Superior KeyPad Outdoor Fibra

Clavier filaire avec authentification par Pass, Tag, smartphones et codes. Pour une utilisation extérieure et intérieure.

Gérez votre espace, qu'il fasse beau ou qu'il pleuve

Découvrez la clé tout temps pour votre sécurité et votre automatisation. Contrôlez les modes de sécurité, activez le mode nuit, gérez des groupes spécifiques et exécutez des scénarios avec un seul clavier. Utilisez des codes d'accès classiques ou choisissez la facilité du sans contact. Le boîtier ultra-étroite s'intègre partout et dispose de grands boutons mécaniques, faciles à utiliser avec des gants, offrant un retour tactile agréable. Le boîtier robuste est conçue pour résister à toutes les conditions d'utilisation et conserver sa pleine fonctionnalité, même après des chocs ou des dommages physiques. Un clavier de sécurité solide qui complique la tâche aux intrus pour le forcer.

Caractéristiques clés

Prise en charge des dispositifs d'accès sans contact Cartes Pass et badges Tag dotés de la technologie DESFire®	**Code de contrainte** quand un utilisateur est contraint de désarmer un système	**Quatre types de codes d'accès** ● code clavier principal ● codes personnels ● codes pour les utilisateurs non enregistrés ● code GIR	**Grands boutons mécaniques** retour tactile agréable même pour un utilisateur portant des gants ou des moufles
Contrôle sans contact via smartphone en utilisant Bluetooth Low Energy (BLE)	**Deux modes de fonctionnement :** **Sécurité** **Automatisation** changement facile de mode par une pression prolongée sur le bouton OK	**Protection contre les tentatives de devinette de code d'accès**	**Mode bypass** le clavier démarre une temporisation pour confirmer un changement de mode de sécurité
Bouton de panique intégré	**IP66** protection contre la poussière, l'eau et les températures extrêmes	**IK08** protection contre les impacts physiques	**Jusqu'à 2 000 m (6 550 ft) de communication filaire[1]** avec une centrale Ajax ou un module qui prolonge la ligne Fibra
Mise à jour à distance du firmware	**Gestion et configuration à distance**	**Alarme anti-sabotage** le boîtier est muni de deux bouton anti-sabotage	**Buzzer de 60 dB pour les notifications sonores** informe sur les alarmes, le changement de mode de sécurité, la temporisation à l'armement et au désarmement, le Carillon d'entrée et sur d'autres événements
Connexion filaire Fibra	**Trois couleurs de boîtier en acier inoxydable**		
Connexion avec d'autres dispositifs Fibra sur la ligne	**Notifications push détaillées** **Ajax** Maison: Jardin armé par John **Ajax** Bureau: Mode nuit activé par Anne	**Trois couleurs de boîtier en acier inoxydable**	**Conformité** Grade 3 (EN 50131) PD 6662:2017 ANSI/SIA CP-01-2019 INCERT SSF

Dans un système Ajax, vous pouvez combiner des dispositifs de toutes les catégories de produits : **Protection contre les intrusions** (Superior et Baseline), **Vidéosurveillance**, **Sécurité incendie** et protection des personnes, ou **Confort et automatisation**. Créez un système adapté à vos besoins et gérez-le dans une interface unique.

Il s'agit du dispositif de la **ligne de produits Superior**. Seuls les partenaires accrédités par Ajax Systems peuvent installer, vendre et administrer les produits Superior.

