Instrukcja użytkownika KeyPad

Zaktualizowano 24 lipca, 2023

KeyPad to bezprzewodowa wewnętrzna klawiatura dotykowa do obsługi systemu Ajax. Przeznaczona do użytku wewnętrznego. Za pomocą tego urządzenia użytkownik może uzbroić i rozbroić system oraz sprawdzić jego status. Klawiatura KeyPad jest chroniona przed próbami odgadnięcia kodu dostępu i może wywołać cichy alarm, gdy kod zostanie wprowadzony pod przymusem.

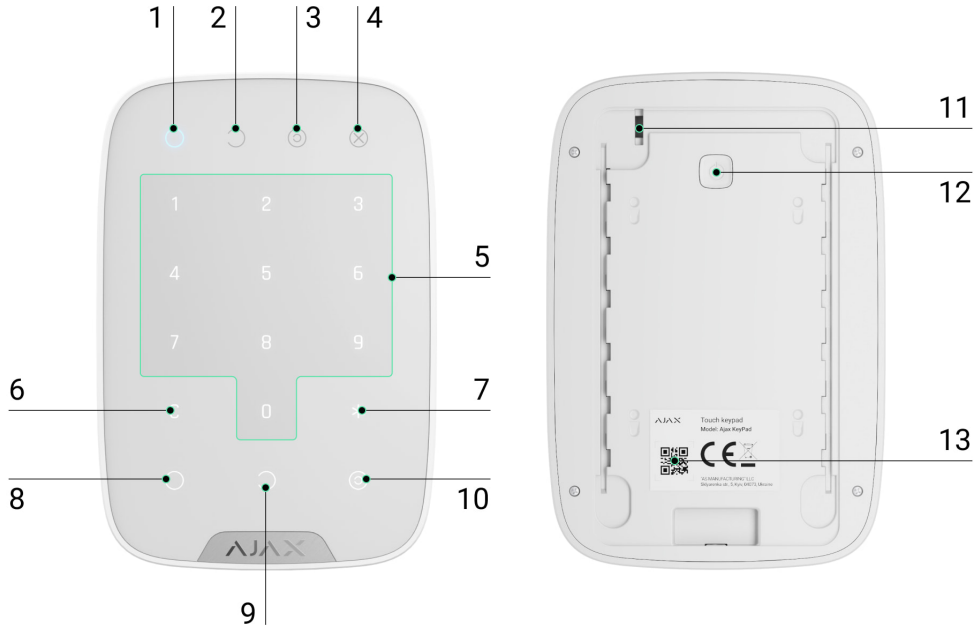
Łącząc się z systemem Ajax za pomocą bezpiecznego protokołu radiowego **Jeweller**, KeyPad komunikuje się z **hubem** na odległość do 1700 m.

KeyPad działa tylko z hubami Ajax i nie komunikuje się z modułami integracji ocBridge Plus i uartBridge.

Urządzenie konfiguruje się za pomocą **aplikacji Ajax** dla systemów iOS, Android, macOS i Windows.

Kup klawiaturę KeyPad

Elementy funkcjonalne



1. Wskaźnik trybu **uzbrojenia**
2. Wskaźnik trybu **rozbrojenia**
3. Wskaźnik **trybu nocnego**
4. Wskaźnik awarii
5. Blok przycisków numerycznych
6. Przycisk **kasowania**
7. Przycisk **funkcyjny**
8. Przycisk **uzbrojenia**
9. Przycisk **rozbrojenia**
10. Przycisk **trybu nocnego**
11. Przycisk antysabotażowy
12. Włącznik
13. Kod QR

Aby zdjąć uchwyt SmartBracket, przesuń go w dół (perforowana część jest niezbędna do działania zabezpieczenia przed sabotażem w przypadku próby

oderwania urządzenia od podłoża).

Zasada działania

KeyPad to dotykowa klawiatura do zarządzania systemem Ajax. Steruje trybami ochrony całego obiektu lub poszczególnych grup oraz umożliwia aktywację **trybu nocnego**. Klawiatura obsługuje funkcję „cichego alarmu” — użytkownik informuje agencję ochrony o tym, że został zmuszony do rozbrojenia systemu alarmowego, ale nie zostanie przy tym zdemaskowany włączeniem syreny ani w aplikacji Ajax.

Tryby ochrony można kontrolować za pomocą KeyPada przy użyciu kodów. Przed wprowadzeniem kodu należy aktywować („wybudzić”) klawiaturę poprzez jej dotknięcie. Gdy opcja jest aktywna, podświetlenie przycisków jest włączone, a klawiatura emituje sygnały dźwiękowe.

KeyPad obsługuje następujące typy kodów:

- **Kod klawiatury** – kod ogólny, który jest ustawiony dla klawiatury. Gdy jest używany, wszystkie zdarzenia są dostarczane do aplikacji Ajax w imieniu klawiatury.
- **Kod użytkownika** – kod osobisty ustawiony dla użytkowników podłączonych do huba. Gdy jest używany, wszystkie zdarzenia są dostarczane do aplikacji Ajax w imieniu użytkownika.
- **Kod dostępu do klawiatury** – skonfigurowany dla osoby, która nie jest zarejestrowana w systemie. Gdy jest używany, zdarzenia są dostarczane do aplikacji Ajax z nazwą skojarzoną z tym kodem.

