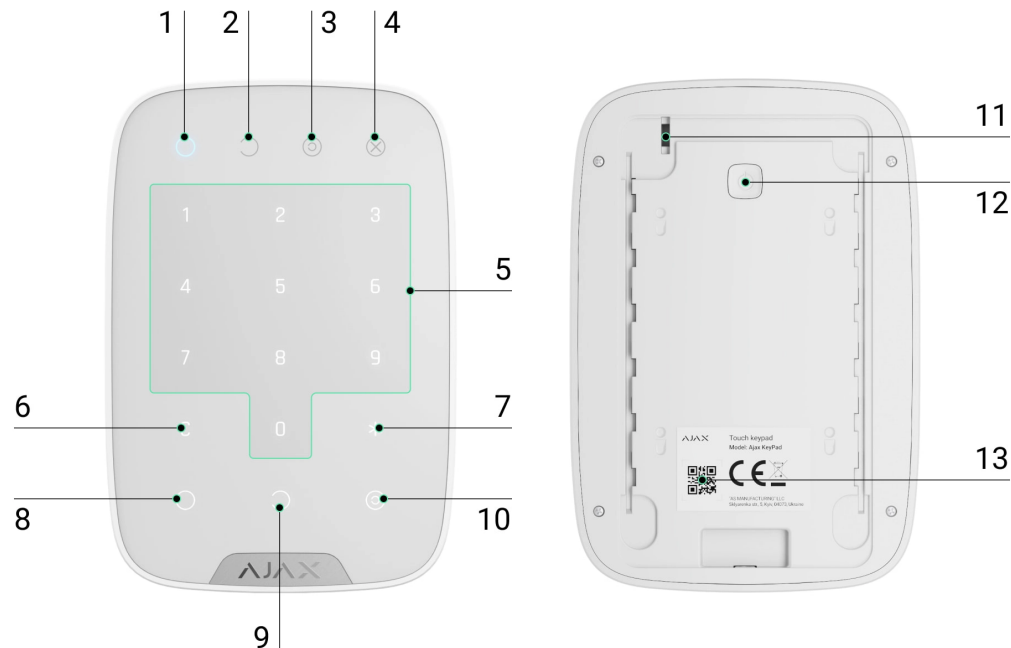


KeyPad funcționează numai cu hub-uri Ajax și nu acceptă conectarea prin modulele de integrare ocBridge Plus sau uartBridge.

Dispozitivul este configurat prin [aplicațiile Ajax](#) pentru iOS, Android, macOS și Windows.

Cumpărați tastatură KeyPad

Elemente funcționale



1. Indicator de mod armat
2. Indicator mod dezarmat
3. Indicator mod de noapte
4. Indicator de defecțiune
5. Blocul de butoane numerice
6. Butonul „Șterge”.
7. Butonul „Funcție”.
8. Butonul „Armare”.
9. Butonul „Dezarmare”.
10. Butonul „Mod noapte”.
11. Buton de manipulare

12. Buton Pornit/Oprit

13. cod QR

Pentru a scoate panoul SmartBracket, glisați-l în jos (partea perforată este necesară pentru acționarea tamperului în cazul oricărei încercări de a smulge dispozitivul de la suprafață).

Principiul de funcționare

KeyPad este o tastatură tactilă pentru gestionarea sistemului de securitate Ajax. Controlează modurile de securitate ale întregului obiect sau ale grupurilor individuale și permite activarea **modului Noapte**. Tastatura acceptă funcția de „alarma silențioasă” – utilizatorul informează compania de securitate despre faptul că a fost forțat să dezarmeze sistemul de securitate și nu este expus de sunetele sirenei sau de aplicațiile Ajax.

Puteți controla modurile de securitate cu KeyPad folosind coduri. Înainte de a introduce codul, ar trebui să activați („trezire”) tastatura atingând-o. Când este activat, iluminarea de fundal a butoanelor este activată, iar tastatura emite un bip.

