

Manuel utilisateur Hub Hybrid

Bientôt : Superior Hub Hybrid (2G) / (4G)

Mis à jour January 2, 2025



Hub Hybrid est un panneau de contrôle hybride du système de sécurité Ajax. Compatible avec des dispositifs filaires et sans fil. Contrôle le fonctionnement des dispositifs connectés, interagit avec l'utilisateur et avec l'entreprise de sécurité. Conçu pour une installation à l'intérieur.

La centrale Hub Hybrid nécessite un accès à Internet pour la connexion au service Ajax Cloud. Réseaux de communication disponibles : Ethernet et deux cartes SIM. La centrale est disponible en deux versions : avec modem 2G et 2G/3G/4G (LTE).

La carte imprimée Hub Hybrid est vendue avec son boîtier, mais vous pouvez installer la carte sans boîtier dans le **Case D (430)** en utilisant le Module Holder (type B). Le boîtier Case et les supports sont vendus séparément.



L'installation de la centrale dans Case D (430) ne répond pas aux exigences du Grade (EN 50131). La version conforme sera bientôt disponible.

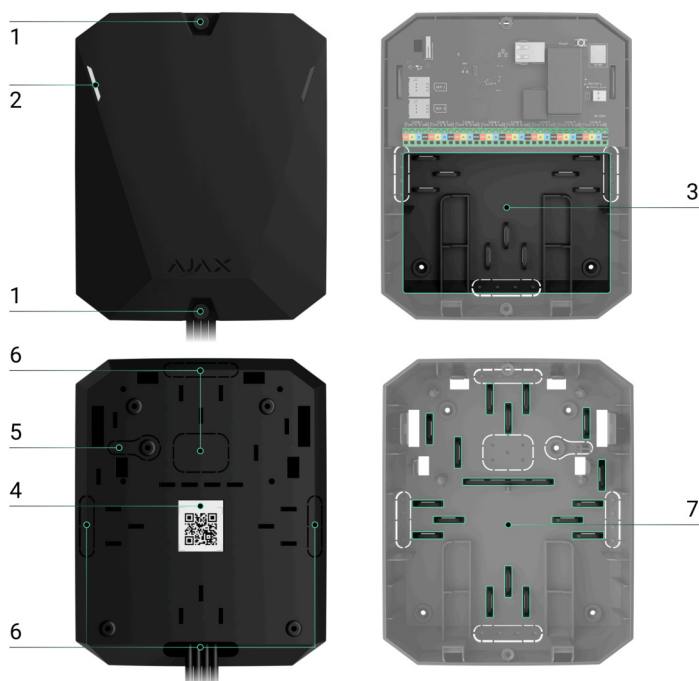
[Acheter Hub Hybride](#)

[Acheter Case D \(430\)](#)



Éléments fonctionnels

Éléments du boîtier



1. Vis qui fixent le couvercle du boîtier. Dévisser à l'aide d'une clé hexagonale fournie (Ø 4 mm).
2. Guides de lumière pour l'indication de l'état de la centrale (disponible dans la nouvelle version du boîtier ; dans la version précédente, l'indicateur LED est situé sur la carte imprimée).
3. Une section avec des supports pour une batterie de secours.

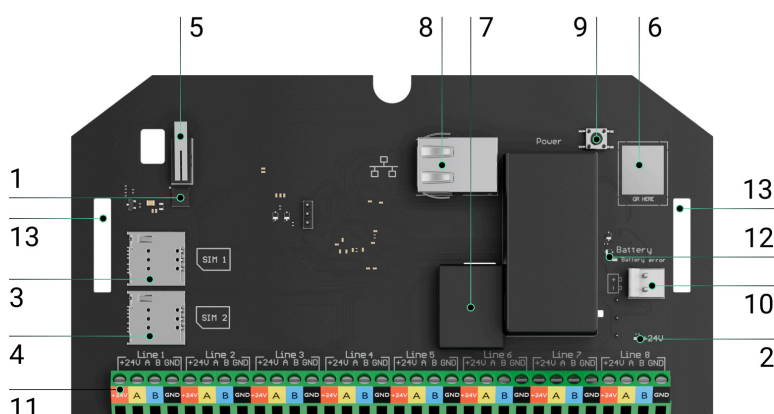


Batterie non incluse.

4. Code QR et ID (numéro de série) du panneau de contrôle.
5. Partie perforée du boîtier. Nécessaire pour le déclenchement du bouton anti-sabotage en cas de tentative de détacher le dispositif de la surface. Ne la cassez pas.
6. Parties perforées du boîtier pour la sortie des fils des détecteurs et dispositifs connectés.
7. Attaches de câbles.



Éléments de la carte imprimée

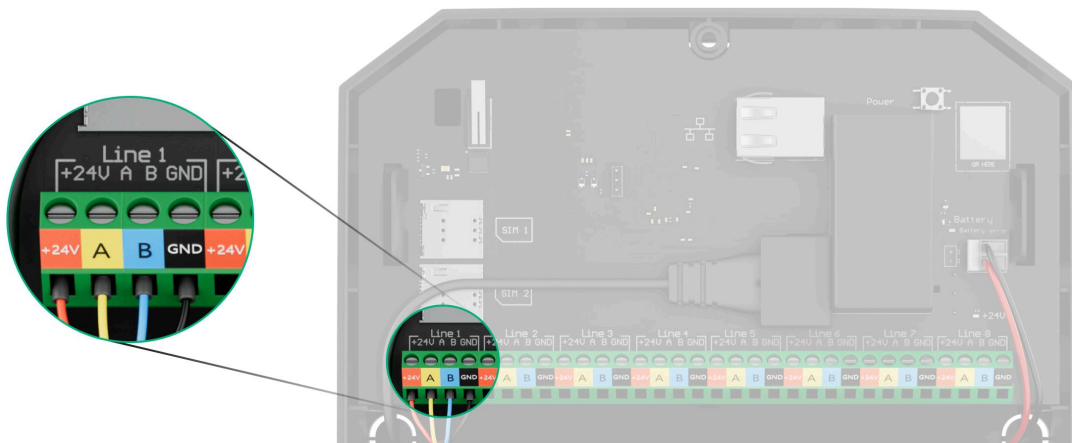


1. Indicateur d'état à LED de la centrale et des réseaux de communication connectés.
2. Indicateur d'état à LED des dispositifs connectés à la ligne Fibra de la centrale.
3. Emplacement pour micro SIM 1.
4. Emplacement pour micro SIM 2.
5. Bouton anti-sabotage. Détecte le retrait du couvercle du Hub Hybrid (2G) / (4G).
6. Code QR et ID (numéro de série) du dispositif.

7. Prise pour câble d'alimentation.
8. Connecteur de câble Ethernet.
9. Bouton d'alimentation.
10. Bornes pour le raccordement d'une batterie de secours de 12 V.
11. Terminaux de lignes Fibra pour la connexion de dispositifs câblés.
12. Indicateur **d'erreur de batterie**. S'allume en cas d'inversion de polarité lors de la connexion de la batterie (lorsque le "-" de la batterie est connecté à la borne "+" et vice versa).
13. Points de fixation pour attacher la carte Hub Hybrid dans le Case D (430) avec le Module Holder (type B) ou dans le boîtier de la centrale.



Terminaux de lignes Fibra



Hub Hybride (2G) / (4G) possède 8 lignes Fibra. Les numéros de 1 à 8 sont indiqués sur la carte imprimée de la centrale.

Terminaux de lignes Fibra :

- **+24 V** – borne d'alimentation de 24 V $\equiv$.
- **A** – première borne de signal.
- **B** – deuxième borne de signal.

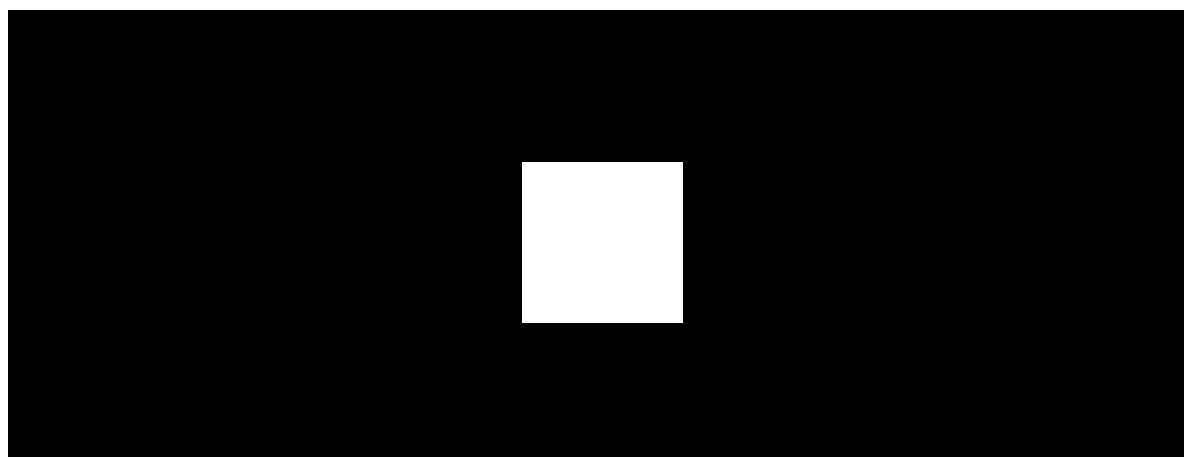
- **GND** – borne de mise à la terre de l'alimentation.



