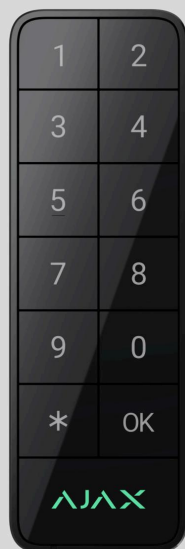


Manuel utilisateur Superior KeyPad Outdoor Fibra

Mis à jour November 20, 2024



Superior KeyPad Outdoor Fibra est un clavier filaire conçu pour gérer le système Ajax. Les utilisateurs peuvent s'authentifier à l'aide de smartphones, de télécommandes Tag, de cartes Pass et de codes. Le dispositif est conçu pour une utilisation à l'extérieur et à l'intérieur et est conforme aux exigences de la norme EN 50131 (Grade 3).

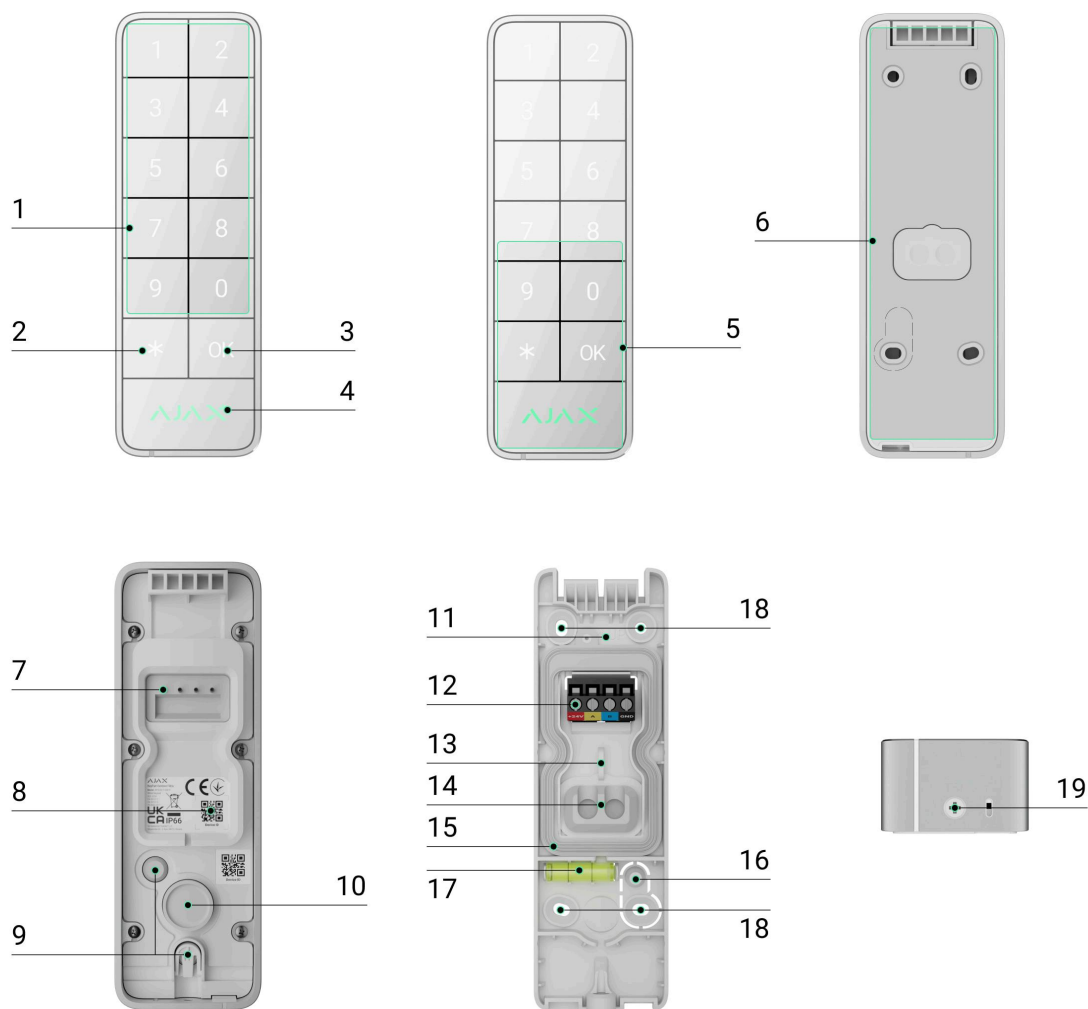
Le clavier fait partie d'un système Ajax et échange des données avec la centrale en utilisant le protocole de communication filaire sécurisé Fibra.

En savoir plus

Superior KeyPad Outdoor Fibra fait partie de la ligne de produits Superior. Seuls les partenaires accrédités par Ajax Systems peuvent installer, vendre et gérer les produits Superior.

Acheter Superior KeyPad Outdoor Fibra

Éléments fonctionnels



1. Numpad.
2. Bouton de **Fonction**.
3. Bouton **OK** avec un indicateur LED.
4. Logo Ajax avec indicateur LED.
5. Lecteur de cartes/portesclés/Bluetooth.
6. Panneau de montage SmartBracket. Pour retirer le panneau, dévisser la vis de fixation.
7. Broches pour connecter le dispositif aux bornes d'entrée du SmartBracket.

8. Code QR avec l'ID de l'appareil. Il est utilisé pour ajouter le détecteur avec la centrale.
9. Boutons anti-sabotage.
10. Buzzer intégré.
11. Clé **UP**, qui indique le haut du clavier.
12. Bornes d'entrée pour connecter la ligne Fibra au Superior KeyPad Outdoor Fibra.
13. Supports pour fixer les câbles avec des attaches.
14. Bague d'étanchéité en caoutchouc pour l'acheminement des câbles à l'arrière du dispositif.
15. Bague d'étanchéité rectangulaire en caoutchouc. Protège le dispositif contre l'eau. Ne l'enlevez pas !
16. Partie perforée du panneau de montage. Nécessaires pour déclencher le bouton anti-sabotage en cas de tentative de détacher le détecteur de la surface. Ne la cassez pas.
17. Niveau à bulle pour vérifier l'angle d'inclinaison du panneau de montage pendant l'installation.
18. Ouvertures pour fixer SmartBracket à la surface.
19. Vis de fixation pour sécuriser le dispositif sur le SmartBracket.



Centrales compatibles

Une centrale Ajax avec la version du firmware OS Malevich 2.28 et supérieure est nécessaire pour que le clavier fonctionne.

Vérifier la compatibilité des dispositifs

Principe de fonctionnement

Superior KeyPad Outdoor Fibra est doté de grandes touches mécaniques, d'un lecteur pour les autorisations sans contact, d'un buzzer intégré et

d'indicateurs LED. Le clavier est utilisé pour contrôler les modes de sécurité et les dispositifs d'automatisation et pour notifier les événements du système par le biais d'un son et d'une indication LED.

Superior KeyPad Outdoor Fibra est doté de modes de fonctionnement **primaire** et **secondaire**. Vous pouvez configurer une fonction de clavier pour chaque mode et passer d'un mode à l'autre en appuyant longuement sur la touche **OK**.



En savoir plus

La partie inférieure de la face avant du clavier est équipée d'un lecteur pour les autorisations sans contact, ce qui permet de présenter un Tag, un Pass ou un smartphone directement au logo ou aux boutons Ajax.

En fonction des paramètres, le buzzer intégré du Superior KeyPad Outdoor Fibra émet les notifications suivantes :

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

Modes de fonctionnement et fonctions du clavier

Le Superior KeyPad Outdoor Fibra dispose de deux modes de fonctionnement : **primaire** et **secondaire**. Vous pouvez configurer chaque mode indépendamment dans les paramètres du clavier dans les applications Ajax. Pour chaque mode de fonctionnement, vous pouvez régler une seule fonction du clavier et passer d'un mode à l'autre en appuyant longuement sur le bouton **OK** du clavier.

Vous pouvez également désactiver le mode de fonctionnement secondaire si vous n'en avez pas besoin.

Trois fonctions du clavier peuvent être configurées pour chaque mode de fonctionnement du clavier :

- **Changement du mode de sécurité.** Cette fonction permet aux utilisateurs d'armer/désarmer l'ensemble du site ou des groupes spécifiques, ou d'activer le **Mode nuit**.
- **Gérer les dispositifs d'automatisation.** Cette fonction permet aux utilisateurs de créer un scénario avec un ou plusieurs dispositifs d'automatisation qui peuvent être contrôlés directement à partir du clavier.
- **Début de la temporisation au désarmement.** Grâce à cette fonction, les utilisateurs peuvent utiliser Superior KeyPad Outdoor Fibra comme **clavier de contournement** pour activer une temporisation au désarmement afin de pouvoir désarmer le site à l'aide du clavier principal.



Une seule fonction primaire et une seule fonction secondaire peuvent être réglées à la fois.