KeyPad acceptă tipuri de cod după cum urmează:

- **Cod tastatură** – cod general care este configurat pentru tastatură. Când sunt utilizate, toate evenimentele sunt livrate în aplicațiile Ajax în numele tastaturii.
- **Cod utilizator** – cod personal care este configurat pentru utilizatorii conectați la hub. Când sunt utilizate, toate evenimentele sunt livrate în aplicațiile Ajax în numele utilizatorului.
- **Cod de acces la tastatură** – configurat pentru o persoană care nu este înregistrată în sistem. Când sunt utilizate, evenimentele sunt livrate în aplicațiile Ajax cu un nume asociat cu acest cod.



Numărul de coduri personale și coduri de acces depinde de modelul hub .

Luminozitatea luminii de fundal și volumul tastaturii sunt reglate în setările acesteia . Cu bateriile descărcate, lumina de fundal se aprinde la nivelul minim indiferent de setări.

Dacă nu atingeți tastatura timp de 4 secunde, KeyPad reduce luminozitatea luminii de fundal, iar 8 secunde mai târziu intră în modul de economisire a energiei și stinge afișajul. Pe măsură ce tastatura intră în modul de economisire a energiei, resetează comenzile introduse!

Tastatura acceptă coduri din 4 până la 6 cifre. Introducerea codului trebuie confirmată prin apăsarea unuia dintre butoanele: ○(braț), ○(dezarma) ☹(Modul de noapte). Toate caracterele introduse din greșală sunt resetate cu butonul C („Resetare”).

Tastatura acceptă, de asemenea, controlul modurilor de securitate fără introducerea unui cod, dacă funcția „Armare fără parolă” este activată în setări. Această funcție este dezactivată implicit.

Buton de funcție

Tastatura are un buton Function care funcționează în 3 moduri:

- **Off** – butonul este dezactivat. Nu se întâmplă nimic după ce faceți clic.
- **Alarmă** – după ce butonul Funcție este apăsat, sistemul trimite o alarmă către stația de monitorizare a companiei de securitate, către utilizatori și activează sirenele conectate la sistem.
- **Dezactivați alarmele detectoarelor de incendiu interconectate** – după ce butonul Funcție este apăsat, sistemul dezactivează sirenele detectorilor de incendiu Ajax. Opțiunea funcționează numai dacă Alarmerele FireProtect interconectate sunt activate (Hub → Setări → Service → Setări detectoare de incendiu).

Codul de constrângere

Codul de constrângere vă permite să simulați dezactivarea alarmei. Spre deosebire de butonul de panică, dacă acest cod este introdus, utilizatorul nu va fi compromis

de sunetul sirenei, iar tastatura și aplicația Ajax vor informa despre dezarmarea cu succes a sistemului. Totodată, firma de pază va primi o alarmă.

Sunt disponibile următoarele tipuri de coduri de constrângere:

- **Cod tastatură** – cod general de constrângere. Când sunt utilizate, evenimentele sunt livrate în aplicațiile Ajax în numele tastaturii.
- **Cod de constrângere utilizator** – cod de constrângere personal, configurat pentru fiecare utilizator conectat la hub. Când sunt utilizate, evenimentele sunt livrate în aplicațiile Ajax în numele utilizatorului.
- **Cod de acces la tastatură** – cod de constrângere configurat pentru o persoană care nu este înregistrată în sistem. Când sunt utilizate, evenimentele sunt livrate în aplicațiile Ajax cu un nume asociat cu acest cod.

[Află mai multe](#)

Blocare automată a accesului neautorizat

Dacă un cod greșit este introdus de trei ori în decurs de 1 minut, tastatura va fi blocată pentru timpul specificat în setări. În acest timp, hub-ul va ignora toate codurile și va informa utilizatorii sistemului de securitate și CMS-ului despre o încercare de a ghici codul.

Tastatura se va debloca automat după expirarea timpului de blocare definit în setări. Cu toate acestea, utilizatorul sau PRO cu drepturi de administrator poate debloca tastatura prin aplicația Ajax.

