Manuel de l’utilisateur du Hub 2 Plus

Mis à jour March 17, 2021



Hub 2 Plus est un appareil central du système de sécurité Ajax, qui contrôle le fonctionnement de tous les appareils connectés et interagit avec l’utilisateur et le centre de télésurveillance.

Le hub signale l’ouverture des portes, le bris des fenêtres, les menaces d’incendie ou d’inondation, et automatise les actions de routine à l’aide de scénarios. Si des personnes

extérieures pénètrent dans la salle sécurisée, Hub 2 Plus enverra des photos provenant des détecteurs de mouvement **MotionCam** et avertira une patrouille du centre de télésurveillance.

> L'unité centrale Hub 2 Plus doit être installée uniquement à l'intérieur.

Hub 2 Plus a besoin d'un accès à Internet pour se connecter au service Ajax Cloud. L'unité centrale est connectée à Internet via Ethernet, Wi-Fi et deux cartes SIM (2G/3G/4G).

La connexion au Cloud Ajax est nécessaire pour configurer et gérer le système par le biais d'app Ajax, pour transmettre des notifications sur les alarmes et les événements, ainsi que pour mettre à jour l'**OS Malevich**. Toutes les données sur Ajax Cloud sont stockées sous une protection à plusieurs niveaux, les informations sont échangées avec le hub via un canal crypté.

> Connectez tous les canaux de communication pour assurer une connexion plus fiable avec le Cloud Ajax et pour se prémunir contre les interruptions de travail des opérateurs de télécommunications.

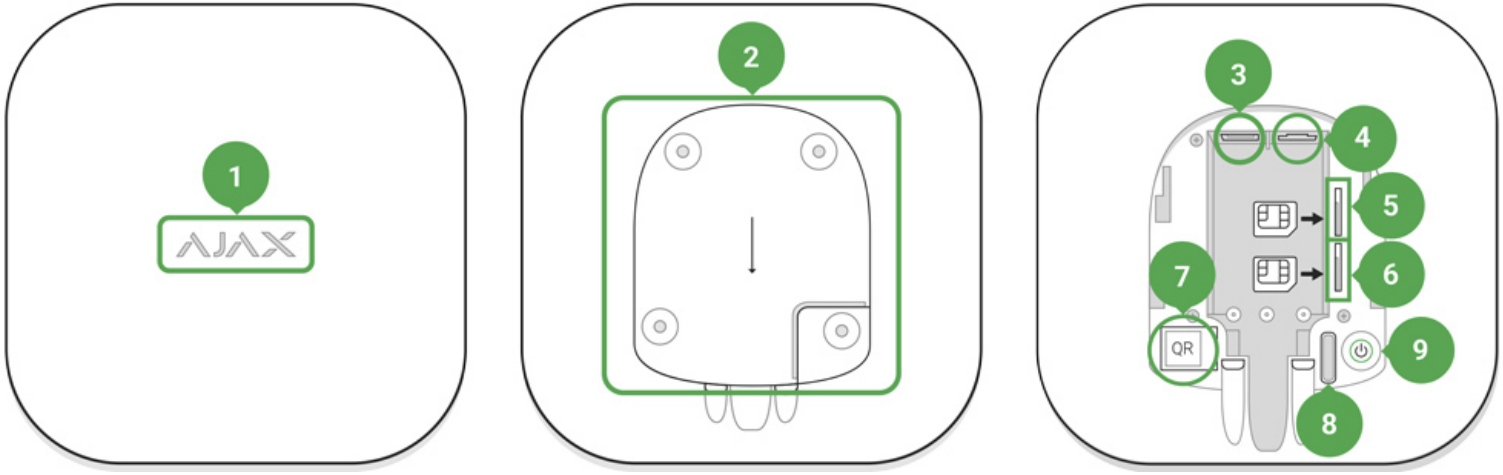
Vous pouvez gérer le système de sécurité et répondre rapidement aux alarmes et notifications grâce à des **app** pour iOS, Android, macOS et Windows. Le système vous permet de choisir les événements et la manière de les notifier à l'utilisateur : par des notifications push, des SMS ou des appels.

