Manuel utilisateur KeyPad

Mis à jour September 1, 2025

KeyPad est un clavier tactile intérieur sans fil, permettant de gérer le système Ajax. Conçu pour l'utilisation intérieure uniquement. Grâce à cet dispositif, l'utilisateur peut armer et désarmer le système et voir son statut de sécurité. KeyPad est protégé contre les tentatives de deviner le code d'accès et peut déclencher une alarme silencieuse lorsque le code d'accès est saisi sous la contrainte.

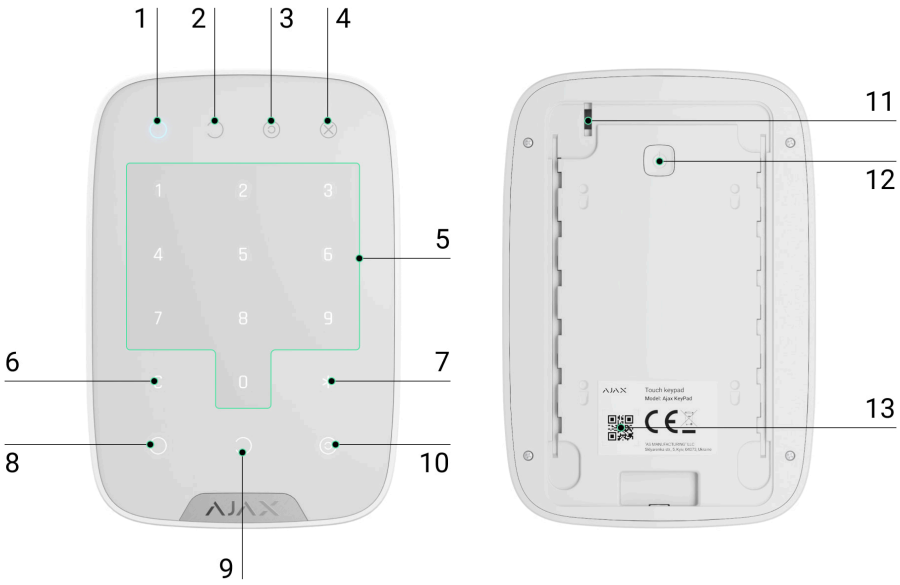
Connecté au système Ajax via un protocole radio sécurisé **Jeweller**, KeyPad communique avec la **centrale** à une distance allant jusqu'à 1 700 m en champ ouvert.

KeyPad fonctionne uniquement avec les centrales Ajax et n'est pas compatible avec les modules d'intégration ocBridge Plus ou uartBridge.

Le dispositif est configuré via les **applications Ajax** pour iOS, Android, macOS et Windows.

Acheter un clavier KeyPad

Éléments fonctionnels



1. Indicateur **Armé**
2. Indicateur **Désarmé**
3. Indicateur de **mode Nuit**
4. Indicateur de **dysfonctionnement**
5. Bloc de boutons numériques
6. Bouton **Effacer**
7. Bouton de **Fonction**
8. Bouton **Armer**
9. Bouton **Désarmer**
10. Bouton du **mode Nuit**
11. Bouton anti-sabotage
12. Bouton marche/arrêt
13. Code QR

Pour retirer le panneau SmartBracket, faites-le glisser vers le bas (une pièce perforée est nécessaire pour actionner le bouton anti-sabotage en cas de tentative d'arrachage du dispositif de la surface).

Principe de fonctionnement

KeyPad est un clavier tactile pour la gestion du système Ajax. Il contrôle les modes de sécurité du site entier ou de groupes individuels et permet d'activer le **mode Nuit**. Le clavier prend en charge la fonction « alarme silencieuse », l'utilisateur informe le centre de télésurveillance qu'il a été contraint de désarmer le système de sécurité, sans être exposé par les sirènes sonores ou les applications Ajax.

Vous pouvez contrôler les modes de sécurité avec le KeyPad, en utilisant des codes. Avant de saisir le code, vous devez activer (réveiller) le clavier en le touchant. Lorsqu'il est activé, le rétroéclairage des touches est activé et le clavier émet des bips.

Le KeyPad prend en charge les types de codes suivants :

- **Code clavier** est un code commun, configuré pour le clavier. Lorsqu'il est utilisé, tous les événements sont transmis aux applications Ajax au nom du clavier.
- **Code utilisateur** est un code personnel, configuré pour les utilisateurs connectés à la centrale. Lorsqu'il est utilisé, tous les événements sont transmis aux applications Ajax au nom de l'utilisateur.
- **Code d'accès** est un code configuré pour les personnes qui ne sont pas enregistrées dans le système. Lorsqu'il est utilisé, les événements sont transmis aux applications Ajax avec un nom associé à ce code.
- **Code GIR** est un code d'accès pour les groupes d'intervention rapide (GIR) qui est activé après une alarme et qui est valable pour une durée déterminée. Lorsque le code est activé et utilisé, les événements sont envoyés aux applications Ajax avec un nom associé à ce code.

Le nombre de codes d’accès personnels, codes d’accès et codes GIR dépend du modèle de centrale.

Le panneau de contrôle Hub (2G) Jeweller ne prend pas en charge les codes d’accès.

