

# Hub manuel utilisateur

Mis à jour August 10, 2020



**Hub** est un appareil central du système de sécurité Ajax, qui coordonne les appareils connectés et interagit avec l'utilisateur et le centre de télésurveillance. Utilisé à l'intérieur.

Hub nécessite un accès Internet pour communiquer avec le serveur Ajax Cloud – pour la configuration et le contrôle depuis n'importe quel point du monde, le transfert des notifications d'événements et la mise à jour du logiciel. Les données personnelles et les journaux du fonctionnement du système sont stockés sous une protection à plusieurs niveaux, et l'échange d'informations avec le Hub est effectué par un canal crypté sur une base de 24 heures.

En communiquant avec Ajax Cloud, le système peut utiliser la connexion Ethernet et le réseau GSM.



Veuillez utiliser les deux canaux de communication pour assurer une communication plus fiable entre le hub et Ajax Cloud.

Hub peut être contrôlé via l'[app](#) pour iOS, Android, macOS ou Windows. L'app permet de répondre rapidement à toute notification du système de sécurité.

Suivez le lien pour télécharger l'application pour votre système d'exploitation :

## [Android](#)

## [iOS](#)

L'utilisateur peut personnaliser les notifications dans les paramètres du hub. Choisissez ce qui vous convient le mieux : notifications push, SMS ou appels. Si le système Ajax est connecté au centre de télésurveillance, le signal d'alarme lui sera directement envoyé, en contournant Ajax Cloud.

## [Achetez le panneau de contrôle de sécurité intelligent Hub](#)

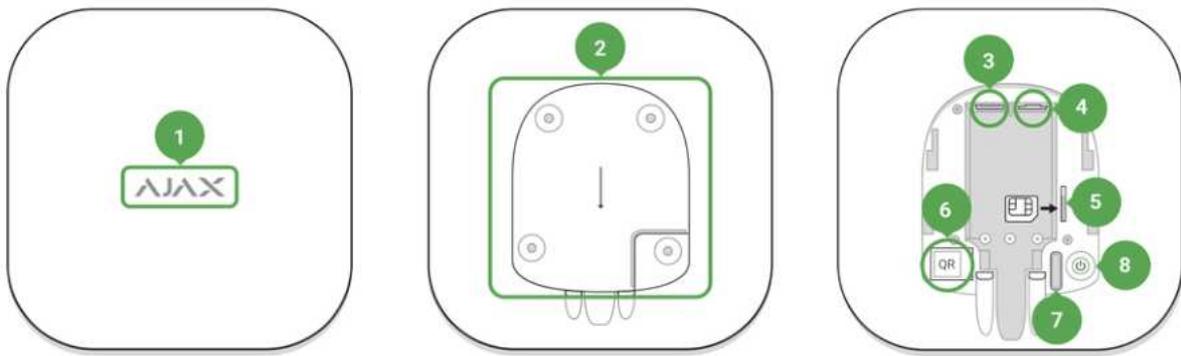
Jusqu'à 100 appareils Ajax peuvent être connectés au hub. Le protocole radio protégé de [Jeweller](#) assure une communication fiable entre les appareils à une distance allant jusqu'à 2 km dans la ligne de visée.

## [Liste des appareils Ajax](#)

Utilisez des scénarios pour automatiser le système de sécurité et diminuer le nombre d'actions de routine. Ajustez l'horaire de sécurité, programmez les actions des appareils d'automatisation ( [Relay](#), [WallSwitch](#) ou [Socket](#) ) en réponse à une alarme, en appuyant sur [Button](#) ou selon l'horaire. Un scénario peut être créé à distance dans l'app Ajax.

## [Comment créer et configurer un scénario dans le système de sécurité Ajax](#)

## Prises et indication



1. Le logo LED indiquant le statut du hub
2. Panneau de fixation du SmartBracket (une partie perforée est nécessaire pour actionner l'anti-sabotage en cas de tentative de démontage du hub)
3. Prise pour le câble d'alimentation
4. Prise pour le câble Ethernet
5. Emplacement pour la micro carte SIM
6. QR code
7. Bouton anti-sabotage
8. Bouton marche/arrêt

## Indication du logo



En cliquant sur le bouton d'alimentation, le logo Ajax s'allume en vert pendant une seconde. Juste après, le logo change de couleur pour devenir rouge, indiquant que le hub est en train de charger. Une fois le chargement terminé, la couleur du logo dépend de la connexion avec Ajax Cloud.

Si le hub n'est pas connecté à l'alimentation, le logo s'allume pendant 3 minutes, puis clignote toutes les 20 secondes.