Superior KeyPad Outdoor Fibra montre quel mode est actuellement actif par indication LED selon la fonction configurée :

- **Changement du mode de sécurité** — le logo Ajax s'allume en rouge ou en vert, en fonction de l'état de sécurité du système. Le bouton **OK** s'allume en blanc, de même que les boutons numériques.
- **Gérer les dispositifs d'automatisation** — le bouton **OK** s'allume en rouge ou en vert, selon l'état du dispositif d'automatisation. Le logo Ajax LED est éteint. Si le clavier contrôle un scénario avec plusieurs dispositifs d'automatisation, l'état du scénario n'est pas disponible sur le clavier.
- **Début de la temporisation au désarmement** — le logo Ajax s'allume en rouge lorsque le site est armé et clignote en rouge en même temps qu'un bip lorsque la temporisation au désarmement est lancée. Le bouton **OK** s'allume en blanc, de même que les boutons numériques.



Contrôle de sécurité

Superior KeyPad Outdoor Fibra permet d'armer et de désarmer l'ensemble du site ou des groupes spécifiques, et d'activer le **Mode nuit**. Vous pouvez contrôler la sécurité à l'aide du Superior KeyPad Outdoor Fibra en utilisant :



1. **Codes.** Superior KeyPad Outdoor Fibra supports general codes, personal codes, and codes for unregistered users.
2. **Cartes ou télécommandes.** Pour identifier rapidement et en toute sécurité les utilisateurs, Superior KeyPad Outdoor Fibra 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. Tag et Pass prennent en charge cette technologie et sont compatibles avec Superior KeyPad Outdoor Fibra.
3. **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.
4. **Codes.** Superior KeyPad Outdoor Fibra 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.



Le nombre de codes personnels, codes d'accès des claviers et codes GIR dépend du modèle de centrale.

[Vérifier la compatibilité des dispositifs](#)

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

Superior KeyPad Outdoor Fibra permet de contrôler la sécurité des groupes (si le **Mode groupe** est activé). Un administrateur ou un PRO ayant les droits de configuration du système peut également ajuster les **paramètres** du clavier pour déterminer les groupes qui seront partagés (groupes de clavier). Pour en savoir plus sur la gestion de la sécurité des groupes, consultez [ce chapitre](#).

Bouton de fonction



Superior KeyPad Outdoor Fibra est doté d'une touche de **Fonction** (*) qui fonctionne selon l'un des trois modes suivants :

- **Aucun** – le bouton **Fonction** est désactivé et rien ne se produit lorsque l'utilisateur appuie brièvement sur ce bouton.
- **Panique** – après avoir appuyé sur le bouton de **Fonction**, le système envoie une alarme au centre de télésurveillance de l'entreprise de sécurité et à tous les utilisateurs.
- **Désactiver l'alarme incendie.** – après avoir appuyé sur le bouton de **Fonction**, le système coupe l'alarme des détecteurs d'incendie Ajax. Disponible uniquement si la fonction Alarme incendie interconnectée est activée (Centrale → Paramètres ⚙️ → Service → Paramètres des détecteurs d'incendie).



En outre, les codes incorrectement saisis peuvent être effacés par une pression longue sur la touche de **Fonction** si aucune autre action n'est programmée pour une pression longue.

Code de contrainte

Superior KeyPad Outdoor Fibra 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

Début de la temporisation au désarmement (clavier de contournement)

La fonction **Début de la temporisation au désarmement** (c'est-à-dire un clavier de contournement) est conçue pour activer une temporisation au désarmement avant que le site ne soit désarmé à l'aide du clavier principal.

La technologie de contournement permet de désactiver temporairement les détecteurs de sécurité, tels que les détecteurs d'ouverture et autres. Cela permet aux utilisateurs de disposer de plus de temps entre le moment où ils entrent dans une zone et celui où ils peuvent désarmer le site à l'aide du dispositif de contrôle principal (par exemple, KeyPad TouchScreen Fibra).

[En savoir plus](#)



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.

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

Armement en deux étapes

Le clavier Superior KeyPad Outdoor Fibra 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 de Tag, Pass ou d'un smartphone est similaire à l'utilisation d'un code personnel ou général sur le clavier.

[En savoir plus](#)

Gestion des dispositifs d'automatisation et des scénarios

Superior KeyPad Outdoor Fibra dispose de la fonction **Gérer les dispositifs d'automatisation**, conçue pour contrôler un ou plusieurs

dispositifs d'automatisation. Par exemple, un utilisateur peut ouvrir les portes de garage ou éteindre tous les interrupteurs intelligents du site.

Lorsque le clavier contrôle un dispositif d'automatisation, il indique l'état du dispositif avec l'indication par LED de la touche **OK**. Lorsque le bouton **OK** est vert, un dispositif d'automatisation est actif ; lorsqu'il est rouge, un dispositif d'automatisation est inactif.



Lorsque le clavier contrôle un scénario avec plusieurs dispositifs d'automatisation, il ne peut pas afficher l'état du dispositif ou du scénario. Il indique plutôt si l'action est terminée ou non.



Superior KeyPad Outdoor Fibra ne peut gérer qu'un seul scénario.

La gestion des dispositifs d'automatisation n'est disponible qu'après autorisation sur le clavier.

Indication du mode de sécurité et de l'état des dispositifs d'automatisation

Superior KeyPad Outdoor Fibra informe les utilisateurs du mode de sécurité du système et de l'état du dispositif d'automatisation au moyen de :

- le logo avec indication LED ;
- le bouton **OK** avec indication LED ;
- l'indication sonore.

Si le clavier est en mode Changement du mode de sécurité, le logo Ajax s'allume en vert ou en rouge pour notifier l'état du mode de sécurité du système.

Si le clavier est en mode **Gérer les dispositifs d'automatisation**, le bouton **OK** s'allume en vert ou en rouge pour signaler l'état du dispositif

d'automatisation. Mais lorsque le clavier gère un scénario avec plusieurs dispositifs d'automatisation, il ne peut pas notifier l'état du scénario.

Un buzzer intégré signale les alarmes, les ouvertures de porte et les temporisations à l'armement et au désarmement.

Pour plus d'informations, voir la section [Indication](#).



Silence de l'alarme incendie

Superior KeyPad Outdoor Fibra peut couper le son d'une alarme incendie interconnectée en appuyant sur la touche de **Fonction** (si le paramètre requis est activé). La réponse du système à l'appui sur le bouton dépend des réglages et de l'état du système :

- **L'alarme incendie interconnectée s'est déjà propagée** – dès la première pression sur le bouton, toutes les sirènes des détecteurs d'incendie sont mises en sourdine, à l'exception de celles qui ont enregistré l'alarme. En appuyant à nouveau sur le bouton, les détecteurs restants sont mis sous silence.
- **La temporisation de l'alarme interconnectée est en cours** – l'appui sur le bouton de **Fonction** coupe la sirène du détecteur incendie Ajax déclenché.

N'oubliez pas que l'option n'est disponible que si l'**Alarme des détecteurs d'incendie interconnectés** est activée.

[En savoir plus](#)

Protocole de transfert de données Fibra

Le dispositif utilise la technologie Fibra pour transmettre les alarmes et les événements. 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 dispositifs connectés.

Transmission d'événements au centre de télésurveillance

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



Superior KeyPad Outdoor Fibra peut transmettre les événements suivants :

1. Armement/désarmement du système.
2. Saisie du code de contrainte.
3. Appui sur le bouton de panique.
4. Verrouillage du clavier suite à une tentative d'accès non autorisé.
5. Tentative infructueuse d'armer le système de sécurité (avec vérification de l'intégrité activée).
6. Alarme anti-sabotage. Récupération en cas d'anti-sabotage.
7. Faible tension d'alimentation sur la ligne Fibra et retour de la tension à des valeurs normales.
8. Perte/rétablissement de la connexion avec la centrale.
9. Désactivation forcée / activation du dispositif.
10. Désactivation unique / activation du dispositif.

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 dispositifs 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. La liste des paramètres transmis peut différer selon le type de centre de télésurveillance et le protocole de communication sélectionné.



Vous pouvez trouver l'ID du dispositif, le numéro de boucle (zone) et le numéro de ligne dans les États du dispositif.



Sélection de l'emplacement

Lorsque vous choisissez l'endroit où installer Superior KeyPad Outdoor Fibra, tenez compte des paramètres qui affectent son fonctionnement :

- Test d'intensité du signal Fibra.
- La longueur du câble de raccordement du clavier.

Tenez compte des recommandations de l'emplacement lors de l'élaboration d'un projet pour le système de sécurité du site. Le système Ajax doit être conçu et installé par des spécialistes. Une liste des partenaires officiels autorisés d'Ajax est disponible ici.

Superior KeyPad Outdoor Fibra se place idéalement à l'extérieur ou à l'intérieur, près de l'entrée. Cela permet aux utilisateurs de désarmer le site avant d'entrer dans les locaux ou jusqu'à ce que les temporisations au désarmement expirent. Les utilisateurs peuvent également armer rapidement le site lorsqu'ils quittent les lieux.

Superior KeyPad Outdoor Fibra est doté d'un boîtier protégé, de sorte que le clavier peut être installé dans des lieux publics, tels que des restaurants, des hôpitaux, des bureaux, ou dans des usines de production soumises à des conditions difficiles.