Conçu pour s’adapter à tous les environnements

	Entrepôt	Bureau	Production	Résidence privée

Trois missions, un seul dispositif

Gestion de la sécurité	**Gestion des dispositifs d'automatisation**	**Indication sonore et LED**
Gérez facilement la sécurité d'un site entier, des groupes distincts ou activez le Mode nuit à l'aide d'un seul dispositif. Il dispose également d'un bouton de Fonction, qui peut être configuré comme un bouton de panique ou pour mettre en sourdine les alarmes incendie. Le KeyPad Outdoor peut également fonctionner en mode bypass : il lance une temporisation au désarmement pour que les utilisateurs confirment le changement de mode sécurité via le clavier principal, par exemple, avec un autre clavier Ajax installé à l'intérieur du bâtiment.	Le clavier peut contrôler un ou plusieurs dispositifs d'automatisation, tels que des interrupteurs, des relais, des prises portables intelligentes, des prises encastrées intelligentes et des vannes d'arrêt. Par exemple, un utilisateur peut ouvrir les portes de garage et allumer les lumières extérieures en rentrant chez lui (ou fermer le garage et éteindre les lumières en partant). Il suffit d'appuyer sur un bouton OK pour déclencher un scénario. Le rétroéclairage des boutons indique l'état du dispositif d'automatisation[2] : rouge pour désactivé et vert pour activé.	Le clavier, conçu pour être utilisé avec des gants, dispose de chiffres rétroéclairés qui ne s'estompent pas. Le buzzer intégré vous informe des alarmes, de l'ouverture des portes(**Carillon**), de l'armement/désarmement et des temporisations à l'armement et au désarmement. La luminosité de la LED et le volume du buzzer peuvent être ajustés via les applications Ajax.
● Gestion de la sécurité d'un site entier ou de groupes séparés ● Activation du Mode nuit ● Mode bypass pour démarrer une temporisation au désarmement pour confirmer un changement de mode de sécurité	● Contrôle d'un ou de plusieurs dispositifs d'automatisation à l'aide du bouton OK ● Indication de l'état d'un dispositif d'automatisation avec rétroéclairage	● Notifications sonores des alarmes et des événements ● Boutons mécaniques avec chiffres rétroéclairés qui ne s'estompent pas ● Volume sonore réglable et luminosité LED ajustable

Authentification rapide et sécurisée

Le clavier peut être contrôlé de trois manières différentes, ce qui permet à l'utilisateur de choisir celle qui lui convient le mieux. Les applications Ajax affichent tous les événements, y compris l'activité de l'utilisateur et les détails d'authentification.

Carte Pas et badge Tag

Avec Ajax Pass ou Tag, le système peut être armé ou désarmé d'un seul geste : il suffit de présenter le dispositif d'accès au lecteur de clavier. Chaque utilisation d'un dispositif d'accès sans contact est enregistrée dans l'historique des événements de l'application Ajax. L'administrateur peut révoquer, restreindre ou suspendre temporairement les droits d'accès à tout moment. Les administrateurs peuvent également modifier les droits des utilisateurs en accordant ou en limitant l'accès à des groupes spécifiques.

Le clavier utilise la technologie DESFire®, une solution sans contact pour identifier un utilisateur par une carte ou un badge. DESFire® est basé sur la norme internationale ISO 14443 et combine un chiffrement complet à 128 bits et une protection contre la copie. Cette technologie est également utilisée dans les systèmes de transport des capitales européennes et dans les systèmes d'accès de la NASA.

Smartphone

Obtenez des droits d'accès accordés par l'administrateur système et préautorisez votre smartphone via des applications Ajax pour le contrôle sans contact du clavier en utilisant la technologie Bluetooth Low Energy (BLE).

BLE (Bluetooth Low Energy) est un protocole radio qui permet à un smartphone de gérer le système au lieu de cartes ou de badges. La transmission des données entre un smartphone et le clavier est chiffrée. Le système intègre des mesures visant à empêcher les attaques par Usurpation des données, ce qui rend impossible l'accès non autorisé des cambrioleurs. Le KeyPad Outdoor Fibra prend en charge les smartphones Android et iOS avec BLE 4.2 et supérieur.

Code d'accès

Le clavier prend en charge plusieurs types de codes d'accès :

- **Code clavier (un par clavier)** : un code général configuré pour le clavier.
- **Code personnel** : codes d'accès individuels configurés personnellement par chaque utilisateur du système dans leur application Ajax.
- **Codes pour les utilisateurs non enregistrés** : codes créés par un administrateur pour le personnel de nettoyage ou les agents immobiliers qui n'ont pas de compte Ajax. Ils utilisent le clavier mais n'ont pas accès aux infos du système.
- **Code GIR** : un code d'accès configuré par un administrateur pour que les groupes d'intervention rapide (GIR) puissent accéder aux locaux après avoir reçu une alarme lorsque le propriétaire n'est pas chez lui. Le code n'est activé qu'après une alarme et est valide pour une période spécifiée.

