

Manuel utilisateur Superior KeyPad TouchScreen Fibra

Mis à jour September 25, 2024



Superior KeyPad TouchScreen Fibra est un clavier filaire avec écran tactile conçu pour gérer le système Ajax. Les utilisateurs peuvent s'authentifier à l'aide de smartphones, de badges Tag, de cartes Pass et de codes. Le dispositif est destiné à être utilisé à l'intérieur.

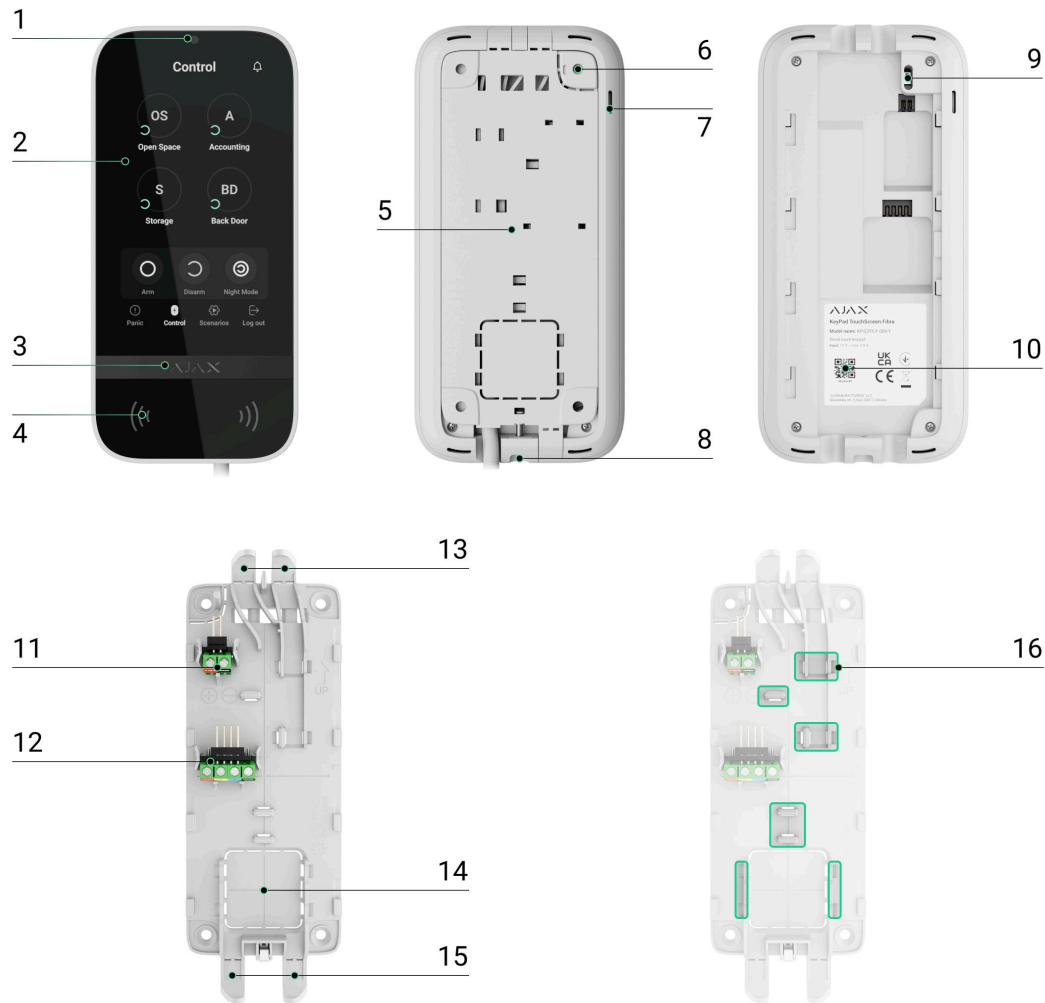
Le clavier fait partie d'un système Ajax et échange des données avec la centrale en utilisant le protocole de communication filaire sécurisé Fibra.

En savoir plus

KeyPad TouchScreen Fibra fait partie de la ligne de produits filaires Fibra. Seuls les partenaires accrédités d'Ajax Systems peuvent installer, vendre et administrer ces produits.

Acheter Superior KeyPad TouchScreen Fibra

Éléments fonctionnels



1. Capteur de lumière ambiante permettant d'ajuster automatiquement la luminosité du rétroéclairage.
2. Écran tactile IPS d'une diagonale de 5 pouces.
3. Logo Ajax avec indicateur LED.
4. Lecteur de cartes/portesclés/Bluetooth.
5. Panneau de montage SmartBracket. Pour retirer le panneau, faites-le glisser vers le bas.
6. Partie perforée du panneau de montage permettant de déclencher un bouton anti-sabotage en cas de tentative de détachement du clavier de la surface. Ne la cassez pas.
7. Buzzer intégré.

8. Trou pour fixer le panneau de montage SmartBracket avec une vis de fixation.
9. Bouton anti-sabotage.
10. Code QR avec l'ID du dispositif pour ajouter le clavier au système Ajax.
11. Bornes pour la connexion d'un bloc d'alimentation externe (non inclus). Les bornes peuvent être retirées des supports si nécessaire.
12. Bornes d'entrée pour connecter la ligne Fibra au Superior KeyPad TouchScreen Fibra.
13. Partie perforée du panneau de montage pour l'acheminement des câbles par le bas.
14. Partie perforée du panneau de montage pour le passage des câbles à travers le mur.
15. Partie perforée du panneau de montage pour l'acheminement des câbles par le bas.
16. Supports pour fixer les câbles avec des attaches.



Centrales compatibles

Pour que le clavier fonctionne, il faut le Hub Hybrid (2G) ou le Hub Hybrid (4G) avec le firmware OS Malevich 2.21 ou supérieur.

Principe de fonctionnement

KeyPad TouchScreen est doté d'un buzzer intégré, d'un écran tactile et d'un lecteur pour l'autorisation sans contact. Le clavier peut être utilisé pour contrôler les modes de sécurité et les dispositifs d'automatisation et pour signaler les alarmes du système.

Le clavier peut régler automatiquement la luminosité du rétroéclairage et se réveiller lorsqu'on s'en approche. La sensibilité est réglable dans l'application. L'interface du clavier KeyPad TouchScreen est héritée de l'application Ajax Security System. Vous pouvez choisir entre une interface foncée et une interface claire. Un écran tactile de 5 pouces de diagonale

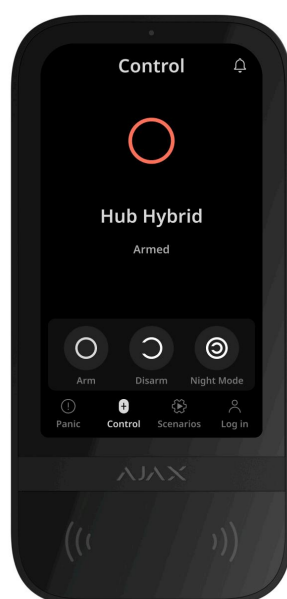
permet d'accéder au mode de sécurité d'un site ou d'un groupe et de contrôler les scénarios d'automatisation. L'écran indique également les dysfonctionnements du système, le cas échéant (lorsque la Vérification de l'intégrité du système est activée).

En fonction des paramètres, l'avertisseur sonore intégré au KeyPad TouchScreen émet une notification concernant :

- les alarmes ;
- le changement de mode de sécurité ;
- les temporisations à l'armement / au désarmement ;
- le déclenchement des détecteurs d'ouverture.

Le clavier est alimenté par le panneau de contrôle et dispose d'une source d'alimentation de secours : des batteries rechargeables préinstallées. KeyPad TouchScreen peut également être alimenté par une unité d'alimentation tierce avec une plage de tension de 10,5 – 14 V₌₌ et un courant de fonctionnement à partir de 0,5 A.

Contrôle de sécurité



KeyPad TouchScreen permet d'armer et de désarmer l'ensemble du site ou des groupes spécifiques, et d'activer le **Mode nuit**. Utilisez l'onglet **Contrôle**  pour modifier le mode de sécurité. Vous pouvez contrôler la sécurité à l'aide du KeyPad TouchScreen en utilisant :

1. **Smartphones.** Avec l'application Ajax Security System installée et la prise en charge du Bluetooth Low Energy (BLE). Les smartphones peuvent être utilisés à la place du Tag ou du Pass pour l'autorisation de l'utilisateur. BLE est un protocole radio à faible consommation d'énergie. Le clavier est compatible avec les smartphones Android et iOS dotés de la technologie BLE 4.2 ou d'une version plus récente.
2. **Cartes ou porteclés.** Pour identifier rapidement et en toute sécurité les utilisateurs, le clavier KeyPad TouchScreen utilise la technologie DESFire®. DESFire® est basé sur la norme internationale ISO 14443 et combine un chiffrement complet à 128 bits et une protection contre la copie.
3. **Codes.** KeyPad TouchScreen prend en charge les codes généraux, les codes personnels et les codes pour les utilisateurs non enregistrés.

Codes d'accès

- **Code clavier** est un code général configuré pour le clavier. Lorsqu'il est utilisé, tous les événements sont transmis aux applications Ajax par le biais du clavier.
- **Code utilisateur** est un code personnel défini pour les utilisateurs connectés à la centrale. Lorsqu'il est utilisé, tous les événements sont transmis aux applications Ajax au nom de l'utilisateur.
- **Codes d'accès des claviers** sont des codes configurés pour des personnes qui ne sont pas enregistrées dans le système. Lorsqu'il est utilisé, les événements sont délivrés 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.



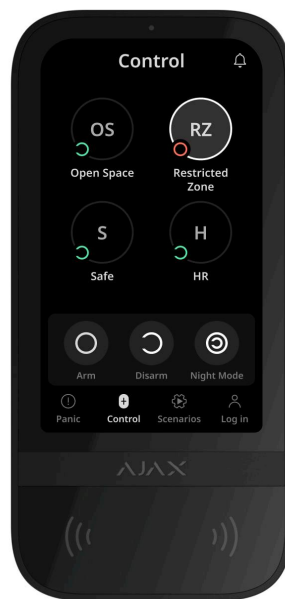


Hub Hybrid (2G) et Hub Hybrid (4G) prennent en charge jusqu'à 50 codes personnels, d'accès des claviers et codes GIR.

Les droits d'accès et les codes peuvent être ajustés dans les applications Ajax. Si le code est compromis, il peut être modifié à distance, sans avoir besoin d'appeler un installateur sur le site. Si un utilisateur perd son Pass, son Tag ou son smartphone, un administrateur ou un PRO disposant de droits de configuration du système peut instantanément bloquer le dispositif dans l'application. En attendant, un utilisateur peut utiliser un code personnel pour gérer le système.

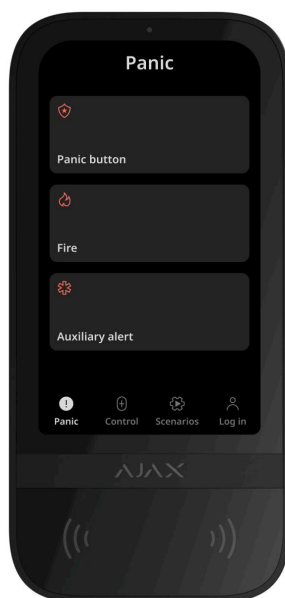


Contrôle de sécurité des groupes



KeyPad TouchScreen permet de contrôler la sécurité des groupes (si le **Mode groupe** est activé). Vous pouvez également régler les paramètres du clavier pour déterminer les groupes qui seront partagés (groupes de clavier). Par défaut, tous les groupes sont visibles sur l'écran du clavier dans l'onglet **Contrôle** . Pour en savoir plus sur la gestion de la sécurité des groupes, consultez [ce chapitre](#).

Boutons d'urgence



En cas d'urgence, le clavier est doté de l'onglet **Panique** (!) avec trois boutons :

- Bouton de panique ;
- Incendie ;
- Appeler les secours.

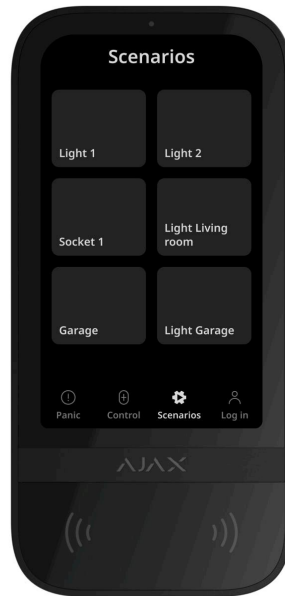
Dans l'application Ajax, un administrateur ou un PRO ayant les droits de configurer le système peut sélectionner le nombre de boutons affichés dans l'onglet **Panique** (!). Deux options sont disponibles dans les paramètres du KeyPad TouchScreen : uniquement **Bouton de panique** (par défaut) ou les trois boutons. Le texte des notifications dans les applications et les codes d'événement transmis au centre de télésurveillance dépendent du type de bouton sélectionné.

Vous pouvez également activer la protection contre les appuis accidentels. Dans ce cas, l'utilisateur confirme la transmission de l'alarme en appuyant sur la touche **Envoyer** sur l'écran du clavier. L'écran de confirmation s'affiche après avoir appuyé sur un bouton de panique.



Le fait d'appuyer sur les boutons d'urgence peut déclencher des Scénarios d'alarme dans le système Ajax.