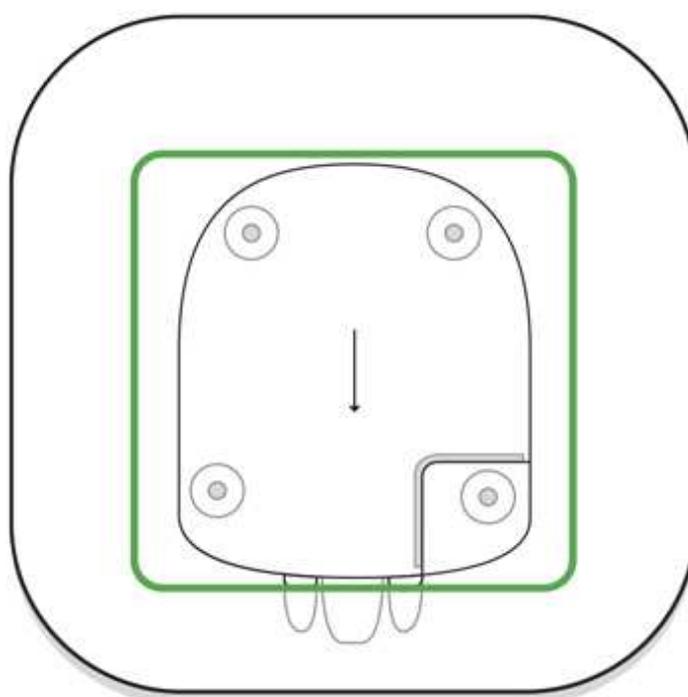
## Communication avec Ajax Cloud

La couleur en surbrillance informe de la communication avec Ajax Cloud

Indication	Événement
Allumé blanc	Les deux canaux de communication sont connectés (Ethernet et GSM)
Allumé vert vif	Un canal de communication est connecté
Allumé rouge	Le hub n'est pas connecté à Internet ou il n'y a pas de communication avec le serveur

## Connexion au réseau

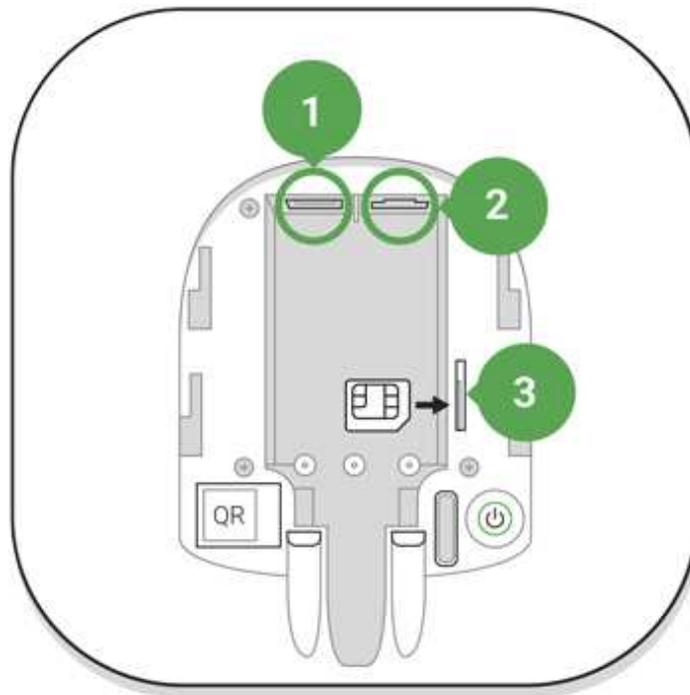
1. Ouvrez le couvercle du hub en le déplaçant vers le bas avec force.





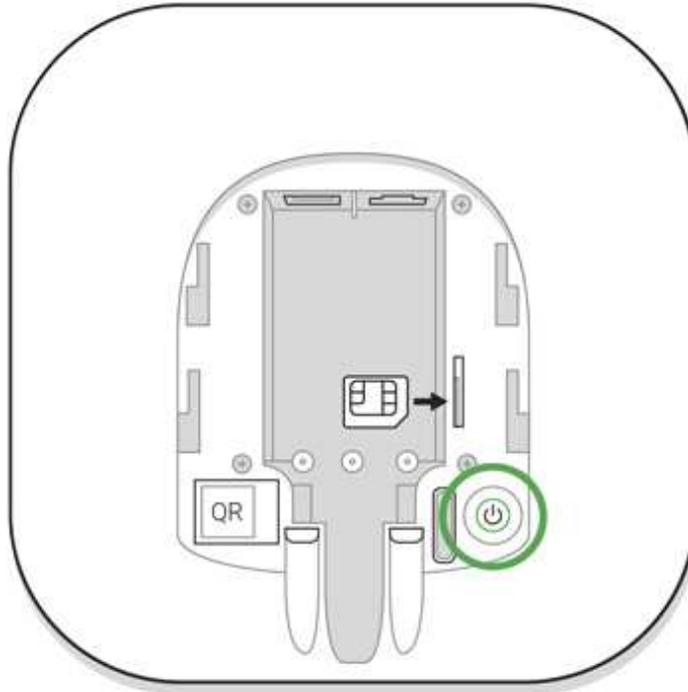
Faites attention et n'endommagez pas l'anti-sabotage qui protège le hub du démontage !