La luminosité du rétroéclairage et le volume du clavier sont réglés dans ses **paramètres**. Lorsque les batteries sont déchargées, le rétroéclairage s’allume au niveau minimum, quels que soient les réglages.

Si vous ne touchez pas le clavier pendant 4 secondes, le KeyPad réduit la luminosité du rétroéclairage, et 8 secondes plus tard, il passe en mode d’économie d’énergie et éteint l’écran. Lorsque le clavier passe en mode d’économie d’énergie, il réinitialise les commandes saisies !

Le clavier prend en charge des codes de 4 à 6 chiffres. La saisie du code doit être confirmée en appuyant sur l’un des boutons : ◯ (armement), ◯ (désarmement) et ◯ (mode Nuit). Les caractères saisis par erreur sont réinitialisés avec le bouton C (Effacer).

Le KeyPad permet également de contrôler les modes de sécurité sans saisir de code, si la fonction « Armement sans code » est activée dans les paramètres. Cette fonction est désactivée par défaut.

Bouton de fonction

Le KeyPad dispose d’une **bouton de fonction** qui fonctionne selon 3 modes :

- **Off** : le bouton est désactivé. Rien ne se passe après avoir cliqué.
- **Alarme** : après avoir appuyé sur le bouton de fonction, le système envoie une alarme au centre de télésurveillance, aux utilisateurs, et active les sirènes connectées au système.
- **Désactiver l’alarme incendie interconnectée** : après avoir appuyé sur le **bouton de fonction**, le système désactive les sirènes des **détecteurs d’incendie Ajax**. L’option ne fonctionne que si les alarmes des

détecteurs d'incendie interconnectés sont activées (Centrale → Paramètres → Service → Paramètres des détecteurs d'incendie).

Code de contrainte

Un code de contrainte vous permet de simuler la désactivation de l'alarme. Contrairement au bouton de panique, si ce code est saisi, l'utilisateur ne sera pas compromis par le déclenchement de la sirène. En même temps, le clavier et l'application Ajax informeront de la réussite du désarmement du système. Parallèlement, le centre de télésurveillance recevra une alarme.

Les types de codes de contrainte suivants sont disponibles :

- **Code clavier** : lorsqu'il est utilisé, tous les événements sont transmis aux applications Ajax au nom du clavier.
- **Code utilisateur** : configuré pour les utilisateurs connectés à la centrale. Lorsqu'il est utilisé, tous les événements sont transmis aux applications Ajax au nom de l'utilisateur.
- **Code d'accès** : configuré pour les personnes qui ne sont pas enregistrées dans le système. Lorsqu'il est utilisé, les événements sont transmis aux applications Ajax avec un nom associé à ce code.

En savoir plus

Accès non autorisé. Auto-verrouillage

Si un code incorrect est saisi trois fois en une minute, le clavier sera verrouillé pendant la durée spécifiée dans les paramètres. Pendant cette période, la centrale ignore tous les codes et informe les utilisateurs du système de sécurité et le centre de télésurveillance d'une tentative de deviner le code.

Le clavier se déverrouille automatiquement après l'expiration du temps de verrouillage défini dans les paramètres. Cependant, l'utilisateur ou le PRO

avec des droits d'administrateur peut déverrouiller le clavier via l'application Ajax.

Armement en deux étapes

Le KeyPad participe à l'armement en deux étapes. Lorsque cette fonction est activée, le système ne s'arme qu'après avoir été réarmé avec SpaceControl ou après le rétablissement d'un détecteur de deuxième étape (par exemple, en fermant la porte d'entrée sur laquelle DoorProtect est installé).

En savoir plus

Protocole de transfert de données Jeweller

Le clavier utilise le protocole radio Jeweller pour transmettre les événements et les alarmes. Il s'agit d'un protocole de transfert de données bidirectionnel sans fil, qui assure une communication rapide et fiable entre la centrale et les dispositifs connectés.

Jeweller prend en charge le chiffrement par blocs avec une clé dynamique et l'authentification des dispositifs à chaque session de communication, afin d'éviter le sabotage et l'usurpation d'identité des dispositifs. Le protocole implique une interrogation régulière des dispositifs par la centrale à des intervalles de 12 à 300 secondes (définis dans l'application Ajax) pour surveiller la communication avec tous les dispositifs et afficher leurs états dans les applications Ajax.

En savoir plus sur Jeweller

Envoi d'événements au centre de télésurveillance

Le système Ajax peut transmettre des alarmes à l'application de télésurveillance PRO Desktop, ainsi qu'au centre de télésurveillance via SurGard (Contact ID), SIA (DC-09), ADEMCO 685, et d'**autres protocoles propriétaires**. Consultez la liste des centres de télésurveillance auxquels vous pouvez connecter le système Ajax **ici**.

Le KeyPad peut transmettre les événements suivants :

- Le code de contrainte est saisi.
- Le bouton de panique est pressé (si le **bouton de fonction** fonctionne en mode de bouton de panique).
- Le clavier est verrouillé, suite à une tentative de deviner un code.
- Alarme de sabotage/rétablissement.
- Perte/rétablissement de la connexion de la centrale.
- Le clavier est éteint/allumé.
- Tentative infructueuse d'armer le système de sécurité (avec la vérification d'intégrité activée).

