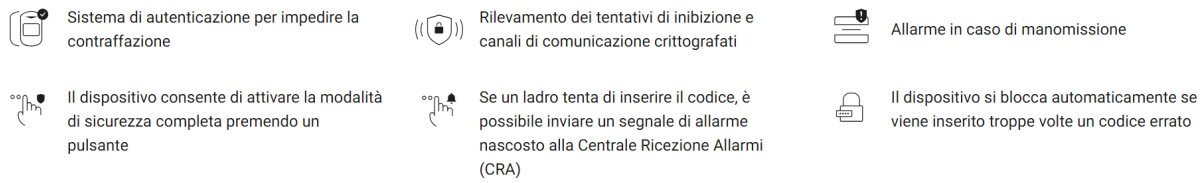
Funzionamento

Il dispositivo attiva le modalità di sicurezza dopo l'inserimento di un codice digitale sulla tastiera. Mostra indicazioni relative allo stato di sicurezza, a eventuali problemi dei rilevatori o all'interruzione delle comunicazioni con l'hub.

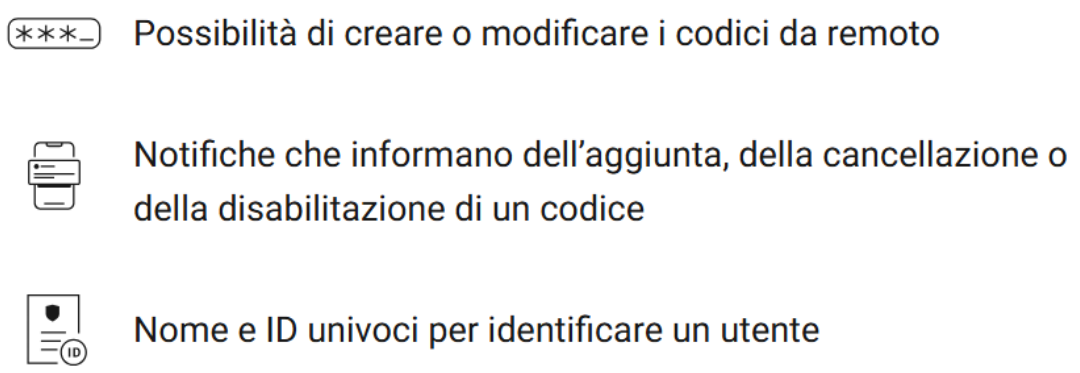
Caratteristiche

Pulsante di allarme disponibile. Invia una notifica a ogni tentativo di inserimento del codice e si blocca automaticamente quando viene raggiunto il numero massimo di tentativi permessi.



Accesso per utenti non registrati al sistema

KeyPad supporta fino a 99 codici di accesso[1] della tastiera per persone non registrate nel sistema Ajax. Grazie a questa funzione non è necessario creare un account per i dipendenti dell'ufficio, per gli addetti alle pulizie o alla manutenzione: è sufficiente assegnare a una persona un codice di accesso nelle impostazioni dell'hub.