2. Branchez l'alimentation et les câbles Ethernet dans les prises.



- 1 – Prise de courant
- 2 – Prise Ethernet
- 3 – Emplacements pour cartes SIM

3. Appuyez sur le bouton d'alimentation et maintenez-le enfoncé pendant 2 secondes jusqu'à ce que le logo s'allume. Le hub a besoin d'environ 2 minutes pour identifier les canaux de communication disponibles.



La couleur verte vive ou blanche du logo indique que le hub est connecté à Ajax Cloud.

Si la connexion Ethernet ne se fait pas automatiquement, désactivez le proxy, le filtrage par les adresses MAC et activez le DHCP dans les paramètres du routeur : le hub recevra une adresse IP. Lors de la prochaine installation dans l'[app](#) web ou mobile, vous pourrez définir une adresse IP statique.

Pour connecter le hub au réseau GSM, vous avez besoin d'une carte micro-SIM avec une demande de code PIN désactivé (vous pouvez le désactiver à l'aide du téléphone portable) et un montant suffisant sur le compte pour payer les services GPRS, SMS et appels.



Dans certaines régions, Hub est vendu avec une carte SIM.

Si le hub ne se connecte pas à Ajax Cloud via GSM, utilisez Ethernet pour configurer les paramètres du réseau dans l'app. Pour le paramétrage correct du point d'accès, du nom d'utilisateur et du mot de passe, veuillez contacter le service de soutien de l'opérateur.

## Compte Ajax

L'utilisateur ayant des droits d'administrateur peut configurer le système de sécurité Ajax via l'app. Le compte de l'administrateur avec les informations sur les hubs ajoutés est crypté et placé sur le Ajax Cloud.

Tous les paramètres du système de sécurité Ajax et des appareils connectés définis par l'utilisateur sont stockés localement sur le hub. Ces paramètres sont inextricablement liés au hub : le changement d'administrateur du hub n'affecte pas les paramètres des appareils connectés.



Un seul numéro de téléphone peut être utilisé pour créer un seul compte Ajax.

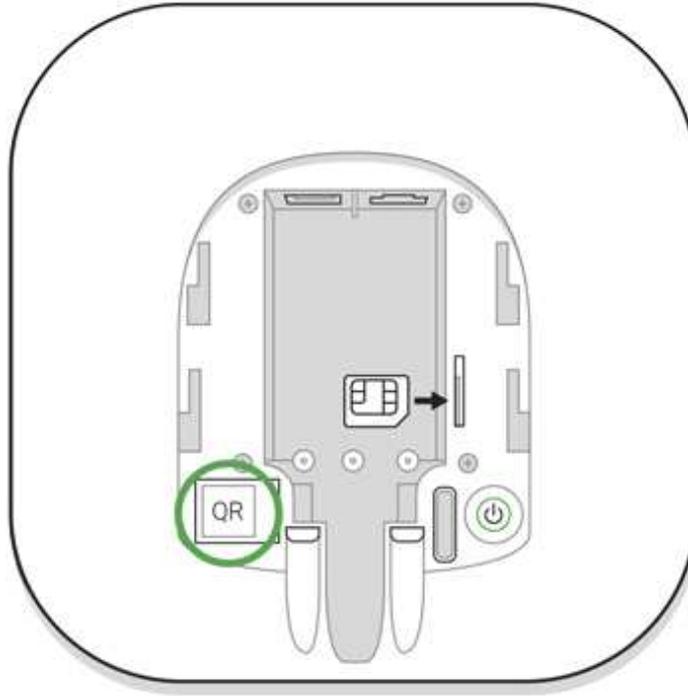
Créez le compte Ajax dans l'app en suivant le guide étape par étape. Dans le cadre de ce processus, vous devez confirmer votre adresse électronique et votre numéro de téléphone.

Le compte Ajax permet de combiner les rôles : vous pouvez être l'administrateur d'un hub, ainsi que l'utilisateur d'un autre hub.

## Ajoutez le hub à l'app Ajax

L'accès à toutes les fonctions du système (pour afficher les notifications en particulier) est une condition obligatoire pour contrôler le système de sécurité Ajax via le smartphone/tablette.

1. Connectez-vous à votre compte.
2. Ouvrez le menu **Ajouter un hub** et sélectionnez le mode d'enregistrement : manuellement ou par un guide étape par étape.
3. Au stade de l'enregistrement, tapez le nom du hub et scannez le QR code situé sous le couvercle (ou entrez une clé d'enregistrement manuellement).