> Liczba kodów osobistych i kodów dostępu zależy od modelu huba.

Jasność podświetlenia i głośność klawiatury są regulowane w jej **ustawieniach**. Przy rozładowanych bateriach podświetlenie włącza się na minimalnym poziomie niezależnie od ustawień.

Jeśli nie dotkniesz klawiatury przez 4 sekundy, KeyPad zmniejszy jasność podświetlenia, a 8 sekund później przejdzie w tryb oszczędzania energii i

wyłączy wyświetlacz. Gdy klawiatura przechodzi w tryb oszczędzania energii, resetuje wprowadzone polecenia!

KeyPad obsługuje kody o długości od 4 do 6 cyfr. Wprowadzenie kodu powinno być potwierdzone naciśnięciem jednego z przycisków: ◯ (uzbrojenie), ◯ (rozbrojenie) lub ◯ (tryb nocny). Omyłkowo wpisane znaki są resetowane przyciskiem C („Reset”).

KeyPad obsługuje również sterowanie trybami ochrony bez wprowadzania kodu, jeśli w ustawieniach włączona jest funkcja „Uzbrojenie bez kodu”. Opcja ta jest domyślnie wyłączona.

Przycisk funkcyjny

KeyPad ma **przycisk funkcyjny**, który działa w 3 trybach:

- **Wyłączony** — przycisk jest wyłączony. Po kliknięciu nic się nie dzieje.
- **Alarm** — po naciśnięciu **przycisku funkcyjnego** system wysyła alarm do stacji monitorowania alarmów agencji ochrony i użytkowników oraz uruchamia syreny podłączone do systemu.
- **Wyciszenie alarmów z połączonych czujników pożarowych** — po naciśnięciu **przycisku funkcyjnego** system wyłącza syreny **czujników pożarowych Ajax**. Opcja działa tylko wtedy, gdy włączona jest funkcja Połączone alarmy czujników FireProtect (Hub → Ustawienia → Serwis → Ustawienia czujników pożarowych).

Kod pod przymusem

Kod pod przymusem umożliwia symulację dezaktywacji alarmu. W przeciwieństwie do przycisku alarmowego po wprowadzeniu tego kodu użytkownik nie zostanie zdemaskowany dźwiękiem syreny, a klawiatura i aplikacja Ajax poinformują o udanym rozbrojeniu systemu. W tym samym czasie agencja ochrony otrzyma alarm.

Dostępne są następujące typy kodów pod przymusem:

- **Kod klawiatury** – ogólny kod pod przymusem. Gdy jest używany, zdarzenia są dostarczane do aplikacji Ajax w imieniu klawiatury.

- **Kod pod przymusem użytkownika** — osobisty kod pod przymusem ustawiany dla każdego użytkownika podłączonego do huba. Gdy jest używany, zdarzenia są dostarczane do aplikacji Ajax w imieniu użytkownika.
- **Kod dostępu do klawiatury** – kod pod przymusem skonfigurowany dla osoby, która nie jest zarejestrowana w systemie. Gdy jest używany, zdarzenia są dostarczane do aplikacji Ajax z nazwą skojarzoną z tym kodem.

Dowiedz się więcej

Automatyczna blokada nieupoważnionego dostępu

Jeżeli w ciągu 1 minuty trzykrotnie zostanie wprowadzony błędny kod, klawiatura zostanie zablokowana na czas określony w ustawieniach. W tym czasie hub będzie ignorował wszystkie kody i poinformuje użytkowników systemu alarmowego oraz CMS o próbie odgadnięcia kodu.

Klawiatura zostanie automatycznie odblokowana po upływie czasu blokady zdefiniowanego w ustawieniach. Mimo to użytkownik lub PRO z uprawnieniami administratora może odblokować klawiaturę w aplikacji Ajax.

Uzbrajanie dwuetapowe

KeyPad uczestniczy w uzbrajaniu w dwóch etapach. Gdy ta funkcja jest włączona, system będzie się uzbrajał dopiero po ponownym uzbrojeniu za pomocą SpaceControl lub po przywróceniu działania czujnika drugiego stopnia (np. poprzez zamknięcie drzwi wejściowych, na których zainstalowany jest DoorProtect).

Dowiedz się więcej

Protokół przesyłania danych Jeweller

Klawiatura używa protokołu radiowego Jeweller do przesyłania zdarzeń i alarmów. Jest to dwukierunkowy protokół bezprzewodowego przesyłania danych zapewniający szybką i niezawodną komunikację między hubem a urządzeniami systemu.

Jeweller obsługuje szyfrowanie blokowe z kluczem zmiennym oraz uwierzytelnianie urządzeń podczas każdej sesji komunikacyjnej, aby zapobiegać sabotażowi i podrabianiu (spoofingowi) urządzeń. Protokół zapewnia regularne odpytywanie czujników przez hub w odstępie od 12 do 300 sekund (ustawienie w aplikacji Ajax) w celu monitorowania komunikacji ze wszystkimi urządzeniami i wyświetlania ich stanów w aplikacjach Ajax.