Installazione e configurazione

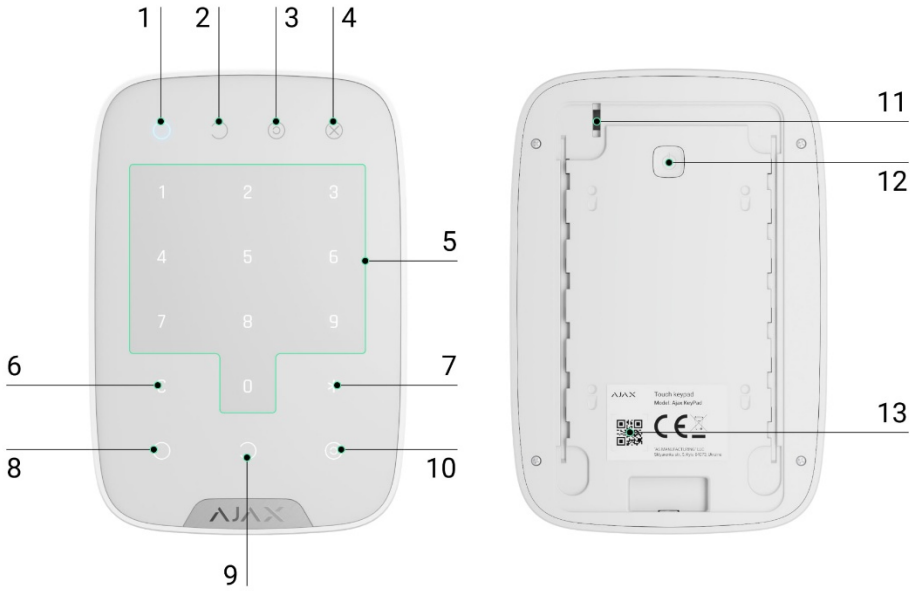
Subito pronto all'uso: la batteria è già inserita, non è necessario smontare il dispositivo. Si connette all'hub tramite applicazione mobile con un clic. Si monta sul supporto SmartBracket in pochi minuti.

Installazione semplice e sicura con un pannello di montaggio SmartBracket

KeyPad è una tastiera touch wireless che gestisce il sistema Ajax. La tastiera è progettata per essere usata negli spazi interni. Il dispositivo consente di inserire e disinserire il sistema, fornisce informazioni sullo stato, è protetto dai tentativi di forzatura del codice d'accesso e supporta la funzione "allarme silenzioso" se viene inserito un codice coercizione.

KeyPad funziona solamente all'interno del sistema Ajax (non può essere usato con sistemi di sicurezza di terze parti), connettendosi all'hub tramite il protocollo protetto Jeweller. Il raggio di comunicazione va fino a 1700 m in campo aperto.

Elementi funzionali



1. Indicatore modalità **inserita**
2. Indicatore modalità **disinserita**
3. Indicatore **Modalità notturna**
4. Indicatore di **malfunzionamento**
5. Tasti touch numerici
6. Tasto **cancella**
7. Tasto **funzione**
8. Tasto per **inserire**
9. Tasto per **disinserire**
10. Tasto **Modalità notturna**
11. Tamper antisabotaggio
12. Pulsante on/off
13. Codice QR

Funzionamento di KeyPad

KeyPad è una tastiera touch per gestire il sistema Ajax. Controlla la modalità di sicurezza di tutto l'impianto o di singole aree e permette di attivare la Modalità notturna. La tastiera supporta la funzione "allarme silenzioso": l'utente avvisa l'istituto di vigilanza che è stato costretto a disinserire il sistema ma la comunicazione avviene senza attivare le sirene o ricevere notifiche nell'applicazione Ajax.

La modalità di sicurezza può essere gestita con KeyPad utilizzando i codici. Prima di digitare un codice, bisogna attivare ("svegliare" dallo standby) la tastiera, toccandola. Una volta attivata, la retroilluminazione della tastiera si accende e viene emesso un breve segnale acustico.

KeyPad supporta i seguenti tipi di codici:

Codice tastiera: codice generale impostato per una tastiera. Se impostato, tutti gli eventi vengono comunicati alle applicazioni Ajax con l'indicazione della tastiera.

Codice utente: codice personale degli utenti connessi all'hub. Se utilizzato, tutti gli eventi vengono inviati alle app Ajax con il nome dell'utente.

Codice di accesso: codice dato agli utenti non registrati nel sistema. Quando utilizzato, gli eventi vengono inviati alle applicazioni Ajax con il nome associato a quel codice.

Codice G.P.G. è un codice di accesso per le guardie particolari giurate (G.P.G.) attivato dopo l'allarme e valido per un periodo specifico. Quando il codice viene attivato e utilizzato, gli eventi vengono inviati alle app Ajax con il nome associato a questo codice.