Armare în două etape

KeyPad participă la armare în două etape. Când această caracteristică este activată, sistemul se va arma numai după ce a fost rearmat cu SpaceControl sau după ce un detector din a doua etapă este restaurat (de exemplu, prin închiderea ușii din față pe care este instalat DoorProtect).

[Află mai multe](#)

Protocol de transfer de date pentru bijutier

Tastatura folosește protocolul radio Jeweler pentru a transmite evenimente și alarme. Acesta este un protocol de transfer de date fără fir bidirecțional care oferă o comunicare rapidă și fiabilă între hub și dispozitivele conectate.

Jeweler acceptă criptarea bloc cu o cheie flotantă și autentificarea dispozitivelor la fiecare sesiune de comunicare pentru a preveni sabotarea și falsificarea dispozitivului. Protocolul implică interogarea regulată a dispozitivelor de către hub la intervale de 12 până la 300 de secunde (setat în aplicația Ajax) pentru a monitoriza comunicarea cu toate dispozitivele și a afișa starea acestora în aplicațiile Ajax.

[Mai multe despre Bijutier](#)

Trimiterea evenimentelor către stația de monitorizare

Sistemul de securitate Ajax poate transmite alarme către aplicația de monitorizare PRO Desktop, precum și către stația centrală de monitorizare (CMS) prin SurGard (Contact ID), SIA (DC-09), ADEMCO 685 și [alte protocoale proprietare](#) . [Consultați aici](#) lista CMS-urilor la care vă puteți conecta sistemul de securitate Ajax .

Tastatura poate transmite următoarele evenimente:

- Este introdus codul de constrângere.
- Este apăsat butonul de panică (dacă butonul Funcție funcționează în modul butonul de panică).
- Tastatura este blocată din cauza unei încercări de a ghici un cod.
- Alarma de manipulare/recuperare.
- Pierderea/restabilirea conexiunii la hub.
- Tastatura este temporar oprită/pornită.
- Încercarea nereușită de armare a sistemului de securitate (cu Verificarea integrității activată).

Când se primește o alarmă, operatorul stației de monitorizare a companiei de pază știe ce s-a întâmplat și unde să trimită echipa de răspuns rapid. Adresabilitatea fiecărui dispozitiv Ajax vă permite să trimiteți nu numai evenimente, ci și tipul dispozitivului, grupul de securitate, numele atribuit acestuia și camera către Desktop-ul PRO sau către CMS. Lista parametrilor transmisi poate diferi în funcție de tipul CMS și de protocolul de comunicare selectat.



ID-ul dispozitivului și numărul buclei (zonei) pot fi găsite în stările sale în aplicația Ajax.

Indicație



Când atingeți KeyPad, se trezește evidențiind tastatura și indicând modul de securitate: Armat, Dezarmat sau Modul Noapte. Modul de securitate este întotdeauna actual, indiferent de dispozitivul de control care a fost folosit pentru a-l schimba (cheiul sau aplicația).

Eveniment	Indicație
Indicatorul de defecțiune X clipește	Indicatorul notifică lipsa comunicării cu deschiderea capacului hub-ului sau a tastaturii. Puteți verifica motivul defecțiunii în aplicația <u>Ajax Security System</u>
Butonul tastaturii a fost apăsat	Un bip scurt, LED-ul de stare de armare curent al sistemului clipește o dată
Sistemul este armat	Semnal sonor scurt, indicatorul LED pentru modul armat/mod noapte se aprinde
Sistemul este dezarmat	Două semnale sonore scurte, LED-ul dezarmat se

	aprinde
Parolă incorectă	Semnal sonor lung, iluminarea tastaturii clipește de 3 ori
O defecțiune este detectată la armare (de exemplu, detectorul este pierdut)	Un bip lung, LED-ul de stare de armare curent al sistemului clipește de 3 ori
Hub-ul nu răspunde la comandă – nicio conexiune	Semnal sonor lung, indicatorul de defecțiune se aprinde
Tastatura este blocată după 3 încercări nereușite de a introduce parola	Semnal sonor lung, indicatoarele modului de securitate clipesc simultan
Baterie descărcată	După armarea/dezarmarea sistemului, indicatorul de defecțiune clipește ușor. Tastatura este blocată în timp ce indicatorul clipește. Când activați KeyPad cu bateriile descărcate, va emite un bip cu un semnal sonor lung, indicatorul de defecțiune se aprinde ușor și apoi se oprește

