Hub manuel utilisateur

Mis à jour November 25, 2020

Hub est un appareil central du système de sécurité Ajax, qui coordonne les appareils connectés et interagit avec l'utilisateur et l'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. 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

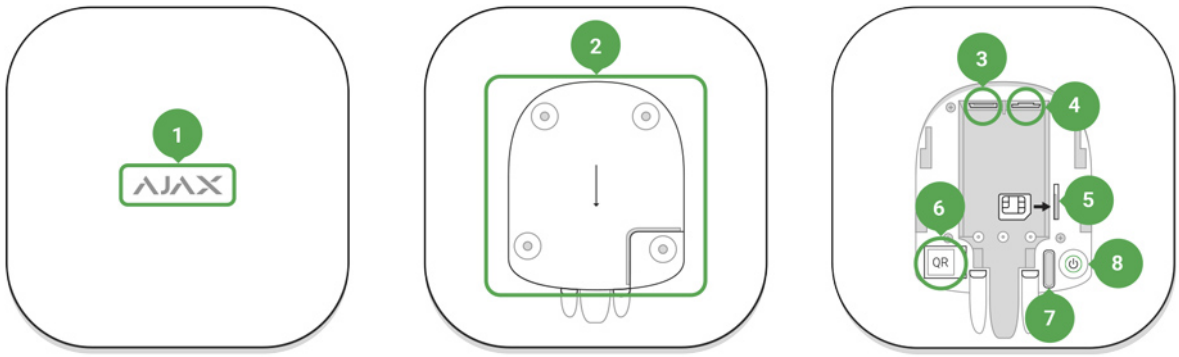
Jusqu'à 100 appareils Ajax peuvent être connectés au hub. Le protocole radio protégé de **Jeweller** assure une communication fiable entre les appareils à une distance allant jusqu'à 2 km dans la ligne de visée.

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

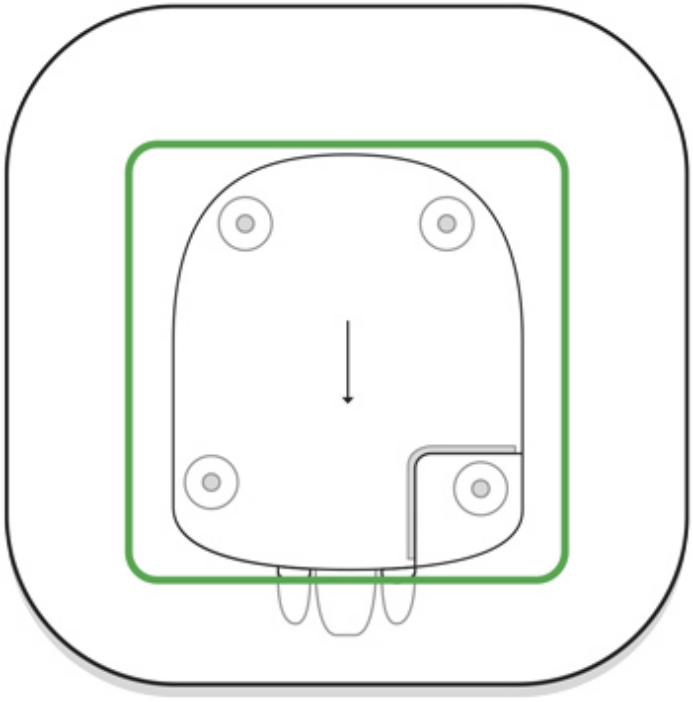
Indicateur LED du hub

Le logo avec un indicateur lumineux peut s’allumer en rouge, blanc ou vert selon le statut de l’appareil.

Événement	Indicateur lumineux
Ethernet et au moins une carte SIM sont connectés	S’allume en blanc
Un seul canal de communication est connecté	S’allume en vert
Le hub n’est pas connecté à internet ou il n’y a pas de connexion avec le service Ajax Cloud	S’allume en rouge
Aucune alimentation	S’allume pendant 3 minutes, puis clignote toutes les 20 secondes. La couleur de l’indicateur dépend du nombre de canaux de communication connectés.