Gestion des scénarios



L'onglet séparé du clavier peut contenir jusqu'à six boutons pour le contrôle d'un seul dispositif d'automatisation ou d'un groupe de dispositifs. Les scénarios de groupe de dispositifs permettent de gérer simultanément plusieurs interrupteurs, relais ou prises.

Créez des scénarios d'automatisation dans les paramètres du clavier et gérez-les à l'aide de KeyPad TouchScreen.

En savoir plus

Indication des dysfonctionnements et du mode de sécurité

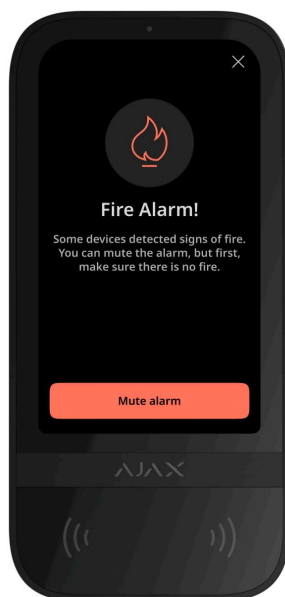
KeyPad TouchScreen informe les utilisateurs des dysfonctionnements du système et du mode de sécurité par le biais de :

- l'écran ;
- le logo ;
- l'indication sonore.

Selon les réglages, le logo s'allume en rouge en permanence ou lorsque le système ou le groupe est armé. L'indication du KeyPad TouchScreen n'apparaît sur l'écran que lorsqu'il est actif. Un buzzer intégré signale les alarmes, les ouvertures de porte et les temporisations à l'armement et au désarmement.



Silence de l'alarme incendie



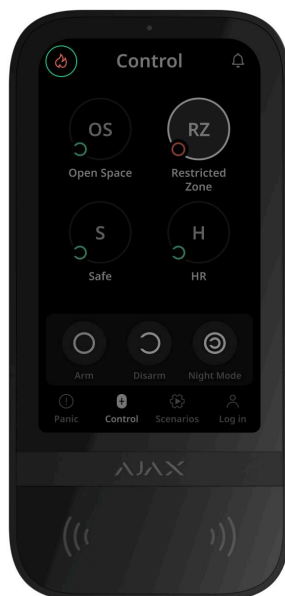
En cas d'alarme incendie dans le système, vous pouvez la mettre en sourdine à l'aide du KeyPad TouchScreen.



Le fait d'appuyer sur le bouton d'urgence **Incendie** dans l'onglet Panique n'active pas Alarme incendie interconnectée (si elle est activée). En cas d'envoi d'un signal d'urgence à partir du clavier, une notification appropriée sera transmise à l'application et au centre de télésurveillance.

L'écran contenant des informations sur l'alarme incendie et le bouton permettant de la mettre en sourdine s'affiche sur tous les claviers KeyPad TouchScreen dont la fonction **Désactiver l'alarme incendie** est activée. Si quelqu'un a déjà appuyé sur le bouton muet d'un clavier, une notification correspondante s'affiche sur les autres écrans des claviers KeyPad TouchScreen. Les utilisateurs peuvent fermer l'écran de mise en sourdine

de l'alarme incendie et utiliser d'autres fonctions du clavier. Pour réouvrir l'écran de mise en sourdine, appuyez sur l'icône 🔥 sur l'écran tactile du KeyPad TouchScreen.



Pour afficher instantanément l'écran de mise en sourdine de l'alarme incendie sur le clavier KeyPad TouchScreen, activez la bascule **Écran toujours actif** dans les paramètres du clavier. Branchez également le bloc d'alimentation tiers.

Sinon, l'écran de mise en sourdine ne s'affichera que lorsque le clavier se réveille.

Code de contrainte

KeyPad TouchScreen prend en charge un **code de contrainte** qui vous permet de simuler le désarmement du système. Dans ce cas, ni l'application Ajax ni les sirènes installées sur le site ne révéleront vos actions. Le centre de télésurveillance et les autres utilisateurs du système de sécurité seront néanmoins avertis de l'incident.

[En savoir plus](#)

Pré-autorisation de l'utilisateur

La fonction de **Pré-autorisation** est essentielle pour empêcher tout accès non autorisé à la centrale et aux données de l'état actuel du système. La fonction peut être activée séparément pour les onglets **Contrôle**  et **Scénarios**  dans les paramètres du clavier.

L'écran de saisie du code s'affiche dans les onglets pour lesquels la pré-autorisation est activée. L'utilisateur doit d'abord s'authentifier, soit en entrant un code, soit en présentant un dispositif d'accès personnel au clavier. La seule exception est l'onglet **Alarme** , qui permet aux utilisateurs non autorisés d'envoyer un signal d'urgence.



Accès non autorisé auto-verrouillage

Si un code incorrect est saisi ou si un dispositif d'accès non vérifié est utilisé trois fois de suite en moins d'une minute, le clavier se verrouille pour la durée spécifiée dans ses paramètres. Pendant ce temps, la centrale ignore tous les codes et dispositifs d'accès, tout en informant les utilisateurs du système de sécurité de la tentative d'accès non autorisé. KeyPad TouchScreen désactivera le lecteur et bloquera l'accès à tous les onglets. L'écran du clavier affiche une notification appropriée.

Un PRO ou un utilisateur disposant de droits de configuration du système peut débloquent le clavier via l'application avant l'expiration du délai de verrouillage spécifié.

Armement en deux étapes

Le clavier KeyPad TouchScreen peut participer à l'armement en deux étapes, mais ne peut pas être utilisé en tant que dispositif de deuxième étape. Le processus d'armement en deux étapes à l'aide d'un Tag, d'un Pass ou d'un smartphone est similaire à l'utilisation d'un code personnel ou général sur le clavier.

[En savoir plus](#)

Protocole de transfert de données Fibra

Le clavier utilise la technologie Fibra pour transmettre les alarmes et les événements et pour mettre à jour le firmware. Il s'agit d'un protocole filaire de transfert de données permettant d'assurer une communication bidirectionnelle rapide et fiable entre la centrale et les appareils connectés.

En savoir plus



Transmission d'événements au centre de télésurveillance

Le système de sécurité Ajax peut transmettre des alarmes à l'application de surveillance PRO Desktop ainsi qu'au centre de télésurveillance au formats **SurGard (Contact ID)**, **SIA (DC-09)**, **ADEMCO 685** et d'autres protocoles.

KeyPad TouchScreen peut transmettre les événements suivants :

1. Saisie du code de contrainte.
2. Appui sur le bouton de panique. Chaque bouton a son propre code d'événement.
3. Verrouillage du clavier suite à une tentative d'accès non autorisé.
4. Alarme/récupération du bouton anti-sabotage.
5. Perte/rétablissement de la connexion entre KeyPad TouchScreen et la centrale.
6. Armement/désarmement du système.
7. Tentative infructueuse d'armer le système de sécurité (avec vérification de l'intégrité activée).
8. Désactivation forcée /activation du clavier.
9. Désactivation unique /activation du clavier.
10. Détection de basse tension sur la ligne Fibra et rétablissement de la tension à des valeurs normales.

11. Faible charge de la batterie de secours et rétablissement de la charge de la batterie.
12. Dysfonctionnement/rétablissement de la batterie de secours.
13. Détection d'un dysfonctionnement ; le module ne peut pas charger la batterie de secours.



Lorsqu'une alarme est reçue, l'opérateur du centre de télésurveillance sait exactement ce qui s'est passé et où envoyer l'équipe d'intervention rapide. L'adressage des appareils Ajax permet d'envoyer des événements au PRO Desktop ou au centre de télésurveillance en précisant le type d'appareil, son nom, le groupe de sécurité et la pièce virtuelle. Veuillez noter que la liste des paramètres transmis peut varier en fonction du type de centre de télésurveillance et du protocole de communication sélectionné avec ce dernier.



L'ID et le numéro de l'appareil se trouvent dans ses [États dans l'application Ajax](#).

Ajout au système



Superior KeyPad TouchScreen Fibra est compatible avec les centrales [Hub Hybrid \(2G\)](#) et [Hub Hybrid \(4G\)](#). Seuls les partenaires vérifiés peuvent ajouter et configurer les dispositifs Fibra dans les applications Ajax PRO.

Avant d'ajouter un appareil

1. Installez une [application Ajax PRO](#).
2. Connectez-vous à un [compte PRO](#) ou créez-en un nouveau.
3. Sélectionnez un espace ou créez-en un nouveau.

[Qu'est-ce qu'un espace](#)

Comment créer un espace



La fonctionnalité d'**espace** est disponible pour les applications à partir des versions suivantes :

- Ajax Security System 3.0 pour iOS ;
- Ajax Security System 3.0 pour Android ;
- Ajax PRO: Tool for Engineers 2.0 pour iOS ;
- Ajax PRO: Tool for Engineers 2.0 pour Android ;
- Ajax PRO Desktop 4.0 pour macOS ;
- Ajax PRO Desktop 4.0 pour Windows.



4. Ajoutez au moins une pièce virtuelle.
5. Ajoutez une centrale compatible à l'espace. Assurez-vous que la centrale est allumée et qu'elle dispose d'un accès Internet via Ethernet, Wi-Fi et/ou réseau mobile.
6. Assurez-vous que l'espace est désarmé et que la mise à jour de la centrale n'est pas en cours, en vérifiant son statut dans l'application Ajax.

Ajout à la centrale

Il y a deux façons d'ajouter des appareils dans l'application Ajax PRO : automatiquement et manuellement.

Automatiquement Manuellement

Pour ajouter un dispositif automatiquement :

1. Ouvrez l'application Ajax PRO et sélectionnez la centrale à laquelle vous souhaitez ajouter votre KeyPad TouchScreen.

2. Allez dans l'onglet **Appareils**  et cliquez sur **Ajouter un appareil**.
3. Sélectionnez **Ajouter tous les appareils Fibra**. La centrale va balayer les lignes Fibra. Après le balayage, tous les dispositifs qui sont physiquement connectés à la centrale, mais qui n'ont pas encore été ajoutés au système, s'affichent.
4. Sélectionnez l'appareil souhaité dans la liste. Une fois sélectionné, l'indicateur LED clignote pour identifier ce dispositif et la notification correspondante apparaît sur l'écran du clavier.
5. Spécifiez un nom, une pièce et un groupe si le Mode groupe est activé. Cliquez sur **Enregistrer**.



Si la tentative de connexion échoue, vérifiez que la connexion câblée soit correctement configurée avant de réessayer. Si le nombre maximal d'appareils (100 pour Hub Hybrid) a déjà été ajouté à la centrale, vous recevrez une notification d'erreur lors de l'ajout.



KeyPad TouchScreen est doté d'un avertisseur sonore intégré qui peut signaler des alarmes et des états spécifiques du système, mais il ne s'agit pas d'une sirène. Vous pouvez ajouter jusqu'à 10 dispositifs de ce type (y compris les sirènes) à la centrale. Pensez-y lors de la conception de votre système de sécurité.

Le clavier connecté à la centrale apparaîtra dans l'application Ajax dans la liste des appareils de la centrale. La mise à jour des états des dispositifs de la liste dépend des paramètres **Jeweller/Fibra** (la valeur par défaut est de 36 secondes).



KeyPad TouchScreen ne fonctionne qu'avec une seule centrale. Lorsqu'il est connecté à une nouvelle centrale, le dispositif cesse d'envoyer des événements à l'ancienne. Une fois ajouté à une nouvelle centrale, le clavier n'est pas automatiquement supprimé de la liste des appareils de l'ancienne centrale. Ceci doit être fait manuellement via l'application Ajax.

Dysfonctionnements

Lorsqu'un dysfonctionnement du KeyPad TouchScreen est détecté, l'application Ajax affiche un compteur de dysfonctionnement sur l'icône du dispositif. Tous les dysfonctionnements sont indiqués dans les états du clavier. Les champs présentant des dysfonctionnements seront mis en évidence en rouge.

Un dysfonctionnement est affiché si :



- le boîtier du clavier est ouvert (le bouton anti-sabotage s'est déclenché) ;
- il n'y a pas de connexion avec la centrale ;
- la batterie de secours du clavier est faible ;
- la batterie de secours n'est pas installée ;
- la batterie de secours est défectueuse ;
- KeyPad TouchScreen présente un dysfonctionnement et ne peut pas charger la batterie de secours ;
- basse tension sur la ligne Fibra ;
- la température du clavier dépasse les limites admissibles.