Lorsqu'une alarme est reçue, l'opérateur du centre de télésurveillance sait ce qui s'est passé et où envoyer l'équipe d'intervention rapide. L'adressage de chaque dispositif Ajax vous permet d'envoyer au PRO Desktop ou au centre de télésurveillance non seulement les événements mais aussi le type de dispositif, le groupe de sécurité, le nom qui lui est attribué et la pièce. La liste des paramètres transmis peut différer selon le type de centre de télésurveillance et le protocole de communication sélectionné.

L'ID du dispositif et le numéro de la boucle (zone) se trouvent dans ses états dans l'application Ajax.

Indication

En touchant le KeyPad, celui-ci se réactive en mettant le clavier en surbrillance et en indiquant le mode de sécurité : mode Armer, Désarmer ou Nuit. Le mode de sécurité est toujours effectif, quel que soit le dispositif de contrôle qui a été utilisé pour le modifier (la télécommande ou l'application).

Événement	Indication
Clignotement de l'indicateur **X** de dysfonctionnement	L'indicateur avertit en cas de perte de communication avec la centrale ou d'ouverture du couvercle du clavier.
Bouton du clavier enfoncé	Un court bip, la LED de l'état d'armement actuel du système clignote une fois
Le système est armé	Signal sonore court, mode **Armé** / l'indicateur LED du **mode Nuit** s'allume
Le système est désarmé	Deux signaux sonores courts, l'indicateur LED du **désarmé** s'allume
Code d'accès incorrect	Signal sonore long, le rétro-éclairage du clavier fait apparaître 3 clignotements
Un dysfonctionnement est détecté lors de l'armement (par exemple, le détecteur est perdu)	Un long bip, la LED de l'état d'armement actuel du système clignote 3 fois
La centrale ne répond pas à la commande — pas de connexion	Signal sonore long, l'indicateur de **dysfonctionnement** s'allume
KeyPad est verrouillé après 3 tentatives infructueuses de saisie du code d'accès	Signal sonore long, les indicateurs de mode de sécurité font apparaître des clignotements simultanés
Batterie faible	Après que le système est armé/désarmé, l'indicateur de **dysfonctionnement** émet des clignotements continus. Le clavier est verrouillé lorsque l'indicateur clignote. Lorsque KeyPad est activé avec de faibles batteries, il émet un long signal sonore, l'indicateur de **dysfonctionnement** s'allume en douceur puis s'éteint

Notifications sonores en cas de dysfonctionnement

Si un dispositif quelconque est hors ligne ou si la batterie est faible, le KeyPad peut en informer les utilisateurs du système par un son audible. Les LED **X** des claviers clignotent. Les notifications de dysfonctionnement seront affichées dans le flux d'événements, dans le texte SMS ou dans la notification push.

Pour activer les notifications sonores de dysfonctionnements, utilisez les **applications** Ajax PRO et PRO Desktop :

1. Cliquez sur **Dispositifs**, choisissez la centrale et ouvrez ses paramètres :
   Cliquez sur **Service** → **Sons et alertes**
2. Activez les interrupteurs : **Si la batterie d'un dispositif est faible** et **Si un dispositif est hors ligne**.
3. Cliquez sur **Retour** pour enregistrer les paramètres.

> Les notifications sonores des dysfonctionnements sont disponibles pour toutes les centrales avec la version du firmware OS Malevich 2.15 ou plus.
>
> Les notifications sonores des dysfonctionnements sont prises en charge par KeyPad avec la version 5.57.1.1 du firmware ou une version plus récente.

Event	Indication	Note
Si un dispositif est hors ligne.	Deux courts signaux sonores, l'indicateur de **dysfonctionnement X** clignote deux fois. Émet un bip toutes les minutes jusqu'à ce que tous les dispositifs du système soient en ligne.	Les utilisateurs peuvent temporiser l'indication sonore pendant 12 heures.
Si le KeyPad est hors ligne.	Deux courts signaux sonores, l'indicateur de	Il est impossible de temporiser l'indication

	dysfonctionnement X clignote deux fois. Émet un bip toutes les minutes jusqu'à ce que le clavier du système soit en ligne.	sonore.
Si la batterie d'un dispositif est faible.	Trois courts signaux sonores, l'indicateur de **dysfonctionnement X** clignote trois fois. Émet un bip une fois par minute jusqu'à ce que la batterie soit rechargée ou que le dispositif soit retiré.	Les utilisateurs peuvent temporiser l'indication sonore pendant 4 heures.

Les notifications sonores des dysfonctionnements apparaissent lorsque l'indication du clavier est terminée. Si plusieurs dysfonctionnements se produisent dans le système, le clavier signale d'abord la perte de connexion entre le dispositif et la centrale.

Connexion

> La centrale et le dispositif fonctionnant à des fréquences radio différentes sont incompatibles. La gamme de radiofréquences du dispositif peut varier selon les régions. Nous recommandons d'acheter et d'utiliser des dispositifs Ajax dans la même région. Vous pouvez vérifier la gamme des fréquences radio opérationnelles auprès du service d'assistance technique.