Więcej o Jeweller

Wysyłanie zdarzeń do stacji monitorowania

System Ajax może przesyłać zdarzenia i alarmy do aplikacji monitorującej PRO Desktop, a także do centralnej stacji monitorowania (CMS) w formatach Sur-Gard (Contact ID), SIA (DC-09), ADEMCO 685 **i innych zastrzeżonych protokołach**. Zobacz listę CMS-ów, do których można podłączyć system Ajax **tutaj**.

KeyPad może przesyłać następujące zdarzenia:

- Wprowadzono kod pod przymusem.
- Naciśnięto przycisk alarmowy (jeśli **przycisk funkcyjny** działa w trybie przycisku alarmowego).
- Klawiatura jest zablokowana z powodu próby odgadnięcia kodu.
- Alarm/przywrócenie ochrony przed manipulacją.
- Utrata/przywrócenie połączenia z hubem.
- Klawiatura jest tymczasowo wyłączona/włączona.
- Nieudana próba uzbrojenia systemu alarmowego (kiedy włączona jest funkcja sprawdzenia integralności systemu).

Po odebraniu alarmu operator stacji monitorowania agencji ochrony wie, co się stało i gdzie wysłać zespół szybkiego reagowania. Adresowalność każdego urządzenia Ajax pozwala na wysyłanie do PRO Desktop lub do CMS nie tylko zdarzeń, ale także typu urządzenia, grupy ochrony, przypisanej nazwy oraz pomieszczenia. Lista przekazywanych parametrów może się różnić w zależności od CMS i wybranego protokołu komunikacyjnego.

ID urządzenia i numer pętli (strefy) można znaleźć w stanach urządzenia w aplikacji Ajax.

Wskazanie

Po dotknięciu KeyPad budzi się, podświetlając klawiaturę i pokazując tryb ochrony: uzbrojony, rozbrojony lub tryb nocny. Tryb ochrony jest zawsze aktualny, niezależnie od urządzenia sterującego, którego użyto do jego zmiany (brelok lub aplikacja).

Zdarzenie	Wskazanie
Wskaźnik usterki miga **X**	Wskaźnik informuje o braku komunikacji z hubem lub otwarciu pokrywy klawiatury. Możesz sprawdzić przyczynę nieprawidłowego działania w **aplikacji Ajax Security System**
Wciśnięty przycisk KeyPad	Krótkie piknięcie, dioda LED informująca o aktualnym stanie uzbrojenia systemu miga raz
System jest uzbrojony	Krótki sygnał dźwiękowy, świeci wskaźnik LED **trybu uzbrojenia**/**trybu nocnego**
System jest rozbrojony	Dwa krótkie sygnały dźwiękowe, dioda LED **rozbrojenia** zapala się
Niepoprawny kod dostępu	Długi sygnał dźwiękowy, podświetlenie klawiatury miga 3 razy
Wykryto usterkę podczas uzbrajania (np. utrata czujnika)	Długie piknięcie, dioda LED informująca o aktualnym stanie uzbrojenia systemu miga 3 razy
Hub nie odpowiada na polecenie — brak połączenia	Długi sygnał dźwiękowy, zapala się wskaźnik **awarii**

Klawiatura jest zablokowana po 3 nieudanych próbach wprowadzenia kodu	Długi sygnał dźwiękowy, wskaźniki trybu ochrony migają jednocześnie
Niski poziom baterii	Po uzbrojeniu/rozbrojeniu systemu wskaźnik awarii miga powoli. Klawiatura jest zablokowana, gdy wskaźnik miga. Podczas aktywacji klawiatury KeyPad przy niskim poziomie naładowania baterii rozlegnie się długi sygnał dźwiękowy, wskaźnik **awarii** powoli zaświeci się, a następnie zgaśnie.

Dźwiękowe powiadamianie o awariach

Jeśli któreś z urządzeń jest w trybie offline lub bateria jest bliska wyczerpania, KeyPad może powiadomić użytkowników systemu dźwiękiem. Diody LED klawiatury **X** będą migać. Powiadomienia o awariach będą wyświetlane w zdarzeniach oraz treści SMS-ów lub powiadomień push.

Aby włączyć dźwiękowe powiadamianie o awariach, użyj **aplikacji** Ajax PRO i PRO Desktop:

1. Kliknij **Urządzenia**, wybierz hub i otwórz jego ustawienia: Kliknij **Opcje systemowe** → **Dźwięki i alerty**
2. Włącz przełączniki: **Jeśli poziom naładowania baterii dowolnego urządzenia jest niski** oraz **Jeśli jakiekolwiek urządzenie jest offline**.
3. Kliknij **Powrót**, aby zapisać ustawienia.

Dźwiękowe powiadamianie o awariach jest dostępne dla wszystkich hubów (z wyjątkiem modelu Hub) z oprogramowaniem sprzętowym OS Malevich w wersji 2.15 lub nowszej.

Dźwiękowe powiadamianie o awariach jest obsługiwane przez KeyPad z oprogramowaniem sprzętowym w wersji 5.57.1.1 lub nowszej.