4. Attendez que le hub soit enregistré et affiché sur le bureau de l'app.

## Installation



Avant d'installer le hub, assurez-vous que vous avez choisi l'emplacement optimal : la carte SIM offre une réception cohérente, tous les appareils ont été testés pour la communication radio et le hub est caché à la vue directe.



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

Le hub doit être fixé de manière fiable à la surface (verticale ou horizontale). Nous ne recommandons pas l'utilisation de ruban adhésif double face : il ne peut pas garantir une fixation sûre et simplifie le retrait de l'appareil.

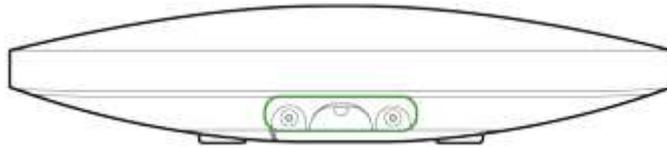
### Ne placez pas le hub :

- à l'extérieur des locaux (en plein air) ;
- à proximité ou à l'intérieur de tout objet métallique ou miroir provoquant l'atténuation et le filtrage du signal ;
- dans des endroits où le signal GSM est faible ;

- à proximité de sources d'interférences radio: à moins d'un mètre du routeur et des câbles d'alimentation ;
- à l'intérieur de tout local dont la température et l'humidité dépassent les limites autorisées.

### Installation du hub :

1. Fixez le tamper du hub sur la surface à l'aide de vis groupées. Lorsque vous utilisez d'autres accessoires de fixation, veillez à ce qu'ils n'endommagent pas ou ne déforment pas le tamper du hub.
2. Mettez le hub sur le tamper et fixez-le avec des vis groupées.



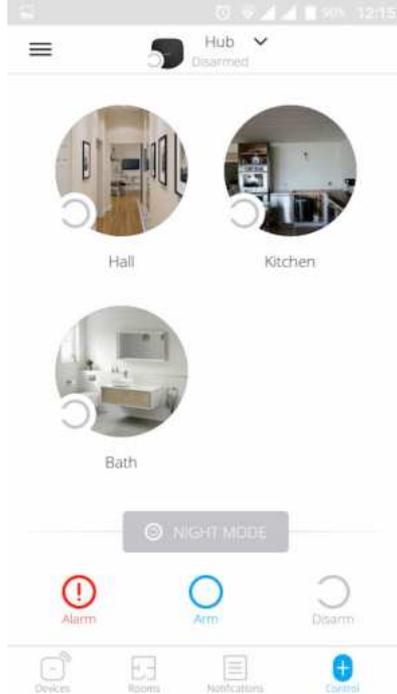
Ne retournez pas le hub lors d'une installation verticale (par exemple, sur un mur). Avec une bonne fixation, le logo Ajax se lira horizontalement.



La fixation du hub sur le tamper à l'aide de vis empêche tout déplacement accidentel du hub et minimise le risque de vol de l'appareil.

Si le hub est solidement fixé, le démontage de son boîtier de la surface déclenche l'alarme de l'anti-sabotage, et le système vous en informe.

## Les pièces dans l'app Ajax



Les pièces virtuelles servent à regrouper les appareils connectés. L'utilisateur peut créer jusqu'à 50 pièces, chaque appareil étant situé dans une seule pièce.



Sans créer la pièce, vous ne pouvez pas ajouter d'appareils dans l'app Ajax !

## Création et configuration de la pièce

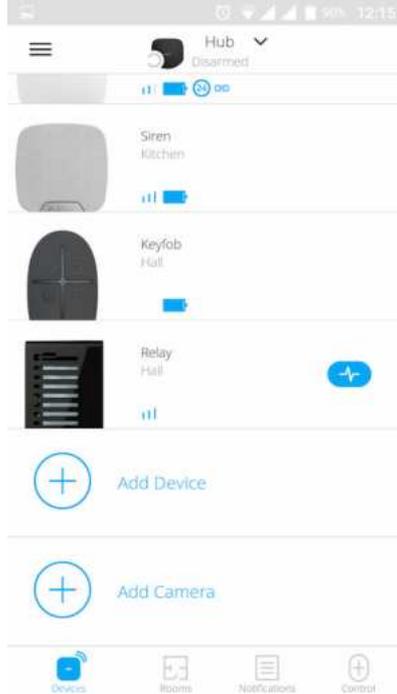
La pièce est créée dans l'app à l'aide du menu **Ajouter une pièce**.

Veillez attribuer un nom à la pièce et, éventuellement, joindre (ou faire) une photo : cela permet de trouver rapidement la pièce nécessaire dans la liste.

En appuyant sur le bouton d'engrenage , vous accédez au menu des paramètres de la pièce.

Pour supprimer la pièce, déplacez tous les appareils dans d'autres pièces à l'aide du menu de configuration des appareils. La suppression de la pièce efface tous ses paramètres.