- **Comment configurer les notifications push sur iOS**
- **Comment configurer les notifications push sur Android**

Si le système est connecté à centre de télésurveillance, les événements et les alarmes seront transmis au centre de télésurveillance — **directement et/ou via Ajax Cloud**.

Achetez l'unité centrale du Hub 2 Plus

Éléments fonctionnels



1. Logo Ajax avec indicateur LED

2. Panneau de montage SmartBracket. Faites-le glisser vers le bas avec force pour l'ouvrir

> Une pièce perforée est nécessaire pour actionner l'anti-sabotage en cas de tentative de démontage du hub. Ne le cassez pas !

3. Prise du câble d'alimentation

4. Prise de câble Ethernet

5. Emplacement pour micro SIM 2
6. Emplacement pour micro SIM 1
7. Code QR
8. Bouton anti-sabotage
9. Bouton d'alimentation

Principe de fonctionnement

Le hub surveille le fonctionnement du système de sécurité en communiquant avec les appareils connectés via le **protocole crypté Jeweller**. La portée de communication peut atteindre 2000 m en champ ouvert (par exemple, murs, portes, constructions entre étages). Si le détecteur est déclenché, le système déclenche l'alarme en 0,15 seconde, active les sirènes et informe le centre de télésurveillance de l'organisme de sécurité et des utilisateurs.

En cas d'interférence sur les fréquences de fonctionnement ou de tentative de brouillage, Ajax passe sur une fréquence radio libre et envoie des notifications au centre de télésurveillance de l'organisme de sécurité et aux utilisateurs du système.

Qu'est-ce que le brouillage d'un système de sécurité sans fil et comment y résister

Hub 2 Plus prend en charge jusqu'à 200 appareils Ajax connectés, qui protègent contre les intrusions, les incendies et les inondations, et contrôlent les appareils électriques automatiquement selon des scénarios ou manuellement à partir d'une app.

Pour envoyer des photos à partir du détecteur de mouvement **MotionCam**, un protocole radio Wings distinct et une antenne dédiée sont utilisés. Cela permet d'assurer la prise de photos en

cas des alarmes même en cas de niveau de signal instable et d'interruptions de la communication.

Tous les appareils Ajax

Hub 2 Plus fonctionne sous un système d'exploitation OS Malevich en temps réel. Des systèmes d'exploitation similaires contrôlent les systèmes d'engins spatiaux, les missiles balistiques et les freins de voiture. OS Malevich étend les capacités du système de sécurité, en effectuant une **mise à jour automatique** par voie aérienne sans intervention de l'utilisateur.

Utilisez des **scénarios** pour automatiser le système de sécurité et réduire le nombre d'actions de routine. Établir la sécurité planifiée, programmer les actions des appareils d'automatisation (**Relay**, **WallSwitch** ou **Socket**) en réponse à une alarme, en appuyant sur le **Button** ou selon un planning. Un scénario peut être créé à distance dans l'app Ajax.

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

Indicateur LED



Le logo Ajax sur la façade du hub s’allume en rouge, blanc ou vert selon l’état de l’alimentation électrique et de la connexion Internet.

Événement	Indicateur LED
Au moins deux canaux de communication — Wi-Fi, Ethernet ou 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 l’Internet ou il n’y a pas de connexion avec le serveur Ajax Cloud	S’allume en rouge
Aucune alimentation	S’allume pendant 3 minutes, puis clignote toutes les 10 secondes. La couleur de l’indicateur dépend du nombre de canaux de communication connectés

Compte Ajax

Le système de sécurité est configuré et contrôlé par le biais **d'app Ajax**. Les applications Ajax sont disponibles pour les professionnels et les utilisateurs sur iOS, Android, macOS et Windows.