Dispositifs d'accès sans contact

Pass et Tag sont équipés de puces DESFire® originales et partagent les mêmes fonctionnalités, mais dans des boîtiers de forme différente. Un seul Tag ou Pass peut gérer 13 systèmes de sécurité. Les dispositifs d'accès sont vendus séparément par lots de 3,10 ou 100.

Pass Carte sans contact pour gérer les modes de sécurité	Tag Badge sans contact pour gérer les modes de sécurité

Accès et contrôle à distance

Modifiez les droits d'accès et les codes en temps réel via les applications Ajax. Les dispositifs d'accès perdus et les codes compromis peuvent être modifiés à distance en quelques minutes. Un installateur n'a pas besoin de visiter le site.

- Changement de code à distance
- Modification des droits d'accès des utilisateurs à distance
- Blocage à distance des cartes, des badges et des smartphones

Accès pour les utilisateurs non enregistrés

Avec une simple configuration dans les paramètres de la centrale, un professionnel peut créer un code d'accès temporaire pour les employés de bureau, le personnel de nettoyage ou d'autres visiteurs vérifiés.

- Notifications d'ajout, de suppression ou de désactivation de codes

- Un nom unique et un lien ID pour identifier l'utilisateur
- Jusqu'à 99 codes pour les utilisateurs non enregistrés

Prêt à intervenir en cas d'urgence

L'utilisateur est prévenu de l'urgence	Le système transmet une alarme	Le centre de télésurveillance appelle un groupe d'intervention rapide

Le clavier est doté d'un bouton de panique qui déclenche une alarme lorsqu'il est actionné. Le bouton de panique peut être configuré pour avertir les utilisateurs de l'alarme, activer les sirènes ou lancer un scénario d'automatisation. Si l'utilisateur est contraint de laisser entrer des intrus, il peut utiliser un code de contrainte pour simuler un désarmement : le clavier simule un désarmement régulier et envoie immédiatement une alarme à l'entreprise de sécurité, les informant de l'urgence. Pendant ce temps, les applications Ajax et les sirènes installées sur le site restent silencieuses pour éviter de révéler un utilisateur.

- Bouton de panique pour notifier une alarme
- Code de contrainte pour un désarmement simulé

Découvrez le matériel à l'épreuve du temps

Boîtier IP66 étanche avec protection contre les chocs IK08
pour résister à tous les environnements, même sous la pluie, la neige ou le soleil brûlant
Grands boutons mécaniques
pour un accès facile et rapide, même avec des gants ou des moufles
Rétroéclairage LED
pour indiquer les modes de sécurité, l'exécution de scénarios, le changement de mode et d'autres commandes du clavier
Lecteur DESFire® et BLE
pour un accès sans contact avec Tag, Pass ou smartphones
Buzzer de 60 dB
pour informer sur les alarmes, le changement de mode de sécurité, la temporisation à l'armement et au désarmement, Carillon d'entrée, et sur d'autres événements
Panneau de montage SmartBracket
pour installer le clavier sans avoir besoin de désassembler le boîtier
Bornier amovible
pour simplifier le processus de câblage
Deux boutons anti-sabotage
notifications de tentatives d'arracher le clavier de la surface ou de le retirer du panneau de montage
Vis de fixation
pour fixer le clavier sur le panneau de montage

Technologie filaire inédite

Le système Ajax utilise une communication radio bidirectionnelle basée sur le protocole propriétaire Fibra. Il est doté d'un système de chiffrement et d'un système d'authentification pour empêcher le sabotage, l'usurpation ou le vol de données. Les lignes Fibra sont multifonctionnelles et permettent de connecter différents types de dispositifs à une ligne : sirènes, claviers et détecteurs avec levée de doute.

- Jusqu'à 2 000 m (6 550 ft) de communication filaire[1] avec une centrale ou un module qui prolonge la ligne Fibra
- Une ligne pour différents types de dispositifs
- Livraison de photos par la ligne Fibra sans interférence
- Protection contre le sabotage et l'usurpation

L'efficacité énergétique avant tout

La communication Fibra nécessite une consommation d'énergie minimale : le clavier ne consomme que 0,6 W à son maximum. Fibra repose sur le principe de l'accès multiple par répartition dans le temps (TDMA). Chaque dispositif dispose d'un court laps de temps pour échanger des données avec une centrale et son module de communication est inactif le reste du temps. Cela permet de réduire

considérablement la consommation électrique et d'éviter les interférences, même lorsque plusieurs dispositifs communiquent simultanément.