## Connexion des appareils



Lors de la première inscription au hub dans l'app, il vous sera demandé d'ajouter des appareils pour surveiller la pièce. Cependant, vous pouvez refuser et revenir à cette étape plus tard.



L'utilisateur ne peut ajouter l'appareil que lorsque le système de sécurité est désarmé !

1. Ouvrez la pièce dans l'app et sélectionnez l'option **Ajouter un appareil**.
2. Nommez l'appareil, scannez le **QR code** (ou insérez l'ID manuellement), sélectionnez la pièce et passez à l'étape suivante.
3. Lorsque l'app commence la recherche et lance le compte à rebours, allumez l'appareil : sa LED clignotera une fois. Pour qu'il y ait détection et jumelage, l'appareil doit être situé dans la zone de couverture du réseau sans fil du hub (au niveau d'un seul objet protégé).



La demande de connexion est transmise pour une courte durée, au moment de la mise en marche de l'appareil.

Si la connexion échoue du premier coup, éteignez l'appareil pendant 5 secondes et réessayez.

Jusqu'à 10 caméras ou DVR supportant le protocole RTSP peuvent être connectés au Hub.

## Comment configurer et connecter une caméra IP au Système de sécurité Ajax

### États du Hub

### Icônes

Les icônes affichent certains des états de Hub. Vous pouvez les voir dans l'app Ajax, dans le menu **Appareils** .

Icône	Valeur
	2G connecté
	La carte SIM n'est pas installée
	La carte SIM est défectueuse ou comporte un code PIN
	Niveau de charge de la batterie du Hub. Affichage par tranches de 5%
	Le dysfonctionnement du Hub est détecté. La liste est disponible dans la liste des États du hub
	Le hub est directement relié au centre de télésurveillance de l'organisme de sécurité
	Le hub a perdu la connexion avec le centre de télésurveillance de l'organisme de sécurité par connexion directe

### États

Les États peuvent être trouvés dans l'app Ajax :

1. Aller à l'onglet **Appareils** .
2. Sélectionnez Hub dans la liste.

Paramètre	Signification
Dysfonctionnement	Cliquez  pour ouvrir la liste des

	<p>dysfonctionnements de Hub.</p> <p>Le champ n'apparaît que si un dysfonctionnement est détecté</p>
Intensité du signal cellulaire	<p>Indique l'intensité du signal du réseau mobile pour la carte SIM active. Nous recommandons d'installer le hub dans des endroits où l'intensité du signal est de 2 à 3 barres. Si l'intensité du signal est faible, le hub ne pourra pas appeler ou envoyer un SMS concernant un événement ou une alarme</p>
Charge de la batterie	<p>Niveau de charge de la batterie. Affichage par tranches de 5%</p>
Couvercle	<p>État de l'anti-sabotage qui réagit au démontage du hub :</p> <ul style="list-style-type: none"> <li>• Fermé – le couvercle du hub est fermé</li> <li>• Ouvert – le hub a été retiré du support du SmartBracket</li> </ul> <p><b><u>Qu'est-ce qu'un anti-sabotage ?</u></b></p>
Alimentation externe	<p>État de la connexion de l'alimentation externe :</p> <ul style="list-style-type: none"> <li>• Connecté – le hub est connecté à une alimentation externe</li> <li>• Déconnecté – pas d'alimentation électrique externe</li> </ul>
Connexion	<p>État de connexion entre le hub et Ajax Cloud :</p> <ul style="list-style-type: none"> <li>• En ligne – le hub est connecté à Ajax Cloud</li> <li>• Hors ligne – le hub n'est pas connecté à Ajax Cloud</li> </ul>
Réseau Mobile	<p>L'état de la connexion du hub à l'Internet mobile :</p> <ul style="list-style-type: none"> <li>• Connecté – le hub est connecté à Ajax Cloud via l'Internet mobile</li> <li>• Déconnecté – le hub n'est pas connecté à Ajax Cloud via l'Internet mobile</li> </ul>

	Si le hub dispose de suffisamment de fonds sur le compte ou a des SMS/appels bonus, il pourra passer des appels et envoyer des SMS même si le statut <b>Non connecté</b> est affiché dans ce champ
Ethernet	<p>État de la connexion Internet du hub via Ethernet :</p> <ul style="list-style-type: none"> <li>• Connecté – le hub est connecté à Ajax Cloud via Ethernet</li> <li>• Déconnecté – le hub n'est pas connecté à Ajax Cloud via Ethernet</li> </ul>
Bruit moyen (dBm)	<p>Le niveau de puissance sonore aux fréquences du Protocole radio Jeweller, de l'endroit où le hub est installé.</p> <p>La valeur acceptable est de 80 dB ou moins</p>
Centre de télésurveillance	<p>L'état de la connexion directe du hub au centre de télésurveillance de l'organisme de sécurité :</p> <ul style="list-style-type: none"> <li>• Connecté – le hub est directement relié au centre de télésurveillance de l'organisme de sécurité</li> <li>• Déconnecté – le hub n'est pas directement connecté au centre de télésurveillance de l'organisme de sécurité</li> </ul> <p>Si ce champ est affiché, le centre de télésurveillance utilise une connexion directe pour recevoir les événements et les alarmes du système de sécurité.</p> <p><b><u>Qu'est-ce qu'une connexion directe ?</u></b></p>
Modèle hub	Nom du modèle du hub
Version du matériel	Version du matériel. Impossible de mettre à jour
Firmware	Version du firmware. Peut être mis à jour à distance
ID	ID/numéro de série. Se trouve également sur le boîtier de l'appareil, sur le circuit imprimé de l'appareil et sur le code QR sous le panneau du SmartBracket