Les paramètres des utilisateurs du système de sécurité Ajax et les paramètres des appareils connectés sont stockés localement sur le hub et sont inextricablement liés à celui-ci. Le changement d'administrateur du hub ne réinitialise pas les paramètres des appareils connectés.

Pour configurer le système, installez l'app Ajax et **créez un compte**. Un seul numéro de téléphone et une seule adresse électronique peuvent être utilisés pour créer un seul compte Ajax ! Il n'est pas nécessaire de créer un nouveau compte pour chaque hub — un compte peut gérer plusieurs hubs.

> Votre compte peut combiner deux rôles : l'administrateur d'un hub et l'utilisateur d'un autre hub.

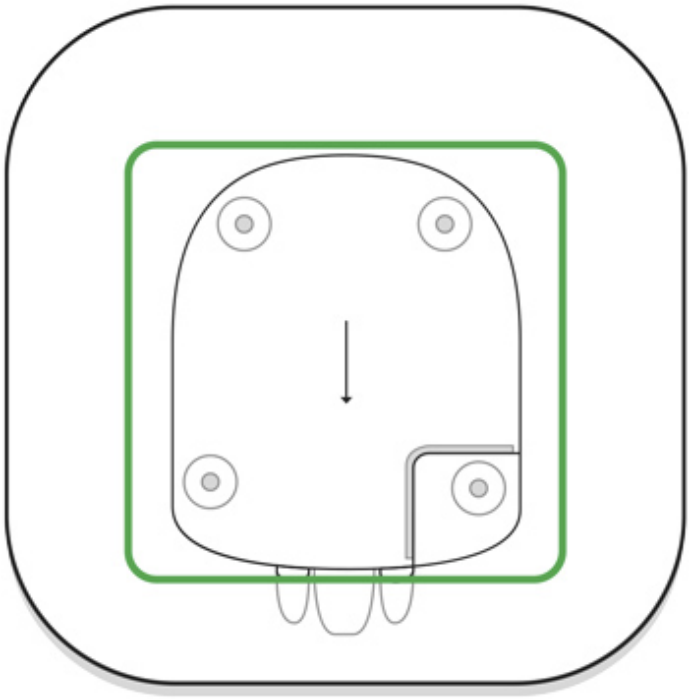
Exigences de sécurité

Lors de l'installation et de l'utilisation de Hub 2 Plus, respectez strictement les règles générales de sécurité électrique pour l'utilisation des appareils électriques, ainsi que les exigences des actes juridiques réglementaires sur la sécurité électrique.

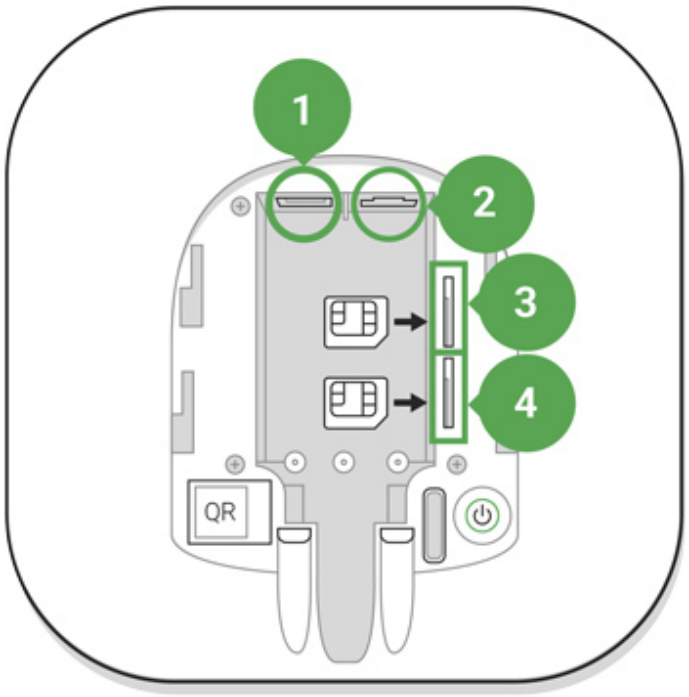
Il est strictement interdit de démonter l'appareil sous tension ! De plus, n'utilisez pas l'appareil avec un câble d'alimentation endommagé.