Icônes

Icônes dans l'application

Les icônes dans l'application affichent certains états du clavier. Pour y accéder :

1. Connectez-vous à l'application Ajax.
2. Sélectionnez la centrale.
3. Allez dans l'onglet **Appareils**



Icône	Signification
	Intensité du signal Fibra. Affiche l'intensité du signal entre la centrale et le dispositif. La valeur recommandée est de 2 ou 3 barres. <u>En savoir plus</u>
	Le niveau de charge de la batterie de secours du clavier est OK ou elle est en cours de chargement.
	Le niveau de charge de la batterie de secours du clavier est faible.
	La batterie de secours a un dysfonctionnement ou n'est pas installée.
	S'affiche lorsque le module Bluetooth du clavier est activé.
	La configuration du Bluetooth n'est pas terminée. La description est disponible dans les états du clavier.
	Une mise à jour du firmware est disponible. Allez dans les états ou les paramètres du clavier pour trouver la description et lancer une mise à jour.  L'icône n'est pas disponible dans l'application Ajax Security System avec la version 3.0 et plus pour iOS et Android. <u>En savoir plus</u>
	La Lecture du Pass/Tag est activée dans les paramètres du KeyPad TouchScreen.
	Le Carillon à l'ouverture est activé dans les paramètres du KeyPad TouchScreen.
	Le dispositif est désactivé de façon permanente. <u>En savoir plus</u>

	Les notifications d'alarme anti-sabotage sont désactivées de manière permanente. <u>En savoir plus</u>
	Le dispositif est désactivé jusqu'au premier désarmement du système. <u>En savoir plus</u>
	Les notifications d'alarme anti-sabotage sont désactivées jusqu'au premier désarmement du système. <u>En savoir plus</u>
	L'appareil n'a pas été transféré à la nouvelle centrale. <u>En savoir plus</u>



Icônes sur l'écran

Des icônes apparaissent en haut de l'écran et informent sur des états ou des événements spécifiques du système.

Icône	Signification
	La restauration du système est nécessaire après une alarme. En fonction de son <u>type de compte</u>, l'utilisateur peut soit envoyer une demande de restauration, soit restaurer le système. Pour ce faire, cliquez sur l'icône et sélectionnez le bouton requis à l'écran. <u>En savoir plus</u>
	Désactiver l'alarme incendie. Elle apparaît après la fermeture de <u>l'écran de mise en sourdine de l'alarme incendie</u>. Les utilisateurs peuvent cliquer sur l'icône à tout moment et mettre en sourdine l'alarme incendie, y compris l'alarme incendie interconnectée.

	<u>En savoir plus</u>
	Le Carillon à l'ouverture est désactivé. Cliquez sur l'icône pour l'activer. Apparaît sur l'écran lorsque les <u>paramètres requis sont ajustés</u>.
	Le Carillon à l'ouverture est activé. Cliquez sur l'icône pour le désactiver. Apparaît sur l'écran lorsque les <u>paramètres requis sont ajustés</u>.



États

Les états comprennent des informations sur l'appareil et ses paramètres de fonctionnement. Les états du KeyPad TouchScreen se trouvent dans les applications Ajax :

1. Allez dans l'onglet **Appareils** .
2. Sélectionnez votre **KeyPad TouchScreen** dans la liste.

Paramètre	Valeur
Dysfonctionnement	En cliquant sur ⓘ, vous ouvrez la liste des dysfonctionnements du KeyPad TouchScreen. Ce champ s'affiche si un dysfonctionnement est détecté.
Nouvelle version du firmware disponible 	En cliquant sur ⓘ, les instructions de mise à jour du firmware du clavier s'affichent. Le champ s'affiche si une <u>nouvelle version du firmware</u> est disponible.

	 L'état n'est pas affiché dans l'application Ajax Security System avec la version 3.0 et plus pour iOS et Android.
Avertissement 	En cliquant sur  , la liste des paramètres et des autorisations à accorder à l'application pour le bon fonctionnement du clavier s'affiche.
Intensité du signal Fibra	Intensité du signal Fibra entre l'appareil et la centrale. La valeur recommandée est de 2 ou 3 barres. Fibra est un protocole pour transmettre des événements et des alarmes du KeyPad TouchScreen.
Connexion via Fibra	État de la connexion sur le canal Fibra entre l'appareil et le hub : • En ligne — le détecteur est connecté à la centrale. État normal. • Hors ligne — le dispositif n'est pas connecté à la centrale. Vérifiez la connexion de l'appareil.
Tension de la ligne	La valeur de la tension sur la ligne Fibra à laquelle le clavier d'intégration est connecté.





Charge de la batterie	L'état de batterie de l'appareil : • OK. • Faible. • Charge. • Erreur. • La batterie n'est pas installée. L'indication de la charge de batterie sur la ligne Fibra est affichée par l'icône .
Couvercle	L'état du bouton anti-sabotage du clavier qui réagit à l'arrachement ou à l'ouverture du boîtier du dispositif : • Ouvert – le clavier a été retiré du SmartBracket, ou l'intégrité du boîtier a été compromise. Vérifiez l'appareil. • Fermé – le clavier est installé sur le panneau de montage SmartBracket. L'intégrité du boîtier du dispositif et du panneau de montage n'est pas compromise. État normal. <u>En savoir plus</u>
Alimentation externe	État de la connexion de l'alimentation externe du clavier : • Connecté – l'alimentation externe est connectée au dispositif. • Déconnecté – l'alimentation externe est déconnectée. L'appareil fonctionne sur batterie. <u>En savoir plus</u>
Écran toujours actif	Affiché lorsque la bascule Écran toujours actif est activée dans les paramètres du



	clavier et que l'alimentation externe est connectée.
Indication sonore des alarmes	Indique l'état du paramètre Activer le buzzer du clavier si une alarme est détectée dans le système.
Durée de l'alarme	Durée du signal sonore en cas d'alarme. Réglage par incréments de 3 secondes. Affiché lorsque l'option Activer le buzzer du clavier si une alarme est détectée dans le système est activée.
Lecture du Pass/Tag	Indique si le lecteur de cartes et de porteclés est activé.
Bluetooth	Indique si le module Bluetooth du clavier est activé pour contrôler le système à l'aide d'un smartphone.
Signaux sonores	
Armement/Désarmement	Si activé, le clavier notifie l'armement et le désarmement par un bip court.
Activation/Désactivation du Mode nuit	Si activé, le clavier vous informe de l'activation ou de la désactivation du <u>Mode nuit</u> en émettant un bip court.
Temporisations désarmement	Si activé, le clavier émet un bip pour signaler les <u>temporisations au désarmement.</u>
Temporisations armement	Si activé, le clavier émet un bip pour signaler les <u>temporisations à l'armement.</u>
Temporisations désarm/Nuit	Si activé, le clavier émet des bips pour signaler les <u>temporisations au désarmement</u> en Mode nuit.
Temporisations arm/Nuit	Si activé, le clavier émet des bips pour signaler les <u>temporisations à l'armement</u> en Mode nuit.
Carillon à l'ouverture	Si activé, une sirène notifie le déclenchement du détecteur d'ouverture lorsque le système est Désarmé.

	<u>En savoir plus</u>
Volume du bip	Affiché lorsque les notifications d'armement/désarmement, de temporisations à l'armement et au désarmement et d'ouverture sont activées. Indique le niveau de volume du buzzer pour les notifications.
Désactivation forcée	Indique l'état du réglage de la désactivation forcée du clavier : • Non – le dispositif fonctionne normalement. • Couvercle seulement – l'administrateur de la centrale a désactivé les notifications d'activation d'alarme pour le bouton anti-sabotage du clavier. • Entièrement – le clavier est entièrement exclu du fonctionnement du système. L'appareil ne réagit pas aux commandes du système et ne signale pas les alarmes ou autres événements. <u>En savoir plus</u>
Désactivation unique	Indique l'état du réglage de la désactivation unique du clavier : • Non – le dispositif fonctionne normalement. • Couvercle seulement – les notifications concernant 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. L'appareil ne réagit pas aux commandes du système et ne signale pas les alarmes ou autres événements.



	<u>En savoir plus</u>
Firmware	Version firmware du clavier.
ID	ID du clavier. Également disponible sur le code QR figurant sur le boîtier du dispositif et son emballage.
Appareil n°	Numéro de la boucle du dispositif (zone).
Ligne n°	Le numéro de la ligne Fibra à laquelle KeyPad TouchScreen est connecté.



Paramètres

Pour modifier les paramètres du KeyPad TouchScreen dans l'application Ajax :

1. Allez dans l'onglet **Appareils** .
2. Sélectionnez le **KeyPad TouchScreen** dans la liste.
3. Allez dans les **Paramètres** en cliquant sur l'icône de l'engrenage .
4. Définissez les paramètres requis.
5. Cliquez sur **Retour** pour enregistrer les paramètres.

Paramètre	Valeur
Nom	Nom du clavier. Il est affiché dans la liste des dispositifs de la centrale, dans le texte SMS et dans les notifications du flux d'événements. Pour modifier le nom de la prise intelligente, cliquez sur le champ de texte. Le nom peut contenir 12 caractères cyrilliques ou 24 caractères latins.



Pièce	Sélection de la pièce virtuelle à laquelle le Keypad TouchScreen est assigné. Le nom de la pièce est affiché dans le texte SMS et les notifications dans le flux d'événement.
Options d'accès	Sélection de la méthode d'armement/désarmement : • Codes clavier uniquement. • Codes de l'utilisateur uniquement. • Codes clavier et de l'utilisateur. Pour activer les Codes d'accès des claviers configurés pour les personnes qui ne sont pas enregistrées dans le système, sélectionnez les options sur le clavier : Codes des claviers uniquement ou Codes des claviers et de l'utilisateur.
Code clavier	Sélection d'un code général pour le contrôle de sécurité. Contient 4 à 6 chiffres.
Code de contrainte	Sélection d'un code de contrainte générale pour l'alarme silencieuse. Contient 4 à 6 chiffres. <u>En savoir plus</u>
Distance de réveil de l'écran	Configuration d'une distance à laquelle le clavier réagit à l'approche et active son écran : • Minimum. • Faible. • Normal (par défaut). • Élevé. • Maximum.

	Sélectionnez la sensibilité optimale pour que le clavier réagisse à l'approche comme vous le souhaitez.
Désactiver l'alarme incendie	Lorsque cette fonction est activée, les utilisateurs peuvent mettre en sourdine l'alarme des détecteurs d'incendie Ajax (même Interconnectée) à l'aide d'un clavier. <u>En savoir plus</u>
Lecture du Pass/Tag	Lorsque cette option est activée, le mode de sécurité peut être contrôlé par les dispositifs d'accès Pass et Tag .
Bluetooth	Lorsque cette option est activée, le mode de sécurité peut être contrôlé par un smartphone.
Sensibilité Bluetooth	Réglage de la sensibilité du module Bluetooth du clavier : • Minimum. • Faible. • Normal (par défaut). • Élevé. • Maximum. Disponible si la bascule Bluetooth est activée.



Accès non autorisé auto-verrouillage	Lorsque cette fonction est activée, le clavier est verrouillé pendant une durée prédéfinie si un code incorrect est saisi ou si des dispositifs d'accès non vérifiés sont utilisés plus de trois fois de suite en l'espace d'une minute. Un PRO ou un utilisateur disposant de droits de configuration du système peut débloquent le clavier via l'application avant l'expiration du délai de verrouillage spécifié.
Temps auto-verrouillage, min	Sélection de la période de verrouillage du clavier après des tentatives d'accès non autorisées : • 3 minutes. • 5 minutes. • 10 minutes. • 20 minutes. • 30 minutes. • 60 minutes. • 90 minutes. • 180 minutes. Disponible si la bascule Accès non autorisé. Auto-verrouillage est activée.
Activation du Carillon par le clavier	Si activé, l'utilisateur peut activer/désactiver à partir de l'écran du clavier les notifications de déclenchement des détecteurs d'ouverture. Activez la fonction du Carillon à l'ouverture dans les réglages du clavier et pour au moins un détecteur bistable. <u>En savoir plus</u>
Mise à jour du firmware	Bascule le dispositif en mode de mise à jour du firmware.



	<u>En savoir plus</u>
Test d'intensité du signal Fibra	Bascule le détecteur en mode test d'intensité du signal. <u>En savoir plus</u>
Réinitialisation du Pass/Tag	Permet de supprimer de la mémoire du dispositif toutes les centrales associées au Tag ou au Pass. <u>En savoir plus</u>
Guide de l'utilisateur	Ouvre le manuel utilisateur du KeyPad TouchScreen dans l'application Ajax.
Désactivation forcée	Permet à l'utilisateur de désactiver l'appareil sans le retirer du système. Trois options sont disponibles : • Non – l'appareil fonctionne normalement et transmet tous les événements. • Entièrement – l'appareil n'exécute pas les commandes du système et ne participe pas aux scénarios d'automatisation, et le système ignore les alarmes et autres notifications du dispositif. • Couvercle seulement – le système ignore les notifications déclenchées par le bouton anti-sabotage du dispositif. <u>En savoir plus</u>
Désactivation unique	Permet à l'utilisateur de désactiver les événements du dispositif jusqu'au premier désarmement. Trois options sont disponibles :





	• Non – le dispositif fonctionne normalement. • Couvercle seulement – les notifications concernant le déclenchement du bouton anti-sabotage du dispositif sont désactivées lorsque le mode armé est actif. • Entièrement – le dispositif est entièrement exclu du fonctionnement du système lorsque le mode armé est actif. L'appareil ne réagit pas aux commandes du système et ne signale pas les alarmes ou autres événements. <u>En savoir plus</u>
Dissocier l'appareil	Dissocie le dispositif, le déconnecte de la centrale et supprime ses paramètres.

Gestion de la sécurité

Paramètre	Valeur
Écran de contrôle	Active/désactive la gestion de la sécurité à partir du clavier. Lorsque l'option est désactivée, l'onglet Contrôle  est caché de l'écran du clavier. L'utilisateur ne peut pas contrôler le mode de sécurité du système et des groupes à partir du clavier.
Groupes partagés	Sélection des groupes qui seront partagés et disponibles pour la gestion par tous les utilisateurs autorisés. Tous les groupes du système et les groupes créés après l'ajout du KeyPad TouchScreen à la centrale sont partagés par défaut.