Avant de connecter le dispositif

1. Allumez la centrale et vérifiez sa connexion Internet (le logo s'illumine en blanc ou en vert).
2. Installez l'**application Ajax**. Créez le compte, ajoutez la centrale à l'application, et créez au moins une pièce.

3. Assurez-vous que la centrale n’est pas armée, et que la mise s à jour n’est pas en cours en vérifiant son état dans l’application Ajax.

Seuls les utilisateurs disposant de droits d’administrateur peuvent ajouter un périphérique à l’application

Comment connecter KeyPad à la centrale

1. Sélectionnez **Ajouter un dispositif** dans l’application Ajax.
2. Attribuez un nom à le dispositif, scannez/saisissez manuellement le **Code QR** (situé sur le boîtier et l’emballage), puis sélectionnez la pièce de localisation.
3. Sélectionnez **Ajouter** — le compte à rebours commencera.
4. Allumez KeyPad en maintenant le bouton d’alimentation enfoncé pendant 3 secondes — il émet un seul clignotement avec le rétro-éclairage du clavier.

Pour que la détection et le jumelage aient lieu, KeyPad doit être situé dans la couverture du réseau sans fil de la centrale (sur le même site protégé).

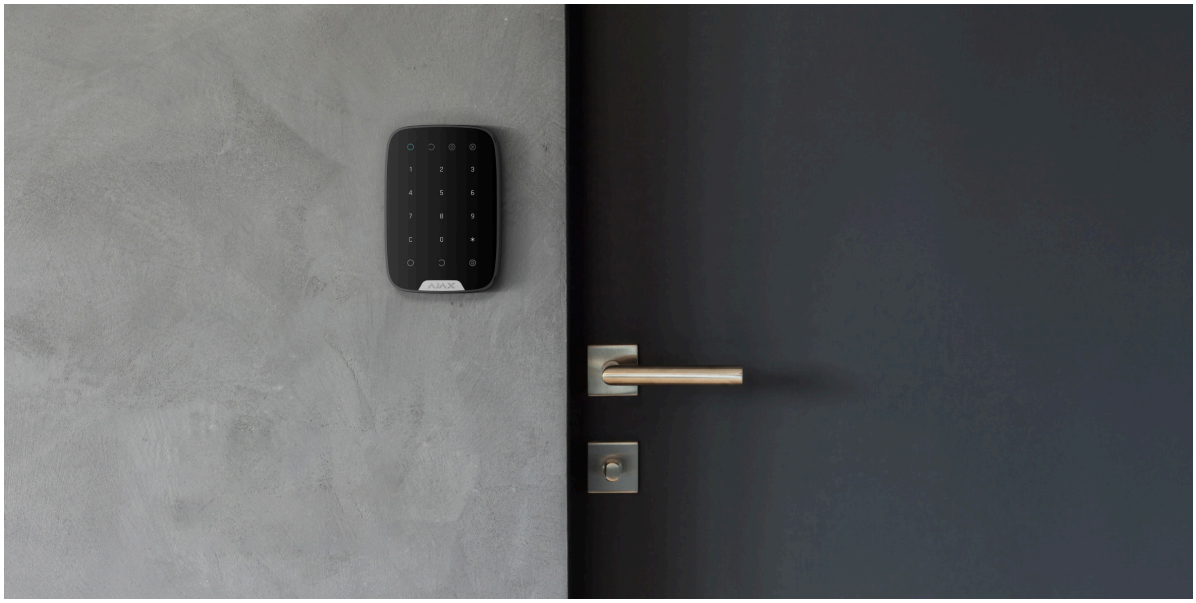
Une demande de connexion à la centrale est transmise pendant une courte durée au moment de la mise en marche du dispositif.

Si KeyPad n’a pas réussi à se connecter à la centrale, éteignez-le pendant 5 secondes et réessayez.

Le dispositif connecté apparaîtra dans la liste des dispositifs de l’application. La mise à jour des états des dispositifs dans la liste dépend de l’intervalle ping du détecteur dans les paramètres de la centrale (la valeur par défaut est de 36 secondes).

Il n’y a pas de codes d’accès prédéfinis pour KeyPad. Avant d’utiliser KeyPad, veuillez définir tous les codes nécessaires: code d’accès général, personnel et aussi un code de contrainte si vous êtes obligé de désarmer le système.

Sélection de l’emplacement



L’emplacement de le dispositif dépend de son éloignement de la centrale et des obstacles qui entravent la transmission du signal radio : murs, sols, grands objets à l’intérieur de la pièce.

> ⚠ Le dispositif est destiné à être installé à l’intérieur uniquement.

N’installez pas KeyPad :

1. Près des équipements de transmission radio, notamment ceux qui fonctionnent sur les réseaux mobiles 2G/3G/4G, des routeurs Wi-Fi, des émetteurs-récepteurs, des stations radio, ainsi qu’une centrale Ajax (il utilise un réseau GSM).
2. Près d’un câblage électrique.
3. Près d’objets métalliques et de miroirs qui peuvent provoquer une atténuation ou un brouillage du signal radio.
4. À l’extérieur des locaux (en plein air).
5. À l’intérieur de locaux dont la température et l’humidité dépassent les limites autorisées.
6. À moins d’un (1) mètre de la centrale.