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

Intensité du signal Fibra

L'Intensité du signal Fibra est déterminée en fonction du rapport entre le nombre de paquets de données non livrés ou corrompus et ceux prévus sur une certaine période de temps. L'icône ||| dans l'onglet **Dispositifs**  dans les applications Ajax indique l'Intensité 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

Test d'alimentation des lignes

Le test simule la consommation maximale d'énergie des dispositifs connectés à la centrale. Si le système passe le test avec succès, tous ses dispositifs disposent d'une puissance suffisante dans n'importe quelle situation. Après le test, l'application affiche une notification indiquant l'état de chaque ligne :

- Test réussi.
- Test réussi avec des dysfonctionnements.
- Test échoué.

Qu'est-ce que le test d'alimentation des lignes

N'installez pas le clavier

1. Dans les endroits où des câbles d'alimentation ou Ethernet, des objets décoratifs ou autres peuvent obstruer le clavier.
2. Dans les endroits où la température et l'humidité dépassent les limites autorisées. Cela pourrait endommager le dispositif.

3. Dans les endroits où le signal sonore sera atténué (à l'intérieur de meubles, derrière des rideaux épais, etc.).
4. Près des détecteurs de bris de glace. Le son du buzzer intégré peut déclencher une alarme.
5. Dans les endroits où l'intensité du signal Fibra est faible ou instable.



Conception et préparation

Il est essentiel de bien concevoir le projet de système afin d'installer et de configurer correctement les dispositifs. 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.

Conseils pour la conception du projet de système Fibra



Les systèmes Ajax prennent également en charge les topologies **Linéaire** et **En anneau**.

[En savoir plus](#)

Longueur et type de câble

La portée maximale d'une connexion filaire utilisant la topologie **Linéaire** est de 2 000 mètres et celle utilisant la topologie **En anneau** est de 500 mètres.

Types de câbles recommandés pour connecter Superior KeyPad Outdoor Fibra à la centrale :

- U/UTP cat.5 4 × 2 × 0,51 mm (24 AWG), conducteur en cuivre.
- Câble de signal 4 × 0,22 mm², conducteur en cuivre.



La portée de la connexion filaire peut varier si vous utilisez un autre type de câble. Aucun autre type de câble n'a été testé.

Vérification avec un calculateur

Utilisez le [Calculateur d'alimentation Fibra](#) pour vous assurer que le projet est conçu correctement et que le système fonctionnera dans la pratique. 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

Lors de la préparation de la pose des câbles, vérifiez les réglementations en matière d'électricité et de sécurité 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

Nous vous recommandons de lire attentivement la section [Sélection du lieu d'installation](#) avant l'installation. Essayez d'éviter toute modification de la conception du système. Le non-respect des règles d'installation de base de Superior KeyPad Outdoor Fibra et des recommandations de ce manuel peut entraîner un mauvais fonctionnement et la perte de la 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 et connexion



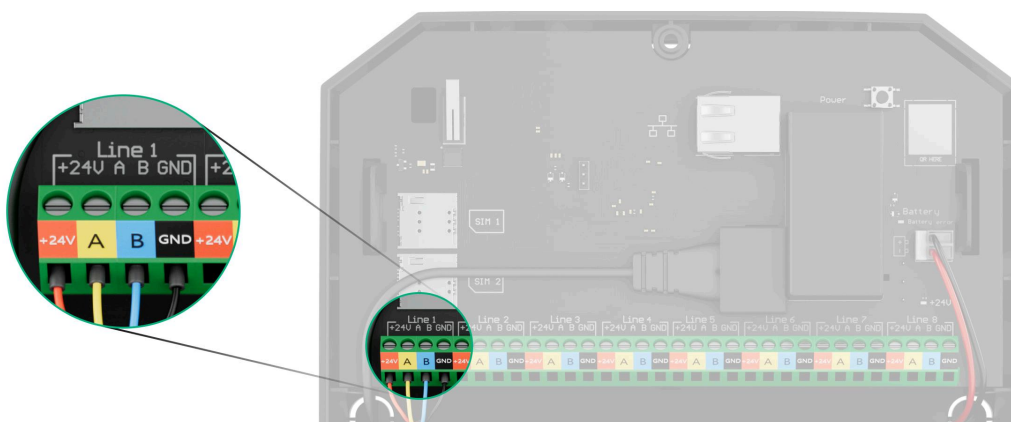
Avant d'installer **Superior KeyPad Outdoor Fibra**, assurez-vous que l'emplacement optimal du clavier a été sélectionné et qu'il répond aux exigences de ce manuel. Les câbles doivent être cachés et placés à un endroit difficile d'accès pour les intrus, afin de réduire les risques de sabotage. Il serait préférable de les faire passer dans les murs, le sol ou le plafond. Avant l'installation finale, effectuez le [Test d'intensité du signal Fibra](#).

Pour installer un clavier :

1. Désactivez l'alimentation des lignes dans [l'application Ajax PRO](#) :

- Centrale → Paramètres ⚙️ → Lignes → Alimentation des lignes

2. Acheminez le câble pour connecter Superior KeyPad Outdoor Fibra au boîtier de la centrale. Connectez les fils à la ligne requise de la centrale.

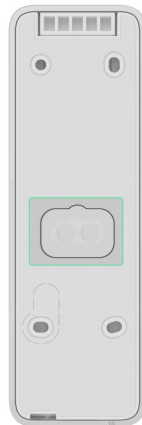


+24V – borne d'alimentation 24 V $\overline{=}$.

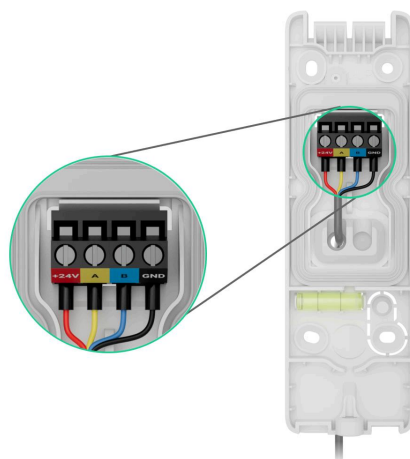
A, B – bornes de signal.

GND – mise à la terre.

3. Dévissez la vis de fixation située au bas de l'appareil et retirez le panneau de montage SmartBracket du clavier.
4. Faire un ou deux trous dans la bague d'étanchéité en caoutchouc dans les évidements, en fonction du nombre de câbles.



5. Faites passer le câble de la centrale dans le boîtier du détecteur par l'orifice prévu à cet effet.
6. Connectez les fils aux bornes 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.

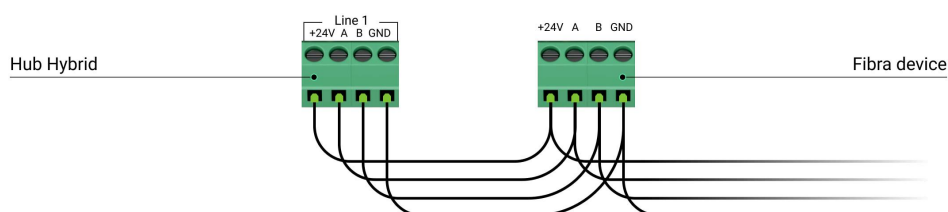


+24V – borne d'alimentation 24 V_{DC}.

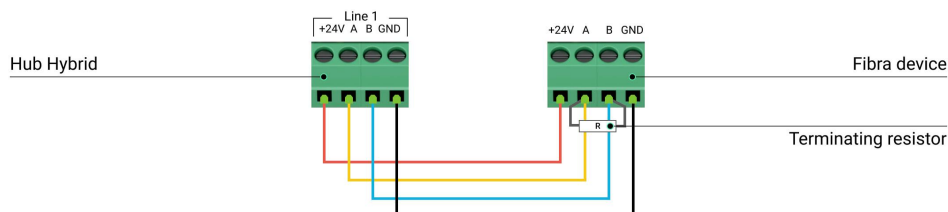
A, B – bornes de signal.

GND – mise à la terre.

1. Si le détecteur n'est pas le dernier de la ligne de connexion, préparez un deuxième câble à l'avance. 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 Superior KeyPad Outdoor Fibra est le dernier dispositif 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 dispositif. La résistance de terminaison (120 Ohm) est incluse dans le kit complet de la centrale. Lorsque la **topologie En anneau** est utilisée, une résistance de terminaison n'est pas nécessaire.



Nous recommandons d'utiliser la méthode de connexion **En anneau** (centrale – dispositif – centrale). Si l'anneau est rompu, aucun dispositif ne sera désactivé. En cas de rupture, deux lignes seraient formées et pourraient continuer à fonctionner et à transmettre les événements à la centrale. Si l'anneau est rompu, les utilisateurs et le centre de télésurveillance en seront informés.

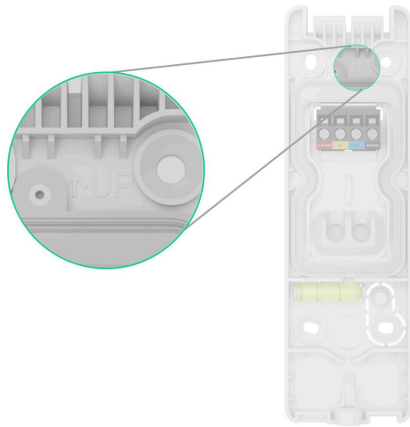
7. Fixez temporairement le panneau SmartBracket à une surface verticale ou à un coin à l'aide d'une bande adhésive double face ou d'autres fixations temporaires.