Zdarzenie	Wskazanie	Uwaga

Jeśli jakiekolwiek urządzenie jest offline.	Dwa krótkie sygnały dźwiękowe, wskaźnik **awarii X** miga dwukrotnie. Sygnał dźwiękowy jest emitowany co minutę, aż wszystkie urządzenia w systemie będą w trybie online.	Użytkownicy mogą opóźnić sygnalizację dźwiękową o 12 godzin.
Jeśli KeyPad jest offline.	Dwa krótkie sygnały dźwiękowe, wskaźnik **awarii X** miga dwukrotnie. Sygnał dźwiękowy jest emitowany co minutę, aż klawiatura w systemie będzie w trybie online.	Nie można opóźnić sygnalizacji dźwiękowej.
Jeśli poziom naładowania baterii dowolnego urządzenia jest niski.	Trzy krótkie sygnały dźwiękowe, wskaźnik **awarii X** miga trzykrotnie. Sygnał dźwiękowy jest emitowany co minutę, aż bateria zostanie naładowana lub urządzenie zostanie usunięte z systemu.	Użytkownicy mogą opóźnić sygnalizację dźwiękową o 4 godziny.

Dźwiękowe powiadamianie o awariach pojawia się po sygnalizacji klawiatury. Jeśli w systemie wystąpi kilka awarii, klawiatura w pierwszej kolejności powiadamia o utracie połączenia między urządzeniem a hubem.

Podłączenie

Przed podłączeniem urządzenia:

1. Włącz hub i sprawdź połączenie internetowe (logo świeci na biało lub zielono).
2. Zainstaluj **aplikację Ajax**. Utwórz konto, dodaj hub do aplikacji i utwórz przynajmniej jedno pomieszczenie.

3. Upewnij się, że system nie jest uzbrojony i nie aktualizuje się, sprawdzając jego status w aplikacji Ajax.

> Tylko użytkownicy z uprawnieniami administratora mogą dodawać urządzenie do aplikacji

Jak podłączyć KeyPad do huba:

1. Wybierz opcję **Dodaj urządzenie** w aplikacji Ajax.
2. Nazwij urządzenie, zeskanuj lub wpisz ręcznie **kod QR** (umieszczony na obudowie i opakowaniu), a następnie wybierz pomieszczenie instalacji.
3. Wybierz **Dodaj** — rozpocznie się odliczanie.
4. Włącz KeyPad, przytrzymując przycisk zasilania przez 3 sekundy — podświetlenie klawiatury mignie raz.

Aby nastąpiło wykrycie i sparowanie, KeyPad musi się znajdować w zasięgu sieci bezprzewodowej huba (w jednym chronionym obiekcie).

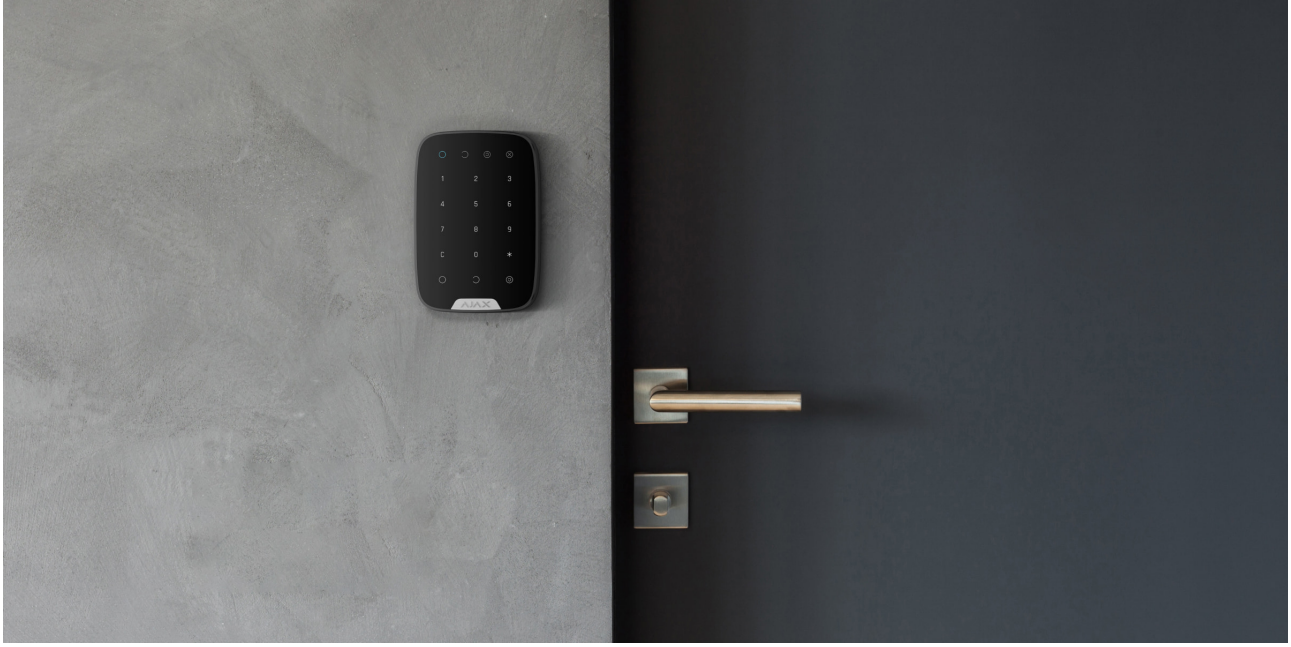
Żądanie podłączenia do huba jest przesyłane przez krótki czas w momencie włączenia urządzenia.

Jeśli KeyPad nie może połączyć się z hubem, wyłącz go na 5 sekund i spróbuj ponownie włączyć.