Respectez la polarité et l'ordre de connexion des fils lors de l'installation des dispositifs Fibra.



Principe de fonctionnement



00:00

00:12

Hub Hybrid est un panneau de contrôle hybride du système de sécurité Ajax. Il contrôle le fonctionnement des dispositifs connectés.

Vous pouvez connecter jusqu'à 100 dispositifs Ajax filaires et sans fil au Hub Hybrid. Les dispositifs connectés protègent contre les intrusions, les incendies et les inondations, et permettent également de contrôler les dispositifs électriques en fonction de scénarios ou manuellement – à l'aide d'une application mobile ou en appuyant sur le bouton de panique, le LightSwitch ou le clavier à écran tactile.

Pour surveiller le fonctionnement de tous les dispositifs du système de sécurité, la centrale communique avec les dispositifs connectés à l'aide de trois protocoles sécurisés :

1. **Jeweller** est un protocole radio permettant de transmettre des événements et des alarmes à partir de dispositifs sans fil Ajax. La portée de communication peut atteindre 2 000 m sans obstacles : murs, portes ou ossature du bâtiment.

En savoir plus sur Jeweller

2. **Wings** est un protocole radio permettant de transmettre les photos provenant des détecteurs MotionCam et MotionCam Outdoor. La portée de communication peut atteindre 1 700 m sans obstacles : murs, portes ou ossature du bâtiment.



En savoir plus sur Wing

3. **Fibra** est un protocole filaire pour la transmission d'événements et d'alarmes provenant de dispositifs filaires Ajax. La portée de communication peut atteindre 2 000 m en cas de connexion par paire torsadée U/UTP cat.5.

En savoir plus sur Fibra

Si un détecteur est déclenché, le système déclenche une alarme en moins d'une seconde, quel que soit le protocole de communication. En cas d'alarme, la centrale active les sirènes, déclenche les scénarios et avertit le centre de télésurveillance et tous les utilisateurs.

Protection contre le sabotage

Le Hub Hybrid dispose de 3 réseaux de communication pour se connecter au serveur Ajax Cloud : Ethernet et deux cartes SIM. Cela vous permet de connecter le dispositif à trois fournisseurs de services de communication différents en même temps. Si l'un des réseaux de communication est indisponible, la centrale bascule automatiquement sur un autre et en informe le centre de télésurveillance et les utilisateurs du système.

Lorsqu'une tentative de brouillage est détectée, le système passe sur une fréquence radio libre et envoie des notifications au centre de télésurveillance et aux utilisateurs du système.

Que signifie le brouillage des systèmes de sécurité

La centrale vérifie régulièrement la qualité de la communication avec tous les dispositifs connectés. Si un dispositif perd la connexion avec la centrale, tous les utilisateurs du système (en fonction des paramètres), ainsi que le centre de télésurveillance, recevront une notification de l'incident à l'expiration du délai spécifié par l'administrateur.



En savoir plus

Personne ne peut éteindre la centrale sans se faire remarquer, même lorsque le site est désarmé. Si un intrus tente d'ouvrir le boîtier de la centrale, le bouton anti-sabotage se déclenche immédiatement. La notification d'alarme sera envoyée au centre de télésurveillance et aux utilisateurs du système.

Lorsque la carte imprimée Hub Hybrid est installée dans le boîtier **Case D (430)**, l'application affiche que le couvercle de la centrale est ouvert. L'installation de la centrale dans Case D (430) ne répond pas aux exigences du Grade (EN 50131). La version conforme sera bientôt disponible.

Qu'est-ce qu'un bouton anti-sabotage

La centrale vérifie la connexion à Ajax Cloud à intervalles réguliers. La période d'interrogation peut être réglée dans les paramètres de la centrale. Si une période minimale de ping est définie, le serveur peut avertir les utilisateurs et l'entreprise de sécurité en 60 secondes seulement après la perte de la connexion.

En savoir plus

La batterie de secours de 7 A·h peut être connectée à la centrale, ce qui peut fournir à un système composé de 30 détecteurs une alimentation de secours pendant 60 heures.



Utilisez des batteries de 12 V $\overline{=}$ d'une capacité de 4, 7 ou 9 A·h. Le boîtier de la centrale et le Case D (430) comportent des supports spéciaux pour les batteries.

Vous pouvez utiliser des batteries de capacité différente, adaptées à la taille de la centrale et dont le temps de charge complet ne dépasse pas 40 heures. Le courant maximal de charge de la batterie à partir du Hub Hybrid est de 300 mA. Les dimensions maximales de la batterie à installer dans le boîtier Hub Hybrid sont de 151 × 65 × 94 mm, et son poids est de 5 kg.

En savoir plus

OS Malevich

Hub Hybrid est géré par le système d'exploitation en temps réel OS Malevich. Il est protégé contre les virus et les cyberattaques.

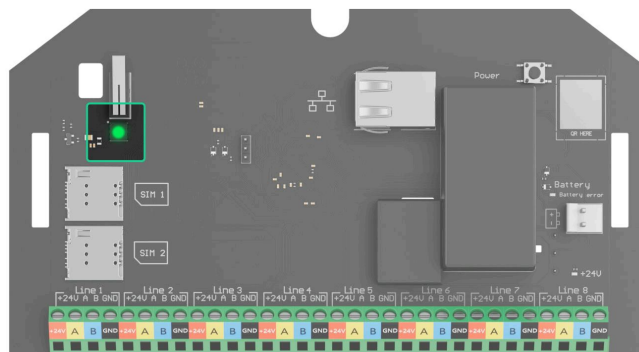
OS Malevich apporte de nouvelles possibilités et fonctionnalités au système de sécurité Ajax par le biais de mises à jour over-the-air. La mise à jour ne nécessite pas l'intervention d'un utilisateur ou d'un ingénieur d'installation.

La mise à jour prend jusqu'à 2 minutes lorsque le système de sécurité est désarmé et que l'alimentation externe et la batterie de secours sont connectées.

Indication

La centrale a deux modes d'indication par LED :

- **Connexion entre la centrale et le serveur.**
- **Alertes et dysfonctionnements.**



Connexion entre la centrale et le serveur

Le mode de connexion entre la centrale et le serveur est activé par défaut. En fonction de son état de communication avec le serveur Ajax Cloud, l'indicateur LED du Hub Hybrid peut s'allumer en rouge, blanc, violet, jaune, bleu ou vert.



Dans la version précédente du boîtier du Hub Hybrid et lorsque la carte est installée dans le boîtier Case D (430), l'indicateur LED n'est pas visible lorsque le couvercle du boîtier est fermé. L'indicateur n'est utile que pendant la connexion et la configuration de la centrale. Dans la nouvelle version, le boîtier du Hub Hybrid comporte des guides de lumière, permettant de visualiser l'état de la centrale à tout moment.

Les états du Hub Hybrid peuvent également être contrôlés dans les applications Ajax.





Indication	Événement	Remarque
S'allume en blanc.	Au moins deux réseaux de communication sont connectés : Ethernet et une ou deux cartes SIM.	En cas de fonctionnement sur une batterie de secours uniquement, l'indicateur clignote toutes les 10 secondes.
S'allume en vert.	Un réseau de communication est connecté : Ethernet ou une/deux cartes SIM. <u>En savoir plus</u>	
S'allume en rouge.	La centrale n'a aucune connexion à l'Internet ou au service Ajax Cloud.	En cas de fonctionnement sur une batterie de secours uniquement, l'indicateur clignote toutes les 10 secondes.
L'alimentation externe est déconnectée (si une batterie de secours est connectée).	S'allume pendant 3 minutes, puis clignote toutes les 10 secondes.	La couleur de l'indication dépend du nombre de réseaux de communication connectés.



Si, lors de l'utilisation du système, vous constatez une indication qui ne figure pas dans ce manuel d'utilisation, veuillez contacter le [service d'assistance Ajax](#).

Accès aux indications

Les utilisateurs du Hub Hybrid peuvent consulter l'indication des Alertes et dysfonctionnements après avoir :

- armé/désarmé le système à l'aide du clavier Ajax ;
- saisi l'ID utilisateur ou le code personnel correct sur le clavier, puis effectué une action qui a déjà été réalisée (par exemple, l'utilisateur a

désarmé le système et a appuyé sur la touche de désarmement du clavier) ;

- appuyé sur le bouton du SpaceControl pour armer/désarmer le système ou activé **Mode nuit** ;
- armé/désarmé le système dans l'application Ajax.



Tous les utilisateurs peuvent voir l'indication sur le **Changement de l'état de la centrale**.

Alertes et dysfonctionnements

La fonction peut être activée dans les paramètres de la centrale dans l'application PRO (Centrale → Paramètres → Services → Indication LED).



L'indication est disponible pour les centrales avec le firmware OS Malevich 2.14 et plus et dans les applications de ces versions et plus :

- Ajax PRO: Tool for Engineers 2.22.2 pour iOS.
- Ajax PRO: Tool for Engineers 2.25.2 pour Android.
- Ajax PRO Desktop 3.5.2 pour macOS.
- Ajax PRO Desktop 3.5.2 pour Windows.

Indication	Événement	Remarque
Changement de l'état de la centrale		
La LED blanche clignote une fois par seconde.	Armement en deux étapes ou Temporisation à l'armement .	Un des dispositifs est en cours d'exécution de l' Armement en deux étapes ou de la Temporisation à l'armement .