	Disponible si le <u>Mode groupe</u> est activé.
Pré-autorisation	Lorsque cette fonction est activée, l'utilisateur doit d'abord s'authentifier pour avoir accès à la centrale et à l'état actuel du système : il doit saisir un code ou présenter un dispositif d'accès personnel.
Armement sans code	Lorsque cette fonction est activée, l'utilisateur peut armer le site sans saisir de code ni présenter son dispositif d'accès personnel. Si cette fonction est désactivée, saisissez un code ou présentez le dispositif d'accès pour armer le système. L'écran de saisie du code apparaît après avoir appuyé sur la touche Armer . Disponible si la bascule Pré-autorisation est désactivée.
Changement facile du mode de sécurité / Gestion facile du groupe assigné	Lorsque cette fonction est activée, les utilisateurs peuvent passer en mode armé du système (ou du groupe) à l'aide de dispositifs d'accès sans confirmation par les touches du clavier. Disponible si le <u>Mode groupe</u> est désactivé ou si un seul groupe est activé dans le menu Groupes partagés.
Afficher la liste des dysfonctionnements à l'écran	Si activé, la liste des dysfonctionnements empêchant l'armement apparaît sur l'écran du clavier. Activez la <u>Vérification de l'intégrité du système</u> pour cela.



Scénarios d'automatisation

Paramètre	Valeur
-----------	--------



Gestion des scénarios	Active/désactive la gestion des scénarios à partir du clavier. Lorsque l'option est désactivée, l'onglet Scénarios  est caché de l'écran du clavier. L'utilisateur ne peut pas contrôler les scénarios d'automatisation à partir du clavier.
Scénarios de clavier	Le menu vous permet de créer jusqu'à six scénarios pour contrôler un dispositif d'automatisation ou un groupe de dispositifs. Lorsque les paramètres sont enregistrés, des boutons permettant de gérer les scénarios apparaissent sur l'écran du clavier (l'onglet Scénarios . Un utilisateur ou un PRO ayant le droit de configurer le système peut ajouter ou supprimer des scénarios et les activer ou les désactiver. Les scénarios désactivés n'apparaissent pas dans l'onglet Scénarios  de l'écran du clavier.
Pré-autorisation	Lorsque cette fonction est activée, l'utilisateur doit d'abord s'authentifier pour avoir accès à la gestion des scénarios : il doit saisir un code ou présenter un dispositif d'accès personnel.

Signaux d'urgence

Paramètre	Valeur
-----------	--------



Boutons d'urgence à l'écran	Lorsque cette fonction est activée, l'utilisateur peut envoyer un signal d'urgence ou appeler au secours à partir de l'onglet Panique (!) du clavier. Lorsque l'option est désactivée, l'onglet Panique (!) est caché de l'écran du clavier.
Type de bouton	Sélection du nombre de boutons à afficher dans l'onglet Panique (!). Deux options sont disponibles : • Bouton de panique uniquement (par défaut). • Trois boutons : Panique, Incendie, Appeler les secours.
Protection contre la pression accidentelle	Lorsque cette option est activée, l'envoi d'une alarme nécessite une confirmation supplémentaire de la part de l'utilisateur.
Alerte par sirène	
Si le bouton de panique est appuyé	Lorsque cette fonction est activée, les sirènes ajoutées au système sont activées lorsque le Bouton de panique est enfoncé.
Si le bouton d'alarme incendie est enfoncé	Lorsque cette fonction est activée, les sirènes ajoutées au système sont activées lorsque le bouton Incendie est enfoncé. La bascule s'affiche si une option avec trois boutons est activée dans le menu Type de bouton.
Si le bouton d'appel de secours est enfoncé	Lorsque cette fonction est activée, les sirènes ajoutées au système sont activées lorsque le bouton Appeler les secours est enfoncé. La bascule s'affiche si une option avec trois boutons est activée dans le menu Type de bouton.

Réglages de l'écran

Paramètre	Valeur
Automatique	La bascule est activée par défaut. La luminosité du rétroéclairage de l'écran est automatiquement ajustée en fonction de la luminosité ambiante.
Réglage manuel de la luminosité	Sélection du niveau de rétroéclairage de l'écran : de 0 à 100 % (0 – le rétroéclairage est minimal, 100 – le rétroéclairage est maximal). Réglé par incréments de 10 %. Le rétroéclairage n'est allumé que lorsque le clavier est actif. Le réglage manuel est possible lorsque la bascule Automatique est désactivée.
Apparence	Ajustement de l'apparence de l'interface : • Sombre (par défaut). • Clair.
Écran toujours actif	L'écran du clavier reste toujours allumé lorsque la bascule est activée et que l'alimentation externe est connectée. La bascule est désactivée par défaut. Dans ce cas, le clavier se met en veille après un certain temps à compter de la dernière interaction avec l'écran.
Indication du Mode armé	Réglage de l'indication LED du clavier : • Off (par défaut) – l'indication LED est éteinte. • Lorsque armé uniquement – l'indication LED s'allume lorsque le système est armé et le clavier passe en mode veille (l'affichage s'éteint).



	• Toujours – l'indication LED est allumée quel que soit le mode de sécurité. Elle est activée lorsque le clavier passe en mode veille. <u>En savoir plus</u>
Langue	Configuration de la langue de l'interface du clavier. L'anglais est défini par défaut. Pour changer de langue, sélectionnez celle qui vous convient et cliquez sur Enregistrer.



Réglages de l'Indication sonore

Le clavier KeyPad TouchScreen est doté d'un avertisseur sonore intégré qui remplit les fonctions suivantes en fonction des paramètres :

1. Indique l'état de la sécurité ainsi que les **Temporisations à l'armement et au désarmement**.
2. Carillon à l'ouverture.
3. Avertissement en cas d'alarme.



Nous déconseillons l'utilisation du KeyPad TouchScreen à la place de la sirène. L'avertisseur sonore du clavier n'est destiné qu'à des notifications supplémentaires. Les **sirènes Ajax** sont conçues pour dissuader les intrus et attirer l'attention. Une sirène correctement installée est plus difficile à démonter en raison de sa position de montage surélevée par rapport à un clavier situé au niveau des yeux.

Paramètre	Valeur
Signaux sonores. Bip lors du changement de mode de sécurité	



Armement/Désarmement	Si activé : une notification sonore est envoyée si le mode de sécurité est modifié à partir du clavier, d'un autre dispositif ou de l'application. Si désactivé : une notification sonore est envoyée si le mode de sécurité est modifié à partir du clavier uniquement. Le volume du bip dépend du volume configuré des boutons.
Activation/Désactivation du Mode nuit	Si activé : une notification sonore est envoyée si le Mode nuit est activé/désactivé à partir du clavier, d'un autre dispositif ou de l'application. Si désactivé : une notification sonore est envoyée si le Mode nuit est activé/désactivé à partir du clavier uniquement. <u>En savoir plus</u> Le volume du bip dépend du volume des boutons configurés.
Bip pour les temporisations	
Temporisations désarmement	Si activé, le buzzer du clavier émet un bip pour signaler les temporisations au désarmement. <u>En savoir plus</u>
Temporisations armement	Si activé, le buzzer du clavier émet un bip pour signaler les temporisations à l'armement. <u>En savoir plus</u>



Temporisations désarm/Nuit	Si activé, le buzzer du clavier émet un bip pour signaler une temporisation au désarmement en <u>Mode nuit.</u> <u>En savoir plus</u>
Temporisations arm/Nuit	Si activé, le buzzer du clavier émet un bip pour signaler une temporisation à l'armement en <u>Mode nuit.</u> <u>En savoir plus</u>
Bip lorsque désarmé	
Carillon à l'ouverture	Si activé, le buzzer intégré informe par un court bip que les détecteurs d'ouverture se sont déclenchés lorsque le système est Désarmé. <u>En savoir plus</u>
Volume du bip	Sélection du niveau de volume du buzzer pour les notifications d'armement/désarmement, de temporisations à l'armement/désarmement et d'ouverture : • Faible. • Moyen. • Fort.
Boutons	
Volume	Réglage du volume de notification du buzzer pour les interactions avec l'écran du clavier.
Réaction aux alarmes	
Alarme sonore	Réglage du mode de déclenchement de l'alarme par le buzzer intégré : • Toujours – une alarme sonore est activée quel que soit le mode de sécurité

	du système. • Lorsque armé uniquement – une alarme sonore est activée si le système ou le groupe auquel un clavier est assigné est armé.
Activer le buzzer du clavier si une alarme est détectée dans le système	Si activé, le buzzer sonore intégré signale une alarme dans le système.
Alarmes en Mode groupe	Sélection du groupe (parmi les groupes partagés) pour lequel le clavier notifiera l'alarme. L'option Tous les groupes partagés est activée par défaut. Si le clavier n'a qu'un seul groupe partagé et qu'il est supprimé, le réglage revient à sa valeur initiale. Disponible si le Mode groupe est activé.
Durée de l'alarme	Durée du signal acoustique en cas d'alarme : 3 secondes à 3 minutes. La connexion d'une alimentation externe au clavier est recommandée pour un signal sonore d'une durée supérieure à 30 secondes.



Réglez les temporisations à l'armement / au désarmement dans les paramètres appropriés des détecteurs et non dans les paramètres du clavier.

[En savoir plus](#)

Réglage de la réponse du clavier aux alarmes de l'appareil

KeyPad TouchScreen peut répondre aux alarmes de chaque détecteur du système grâce à un buzzer intégré. Cette fonction est utile si vous n'avez pas besoin d'activer le buzzer en cas d'alarme d'un appareil spécifique.



Par exemple, cela peut s'appliquer au déclenchement du détecteur de fuites d'eau LeaksProtect.



Par défaut, la réponse du clavier est activée pour les alarmes de tous les dispositifs du système.



Pour régler la réponse du clavier à une alarme de l'appareil :

1. Ouvrez l'application Ajax.
2. Allez dans l'onglet **Appareils** .
3. Sélectionnez dans la liste l'appareil, pour lequel vous souhaitez configurer la réponse du clavier.
4. Allez dans les **Paramètres** du dispositif en cliquant sur l'icône de l'engrenage .
5. Trouvez l'option **Alerte par sirène** et sélectionnez les commandes qui activeront la sirène. Activez ou désactivez la fonction.
6. Répétez les étapes 3 à 5 pour les autres appareils du système.

Réglage de la réponse du clavier à une alarme du bouton anti-sabotage

KeyPad TouchScreen peut répondre aux alarmes anti-sabotage de chaque dispositif du système grâce à un buzzer intégré. Lorsque la fonction est activée, le buzzer intégré émet un signal sonore lorsque le bouton anti-sabotage de l'appareil est déclenché.

Pour régler la réponse du clavier à une alarme du bouton anti-sabotage :

1. Ouvrez l'application Ajax.
2. Allez dans l'onglet **Appareils** .
3. Sélectionnez une centrale et allez dans ses **Paramètres** .

4. Sélectionnez le menu **Service**.
5. Allez à la section **Sons et alertes**.
6. Activez le commutateur **Si la centrale ou le boîtier du détecteur est ouvert**.
7. Cliquez sur **Retour** pour enregistrer les paramètres.



Le bouton anti-sabotage répond à l'ouverture et à la fermeture du boîtier, quel que soit le mode de sécurité de l'appareil ou du système.

Définir la réponse à l'appui sur le bouton de panique dans les applications Ajax

Vous pouvez configurer la réponse du clavier à l'alarme lorsque le bouton de panique est pressé dans les applications Ajax. Pour ce faire, suivez les étapes suivantes :

1. Ouvrez l'application Ajax.
2. Allez dans l'onglet **Appareils** .
3. Sélectionnez une centrale et allez dans ses **Paramètres** .
4. Sélectionnez le menu **Service**.
5. Allez à la section **Sons et alertes**.
6. Activez le commutateur **Si un bouton panique est appuyé dans l'app**.
7. Cliquez sur **Retour** pour enregistrer les paramètres.

Paramètres de l'indication du clavier après l'alarme



Le clavier peut signaler le déclenchement dans le système armé à l'aide de l'indication LED.



L'option fonctionne comme suit :

1. Le système enregistre l'alarme.
2. Le clavier émet un signal d'alarme (si activé). La durée et le volume du signal émis dépendent des paramètres du dispositif.
3. La LED du clavier clignote deux fois (une fois toutes les 3 secondes) jusqu'à ce que le système soit désarmé.

Grâce à cette fonction, les utilisateurs du système et les patrouilles de l'entreprise de sécurité peuvent comprendre que l'alarme s'est produite.



L'indication du KeyPad TouchScreen après alarme ne fonctionne pas pour les détecteurs toujours actifs, si le détecteur a été déclenché lorsque le système était désarmé.

Pour activer l'indication du KeyPad TouchScreen après alarme, dans l'application Ajax PRO :

1. Allez dans les paramètres de la centrale :
 - Centrale → Paramètres  → Service → Indication LED.
2. Spécifiez les événements que le KeyPad TouchScreen signalera par un double clignotement de la LED, avant que le système de sécurité ne soit désarmé :

- Alarme d'intrusion/Bouton d'urgence confirmé.
 - Alarme d'intrusion/Bouton d'urgence unique.
 - Ouverture du couvercle.
3. Sélectionnez le KeyPad TouchScreen requis dans le menu **Appareils**. Cliquez sur **Retour** pour enregistrer les paramètres.
 4. Cliquez sur **Retour**. Tous les paramètres seront appliqués.