# Paramètres

Les paramètres du hub et des appareils connectés se trouvent dans le menu **Paramètres du hub** .

## Paramètres réglables :

- **Utilisateurs** – définissez qui a accès à votre système de sécurité, quels droits leur sont accordés, comment le hub notifie les événements.
- **Ethernet** – configurer la connexion Ethernet.
- **GSM** – activer/désactiver la communication cellulaire, configurer la connexion et vérifier le crédit.
- **Geofence** – permet de rappeler l'armement/le désarmement du système de sécurité, lors de l'entrée dans la zone spécifiée.



La localisation de l'utilisateur est déterminée sur la base des données de l'antenne GPS ou de l'iBeacon (uniquement pour les appareils Apple).

- **Groupes** – ouvrir les paramètres du mode groupe.
- **Calendrier de sécurité** – établir un horaire pour armer/désarmer automatiquement le système de sécurité.
- **Test de zone de détection** – exécutez le test de la zone de détection pour les appareils connectés.
- **Jeweller** – configurez l'intervalle ping du détecteur du hub et le nombre de paquets non livrés qui détermine l'échec de la connexion.

L'intervalle ping détermine la fréquence à laquelle les appareils communiquent. L'intervalle plus court (en secondes) signifie une transmission plus rapide des événements entre le hub et les appareils connectés. Le nombre de paquets non livrés détermine la rapidité avec laquelle le hub identifie la perte de connexion avec l'appareil.

**Calcul du délai de déclenchement de l'alarme (avec les paramètres par défaut) :**

(8 paquets + 1 correctif) × 36 secondes intervalle d'enquête = 5 minutes 24 secondes

Dans tous les cas, les alarmes sont transmises immédiatement. N'oubliez pas que l'intervalle ping peut réduire le nombre maximum d'appareils connectés :

Intervalle	Limite de connexion
12 secondes	39 appareils
24 secondes	79 appareils
36 secondes et plus	100 appareils

- **Service** – ouvre les paramètres de service du hub.

**Délai d'alarme en raison d'échec de connexion (sec)** – règle le délai de notification d'alarme en cas de perte de connexion au serveur.

**Intervalle de ping du serveur** – règle l'intervalle d'envoi des pings du hub au serveur.

Le temps de génération du message de perte de connexion entre le serveur et le hub est calculé comme suit (avec les paramètres par défaut) :

$(3 \text{ pings} + 1 \text{ correctif}) \times 60 \text{ secondes d'intervalle d'enquête} + 300 \text{ secondes de filtre temporel} = 9 \text{ minutes.}$

Vous pouvez désactiver la mise à jour automatique du firmware du hub (activée par défaut).

### Comment désactiver la mise à jour automatique du firmware du hub

- **Luminosité LED.** Réglage de la luminosité des LED dans le logo du hub. Réglée dans la plage de 1 à 10 (la valeur par défaut est 10).
- **Vérification de l'intégrité du système.** Une fois la fonction activée, le hub vérifie l'état de tous les appareils avant de s'armer : charge de la

batterie, autoprotection, connexion. Si un problème est détecté pendant l'armement, le hub n'active pas le mode armé et émet un avertissement.

- **Autorisation d'armement** (l'option ne devient active qu'après avoir activé le **contrôle de l'intégrité du système**). Lorsque la fonction est active, le système de sécurité peut être armé même en cas de dysfonctionnement.

### **Afin d'armer le système de sécurité défectueux via l'application Ajax:**

1. Activez le mode armé – vous recevrez une alerte appropriée avec une liste de dysfonctionnements.
2. Confirmez l'armement du système de sécurité en appuyant sur **Armer**.

### **Pour confirmer l'activation du mode armé dans le système de sécurité en cas de dysfonctionnement lorsque vous utilisez un clavier KeyPad ou une télécommande SpaceControl:**

1. Activez le mode armé – vous recevrez un message de refus.
2. Confirmez l'armement du système en réactivant le mode armé dans les 30 s.