La LED verte clignote une fois par seconde.	Indication d'entrée.	Un des dispositifs est en cours d'exécution de la Temporisation au désarmement .
La LED blanche s'allume pendant 2 secondes.	L'armement est terminé.	La centrale (ou l'un des groupes) passe de l'état désarmé à l'état armé.
La LED verte s'allume pendant 2 secondes.	Le désarmement est terminé.	La centrale (ou l'un des groupes) passe de l'état armé à l'état désarmé.
Alertes et dysfonctionnements		
Les LED rouge et violette clignotent successivement pendant 5 secondes.	Alarme d'urgence confirmée.	Après une alarme d'urgence, le système n'a pas été restauré.  L'indication n'est affichée que si la Restauration après Alarme du bouton d'urgence confirmée est activée dans les paramètres.
La LED rouge clignote pendant 5 secondes.	Alarme d'urgence unique.	Après une alarme d'urgence, le système n'a pas été restauré.  L'indication n'est pas affichée si l'alarme d'urgence est confirmée.

		 L'indication n'est affichée que si la Restauration après Alarme du bouton d'urgence unique est activée dans les paramètres.
La LED rouge clignote.	Le nombre de clignotements correspond au numéro d'appareil (de dispositif d'urgence DoubleButton), qui est le premier à déclencher l'alarme d'urgence.	Après une alarme d'urgence confirmée ou non confirmée, le système n'a pas été restauré : • Alarme du bouton d'urgence unique or • Alarme du bouton d'urgence confirmée
Les LED jaune et violette clignotent successivement pendant 5 secondes.	Alarme d'intrusion confirmée.	Après une alarme d'intrusion, le système n'a pas été restauré.  L'indication n'est affichée que si la Restauration après Alarme d'intrusion confirmée est activée dans les paramètres.
La LED jaune clignote pendant 5 secondes.	Alarme d'intrusion unique.	Après une alarme d'intrusion, le système n'a pas été restauré.



		 L'indication n'est pas affichée si une alarme d'intrusion est confirmée.  L'indication n'est affichée que si la Restauration après Alarme d'intrusion unique est activée dans les paramètres.
La LED jaune clignote	Le nombre de clignotements correspond au numéro d'appareil, qui est le premier à déclencher l'alarme d'intrusion.	Après une alarme d'intrusion confirmée ou non confirmée, le système n'a pas été restauré : • Alarme d'intrusion unique or • Alarme d'intrusion confirmée
Les LED rouge et bleue clignotent successivement pendant 5 secondes.	Ouverture du couvercle.	Le système n'a pas été restauré après un déclenchement du bouton anti-sabotage ou une ouverture du couvercle sur l'un des dispositifs ou sur la centrale.  L'indication n'est affichée que si la





		Restauration après Ouverture du couvercle est activée dans les paramètres.
Les LED jaune et bleue clignotent successivement pendant 5 secondes.	Autres dysfonctionnements.	Le système n'a pas été restauré après un dysfonctionnement ou une erreur de fonctionnement d'un dispositif ou de la centrale. L'indication n'est affichée que si la Restauration après Autres dysfonctionnements est activée dans les paramètres. Actuellement, Restauration après Autres dysfonctionnements n'est pas disponible dans les applications Ajax.
La LED bleue foncée clignote pendant 5 secondes.	Désactivation forcée.	L'un des dispositifs est désactivé ou les notifications d'état du couvercle sont désactivées.
La LED bleue clignote pendant 5 secondes.	Désactivation automatique.	L'un des dispositifs est automatiquement désactivé par une minuterie d'ouverture ou par le nombre de détections.

Les LED verte et bleue clignotent successivement.	Expiration de la minuterie de confirmation d'intrusion. <u>En savoir plus sur la fonction de Confirmation d'alarme</u>	S'affiche à l'expiration de la minuterie de confirmation d'intrusion (pour confirmer l'alarme).
---	--	---



Lorsque rien ne se passe dans le système (pas d'alarmes, de dysfonctionnements, d'ouvertures de couvercles, etc.), la LED est soit blanche, soit verte, ce qui représente les états suivants de la centrale :

- Armé / Partiellement armé ou **Mode nuit** activé : la LED s'allume en blanc.
- Désarmé : la LED s'allume en vert.



Dans les centrales avec le firmware **OS Malevich 2.15.2** et plus, la LED s'allume en vert lorsqu'elle est réglée sur Armé / Partiellement armé ou **Mode nuit**.

Indication d'alerte

Si le système est désarmé et que l'une des indications du tableau est présente, la LED jaune clignote une fois par seconde.



Si le système présente plusieurs événements, les indications sont affichées une par une, dans l'ordre indiqué dans le tableau.

Compte Ajax

Pour mettre en place le système, installez la version PRO de l'application et créez un compte si vous n'en avez pas. Ne créez pas un nouveau compte pour chaque centrale, car un seul compte peut gérer plusieurs

systèmes de sécurité. Si nécessaire, vous pouvez configurer des droits d'accès individuels pour chaque centrale.

Comment enregistrer un compte PRO

Les paramètres de l'utilisateur, les systèmes et les paramètres des dispositifs connectés sont stockés dans la centrale. La modification de l'administrateur de la centrale, l'ajout ou la suppression d'utilisateurs ne réinitialise pas les paramètres des dispositifs connectés à la centrale.



Le **Hub Hybrid** ne peut être ajouté et configuré que dans les applications Ajax PRO.

Connecter la centrale à Ajax Cloud

Le Hub Hybrid a besoin d'un accès Internet pour se connecter au serveur Ajax Cloud. La connexion est nécessaire pour le fonctionnement des applications Ajax, la configuration et la gestion à distance du système, ainsi que pour l'envoi de notifications push aux utilisateurs.

Le Hub Hybrid est connecté à Internet via Ethernet et deux cartes SIM. Connectez tous les réseaux de communication pour obtenir une plus grande fiabilité et disponibilité du système.

Pour connecter la centrale à Ajax Cloud :

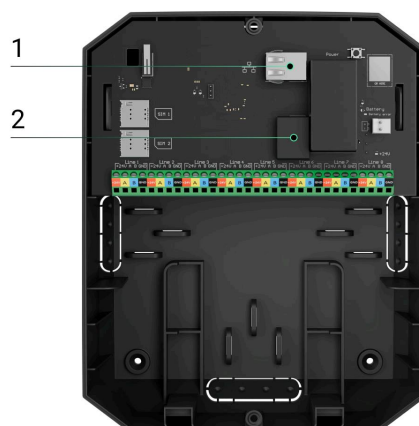
1. Dévissez les vis de fixation du boîtier, si elles sont présentes. Dévisser avec une clé hexagonale de Ø 4 mm. Cette clé hexagonale est incluse dans le kit du panneau de contrôle.



2. Retirez le couvercle du boîtier de la centrale.



3. Installez la carte Hub Hybrid dans le Case D (430) en utilisant le Module Holder (type B) si nécessaire.
4. Branchez les câbles d'alimentation et Ethernet sur les connecteurs appropriés :



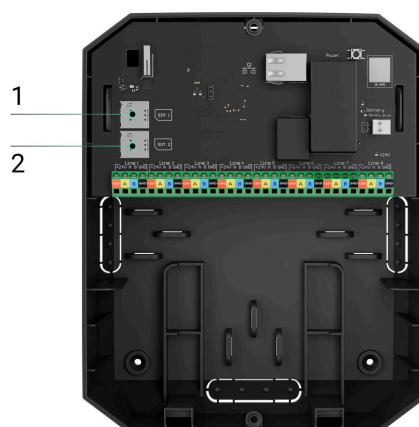
- 1 – Connecteur du câble Ethernet.
- 2 – Connecteur du câble d'alimentation.



Pour se conformer aux exigences de la norme INCERT, utilisez l'adaptateur de bornier à vis pour connecter l'alimentation externe. [En savoir plus.](#)



5. Installez les cartes SIM :



- 1 – premier emplacement micro-SIM.
- 2 – deuxième emplacement micro-SIM.

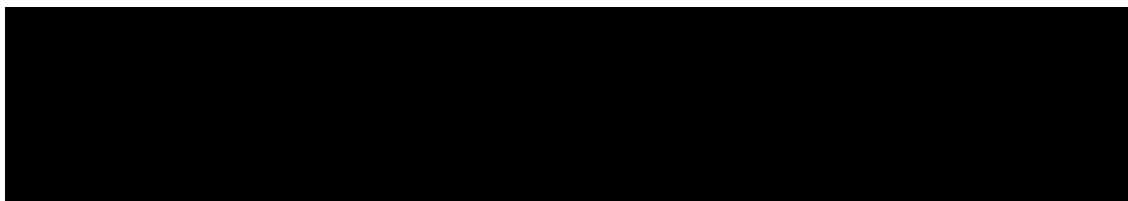
6. Connectez une batterie de secours de 12 V $\equiv$ d'une capacité de 4, 7 ou 9 A·h. Le boîtier de la centrale et le boîtier Case D (430) sont conçus pour être utilisés avec ce type de batterie.
7. Maintenez le bouton d'alimentation de la centrale enfoncé. Dès que la centrale est sous tension, les LED de la ligne Fibra sur la carte de la centrale s'allument.
8. Attendez que la centrale soit connectée à Internet. La couleur verte ou blanche de la LED indique que la centrale est prête à fonctionner.