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 a la touche **UP** qui indique le haut du clavier. Il faut en tenir compte lors de l'installation du dispositif.



8. Placez le clavier sur le panneau de montage SmartBracket.
9. Activez l'alimentation électrique des lignes dans l'application Ajax PRO :
 - Centrale → Paramètres ⚙️ → Lignes → Alimentation des lignes
10. 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.

11. Ajoutez le clavier à la centrale.

12. Exécutez le test de fonctionnalité.

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

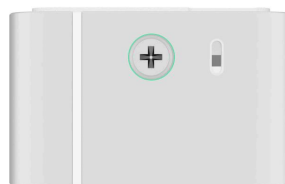
14. Fixez le panneau SmartBracket sur la surface à l'aide des vis jointes. Utilisez tous les points de fixation.



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

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

16. 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. De plus, la vis est dotée d'un bouton anti-sabotage qui réagit si quelqu'un tente de dévisser la vis de fixation. Le système envoie une notification de déclenchement du bouton anti-sabotage aux applications Ajax et au centre de télésurveillance.



Ajout au système





Vérifier la compatibilité du dispositif avant d'ajouter le clavier au système. Seuls les partenaires vérifiés peuvent ajouter et configurer les dispositifs Superior dans les applications Ajax PRO.

Types de comptes et leurs droits



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.
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

Deux façons d'ajouter des dispositifs sont disponibles dans l'application Ajax PRO : automatiquement et manuellement.

Automatiquement Manuellement

Pour ajouter un dispositif automatiquement :

1. Ouvrez l'app Ajax PRO. Sélectionnez la centrale à laquelle vous souhaitez ajouter Superior KeyPad Outdoor Fibra.
2. Allez dans l'onglet **Dispositifs**  et appuyez sur **Ajouter un dispositif**.

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.



Le balayage est également disponible dans le menu **Lignes** :

Centrale → **Paramètres** → **Lignes** → **Ajouter tous les dispositifs Fibra**.



4. Sélectionnez l'appareil dans la liste. Après avoir appuyé, l'indicateur LED clignote pour identifier ce dispositif.
5. Spécifiez un nom, une pièce et un groupe si le **Mode groupe** est activé.
6. Appuyez sur **Enregistrer**.

Le dispositif connecté à la centrale apparaîtra dans l'application Ajax dans la liste des appareils de la centrale.

Si la connexion échoue, vérifiez que la connexion filaire est correcte et réessayez. Si le nombre maximum de dispositifs a déjà été ajouté à la centrale, vous recevrez une notification d'erreur lors de l'ajout.



Superior KeyPad Outdoor Fibra 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).



Superior KeyPad Outdoor Fibra fonctionne 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.



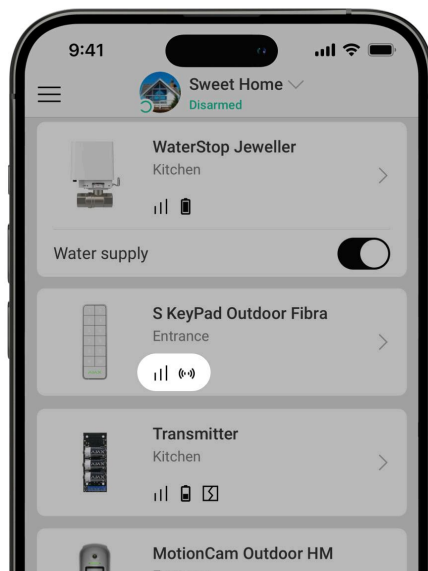
Test de fonctionnalité

Le système de sécurité Ajax propose plusieurs types de tests pour vous aider à choisir le bon endroit pour installer les appareils. Test de l'intensité du signal Fibra est disponible pour Superior KeyPad Outdoor Fibra. Ce test détermine l'intensité et la stabilité du signal sur le site d'installation de l'appareil.

Pour exécuter un test dans l'application Ajax :

1. Sélectionnez l'espace requis.
2. Allez dans l'onglet **Appareils** .
3. Sélectionnez **Superior KeyPad Outdoor Fibra** dans la liste.
4. Allez dans **Paramètres** .
5. Exécutez le Test d'intensité du signal.

Icônes



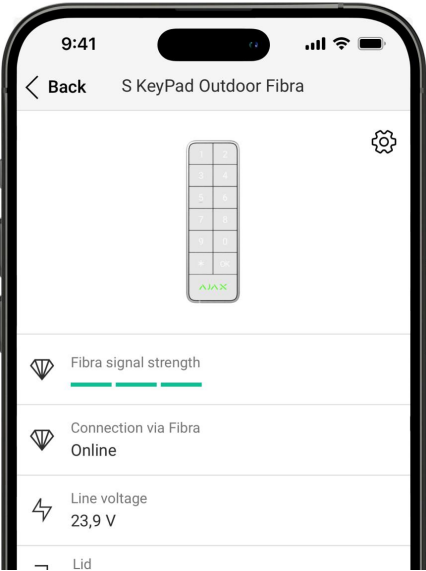
Les icônes de l'application Ajax affichent certains états de Superior KeyPad Outdoor Fibra. Les icônes peuvent être visualisées dans l'onglet **Dispositifs** .

Icône	Signification
	Intensité du signal Fibra : affiche l'intensité du signal entre la centrale et le dispositif. Valeurs recommandées de 2 à 3 barres. <u>En savoir plus</u>
	Lecture du Pass/Tag est activée dans les paramètres du clavier.
	Le Bluetooth est activé dans les paramètres du clavier.
	La configuration du Bluetooth n'est pas terminée. La description est disponible dans les états du clavier.
	Le carillon à l'ouverture est activé dans les paramètres du clavier.
	Le panneau de montage est déverrouillé.
	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'à ce que le site soit désarmé pour la première fois. <u>En savoir plus</u>
	Les notifications d'alarme du bouton anti-sabotage sont désactivées jusqu'à ce que le site soit désarmé pour la première fois. <u>En savoir plus</u>
	Le dispositif n'a pas été transféré à la nouvelle centrale. <u>En savoir plus</u>



États



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

1. Allez dans l'onglet **Dispositifs** .

2. Sélectionnez **Superior KeyPad Outdoor Fibra** dans la liste.

Paramètre	Signification
Dysfonctionnement	Un clic sur ⓘ ouvre la liste des dysfonctionnements. Ce champ s'affiche si un dysfonctionnement est détecté.
Avertissement !⚠	Un clic sur ⓘ ouvre la liste des paramètres et des autorisations que l'application doit obtenir pour le bon fonctionnement du clavier.
Température	Température du dispositif. Elle est mesurée par le processeur et varie en fonction de la température ambiante. Vous pouvez configurer un scénario par température pour contrôler les dispositifs d'automatisation. <u>En savoir plus</u>
Intensité du signal Fibra	Intensité du signal entre la centrale et Superior KeyPad Outdoor Fibra. Valeurs recommandées de 2 à 3 barres. Fibra est un protocole de transmission des événements et des alarmes. <u>En savoir plus</u>





Connexion via Fibra	État de la connexion entre la centrale et le dispositif : • En ligne — le dispositif est connecté à la centrale. • Hors ligne – le détecteur n'est pas connecté à la centrale. Vérifiez la connexion du dispositif à la centrale.
Tension de la ligne	La valeur de la tension sur la ligne Fibra à laquelle le dispositif est connecté.
Couvercle	L'état du bouton anti-sabotage du dispositif qui réagit à l'arrachement ou à l'ouverture du boîtier du dispositif : • Ouvert – le déclencheur a été retiré du panneau de montage SmartBracket ou l'intégrité de son boîtier a été compromise. Vérifiez la fixation du dispositif. • Fermé – le dispositif 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>



Panneau de montage	L'état du bouton anti-sabotage du dispositif qui répond au déverrouillage du panneau de montage SmartBracket : • Déverrouillé – le verrou du SmartBracket est déverrouillé ou son intégrité est compromise. Vérifier la vis de fixation et le montage de l'appareil. • Verrouillé – la vis de maintien du SmartBracket est vissée. L'intégrité du boîtier du dispositif et du panneau de montage n'est pas compromise. État normal. <u>En savoir plus</u>
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.
Paramètres des signaux sonores	
Armé/desarmé	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.