Podłączone urządzenie pojawi się na liście urządzeń w aplikacji. Aktualizacja stanu urządzeń na liście uzależniona jest od interwału pingu czujnika wybranego w ustawieniach huba (domyślnie 36 sekund).

> Nie ma wstępnie ustawionych kodów dla klawiatury KeyPad. Przed użyciem KeyPada należy ustawić wszystkie niezbędne kody: kod klawiatury (kod ogólny), osobiste kody użytkowników oraz kody pod przymusem (ogólny i osobisty).

Wybór miejsca instalacji



Miejsce instalacji czujnika zależy od jego odległości od huba oraz przeszkód tłumiących sygnał radiowy: ściany, podłogi, duże obiekty w pomieszczeniach.

Urządzenie przeznaczone wyłącznie do pracy wewnątrz pomieszczeń.

Nie instaluj KeyPad:

1. W pobliżu sprzętu do transmisji radiowej, w tym działającego w sieciach komórkowych 2G/3G/4G, routerów Wi-Fi, nadajników, stacji radiowych, a także obok huba Ajax (wykorzystuje sieć GSM).
2. Blisko okablowania elektrycznego.
3. W pobliżu metalowych przedmiotów i luster, które mogą powodować osłabienie sygnału radiowego.
4. poza pomieszczeniem (na zewnątrz);
5. W jakimkolwiek pomieszczeniu o temperaturze i wilgotności poza dopuszczalnym zakresem.
6. Bliżej niż 1 m od huba.

Sprawdź siłę sygnału Jeweller w miejscu instalacji

Podczas testowania poziom sygnału jest wyświetlany w aplikacji i na klawiaturze wraz ze wskaźnikami stanu systemu (tryb uzbrojony), (tryb rozbrojony), (tryb nocny) i wskaźnikiem awarii **X**.

Jeśli poziom sygnału jest niski (jedna kreska), to nie można zagwarantować stabilnej pracy urządzenia. Podejmij wszelkie możliwe kroki, aby poprawić jakość sygnału! W pierwszej kolejności przesuń urządzenie: zmiana położenia o zaledwie 20 cm może znacznie poprawić jakość odbioru sygnału.

Jeśli sygnał odbierany przez urządzenie jest słaby lub niestabilny nawet po zmianie położenia, użyj **podwajacza zasięgu sygnału radiowego ReX**.

Klawiatura KeyPad została zaprojektowana do pracy po zamocowaniu do pionowej powierzchni. Nie możemy zagwarantować poprawnej obsługi klawiatury KeyPad trzymanej w rękach.

Stany

1. Urządzenia
2. KeyPad

Parametr	Znaczenie
Temperatura	Temperatura urządzenia. Mierzona na procesorze i zmienia się stopniowo. Dopuszczalny błąd pomiaru pomiędzy wartością w aplikacji a temperaturą otoczenia wynosi 2°C. Wartość jest aktualizowana, gdy tylko urządzenie wykryje zmianę temperatury o co najmniej 2°C. Można skonfigurować scenariusz według temperatury, aby sterować urządzeniami automatyzacji **Dowiedz się więcej**
Siła sygnału Jewellera	Siła sygnału między hubem a klawiaturą KeyPad

Połączenie przez Jeweller	Wyświetla status użycia podwajacza zasięgu sygnału Jewellera
Stan naładowania akumulatora	Poziom naładowania baterii urządzenia Możliwe są dwa stany: • OK • Bateria rozładowana **Jak wyświetlany jest poziom naładowania baterii w aplikacjach Ajax**
Obudowa	Tryb zabezpieczenia przeciw sabotażowego reagujący na oderwanie lub uszkodzenie obudowy
Permanentna dezaktywacja	Pokazuje stan urządzenia: aktywność, całkowite wyłączenie przez użytkownika lub wyłączenia powiadomień o sabotażu urządzenia.
Aktualizacja	Wersja oprogramowania sprzętowego czujnika
ID urządzenia	Identyfikator urządzenia

Ustawienia

1. Urządzenia
2. KeyPad
3. Ustawienia

Ustawienie	Znaczenie
Imię	Nazwa urządzenia, może być edytowana
Pomieszczenie	Wybór wirtualnego pomieszczenia, do którego jest przypisane urządzenie
Zarządzanie grupą	Wybór grupy, do której przypisany jest KeyPad
Opcje dostępu	Wybór sposobu weryfikacji uzbrojenia/rozbrojenia

	• Tylko kod klawiatury • Tylko kod użytkownika • Kody klawiatury lub kod użytkownika Aby uaktywnić **kody dostępu** ustawione dla osób, które nie są zarejestrowane w systemie, należy wybrać na klawiaturze opcje: **Tylko kod klawiatury** lub **Kody klawiatury lub kod użytkownika**
Kod klawiatury	Ustawienie kodu do uzbrajania/rozbrajania
Kod pod przymusem	Ustawienie **kodu przymusu dla cichego alarmu**
Funkcje przycisków pilota	Wybór funkcji przycisku * • **Wyłączony** — **przycisk funkcyjny** jest wyłączony i po naciśnięciu nie wykonuje żadnych poleceń • **Alarm** — po naciśnięciu **przycisku funkcyjnego** system wysyła alarm do stacji monitorowania agencji ochrony oraz do wszystkich użytkowników • **Wycisz sygnał pożarowy** — po naciśnięciu wycisza alarmy **czujników pożarowych Ajax**. Funkcja działa tylko wtedy, gdy włączona jest synchronizacja alarmów FireProtect. **Dowiedz się więcej**
Uzbrojenie bez kodu	Jeśli opcja jest aktywna, system może być **uzbrojony** przez naciśnięcie przycisku uzbrojenia bez podawania kodu.
Blokada nieautoryzowanego dostępu	Jeśli opcja jest aktywna, po trzykrotnym wprowadzeniu błędnego kodu w ciągu 1 minutyklawiatura zostaje zablokowana na ustawiony czas.