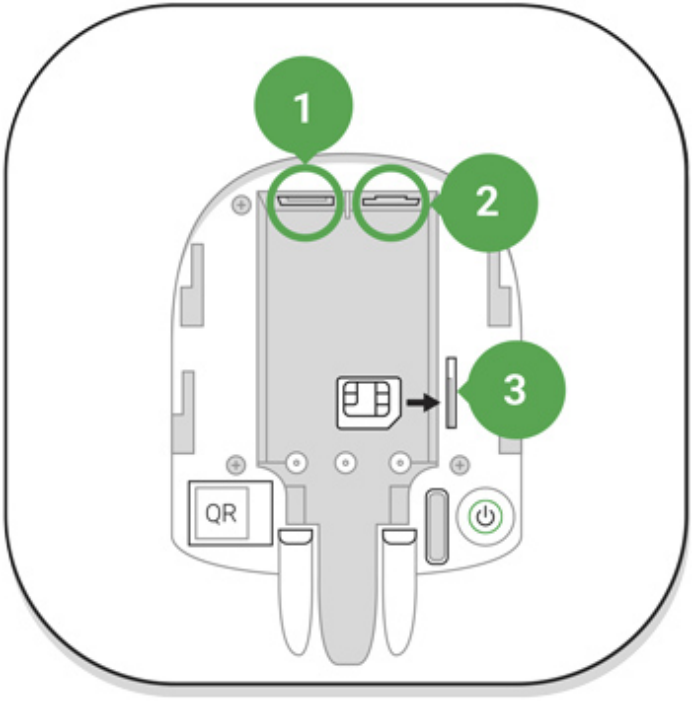
Connexion au réseau

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



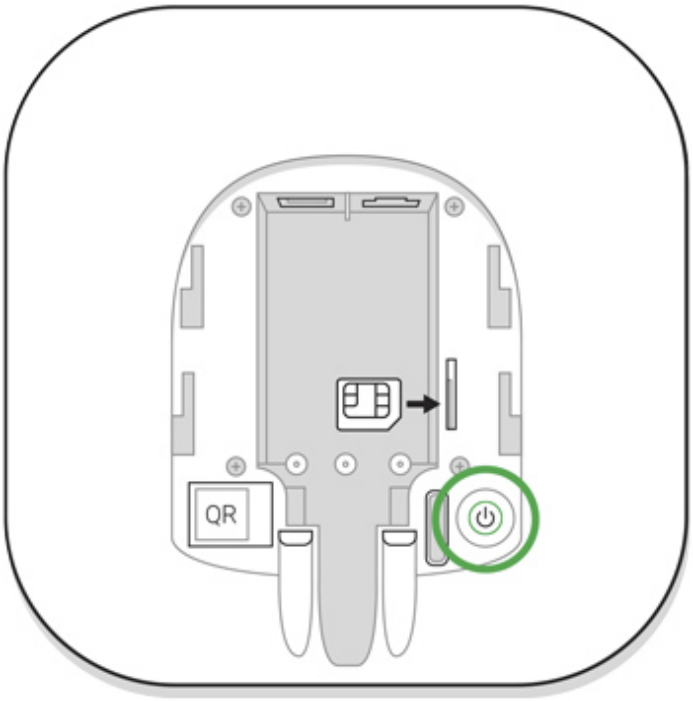
Faites attention et n’endommagez pas l’anti-sabotage qui protège le hub du démontage !

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** 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.

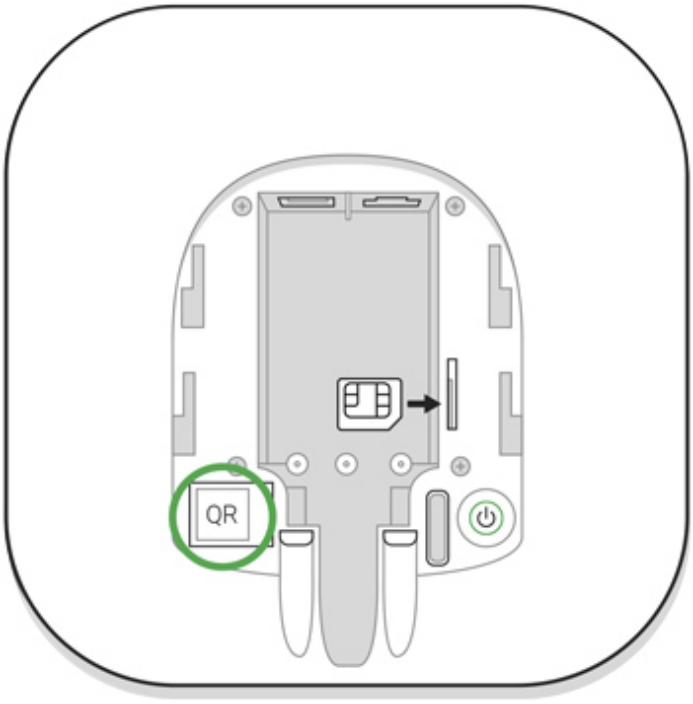
Créez le compte Ajax dans l'app en suivant le guide étape par étape. Dans le cadre de ce processus, vous devez confirmer votre adresse électronique et votre numéro de téléphone.