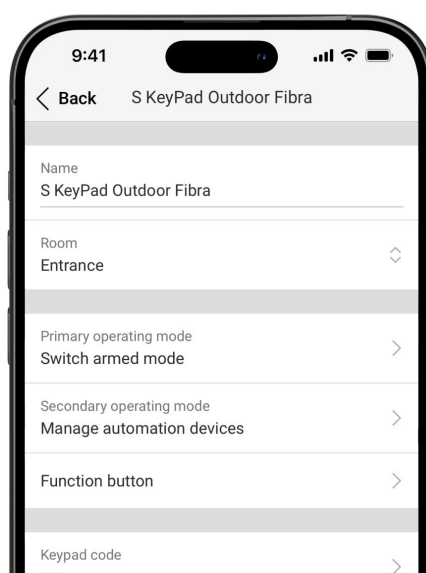


Désactivation forcée	L'état du réglage de la désactivation forcée du dispositif : • Non – le dispositif fonctionne normalement et transmet tous les événements. • Entièrement – le dispositif est complètement exclu du fonctionnement du système. L'appareil ne réagit pas aux commandes du système et ne signale pas les alarmes ou autres événements. • Couvercle seulement – l'administrateur de la centrale a désactivé les notifications relatives aux alarmes anti-sabotage. <u>En savoir plus</u>
Désactivation unique	Indique l'état du réglage de la désactivation unique du dispositif : • Non – le dispositif fonctionne en mode normal. • 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. • Couvercle seulement – les notifications concernant le déclenchement du bouton anti-sabotage sont désactivées lorsque le mode armé est actif. <u>En savoir plus</u>
Firmware	Version firmware du dispositif.
ID du dispositif	ID du dispositif. Également disponible sur le code QR figurant sur le boîtier du dispositif et son emballage.

Appareil n°	Numéro du dispositif. Ce numéro est transmis au centre de télésurveillance en cas d'alarme ou d'événement.
Ligne n°	Le numéro de la ligne Fibra de la centrale à laquelle le dispositif est connecté. Affiché dans le cas d'une connexion Linéaire .
Anneau n°	Le numéro de l'anneau Fibra de la centrale auquel le dispositif est connecté. Affiché en cas de connexion En anneau .



Paramètres



Pour modifier les paramètres de Superior KeyPad Outdoor Fibra dans les applications Ajax:

1. Allez dans l'onglet **Dispositifs** .
2. Sélectionnez **Superior KeyPad Outdoor Fibra** dans la liste.
3. Allez dans **Paramètres** .
4. Définissez les paramètres requis.
5. Cliquez sur **Retour** pour enregistrer les paramètres.



Paramètres	Signification
Nom	Nom du dispositif. Il est affiché dans la liste des dispositifs de la centrale, dans le texte SMS et dans les notifications du flux d'événements. Pour changer le nom du dispositif, cliquez sur le texte du nom. Le nom peut contenir 24 caractères cyrilliques ou 12 caractères latins.
Pièce	Sélection de la pièce virtuelle à laquelle votre Superior KeyPad Outdoor Fibra est assigné. Le nom de la pièce est affiché dans le texte SMS et les notifications dans le flux d'événement.
Mode de fonctionnement primaire	Ouvre le menu avec les paramètres du mode de fonctionnement primaire.
Mode de fonctionnement secondaire	Ouvre le menu avec les paramètres du mode de fonctionnement secondaire.



Bouton de fonction	Sélection de la fonction du ✱ bouton (de Fonction) : • Non – le bouton est désactivé et n'exécute aucune commande lorsqu'il est pressé. • Panique – après avoir appuyé sur le bouton de fonction, le système envoie une alarme au centre de télésurveillance et à tous les utilisateurs. • Désactiver l'alarme incendie – en appuyant sur le bouton, l'alarme des détecteurs d'incendie Ajax est mise en sourdine. Disponible uniquement si la fonction Alarme incendie interconnectée est activée. <u>En savoir plus</u>
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>
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 débloquer le clavier via l'application avant l'expiration du délai de verrouillage spécifié.
Temps de verrouillage automatique	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.
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. • Max. Disponible si la bascule Bluetooth est activée.
Rétroéclairage et indication	Ouvre le menu avec les paramètres de Rétroéclairage et d'indication .

Indication sonore	Ouvre le menu avec les paramètres de Indication sonore .
Test d'intensité du signal Fibra	Bascule le détecteur en mode test d'intensité du signal. Le test vous permet de vérifier l'intensité du signal entre la centrale et le détecteur, via le protocole de transfert de données filaire Fibra, afin de déterminer l'emplacement optimal de l'installation. <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>
Manuel de l'utilisateur	Ouvre le manuel utilisateur de Superior KeyPad Outdoor Fibra dans l'application Ajax.
Désactivation forcée	Permet à l'utilisateur de désactiver le dispositif sans le retirer du système. Trois options sont disponibles : • Non – l'appareil fonctionne normalement et transmet tous les événements. • Entièrement – le dispositif n'exécutera pas les commandes du système et ne participera pas aux scénarios, et le système ignorera les alarmes et autres notifications du dispositif. • Couvercle seulement – le système ignorera uniquement des notifications relatives au déclenchement du 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 – l'appareil fonctionne normalement et transmet tous les événements. • Entièrement – le dispositif 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. • Couvercle seulement – les notifications concernant le déclenchement du bouton anti-sabotage sont désactivées jusqu'au premier désarmement. <u>En savoir plus</u>
Dissocier le dispositif	Dissocie le dispositif, le déconnecte de la centrale et supprime ses paramètres.



Modes de fonctionnement primaire et secondaire

Le Superior KeyPad Outdoor Fibra dispose de deux modes de fonctionnement : **primaire** et **secondaire**. Trois fonctions du clavier peuvent être configurées pour chaque mode de fonctionnement : **Début de la temporisation au désarmement**, **Gérer les dispositifs d'automatisation** ou **Démarrer la temporisation au désarmement**.

Une seule fonction primaire et une seule fonction secondaire peuvent être réglées à la fois. Pour passer d'une fonction à l'autre, appuyez sur la touche **OK** du clavier et maintenez-la enfoncée.



Paramètre	Signification
Mode de fonctionnement primaire	
Fonction du clavier	Sélection de la fonction du clavier pour le mode de fonctionnement principal : • Changement du mode de sécurité • Gérer les dispositifs d'automatisation • Début de la temporisation au désarmement Une seule fonction primaire et une seule fonction secondaire peuvent être réglées à la fois.
Mode de fonctionnement secondaire	
Fonction du clavier	Sélection de la fonction du clavier pour le mode de fonctionnement secondaire : • Non • Changement du mode de sécurité • Gérer les dispositifs d'automatisation • Début de la temporisation au désarmement Une seule fonction primaire et une seule fonction secondaire peuvent être réglées à la fois.
Changement du mode de sécurité	
Sites de sécurité	Sélection des sites de sécurité contrôlés par l'appareil. Vous pouvez sélectionner l'ensemble de l'espace, tous les groupes ou des groupes particuliers, ou le mode Nuit. La sélection de groupes est possible si le <u>mode Groupe</u> est activé.



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.
Pré-autorisation	Lorsque cette option est activée, l'utilisateur doit être authentifié pour utiliser le clavier : il doit saisir un code ou présenter un dispositif d'accès personnel au clavier.
Confirmation de l'autorisation avec un code d'accès	Lorsque cette fonction est activée, les utilisateurs ne peuvent armer ou désarmer le système que s'ils ont été autorisés avec succès à l'aide de deux formes d'identification, c'est-à-dire en utilisant les dispositifs Pass, Tag ou le smartphone et en saisissant le code d'accès approprié. <u>En savoir plus</u>
Changement facile du mode de sécurité	Lorsque cette option est activée, les utilisateurs n'ont pas besoin d'appuyer sur le bouton OK après la saisie d'un code d'accès ou la lecture d'un dispositif d'accès.
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. Disponible si la bascule Pré-autorisation est désactivée.



Passage automatique en mode secondaire	 Disponible uniquement pour le mode de fonctionnement secondaire. Cette option permet à l'utilisateur de définir le moment où le clavier commence automatiquement à fonctionner en mode secondaire sans pression prolongée sur le bouton OK : • Off. • Le système est désarmé. • Le système est armé.
Gérer les dispositifs d'automatisation	
Scénario d'automatisation	Crée et configure un scénario pour gérer les dispositifs d'automatisation à l'aide d'un clavier. Vous pouvez créer un scénario sur une action prédéfinie ou sur le changement d'état d'un ou de plusieurs dispositifs d'automatisation. Le clavier ne peut gérer qu'un seul scénario.



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.
Pré-autorisation	Lorsque cette option est activée, l'utilisateur doit être authentifié pour utiliser le clavier : il doit saisir un code ou présenter un dispositif d'accès personnel au clavier.
Changement facile de dispositif assigné	Lorsque cette option est activée, les utilisateurs n'ont pas besoin d'appuyer sur le bouton OK après la saisie d'un code d'accès ou la lecture d'un dispositif d'accès.
Restreindre la gestion des appareils	Cette option permet à l'utilisateur de définir le moment où le contrôle du dispositif d'automatisation à l'aide du clavier doit être bloqué : • Off. • Le système est désarmé. • Le système est armé.
Passage automatique en mode secondaire	 Disponible uniquement pour le mode de fonctionnement secondaire. Cette option permet à l'utilisateur de définir le moment où le clavier commence



automatiquement à fonctionner en mode secondaire sans pression prolongée sur le bouton **OK** :

- Off.
- Le système est désarmé.
- Le système est armé.

Début de la temporisation au désarmement

Temporisation au désarmement

Sélection de la temporisation au désarmement : 5 à 255 secondes.

La temporisation au désarmement (temporisation d'activation de l'alarme) est le temps dont dispose l'utilisateur pour désarmer le site à l'aide du clavier principal.

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**.