Conectare

Înainte de a conecta dispozitivul:

1. Porniți hub-ul și verificați conexiunea acestuia la internet (sigla luminează alb sau verde).
2. Instalați [aplicația Ajax](#) . Creați contul, adăugați hub-ul în aplicație și creați cel puțin o cameră.
3. Asigurați-vă că hub-ul nu este armat și că nu se actualizează verificând starea acestuia în aplicația Ajax.



Numai utilizatorii cu drepturi de administrator pot adăuga un dispozitiv în aplicație

Cum se conectează KeyPad la hub:

1. Selectați opțiunea **Adăugați dispozitiv** în aplicația Ajax.
2. Denumiți dispozitivul, scanați/scrieți manual **codul QR** (situat pe corp și pe ambalaj) și selectați camera de locație.
3. Selectați **Adăugați** – va începe numărătoarea inversă.
4. Porniți tastatura ținând apăsat butonul de pornire timp de 3 secunde - va clipi o dată cu iluminarea de fundal a tastaturii.

Pentru ca detectarea și împerecherea să aibă loc, KeyPad ar trebui să fie amplasată în acoperirea rețelei wireless a hub-ului (la același obiect protejat).

O cerere de conectare la hub este transmisă pentru o perioadă scurtă de timp în momentul pornirii dispozitivului.

Dacă KeyPad nu s-a conectat la hub, opriți-l timp de 5 secunde și încercați din nou.

Dispozitivul conectat va apărea în lista de dispozitive din aplicație. Actualizarea stărilor dispozitivului din listă depinde de intervalul de ping al detectorului din setările hub (valoarea implicită este de 36 de secunde).



Nu există coduri prestabilite pentru KeyPad. Înainte de a utiliza KeyPad, setați toate codurile necesare: codul tastaturii (codul general), codurile personale de utilizator și codurile de constrângere (generale și personale).

Selectarea locației



Locația dispozitivului depinde de distanța sa față de hub și de obstacolele care împiedică transmiterea semnalului radio: pereți, podele, obiecte mari din interiorul încăperii.



Aparatul dezvoltat doar pentru utilizare în interior.

Nu instalați KeyPad:

1. Lângă echipamentele de transmisie radio, inclusiv cele care funcționează în rețele mobile 2G/3G/4G, routere Wi-Fi, transceiver, posturi radio, precum și un hub Ajax (folosește o rețea GSM).
2. Aproape de cablurile electrice.
3. Aproape de obiecte metalice și oglinzi care pot cauza atenuarea sau umbrirea semnalului radio.
4. În afara incintei (în aer liber).
5. În interiorul spațiilor cu temperatura și umiditatea peste limitele admise.
6. Mai aproape de 1 m de hub.



În timpul testării, nivelul semnalului este afișat în aplicație și pe tastatură cu indicatori de mod de securitate ○ (mod armat), ○ (mod dezarmat), ☾ (Mod noapte) și indicator de defecțiune **X**.

Dacă nivelul semnalului este scăzut (o bară), nu putem garanta funcționarea stabilă a dispozitivului. Luați toate măsurile posibile pentru a îmbunătăți calitatea semnalului. Cel puțin, mutați dispozitivul: chiar și o deplasare de 20 cm poate îmbunătăți semnificativ calitatea recepției semnalului.

Dacă, după mutare, dispozitivul are încă o putere scăzută sau instabilă a semnalului, utilizați un extintor de rază de semnal radio.