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.

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.

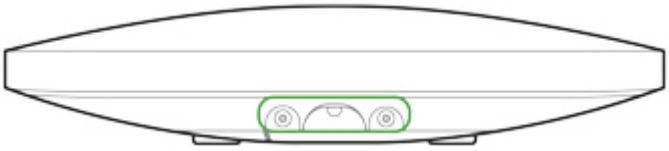
Le hub doit être fixé de manière fiable à la surface (verticale ou horizontale). Nous ne recommandons pas l’utilisation de ruban adhésif double face : il ne peut pas garantir une fixation sûre et simplifie le retrait de l’appareil.

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 lorsque 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

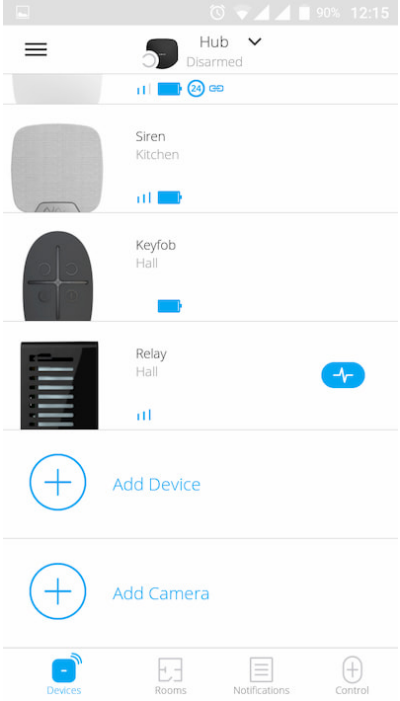
La pièce est créée dans l’app à l’aide du menu **Ajouter une pièce**.

Veuillez 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, scanner 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	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

	dysfonctionnements de Hub. Le champ n'apparaît que si un dysfonctionnement est détecté
Intensité du signal cellulaire	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
Charge de la batterie	Niveau de charge de la batterie du appareil. Affiché en pourcentage **Comment la charge de la batterie est affichée dans les app Ajax**
Couvercle	État de l'anti-sabotage qui réagit au démontage du hub : • Fermé — le couvercle du hub est fermé • Ouvert — le hub a été retiré du support du SmartBracket **Qu'est-ce qu'un anti-sabotage ?**
Alimentation externe	État de la connexion de l'alimentation externe : • Connecté — le hub est connecté à une alimentation externe • Déconnecté — pas d'alimentation électrique externe
Connexion	État de connexion entre le hub et Ajax Cloud : • En ligne — le hub est connecté à Ajax Cloud • Hors ligne — le hub n'est pas connecté à Ajax Cloud
Réseau Mobile	L'état de la connexion du hub à l'Internet mobile :

	• Connecté — le hub est connecté à Ajax Cloud via l'Internet mobile • Déconnecté — le hub n'est pas connecté à Ajax Cloud via l'Internet mobile 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 **Non connecté** est affiché dans ce champ
Ethernet	État de la connexion Internet du hub via Ethernet : • Connecté — le hub est connecté à Ajax Cloud via Ethernet • Déconnecté — le hub n'est pas connecté à Ajax Cloud via Ethernet
Bruit moyen (dBm)	Le niveau de puissance sonore aux fréquences du Protocole radio Jeweller, de l'endroit où le hub est installé. La valeur acceptable est de 80 dB ou moins
Centre de télésurveillance	L'état de la connexion directe du hub au centre de télésurveillance de l'organisme de sécurité : • Connecté — le hub est directement relié au centre de télésurveillance de l'organisme de sécurité • Déconnecté — le hub n'est pas directement connecté au centre de télésurveillance de l'organisme de sécurité Si ce champ est affiché, le centre de télésurveillance utilise une connexion directe pour recevoir les événements et les alarmes du système de sécurité. **Qu'est-ce qu'une connexion directe ?**
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 peuvent être modifiés dans **app Ajax** :

1. Aller à l'onglet **Appareils**.
2. Sélectionnez Hub dans la liste.
3. Allez à **Paramètres** en cliquant sur l'icône.

Notez qu'après avoir modifié les paramètres, vous devez cliquer sur le bouton **Précédent** pour les enregistrer.