Comment configurer le Carillon d'entrée

Quand la fonction **Carillon d'entrée est activée**, le KeyPad TouchScreen vous informe par un court bip si les détecteurs d'ouverture se déclenchent, lorsque le système est désarmé. Cette fonction est utilisée, par exemple, dans les magasins, pour avertir les employés que quelqu'un est entré dans le bâtiment.

Le paramétrage des notifications s'effectue en deux étapes : le paramétrage du clavier et le paramétrage des détecteurs d'ouverture. Vous trouverez dans [cet article](#) de plus amples informations sur le **Carillon d'entrée** et sur la manière de configurer les détecteurs.

Pour configurer la réponse du clavier :

1. Ouvrez l'application Ajax.
2. Allez dans l'onglet **Appareils** .
3. Sélectionnez KeyPad TouchScreen et allez dans ses **Paramètres** .
4. Allez dans le menu **Indication sonore** → **Signaux sonores**.
5. Activez l'option **Carillon à l'ouverture** dans la catégorie **Bip lorsque désarmé**.
6. Définissez le volume requis de notifications.
7. Cliquez sur **Retour** pour enregistrer les paramètres.

Si les réglages sont corrects, une icône de cloche apparaît dans l'onglet **Contrôle** de l'application Ajax. Cliquez dessus pour activer ou désactiver le carillon à l'ouverture.

Pour paramétrer la gestion du carillon à partir de l'écran du clavier :

1. Ouvrez l'application Ajax.
2. Allez dans l'onglet **Appareils** .
3. Sélectionnez KeyPad TouchScreen et allez dans ses **Paramètres** .
4. Activez la fonction **Activation du Carillon par le clavier**.



Si les réglages sont corrects, une icône de cloche apparaît dans l'onglet **Contrôle**  sur l'écran du clavier. Cliquez dessus pour activer/désactiver le carillon à l'ouverture.



Configuration des codes

Codes d'accès des claviers



Code utilisateur



Codes des utilisateurs non enregistrés



Code GIR



Ajout de cartes et de badges



KeyPad TouchScreen peut fonctionner avec les badges Tag, les cartes Pass et les dispositifs tiers qui prennent en charge la technologie DESFire®.

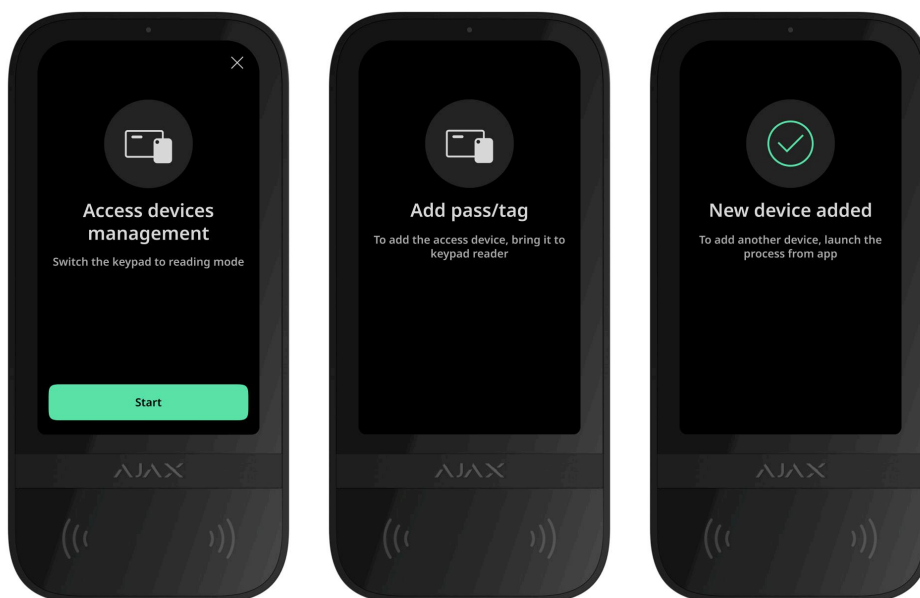


Avant d'ajouter des appareils tiers prenant en charge DESFire®, assurez-vous qu'ils disposent de suffisamment de mémoire libre pour prendre en charge le nouveau clavier. De préférence, le dispositif tiers doit être formaté à l'avance.

Cet article fournit des informations sur la manière de réinitialiser **Tag** ou **Pass**.

Le nombre maximum de cartes Pass et de badges Tag pouvant être connectées est de 50 pour Hub Hybrid (2G) et Hub Hybrid (4G). Les Pass et Tag connectés n'affectent pas la limite totale d'appareils connectés à la centrale.

Comment ajouter un Tag ou un Pass au système



1. Ouvrez l'application Ajax.
2. Sélectionnez la centrale à laquelle vous souhaitez ajouter un tag ou un Pass.
3. Allez dans l'onglet **Appareils** .



Assurez-vous que la fonction **Lecture du Pass/Tag** est activée dans les paramètres d'au moins un clavier.

4. Cliquez sur **Ajouter un appareil**.
5. Sélectionnez **Ajouter un Pass/Tag**.
6. Spécifiez le type (Tag ou Pass), la couleur, le nom de l'appareil et l'utilisateur (si nécessaire).
7. Cliquez sur **Suivant**. Ensuite, la centrale passe en mode d'enregistrement des appareils.
8. Allez sur n'importe quel clavier avec la fonction **Lecture du Pass/Tag** activée et activez le dispositif.

Après l'activation, KeyPad TouchScreen affiche un écran permettant de basculer le clavier en mode d'enregistrement du dispositif d'accès. Cliquez sur le bouton **Démarrer**.



Un écran se met à jour automatiquement si l'alimentation externe est connectée et si la bascule **Écran toujours actif** est activée dans les paramètres du clavier.

L'écran permettant de passer le clavier en mode enregistrement s'affiche sur tous les KeyPad TouchScreen du système. Lorsqu'un administrateur ou un PRO ayant le droit de configurer le système commence à enregistrer un Tag/Pass sur un clavier, les autres claviers reviennent à leur état initial.



9. Approcher le Pass ou le Tag avec le côté large contre le lecteur de clavier pendant quelques secondes. Le lecteur est marqué par des icônes de vagues (〰) sur le boîtier. Si l'ajout est réussi, vous recevrez une notification dans l'application Ajax et sur l'écran du clavier.

Si la connexion échoue, réessayez dans 5 secondes. Veuillez noter que si le nombre maximum d'appareils Tag ou Pass a déjà été ajouté à la centrale, vous recevrez une notification correspondante dans l'application Ajax lors de l'ajout d'un nouvel appareil.



Tag et Pass peuvent fonctionner avec plusieurs centrales en même temps. Le nombre maximal de centrales est de 13. Si vous essayez de lier un Tag ou un Pass à une centrale qui a déjà atteint sa limite, vous recevrez une notification correspondante. Effacez toutes les données de la mémoire du porteclé / de la carte avant de l'associer à une nouvelle centrale.

Si vous avez besoin d'ajouter un autre Tag ou Pass, cliquez sur **Ajouter autre Pass/Tag** dans l'application. Répétez les étapes 6 à 9.

Comment supprimer un Tag ou un Pass de la centrale



La réinitialisation efface tous les réglages et toutes les connexions des porteclés et des cartes. Dans ce cas, le Tag et le Pass réinitialisés ne sont retirés que de la centrale à partir de laquelle la réinitialisation a été effectuée. Sur d'autres centrales, le Tag ou le Pass sont toujours affichés dans l'application, mais ne

peuvent pas être utilisés pour gérer les modes de sécurité. Ces dispositifs doivent être supprimés manuellement.

1. Ouvrez l'application Ajax.
2. Sélectionnez la centrale.
3. Allez dans l'onglet **Appareils** .
4. Sélectionnez un clavier compatible dans la liste des appareils.



Assurez-vous que la fonction **Lecture du Pass/Tag** est activée dans les paramètres du clavier.

5. Accédez aux paramètres du clavier en cliquant sur l'icône .
6. Cliquez sur **Réinitialisation du Pass/Tag**.
7. Cliquez sur **Continuer**.
8. Allez sur n'importe quel clavier avec la fonction **Lecture du Pass/Tag** activée et activez le dispositif.

Après l'activation, KeyPad TouchScreen affiche un écran permettant de basculer le clavier en mode de réinitialisation du dispositif d'accès. Cliquez sur le bouton **Démarrer**.



Un écran se met à jour automatiquement si l'alimentation externe est connectée et si la bascule **Écran toujours actif** est activée dans les paramètres du clavier.

L'écran permettant de passer le clavier en mode de réinitialisation s'affiche sur tous les KeyPad TouchScreen du système. Lorsqu'un administrateur ou un PRO ayant le droit de configurer le système commence à réinitialiser un Tag/Pass sur un clavier, les autres claviers reviennent à leur état initial.



9. Approchez le Pass ou le Tag avec le côté large contre le lecteur de clavier pendant quelques secondes. Le lecteur est marqué par des icônes de vagues (〰️) sur le boîtier. Si le formatage est réussi, vous recevrez une notification dans l'application Ajax et sur l'écran du clavier. Si le formatage échoue, réessayez.
10. Si vous devez réinitialiser un autre Pass ou un autre Tag, cliquez sur **Réinitialiser autre Pass/Tag** dans l'application. Répétez l'étape 9.



Paramètres Bluetooth

KeyPad TouchScreen permet de contrôler les modes de sécurité en approchant un smartphone du capteur. La gestion de la sécurité est assurée par un canal de communication Bluetooth. Cette méthode est pratique, sûre et rapide, car il n'est pas nécessaire de saisir un code, d'ajouter un téléphone au clavier ou d'utiliser un Tag ou un Pass qui pourrait être perdu.



L'authentification Bluetooth n'est disponible que pour les utilisateurs d'Ajax Security System.

Pour activer l'authentification Bluetooth dans l'application

1. Connectez KeyPad TouchScreen à la centrale.
2. Activez le capteur Bluetooth du clavier :

Appareils  → **KeyPad Touchscreen** → **Paramètres**  → Activez la bascule **Bluetooth**.

3. Cliquez sur **Retour** pour enregistrer les paramètres.

Pour configurer l'authentification Bluetooth

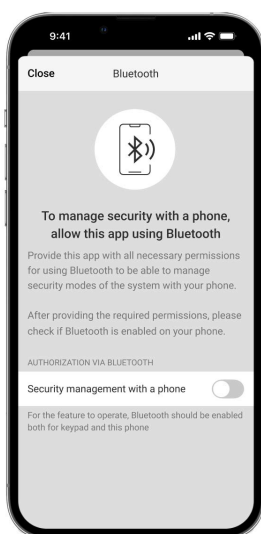
1. Ouvrez l'application Ajax Security System et sélectionnez la centrale à laquelle le KeyPad TouchScreen avec authentification Bluetooth activée est ajouté. Par défaut, l'authentification par Bluetooth est disponible pour tous les utilisateurs de ce système.



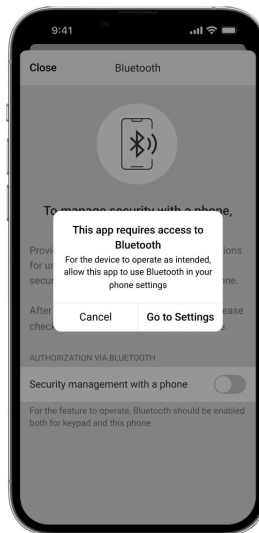
Pour interdire l'authentification Bluetooth à certains utilisateurs :

1. Dans l'onglet **Appareils** sélectionnez la centrale et accédez à ses paramètres .
2. Ouvrez le menu **Utilisateurs** et sélectionnez l'utilisateur souhaité dans la liste.
3. Dans la section **Autorisations**, désactivez la bascule **Gestion de la sécurité via Bluetooth**.

2. Autorisez l'application Ajax Security System à utiliser Bluetooth si cette autorisation n'a pas été accordée au préalable. Dans ce cas, l'avertissement ⚠ s'affiche dans les **États** du KeyPad TouchScreen. En appuyant sur le symbole ⓘ, vous ouvrez une fenêtre contenant des explications sur la marche à suivre. Activez la **Gestion de la sécurité avec un smartphone** en bas de la fenêtre ouverte.

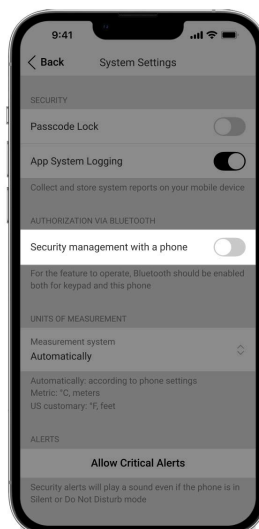


Autorisez l'application à trouver des appareils à proximité et à s'y connecter. La fenêtre contextuelle pour les smartphones Android et iOS peut être différente.



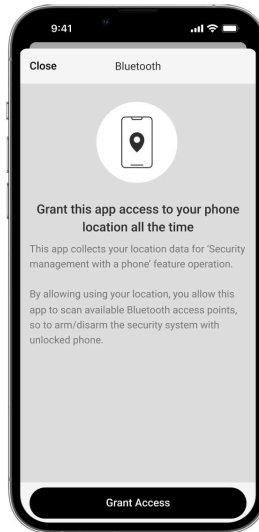
De plus, la **Gestion de la sécurité avec un smartphone** peut être activée dans les paramètres de l'application :

- Cliquez sur l'icône  dans le coin supérieur gauche de l'écran, sélectionnez le menu **Paramètres de l'app**.
- Ouvrez le menu **Paramètres du système** et activez la **Gestion de la sécurité avec un smartphone**.