00:00

00:13

En



Si la connexion Ethernet n'est pas établie, désactivez le proxy et le filtrage des adresses MAC et activez le DHCP dans les paramètres du routeur. La centrale recevra automatiquement une adresse IP. Après cela, vous pouvez attribuer une adresse IP statique à la centrale dans l'application Ajax.

Si la connexion SIM échoue

Pour vous connecter au réseau cellulaire, vous devez installer une carte micro-SIM avec une demande de code PIN désactivée et un montant suffisant sur le compte pour payer les services selon le tarif de l'opérateur. Pour désactiver la demande de code PIN, insérez la carte SIM dans le téléphone.

Si la centrale ne parvient pas à se connecter au réseau cellulaire, utilisez Ethernet pour configurer les paramètres du réseau : itinérance, point d'accès APN, nom d'utilisateur et mot de passe. Pour connaître ces paramètres, contactez le service d'assistance de votre opérateur mobile.

[Comment définir ou modifier les paramètres APN dans la centrale](#)

Ajout de la centrale à la version PRO de l'application



Le **Hub Hybrid** ne peut être ajouté et configuré que dans les applications Ajax PRO.

Après avoir ajouté une centrale à votre compte, vous devenez l'administrateur du dispositif. Les administrateurs peuvent inviter d'autres utilisateurs dans le système et déterminer leurs droits. Vous pouvez connecter jusqu'à 50 utilisateurs au Hub Hybrid.

Chaque compte PRO connecté à la centrale, ainsi que le profil de l'entreprise de sécurité est considéré comme un utilisateur du système.

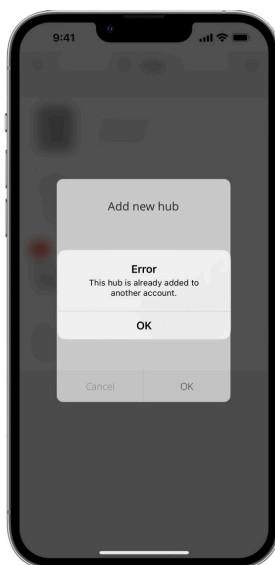


La modification ou la suppression de l'administrateur de la liste des utilisateurs de la centrale ne réinitialise pas les paramètres du système ou des dispositifs connectés.



S'il y a déjà des utilisateurs sur la centrale, l'administrateur, un PRO ayant des pleins droits ou l'entreprise d'installation qui gère la centrale sélectionnée peut ajouter votre compte. Vous recevrez une notification indiquant que la centrale est déjà ajoutée à un autre compte. Contactez l'[Assistance technique](#) pour savoir qui a les droits d'administration sur la centrale.

Droits des utilisateurs dans le système de sécurité Ajax



Pour ajouter une centrale à la version PRO de l'application :

1. Connectez l'alimentation externe, la batterie de secours, Ethernet, et/ou les cartes SIM à la centrale.
2. Allumez la centrale et attendez que le voyant d'état de la connexion s'allume en vert ou en blanc.
3. Ouvrez la version PRO de l'application. Autorisez l'application à accéder aux fonctionnalités demandées. Cela vous permettra d'utiliser pleinement les capacités des applications Ajax et de ne pas manquer les notifications d'alarmes ou d'événements.
4. Créez un espace virtuel.



Qu'est-ce qu'un espace

Comment créer un nouvel espace dans l'application Ajax



La fonctionnalité espace est disponible dans les applications des versions suivantes et ultérieures :

- 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.

5. Cliquez sur **Ajouter une centrale**.
6. Choisissez une méthode appropriée : manuellement ou à l'aide d'un guide étape par étape. Si vous installez le système pour la première fois, suivez les instructions étape par étape.

Si vous avez sélectionné l'ajout manuel.

1. Attribuez un nom à la centrale.
2. Scannez le code QR de la centrale ou saisissez l'identifiant manuellement.
3. Attendez que la centrale soit ajoutée. Après la liaison, la centrale sera affichée dans le menu **Dispositifs** de la version PRO de l'application.



Si vous avez choisi un guide étape par étape.

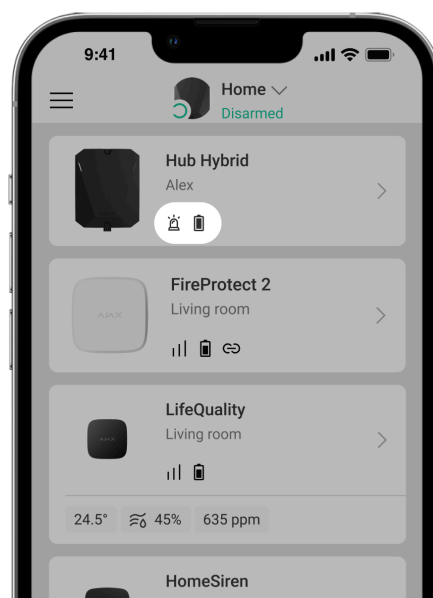
Suivez les instructions dans l'application. Une fois l'opération terminée, la centrale et les dispositifs connectés seront affichés dans le menu **Dispositifs** de la version PRO de l'application.

Compteur de dysfonctionnement

Si un défaut de la centrale est détecté (par exemple, aucune alimentation externe n'est disponible), le compteur de dysfonctionnement s'affiche sur l'icône du dispositif dans l'application Ajax.

Toutes les erreurs peuvent être affichées dans les états de la centrale. Les champs présentant des erreurs sont mis en évidence en rouge.

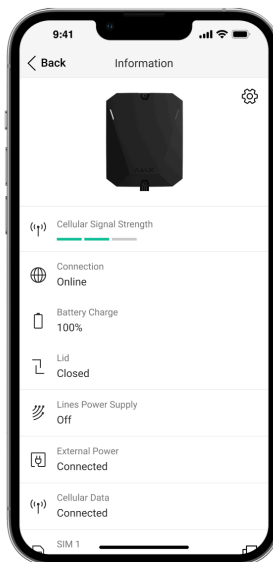
Icônes de la centrale



Les icônes affichent certains des états du Hub Hybrid. Vous pouvez les consulter dans l'application Ajax, dans l'onglet **Dispositifs** .

Icône	Signification
	La centrale fonctionne dans le réseau 2G.
	La centrale fonctionne dans le réseau 3G. Disponible uniquement pour le Hub Hybride (4G).
	La centrale fonctionne sur le réseau 4G (LTE). Disponible uniquement pour le Hub Hybride (4G).
	Aucune carte SIM. Insérez au moins une carte SIM.
	La carte SIM est défectueuse ou un code PIN a été configuré. Vérifiez le fonctionnement de la carte SIM dans le téléphone et désactivez la demande de code PIN.
	Niveau de charge de la batterie du Hub Hybrid. Affiché par incréments de 1%.
	Dysfonctionnement du Hub Hybrid détecté. Ouvrez les états de la centrale pour plus de détails.
	La centrale est directement connectée au centre de télésurveillance. L'icône ne s'affiche pas si la connexion directe n'est pas disponible ou n'est pas configurée. <u>En savoir plus</u>
	La centrale n'est pas directement connectée au centre de télésurveillance. L'icône ne s'affiche pas si la connexion directe n'est pas disponible ou n'est pas configurée. <u>En savoir plus</u>

États de la centrale



Les États peuvent être trouvés dans [l'application Ajax](#) :

1. Allez dans l'onglet **Dispositifs** .
2. Sélectionnez **Hub Hybrid** dans la liste.

Paramètre	Signification
Dysfonctionnement	Cliquez sur le bouton  pour ouvrir la liste des dysfonctionnements du Hub Hybrid. Le champ n'apparaît que si un dysfonctionnement est détecté.
Intensité du signal cellulaire	L'intensité du signal du réseau mobile de la carte SIM active. Installez la centrale dans des endroits où le niveau de communication cellulaire atteint 2-3 barres. Si la centrale est installée dans un endroit où la puissance du signal est faible ou instable, elle ne pourra pas appeler ou envoyer un SMS à propos d'un événement ou d'une alarme.

Connexion	L'état de la connexion entre la centrale et Ajax Cloud : • En ligne – la centrale est connectée à Ajax Cloud. • Hors ligne – la centrale n'est pas connectée à Ajax Cloud. Vérifiez la connexion Internet de la centrale. Si le Hub Hybrid n'est pas connecté au serveur, les icônes de la centrale et de tous les dispositifs connectés deviennent semi-transparentes dans la liste des dispositifs.
Charge de la batterie	Niveau de charge de la batterie de secours de la centrale. Affiché par incréments de 1%. À un niveau de charge de 20 % ou moins, la centrale signale une faible charge de la batterie. <u>En savoir plus</u>
Couvercle	L'état des boutons anti-sabotage qui réagissent au démontage ou à l'ouverture du caisson de la centrale : • Fermé – le couvercle de la centrale est fermé. État normal du caisson de la centrale. • Ouvert – le boîtier de la centrale est ouvert ou l'intégrité du boîtier est autrement compromise. Vérifiez l'état du boîtier de la centrale. <u>En savoir plus</u>
Alimentation des lignes	État de l'alimentation électrique des lignes Fibra de la centrale : • On – l'alimentation électrique est assurée pour toutes les lignes Fibra.