⚠ Vérifiez l’intensité du signal Jeweller sur le lieu d’installation

Pendant le test, le niveau du signal est affiché dans l’application et sur le clavier avec les indicateurs de mode de sécurité ◯ (mode Armé), ◯ (mode Désarmé), ◯ (mode Nuit) et l’indicateur de dysfonctionnement **X**.

Si le niveau du signal est faible (une barre), nous ne pouvons pas garantir le fonctionnement stable du dispositif. Prenez toutes les mesures possibles pour améliorer la qualité du signal. Au moins, déplacez le dispositif : même un décalage de 20 cm peut améliorer sensiblement la qualité de la réception du signal.

Si l’intensité du signal du dispositif est faible ou instable même après un déplacement, utilisez un **prolongateur de portée du signal radio**.

KeyPad est conçu pour fonctionner lorsqu’il est fixé à la surface verticale. Lorsque vous utilisez KeyPad dans les mains, nous ne pouvons pas garantir le fonctionnement correct du clavier tactile.

États

> **1.** Dispositifs –
>
> **2.** KeyPad

Paramètre	Valeur
Importation de données	Affiche l’erreur lors du transfert de données vers la nouvelle centrale : • **Échoué** – le dispositif n’a pas été transféré vers la nouvelle centrale. En savoir plus

Température	Température du dispositif. Mesuré sur le processeur et change progressivement. L'erreur acceptable entre la valeur dans l'application et la température ambiante est de 2°C. La valeur est mise à jour dès que le dispositif identifie une variation de température d'au moins 2°C. Un scénario par température peut être défini pour contrôler les dispositifs d'automatisation. **En savoir plus**
Intensité du signal Jeweller	Intensité du signal entre la centrale et KeyPad.
Connexion	État de connexion entre la centrale et KeyPad.
Puissance de l'émetteur	Affiche la puissance sélectionnée de l'émetteur. Ce paramètre apparaît lorsque l'option **Max** ou **Atténuation** est sélectionnée dans le menu **Test d'atténuation du signal**. **En savoir plus**
Charge de la batterie	Niveau de charge de la batterie du dispositif. Il y a deux états: • **OK.** • **Batterie faible.** **Comment la charge de la batterie est affichée dans les applications Ajax**
Couvercle	Le mode anti-sabotage du dispositif, qui réagit au détachement ou à l'endommagement du boîtier.

ReX	Affiche l'état d'utilisation du **prolongateur de portée**.
Désactivation forcée	Indique l'état du dispositif : actif, complètement désactivé par l'utilisateur, ou uniquement les notifications sur le déclenchement du bouton anti-sabotage du dispositif sont désactivées.
Désactivation unique	Indique l'état de la désactivation du dispositif jusqu'au premier désarmement : actif, complètement désactivé par l'utilisateur, ou seules les notifications concernant le déclenchement du bouton anti-sabotage du dispositif sont désactivées.
Firmware	Version du firmware du détecteur.
ID du dispositif	Identifiant du dispositif.

Paramètres

1. Dispositifs
2. KeyPad
3. Paramètres

Paramètre	Signification
Nom	Nom du dispositif, peut être modifié.
Pièce	Sélection de la pièce virtuelle à laquelle le v est assigné.
Gestion de groupe	Sélection des groupes de sécurité contrôlés par le dispositif. Vous pouvez sélectionner tous les groupes ou un seul. **Le champ est affiché lorsque le Mode de groupe est activé.**

	Si la fonction Groupes suivis est configurée pour les groupes, leur état de sécurité peut changer automatiquement en fonction de leurs paramètres et des états des groupes initiateurs.
Options d'accès	Choix du mode de vérification pour armer/désarmer • Code des claviers uniquement. • Code d'utilisateur uniquement. • Code des claviers et de l'utilisateur. Pour activer les **Codes d'accès**, configurés pour les personnes qui ne sont pas enregistrées dans le système, sélectionnez les options sur le clavier : **Code des claviers uniquement** ou **Code des claviers et de l'utilisateur**.
Code clavier	Définir d'un code d'accès pour armer/désarmer.
Code de contrainte	Définir un **code de contrainte pour l'alarme silencieuse**.
Bouton de fonction	Sélection du bouton de fonction *: • **Off** : le **bouton de fonction** est désactivé et n'exécute aucune commande lorsqu'il est enfoncé. • **Panique** : en appuyant sur le **bouton de fonction**, le système envoie une alarme

