Manuel d’utilisateur de KeyPad

Mis à jour November 17, 2021

KeyPad est un clavier tactile d’intérieur sans fil permettant de gérer le système de sécurité Ajax. Utilisé à l’intérieur. Grâce à cet appareil, l’utilisateur peut armer et désarmer le système et voir son statut de sécurité. KeyPad est protégé contre les tentatives de déchiffrage du code d’accès et peut déclencher une alarme silencieuse lorsque le code d’accès est entré sous la contrainte.

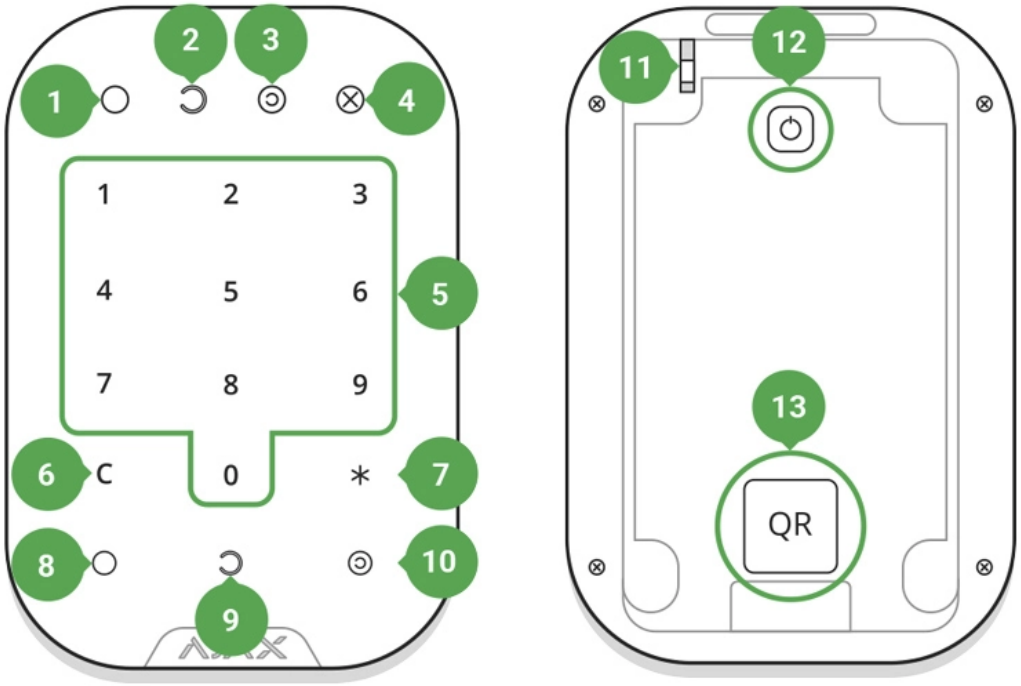
Connecté au système de sécurité Ajax via un protocole radio sécurisé **Jeweller**, KeyPad communique avec le **hub** à une distance allant jusqu’à 1700 m en ligne de mire.

KeyPad fonctionne uniquement avec des hubs Ajax et ne supporte pas la connexion via les modules d’intégration ocBridge Plus ou uartBridge.

L’appareil est configuré via les **apps Ajax** pour iOS, Android, macOS et Windows.

Acheter un clavier KeyPad

Éléments fonctionnels



1. Indicateur en mode armé
2. Indicateur en mode désarmé
3. Indicateur en mode nuit
4. Indicateur de dysfonctionnement
5. Le bloc de boutons numériques
6. Bouton « Effacer »
7. Bouton « Fonction »
8. Bouton « Armer »
9. Bouton « Désarmer »
10. Bouton « Mode nuit »
11. Bouton anti-sabotage
12. Bouton marche/arrêt
13. Code QR

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

Principe de fonctionnement

KeyPad est un appareil de contrôle stationnaire situé à l'intérieur. Ses fonctions comprennent l'armement/le désarmement du système avec une combinaison numérique (ou simplement en appuyant sur le bouton), l'activation du mode Nuit, l'indication du mode de sécurité, le blocage lorsque quelqu'un tente de déchiffrer le code d'accès et le déclenchement de l'alarme silencieuse lorsque quelqu'un force l'utilisateur à désarmer le système.

KeyPad indique l'état de la communication avec le hub et les dysfonctionnements du système. Les boutons sont mis en évidence dès que l'utilisateur touche le clavier, ce qui permet de saisir le code sans éclairage extérieur. KeyPad utilise également un signal sonore pour l'indication.