Avatar est une image de titre personnalisée pour le système de sécurité Ajax. Il est affiché dans le menu de sélection du hub et aide à identifier l'objet requis.

Pour modifier ou définir un avatar, cliquez sur l'icône de l'appareil photo et configurez l'image souhaitée.

Nom du hub. S'affiche dans le SMS et le texte de la notification push. Le nom peut contenir jusqu'à 12 caractères cyrilliques ou jusqu'à 24 caractères latins.

Pour le modifier, cliquez sur l'icône du crayon et entrez le nom du hub souhaité.

Utilisateurs — Les paramètres des utilisateurs d'un système de sécurité : quels sont les droits accordés aux utilisateurs et comment le système de sécurité les informe des événements et des alarmes.

Pour modifier les paramètres de l'utilisateur, cliquez en ⚙ face du nom de l'utilisateur.

> **Comment le système de sécurité Ajax notifie les utilisateurs des alertes**
>
> **Comment ajouter de nouveaux utilisateurs au hub**

Ethernet — paramètres de la connexion Internet filaire.

- Ethernet — vous permet d'activer et de désactiver Ethernet sur le hub
- DHCP / Statique — sélection du type d'adresse IP du hub à recevoir : dynamique ou statique
- Adresse IP — Adresse IP du hub
- Masque de sous-réseau — masque de sous-réseau dans lequel le hub fonctionne
- Routeur — passerelle utilisée par le hub
- DNS — DNS du hub

Cellulaire — activation/désactivation de la communication cellulaire, configuration des connexions et vérification du compte.

- Données mobiles — désactivation et activation des cartes SIM sur le hub

- Itinérance — si elle est activée, les cartes SIM installées dans le hub peuvent fonctionner en itinérance
- Ignorer l'erreur d'enregistrement du réseau — lorsque ce paramètre est activé, le hub ignore les erreurs lors de la tentative de connexion via une carte SIM. Activez cette option si la carte SIM ne peut pas se connecter au réseau
- Désactiver le Ping avant de connexion — lorsque ce paramètre est activé, le hub ignore les erreurs de communication de l'opérateur. Activez cette option si la carte SIM ne peut pas se connecter au réseau
- Carte SIM 1 — affiche le numéro de la carte SIM installée. Cliquez sur le champ pour accéder aux paramètres de la carte SIM

Paramètres de la carte SIM

Paramètres de connexion

- **APN**, **Nom d'utilisateur** et **Mot de passe** — paramètres de connexion à l'internet via une carte SIM. Pour connaître les paramètres de votre opérateur de téléphonie mobile, contactez le service d'assistance de votre fournisseur.

Comment définir ou modifier les paramètres de l'APN dans le hub

Utilisation de données mobiles

- **Entrant** — la quantité de données reçues par le hub. Affiché en KB ou MB.
- **Sortant** — la quantité de données envoyées par le hub. Affiché en KB ou MB.

> N'oubliez pas que les données dépendent du hub et peuvent différer des statistiques de votre opérateur.

Réinitialiser les statistiques — réinitialise les statistiques sur le trafic entrant et sortant.

Vérification du solde

- **Code USSD** — entrez le code qui est utilisé pour vérifier le solde dans ce champ. Par exemple, *111#. Ensuite, cliquez sur **Vérifier le crèdit** pour envoyer une demande. Le résultat sera affiché sous le bouton.

Geofence — configuration de rappels pour l'armement/désarmement du système de sécurité lors du franchissement d'une zone déterminée. La localisation de l'utilisateur est déterminée à l'aide du module GPS du smartphone.

Qu'est-ce qu'une géofences et comment fonctionne-t-elle ?

Groupes — configuration du mode groupe. Cela vous permet de :

- Gérer les modes de sécurité pour des locaux séparés ou des groupes de détecteurs.
  Par exemple, le bureau est armé tandis que le personnel d'entretien travaille dans la cuisine.
- Délimiter l'accès au contrôle des modes de sécurité.
  Par exemple, les employés du département marketing n'ont pas accès au cabinet d'avocats.

OS Malevich 2.6 : un nouveau niveau de sécurité

Calendrier de sécurité — armement/désarmement du système de sécurité selon le programme.