	• Off – l'alimentation électrique n'est pas assurée pour toutes les lignes Fibra.
Alimentation externe	État de la connexion de l'alimentation externe : • Connecté – la centrale est connectée à une source d'alimentation externe. • Déconnecté – pas d'alimentation externe. Vérifiez la connexion du Hub Hybrid à l'alimentation externe.
Bruit moyen (dBm)	Bruit moyen dans le canal radio. Mesuré à l'endroit où la centrale est installée. Les deux premières valeurs indiquent le niveau aux fréquences Jeweller, et la troisième – aux fréquences Wings. La valeur acceptable est de -80 dBm ou moins. Par exemple, -95 dBm est considéré comme acceptable et -70 dBm est invalide. <u>Que signifie le brouillage des systèmes de sécurité</u>
Réseau mobile	État de la connexion Internet mobile de la centrale : • Connecté – la centrale est connectée à Ajax Cloud via l'Internet mobile. • Pas connecté – la centrale n'est pas connectée à Ajax Cloud via l'Internet mobile. Vérifiez la connexion du Hub Hybrid à Internet via le réseau mobile. • Désactivé – l'option est désactivée dans les paramètres de la centrale. Si la puissance du signal cellulaire atteint 1 à 3 barres, et que la centrale dispose de suffisamment de fonds et/ou de SMS/appels bonus, elle pourra appeler et



	envoyer des SMS, même si ce champ affiche l'état Pas connecté .
Actif	Affiche les cartes SIM actives : • Carte SIM 1 – la centrale fonctionne avec une carte SIM installée dans le premier emplacement. • Carte SIM 2 – la centrale fonctionne avec une carte SIM installée dans le deuxième emplacement.
SIM 1	Le numéro de la carte SIM installée dans le premier emplacement. Pour copier le numéro, cliquez dessus. Si le numéro de téléphone est affiché comme Numéro inconnu, l'opérateur ne l'a pas enregistré dans la mémoire de la carte SIM.
SIM 2	Le numéro de la carte SIM installée dans le deuxième emplacement. Pour copier le numéro, cliquez dessus. Si le numéro de téléphone est affiché comme Numéro inconnu, l'opérateur ne l'a pas enregistré dans la mémoire de la carte SIM.





Ethernet	État de la connexion Internet de la centrale via Ethernet : • Connecté – la centrale est connectée à Ajax Cloud via Ethernet. État normal. • Pas connecté – la centrale n'est pas connectée à Ajax Cloud via Ethernet. Vérifiez la connexion du Hub Hybrid à Internet via l'Internet filaire. • Désactivé – l'option est désactivée dans les paramètres de la centrale.
Centre de télésurveillance	L'état de la connexion directe de la centrale au centre de télésurveillance : • Connecté – la centrale est directement connectée au centre de télésurveillance. • Pas connecté – la centrale n'est pas directement connectée au centre de télésurveillance. Si ce champ est affiché, l'entreprise de sécurité utilise la connexion directe pour recevoir les événements et les alarmes du système de sécurité. <u>En savoir plus</u>
Modèle de centrale	Nom du modèle de centrale : Hub Hybrid (2G) ou Hub Hybrid (4G). <u>Différences entre les centrales Ajax</u>
Version du matériel	Version matérielle du Hub Hybrid. Pas de mise à jour.
Firmware	Version du firmware du Hub Hybrid. Mises à jour à distance. <u>En savoir plus</u>

ID	Identifiant (8 premiers chiffres du numéro de série) du Hub Hybrid. L'identifiant se trouve sur le boîtier du dispositif et sur la carte, sous le code QR.
IMEI	Numéro de série unique à 15 chiffres permettant d'identifier le modem de la centrale sur un réseau GSM. Il n'est affiché que lorsqu'une carte SIM est installée dans la centrale.



Sélection du site d'installation

Le boîtier Hub Hybrid peut être fixé sur une surface verticale à l'aide d'attaches jointes. Tous les trous nécessaires à la fixation de la centrale ont déjà été percés.



La fixation verticale de la centrale est nécessaire pour que le bouton anti-sabotage réagisse si quelqu'un tente de détacher un dispositif. Consultez la documentation de la batterie avant de l'installer – certaines batteries ne peuvent être montées que verticalement (avec les bornes vers le haut). Une autre position d'installation pourrait entraîner une dégradation rapide de la batterie.

Il est conseillé de choisir un site d'installation où la centrale est cachée des regards indiscrets – par exemple, dans une pièce de rangement. Cela permettra de réduire les risques de sabotage ou de brouillage du système de sécurité. Notez que le dispositif est destiné à être installé à l'intérieur uniquement.

Choisissez un site où la centrale peut être connectée via tous les réseaux de communication possibles : Ethernet et deux cartes SIM. L'intensité du signal cellulaire sur le site d'installation doit être stable et atteindre 2 à 3 barres. Nous ne garantissons pas le bon fonctionnement du dispositif lorsque la puissance du signal cellulaire est faible.

Lors du choix du site d'installation, tenez compte de la distance entre la centrale et les dispositifs sans fil, et de la présence d'obstacles entre eux gênant le passage du signal radio : murs, ossature du bâtiment ou objets de grande taille situés dans la pièce.

Pour calculer approximativement l'intensité du signal sur le lieu d'installation des dispositifs sans fil, utilisez notre [calculateur de portée de communication radio](#). Utilisez le [Calculateur d'alimentation Fibra](#) pour calculer la portée de la connexion filaire.



Exécutez les tests d'intensité du signal Jeweller, Wings et Fibra. Une puissance de signal stable de 2 à 3 barres avec tous les dispositifs connectés doit être assurée sur le lieu d'installation choisi. Avec une intensité de signal de 1 ou 0 barres, nous ne garantissons pas un fonctionnement stable du système de sécurité.

Si le système comporte des dispositifs dont l'intensité du signal est de 1 ou 0 barre, envisagez de déplacer la centrale ou le dispositif. Si cela n'est pas possible ou si le signal du dispositif reste faible ou instable après avoir été déplacé, utilisez des [prolongateurs de portée](#).

Installation du panneau de contrôle



Pendant l'installation et le fonctionnement du système de sécurité Ajax, respectez les règles et les exigences des actes juridiques réglementaires en matière de sécurité électrique. Ne démontez pas le dispositif lorsqu'il est sous tension et ne l'utilisez pas avec un câble d'alimentation endommagé.

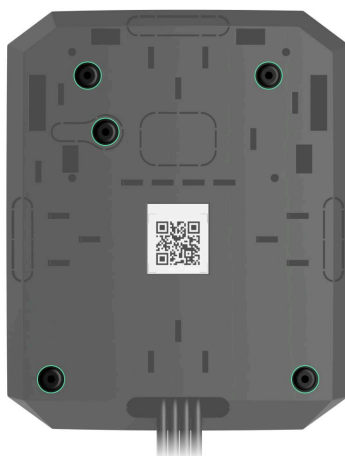
Avant l'installation, assurez-vous que vous avez choisi l'emplacement optimal pour le dispositif et qu'il est conforme aux exigences de ce manuel.

Pour installer la carte Hub Hybrid dans le boîtier de la centrale :

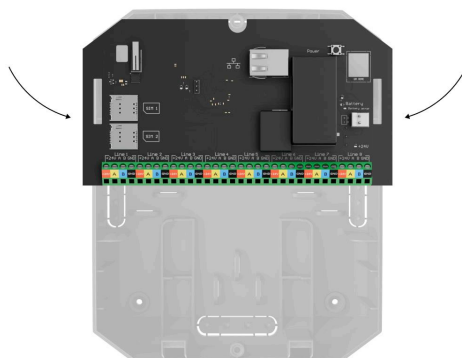
1. Préparez les sorties de câble à l'avance en brisant soigneusement les parties perforées du boîtier du Hub Hybrid.



2. Fixez le boîtier sur la surface verticale à l'emplacement d'installation choisi à l'aide des vis fournies en utilisant tous les points de fixation. L'un d'entre eux se trouve dans la partie perforée au-dessus du bouton anti-sabotage : il est nécessaire pour déclencher le bouton anti-sabotage en cas de tentative de détachement du boîtier de la centrale.



3. Placez la carte Hub Hybrid dans le boîtier sur les supports.



4. Connectez la batterie de secours de 12 V $\overline{\text{=}}$. Ne connectez pas de blocs d'alimentation tiers. Cela pourrait entraîner une défaillance du

panneau de contrôle.



Utilisez une batterie de 12 V $\overline{=}$ d'une capacité de 4, 7 ou 9 A·h. Les dimensions maximales de la batterie à installer dans le caisson sont de 151 × 65 × 94 mm, et son poids est de 5 kg. Des supports spécifiques sont prévus pour cette configuration de batterie dans le caisson de la centrale. Vous pouvez utiliser des batteries d'une capacité différente si leur taille est adaptée et si le temps de charge ne dépasse pas 40 heures. Le courant maximal de charge de la batterie à partir du Hub Hybrid est de 300 mA.



5. Allumez la centrale.

6. Installez le couvercle sur le caisson de la centrale et fixez-le avec les vis fournies.

Vérifiez l'état du boîtier de la centrale dans la version PRO de l'application. Si l'application affiche une alarme de sabotage, vérifiez l'étanchéité du boîtier du Hub Hybrid.

Comment installer la carte Hub Hybrid dans le boîtier Case D (430

Ne pas installer la centrale

À l'extérieur. Cela pourrait entraîner une défaillance du panneau de contrôle.

Près des objets métalliques et des miroirs. Ils peuvent provoquer une atténuation ou un blindage du signal radio. Cela pourrait entraîner une perte de connexion entre la centrale et les dispositifs Ajax sans fil.