Pour activer le KeyPad, touchez le clavier : le rétro-éclairage s'allumera et le bip sonore indiquera que le KeyPad s'est réactivé.

Si la batterie est faible, le rétro-éclairage s'allume à un niveau minimum, quels que soient les réglages.

Si vous ne touchez pas le clavier pendant 4 secondes, le KeyPad diminue le rétro-éclairage, et après 12 secondes supplémentaires, l'appareil passe en mode veille.

> Lors du passage en mode veille, KeyPad efface les commandes saisies !

KeyPad prend en charge les codes de 4 à 6 chiffres. Le code d'accès saisi est envoyé au hub après avoir appuyé sur le bouton : ◯ (armer), ◯ (désarmer) ou ◯ (mode nuit). Les commandes incorrectes peuvent être réinitialisées avec le bouton C (Réinitialiser).

Lorsqu'un code d'accès incorrect est saisi trois fois pendant 30 minutes, le clavier se verrouille pour la durée prédéfinie par l'utilisateur administrateur. Une fois que le KeyPad est verrouillé, le hub ignore toute commande, avertissant simultanément les utilisateurs du système de sécurité de la tentative de déchiffrer le code d'accès. L'utilisateur administrateur peut déverrouiller le KeyPad dans l'app. Lorsque le temps prédéfini est écoulé, le KeyPad se déverrouille automatiquement.

Le KeyPad autorise le système à être armé sans code d'accès : en appuyant sur le bouton ◯ (Armer). Cette fonction est désactivée par défaut.

Lorsque le bouton de fonction (*) est pressé sans entrer le code d'accès, le hub exécute la commande assignée à ce bouton dans l'app.

KeyPad peut signaler à une société de sécurité que le système est en train d'être désarmé par force. Le **Code de contrainte** — contrairement au bouton d'alerte — n'active pas les sirènes. KeyPad et l'app signalent que le système a été désarmé avec succès, mais le centre de télésurveillance reçoit une alarme.

> Le système de sécurité Ajax contrôlé par des hubs avec OS Malevich 2.10 et supérieur peut être configuré conformément aux exigences du PD 6662:2017. La norme PD6662: 2017 est une norme d'origine britannique. Cette dernière est prise en charge par les appareils Ajax destinés exclusivement au marché britannique.

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 l'appareil de contrôle qui a été utilisé pour le modifier (la télécommande ou l'app).

Événement	Indication
Clignotement de l'indicateur **X** de dysfonctionnement	L'indicateur avertit en cas de perte de communication avec le hub 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 LED 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

Le hub 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

Connexion

Avant de connecter l'appareil :

1. Allumez le hub et vérifiez sa connexion Internet (le logo s'illumine en blanc ou en vert).
2. Installez l'**app Ajax**. Créez le compte, ajoutez le hub à l'app, et créez au moins une pièce.
3. Assurez-vous que le hub n'est pas armé, et qu'il ne se met pas à jour en vérifiant son statut dans l'app Ajax.

> ⚠ Seuls les utilisateurs disposant de droits d'administrateur peuvent ajouter un périphérique à l'app

Comment connecter KeyPad au hub :

1. Sélectionnez **Ajouter un appareil** dans l'app Ajax.
2. Nommez l'appareil, scannez/écrivez 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 qu'il y ait détection et jumelage, KeyPad doit être situé dans la couverture du réseau sans fil du hub (au même endroit que l'objet protégé).

Une demande de connexion au hub est transmise pendant une courte durée au moment de la mise en marche de l'appareil.

Si KeyPad n'a pas réussi à se connecter au hub, éteignez-le pendant 5 secondes et réessayez.

L'appareil connecté apparaîtra dans la liste des appareils de l'app. La mise à jour des états des appareils dans la liste dépend de l'intervalle ping du détecteur dans les paramètres du hub (la valeur par défaut est de 36 secondes).

Il n'y a pas de mots de passe prédéfinis pour KeyPad. Avant d'utiliser KeyPad, veuillez définir tous les mots de passe nécessaires: mot de passe générale, personnel et aussi le code de contrainte si vous êtes obligé de désarmer le système.

Sélection de l'emplacement

L'emplacement de l'appareil dépend de son éloignement du hub et des obstacles qui entravent la transmission du signal radio : murs, sols, grands objets à l'intérieur de la pièce.

L'appareil est destiné à être installé à l'intérieur uniquement.

N'installez pas KeyPad :

1. Près des équipements de transmission radio, notamment ceux qui fonctionnent dans les réseaux mobiles 2G/3G/4G, des routeurs Wi-Fi, des émetteurs-récepteurs, des stations radio, ainsi qu'un hub 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 du hub.