Tastatura este proiectată pentru funcționare atunci când este fixată pe suprafața verticală. Când folosiți KeyPad în mâini, nu putem garanta funcționarea cu succes a tastaturii senzorului.

state

1. Dispozitive 

2. Tastatura

Parametru	Sens
Temperatura	Temperatura aparatului. Măsurat pe procesor și se modifică treptat
Puterea semnalului de bijutier	Puterea semnalului dintre hub și KeyPad
Încărcare baterie	Nivelul bateriei dispozitivului. Două state disponibile: <ul style="list-style-type: none">• OK• Bateria descărcată

Cum este afișată încărcarea bateriei în aplicațiile Ajax

Capac	Modul de manipulare a dispozitivului, care reacționează la detașarea sau deteriorarea corpului
Conexiune	Starea conexiunii între hub și KeyPad
ReX	Afișează starea utilizării unui <u>extintor de rază de semnal radio</u>
Dezactivare temporară	Afișează starea dispozitivului: activ, complet dezactivat de utilizator sau numai notificările despre declanșarea butonului de manipulare a dispozitivului sunt dezactivate
Firmware	Versiunea de firmware a detectorului
Identificatorul dispozitivului	Identificatorul dispozitivului


Setări

1. Dispozitive 

2. Tastatura

3. Setări 

Setare	Sens
Primul câmp	Numele dispozitivului, poate fi editat
Cameră	Selectarea camerei virtuale căreia este alocat dispozitivul
Managementul grupului	Selectarea grupului de securitate căruia îi este atribuită KeyPad
Accesați Setări	Selectarea modului de verificare pentru armare/dezarmare <ul style="list-style-type: none">• Numai coduri de tastatură

	<ul style="list-style-type: none"> • Numai coduri de utilizator • Tastatură și coduri utilizator <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p> Pentru a activa codurile de acces configurate pentru persoanele care nu sunt înregistrate în sistem, selectați opțiunile de pe tastatură: numai coduri de tastatură sau coduri de tastatură și utilizator</p> </div>
Codul tastaturii	Setarea unui cod pentru armare/dezarmare
Codul de constrângere	Setarea <u>unui cod de constrângere pentru alarmă silențioasă</u>
Buton de funcție	<p>Selectarea funcției butonului *</p> <ul style="list-style-type: none"> • Off – butonul Funcție este dezactivat și nu execută nicio comandă atunci când este apăsat • Alarmă – prin apăsarea butonului Funcție, sistemul trimite o alarmă către stația de monitorizare a companiei de securitate și către toți utilizatorii • Dezactivați alarma detectorilor de incendiu interconectați – când este apăsat, dezactivează alarma de incendiu a detectorilor FireProtect/FireProtect Plus. Funcția funcționează numai dacă Alarma detectoare de incendiu interconectate este activată <p><u>Află mai multe</u></p>
Armare fără Parolă	Dacă este activ, sistemul poate fi armat apăsând butonul Armare fără cod
Acces neautorizat Blocare automată	Dacă este activă, tastatura este blocată pentru timpul prestabilit după introducerea unui cod incorect de trei ori la rând (în 30 de minute). În

	acest timp, sistemul nu poate fi dezarmat prin KeyPad
Timp de blocare automată (min)	Perioada de blocare după încercări greșite de a introduce un cod
Luminozitate	Luminozitatea luminii de fundal a tastaturii
Volum butoane	Volumul semnalului sonor
Alertă cu o sirenă dacă este apăsat butonul de panică	<p>Setarea apare dacă este selectat modul Alarmă pentru butonul Funcție .</p> <p>Dacă este activ, apăsarea butonului Funcție declanșează sirenele instalate la obiect</p>
Test de putere a semnalului de bijutier	Comută dispozitivul în modul de testare a intensității semnalului
Test de atenuare a semnalului	Comută tastatura în modul de testare a decolorării semnalului (disponibil în dispozitivele cu versiunea de firmware 3.50 și ulterioară)
Dezactivare temporară	<p>Permite utilizatorului să deconecteze dispozitivul fără a-l scoate din sistem.</p> <p>Sunt disponibile două opțiuni:</p> <ul style="list-style-type: none"> • În totalitate – dispozitivul nu va executa comenzi de sistem și nu va participa la scenarii de automatizare, iar sistemul va ignora alarmele dispozitivului și alte notificări • Numai capac – sistemul va ignora doar notificările despre declanșarea butonului de manipulare a dispozitivului <p><u>Aflați mai multe despre dezactivarea temporară a dispozitivelor</u></p>
Manualul utilizatorului	Deschide manualul de utilizare al tastaturii
Deconectați dispozitivul	Deconectează dispozitivul de la hub și șterge setările acestuia

Configurarea codurilor

Sistemul de securitate Ajax vă permite să configurați un cod de tastatură, precum și coduri personale pentru utilizatorii adăugați la hub.