Czas blokowania, min	Czas blokady po błędnych próbach wprowadzenia kodu
Jasność	Jasność podświetlenia klawiatury
Głośność przycisków	Głośność pikania
Alarm głośny, jeśli użyto przycisk napadowy	Ustawienie pojawia się, jeśli dla **przycisku funkcyjnego** wybrano **tryb alarmowy**. Jeśli opcja jest włączona, naciśnięcie **przycisku funkcyjnego** powoduje uruchomienie syren zainstalowanych w obiekcie.
Test siły sygnału Jewellera	Przełącza urządzenie w tryb testu siły sygnału
Test tłumienia sygnału	Przełącza KeyPad w tryb testu zanikania sygnału (dostępny w urządzeniach z **oprogramowaniem sprzętowym w wersji 3.50 lub nowszej**)
Permanentna dezaktywacja	Umożliwia użytkownikowi odłączenie urządzenia bez usuwania go z systemu. Dostępne są dwie opcje: • **Całkowicie** — urządzenie nie będzie wykonywać poleceń systemowych ani uczestniczyć w scenariuszach automatyzacji, a system będzie ignorował alarmy urządzenia i inne powiadomienia • **Tylko obudowa centrali** — system będzie ignorował tylko powiadomienia o próbie sabotażu urządzenia Dowiedz się więcej
Instrukcja użytkownika	Otwiera instrukcję obsługi KeyPad
Usuń urządzenie	Odłącza urządzenie od huba i usuwa jego ustawienia

Konfigurowanie kodów

System Ajax pozwala na ustawienie kodu klawiatury, a także kodów osobistych dla użytkowników dodanych do huba.

Wraz z aktualizacją OS Malevich 2.13.1 dodaliśmy możliwość utworzenia hasła dla osób, które nie są podłączone do huba. Jest to wygodne, na przykład w celu zapewnienia firmie sprzątającej dostępu do zarządzania bezpieczeństwem. Zobacz poniżej, jak ustawić i używać każdego rodzaju kodu.

Aby ustawić kod klawiatury

1. Przejdź do ustawień klawiatury.
2. Wybierz Kod klawiatury.
3. Ustaw żądany kod klawiatury.

Aby ustawić kod pod przymusem dla klawiatury

1. Przejdź do ustawień klawiatury.
2. Wybierz kod pod przymusem.
3. Ustaw żądany kod klawiatury pod przymusem.

Aby ustawić kod osobisty dla zarejestrowanego użytkownika:

1. Przejdź do ustawień profilu: **Hub** → **Ustawienia** ⚙ → **Użytkownicy** → **Ustawienia użytkownika.** W tym menu można również znaleźć identyfikator użytkownika.
2. Kliknij Ustawienia **kodu.**
3. Określ **Kod użytkownika** i **Kod użytkownika pod przymusem**

ⓘ Każdy użytkownik ustawia osobisty kod samodzielnie!

Aby ustawić kod dostępu dla osoby niezarejestrowanej w systemie

1. Przejdź do ustawień huba (**Hub** → **Ustawienia** ⚙).
2. Wybierz **Kody dostępu klawiatury**.
3. Ustaw **nazwę** i **kod dostępu**.

Jeśli chcesz ustawić kod pod przymusem, zmienić kod dostępu, ustawienia dostępu do grup, tryb nocny, ID kodu, czasowo wyłączyć lub usunąć ten kod, wybierz go na liście i wprowadź zmiany.

PRO lub użytkownik z uprawnieniami administratora może skonfigurować kod dostępu lub zmienić jego ustawienia. Funkcja ta jest obsługiwana przez huby z systemem OS Malevich w wersji 2.13.1 lub nowszej. Kody dostępu nie są obsługiwane przez centralę alarmową Hub.

Sterowanie bezpieczeństwem za pomocą kodów

Możesz sterować bezpieczeństwem całego obiektu lub oddzielnych grup za pomocą kodów ogólnych lub osobistych, a także za pomocą kodów dostępu (skonfigurowanych przez PRO lub użytkownika z uprawnieniami administratora).

Jeśli używany jest osobisty kod użytkownika, nazwa użytkownika, który uzbroił/rozbroił system, jest wyświetlana w powiadomieniach i w kanale zdarzeń huba. Jeśli używany jest kod ogólny, nazwa użytkownika, który zmienił tryb ochrony, nie jest wyświetlana.

Kody dostępu klawiatury są obsługiwane przez huby z systemem OS Malevich w wersji 2.13.1 lub nowszej. Centrala alarmowa Hub nie obsługuje tej funkcji.