Confirmation de l'autorisation avec un code d'accès

Lorsque cette fonction est activée, les utilisateurs ne peuvent armer ou désarmer le système que s'ils ont été autorisés avec succès à l'aide de deux formes d'identification, c'est-à-dire en utilisant les dispositifs Pass, Tag ou le smartphone et en saisissant le code d'accès approprié.

En savoir plus

Démarrage facile de la temporisation	Lorsque cette option est activée, les utilisateurs n'ont pas besoin d'appuyer sur le bouton OK après la saisie d'un code d'accès ou la lecture d'un dispositif d'accès.
Passage automatique en mode secondaire	 Disponible uniquement pour le mode de fonctionnement secondaire. Cette option permet à l'utilisateur de définir le moment où le clavier commence automatiquement à fonctionner en mode secondaire sans appuyer longuement sur le bouton OK : • Off. • Le système est désarmé. • Le système est armé.



Rétroéclairage et indication

Paramètres	Signification
Luminosité	Réglage du niveau de luminosité du rétroéclairage du clavier.
Rétroéclairage toujours actif	Lorsque cette option est activée, le rétroéclairage du clavier reste toujours actif.
Indication du Mode armé	Cette option permet à l'utilisateur de définir quand il est nécessaire d'afficher l'état de sécurité du système sur le clavier : • Jamais – pas d'indication LED de l'état de sécurité.

- **Uniquement en cas d'armement** – le logo est rouge lorsque le site est armé, partiellement armé ou en **mode Nuit**.
- **Toujours** – le logo est rouge lorsque le site est armé, vert lorsqu'il est désarmé et jaune lorsque l'armement est incomplet.



Indication sonore

Superior KeyPad Outdoor Fibra a un buzzer intégré qui, selon les paramètres, peut notifier les éléments suivants :

1. Alarmes.
2. Temporisation à l'armement / au désarmement.
3. Carillon à l'ouverture.
4. Exécution des commandes (par exemple, armement, désarmement).
5. Appui sur les touches du clavier.



Nous déconseillons l'utilisation du Superior KeyPad Outdoor Fibra 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	Signification
Paramètres des signaux sonores	Allez dans le menu Signaux sonores .
Bip lors du changement de mode de sécurité	
Armé/desarmé	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	
Temporisation au 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 Mode nuit. <u>En savoir plus</u>
Bip accéléré pour les temporisations	
Bip rapide à l'expiration de la Temporisation au désarmement	Notifie à l'utilisateur que la Temporisation au désarmement est en train de s'écouler. Vous pouvez choisir l'une des quatre options pour le démarrage du bip rapide : • Jamais • 5 dernières secondes • 10 dernières secondes • 15 dernières secondes L'option est disponible lorsque l'option Bip sur les temporisations au désarmement est activée.
Bip rapide à l'expiration de la Temporisation à l'armement	Notifie à l'utilisateur que la Temporisation à l'armement est en train de s'écouler. Vous pouvez choisir l'une des quatre options pour le démarrage du bip rapide : • Jamais • 5 dernières secondes • 10 dernières secondes • 15 dernières secondes L'option est disponible lorsque l'option Bip sur les temporisations à l'armement est activée.
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.



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

[En savoir plus](#)

Réponse du clavier aux alarmes de l'appareil

Superior KeyPad Outdoor Fibra 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 Jeweller.



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 **Paramètres** .
5. Trouvez l'option **Alerte par sirène** et sélectionnez les commandes qui l'activeront. Activez ou désactivez la fonction.
6. Répétez les étapes 3 à 5 pour les autres appareils du système.

Réponse du clavier aux alarmes anti-sabotage

Superior KeyPad Outdoor Fibra 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

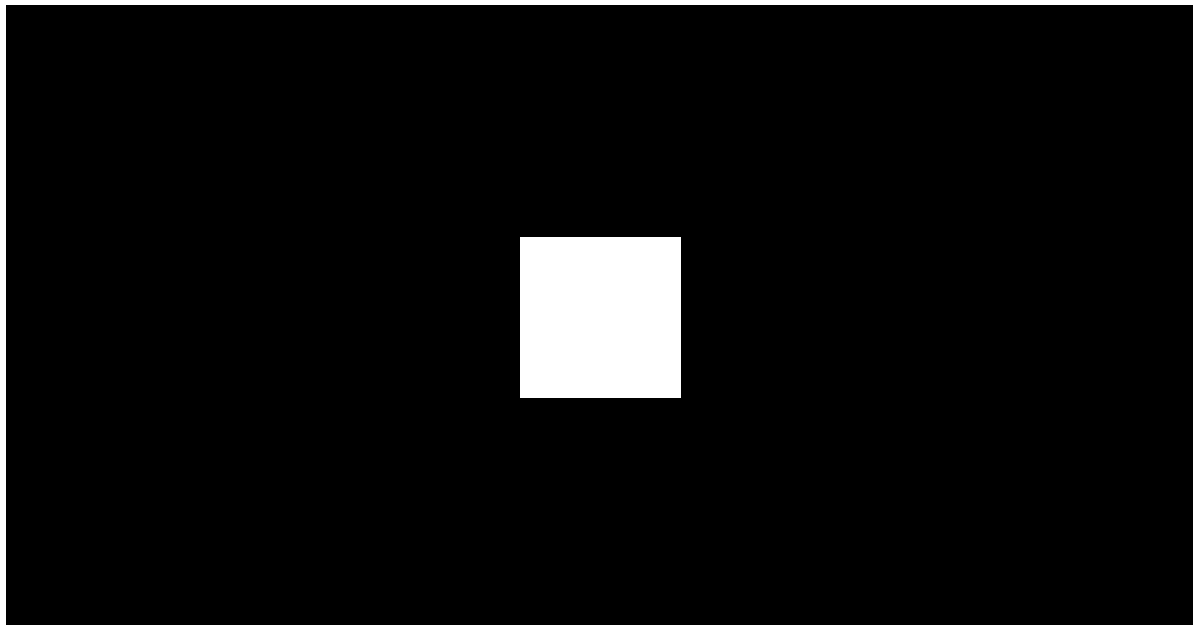
Un administrateur ou un PRO ayant le droit de configurer le système peut configurer la réponse du clavier à l'alarme lorsque le bouton de panique est enfoncé dans les applications Ajax. Pour ce faire, suivez les étapes suivantes :

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 la bascule **Si un bouton panique est appuyé dans l'app**.
7. Cliquez sur **Retour** pour enregistrer les paramètres.



Indication après-alarme du clavier



00:00

00:07

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 de Superior KeyPad Outdoor Fibra 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 de Superior KeyPad Outdoor Fibra 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 Superior KeyPad Outdoor Fibra signalera par un double clignotement de la LED, avant que le système de sécurité ne soit désarmé :

- Alarme d'intrusion/Bouton d'urgence confirmée.
- Alarme d'intrusion/Bouton d'urgence unique.
- Ouverture du couvercle.

3. Sélectionnez Superior KeyPad Outdoor Fibra requis dans le menu **Dispositifs** . Appuyez sur **Retour** pour enregistrer les paramètres.

4. Appuyez sur **Retour**. Tous les paramètres seront appliqués.

Carillon à l'ouverture

Quand la fonction **Carillon d'entrée** est activée, Superior KeyPad Outdoor Fibra 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 Superior KeyPad Outdoor Fibra 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 paramètres sont correctement définis, une icône de cloche apparaît dans l'onglet **Contrôle**  de l'application Ajax. Cliquez dessus pour activer ou désactiver le carillon à l'ouverture.

Configuration des codes



Dans les applications Ajax PRO, dans les paramètres de la centrale, vous pouvez définir les exigences relatives à la longueur des codes d'accès utilisés pour l'autorisation de l'utilisateur et l'accès au système. Vous pouvez sélectionner l'option **Flexible (4 à 6 symboles)** ou définir la longueur de code fixe : **4 symboles**, **5 symboles**, ou **6 symboles**.

La définition d'une longueur de code fixe réinitialise tous les codes d'accès précédemment configurés.

La longueur du code fixe est nécessaire pour la fonction de **Changement facile du mode de sécurité**, qui permet de désarmer le système sans appuyer sur le bouton **OK** du clavier après avoir saisi un code d'accès ou utilisé un dispositif d'accès.

Codes d'accès des claviers

Pour définir le code clavier et le code de contrainte du clavier :

1. Dans l'application Ajax, allez dans l'onglet **Dispositifs** .
2. Sélectionnez le clavier pour lequel vous souhaitez configurer un code d'accès.
3. Allez dans **Paramètres** .
4. Sélectionnez l'option **Codes des claviers uniquement** ou **Codes des claviers et de l'utilisateur** dans le menu **Options d'accès**.
5. Allez dans le menu **Codes d'accès des claviers**.
6. Définissez le code du clavier. Contient de 4 à 6 chiffres.
7. Appuyez sur **Terminé**.
8. Allez au menu **Code de contrainte**.
9. Définissez le code de contrainte du clavier. Contient de 4 à 6 chiffres.
10. Appuyez sur **Terminé**.