### Qu'est-ce que le contrôle de l'intégrité du système?

- **Mise à jour automatique du logiciel.** Configuration des mises à jour automatiques du firmware d'OS Malevich. Lorsque le hub est allumé, il met automatiquement à jour son firmware si une nouvelle version est disponible.

### En quoi consistent les mises à jour d'OS Malevich

### **Configuration des détecteurs d'incendie FireProtect et FireProtect Plus**

- **Alarmes FireProtect interconnectés.** Cette fonction active les sirènes intégrées de tous les détecteurs d'incendie si au moins l'un d'entre eux détecte une menace.



Les Alarmes interconnectés sont prises en charge par les détecteurs FireProtect et

FireProtect Plus avec les versions de firmware 3.42 et plus. Veuillez noter que lorsque vous activez les Interconnexion d'Alarmes, vous ne pouvez pas régler l'intervalle ping du détecteur du hub (réglages du Jeweller) à plus de 48 secondes.

## Qu'est-ce qu'une interconnexion d'alarmes dans FireProtect?

- **Ignorer la première alarme.** Fonction de répétition d'alarme pour vérifier la présence de fumée.

### **L'option fonctionne comme suit:**

1. Un détecteur détecte le détecteur de fumée.
2. Une minuterie intégrée de 30 s au sein du détecteur est activée.
3. Si le détecteur détecte toujours une menace après 30 s, une alarme est transmise au hub.

Ce réglage est recommandé s'il existe des sources potentielles de fausses alarmes à l'intérieur des locaux, par exemple, si le détecteur est installé à l'endroit où surviennent probablement les courants d'air.

### **Les paramètres de collecte et de stockage des rapports du système de sécurité Ajax**

- **Logs du Hub.** Vous pouvez désactiver les journaux ou sélectionner un canal de transmission:
  - Ethernet
  - Wi-Fi (uniquement dans Hub Plus)
  - Non – l'enregistrement est désactivé



Nous ne recommandons pas de désactiver les journaux car ces informations peuvent être utiles en cas d'erreurs dans le fonctionnement du système!

### **Réglages d'activation des sirènes**

- **Si le hub ou le boîtier du détecteur est ouvert.** Lorsque la fonction est active, le hub active les sirènes connectées si le boîtier du hub, du détecteur ou de tout autre appareil Ajax est ouvert.
- **Si un bouton panique est appuyé dans l'application.** Lorsque la fonction est active, le hub active les sirènes connectées si le bouton d'urgence est actionné dans l'application Ajax.



Désactivez la réponse de la sirène en appuyant sur le bouton d'urgence de la télécommande SpaceControl dans les réglages de la télécommande (**Appareils** )  
> **SpaceContol** > **Réglages** )

- **Centre de télésurveillance** – configuration des paramètres de connexion au CT.
- **PRO** – configurer les comptes PRO connectés au hub.
- **Entreprises de sécurité** – choisissez et connectez vous à une entreprise de sécurité dans votre région.
- **Importation des données** – un menu permettant de transférer automatiquement des appareils et des paramètres depuis un autre hub.  
**Notez que vous êtes dans les paramètres du hub dans lequel vous voulez importer des données.**

[En savoir plus sur l'importation des données](#)

## Réinitialisation des paramètres

Pour rétablir les paramètres par défaut du hub, allumez-le, puis maintenez le bouton d'alimentation enfoncé pendant 30 secondes (le logo se mettra à clignoter en rouge).

Dans le même temps, tous les détecteurs connectés, les paramètres de la pièce et les paramètres de l'utilisateur seront supprimés. Les profils d'utilisateurs resteront connectés au système.

## Utilisateurs

Après avoir ajouté le hub au compte, vous devenez l'administrateur de cet appareil. Un hub peut avoir jusqu'à 50 utilisateurs/administrateurs. L'administrateur peut inviter les utilisateurs au système de sécurité et déterminer leurs droits.

## Notifications d'événements et d'alarmes



Le hub informe les utilisateurs des événements de trois manières : notifications push, SMS et appels.

Les notifications sont définies dans le menu **Utilisateurs** :

Types d'événements	Pour ce qu'il est utilisé	Types de notifications
Armé/desarmé	Les notifications sont reçues après avoir armé/désarmé	<ul style="list-style-type: none"> <li>• SMS</li> <li>• Notification push</li> </ul>
Alarme	Notifications d'intrusion, d'incendie, d'inondation	<ul style="list-style-type: none"> <li>• SMS</li> <li>• Notification push</li> <li>• Appel</li> </ul>
Événements	Notifications d'événements relatifs à Ajax WallSwitch, Relay contrôle	<ul style="list-style-type: none"> <li>• SMS</li> <li>• Notification push</li> </ul>
Dysfonctionnements	Notifications de la perte de communication, de l'inhibition, de la faible charge de la batterie ou de l'ouverture du boîtier du détecteur	<ul style="list-style-type: none"> <li>• SMS</li> <li>• Notification push</li> </ul>

- La **notification push** est envoyée par Ajax Cloud à l'app du système de sécurité Ajax, si une connexion Internet est disponible.
- Le **SMS** est envoyé au numéro de téléphone indiqué par l'utilisateur lors de l'enregistrement du compte Ajax.
- L'**appel téléphonique** signifie que le hub appelle le numéro spécifié dans le compte Ajax.