Odată cu actualizarea OS Malevich 2.13.1 , am adăugat și posibilitatea de a crea coduri de acces pentru persoanele care nu sunt conectate la hub. Acest lucru este convenabil, de exemplu, pentru a oferi unei companii de curățenie acces la managementul securității. Vedeți mai jos cum să configurați și să utilizați fiecare tip de cod.


Pentru a seta codul tastaturii

1. Accesați setările tastaturii.
2. Selectați **codul tastaturii** .
3. Setati codul de tastatură dorit.

Pentru a seta codul de constrângere al tastaturii

1. Accesați setările tastaturii.
2. Selectați **Codul de constrângere** .
3. Setati codul de constrângere de la tastatură dorit.


Pentru a seta un cod personal pentru un utilizator înregistrat:

1. Accesați setările profilului: **Hub** → **Setări**  → **Utilizatori** → **Setări utilizator** . În acest meniu puteți găsi și ID-ul utilizatorului.
2. Faceți clic pe **Setări cod de acces** .
3. Setati **codul utilizatorului** și **codul de constrângere utilizator** .



Fiecare utilizator setează individual un cod personal!

Pentru a seta un cod de acces pentru o persoană neînregistrată în sistem

1. Accesați setările hub (**Hub** → **Setări** ).
2. Selectați **coduri de acces la tastatură** .
3. Configurați **numele** și **codul de acces** .

Dacă doriți să configurați un cod de constrângere, să modificați setările de acces la grupuri, modul Noapte, codul ID, să dezactivați temporar sau să ștergeți acest cod, selectați-l din listă și faceți modificări.



PRO sau un utilizator cu drepturi de administrator poate configura un cod de acces sau poate modifica setările acestuia. Această funcție este acceptată de hub-uri cu OS Malevich 2.13.1 și o versiune ulterioară. Codurile de acces nu sunt acceptate de panoul de control Hub.

Controlul securității prin coduri




Puteți controla securitatea întregii unități sau a grupurilor separate folosind coduri generale sau personale, precum și folosind coduri de acces (configurate de PRO sau un utilizator cu drepturi de administrator).

Dacă se folosește un cod de utilizator personal, numele utilizatorului care a armat/dezarmat sistemul este afișat în notificări și în fluxul de evenimente hub. Dacă se folosește un cod general, numele utilizatorului care a schimbat modul de securitate nu este afișat.



Codurile de acces la tastatură acceptă hub-uri cu OS Malevich 2.13.1 și o versiune ulterioară. Panoul de control al hub-ului nu acceptă această funcție .

Managementul securității întregii unități folosind un cod general

Introduceți **codul general** și apăsați pe **armare**  / **dezarmare**  / **Activarea modului de noapte** .

De exemplu: 1234 → ○

Managementul securității de grup cu un cod general

Introduceți **codul general** , apăsați ***** , introduceți **ID-ul grupului** și apăsați pe **armare** ○ / **dezarmare** ○ / **Activarea modului de noapte** ☹.

De exemplu: 1234 → * → 2 → ○

Ce este ID-ul grupului

Dacă un grup este alocat tastaturii (câmpul de **permisiune Armare / Dezarmare** din setările tastaturii), nu este necesar să introduceți ID-ul grupului. Pentru a gestiona modul de armare al acestui grup, este suficientă introducerea unui cod de utilizator general sau personal.

Vă rugăm să rețineți că, dacă un grup este alocat tastaturii, nu veți putea gestiona **modul Noapte** folosind un cod general.