Dans des endroits où les niveaux d'interférences radio sont élevés. Cela pourrait entraîner une perte de connexion entre la centrale et les

dispositifs Ajax sans fil ou de fausses notifications concernant le brouillage du système de sécurité.

Avec une autre carte imprimée de la centrale dans le Case D (430).



À moins de 1 mètre du routeur et des câbles d'alimentation. Cela pourrait entraîner une perte de connexion entre la centrale et les dispositifs sans fil.

À moins de 1 mètre de distance des dispositifs Jeweller. Cela pourrait entraîner une perte de connexion entre la centrale et ces dispositifs.

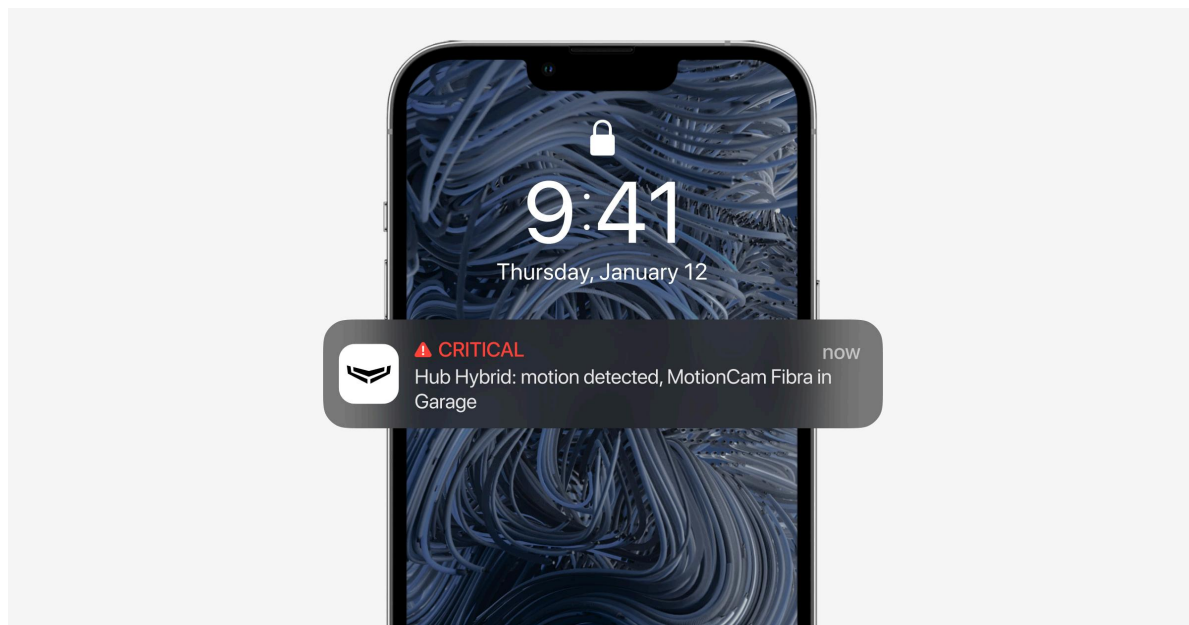
Dans les endroits où la centrale aura une force de signal de 1 ou 0 barres avec les dispositifs connectés. Cela pourrait entraîner une perte de connexion entre la centrale et ces dispositifs.

À l'intérieur de locaux dont la température et l'humidité dépassent les limites admissibles. Cela pourrait entraîner une défaillance du panneau de contrôle.

Dans les endroits où il n'y a pas de signal cellulaire ou où le signal est faible. Nous ne garantissons pas le bon fonctionnement du dispositif

lorsque la puissance du signal cellulaire est faible.

Avant de connecter les dispositifs



Créez au moins une pièce virtuelle avant d'ajouter des périphériques au système. Des pièces sont nécessaires pour regrouper les dispositifs et augmenter le contenu informatif des notifications. Les noms des dispositifs et des pièces sont affichés dans le texte des événements et des alarmes du système de sécurité Ajax.

Connexion de dispositifs sans fil



La centrale est incompatible avec les autres centrales, uartBridge et ocBridge Plus.

Pour ajouter un dispositif à la centrale, dans la version PRO de l'application :

1. Ouvrez la pièce et sélectionnez **Ajouter un dispositif** .

2. Attribuez un nom à le dispositif, scannez ou saisissez manuellement son code QR, sélectionnez un groupe si le **Mode groupe** est activé.
3. Cliquez sur **Ajouter** – le compte à rebours pour l'ajout d'un dispositif démarrera.
4. Suivez les instructions dans l'application pour connecter le dispositif.
5. Répétez les étapes 1 à 4 pour ajouter tous les périphériques nécessaires.



Pour jumeler (lier) un dispositif avec la centrale, le dispositif doit se trouver dans la portée de communication radio de la centrale – sur le même site sécurisé.

Connexion d'appareils filaires



La centrale est incompatible avec les autre centrales, uartBridge et ocBridge Plus.

Technologie de la communication filaire Fibra permet de créer des segments jusqu'à 2 000 mètres de long. Jusqu'à 8 segments dans un seul système sous contrôle du Hub Hybrid.

Le Hub Hybrid comporte 8 lignes compatibles avec tous les dispositifs Fibra, quel que soit leur type. Les détecteurs de sécurité, les claviers et les sirènes sont connectés à la même ligne et assurent la sécurité d'une zone spécifique du site.

Conception et préparation

Pour que le système fonctionne correctement, il est important de bien concevoir le projet et d'installer correctement tous les dispositifs. Le non-respect des règles d'installation de base et des recommandations du manuel d'utilisation peut entraîner un fonctionnement incorrect ou une perte de connexion entre la centrale et les dispositifs installés.

Lors de la conception du schéma d'implantation des dispositifs, tenez compte du schéma de câblage des câbles électriques posés sur le site. Les câbles de signal des dispositifs Fibra doivent être posés à une distance d'au moins 50 cm des câbles d'alimentation lorsqu'ils sont parallèles et, s'ils se croisent, ce doit être à un angle de 90°.

Au total, vous pouvez connecter jusqu'à 100 dispositifs Ajax au Hub Hybrid. Le rapport entre les dispositifs filaires et sans fil au sein du système n'a aucune importance. Par exemple, vous pouvez connecter 50 dispositifs filaires et 50 dispositifs sans fil ou 99 dispositifs filaires et 1 dispositif sans fil.



Pour les installations en construction ou en rénovation, les câbles des dispositifs filaires sont posés après le câblage principal de l'installation. Utilisez des tubes de protection pour acheminer les câbles des dispositifs filaires afin d'organiser et de sécuriser les fils ; des attaches, des clips et des agrafes peuvent être utilisés pour les fixer.

Évitez autant que possible que les câbles soient endommagés de l'extérieur. Lorsque vous posez des fils à l'extérieur (sans les monter dans les murs), utilisez une goulotte électrique. Les canalisations ne doivent pas être remplies à plus de la moitié par des câbles. Ne laissez pas les câbles s'affaisser. Le chemin de câbles doit être caché si possible – par exemple, derrière un meuble.

Nous recommandons de poser les câbles à l'intérieur des murs, des planchers et/ou des plafonds. La sécurité sera ainsi renforcée : les fils ne seront pas visibles, il sera impossible de les endommager accidentellement et il sera impossible pour un intrus d'y accéder.

Lors du choix d'un câble, tenez compte de la longueur des lignes de connexion et du nombre d'appareils à connecter ; ces paramètres influent sur la puissance du signal. Nous recommandons d'utiliser des câbles en cuivre blindés avec une couche d'isolation de haute qualité. Avant de procéder à l'installation, assurez-vous que les câbles ne sont pas pliés ou endommagés.

Lors de l'installation, respectez le rayon de courbure spécifié par le fabricant dans les spécifications du câble. Sinon, vous risquez

d'endommager ou de casser le conducteur. Le rayon de courbure est spécifié par le fabricant dans les spécifications du câble.

Puissance du signal et longueur du câble

Le niveau du signal Fibra est déterminé par le nombre de paquets de données non livrés ou corrompus sur une certaine période. La force du signal est affichée par l'icône ||| dans l'onglet **Dispositifs** :



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

L'intensité du signal est influencée par les facteurs suivants : le nombre de dispositifs connectés à une ligne, la longueur et le type de câble, et la bonne connexion des fils aux bornes des dispositifs.

La longueur maximale du câble dépend du type de câble, du matériau et de la méthode de connexion des dispositifs. Lorsque vous utilisez la **méthode de connexion Linéaire** (centrale – dispositifs – résistance de terminaison) avec une paire torsadée U/UTP cat.5 (4×2×0,51), la longueur de la connexion câblée peut atteindre 2 000 mètres. La longueur minimale du câble pour la connexion de dispositifs câblés est de 1 mètre.

Lorsque vous utilisez la **méthode de connexion en Anneau** (centrale – dispositifs – centrale), la longueur maximale du câble est de 500 mètres si vous utilisez une paire torsadée.



La topologie En anneau est disponible à partir de l'OS Malevich 2.16.

Installation et connexion



difficile d'accès pour les intrus afin de réduire les risques de sabotage. Idéalement, les fils doivent être fixés aux murs, au sol et/ou au plafond. Avant l'installation finale, testez l'Intensité du signal Fibra.