	au centre de télésurveillance et à tous les utilisateurs. • **Désactiver l'alarme incendie interconnectée** : lorsque vous appuyez sur, arrêt de l'alarme sur des **détecteurs d'incendie Ajax**. L'option ne fonctionne que si **l'alarme incendie interconnecté** est activée. ## En savoir plus
Protection contre la pression accidentelle	⚠ Disponible avec OS Malevich 2.31 ou une version ultérieure. Une fois l'option activée, le bouton **Fonction** doit être pressé deux fois pour déclencher une alarme panique. Ce réglage est disponible si le **Bouton de fonction** est réglé sur **Panique**.
Armement sans code	S'il est actif, le système peut être armé en appuyant sur le bouton **Armement** sans code.
Accès non autorisé auto-verrouillage	S'il est actif, le clavier est verrouillé pendant la durée prédéfinie après la saisie d'un code incorrect trois fois de suite en 1 minute. Pendant ce temps, le système ne peut pas être désarmé via KeyPad.
Temps auto-verrouillage, min	Période de verrouillage après une tentative de code d'accès erroné.
Luminosité	Luminosité du rétro-éclairage du clavier.
Volume d'appui	Volume du beeper.
Alerte par sirène si un bouton de panique est appuyé	Le paramètre apparaît si le mode **Alarme** est sélectionné pour le **bouton de fonction**.

	S'il est actif, la pression du **bouton de fonction** déclenche les sirènes installées sur le site.
Test d'intensité du signal Jeweller	Bascule le dispositif en mode de test d'intensité du signal.
Test d'atténuation du signal	Basculez le clavier en mode de test d'affaiblissement du signal (disponible dans les dispositifs à partir de la **version 3.50 du firmware et plus récente**).
Désactivation forcée	Permet à l'utilisateur de déconnecter le dispositif sans le retirer du système. Trois options sont disponibles : • **Non** : le dispositif fonctionne normalement et transmet tous les événements. • **Entièrement** : le dispositif n'exécutera pas les commandes du système ou ne participera pas aux scénarios d'automatisation, et le système ignorera les alarmes du dispositif et autres notifications. • **Couvercle seulement** : le système ignorera uniquement les notifications concernant le déclenchement du bouton anti-sabotage du dispositif. ## En savoir plus
Désactivation unique	Indique l'état du réglage de la désactivation unique du clavier. Trois options sont disponibles : • **Non** : le clavier fonctionne normalement. • **Couvercle seulement** : les notifications sur le déclenchement du bouton anti-sabotage du clavier sont désactivées jusqu'au premier désarmement.

	• **Entièrement** : le clavier est entièrement exclu du fonctionnement du système jusqu'au premier désarmement. Le dispositif n'exécute pas les commandes du système et ne signale pas les alarmes ou autres événements. En savoir plus
Manuel de l'utilisateur	Ouvre le Manuel de l'utilisateur du clavier.
Dissocier le dispositif	Déconnecte le dispositif de la centrale et supprime ses paramètres.

Configuration des codes

Le système Ajax vous permet de configurer un code de clavier, ainsi que des codes personnels pour les utilisateurs ajoutés à la centrale.

Avec la mise à jour de l'**OS Malevich 2.13.1**, nous avons également ajouté la possibilité de créer des codes d'accès pour les personnes qui ne sont pas connectées à la centrale. Ceci est pratique, par exemple, pour permettre à une entreprise de nettoyage d'accéder à la gestion de la sécurité. Découvrez ci-dessous comment configurer et utiliser chaque type de code d'accès.

Pour configurer un code de clavier

1. Allez dans les paramètres du clavier.
2. Sélectionnez **Code du clavier**.
3. Définissez le code du clavier que vous souhaitez.

Pour définir un code de contrainte du clavier

1. Allez dans les paramètres du clavier.
2. Sélectionnez **Code de contrainte**.

3. Définissez le code de contrainte du clavier que vous souhaitez.

Pour configurer un code d'accès personnel

1. Allez aux paramètres de profil (**Centrale** → **Paramètres** → **Utilisateur** → **Vos paramètres de profil**)
2. Cliquez sur **Paramètres code d'accès** (dans ce menu, vous pouvez également voir l'identifiant de l'utilisateur)
3. Définir le **Code utilisateur** et le **Code de contrainte**

Chaque utilisateur définit un code d'accès personnel individuellement !

Pour configurer un code d'accès pour une personne non enregistrée dans le système

1. Accédez aux paramètres de la centrale (**Centrale** → **Paramètres**)
2. Sélectionnez **Codes d'accès des claviers**.
3. Configurez le **Nom d'utilisateur** et le **Code d'accès**.

Si vous souhaitez configurer un code de contrainte, modifier les paramètres d'accès aux groupes, au mode Nuit, à l'ID du code, désactiver temporairement ou supprimer ce code, sélectionnez-le dans la liste et effectuez les modifications.

Un utilisateur PRO ou un utilisateur disposant de droits d'administrateur peut configurer un code d'accès ou modifier ses paramètres. Cette fonction est prise en charge par les centrales avec OS Malevich 2.13.1 et supérieur. Les codes d'accès ne sont pas pris en charge par le panneau de contrôle Hub.

Pour définir le code GIR

Seul un PRO ayant les permissions de configurer le système peut créer et configurer les codes GIR dans les **applications Ajax PRO**. De plus amples informations sur la configuration de cette fonction sont disponibles dans **cet article**.

Les codes GIR sont pris en charge par les centrales (sauf le modèle Hub) avec OS Malevich 2.17 et les versions ultérieures.