În acest caz, **modul Noapte** poate fi gestionat numai folosind un cod de utilizator personal (dacă utilizatorul are drepturile corespunzătoare).

Drepturi în sistemul de securitate Ajax

Managementul securității întregii unități folosind un cod personal

Introduceți **ID utilizator** , apăsați ***** , introduceți **codul personal de utilizator** și apăsați pe **armare** ○ / **dezarmare** ○ / **Activarea modului de noapte** ☹.

De exemplu: 2 → * → 1234 → ○

Ce este User ID

Gestionarea securității grupului folosind un cod personal

Introduceți **ID-ul utilizatorului** , apăsați * , introduceți **codul de utilizator personal** , apăsați * , introduceți **ID-ul grupului** și apăsați butonul de **armare** ○ / **dezarmare** ○ / **Activarea modului de noapte** ☹.

De exemplu: 2 → * → 1234 → * → 5 → ○

Ce este ID-ul grupului

Ce este User ID

Dacă un grup este alocat tastaturii (câmpul de **permisiune Armare / Dezarmare** din setările tastaturii), nu este necesar să introduceți ID-ul grupului. Pentru a gestiona modul de armare al acestui grup, este suficientă introducerea unui cod de utilizator personal.

Controlul de securitate al întregului obiect folosind un cod de acces

Introduceți **codul de acces** și apăsați pe **armare** ○ / **dezarmare** ○ / **Activarea modului de noapte** ☹cheie.

De exemplu: 1234 → ○

Managementul securității grupului folosind un cod de acces

Introduceți **codul de acces** , apăsați * , introduceți **ID-ul grupului** și apăsați pe **armare** ○ / **dezarmare** ○ / **Activarea modului de noapte** ☹cheie.

De exemplu: 1234 → * → 2 → ○

Ce este ID-ul grupului

Utilizarea codului de constrângere

Codul de constrângere vă permite să ridicați o alarmă silențioasă și să imitați dezactivarea alarmei. O alarmă silențioasă înseamnă că aplicația Ajax și sirenele

nu vă vor țipa și nu vă vor expune. Dar o companie de securitate și alți utilizatori vor fi alertați instantaneu. Puteți utiliza atât coduri **personale**, cât și coduri **generale de constrângere**. De asemenea, puteți configura un cod de acces prin constrângere pentru persoanele care nu sunt înregistrate în sistem.

Ce este codul de constrângere și cum îl folosiți



Scenariile și sirenele reacționează la dezarmare sub constrângere în același mod ca la dezarmarea normală.

Pentru a utiliza un cod general de constrângere:

Introduceți **codul general de constrângere** și apăsați tasta de **dezarmare** ○.

De exemplu: 4321 → ○

Pentru a utiliza un cod personal de constrângere al utilizatorului înregistrat:

Introduceți **ID-ul utilizatorului**, apăsați *****, apoi introduceți **codul personal de constrângere** și apăsați tasta de **dezarmare** ○.

De exemplu: 2 → * → 4422 → ○

Pentru a utiliza un cod de constrângere al unei persoane neînregistrate în sistem:

Introduceți **codul de constrângere** setat în **Coduri de acces la tastatură** și apăsați tasta de **dezarmare** ○.

De exemplu: 4567 → ○

Cum funcționează funcția de oprire a alarmei de incendiu

Folosind tastatura, puteți dezactiva alarma detectoarelor de incendiu interconectate apăsând butonul Funcție (dacă setarea corespunzătoare este activată). Reacția sistemului la apăsarea unui buton depinde de starea sistemului:

- **Detectoare de incendiu interconectate Alarmerle s-au propagat deja** – la prima apăsare a butonului Funcție, toate sirenele detectorilor de incendiu sunt dezactivate, cu excepția celor care au înregistrat alarma. Dacă apăsați din nou butonul, detectorii rămași sunt dezactivați.
- **Timpul de întârziere al alarmelor interconectate durează** - prin apăsarea butonului Funcție, sirena detectorului FireProtect/FireProtect Plus declanșat este dezactivată.