Nelle impostazioni di KeyPad si può regolare l'intensità della retroilluminazione e il volume della tastiera. Con le batterie scariche, la retroilluminazione si accende al livello minimo indipendentemente dalle impostazioni.

Se la tastiera non viene utilizzata per 4 secondi, KeyPad riduce la luminosità della retroilluminazione e dopo 8 secondi passa in modalità risparmio energetico e il display si spegne. Se la tastiera entra in modalità risparmio energetico, resetta i codici inseriti!

KeyPad supporta codici formati da 4 a 6 cifre. Il codice digitato deve essere confermato premendo uno dei pulsanti: ○ (inserimento), ◯ (disinserimento) и ◎ (Attivazione Modalità notturna). Qualsiasi cifra digitata per errore può essere cancellata premendo il pulsante C ("Reset").

KeyPad supporta anche la gestione delle modalità di inserimento senza usare un codice, se l'opzione "Inserimento senza codice" è abilitata nelle impostazioni. Questa funzione è disabilitata per impostazioni predefinite.

Pulsante funzione

KeyPad ha un pulsante **Funzione** che che può operare in 3 modalità:

- **Off**: funzione disabilitata. Non succede nulla se si preme il pulsante.
- **Allarme**: dopo aver premuto il pulsante **Funzione**, il sistema invia un allarme all'unità centrale dell'istituto di vigilanza, agli utenti e le sirene collegate al sistema si attivano.
- **Silenzia allarme incendio**: dopo aver premuto il pulsante **Funzione**, il sistema disabilita le sirene dei rilevatori antincendio Ajax. L'opzione funziona solo se è abilitata l'opzione Allarmi antincendio interconnessi (Hub → Impostazioni → Servizio → Impostazioni rilevatori antincendio).

Codice coercizione

Un codice coercizione permette di simulare la disattivazione del sistema. A differenza del pulsante antipanico, se l'utente digita questo codice, l'evento non viene segnalato dalle sirene, la tastiera e l'applicazione non segnalano il disinserimento del sistema ma l'istituto di vigilanza riceve una notifica di allarme.

Sono disponibili i seguenti tipi di codice coercizione:

- **Codice tastiera**: se impostato, gli eventi vengono comunicati alle applicazioni Ajax con il nome della tastiera.
- **Codice utente**: codice personale degli utenti connessi all'hub. Se utilizzato, tutti gli eventi vengono consegnati alle app Ajax con il nome dell'utente.
- **Codice di accesso**: impostato per gli utenti non registrati al sistema. Quando utilizzato, gli eventi vengono consegnati alle applicazioni Ajax con il nome associato a un certo codice.

Blocco in caso di accesso non autorizzato

Se viene inserito un codice errato per tre volte in 1 minuto, la tastiera si blocca per il tempo specificato nelle impostazioni. Durante questo periodo, l'hub ignorerà tutti i codici e informerà gli utenti del sistema di sicurezza e la CRA del tentativo di indovinare il codice.

La tastiera si sbloccherà automaticamente allo scadere del tempo selezionato nelle impostazioni. Altrimenti, un utente o un PRO con diritti di amministratore possono sbloccare la tastiera attraverso l'applicazione Ajax.

Inserimento in due fasi

KeyPad permette di inserire il sistema in due fasi. Se questa funzione è abilitata, il sistema si armerà solo dopo che l'inserimento è stato confermato con SpaceControl o con l'attivazione di un rilevatore (ad esempio, dopo aver chiuso la porta su cui è installato DoorProtect).

Protocollo di trasferimento dati Jeweller

La tastiera utilizza il protocollo Jeweller per trasmettere eventi ed allarmi. Questo è un protocollo di trasferimento dati wireless bidirezionale che fornisce una comunicazione veloce e affidabile tra l'hub e i dispositivi collegati.