Gestion de la sécurité par codes

Vous pouvez contrôler la sécurité de l'ensemble de l'installation ou de groupes distincts en utilisant des codes généraux, personnels, GIR et des codes d'accès (configurés par un PRO ou par un utilisateur ayant des droits d'administration).

Si un code personnel est utilisé, le nom de l'utilisateur qui a armé/désarmé le système est affiché dans les notifications et dans l'historique des événements de la centrale. Si un code GIR est utilisé, le nom du code GIR est affiché. Si un code commun est utilisé, le nom de l'utilisateur qui a changé le mode de sécurité n'est pas affiché.

Les **codes d'accès des claviers** sont compatibles avec les centrales avec OS Malevich 2.13.1 et supérieur. La centrale Hub ne prend pas en charge cette fonction.

Les **codes GIR** sont pris en charge par les centrales (sauf le modèle Hub) avec OS Malevich 2.17 et les versions ultérieures.

Gestion de la sécurité de l'ensemble de l'installation à l'aide d'un code commun

Saisissez le **code commun** et appuyez sur la touche d'activation du mode **Armé** / **Désarmé** / **Nuit** .

Par exemple : 1234 →

Gestion de la sécurité du groupe avec un code commun

Saisissez le **code commun**, appuyez sur *, saisissez l'**ID du groupe** et appuyez sur la touche d'activation du mode **Armé** ◯ / **Désarmé** ◯ / **Nuit** ◯.

Par exemple : 1234 → * → 2 → ◯

Qu'est-ce que l'ID du Groupe ?

Si un KeyPad a été assigné à un groupe (**champ de permission Armé / Désarmé** dans les paramètres du clavier), vous n'avez pas besoin de saisir l'ID du groupe. Pour gérer le mode Armé de ce groupe, il suffit de saisir un code commun ou personnel.

Veuillez noter que si un Keypad est assigné à un groupe, vous ne pourrez pas gérer le **mode Nuit** en utilisant un code commun.

Dans ce cas, le **mode Nuit** ne peut être géré qu'à l'aide d'un code personnel (si l'utilisateur dispose des droits appropriés).

Droits d'utilisation du système Ajax

Gestion de la sécurité de l'ensemble de l'installation à l'aide d'un code personnel

Saisissez l'**ID utilisateur**, appuyez sur *, saisissez votre **code personnel** et appuyez sur la touche d'activation du mode **Armé** ◯ / **Désarmé** ◯ / **Nuit** ◯.

Par exemple : 2 → * → 1234 → ◯

Qu'est-ce que l'ID Utilisateur ?

Gestion de la sécurité du groupe à l'aide d'un code personnel

Saisissez l'**ID d'utilisateur**, appuyez sur *, saisissez le **code personnel**, appuyez sur *, saisissez l'**ID du groupe** et appuyez sur la touche d'activation du mode **Armé** ◯ / **Désarmé** ◯ / **Nuit** ◎.

Par exemple : 2 → * → 1234 → * → 5 → ◯

Qu'est-ce que l'ID du Groupe ?

Qu'est-ce que l'ID Utilisateur ?

Si un KeyPad a été assigné à un groupe (**champ de permission Armé / Désarmé** dans les paramètres du clavier), vous n'avez pas besoin de saisir l'ID du groupe. Pour gérer le mode armé de ce groupe, il suffit de saisir un code personnel.

Gestion de la sécurité de l'ensemble de l'installation à l'aide d'un code d'accès

Saisissez le code d'accès et appuyez sur la touche d'activation du mode **Armé** ◯ / **Désarmé** ◯ / **Nuit** ◎.

Par exemple : 1234 → ◯

Gestion de la sécurité du groupe à l'aide d'un code d'accès

Saisissez le **code d'accès**, appuyez sur l'icône *звезда*, saisissez l'**ID du groupe** et appuyez sur la touche d'activation du mode **Armé** ◯ / **Désarmé** ◯ / **Nuit** ◎.

Par exemple : 1234 → * → 2 → ◯

Qu'est-ce que l'ID du Groupe ?

Utilisation du code de contrainte

Un **code de contrainte** vous permet de déclencher une alarme silencieuse et d'imiter la désactivation de l'alarme. Une alarme silencieuse signifie que l'application Ajax et les sirènes ne se déclencheront pas et ne vous mettront pas en danger. Mais le centre de télésurveillance et d'autres utilisateurs seront alertés instantanément. Vous pouvez utiliser un code de contrainte **personnel** ou **commun**. Vous pouvez également configurer un code de contrainte pour les personnes non enregistrées dans le système.

Qu'est-ce qu'un code de contrainte et comment l'utiliser ?

> Les scénarios et les sirènes réagissent au désarmement de contrainte de la même manière qu'au désarmement normal.

Pour utiliser un code de contrainte commun :

Saisissez le **code de contrainte commun** et appuyez sur la touche **désarmer**.

Par exemple : 4321 →

Pour utiliser un code personnel de contrainte :

Saisissez l'**ID d'utilisateur**, appuyez sur *, puis saisissez votre **code de contrainte personnel** et appuyez sur la touche **désarmer**.

Par exemple : 2 → * → 4422 →

Pour utiliser un code de contrainte :

Saisissez le code de contrainte et appuyez sur la touche de **désarmer**.