3. Il est recommandé de configurer le **Géorepérage** pour assurer un fonctionnement stable de l'authentification Bluetooth. L'avertissement  s'affiche dans les **États** du KeyPad TouchScreen si le **Géorepérage** est désactivé et que l'application n'est pas autorisée à utiliser

l'emplacement du smartphone. En appuyant sur le symbole ⓘ, vous ouvrez une fenêtre contenant des explications sur la marche à suivre.



L'authentification Bluetooth peut être instable si la fonction **Géorepérage** est désactivée. Lancez et réduisez l'application si le système la fait passer en mode veille.

Vous pouvez contrôler le système plus rapidement via Bluetooth, lorsque la fonction **Géorepérage** est activée et configurée. Il suffit de déverrouiller le téléphone et de l'approcher au capteur du clavier.

[Comment configurer le Géorepérage](#)

4. Activez l'option **Maintenir l'application active pour gérer la sécurité via Bluetooth**. Pour ce faire, rendez-vous sur **Appareils**  → **Centrale** → **Paramètres**  → **Géorepérage**.
5. Assurez-vous que le Bluetooth est activé sur votre smartphone. S'il est désactivé, l'avertissement ⚠ apparaît dans les **États** du clavier. En appuyant sur le symbole ⓘ, vous ouvrez une fenêtre contenant des explications sur la marche à suivre.
6. Activez l'option **Service de Keep-Alive** dans les paramètres de l'application pour les smartphones Android. Pour cela, dans le coin supérieur gauche de l'écran, cliquez sur ≡ → **Paramètres de l'app** → **Paramètres du système**.

Pré-autorisation

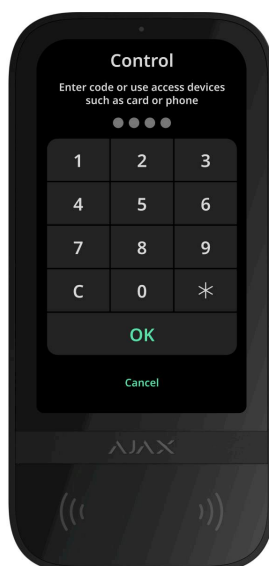
Lorsque la fonction est activée, l'accès à la centrale et à l'état actuel du système est bloqué. Pour le débloquent, l'utilisateur doit s'authentifier : saisir un code approprié ou présenter un dispositif d'accès personnel au clavier.



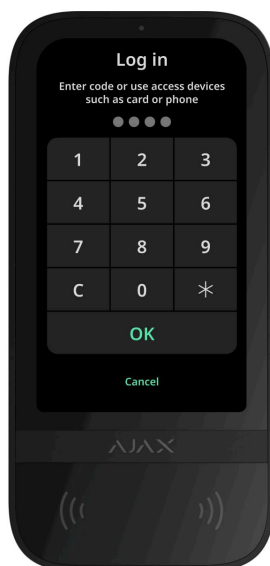
Si la pré-autorisation est activée, la fonction **Armement sans code** n'est pas disponible dans les paramètres du clavier.

Vous pouvez vous authentifier de deux manières :

1. Dans l'onglet **Contrôle** . Après s'être connecté, l'utilisateur verra les groupes partagés du système (si le Mode groupe est activé). Ils sont spécifiés dans les paramètres du clavier : **Gestion de la sécurité** → **Groupes partagés**. Par défaut, tous les groupes de systèmes sont partagés.



2. Dans l'onglet **S'identifier** . Après s'être connecté, l'utilisateur verra les groupes disponibles qui étaient cachés dans la liste des groupes partagés.



L'écran du clavier passe à l'écran initial 10 secondes après la dernière interaction avec celui-ci. Saisissez le code ou approchez à nouveau un dispositif d'accès personnel pour contrôler le système à l'aide du KeyPad TouchScreen.

Pré-autorisation à l'aide d'un code clavier



Pré-autorisation à l'aide d'un code personnel



Pré-autorisation à l'aide d'un code d'accès



Pré-autorisation à l'aide d'un code GIR



Pré-autorisation avec Tag ou Pass



Pré-autorisation à l'aide d'un smartphone



Gestion de la sécurité

En utilisant les codes, Tag/Pass, ou un smartphone, vous pouvez contrôler le **Mode nuit** et la sécurité du site entier ou de groupes séparés.

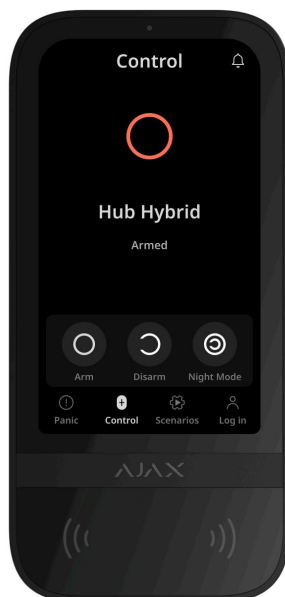
L'utilisateur ou le PRO ayant les droits de configuration du système peut configurer les codes d'accès. Ce chapitre fournit des informations sur la manière d'ajouter un Tag ou un Pass à la centrale. Pour piloter le système avec un smartphone, réglez les paramètres Bluetooth dans les paramètres du clavier. Activez le Bluetooth, le Service de localisation du smartphone et déverrouillez l'écran.



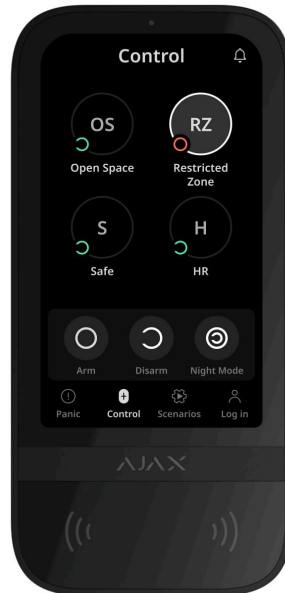
KeyPad TouchScreen est verrouillé pour la durée spécifiée dans les paramètres si un code incorrect est saisi ou si un dispositif d'accès non vérifié est présenté trois fois de suite en l'espace d'une minute. Les notifications correspondantes sont envoyées aux utilisateurs et au centre de télésurveillance. Un utilisateur ou un PRO disposant des droits de configuration du système peut déverrouiller le KeyPad TouchScreen dans l'application Ajax.

Si le Mode groupe est désactivé, une icône appropriée sur l'écran du clavier indique le mode de sécurité en cours :

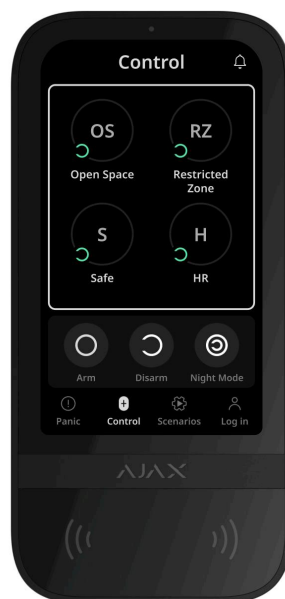
-  – Armé.
-  – Désarmé.
-  – Mode nuit.



Si le Mode groupe est activé, les utilisateurs voient le mode de sécurité de chaque groupe séparément. Le groupe est armé si le contour de son bouton est blanc et s'il est marqué de l'icône . Le groupe est désarmé si le contour de son bouton est gris et s'il est marqué de l'icône .



Les touches des groupes en **Mode nuit** sont encadrées dans un carré blanc sur l'écran du clavier.



Si un code personnel ou d'accès, un Tag/Pass ou un smartphone est utilisé, le nom de l'utilisateur qui a modifié le mode de sécurité est affiché dans le flux d'événements de la centrale et dans la liste des notifications. Lorsqu'un code

général est utilisé, le nom du clavier à partir duquel la modification du mode de sécurité a été effectuée s'affiche.

Les étapes à suivre pour modifier le mode de sécurité à l'aide du clavier dépendent de l'activation ou non de la pré-autorisation de l'utilisateur dans les paramètres du KeyPad TouchScreen.



Si la pré-autorisation est activée

Gestion de la sécurité du site ▼

Gestion de la sécurité du groupe ▼

Utilisation d'un code de contrainte ▼

Si la pré-autorisation est désactivée

Gestion de la sécurité du site ▼

Gestion de la sécurité du groupe ▼

Utilisation d'un code de contrainte ▼

Exemple de saisie de codes

Code	Exemple	Remarque
Code clavier	1234 → OK	Les chiffres saisis de manière incorrecte peuvent

Code de contrainte du clavier		être effacés à l'aide de la touche C .
Code utilisateur		Saisissez d'abord l' ID utilisateur , appuyez sur la touche * et saisissez ensuite un code personnel.
Code de contrainte de l'utilisateur	2 → * → 1234 → OK	Les chiffres saisis de manière incorrecte peuvent être effacés à l'aide de la touche C .
Code de l'utilisateur non enregistré		Les chiffres saisis de manière incorrecte peuvent être effacés à l'aide de la touche C .
Code de contrainte de l'utilisateur non enregistré	1234 → OK	
Code GIR	1234 → OK	Les chiffres saisis de manière incorrecte peuvent être effacés à l'aide de la touche C .



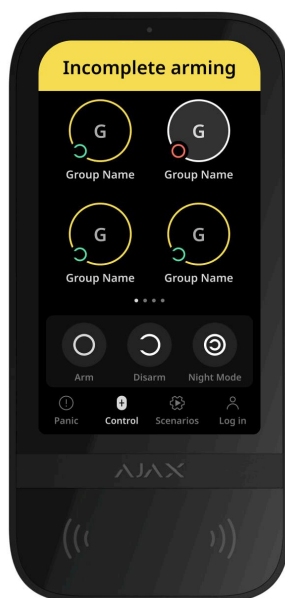
Changement facile du mode de sécurité

La fonction **Changement facile du mode de sécurité** permet de changer le mode de sécurité en sens inverse en utilisant le Tag/Pass ou le smartphone, sans confirmation par les boutons Armer  ou Désarmer . Allez dans les paramètres du clavier pour activer la fonction.

Pour modifier le mode de sécurité dans le sens inverse

1. Activez le clavier en vous approchant ou en passant la main devant le capteur. Effectuez une pré-autorisation si nécessaire.
2. Approchez votre Tag/Pass ou votre smartphone.

Armement en deux étapes



Le clavier KeyPad TouchScreen peut participer à l'armement en deux étapes, mais ne peut pas être utilisé en tant que dispositif de deuxième étape. Le processus d'armement en deux étapes à l'aide d'un Tag, d'un Pass ou d'un smartphone est similaire à l'utilisation d'un code personnel ou général sur le clavier.

En savoir plus

Les utilisateurs du système peuvent voir sur l'écran du clavier si l'armement est commencé ou incomplet. Si le Mode groupe est activé, la couleur des boutons de groupe dépend de l'état actuel :

- **Gris** : désarmé, le processus d'armement n'a pas commencé.
- **Vert** : le processus d'armement a commencé.
- **Jaune** : l'armement est incomplet.
- **Blanc** : armé.

Gestion des scénarios à l'aide du clavier

KeyPad TouchScreen vous permet de créer jusqu'à six scénarios pour contrôler un ou un groupe de dispositifs d'automatisation.

Pour créer un scénario :

1. Ouvrez l'application Ajax. Sélectionnez la centrale avec au moins un KeyPad TouchScreen et un dispositif d'automatisation. En ajouter un si nécessaire.
2. Allez dans l'onglet **Appareils** .
3. Sélectionnez KeyPad TouchScreen dans la liste et accédez au menu **Paramètres** .
4. Allez dans le menu **Scénarios d'automatisation**. Activez l'option de **Gestion des scénarios**.
5. Ouvrez le menu **Scénarios de clavier**.
6. Appuyez sur **Ajouter un scénario**.
7. Sélectionnez un ou plusieurs dispositifs d'automatisation. Appuyez sur **Suivant**.
8. Saisissez le nom du scénario dans le champ **Nom**.
9. Sélectionnez l'action du dispositif pendant l'exécution du scénario.
10. Cliquez sur **Enregistrer**.
11. Appuyez sur **Retour** pour revenir au menu **Scénarios d'automatisation**.
12. Activez la bascule **Pré-autorisation** si nécessaire.

Les scénarios créés sont affichés dans l'application : **KeyPad TouchScreen** → **Paramètres**  → **Scénarios d'automatisation** → **Scénarios de clavier**. Vous pouvez les désactiver, ajuster les paramètres ou les supprimer à tout moment.

Pour supprimer un scénario :

1. Allez dans les **Paramètres**  du KeyPad TouchScreen.
2. Ouvrez le menu **Scénarios d'automatisation** → **Scénarios de clavier**.
3. Sélectionnez le scénario que vous souhaitez supprimer.
4. Appuyez sur **Suivant**.



5. Cliquez sur **Supprimer le scénario**.

L'utilisateur peut voir et gérer les scénarios d'automatisation après l'authentification lorsque la fonction **Pré-autorisation** est activée. Allez dans l'onglet **Scénarios** , saisissez le code ou approchez un dispositif d'accès personnel du clavier.