Connectez les dispositifs à la centrale à l'aide d'un câble à quatre fils. Deux fils fournissent l'alimentation au dispositif (24 V et GND), et les deux autres (A et B) sont utilisés pour l'échange de données entre les dispositifs connectés et la centrale. Lors de la connexion, veillez à respecter la polarité et l'ordre de connexion des fils.

Les périphériques sont connectés à la centrale à l'aide de deux topologies de connexion : **Anneau** et **Linéaire**. Les dispositifs sont connectés à la même ligne Fibra un par un, comme le montre la figure.



Nous recommandons de répartir les dispositifs câblés de manière égale sur toutes les lignes Fibra de la centrale pour augmenter la fiabilité.

Nous recommandons de connecter les dispositifs filaires via la **méthode de connexion en Anneau**. Ainsi, en cas de rupture de la ligne, les dispositifs seront connectés au Hub Hybrid via la **méthode de connexion Linéaire** et continueront à transmettre les événements et les alarmes à la centrale. Une notification concernant le défaut d'ouverture de la ligne sera envoyée aux utilisateurs et à l'entreprise de sécurité.

En cas de connexion via la **méthode de connexion en Anneau**, connectez deux lignes par segment et réduisez la longueur maximale de la connexion câblée à 500 mètres (en cas de **connexion Linéaire** – à 2 000 mètres).



Linéaire	En Anneau
• occupe une ligne Fibrà de la centrale • jusqu'à 8 lignes avec la même centrale • jusqu'à 2 000 m de communication filaire pour une même ligne • une résistance de terminaison est installée à l'extrémité de la ligne	• occupe deux lignes Fibrà de la centrale • jusqu'à 4 lignes avec la même centrale • jusqu'à 500 m de communication filaire pour un même anneau • pas de résistance de terminaison à l'extrémité de la ligne



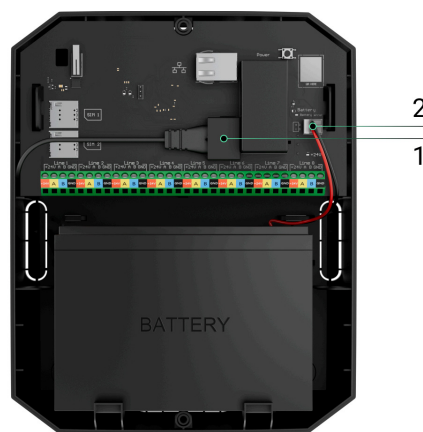
La topologie En anneau est disponible à partir de l'OS Malevich 2.16.

Lorsque vous connectez des dispositifs, ne tordez pas les fils ensemble ; soudez-les. Les extrémités des fils à insérer dans les bornes de la sirène doivent être étamées pour augmenter la fiabilité de la connexion.

Respectez la polarité et l'ordre de connexion des fils. Fixez solidement les fils aux bornes. Si le boîtier du dispositif fournit des fixations pour les câbles, fixez le câble avec des attaches.

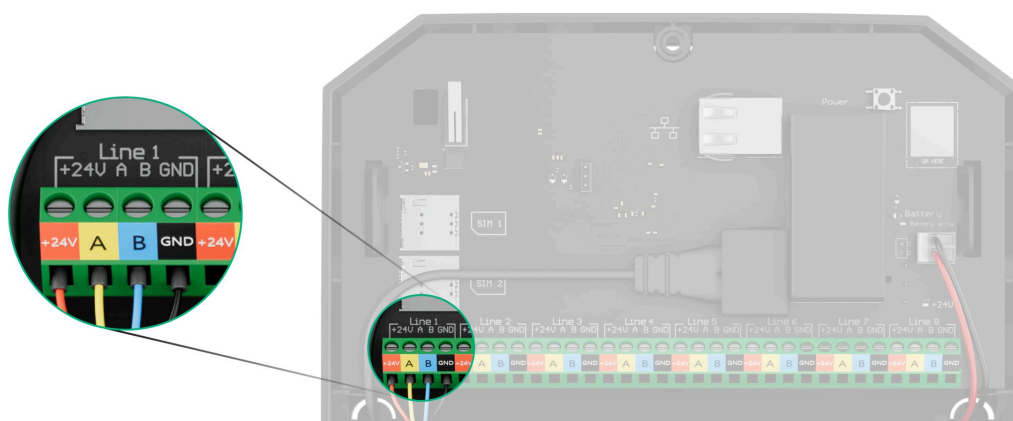
Pour connecter un détecteur ou un dispositif :

1. Mettez la centrale hors tension et éteignez-la. Débranchez la batterie de secours.



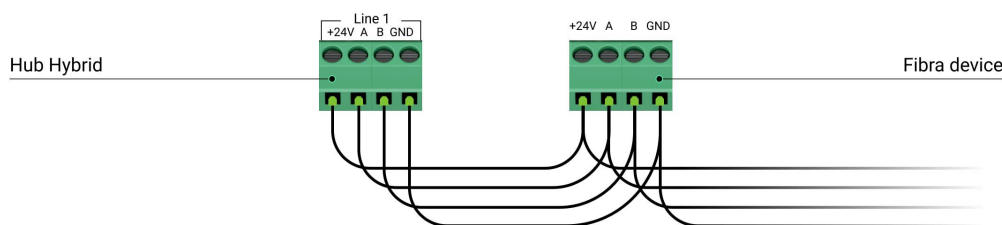
- 1 – Alimentation externe
- 2 – Batterie de secours

2. Faites passer les câbles à quatre fils dans la centrale. Connectez les fils aux terminaux de ligne du Hub Hybrid :



- +24 V** – borne d'alimentation de 24 V $\overline{\text{=}}$.
- A, B** – bornes de signal.
- GND** – mise à la terre.

3. Connectez l'autre extrémité du câble à quatre fils aux bornes du premier dispositif de la ligne, en respectant la polarité et l'ordre de câblage. Fixez solidement le câble aux bornes du dispositif.
4. Si d'autres dispositifs sont connectés au segment, préparez et connectez le câble du dispositif suivant aux bornes.

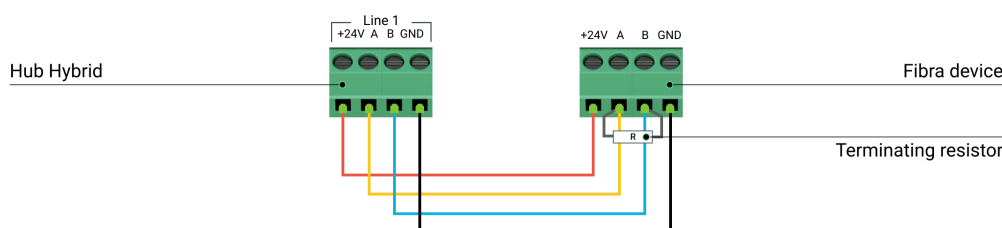


+24 V – borne d'alimentation de 24 V_~.

A, B – bornes de signal.

GND – mise à la terre.

5. Connectez d'autres dispositifs à la ligne, si nécessaire.
6. Installez une résistance de terminaison de 120 ohms pour le dernier dispositif de la ligne avec la topologie de connexion **Linéaire**. Une résistance de terminaison est installée entre les bornes A et B du dernier dispositif de la ligne.



Avec la topologie de connexion en **Anneau**, une résistance de terminaison n'est pas nécessaire. Dans ce cas, connectez le dernier dispositif de la ligne à la ligne Fibra suivante de la centrale.



La valeur nominale des résistances de terminaison est de 120 Ω. Les résistances de terminaison sont incluses dans le kit complet de Hub Hybrid.



La topologie En anneau est disponible à partir de l'OS Malevich 2.16.

7. Branchez la centrale et mettez-la sous tension.
8. Ajouter des dispositifs au système manuellement ou en utilisant le balayage des lignes.
9. Exécutez le test d'Intensité du signal Fibra pour chaque dispositif connecté. La puissance du signal recommandée est de deux ou trois barres. Sinon, vérifiez la connexion et l'intégrité des fils ou déplacez les dispositifs du système.



Ajout de dispositifs filaires

Il existe deux façons d'ajouter des périphériques câblés : manuellement et en utilisant le balayage des lignes. Il est pratique d'ajouter manuellement un petit nombre de dispositifs – par exemple, lors du remplacement d'un détecteur défectueux par un nouveau. Le balayage automatique des lignes est utile lors de l'ajout de nombreux dispositifs.

Pour ajouter un périphérique filaire manuellement :

1. Ouvrez la version PRO de l'application.
2. Sélectionnez le site auquel vous souhaitez ajouter le périphérique.
3. Allez dans l'onglet **Dispositifs**  et cliquez sur **Ajouter un dispositif** .
4. Attribuez un nom à le dispositif, scannez ou saisissez le code QR (disponible sur le boîtier du dispositif et sur son emballage), sélectionnez une pièce et un groupe (si le mode Groupe est activé).
5. Cliquez sur **Ajouter**.

Pour ajouter des périphériques en utilisant le balayage des lignes :

1. Ouvrez la version PRO de l'application.
2. Sélectionnez le site auquel vous souhaitez ajouter le périphérique.
3. Allez à l'onglet  **Dispositifs**.

4. Cliquez sur **Ajouter un dispositif**.
5. Cliquez sur **Ajouter tous les dispositifs Fibra**.
6. La centrale démarre le processus de balayage des lignes.

Après le balayage des lignes, l'application PRO affichera une liste des dispositifs filaires connectés à la centrale. Les périphériques de la liste sont triés par les lignes auxquelles ils sont physiquement connectés.