Comment créer et configurer un scénario dans le système de sécurité Ajax

Test de zone de détection — exécution du test de la zone de détection pour les détecteurs connectés. Le test détermine la distance suffisante pour que les détecteurs puissent enregistrer les alarmes.

Qu'est-ce que le test de la zone de détection ?

Jeweller — configuration de l'intervalle ping du détecteur de hub. Les paramètres déterminent la fréquence à laquelle le hub communique avec les appareils et la rapidité avec laquelle la perte de connexion est détectée.

En savoir plus

- **Intervalle de ping du détecteur** — la fréquence d'interrogation des appareils connectés par le hub est fixée dans la plage de 12 à 300 s (36 s par défaut)
- **Nombre de paquets non livrés pour déterminer l'échec de la connexion** — un compteur de paquets non livrés (30 paquets par défaut).

Le délai avant le déclenchement de l'alarme par la perte de communication entre le hub et l'appareil est calculé avec la formule suivante :

*Intervalle ping * (nombre de paquets non livrés + 1 paquet de correction).*

Un intervalle ping plus court (en secondes) signifie une transmission plus rapide des événements entre le hub et les appareils connectés ; cependant, un intervalle ping court réduit la durée de vie de la batterie. En même temps, les alarmes sont transmises immédiatement, quel que soit l'intervalle de ping.

Nous ne recommandons pas de réduire les paramètres par défaut de la période et de l'intervalle de ping.

Notez que l'intervalle limite le nombre maximum d'appareils connectés :

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

Quels que soient les paramètres, le hub supporte 10 sirènes connectées au maximum !

Service est un groupe de paramètres de service du hub. Ils sont divisés en 2 groupes : les paramètres généraux et les paramètres avancés.

Paramètres généraux

Fuseau horaire

Sélection du fuseau horaire dans lequel fonctionne le hub. Il est utilisé pour les scénarios par horaire. Par conséquent, avant de créer des scénarios, définissez le fuseau horaire correct.

En savoir plus sur les scénarios

Luminosité LED

Ajustement de la luminosité du rétroéclairage LED du logo du hub. Fixé entre 1 à 10. La valeur par défaut est de 10.

Mise à jour automatique du logiciel

Configuration des mises à jour automatiques du firmware d'OS Malevich.

- **S'il est activé**, le firmware est automatiquement mis à jour lorsqu'une nouvelle version est disponible, lorsque le système n'est pas armé et que l'alimentation externe est connectée.
- **S'il est désactivé**, le système ne se met pas à jour automatiquement. Si une nouvelle version de firmware est disponible, l'app proposera de mettre à jour l'OS Malevich.

En quoi consistent les mises à jour d'OS Malevich

Logs du hub

Les registres sont des fichiers contenant des informations sur le fonctionnement du système. Ils peuvent aider à résoudre le problème en cas d'erreurs ou de défaillances.

Ce paramètre vous permet de sélectionner le canal de transmission pour les journaux du hub ou de désactiver leur enregistrement :

- Ethernet
- Non — connexion désactivé

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

Comment envoyer un rapport d'erreur

Paramètres avancés

La liste des paramètres avancés du hub dépend du type d'application : standard ou PRO.

Ajax Security System	Ajax PRO

Connexion du serveur Paramètres des sirènes Paramètres des détecteurs d'incendie Vérification de l'intégrité du système	Assistant de configuration PD 6662 Connexion du serveur Paramètres des sirènes Paramètres des détecteurs d'incendie Vérification de l'intégrité du système Confirmation d'alarme Restaurer après l'alarme Processus d'armé/desarmé Désactivation automatique des appareils

Assistant de configuration PD 6662

Ouvrez un guide étape par étape sur la façon de configurer votre système pour qu'il soit conforme à la norme de sécurité britannique PD 6662:2017.

> **En savoir plus sur le PD 6662:2017**
>
> **Comment configurer le système pour qu'il soit conforme au PD 6662:2017**

Connexion du serveur

Le menu contient les paramètres de communication entre le hub et Ajax Cloud :

- **Intervalle de ping du serveur**. Fréquence d'envoi des pings depuis le hub vers le serveur Ajax Cloud. Il est fixé dans une plage de 10 à 300 s. La valeur par défaut recommandée est de 60 s.
- **Délai d'alarme en raison d'échec de connexion**. Il s'agit d'un Retard destiné à réduire le risque d'une fausse alarme associée à la perte de connexion au serveur Ajax Cloud. Il est activé après 3 interrogations infructueuses du serveur central. Le délai est fixé dans une période de 30 à 600 s. La valeur par défaut recommandée est de 300 s.