Zarządzanie bezpieczeństwem całego obiektu za pomocą kodu ogólnego

Wprowadź kod ogólny i naciśnij przycisk **uzbrojenia** / **rozbrojenia** / **włączenia trybu nocnego** .

Na przykład: 1234 →

Zarządzanie bezpieczeństwem grupy za pomocą kodu ogólnego

Wprowadź **kod ogólny** , naciśnij *, wprowadź **identyfikator grupy** i naciśnij **uzbrojenie** / **rozbrojenie** / **aktywacja trybu nocnego** .

Na przykład: 1234 → * → 2 →

Czym jest identyfikator grupy

Jeżeli do KeyPada przypisana jest grupa (pole **Zezwolenie na uzbrajanie/rozbrajanie** w ustawieniach klawiatury), nie trzeba wpisywać ID grupy. Do zarządzania trybem uzbrojenia tej grupy wystarczy wprowadzenie ogólnego lub osobistego kodu użytkownika.

Należy pamiętać, że jeśli do KeyPada przypisana jest grupa, nie będzie można zarządzać **trybem nocnym** za pomocą kodu ogólnego.

W tym przypadku **trybem nocnym** można zarządzać tylko przy użyciu osobistego kodu użytkownika (jeśli użytkownik ma odpowiednie uprawnienia).

Uprawnienia w systemie Ajax

Zarządzanie bezpieczeństwem całego obiektu za pomocą osobistego hasła

Wprowadź **ID użytkownika**, naciśnij *, wprowadź **kod użytkownika** i naciśnij przycisk **uzbrojenia** / **rozbrojenia** / **włączenia trybu nocnego** .

Na przykład: 2 → * → 1234 →

Co to jest ID użytkownika

Zarządzanie bezpieczeństwem grupy za pomocą osobistego hasła

Wprowadź **ID użytkownika**, naciśnij *, wprowadź **kod użytkownika**, naciśnij *, wprowadź **ID grupy** i naciśnij przycisk **uzbrojenia** / **rozbrojenia** / **włączenia trybu nocnego** .

Na przykład: 2 → * → 1234 → * → 5 →

Co to jest ID grupy

Co to jest ID użytkownika

Jeśli do klawiatury KeyPad przypisana jest grupa (pole **Uprawnienia do uzbrajania/rozbrajania** w ustawieniach klawiatury), nie trzeba podawać ID grupy. Aby zarządzać trybem uzbrajania tej grupy, wystarczy wprowadzić osobiste hasło.

Kontrola bezpieczeństwa całego obiektu za pomocą kodu dostępu

Wprowadź **kod dostępu** i naciśnij przycisk **uzbrojenia** / **rozbrojenia** / włączenia **trybu nocnego** .

Na przykład: 1234 →

Zarządzanie bezpieczeństwem grupy za pomocą kodu dostępu

Wprowadź **kod dostępu**, naciśnij *, wprowadź ID grupy i naciśnij przycisk **uzbrojenia** / **rozbrojenia** / **aktywacji trybu nocnego** .

Na przykład: 1234 → * → 2 →

Czym jest identyfikator grupy?

Używanie kodu pod przymusem

Kod pod przymusem pozwala na wywołanie cichego alarmu i pozorowane wyłączenia alarmu.Cichy alarm oznacza, że aplikacja Ajax i syreny nie będą emitować dźwięków alarmowych, aby nie narażać użytkownika na niebezpieczeństwo. Ale agencja ochrony i inni użytkownicy zostaną natychmiast zaalarmowani. Można używać zarówno **osobistych**, jak i ogólnych kodów pod przymusem. Można również ustawić kod dostępu pod przymusem dla osób niezarejestrowanych w systemie. Możesz użyć zarówno osobistego, jak i wspólnego kodu przymusu.

Co to jest kod przymusu i jak go używać?

> Scenariusze i syreny reagują na rozbrojenie pod przymusem w taki sam sposób, jak na normalne rozbrojenie.

Aby użyć kodu ogólnego pod przymusem:

Wprowadź **ogólny kod pod przymusem** i naciśnij przycisk **rozbrojania** .

Na przykład: 4321 →

Użycie osobistego kodu pod przymusem zarejestrowanego użytkownika:

Wprowadź **identyfikator użytkownika**, naciśnij *, następnie wprowadź **osobisty kod pod przymusem** i naciśnij przycisk **rozbrojenia** .

Na przykład: 2 → * → 4422 →

Aby użyć kodu pod przymusem osoby niezarejestrowanej w systemie:

Wprowadź kod pod przymusem ustawiony w **Kodach dostępu do klawiatury** i naciśnij przycisk rozbrojenia .

Na przykład: 4567 →

Jak działa funkcja wyciszania alarmu pożarowego

KeyPad może wyciszyć zsynchronizowany alarm pożarowy po naciśnięciu przycisku funkcyjnego (jeśli włączono odpowiednie ustawienie). Reakcja systemu na naciśnięcie przycisku zależy od stanu systemu:

- **Zsynchronizowane alarmy FireProtect już zostały rozpropagowane** — po pierwszym naciśnięciu **przycisku funkcyjnego** wszystkie syreny czujników pożarowych są wyciszone, z wyjątkiem tych, które zarejestrowały alarm. Ponowne naciśnięcie przycisku powoduje wyciszenie pozostałych czujników.