Par défaut, la désignation du dispositif comprend son nom et son ID. Pour jumeler un dispositif à la centrale, modifier son nom, l'affecter à une pièce et à un groupe si le mode Groupe est activé.



Le balayage est également disponible dans le menu des **Lignes** (Centrale → Paramètres → Lignes → Ajouter tous les dispositifs Fibra).

Pour que l'installateur puisse nommer correctement le dispositif ou lui attribuer une pièce et un groupe, nous avons prévu deux méthodes d'identification du dispositif : par indication LED et par alarme.

Méthode 1 : Identification du dispositif par le clignotement

Après le balayage des lignes, l'application PRO affichera une liste des dispositifs filaires connectés à la centrale.

Cliquez sur n'importe quel dispositif de cette liste. Après avoir cliqué, le voyant lumineux du dispositif se met à clignoter. Après avoir identifié le périphérique, reliez-le à la centrale.

Pour jumeler un dispositif à une centrale :

1. Cliquez sur le dispositif dans la liste.
2. Attribuez un nom à le dispositif.
3. Spécifiez une pièce et un groupe si le mode Groupe est activé.
4. Cliquez sur **OK**.

5. Le dispositif jumelé disparaît de la liste des dispositifs à ajouter.

Méthode 2 : Ajout de dispositifs par alertes

Activez le commutateur **Priorité aux dispositifs déclenchés**.

Déclenchez une alarme. Par exemple, marchez devant un détecteur de mouvement, appuyez sur n'importe quel bouton du clavier ou déclenchez une alarme anti-sabotage.



Après avoir été déclenché, le détecteur passe en tête de liste dans la catégorie **Dispositifs récemment déclenchés**. le Dispositif restera dans cette catégorie pendant 5 secondes, puis reviendra dans la catégorie de la ligne. Après avoir identifié le périphérique, reliez-le à la centrale.

Pour jumeler un dispositif à une centrale :

1. Cliquez sur le dispositif dans la liste.
2. Attribuez un nom à le dispositif.
3. Spécifiez une pièce et un groupe si le mode Groupe est activé.
4. Cliquez sur **OK**.
5. Le dispositif jumelé disparaît de la liste des dispositifs à ajouter.

La mise à jour des états des dispositifs câblés dépend de la période de ping (ajustée dans les paramètres Jeweller/Fibra).

Si la centrale comporte déjà le nombre maximal de dispositifs ajoutés (pour le Hub Hybrid, la valeur par défaut est 100), vous recevrez une notification d'erreur lorsque vous en ajouterez un.

Les dispositifs Ajax connectés ne fonctionnent qu'avec une seule centrale. Une fois ajoutés à une nouvelle centrale, ces dispositifs ne sont pas supprimés de la liste des dispositifs de la centrale initiale. Cela doit être fait via l'application Ajax PRO.

Paramètres du Hub

Les paramètres du panneau de contrôle peuvent être modifiés dans les applications Ajax PRO. Afin de modifier les paramètres :

1. Connectez-vous à la version PRO de l'application.
2. Sélectionnez un site dans la liste.
3. Allez au menu **Dispositifs** .
4. Sélectionnez une centrale.
5. Accédez à ses **Paramètres** en cliquant sur l'icône de l'engrenage .
6. Sélectionnez un groupe de paramètres et effectuez des modifications.
Après avoir effectué les modifications, cliquez sur **Retour** pour enregistrer les nouveaux paramètres.

Nom 

Pièce 

Ethernet 

Cellulaire 

Codes d'accès aux claviers 

Restrictions sur la longueur des codes 

Calendrier de sécurité 

Test de zone de détection 

Jeweller/Fibra 



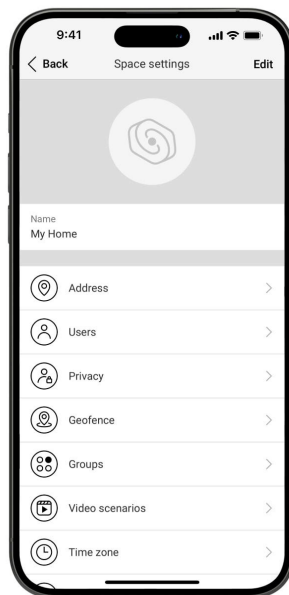
Paramètres de téléphonie	▼	
Lignes	▼	
Service	▼	
Manuel de l'utilisateur	▼	
Transférer les paramètres vers une autre centrale	▼	
Dissocier la centrale	▼	

Réinitialisation des paramètres de la centrale

Réinitialisation de la centrale aux réglages d'usine :

1. Allumez la centrale si elle est éteinte.
2. Retirez tous les utilisateurs et installateurs de la centrale.
3. Maintenez le bouton d'alimentation pendant 30 secondes – le voyant LED sur la carte imprimée de la centrale commence à clignoter en rouge.
4. Supprimez la centrale de votre compte.

Paramètres de l'espace



Les paramètres peuvent être modifiés dans [l'application Ajax](#) :

1. Sélectionnez l'espace si vous en avez plusieurs ou si vous utilisez une application PRO.
2. Allez dans l'onglet **Contrôle**.
3. Accédez aux **Paramètres** en appuyant sur l'icône ⚙️ d'engrenage dans le coin inférieur droit.
4. Définissez les paramètres requis.
5. Cliquez sur **Retour** pour enregistrer les paramètres.

[Comment configurer un espace ?](#)

Caractéristiques supplémentaires

Vidéosurveillance

Des caméras tierces peuvent être connectées au système de sécurité : grâce à la prise en charge du protocole RTSP, l'intégration avec les caméras IP et les enregistreurs numériques Dahua, Hikvision, Safire, EZVIZ et Uniview est possible.

Vous pouvez connecter jusqu'à 25 dispositifs de vidéosurveillance au système.

Comment ajouter une caméra au système de sécurité Aja

Scénarios



Le Hub Hybrid permet de créer 32 scénarios et de minimiser l'impact du facteur humain sur la sécurité. La centrale peut gérer la sécurité de l'ensemble du site ou d'un groupe en fonction d'un programme, activer la machine à fumée si des intrus pénètrent dans la pièce, mettre hors tension la pièce et allumer l'éclairage de secours en cas d'incendie, couper l'eau en cas de fuite, contrôler les dispositifs d'éclairage, les serrures électriques, les volets roulants et les portes de garage, tout en changeant le mode de sécurité en appuyant sur un bouton ou par l'alarme d'un détecteur.

Les scénarios peuvent être utilisés pour réduire le nombre d'actions de routine et améliorer la productivité. Les dispositifs d'automatisation Ajax réagissent aux changements de température et de qualité de l'air. Par exemple, vous pouvez régler le chauffage pour qu'il s'allume lorsqu'il fait froid, contrôler le système de ventilation, l'humidificateur et le climatiseur pour maintenir un climat confortable dans les pièces.

Comment créer et personnaliser un scénario

Levée de doute

Le Hub Hybrid prend en charge les détecteurs de mouvement sans fil MotionCam et MotionCam Outdoor. Lorsqu'ils sont déclenchés, les détecteurs prennent une série de clichés que vous pouvez utiliser pour évaluer le déroulement des événements survenus sur le site au fil du temps. Cela permet de réduire l'anxiété des utilisateurs et d'éviter les envois inutiles de patrouilles.

Le détecteur active la caméra quand il est armé et détecte un mouvement. Seuls les utilisateurs ayant accès au flux des événements, ainsi que les

employés autorisés de la société de sécurité peuvent voir les vérifications visuelles des alarmes, à condition que le système de sécurité soit connecté au centre de télésurveillance.

Si la fonction **Photo à la demande** est activée, les détecteurs peuvent prendre une photo sur commande d'un utilisateur du système ou d'un utilisateur PRO disposant des droits appropriés. Le fait de prendre une photo est toujours enregistré dans le flux d'événements de la centrale.



Les clichés sont protégés par chiffrement à chaque étape de la transmission. Elles sont stockées sur le serveur Ajax Cloud et ne sont ni traitées ni analysées.

[En savoir plus](#)

Maintenance

Vérifiez régulièrement le fonctionnement du Hub Hybrid et des dispositifs connectés. La fréquence optimale des contrôles est d'une fois tous les trois mois. Nettoyez le boîtier de la centrale de la poussière, des toiles d'araignée et des autres contaminants dès leur apparition. Utilisez un chiffon doux et sec, adapté à l'entretien de l'équipement.

N'utilisez pas de substances contenant de l'alcool, de l'acétone, de l'essence et d'autres solvants actifs pour nettoyer le dispositif.

Spécifications techniques

[Toutes les spécifications techniques de Hub Hybrid \(2G\)](#)

[Toutes les spécifications techniques de Hub Hybrid \(4G\)](#)

[Conformité aux normes](#)

[Conformité d'installation INCERT](#)

Kit complet



1. Hub Hybrid (2G) ou Hub Hybrid (4G).
2. Câble d'alimentation.
3. Adaptateur de bornier à vis (uniquement pour la conformité INCERT).
4. Câble Ethernet.
5. Caisson
6. Huit résistances de terminaison de 120 Ω .
7. Kit d'installation.
8. Guide de démarrage rapide

Garantie

La garantie des produits de la Limited Liability Company "Ajax Systems Manufacturing" est valable 2 ans après l'achat.

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

Obligations de garantie

Conditions générales d'utilisation

Contacter l'assistance technique :

- e-mail
- Telegram



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

S'abonner