Le temps nécessaire pour générer un message concernant la perte de communication entre le hub et le serveur Ajax Cloud est calculé selon la formule suivante :

*(Intervalle ping * 4) + Filtre horaire*

Avec les paramètres par défaut, Ajax Cloud signale la perte du hub en 9 minutes :

*(60 s * 4) + 300 s = 9 min*

- **Désactivez les alertes en cas de perte de connexion avec le serveur**. Les app Ajax peuvent notifier la perte de communication hub-serveur de deux manières : par un signal de notification push standard ou par un son de sirène (activé par défaut). Lorsque l'option est active, la notification est accompagnée d'un signal de notification standard en mode push.

Paramètres des sirènes

Le menu contient deux groupes de paramètres de la sirène : les paramètres d'activation de la sirène et l'indication de l'après-alarme de la sirène.

Paramètres d'activation des sirènes

Si le hub ou le boîter du détecteur est ouvert. S'il est activé, 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'app. Lorsque la fonction est active, le hub active les sirènes connectées si le bouton de panique a été appuyé dans l'app Ajax.

> Vous pouvez désactiver la réponse des sirènes lorsque vous appuyez sur le bouton de panique de la télécommande SpaceControl dans les paramètres de la télécommande (Appareils → SpaceContol → Paramètres ⚙).

Réglages de l'indication d'après-alarme des sirènes

> Ce paramètre n'est disponible que dans les app PRO Ajax

La sirène peut informer sur le déclenchement dans le système armé au moyen d'un indicateur LED. Grâce à cette fonction, les utilisateurs du système et les centres de télésurveillance de passage peuvent voir que le système a été déclenché.

Mise en œuvre des fonctionnalités dans HomeSiren

Mise en œuvre des fonctionnalités dans StreetSiren

Mise en œuvre des fonctionnalités dans StreetSiren DoubleDeck

Paramètres des détecteurs d'incendie

Menu des paramètres des détecteurs d'incendie FireProtect et FireProtect Plus. Permet de configurer l'interconnexion d'alarmes dans FireProtect des détecteurs d'incendie.

Cette fonctionnalité est recommandée par les normes européennes en matière d'incendie, qui exigent, en cas d'incendie, une puissance de signal d'avertissement d'au moins 85 dB à 3 mètres de la source sonore. Une telle puissance sonore réveille même une personne qui dort profondément pendant un incendie. Et vous pouvez rapidement désactiver les détecteurs d'incendie déclenchés en utilisant l'app Ajax, Button ou KeyPad.

En savoir plus

Vérification de l'intégrité du système

Le **Vérification d'intégrité du système** est un paramètre qui permet de vérifier l'état de tous les détecteurs et appareils de sécurité avant d'armer. La vérification est désactivée par défaut.

En savoir plus

Confirmation d'alarme

⚠ Ce paramètre n'est disponible que dans les app PRO Ajax

La **Confirmation d'alarme** est un événement spécial que le hub envoie au centre de télésurveillance et aux utilisateurs du système si plusieurs appareils déterminés se sont déclenchés dans une période de temps donnée. En répondant uniquement aux alarmes confirmées, le centre de télésurveillance et la police réduisent le nombre de visites sur les fausses alarmes.

En savoir plus

Restaurer après l'alarme

Ce paramètre n'est disponible que dans les app PRO Ajax

La fonction ne permet pas d'armer le système si une alarme a été enregistrée précédemment. Pour armer, le système doit être restauré par un utilisateur autorisé ou un utilisateur PRO. Les types d'alarmes qui nécessitent une restauration du système sont définis lors de la configuration de la fonction.

La fonction élimine les situations où l'utilisateur arme le système avec des détecteurs qui génèrent de fausses alarmes.

En savoir plus

Processus d'armé/desarmé

Ce paramètre n'est disponible que dans les app PRO Ajax

Le menu permet d'activer l'armement en deux étapes, ainsi que de régler le délai de transmission de l'alarme pour le processus de désarmement du système de sécurité Ajax.