Par exemple : 4567 →

Utilisation du code GIR

Le code GIR est activé après le déclenchement de l’alarme pendant la durée configurée dans les paramètres de la centrale et il est valable pendant une période déterminée. Cela garantit que ces codes ne seront utilisés qu’en cas de risque, contrairement aux codes clavier ou utilisateur.

Comment configurer le code GIR

Contrôle de sécurité du site à l’aide du code GIR :

Saisissez le **code GIR** et appuyez sur la touche pour **Armé** ◯ / **Désarmé** ◯ / **Nuit** ◎.

Par exemple : 1234 → ◯

Contrôle de sécurité du groupe à l’aide du code GIR :

Saisissez le **code GIR**, appuyez sur *, entrez l’**ID du groupe** et appuyez sur armer **Armé** ◯ / **Désarmé** ◯ / **Nuit** ◎.

Par exemple : 1234 → * → 2 → ◯

Comment désactiver l’alarme incendie interconnectée

Le clavier KeyPad peut désactiver les alarmes incendie interconnectée en appuyant sur le **bouton de fonction** (si le paramètre correspondant est activé). La réponse du système à une pression sur un bouton dépend des réglages et de l’état du système :

- **Alarmes incendie interconnectées déjà propagées** : par la première pression sur le **bouton de fonction**, toutes les sirènes des détecteurs d’incendie sont mises sous silence, sauf celles qui ont enregistré l’alarme. En appuyant à nouveau sur le bouton, les autres sirènes des détecteurs restent sous silence.
- **Temporisation des alarmes interconnectées, min** : en appuyant sur le **bouton de fonction**, la sirène des détecteurs d’incendie Ajax déclenché est mise sous silence.

En savoir plus sur l’interconnexion d’alarmes incendie interconnectée

Avec la mise à jour d’OS Malevich 2.12, les utilisateurs peuvent désactiver les alarmes des détecteurs d’incendie de leurs groupes, sans affecter le fonctionnement des détecteurs dans des groupes auxquels ils n’ont pas accès.

En savoir plus

Test de fonctionnalité

Le système Ajax permet d’effectuer des tests pour vérifier la fonctionnalité des dispositifs connectés.

Les tests ne démarrent pas tout de suite mais dans un délai de 36 secondes lorsqu’on utilise les réglages standard. Le début de la période d’essai dépend des réglages de l’intervalle ping du détecteur (le paragraphe sur les réglages du **Jeweller** dans les réglages de la centrale).

Test d’intensité du signal Jeweller

Test d’atténuation du signal

Installation

Avant d’installer le détecteur, assurez-vous que vous avez choisi l’emplacement optimal et qu’il est conforme aux directives contenues dans ce manuel !

Le clavier doit être fixé à la surface verticale.

1. Fixez le panneau SmartBracket à la surface à l’aide de vis fournies, en utilisant au moins deux points de fixation (dont un – au-dessus du bouton anti-sabotage). Lors de l’utilisation d’autres moyens de

fixation, assurez-vous qu'ils n'endommagent ni ne déforment le panneau de montage.

> La bande adhésive double face ne peut être utilisée que pour la fixation temporaire du clavier. La bande s'asséchera avec le temps, ce qui peut entraîner la chute du clavier et l'endommagement du dispositif.

2. Placez le clavier sur le panneau de montage et serrez la vis de montage sur le dessous du boîtier.

Dès que le clavier est fixé sur le SmartBracket, il clignote avec l'indicateur de dysfonctionnement **X**, signalant que l'anti-sabotage a été activé.

Si l'indicateur de dysfonctionnement **X** n'a pas clignoté après l'installation dans le SmartBracket, vérifiez l'état de l'anti-sabotage dans l'**application Ajax**, puis contrôlez l'étanchéité de la fixation du panneau.

Si KeyPad est arraché de la surface ou retiré du panneau de montage, vous recevrez la notification.

Entretien du KeyPad et remplacement de la batterie

Vérifiez régulièrement la capacité de fonctionnement du KeyPad.

La batterie installée dans le clavier assure jusqu'à 2 ans de fonctionnement autonome (avec une fréquence d'interrogation de dispositifs par la centrale de 3 minutes). Si la batterie du clavier est faible, le système de sécurité envoie les notifications appropriées, et l'indicateur de dysfonctionnement s'allume et s'éteint en douceur après chaque saisie réussie du code.

Combien de temps les dispositifs Ajax fonctionnent-ils avec des batteries, et qu'est-ce qui influe sur cela

Remplacement de la batterie

Spécifications techniques

Toutes les caractéristiques techniques KeyPad Jeweller

Conformité aux normes

Garantie

La garantie des produits de la Limited Liability Company « Ajax Systems Manufacturing » est valable pendant 2 ans à compter de la date d’achat.

Si le dispositif ne fonctionne pas correctement, veuillez d’abord contacter le service d’assistance technique Ajax. Dans la plupart des cas, les problèmes techniques peuvent être résolus à distance.

Obligations de garantie

Contrat de l’utilisateur

Veuillez contacter notre Assistance technique

- e-mail
- Telegram