Jeweller supporta la crittografia a blocchi con una chiave mobile e l'autenticazione dei dispositivi ad ogni sessione di comunicazione per prevenire il sabotaggio e la contraffazione. Il protocollo prevede il polling regolare dei dispositivi da parte dell'hub a intervalli da 12 a 300 secondi (impostati nell'app Ajax) per monitorare la comunicazione con tutti i dispositivi e visualizzarne gli stati nelle app Ajax.

Invio degli eventi alla centrale ricezione allarmi

Il sistema Ajax può trasmettere allarmi all'app di monitoraggio PRO Desktop e alla centrale ricezione allarmi (CRA) tramite SurGard (Contact ID), SIA (DC-09), ADEMCO 685 e altri protocolli proprietari. Qui si trova l'elenco delle CRA a cui si può collegare un sistema Ajax.

KeyPad può trasmettere i seguenti eventi:

- Digitazione del Codice coercizione.
- Pressione del pulsante antipanico (se il pulsante **Funzione** è in modalità panico).
- Tastiera bloccata a causa di un tentativo di indovinare il codice.
- Allarme/ripristino tamper.
- Perdita/ripristino connessione con l'hub.
- Tastiera disattivata/accesa.
- Tentativo di inserire il sistema non riuscito (se abilitata l'opzione: verifica dell'integrità del sistema).

Quando viene ricevuto un allarme, l'operatore della centrale ricezione allarmi dell'istituto di vigilanza sa cosa è successo e dove inviare una pattuglia di risposta rapida. L'indirizzabilità di ciascun dispositivo Ajax consente di inviare a PRO Desktop

o alla CRA non solo gli eventi ma anche il tipo di dispositivo, il nome, l'area di sicurezza e la stanza. L'elenco dei parametri trasmessi può variare a seconda del tipo di CRA e del protocollo di comunicazione selezionato.

Indicazioni di funzionamento della tastiera

Quando la tastiera si accende, il LED si illumina in base alla modalità di funzionamento del sistema di sicurezza (O, C, (c)).

Gli indicatori mostrano lo stato del sistema: modalità inserita/modalità disinserita/ modalità notturna.

Le informazioni sono aggiornate anche se lo stato è stato modificato da un altro dispositivo di controllo — applicazione mobile, telecomando.

Connettere la tastiera all'hub

Prima di avviare la connessione

Installare l'applicazione Ajax sul proprio smartphone, seguendo le indicazioni contenute nelle istruzioni dell'hub. Creare un account, aggiungere l'hub all'applicazione e creare almeno una stanza.

Aprire l'applicazione Ajax. Accendere l'hub e verificare la connessione internet (via cavo Ethernet e/o rete GSM).

Assicurarsi che l'hub sia disinserito e non stia eseguendo aggiornamenti verificando il suo stato tramite l'applicazione mobile.

Connettere KeyPad all'hub

1. Aprire una stanza sull'applicazione mobile o sull'applicazione web e selezionare l'opzione **Aggiungi dispositivo**.
2. Dare un nome al dispositivo, scansionare/trascrivere il suo **codice Q**R (che si trova sulla custodia e sulla scatola) e selezionare la stanza dove è localizzato.

3. Quando l'hub inizia la ricerca dispositivi e lancia il conto alla rovescia, accendere KeyPad tenendo premuto il pulsante on/off per 3 secondi. Il LED del dispositivo lampeggia una volta.

Per avviare il processo di rilevamento e interfacciamento, il rilevatore deve essere localizzato all'interno dell'area di copertura della rete wireless dell'hub (in un unico locale protetto).

La richiesta di connessione all'hub viene trasmessa per un breve periodo di tempo appena si accende il dispositivo. Se la connessione all'hub fallisce, KeyPad si spegne dopo 5 secondi. Ripetere il tentativo di connessione.