- **Trwa czas opóźnienia synchronizacji alarmów** — naciśnięcie **przycisku funkcyjnego** powoduje wyciszenie syreny wyzwolonych czujnikow pożarowych Ajax.

Dowiedz się więcej o synchronizacji alarmów czujników pożarowych

Dzięki aktualizacji OS Malevich 2.12 użytkownicy mogą wyciszać alarmy pożarowe w swoich grupach bez wpływu na czujniki w grupach, do których nie mają dostępu.

Dowiedz się więcej

Testowanie funkcjonalności

System Ajax umożliwia przeprowadzanie testów w celu sprawdzenia funkcjonalności podłączonych urządzeń.

Testy nie rozpoczynają się natychmiast, ale w ciągu 36 sekund przy ustawieniach domyślnych. Czas rozpoczęcia testu zależy od ustawień okresu skanowania czujnika (akapit o ustawieniach **Jeweller** w ustawieniach huba).

Test siły sygnału Jewellera

Test tłumienia sygnału

Instalacja

Przed zainstalowaniem czujnika upewnij się, że wybrana lokalizacja jest optymalna i zgodna z wytycznymi zawartymi w niniejszej instrukcji!

KeyPad powinien być przymocowany do pionowej powierzchni.

1. Przymocuj uchwyt SmartBracket do powierzchni za pomocą dołączonych śrub, używając co najmniej dwóch punktów mocowania (w tym jednego nad

zabezpieczeniem antysabotażowym). W przypadku wybrania innych śrub montażowych upewnij się, że nie uszkodzą one ani nie zdeformują panelu.

> Dwustronna taśma klejąca może być używana tylko do tymczasowego zamocowania klawiatury KeyPad. Taśma z czasem wyschnie, co może spowodować upadek klawiatury i uszkodzenie urządzenia.

2. Umieść KeyPad na uchwycie i dokręć śrubę mocującą na spodzie obudowy.

Gdy tylko KeyPad zostanie zainstalowany w SmartBracket, zacznie migać dioda **X** (Usterka) — jest to potwierdzenie włączenia zabezpieczenia antysabotażowego.

Jeżeli po zamocowaniu w SmartBracket dioda usterki **X** nie miga, sprawdź stan zabezpieczenia przed sabotażem w **aplikacji Ajax** oraz prawidłowość zamocowania uchwytu.

Jeśli KeyPad zostanie oderwany od powierzchni lub wyjęty z uchwytu, otrzymasz powiadomienie.

Konserwacja i wymiana baterii klawiatury KeyPad

Regularnie sprawdzaj działanie klawiatury KeyPad.

Sprawdzaj regularnie poprawność działania klawiatury KeyPad.

Fabrycznie zainstalowane baterie zapewniają do 2 lat autonomicznej pracy (z częstotliwością odpytywania przez hub co 3 minuty). Jeśli poziom naładowania baterii KeyPad jest niski, hub wyśle odpowiednie powiadomienia, a wskaźnik awarii zaświeci się powoli i zgaśnie po każdym udanym wprowadzeniu kodu.

Jak długo urządzenia Ajax działają na bateriach i co ma na to wpływ

Wymiana baterii

Pełny zestaw

1. KeyPad

2. Uchwyt montażowy SmartBracket

3. Baterie AAA (w komplecie) — 4 szt.

4. Zestaw instalacyjny

5. Skrócona instrukcja obsługi

Dane techniczne

Typ sensora/td>	Pojemnościowy
Styk przeciwsabotażowy	Tak
Ochrona przed odgadnięciem kodu	Tak
Pasmo częstotliwości	868,0 – 868,6 MHz lub 868,7 – 869,2 MHz w zależności od regionu sprzedaży
Kompatybilność	Współpraca ze wszystkimi **hubami** Ajax i **podwajaczami zasięgu**
Maksymalna moc wyjściowa RF	Do 20 mW
Modulacja sygnału radiowego	GFSK
Zasięg sygnału radiowego	Do 1700 m (w terenie otwartym)
Zasilanie	4 × baterie AAA
Napięcie zasilania	3 V (baterie są zainstalowane parami)
Żywotność baterii	Do 2 lat
Metoda instalacji	Wewnątrz
Zakres temperatury pracy	Od -10°C do +40°C
Dopuszczalna wilgotność	Do 75%
Wymiary	150 × 103 × 14 mm
Waga	197 g

Okres użytkowania	10 lat
Certyfikaty	Klasa bezpieczeństwa 2, klasa środowiskowa II zgodnie z wymaganiami EN 50131-1, EN 50131-3, EN 50131-5-3

Zgodność z normami

Gwarancja

Gwarancja na produkty Limited Liability Company „Ajax Systems Manufacturing” jest ważna przez 2 lata od zakupu i nie dotyczy dołączonych baterii.

Jeśli urządzenie nie działa prawidłowo, najpierw skontaktuj się z działem wsparcia technicznego — w połowie przypadków problemy techniczne można rozwiązać zdalnie!

Pełny tekst gwarancji

Zgoda użytkownika

Wsparcie techniczne:

- e-mail
- Telegram

Subskrybuj nasz newsletter dotyczący bezpieczeństwa. Obiecujemy zero spamu

Email

Subscribe