Qu'est-ce que l'armement en deux étapes et pourquoi est-il nécessaire

Qu’est-ce que le délai de transmission des alarmes et pourquoi est-il nécessaire

Désactivation automatique des appareils

> ⚠ Ce paramètre n’est disponible que dans les app PRO Ajax

Le système de sécurité Ajax peut ignorer les alarmes ou autres événements des appareils sans les retirer du système. Selon certains paramètres, les notifications concernant les événements d’un appareil spécifique ne seront pas envoyées au centre de télésurveillance et aux utilisateurs du système de sécurité.

Il existe deux types d’**appareils de désactivation automatique** : par la minuterie et par le nombre d’alarmes.

Qu’est-ce que la désactivation automatique des appareils

Il est également possible de désactiver manuellement un appareil spécifique. Pour en savoir plus sur la désactivation manuelle des appareils, **cliquez ici**.

Effacez l’historique des notifications

Cliquer sur le bouton supprimer toutes les notifications dans l’historique des événements du hub.

Centre de télésurveillance — les réglages pour une connexion directe au centre télésurveillance. Les paramètres sont fixés par les ingénieurs du centre télésurveillance. N’oubliez pas que les événements et les alarmes peuvent être envoyés au centre de télésurveillance même sans ces paramètres.

Onglet « centre de télésurveillance » : qu’est-ce que c’est ?

- **Protocole** — le choix du protocole utilisé par le hub pour envoyer les alarmes au centre de télésurveillance via une connexion directe. Protocoles disponibles : Ajax Translator (Contact-ID) et SIA.
- **Connectez-vous sur demande**. Activez cette option si vous devez vous connecter au CMS (Centre de Télésurveillance) uniquement lors de la transmission d'un événement. Si l'option est désactivée, la connexion est maintenue en permanence. Cette option n'est disponible que pour le protocole SIA.
- **Numéro d'objet** — le numéro d'un objet dans centre de télésurveillance (hub).

Adresse IP principale

- L'**adresse IP** et le **Port** sont les paramètres de l'adresse IP principale et du port du serveur du centre de télésurveillance vers lequel les événements et les alarmes sont envoyés.

Adresse IP secondaire

- L'**adresse IP** et le **Port** sont les paramètres de l'adresse IP secondaire et du port du serveur du centre de télésurveillance vers lequel les événements et les alarmes sont envoyés.

Canaux d'envoi d'alarme

Dans ce menu, les canaux d'envoi des alarmes et des événements au centre de télésurveillance sont sélectionnés. Hub 2 Plus peut envoyer des alarmes et des événements au centre de télésurveillance via **Ethernet** et **EDGE**. Nous vous recommandons d'utiliser tous les canaux de communication en même temps – cela augmentera la fiabilité de la transmission et vous protégera contre les défaillances du côté des opérateurs de télécommunications.

- **Ethernet** — permet la transmission d'événements et d'alarmes via Ethernet.
- **Cellulaire** — permet la transmission d'événements et d'alarmes via l'internet mobile.

- **Rapport de test périodique** — si activé, le hub envoie des rapports de test avec une période donnée au CMS (Centre de télésurveillance) pour une surveillance supplémentaire de la connexion des objets.
- **Intervalle ping du centre de télésurveillance** — définit la période d'envoi des messages de test : de 1 minute à 24 heures.

Cryptage

Paramètres de cryptage des transmissions d'événements dans le protocole SIA. Le cryptage AES 128 bits est utilisé.

- **Cryptage** — s'il est activé, les événements et les alarmes transmis au centre de télésurveillance au format SIA sont cryptés.
- **Clé de cryptage** — clé de cryptage des événements et des alarmes transmis. Doit correspondre à la valeur indiquée au Centre de télésurveillance.

Coordonnées du bouton d'alarme

- **Envoyer les coordonnées** — si elle est activée, la pression d'un bouton d'alarme dans l'app envoie les coordonnées de l'appareil sur lequel l'app est installée et le bouton d'alarme est pressé, à la station centrale de surveillance.

Restauration d'alarme sur centre de télésurveillance

Ce paramètre vous permet de sélectionner le moment où l'événement de restauration de l'alarme sera envoyé au centre de télésurveillance : immédiatement/à la restauration du détecteur (par défaut) ou lors du désarmement.

En savoir plus

PRO — Paramètres des utilisateurs PRO (installateurs et représentants du centre de télésurveillance) du système de sécurité. Déterminez qui a accès

à votre système de sécurité, les droits qui sont accordés aux utilisateurs PRO et comment le système de sécurité les informe des événements.