Non installare KeyPad:

1. Vicino ad apparecchiature per la trasmissione radio, tra cui quelle che funzionano con reti mobili 2G/3G/4G, router Wi-Fi, ricetrasmettitori, stazioni radio, e anche un hub Ajax (utilizza una rete GSM).
2. Nelle immediate vicinanze di impianti elettrici.
3. Vicino a oggetti in metallo e specchi, in quanto potrebbero attenuare o bloccare il segnale radio.
4. Fuori dai locali protetti (all'esterno).
5. In stanze con temperature e umidità al di sopra dei limiti indicati nelle specifiche tecniche.
6. A una distanza di meno di 1 metro dall' hub.

Impostazioni codici

Il sistema Ajax permette di attribuire un codice generale a una tastiera o di assegnare un codice personale agli utenti registrati all'hub.

Con l'aggiornamento OS Malevich 2.13.1, è stata aggiunta anche la possibilità di creare codici per persone che non sono registrate a un hub. Questa funzione si usa, ad esempio, per dare un codice di accesso agli addetti alle pulizie. Di seguito è possibile vedere come impostare e usare i diversi tipi di codici.

Per impostare un codice della tastiera

1. Andare alle impostazioni della tastiera.
2. Scegliere il campo **Codice tastiera**.
3. Impostare il codice tastiera desiderato.

Per impostare un codice coercizione della tastiera

1. Andare alle impostazioni della tastiera.
2. Scegliere il campo **Codice coercizione**.
3. Impostare il codice coercizione della tastiera desiderato

Gestione della sicurezza tramite codici

È possibile controllare la sicurezza dell'intero impianto o di aree separate utilizzando i codici generali, codici personali o codici G.P.G., nonché i codici di accesso (configurati da PRO o da un utente con diritti di amministratore).

Se viene utilizzato un codice utente, il nome dell'utente che ha inserito/disinserito il sistema viene visualizzato nelle notifiche e nel registro degli eventi dell'hub. Se viene utilizzato un codice G.P.G., viene visualizzato il titolo del codice G.P.G. Se viene utilizzato un codice generale, il nome dell'utente che ha cambiato lo stato di inserimento non viene visualizzato.

Gestione della sicurezza dell'intero impianto con un codice generale della tastiera

Inserire il **codice generale della tastiera** e premere il tasto di **inserimento** ◯ / **disinserimento** ◯ / **attivazione modalità notturna** ◎.

Per esempio: 1234 → ◯

Gestione della sicurezza di un'area con un codice generale della tastiera

Inserire il **codice generale della tastiera**, premere *, inserire l'**ID dell'area** e premere il tasto di **inserimento** ◯ / **disinserimento** ◯ / **attivazione modalità notturna** ◎.

Cos'è l'ID dell'area?

Se un'area è assegnata a KeyPad (campo di autorizzazione all'inserimento/ disinserimento nelle impostazioni della tastiera), non è necessario inserire l'ID Area. Per gestire lo stato di inserimento di questa area è sufficiente inserire un codice generale o utente.

Notare che se un'area viene assegnata a KeyPad, non sarà possibile gestire la modalità notturna utilizzando un codice generale.

In questo caso, la modalità notturna può essere gestita solo con un codice utente (se l'utente ha i diritti appropriati).

Gestione della sicurezza dell'intero impianto con un codice utente

Inserire l'**ID utente**, premere *, inserire il **codice utente** e premere il tasto di **inserimento** / **disinserimento** / **attivazione modalità notturna**.

Per esempio: 2 → * → 1234 →

Cos'è l'ID Utente?

Gestione della sicurezza di un'area con un codice utente

Inserire l'**ID utente**, premere *, inserire il **codice utente**, premere *, inserire l'**ID Area** e premere il tasto di **inserimento** / **disinserimento** / **attivazione modalità notturna**.