Code utilisateur

Pour définir un code personnel et un code de contrainte personnel :

1. Sélectionnez une centrale dans l'application Ajax.
2. Allez dans le menu **Paramètres** .
3. Ouvrez le menu **Utilisateurs**.
4. Trouvez votre compte dans la liste et cliquez dessus.
5. Allez dans **Paramètres code d'accès**.
6. Saisissez le **Code utilisateur**. Contient de 4 à 6 chiffres.
7. Appuyez sur **Enregistrer**.
8. Définissez le **Code de contrainte**. Contient de 4 à 6 chiffres.
9. Appuyez sur **Enregistrer**.
10. Cliquez sur **Retour** pour enregistrer les paramètres.



Codes des utilisateurs non enregistrés

Pour définir un code d'accès pour un utilisateur sans compte :

1. Sélectionnez la centrale dans l'application Ajax.
2. Allez dans le menu **Paramètres** .
3. Allez dans le menu **Codes d'accès des claviers**.
4. Appuyez sur **Ajouter un code**. Configurez le **Nom** et le **Code d'accès**.
Contient de 4 à 6 chiffres.
5. Cliquez sur **Ajouter** pour enregistrer les données.



Pour définir un code de contrainte pour un utilisateur sans compte :

1. Sélectionnez le menu **Codes d'accès des claviers** dans les paramètres de la centrale.
2. Sélectionnez l'utilisateur non enregistré requis.
3. Appuyez sur **Ajouter un code de contrainte**. Définissez le code.
Contient de 4 à 6 chiffres.
4. Appuyez sur **Terminé**.



Pour les utilisateurs non enregistrés, un administrateur ou un PRO ayant les droits de configurer le système peut ajuster l'accès à la gestion de la sécurité. Tout d'abord, activez le [Mode groupe](#). Ensuite, sélectionnez le menu **Codes d'accès des claviers** dans les paramètres de la centrale, trouvez l'utilisateur requis et définissez les paramètres appropriés dans le menu **Gestion de la sécurité**.

Code GIR

Seul un PRO ayant les droits de configuration du système peut créer et configurer les codes GIR dans [l'application Ajax PRO](#). Vous trouverez plus d'informations sur la configuration de cette fonctionnalité dans [cet article](#).

Cartes et télécommandes

Superior KeyPad Outdoor Fibra peut fonctionner avec les télécommandes **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 d'appareils Pass et Tag ajoutés dépend du modèle de la centrale. Les appareils Pass et Tag ajoutés n'affectent pas la limite totale d'appareils sur la centrale.

Vérifier la compatibilité des dispositifs

Ajout de Tag ou Pass

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 dispositif**.
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. Appuyez sur **Suivant**. Ensuite, la centrale passe en mode d'enregistrement des appareils.
8. Accédez à n'importe quel clavier compatible avec la **Lecture du Pass/Tag**. Appuyez sur le bouton **OK** pour faire passer le clavier en mode d'enregistrement des dispositifs d'accès.
9. Approcher le Pass ou le Tag avec le côté large contre le lecteur de clavier pendant quelques secondes. Si l'ajout est réussi, vous recevrez une notification dans l'application Ajax.



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. Pour ajouter une télécommande/carte de ce type à une nouvelle centrale, vous devrez la réinitialiser.

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.

Suppression du tag ou Pass



La réinitialisation efface tous les réglages et toutes les connexions des portecclés 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 l'espace.

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. Tapez sur **Réinitialisation du Pass/Tag**.

7. Cliquez sur **Continuer**.

8. Accédez à n'importe quel clavier compatible avec la **Lecture du Pass/Tag**. Appuyez sur le bouton **OK** pour faire passer le clavier en mode de réinitialisation du dispositif d'accès.

9. Approcher le Pass ou le Tag avec le côté large contre le lecteur de clavier pendant quelques secondes. Si le formatage est réussi, vous recevrez une notification dans l'application Ajax. Si le formatage échoue, réessayez.

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

Superior KeyPad Outdoor Fibra 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 du Ajax Security System.

Pour activer l'authentification Bluetooth dans l'application

1. Ajouter Superior KeyPad Outdoor Fibra au système.

2. Activez le capteur Bluetooth du clavier :

- **Dispositifs**  → **Superior KeyPad Outdoor Fibra** → **Paramètres**  → Activer 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 Superior KeyPad Outdoor Fibra 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 :

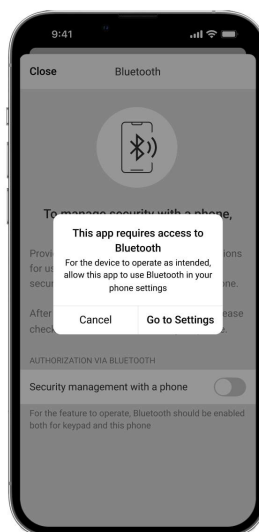
1. Dans l'onglet **Dispositifs** , sélectionnez la centrale et accédez à ses paramètres .
2. Ouvrez le menu **Utilisateurs** et sélectionnez l'utilisateur souhaité dans la liste.
3. Dans la section **Autorisations**, désactivez la bascule **Gestion de la sécurité via Bluetooth**.

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 Superior KeyPad Outdoor Fibra. 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.



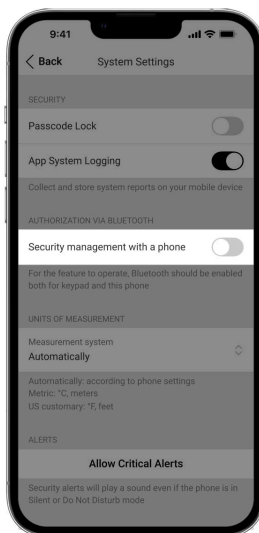


Autorisez l'application à trouver des appareils à proximité et à s'y connecter. La fenêtre contextuelle pour les smartphones Android et iOS peut être différente.

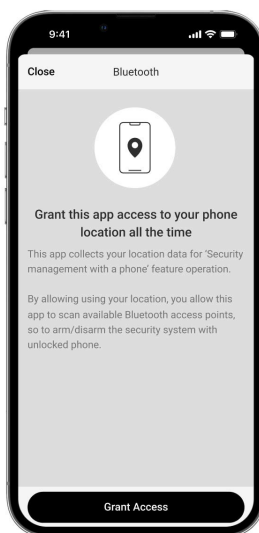


De plus, la **Gestion de la sécurité avec un smartphone** peut être activée dans les paramètres de l'application :

- 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 Superior KeyPad Outdoor Fibra si le **Géorepérage** est désactivé et que l'application n'est pas autorisée à utiliser l'emplacement du smartphone. Appuyer sur le symbole ⓘ ouvre la fenêtre avec des explications sur ce qu'il faut faire.



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.

4. Activez l'option **Maintenir l'application active pour gérer la sécurité via Bluetooth**. Pour cela, allez dans **Dispositifs**  → **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**.

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.

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.



Superior KeyPad Outdoor Fibra 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 Superior KeyPad Outdoor Fibra dans l'application Ajax.

La séquence d'étapes pour modifier le mode de sécurité à l'aide du clavier dépend de l'activation ou non des options **Pré-autorisation**, **Confirmation de l'autorisation avec un code d'accès** et **Changement facile du mode armé** dans les paramètres de Superior KeyPad Outdoor Fibra.

Utilisation de Tag, Pass, ou d'un smartphone



1. Approcher un Tag, un Pass ou un smartphone du clavier.
2. Saisissez le code requis si la fonction **Confirmation de l'autorisation avec un code d'accès** est activée.
3. Appuyez sur le bouton **OK** du clavier pour modifier le mode armé.

Si l'option **Changement facile de mode armé** est activée, il n'est pas nécessaire d'appuyer sur le bouton **OK** après la lecture du dispositif d'accès.

Utilisation de codes d'accès



Les codes introduits de manière incorrecte peuvent être effacés par une pression longue sur le bouton **si aucune autre action n'est programmée pour une pression longue**.

Code	Exemple	Remarque
Gestion des modes armés du site		
Code clavier		
Code de contrainte du clavier	1234 → OK	



Code utilisateur		
Code de contrainte de l'utilisateur	5 → * → 1234 → OK	5 est un identifiant d'utilisateur
Code de l'utilisateur non enregistré		
Code de contrainte de l'utilisateur non enregistré	1234 → OK	
Code GIR	1234 → OK	
Gestion des modes armés du groupe		
Code clavier		
Code de contrainte du clavier	1234 → * → 2 → OK	2 est un identifiant de groupe
Code utilisateur		5 est un identifiant d'utilisateur
Code de contrainte de l'utilisateur	5 → * → 1234 → * → 2 → OK	2 est un identifiant de groupe
Code de l'utilisateur non enregistré		
Code de contrainte de l'utilisateur non enregistré	1234 → * → 2 → OK	2 est un identifiant de groupe
Code GIR	1234 → * → 2 → OK	2 est un identifiant de groupe

[En savoir plus sur l'ID de l'utilisateur](#)

[En savoir plus sur l'ID des groupes](#)

Confirmation de l'autorisation avec un code d'accès

Confirmation de l'autorisation avec un code d'accès est une fonctionnalité qui permet de mettre en place une authentification à deux facteurs pour les utilisateurs lorsqu'ils contrôlent les modes de sécurité du système. Cela signifie que les utilisateurs doivent d'abord utiliser un dispositif d'accès (Pass, Tag ou smartphone), puis saisir un code d'accès pour confirmer leur autorisation d'accès au système.