Pour exécuter un scénario, appuyez sur un bouton approprié dans l'onglet **Scénarios** .



L'écran du KeyPad TouchScreen n'affiche que les scénarios activés dans les paramètres du clavier.

Silence de l'alarme incendie

Chapitre en cours de préparation

Indication

KeyPad TouchScreen informe les utilisateurs des alarmes, des temporisations à l'armement et au désarmement, du mode de sécurité actuel, des dysfonctionnements et d'autres états du système :

- l'écran ;
- le logo avec indicateur LED ;
- le buzzer intégré.

L'indication du KeyPad TouchScreen n'apparaît sur l'écran que lorsqu'il est actif. En haut de l'onglet **Contrôle** , des icônes indiquant certains états du système ou du clavier sont affichées. Par exemple, elles peuvent indiquer une alarme incendie, le rétablissement du système après une alarme et un carillon à l'ouverture. Les informations relatives au mode de sécurité seront mises à jour même si elles sont modifiées par un autre dispositif : porteclé, autre clavier ou dans l'application.





Événement	Indication	Remarque
Alarme.	Le buzzer intégré émet un signal sonore.	Si l'option Activer le buzzer du clavier si une alarme est détectée dans le système est activé. La durée du signal sonore dépend des réglages du clavier.
Une alarme est détectée dans le système armé.	La LED clignote deux fois (une fois toutes les 3 secondes) jusqu'à ce que le système soit désarmé.	Pour l'activer, activez <u>l'Indication après alarme</u> dans les paramètres de la centrale. En outre, spécifiez le KeyPad TouchScreen comme dispositif pour la notification d'alarmes provenant d'autres dispositifs. L'indication est activée une fois que le buzzer intégré a terminé de reproduire le signal d'alarme.
Mise en marche du dispositif/Chargement de la configuration actualisée du système sur le clavier.	Une notification appropriée est affichée à l'écran pendant le chargement des données.	
Mise en arrêt de l'appareil.	La LED s'allume pendant 1 seconde, puis clignote trois fois.	
Le système ou le groupe est armé.	Le buzzer intégré émet un bip court.	Si les notifications pour Armement/Désarmement sont activées.
Le système ou le groupe passe en Mode nuit .	Le buzzer intégré émet un bip court.	Si les notifications pour Activation/Désactivation du Mode nuit sont activées.
Le système est désarmé.	Le buzzer intégré émet deux bips courts.	Si les notifications pour Armement/Désarmement sont activées.



Systeme en mode armé.	La LED s'allume en rouge brièvement toutes les 3 secondes si l'alimentation externe n'est pas connectée. La LED s'allume constamment en rouge si l'alimentation externe est connectée.	Si Indication du Mode armé est activée. L'indication s'allume lorsque le clavier passe en mode veille (l'écran s'éteint).
Un code incorrect a été saisi.	Une notification appropriée s'affiche à l'écran. Le buzzer intégré émet un bip court (si réglé).	Le volume du bip dépend du volume configuré des boutons.
Erreur lors de l'ajout d'une carte ou d'un porteclé.	Une notification appropriée s'affiche à l'écran. La LED s'allume une fois en rouge. Le buzzer intégré émet un long bip.	Le volume du bip dépend du volume configuré des boutons.
Ajout réussi du porteclé/carte.	An appropriate notification is shown on the display. The built-in buzzer emits a short beep.	Le volume du bip dépend du volume configuré des boutons.
Batterie de secours faible.	La LED s'allume et s'éteint progressivement lorsque le bouton anti-sabotage est déclenché, qu'une alarme est activée, ou que le système est armé ou désarmé (si l'indication est activée).	
Déclenchement du bouton anti-sabotage.	La LED s'allume en rouge pendant 1 seconde.	
Test d'intensité du signal Fibra.	L'indicateur LED s'allume en vert pendant le test.	S'allume après avoir lancé un test approprié dans les



		<u>paramètres du</u> <u>clavier.</u>
Mise à jour du firmware.	La LED s'allume périodiquement en vert pendant la mise à jour du firmware.	S'allume après avoir lancé la mise à jour du firmware dans les <u>États</u> du clavier.
Désactivation de l'alarme incendie interconnectée.	Une notification appropriée s'affiche à l'écran. Le buzzer intégré émet un signal sonore.	
Le clavier est désactivé.	Une notification appropriée s'affiche à l'écran.	Si l'option Entièrement est sélectionnée pour les réglages du clavier <u>Désactivation forcée</u> ou <u>Désactivation</u> <u>unique.</u>
Une restauration du système est nécessaire.	Un écran approprié pour restaurer ou envoyer une demande de restauration du système après l'alarme apparaît sur l'écran.	La fonction <u>Restauration après alarme</u> doit être ajustée dans le système. L'écran apparaît lors de l'armement ou du passage du système en Mode nuit si une alarme ou un dysfonctionnement s'est produit dans le système auparavant. Les administrateurs ou les PRO ayant les droits de configurer le système peuvent restaurer le système. Les autres utilisateurs peuvent envoyer une demande de restauration.



L'intention d'armer le système alors qu'il est déjà armé.	Une notification appropriée s'affiche à l'écran. Le buzzer intégré émet un bip court.	Après avoir saisi le code correct et si les notifications pour Armement/Désarmement sont activées.
L'intention de désarmer le système alors qu'il est déjà désarmé.	Une notification appropriée s'affiche à l'écran. Le buzzer intégré émet deux bips courts.	Après avoir saisi le code correct et si les notifications pour Armement/Désarmement sont activées.
Le clavier est retiré de la centrale.	L'indicateur LED clignote 6 fois en rouge, puis 3 fois, mais plus rapidement.	
Le clavier est verrouillé si le code est introduit de manière incorrecte.	Une notification appropriée s'affiche à l'écran. Le buzzer intégré émet un long bip.	Le volume du bip dépend du volume configuré des boutons.

Notifications sonores des dysfonctionnements

Si un dispositif est hors ligne ou si la batterie est faible, KeyPad TouchScreen peut avertir les utilisateurs du système par un signal sonore. La LED du clavier clignote également. Les notifications de dysfonctionnement seront affichées dans le flux d'événements, par SMS ou par notification push.

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

1. Cliquez sur **Appareils** , choisissez la centrale et ouvrez ses paramètres .

Cliquez sur **Service** → **Sons et alertes**.

2. Activez les bascules : **Si la batterie d'un appareil est faible** et **Si un appareil est hors ligne**.

3. Cliquez sur **Retour** pour enregistrer les paramètres.

Événement	Indication	Remarque
Si un appareil est hors ligne.	Deux bips courts, la LED clignote deux fois. Un bip est émis une fois par minute jusqu'à ce que tous les appareils du système soient en ligne.	Les utilisateurs peuvent temporiser l'indication sonore pendant 12 heures.
Si votre KeyPad TouchScreen est hors ligne.	Deux bips courts, la LED clignote deux fois. Un bip est émis une fois par minute jusqu'à ce que le clavier soit en ligne.	La temporisation de l'indication sonore n'est pas possible.
Si la batterie d'un appareil est faible.	Trois bips courts, la LED clignote trois fois. Un bip est émis une fois par minute jusqu'à ce que la batterie soit rétablie 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 l'appareil et la centrale.

Test de fonctionnalité

Le système de sécurité Ajax propose plusieurs types de tests pour vous aider à choisir le bon endroit pour installer les appareils. Les tests ne commencent pas immédiatement. Toutefois, le temps d'attente ne



dépasse pas la durée d'un intervalle d'interrogation entre la centrale et le dispositif. L'intervalle d'interrogation peut être vérifié et configuré dans les paramètres de la centrale (**Centrale** → **Paramètres** ⚙️ → **Jeweller/Fibra**).

Pour exécuter un test dans l'application Ajax :

1. Sélectionnez la centrale requise.
2. Allez dans l'onglet **Appareils** 📱.
3. Sélectionnez le **KeyPad TouchScreen** dans la liste.
4. Allez dans **Paramètres** ⚙️.
5. Effectuez le Test d'intensité du signal Fibra.



Emplacement du dispositif



Le dispositif est conçu pour une utilisation en intérieur uniquement.

Lorsque vous choisissez un emplacement du dispositif, tenez compte des paramètres qui influent sur son fonctionnement :

- Intensité du signal Fibra.
- Longueur du câble utilisé pour connecter le KeyPad TouchScreen.

Tenez compte des recommandations sur l'installation des dispositifs lorsque vous préparez un système pour un site. Seuls des professionnels devraient concevoir et installer le système Ajax. Une liste des partenaires officiels autorisés d'Ajax est disponible ici.

Le meilleur emplacement pour KeyPad TouchScreen est à l'intérieur, près de l'entrée. Cela permet de désarmer le système avant que les temporisations au désarmement n'aient expiré et d'armer rapidement le système lorsque l'on quitte les lieux.

La hauteur d'installation recommandée est de 1,3 à 1,5 mètre au-dessus du sol. Installez le clavier sur une surface plane et verticale. Cela permet de s'assurer que votre KeyPad TouchScreen est solidement fixé à la surface et d'éviter les déclenchements intempestifs du bouton anti-sabotage.



Intensité du signal

Le niveau du signal Fibra est déterminé par le nombre de paquets de données non livrés ou endommagés sur une période de temps donnée. L'icône  dans l'onglet **Appareils**  indique la puissance du signal :

- **Trois barres** – excellente intensité du signal.
- **Deux barres** – bonne intensité du signal.
- **Une barre** – intensité du signal faible, le fonctionnement stable n'est pas garanti.
- **Icône barrée** – pas de signal.

Qu'est-ce que le Test d'intensité du signal Fibra

N'installez pas le clavier

1. À l'extérieur. Cela peut entraîner une défaillance du clavier.
2. Dans les endroits où des parties de vêtements (par exemple, à côté du portemanteau), des câbles d'alimentation ou des fils Ethernet peuvent obstruer le clavier. Cela peut entraîner un déclenchement intempestif du clavier.
3. À l'intérieur de locaux dont la température et l'humidité dépassent les limites admissibles. Cela pourrait endommager le clavier.
4. Dans un endroit où le niveau de signal est faible. Cela pourrait entraîner la perte de connexion avec la centrale.
5. Près des détecteurs de bris de glace. Le son du buzzer intégré peut déclencher une alarme.

6. Dans les endroits où le signal sonore sera atténué (à l'intérieur de meubles, derrière des rideaux épais, etc.).

Conception

Il est essentiel de bien concevoir le projet du système afin de garantir l'installation et la configuration correctes des appareils. Le projet doit tenir compte du nombre et des types de dispositifs présents sur le site, de leur emplacement exact et de leur hauteur d'installation, de la longueur des câbles Fibra, du type de câble utilisé et d'autres paramètres. Consultez [cet article](#) pour savoir comment concevoir le projet de système Fibra.



Longueur et type de câble

La portée maximale d'une connexion filaire utilisant la topologie **Linéaire** est de 2 000 mètres, et de 500 mètres en utilisant la topologie **en Anneau**.

Types de câbles recommandés :

- U/UTP cat.5 4 × 2 × 0,51, conducteur en cuivre.
- Câble de signal 4 × 0,22, conducteur en cuivre.



Veillez noter que la portée de connexion câblée peut varier si d'autres types de câbles sont utilisés. Pour l'instant, aucun autre type de câble n'a été testé.

Vérification avec un calculateur

Pour s'assurer que la conception est calculée correctement et que le système fonctionnera dans la pratique, nous avons développé le [Calculateur d'alimentation Fibra](#). Le calculateur permet de vérifier la qualité de la communication et la longueur du câble pour les appareils filaires Fibra avec la configuration choisie lors de la conception du projet de système.

Préparer l'installation

Gestion des câbles

Avant de poser des câbles, vérifiez les règles de sécurité électrique et anti-incendie en vigueur dans votre région. Suivez scrupuleusement ces normes et réglementations. Des conseils pour la pose des câbles sont disponibles dans [cet article](#).



Cheminement des câbles

Avant de commencer l'installation, nous vous conseillons vivement de lire attentivement la section [Mise en place des appareils](#). S'en tenir au projet de système décrit sans dévier. Le non-respect des règles d'installation de base du KeyPad TouchScreen et des recommandations de ce manuel entraîne un fonctionnement incorrect, ainsi qu'une perte de connexion avec le dispositif. Des conseils pour l'acheminement des câbles sont disponibles dans [cet article](#).

Préparation des câbles pour la connexion

Retirez la couche isolante du câble et dénudez le câble avec une pince à dénuder. Les extrémités des fils insérés dans les bornes du dispositif doivent être étamées ou serties avec un manchon. Cela garantit une connexion fiable et protège le conducteur de l'oxydation. Des conseils pour la préparation des câbles sont disponibles dans [cet article](#).