- Consommation d'énergie jusqu'à 0,6 W
- TDMA et modes d'économie d'énergie

Supervision avancée du système

Le clavier fait partie de l'écosystème Ajax, ce qui en fait un véritable dispositif connecté. Chaque élément de l'écosystème fait l'objet d'une surveillance constante. Le clavier échange des données avec la centrale via le protocole Fibra. La centrale communique dans les deux sens avec Ajax Cloud pour fournir des informations en temps réel aux applications Ajax. Le système Ajax surveille l'état du dispositif chaque minute. Si un clavier présente un problème, vous recevrez une notification.

- Dispositif connecté
- Réglage de l'intervalle de ping dans les paramètres de la centrale
- Notifications instantanées concernant la maintenance

Résistance au sabotage

Alarme anti-sabotage Le boîtier du dispositif dispose de deux boutons anti-sabotage pour alerter lorsque le clavier est détaché de la surface ou enlevé du panneau de montage. De plus, le clavier est sécurisé avec une vis de fixation au bas du boîtier pour renforcer sa résistance à toute tentative de démontage.	**Protection contre les tentatives de pirater le code** Le système bloque le clavier après trois tentatives infructueuses pendant une période spécifiée et notifie immédiatement l'incident, empêchant ainsi efficacement les individus non autorisés de deviner le code d'accès.	**Protection contre les dispositifs d'accès non valides** Le clavier ne répond qu'aux dispositifs d'accès autorisés via les applications Ajax. Les puces DESFire® des cartes et des badges sont conformes à la norme internationale ISO 14443 et combinent un chiffrement complet à 128 bits et une protection contre la copie. Le lecteur BLE ne réagit tout simplement pas sur un smartphone s'il n'est pas validé par des applications Ajax.
Boîtier robuste Le clavier dispose d'une protection IP66 et résiste aux températures de −25°C à +60°C (de -13°F à 140°F). Il fonctionne bien sous la pluie et sous la neige. Les boutons mécaniques ne s'estompent pas, il est donc impossible de déterminer les chiffres les plus utilisés et de déterminer le code. Le boîtier répond aux exigences de l'indice de protection IK08 et reste solide même s'il a été frappé ou endommagé physiquement.	**Authentification des dispositifs contre l'usurpation des données** La centrale vérifie les paramètres uniques du dispositif à des fins d'authentification lors de chaque session de communication. Si un paramètre échoue à la vérification, la centrale ignore les commandes du dispositif.	**Détection de perte de communication** Le dispositif échange régulièrement des données avec la centrale. En utilisant l'intervalle ping minimal (3 paquets de données une fois en 12 secondes), il ne faut que 36 secondes pour identifier la perte de communication et notifier l'incident à la société de sécurité et aux utilisateurs.
Protection contre les courts-circuits Le système détecte instantanément un court-circuit sur la ligne et en informe la	**Chiffrement des données** Toutes les données que le système conserve et transmet sont protégées par un chiffrement par bloc avec une clé	**Notifications push détaillées** Le système Ajax signale instantanément les alarmes et les événements par des notifications riches en données : les centres

société de sécurité et les utilisateurs. Et lorsque le problème est résolu, il n'est pas nécessaire de remplacer les fusibles, car le système se réinitialise automatiquement.	dynamique. Le chiffrement rend extrêmement difficile la reprogrammation du dispositif, l'usurpation ou le vol de données.	de télésurveillance et les utilisateurs savent exactement quel dispositif a été déclenché, quand et où l'événement s'est produit.
Ping permanent Le dispositif échange régulièrement des données avec la centrale. Le système contrôle l'état de chaque dispositif et signale tout dysfonctionnement ou perte de connexion.		

Protection renforcée de la ligne Fibra

Découvrez LineProtect, le module permettant de protéger la centrale Ajax et les dispositifs filaires connectés contre le sabotage lorsqu'un intrus provoque des surtensions, des courts-circuits, applique une tension de 110/230 V~ ou utilise des shockers électriques.