[En savoir plus sur la confirmation de l'autorisation avec un code d'accès](#)

Gestion des dispositifs d'automatisation et des scénarios



Assurez-vous que la fonction **Gérer les dispositifs d'automatisation** est configurée pour le mode de fonctionnement principal ou secondaire dans les paramètres du clavier des applications Ajax.

Pour contrôler le dispositif d'automatisation ou le scénario avec Superior KeyPad Outdoor Fibra :

1. Approcher un dispositif de contrôle d'accès du clavier ou saisir un code d'autorisation sur le clavier.
2. Passer le clavier en mode **Gérer les dispositifs d'automatisation** par un appui long sur le bouton **OK** si ce mode n'est pas actif ou défini comme mode de fonctionnement principal. Le bouton **OK** doit s'allumer en vert ou en rouge selon l'état actuel du dispositif d'automatisation.
3. Appuyez sur le bouton **OK** pour modifier l'état du dispositif d'automatisation ou exécuter un scénario :
 - Si le clavier gère un scénario de **changement d'état**, l'indication de la LED du bouton **OK** doit changer pour correspondre à l'état du dispositif d'automatisation.

- Si le clavier gère un scénario **sur action prédéfinie**, l'indication de la LED du bouton **OK** ne montre pas l'état des dispositifs. Il indique plutôt si l'action est terminée ou non.

La séquence d'étapes pour la gestion des appareils d'automatisation avec le clavier dépend de l'activation ou non des options **Pré-autorisation** et **Changement facile de dispositif assigné** dans les paramètres de Superior KeyPad Outdoor Fibra.



Indication

Superior KeyPad Outdoor Fibra 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 :

- Logo Ajax, bouton **OK** et rétroéclairage avec indication LED ;
- le buzzer intégré.

Événement	LED	Buzzer
Appui court sur un bouton		Bip court
Le dispositif est activé lorsqu'il n'est pas ajouté à la centrale	Le logo s'allume en rouge pendant 0,3 s et s'éteint pendant 0,3 s à trois reprises.	
Pour être ajouté à la centrale, le dispositif est sélectionné dans la liste des dispositifs trouvés en scannant les lignes Fibra	Le logo clignote rapidement en vert.	
Le dispositif est supprimé de la centrale	Le logo s'allume en rouge pendant 0,3 s et s'éteint pendant 0,3 s six fois.	
Le clavier est en mode Changement du mode de sécurité*	Le logo est vert ou rouge en fonction de l'état actuel de la sécurité.	

Le clavier est en mode Gérer les dispositifs d'automatisation	Le bouton OK est vert ou rouge en fonction de l'état actuel du dispositif d'automatisation. Le logo est éteint.	
Le clavier est en mode Début de la temporisation au désarmement*	Le logo est rouge lorsque le site est armé. Le logo clignote en rouge en même temps qu'un signal sonore lors de la temporisation au désarmement.	
Armement ou activation du Mode nuit	Le logo passe du vert au rouge.	Bip pendant environ 0,2 s.
Désarmement	Le logo passe du rouge au vert.	Double bip pendant environ 0,4 s.
Appui sur la touche Panique (✱)		Bip long pendant environ 0,5 s.
Appuyez sur la touche de fonction (✱) et maintenez-la enfoncée pour effacer le code saisi	Le rétroéclairage clignote en même temps qu'un bref signal sonore.	Bip court.
Un code erroné a été saisi	Le rétroéclairage s'allume trois fois pendant un long bip.	Bip long pendant environ 0,6 s.
La demande est refusée en raison d'un manque d'autorisations de l'utilisateur ou d'un dysfonctionnement	Le logo s'allume en jaune trois fois pendant un long bip.	Bip long pendant environ 0,6 s.
Le clavier est verrouillé	Le rétroéclairage s'allume trois fois pendant un long bip.	Bip long pendant environ 0,6 s.
Échec de la vérification de l'intégrité du système	Le logo s'allume en vert ou en rouge (selon l'état actuel de la sécurité) trois fois pendant un long bip.	Bip long pendant environ 0,6 s.
Le changement d'état de la sécurité du système est interdit	Le logo s'allume en jaune trois fois pendant un long bip.	Bip long pendant environ 0,6 s.





Alarme anti-sabotage/restauration	Le logo s'allume en rouge pendant 0,7 s.	
La lecture du Pass/Tag est réussie	Le rétroéclairage s'éteint pendant environ 0,3 s.	Bip pendant environ 0,2 s.
La lecture du Pass/Tag a échoué	Le logo s'allume en jaune et le rétroéclairage s'éteint pendant un bip.	Bip long pendant environ 1 s.
La lecture sur smartphone est un succès	Le rétroéclairage s'éteint pendant environ 0,1 s.	Bips fréquents pendant environ 0,2 s.
La lecture sur smartphone a échoué	Le logo s'allume en jaune pendant un bip.	Bip long pendant environ 1 s.
Le clavier attend de lire Pass/Tag	Le rétroéclairage s'allume pendant 0,2 s et s'éteint pendant 1 s jusqu'à ce que Pass/Tag soit lu.	
L'ajout de Pass/Tag a été effectué avec succès		Deux bips courts.
1. L'ajout de Pass/Tag a échoué. 2. Une carte non valide est lue. 3. D'autres dysfonctionnements se sont produits lors de la lecture d'un dispositif d'accès.	Le logo s'allume en jaune pendant environ 0,3 s.	Bip long pendant environ 0,6 s.
Temporisation à l'armement / au désarmement	Le logo s'allume en rouge en même temps que le signal sonore du délai d'entrée. Le logo s'allume en vert en même temps que le signal sonore du délai de sortie.	Bip court une fois par 1 s.
Une récupération du système est nécessaire (PD 6662:2017)	Le logo s'allume en jaune pendant environ 0,1 s, puis un bref signal sonore retentit. Elle est répétée trois fois.	
Indication après alarme	Le logo clignote en rouge deux fois toutes les 3,4 s.	

Armement incomplet (PD 6662:2017)	Le logo s'allume en jaune de façon continue.	Trois bips courts d'environ 0,3 s toutes les 1 s.
Un appareil du système est hors ligne (UL)	Le logo clignote deux fois en jaune simultanément avec un bip court deux fois toutes les minutes.	
La batterie d'un appareil du système est faible (UL)	Le logo clignote trois fois en jaune, accompagné d'un bref signal sonore avec changement de tonalité toutes les minutes.	
Armement temporisé (initié par le dispositif) (PD 6662:2017)	Le logo s'allume en vert pendant environ 0,8 s à toutes les secondes.	
Armement temporisé (initié par l'application) (PD 6662:2017)	Le logo s'allume en rouge pendant environ 0,8 seconde à toutes les secondes.	
La centrale ne répond pas	Le logo s'allume en jaune pendant un long bip.	Bip long pendant environ 0.5 s.

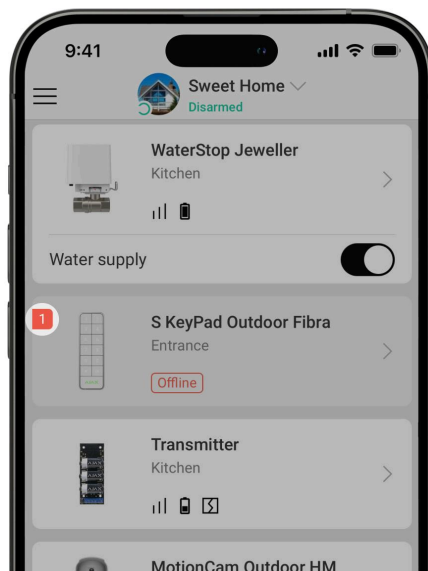


** Lorsque l'indication est activée dans les paramètres du clavier.*

Dysfonctionnements

Lorsque le détecteur détecte un dysfonctionnement (par exemple, il n'y a pas de communication via le protocole Fibra), un compteur de dysfonctionnement s'affiche dans l'application Ajax dans le coin supérieur gauche de l'icône du dispositif.

Tous les dysfonctionnements sont visibles dans les états du dispositif. Les champs présentant des dysfonctionnements seront mis en évidence en rouge.



Un dysfonctionnement est affiché si :

- La température du dispositif dépasse les limites admissibles.
- Le couvercle du dispositif est ouvert (le bouton anti-sabotage s'est déclenché).
- Il n'y a pas de signal via le protocole Fibra.

Maintenance

Vérifiez régulièrement le fonctionnement du dispositif. 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.

Caractéristiques techniques

[Toutes les spécifications techniques](#)

Garantie

La garantie des produits de la société à responsabilité limitée «Ajax Systems Manufacturing» est valable 2 ans après l'achat.

Si le dispositif ne fonctionne pas correctement, nous vous recommandons de contacter d'abord le service d'assistance, car dans la plupart des cas, les problèmes techniques peuvent être résolus à distance.

Obligations de garantie

Contrat de l'utilisateur

Contacter l'assistance technique :

- email
- Telegram

Fabriqué par « AS Manufacturing » LLC





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

S'abonner