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

Pendant le test, le niveau du signal est affiché dans l'app 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 de l'appareil. Prenez toutes les mesures possibles pour améliorer la qualité du signal. Au moins, déplacez l'appareil : même un décalage de 20 cm peut améliorer sensiblement la qualité de la réception du signal.

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

KeyPad est conçu pour fonctionner lorsqu'il est fixé à la surface verticale. Lorsque vous utilisez KeyPad en mains, nous ne pouvons pas garantir le bon fonctionnement du clavier à capteur.

États

1. Appareils –
2. KeyPad

Paramètre	Valeur
Température	Température de l'appareil. Mesuré sur le processeur et change progressivement

Intensité du signal Jeweller	Intensité du signal entre le hub et KeyPad
Connexion	État de connexion entre le hub et KeyPad
Charge de la batterie	Niveau de charge de la batterie du appareil. Il y a deux états: • OK • Batterie faible **Comment la charge de la batterie est affichée dans les app Ajax**
Couvercle	Le mode anti-sabotage de l'appareil, qui réagit au détachement ou à l'endommagement du boîtier
ReX	Affiche l'état d'utilisation du prolongateur de portée ReX
Désactivation temporaire	Indique l'état de l'appareil : actif, complètement désactivé par l'utilisateur, ou uniquement les notifications sur le déclenchement du bouton anti-sabotage de l'appareil sont désactivées
Firmware	Version du firmware du détecteur
ID de l'appareil	Identifiant de l'appareil

Réglages

1. Appareils
2. KeyPad
3. Réglages

Réglage	Valeur
Premier champ	Nom de l'appareil, peut être modifié
Pièce	Sélection de la pièce virtuelle à laquelle l'appareil est assigné
Gestion de groupe	Sélection du groupe de sécurité auquel le KeyPad est affecté
Option d'accès	Choix du mode de vérification pour

	armer/désarmer • Code du clavier • Code de l'utilisateur • Code de l'utilisateur et clavier
Code du clavier	Définir d'un code d'accès pour armer/désarmer
Code contrainte	Définir un **code contrainte pour l'alarme silencieuse**
La fonction bouton	Sélection du bouton de fonction * • **Off** — le bouton de fonction est désactivé et n'exécute aucune commande lorsqu'il est enfoncé • **Alarme** — 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 incendie sur les détecteurs FireProtect / FireProtect Plus. L'option ne fonctionne que si l'alarme incendie interconnecté est activée **En savoir plus**
Armer sans code d'accès	S'il est actif, le système peut être armé en appuyant sur le bouton Armer sans code d'accès
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 (pendant 30 minutes). 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 siréne si un bouton panique est appuyé	Le paramètre apparaît si le mode **Alarme** est sélectionné pour la **Fonction** bouton .

	S'il est actif, la pression de la Fonction bouton déclenche les sirènes installées sur l'objet
Test d'intensité du signal Jeweller	Bascule l'appareil en mode test d'intensité du signal
Test d'atténuation du signal	Basculez le clavier en mode test d'affaiblissement du signal (disponible dans les appareils à partir de la **version 3.50 du firmware et plus récente**)
Désactivation temporaire	Permet à l'utilisateur de déconnecter l'appareil sans le retirer du système. Deux options sont disponibles : • **Entièrement** — l'appareil n'exécutera pas les commandes du système ou ne participera pas aux scénarios d'automatisation, et le système ignorera les alarmes de l'appareil et autres notifications • **Couvercle seulement** — le système ignorera uniquement les notifications concernant le déclenchement du bouton anti-sabotage de l'appareil En savoir plus sur la désactivation temporaire des appareils
Manuel de l'utilisateur	Ouvre le Manuel de l'utilisateur du clavier
Dissocier l'appareil	Déconnecte l'appareil du hub et supprime ses paramètres

KeyPad permet de définir des codes d'accès généraux et personnels pour chaque utilisateur.

Pour installer un code d'accès personnel :

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

Chaque utilisateur définit un code d'accès personnel individuellement !

Gestion de la sécurité par mots de passe

Vous pouvez contrôler la sécurité de l'ensemble de l'installation ou de groupes séparés en utilisant des mots de passe communs ou personnels (configurés dans l'app).

Si un mot de passe 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 du hub. Si un mot de passe commun est utilisé, le nom de l'utilisateur qui a changé le mode de sécurité n'est pas affiché.

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

Saisissez le mot de **passe commun** et appuyez sur la touche d'activation du mode **armé** ◯ / **désarmé** ◯ / **Nuit** ◎.