Aflați mai multe despre alarmele cu detectoare de incendiu interconectate



Cu actualizarea [OS Malevich 2.12](#), utilizatorii pot dezactiva alarmele de incendiu din grupurile lor fără a afecta detectorii din grupurile la care nu au acces.

[Află mai multe](#)

Testarea funcționalității

Sistemul de securitate Ajax permite efectuarea de teste pentru verificarea funcționalității dispozitivelor conectate.

Testele nu încep imediat, ci într-o perioadă de 36 de secunde când se utilizează setările standard. Timpul de începere a testului depinde de setările perioadei de scanare a detectorului (paragraful despre setările „**Bijutier**” din setările hub).

Test de putere a semnalului de bijutier

Test de atenuare

Instalare



Înainte de a instala detectorul, asigurați-vă că ați selectat locația optimă și că este în conformitate cu instrucțiunile cuprinse în acest manual!



Tastatura trebuie atașată la suprafața verticală.

1. Atașați panoul SmartBracket la suprafață folosind șuruburi, folosind cel puțin două puncte de fixare (unul dintre ele – deasupra tamperului). După ce ați selectat alt hardware de atașare, asigurați-vă că acestea nu deteriorează sau deformează panoul.



Banda adezivă cu două fețe poate fi utilizată numai pentru atașarea temporară a KeyPad-ului. Banda se va usca în timp, ceea ce poate duce la căderea tastaturii și deteriorarea dispozitivului.

2. Puneți KeyPad pe panoul de atașare și strângeți șurubul de montare de pe partea inferioară a corpului.

De îndată ce tastatura este fixată în SmartBracket, va clipi cu LED-ul **X** (defecțiune) - acesta va fi un semnal că sabotajul a fost acționat.

Dacă indicatorul de defecțiune **X** nu a clipit după instalarea în SmartBracket, verificați starea tamperului în [aplicația Ajax](#) și apoi verificați etanșeitatea de fixare a panoului.

Dacă tastatura este smulsă de pe suprafață sau îndepărtată de pe panoul de atașare, veți primi notificarea.

Întreținerea tastaturii și înlocuirea bateriei

Verificați în mod regulat capacitatea de funcționare a tastaturii.

Bateria instalată în KeyPad asigură până la 2 ani de funcționare autonomă (cu frecvența de interogare de către hub de 3 minute). Dacă bateria tastaturii este descărcată, sistemul de securitate va trimite notificările relevante, iar indicatorul de defecțiune se va aprinde fără probleme și se va stinge după fiecare introducere cu succes a codului.

Înlocuirea bateriei

Set complet

1. Tastatura
2. Panou de montare SmartBracket
3. Baterii AAA (preinstalate) – 4 buc
4. Kit de instalare
5. Ghid de inițiere rapidă

Specificatii tehnice

Tip senzor	Capacitiv
Comutator anti-manipulare	da
Protecție împotriva ghicirii unui cod	da
Protocol de comunicație radio	Bijutier <u>Află mai multe</u>
Banda de frecvențe radio	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 Depinde de regiunea de vânzare.
Compatibilitate	<u>Funcționează numai cu toate hub-urile</u> Ajax și <u>extindetoarele de rază de semnal radio</u>
Puterea maximă de ieșire RF	Până la 20 mW

Modularea semnalului radio	GFSK
Gama de semnal radio	Până la 1.700 m (dacă nu există obstacole) Află mai multe
Alimentare electrică	4 × baterii AAA
Tensiunea de alimentare	3 V (bateriile sunt instalate în perechi)
Durata de viața a bateriei	Până la 2 ani
Metoda de instalare	În interior
Interval de temperatură de funcționare	De la -10°C la +40°C
Umiditatea de funcționare	Pana la 75%
Dimensiunile per total	150 × 103 × 14 mm
Greutate	197 g
Durata de viața	10 ani
Certificare	Gradul de securitate 2, clasa de mediu II în conformitate cu cerințele EN 50131-1, EN 50131-3, EN 50131-5-3

Respectarea standardelor