Comment ajouter le PRO au hub

Entreprises de sécurité — une liste des centres de télésurveillance de votre région. La région est déterminée par les données GPS ou les paramètres régionaux de votre smartphone.

Manuel de l'utilisateur — ouvre le guide de l'utilisateur de Hub.

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

Dissocier le hub — supprime votre compte du hub. Indépendamment de cela, tous les réglages et les détecteurs connectés restent enregistrés.

Réinitialisation des paramètres

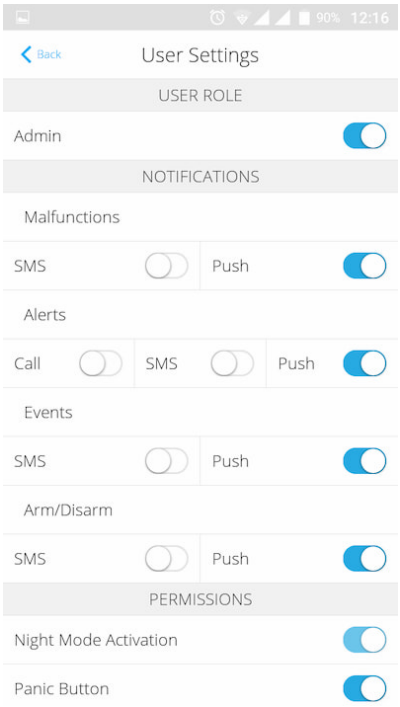
Pour rétablir les paramètres par défaut du hub, allumez-le, puis maintenez le bouton d'alimentation enfoncé pendant 30 secondes (le logo se mettra à clignoter en rouge).

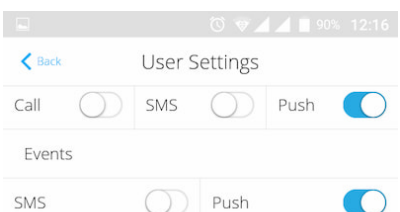
Dans le même temps, tous les détecteurs connectés, les paramètres de la pièce et les paramètres de l'utilisateur seront supprimés. Les profils d'utilisateurs resteront connectés au système.

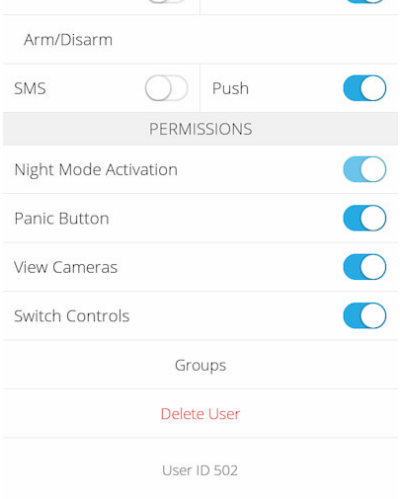
Utilisateurs

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	• SMS • Notification push
Alarme	Notifications d'intrusion, d'incendie, d'inondation	• SMS • Notification push • Appel
Événements	Notifications d'événements relatifs à Ajax WallSwitch, Relay contrôle	• SMS • Notification push
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	• SMS • Notification push

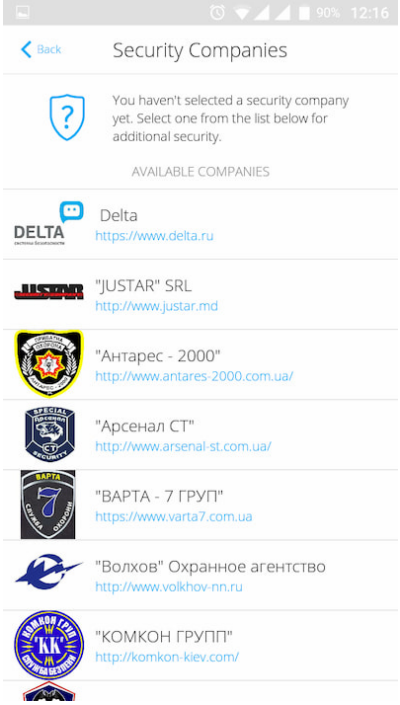
- La **notification push** est envoyée par Ajax Cloud à l'app du système de sécurité Ajax, si une connexion Internet est disponible.
- Le **SMS** est envoyé au numéro de téléphone indiqué par l'utilisateur lors de l'enregistrement du compte Ajax.
- L'**appel téléphonique** signifie que le hub appelle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