Per esempio: 2 → * → 1234 → * → 5 →

Se un'area è assegnata a KeyPad (**campo di autorizzazione all'inserimento/ disinserimento** nelle impostazioni della tastiera), non è necessario inserire l'ID Area. Per gestire lo stato di inserimento di questa area è sufficiente inserire un codice utente.

Gestione della sicurezza di un intero impianto utilizzando un codice di accesso

Inserire il **codice di accesso** e premere di **inserimento** / **disinserimento** / **attivazione modalità notturna**.

Per esempio: 1234 →

Gestione della sicurezza di un'area utilizzando un codice di accesso

Digitare il **codice di accesso**, premere *asterisk icon*, inserire l'**ID dell'area** e premere di **inserimento** / **disinserimento** / **attivazione modalità notturna**.

Per esempio: 1234 → * → 2 →

Utilizzo di un codice coercizione

Un codice coercizione consente di attivare un allarme silenzioso e di imitare la disattivazione dell'allarme. Un allarme silenzioso significa che l'app Ajax e le sirene non faranno rumore e non segnalano nessuno. Ma un istituto di vigilanza e gli altri utenti saranno avvisati immediatamente. È possibile utilizzare sia il codice utente che quello di coercizione generale. Il codice coercizione può anche essere impostato per persone non registrate nel sistema.

Per utilizzare un codice di coercizione generale della tastiera:

Inserire il codice **coercizione generale** e premere il pulsante di **disinserimento** .

Per esempio: 4321 →

Per utilizzare un codice utente coercizione:

Inserire l'**ID Utente**, premere *, quindi inserire il **codice utente coercizione** e premere il pulsante di **disinserimento** .

Per esempio: 2 → * → 4422 →

Per usare un codice di accesso coercizione:

Inserire il **codice di accesso coercizione** e premere il pulsante per **disinserire il sistema** .

Per esempio: 4567 →

Utilizzo del codice G.P.G.

Il codice G.P.G. si attiva dopo l'attivazione dell'allarme durante l'orario configurato nelle impostazioni dell'hub ed è valido per un periodo specificato. In questo modo si garantisce che tali codici vengono utilizzati solo in caso di rischio, a differenza dei codici tastiera o utente.

Controllo di sicurezza dell'impianto tramite il codice G.P.G.:

Inserire il **codice G.P.G.** e premere il pulsante **inserimento** / **disinserimento** / **attivazione modalità notturna** .

Per esempio: 1234 →

Controllo di sicurezza dell'area tramite il codice G.P.G.:

Inserire il **codice G.P.G.**, premere *, inserire ID area, e premere il pulsante **inserimento** / **disinserimento** / **attivazione modalità notturna** .

Per esempio: 1234 → * → 2 →

Come funziona l'opzione di silenziamento degli allarmi antincendio

La tastiera KeyPad può silenziare gli allarmi interconnessi dei rilevatori antincendio premendo il pulsante "Funzione" (se l'impostazione corrispondente è abilitata). La reazione del sistema alla pressione di un pulsante dipende dalle impostazioni e dallo stato del sistema:

Gli Allarmi antincendio interconnessi si sono già propagati: alla prima pressione del pulsante Funzione, tutte le sirene dei rilevatori antincendio vengono silenziate, ad eccezione di quelle che hanno registrato l'allarme. Premendo nuovamente il pulsante, i rilevatori rimanenti vengono silenziati.

Il tempo di ritardo degli allarmi interconnessi è già iniziato: premendo il pulsante Funzione, la sirena del rilevatori incendio Ajax attivato viene silenziata.

Test di funzionamento

Il sistema Ajax consente di effettuare dei test per verificare il funzionamento dei dispositivi connessi.

I test non vengono avviati subito ma entro un periodo di tempo di 36 secondi in base alle impostazioni standard. Il tempo di avvio dei test dipende dalle impostazioni dell'intervallo di scansione del rilevatore (paragrafo sulle impostazioni **Jeweller** all'interno delle impostazioni dell'hub).