Le PRO est roi

Le mythe selon lequel les systèmes filaires sont difficiles à installer est brisé. En mettant au point un ensemble d'outils qui rendent le processus facile et flexible, depuis la conception du projet jusqu'à l'assistance au client et à la maintenance du système, Ajax a minimisé une expérience coûteuse, longue et poussiéreuse pour les utilisateurs PRO. Pas besoin de désassembler le dispositif pour l'installation. Les applications Ajax intuitives permettent d'intégrer rapidement un dispositif au système et chacun d'entre eux peut toujours être reconfiguré à distance. Aucune programmation n'est nécessaire : tout est disponible dès la sortie de l'emballage.

Calculateur d'alimentation Fibra

L'outil en ligne fournit aux ingénieurs de sécurité des données détaillées sur la consommation d'énergie des dispositifs, ce qui permet d'évaluer facilement le projet de système filaire avant l'installation. Il aide à concevoir le projet en temps réel, met en évidence les points problématiques et propose des solutions. Une fois l'opération terminée, les résultats peuvent être téléchargés au format PDF.

Installation

Avec le panneau SmartBracket, l'installateur peut facilement fixer le dispositif au mur. Le kit d'installation comprend tous les éléments de fixation nécessaires. Pas besoin de démonter l'appareil : le panneau avec les bornes est situé à l'extérieur du boîtier sous le SmartBracket pour éviter d'endommager le matériel lors de l'installation. Le panneau est amovible, ce qui facilite l'ensemble du processus. Un niveau à bulle intégré aide le professionnel à obtenir une position de montage parfaitement précise. Pour ranger les câbles, il y a des espaces à l'intérieur du SmartBracket pour les fixer avec des serre-câbles.

- Pas besoin de désassembler le boîtier du dispositif
- Bornier amovible
- Tous les éléments de fixation nécessaires sont inclus dans le kit d'installation
- Vis de fixation pour sécuriser le dispositif sur le panneau de montage

Configuration

Le dispositif est connecté automatiquement à la centrale en scannant la ligne Fibra. Cet outil est disponible dans les applications PRO pour mobile ou pour PC. Il suffit à l'installateur d'attribuer un nom au dispositif et de le relier à une pièce et à un groupe de sécurité. Le dispositif peut également être ajouté en scannant le code QR ou en saisissant manuellement son identifiant.

- Jumelage avec une centrale via le balayage automatique de la ligne ou le code QR
- Identification du dispositif par déclenchement ou indication LED
- Paramètres par défaut optimaux permettant de répondre aux exigences principales

Paramètres

Les applications Ajax sont intuitives et offrent la possibilité de configurer et de tester le dispositif ou obtenir toutes les informations le concernant à distance, partout où une connexion Internet est disponible, à partir d'un smartphone ou d'un PC. L'installateur peut modifier les paramètres à distance et fournir des services rapidement sans avoir à se rendre sur place.

- Configuration et test à distance ou sur place
- Applications iOS, Android, macOS et Windows
- Comptes pour les entreprises et les installateurs

Surveillance

Un système Ajax transmet les alarmes à l'application de télésurveillance **PRO Desktop** ou à un centre de télésurveillance tiers. Le centre de télésurveillance reçoit une notification d'alarme en moins d'une seconde. Les notifications contiennent toutes les informations nécessaires : le nom du dispositif, l'heure de l'événement et la pièce exacte où il se trouve. Le centre de télésurveillance reçoit également une preuve visuelle permettant d'identifier la raison de l'alarme.

- Adressage complet des dispositifs connectés
- Notifications instantanées dans l'application
- Surveillance des alarmes et des événements via Ajax PRO Desktop ou un centre de télésurveillance tiers

[1] Les dispositifs Ajax filaires ont une portée de communication allant jusqu'à 2 000 m (6 550 ft) sans prolongateur de ligne lorsqu'ils utilisent le câble à paires torsadées U/UTP cat.5. D'autres câbles peuvent présenter des valeurs différentes. Veuillez utiliser le Calculateur d'alimentation Fibra pour vérifier avant l'installation si le projet de système filaire fonctionnera dans la réalité.

[2] Lorsque le clavier contrôle un scénario impliquant plusieurs dispositifs d'automatisation, le bouton OK ne peut pas afficher l'état du dispositif ou du scénario avec un indicateur LED. À la place, le clavier notifiera si l'action définie est terminée par un court bip sonore.