Le hub n'appelle qu'en cas d'alarme pour attirer votre attention et réduire la possibilité que vous manquiez une alerte critique. Nous recommandons d'activer ce type de notification. Le hub appelle consécutivement tous les utilisateurs qui ont activé ce type de notification dans l'ordre spécifié dans les Paramètres utilisateurs. Si la deuxième alarme se produit, le hub effectuera un nouvel appel, mais pas plus d'une fois en 2 minutes.



L'appel est automatiquement coupé aussitôt que vous y répondez. Nous vous recommandons d'enregistrer le numéro de téléphone associé à la carte SIM du hub dans votre liste de contacts.

Les paramètres de notification ne peuvent être modifiés que pour les utilisateurs enregistrés.

## Connexion d'une entreprise de sécurité



La liste des organisations connectant le système Ajax au centre de télésurveillance est fournie dans le menu **Entreprises de sécurité** dans les paramètres du hub :

Contactez les représentants de l'entreprise qui fournit des services dans votre ville et négociez sur la connexion.

La connexion au centre de télésurveillance (CT) est possible via les protocoles Contact ID ou SIA.

## Entretien

Vérifiez régulièrement la capacité opérationnelle du système de sécurité Ajax.

Nettoyez le boîtier du hub de la poussière, des toiles d'araignée et des autres contaminants dès leur apparition. Utilisez une serviette sèche et douce, adaptée à l'entretien du matériel.

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

### Comment remplacer la pile du hub

## Kit complet

1. Ajax Hub
2. Panneau de montage SmartBracket
3. Câble d'alimentation
4. Câble Ethernet
5. Kit d'installation
6. Carte Micro SIM (non incluse dans certains pays)
7. Guide de démarrage rapide

## Exigences de sécurité

Lors de l'installation et de l'utilisation du hub, suivez les règles générales de sécurité électrique pour l'utilisation des appareils électriques, ainsi que les exigences des actes juridiques réglementaires sur la sécurité électrique.

Il est strictement interdit de démonter l'appareil sous tension ! N'utilisez pas l'appareil avec un câble d'alimentation endommagé.

## Spécifications techniques

Appareils connectés	Jusqu'à 100
Nombre de groupes	Jusqu'à 9
Nombre d'utilisateurs	Jusqu'à 50

Vidéosurveillance	Jusqu'à 10 caméras ou DVRs
Nombre de pièces	Jusqu'à 50
Scénarios	Jusqu'à 5 (Les scénarios à la modification du mode de sécurité ne sont pas prises en compte dans la limite globale des scénarios du Hub)
<b>ReX</b> connectés	1
Alimentation	110 – 240 V AC, 50 / 60 Hz
Unité d'accumulation	Li-Ion 2 A·h (jusqu'à 15 heures de fonctionnement autonome*)
Consommation d'énergie du réseau	10 W
Anti-sabotage	Oui
Bande de fréquences de fonctionnement	868,0 – 868,6 MHz ou 868,7 – 869,2 MHz, selon la région de vente
Puissance de sortie RF	8.20 dBm / 6.60 mW (limit 25 mW)
Modulation du signal radio	GFSK
Portée du signal radio	Jusqu'à 2000 m (en champ ouvert)
Canaux de communication	GSM 850/900/1800/1900 MHz GPRS, Ethernet
Installation	Intérieur
Plage de température de fonctionnement	De -10°C à +40°C
Humidité de fonctionnement	Jusqu'à 75%
Dimensions	163 × 163 × 36 mm
Poids	362 g
Certification	Niveau de Sécurité 2, Classe Environnementale II SP2 (GSM-SMS), SP5 (LAN) DP3 en conformité avec les exigences des normes EN 50131-1, EN 50131-3, EN 50136-2, EN 50131-10, EN 50136-1, EN 50131-6, EN 50131-5-3

## Garantie

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

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

[Le texte intégral de la garantie](#)

[Accord de l'utilisateur](#)

Support technique : [support@ajax.systems](mailto:support@ajax.systems)



## Besoin d'aide ?

Vous trouverez dans cette rubrique des manuels détaillés et des vidéos pédagogiques sur toutes les fonctionnalités d'Ajax. Si vous avez besoin d'aide notre équipe de techniciens spécialisés est disponible 24h/24 et 7j/7.

[Envoyez une demande](#)