Par exemple : 1234 → ◯

Gestion de la sécurité du groupe avec un mot de passe commun

Saisissez le mot de **passe 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 mot de passe 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 mot de passe commun.

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

Droits d'utilisation du système de sécurité Ajax

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

Saisissez l'**ID utilisateur**, appuyez sur *, saisissez votre mot de **passe 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 mot de passe personnel

Saisissez l'**ID d'utilisateur**, appuyez sur *, saisissez le mot de **passe 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 mot de passe personnel.

Utilisation d'un mot de passe de contrainte

Un **mot de passe de contrainte** vous permet de déclencher une alarme silencieuse et d'imiter la désactivation de l'alarme. Une alarme silencieuse signifie que l'app 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 mot de passe de contrainte personnel ou **commun**.

Qu'est-ce qu'un mot de passe 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 mot de passe de contrainte commun :

Saisissez le mot de **passe de contrainte commun** et appuyez sur la touche **désarmé** .

Par exemple : 4321 →

Pour utiliser un mot de passe personnel de contrainte :

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

Par exemple : 2 → * → 4422 →

Comment fonctionne la fonction silence de l'alarme d'incendie

Le clavier KeyPad peut désactiver les alarmes interconnectées des détecteurs d'incendie en appuyant sur le bouton «Fonction» (si le réglage correspondant est activé). La réponse du système à une pression sur un bouton dépend des réglages et de l'état du système :

- **Interconnexion d'alarmes dans FireProtect déjà propagée** — 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.

- **Durée du délai d'interconnexion d'alarmes dans FireProtect** — en appuyant sur le bouton de fonction, la sirène du détecteur FireProtect/FireProtect Plus déclenché est mise sous silence.

En savoir plus sur l'interconnexion d'alarmes des détecteurs d'incendie

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 de sécurité Ajax permet d'effectuer des tests pour vérifier la fonctionnalité des appareils 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 la période de scannage du détecteur (le paragraphe sur les réglages du « **Jeweller** » dans les réglages du hub).

Test d'intensité du signal Jeweller

Test d'atténuation

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 groupées, en utilisant au moins deux points de fixation (dont un – au-dessus de l'anti-sabotage). Après avoir choisi d'autres pièces de fixation, assurez-vous qu'elles n'endommagent ni ne déforment le panneau.

> La bande adhésif 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 de l'appareil.

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

Dès que le clavier est fixé dans 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'**app Ajax**, puis contrôlez l'étanchéité de la fixation du panneau.

Si KeyPad est arraché de la surface ou retiré du panneau de fixation, 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 par le hub 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 appareils Ajax fonctionnent-ils avec des batteries, et qu'est-ce qui influe sur cela

Remplacement de la batterie

Kit complet

1. KeyPad
2. Panneau de montage SmartBracket
3. Batteries AAA (préinstallées) — 4 pcs
4. Kit d’installation
5. Guide rapide

Spécifications techniques

Type de capteur	Capacitif
Interrupteur anti-sabotage	Oui
Protection contre le déchiffrage du code d’accès	Oui
Protocole de communication radio	Jeweller **En savoir plus**
Bande de fréquences 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 MHzDépend de la région de vente.
Compatibilité	Fonctionne uniquement avec les **centrales Ajax** et les **prolongateurs de portée du signal radio**
Puissance de sortie RF maximale	Jusqu’à 20 mW
Modulation du signal radio	GFSK
Portée du signal radio	Jusqu’à 1700 m (s’il n’y a pas d’obstacles) **En savoir plus**
Alimentation	4 × AAA batteries

Tension d’alimentation	3 V (montage de 4 piles par paire de deux)
Durée de vie de la batterie	Jusqu’à 2 ans
Méthode d’installation	Intérieur
Plage de température de fonctionnement	De -10°C à +40°C
Humidité en fonctionnement	Jusqu’à 75%
Dimensions générales	150 × 103 × 14 mm
Poids	197 g
Durée de vie	10 années
Certification	Niveau de Sécurité 2, Classe Environnementale II en conformité avec les exigences des normes EN 50131-1, EN 50131-3, EN 50131-5-3

Conformité aux normes

Garantie

La garantie des produits de la SOCIÉTÉ À RESPONSABILITÉ LIMITÉE « AJAX SYSTEMS MANUFACTURING » est valable pendant 2 ans après l’achat et ne s’applique pas à la batterie préinstallée.

Si l’appareil ne fonctionne pas correctement, vous devez d’abord contacter le service d’assistance – dans la moitié des cas, les problèmes techniques peuvent être résolus à distance !

Le texte intégral de la garantie

Accord utilisateur

Support technique : **support@ajax.systems**