Installation



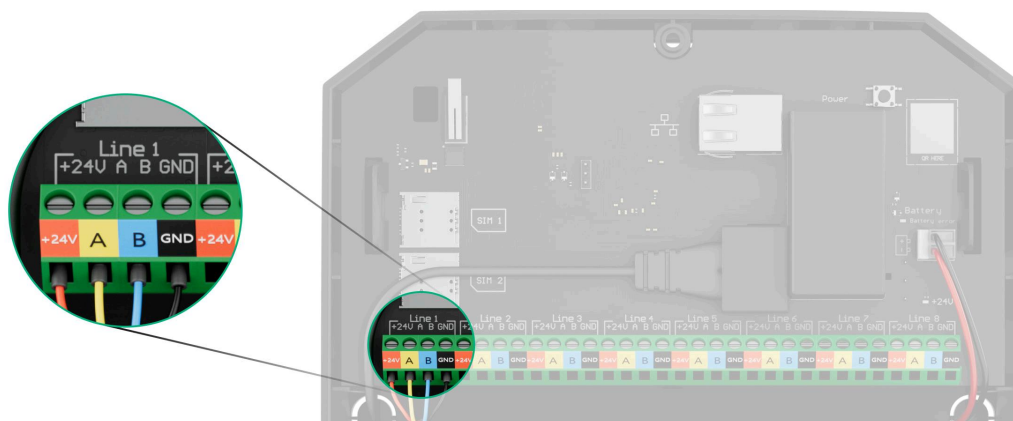
Avant d'installer le KeyPad TouchScreen, assurez-vous que vous avez choisi l'emplacement optimal et qu'il est conforme aux directives de ce manuel.

Pour installer un clavier :

1. Désactivez l'alimentation des lignes dans l'application Ajax PRO :

- **Centrale** → **Paramètres** ⚙️ → **Lignes** → **Alimentation des lignes**.

2. Passez le câble pour connecter le KeyPad TouchScreen au boîtier de la centrale. Connectez les fils à la ligne requise de la centrale.

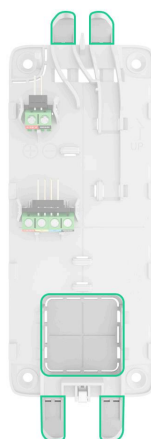


+24V — borne d'alimentation de 24 V $\overline{=}$.

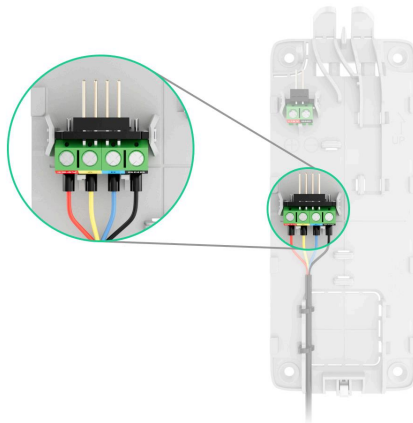
A, B — bornes de signal.

GND — terre.

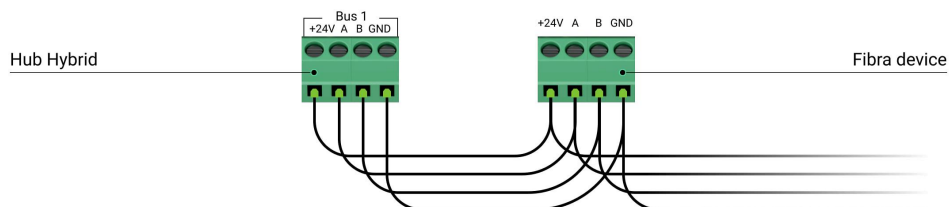
3. Retirez le panneau de montage SmartBracket du clavier. Dévissez d'abord la vis de fixation et faites glisser le panneau vers le bas.
4. Détachez soigneusement la partie perforée nécessaire pour faire sortir le câble par l'arrière (en haut, en bas ou à travers le mur).



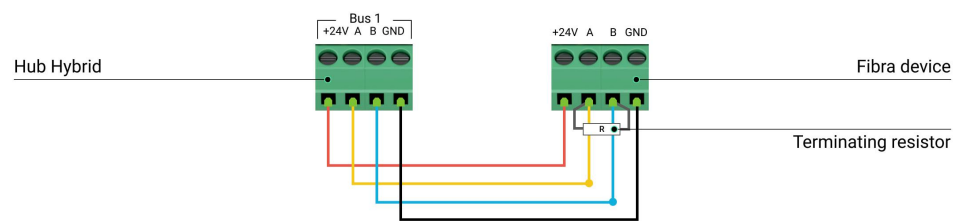
5. Faites passer le câble de la centrale et, en option, d'une alimentation électrique externe dans le boîtier du clavier.
6. Connectez les fils aux bornes du KeyPad TouchScreen selon le schéma ci-dessous. Veillez à ce que la polarité et l'ordre des connexions des câbles soient corrects. Fixez fermement le câble aux bornes.



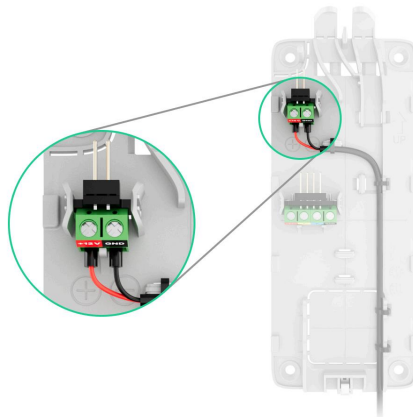
1. Si le Superior KeyPad TouchScreen Fibra n'est pas le dernier dispositif de la ligne de connexion, préparez un deuxième câble à l'avance. Connectez les fils aux bornes selon le schéma ci-dessous. Les extrémités des fils du premier et du second câble, qui seront insérées dans les bornes du clavier, doivent être étamées et soudées ensemble, ou serties avec des embouts spéciaux.



2. Si le KeyPad TouchScreen est le dernier appareil sur la ligne et que vous utilisez la connexion **Linéaire**, installez une résistance de terminaison sur les deux contacts en la connectant aux bornes de signal du module d'intégration. La résistance de terminaison (120 Ω) est incluse dans le kit complet Hub Hybrid.



7. Connectez le câble de l'alimentation externe aux bornes correspondantes. Elle est nécessaire pour maintenir l'écran toujours actif.



8. Faites passer les câbles à travers les conduits et fixez-les à l'aide d'attaches.



Exemples d'acheminement de câbles :

Vers le bas du clavier



Vers le haut du clavier

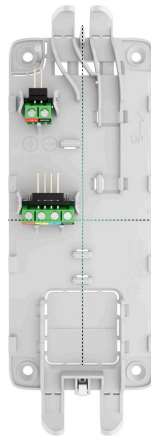


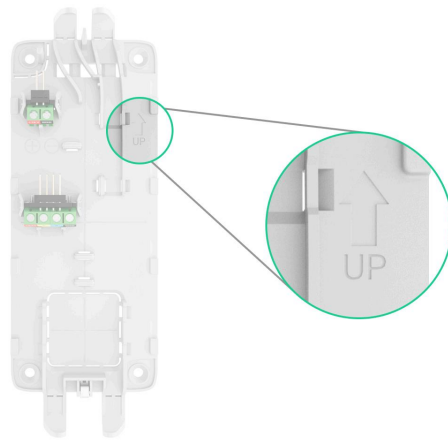
9. Fixez temporairement le panneau de montage SmartBracket à l'aide d'un ruban adhésif double face à l'endroit choisi pour l'installation.



Le ruban adhésif double-face ne peut être utilisé que pour une installation temporaire. Le dispositif fixé par le ruban adhésif peut se décoller de la surface. Tant que le dispositif est scotché, le bouton anti-sabotage ne se déclenche pas lorsque le dispositif est détaché de la surface.

SmartBracket comporte des repères à l'intérieur pour faciliter l'installation. L'intersection de deux lignes marque le centre du dispositif (et non le panneau de montage). De même, la touche **UP** du SmartBracket marque le haut du clavier. Référez-vous à ces marquages lors de l'installation du clavier.





10. Installez le clavier sur le SmartBracket.

11. Activez l'alimentation électrique des lignes dans l'application Ajax PRO :

- **Centrale** → **Paramètres** ⚙️ → **Lignes** → **Alimentation des lignes**.

12. La LED du dispositif clignote. Il s'agit d'un signal indiquant que le boîtier du clavier est fermé.



Si la LED ne s'allume pas lors de l'installation sur SmartBracket, vérifiez l'état du bouton anti-sabotage dans l'application Ajax, l'intégrité de la fixation et l'étanchéité de la fixation du clavier sur le panneau.

13. Ajoutez le clavier à la centrale.

14. Exécutez le test de fonctionnalité.

15. Si les tests sont réussis, retirez le clavier du SmartBracket.

16. Fixez le panneau SmartBracket sur la surface à l'aide des vis jointes. Utilisez tous les points de fixation.



Lorsque vous utilisez d'autres éléments de fixation, assurez-vous qu'ils n'endommagent pas ou ne déforment pas le panneau.

17. Placez le clavier sur le panneau de montage SmartBracket.

- 18.** Serrez la vis de fixation située sous le boîtier du clavier. La vis est nécessaire pour une fixation plus fiable et pour protéger le clavier du démontage rapide.



Raccordement d'un bloc d'alimentation tiers

Lors de la connexion d'une alimentation externe et de l'utilisation du KeyPad TouchScreen, il faut respecter les règles générales de sécurité électrique pour l'utilisation de l'équipement électrique et les exigences de la réglementation en matière de sécurité électrique.

KeyPad TouchScreen est équipé de bornes permettant de connecter un bloc d'alimentation 10,5V–14 V $\overline{=}$. Les paramètres électriques recommandés pour le bloc d'alimentation sont : 12 V $\overline{=}$ avec un courant de 0,5 A.

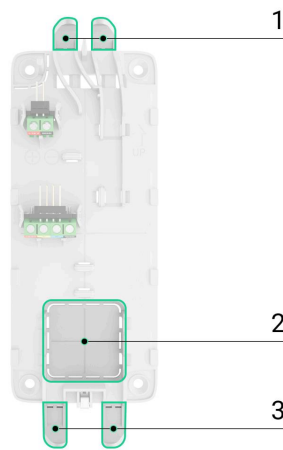
Ne retirez pas les batteries de secours préinstallées pendant le branchement de l'alimentation électrique.



Avant d'installer l'appareil, vérifiez que l'isolation des fils n'est pas endommagée. Utilisez uniquement une source d'alimentation mise à la terre. Ne jamais démonter l'appareil sous tension. N'utilisez pas l'appareil avec un câble d'alimentation endommagé.

Pour connecter un bloc d'alimentation tiers :

1. Retirez le panneau de montage SmartBracket. Cassez délicatement la partie perforée du boîtier pour libérer les ouvertures destinées au passage du câble :



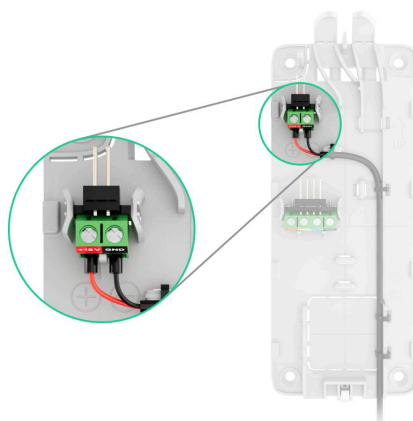
1 – pour faire sortir le câble par le haut ; il suffit de briser une des parties perforées.

2 – pour faire sortir le câble à travers le mur.

3 – pour faire sortir le câble par le bas ; il suffit de briser une des parties perforées.

2. Mettez hors tension le câble d'alimentation externe.

3. Connectez le câble aux bornes en respectant la polarité (marquée sur le plastique).



4. Une fois le clavier installé et ajouté à la centrale, vérifiez l'état des batteries de secours et de l'alimentation externe dans l'application Ajax, ainsi que le fonctionnement général du dispositif.

Mise à jour du firmware

La mise à jour du firmware du KeyPad TouchScreen peut être installée lorsqu'une nouvelle version est disponible. Consultez la liste des appareils dans les applications Ajax PRO: Tool for Engineers et PRO Desktop pour en savoir plus. Si une mise à jour est disponible, le clavier correspondant aura une icône . Un administrateur ou un PRO ayant accès aux paramètres du système peut lancer la mise à jour dans les états ou les paramètres du KeyPad TouchScreen. Une mise à jour peut prendre jusqu'à 1 heure.



Comment mettre à jour le firmware du KeyPad TouchScreen

Maintenance

Vérifiez régulièrement le fonctionnement de votre KeyPad TouchScreen. La fréquence optimale des contrôles est d'une fois tous les trois mois. Nettoyez la poussière, les toiles d'araignée et d'autres contaminants sur le boîtier du dispositif dès leur apparition. Utilisez un chiffon sec et doux, adapté à l'entretien du matériel.

N'utilisez pas de substances contenant de l'alcool, de l'acétone, de l'essence ou d'autres solvants actifs pour nettoyer le dispositif. Essayez délicatement l'écran tactile.

L'appareil fonctionne jusqu'à 1,5 an avec les batteries préinstallées : une valeur calculée sur la base des paramètres par défaut et d'un maximum de 4 interactions quotidiennes avec le clavier.

Le système envoie une notification précoce lorsqu'il est temps de remplacer les batteries. Lors du changement de mode de sécurité, la LED s'allume lentement et s'éteint.

Caractéristiques techniques

Toutes les caractéristiques techniques Superior KeyPad TouchScreen Fibra

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 l'appareil 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

Contacter l'assistance technique :

- e-mail
- Telegram

Fabriqué par « AS Manufacturing » LLC



Abonnez-vous à nos e-mails et découvrez nos derniers conseils sécurité. Aucun spam

Email

S'abonner