Se connecter au réseau

1. Retirez le panneau de montage du SmartBracket en le faisant glisser avec force vers le bas. Évitez d'endommager la partie perforée — c'est essentiel pour l'activation de l'anti-sabotage en cas de démontage du hub !



2. Branchez l'alimentation et les câbles Ethernet aux prises appropriées, installez les cartes SIM.



1 — Prise électrique
2 — Prise Ethernet
3, 4 — Emplacements pour l'installation de cartes micro-SIM

3. Appuyez et maintenez le bouton d'alimentation enfoncé pendant 3 secondes jusqu'à ce que le logo Ajax s'allume. Il faut environ 2 minutes au hub pour se mettre à niveau avec le dernier firmware et se connecter à l'Internet. La couleur verte ou blanche du logo indique que le hub fonctionne et est connecté au Cloud Ajax.

Si la connexion Ethernet n'est pas établie automatiquement, désactivez le filtrage des adresses proxy et MAC et activez le DHCP dans les paramètres du routeur. Le hub recevra automatiquement une adresse IP. Après cela, vous pourrez configurer une adresse IP statique du hub dans l'app Ajax.

4. Pour vous connecter au réseau cellulaire, vous avez besoin d'une micro carte SIM avec une demande de code PIN désactivé (vous pouvez le désactiver avec un téléphone portable) et un montant suffisant sur votre compte pour payer les services aux tarifs de votre opérateur. Si le hub ne se connecte pas au réseau cellulaire, utilisez Ethernet pour configurer les paramètres du réseau : itinérance, point d'accès APN, nom d'utilisateur et mot de passe. Contactez votre opérateur télécom pour obtenir de l'aide afin de connaître ces options.

Ajout d'un hub à l'app Ajax

1. Allumez le hub et attendez que le logo s'allume en vert ou en blanc.
2. Ouvrez l'app Ajax. Donner accès aux fonctions du système demandées pour utiliser pleinement les capacités de l'app Ajax et **ne pas manquer les alertes sur les alarmes ou les événements**.
   - Comment configurer les notifications sur iOS
   - Comment configurer les notifications sur Android
3. Ouvrez le menu **Ajouter hub** Sélectionnez le mode d'enregistrement : manuel ou guide pas à pas. Si vous installez le système pour la première fois, suivez les instructions étape par étape.
4. Précisez le nom du hub et scannez le code QR situé sous le panneau de montage du SmartBracket ou saisissez-le manuellement.
5. Attendez que le hub soit ajouté. Le hub lié sera affiché dans l'onglet **Appareils** .

Après avoir ajouté un hub à votre compte, vous devenez l'administrateur de l'appareil. Les administrateurs peuvent inviter d'autres utilisateurs au système de sécurité et déterminer leurs droits. L'unité centrale du Hub 2 Plus peut compter jusqu'à 200 utilisateurs.

La modification ou la suppression de l'administrateur ne réinitialise pas les paramètres du hub ou des appareils connectés.

Droits des utilisateurs du système de sécurité Ajax

États du Hub

Icônes

Les icônes affichent certains des états de Hub 2 Plus. Vous pouvez les voir dans l'app Ajax, dans le menu **Appareils** .

Icône	Valeur
	2G connecté
	3G connecté
	LTE 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 2 Plus. Affichage par tranches de 5%
	Le dysfonctionnement du Hub 2 Plus 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 2 Plus dans la liste.

Paramètre	Signification
Dysfonctionnement	Cliquez pour ouvrir la liste des dysfonctionnements de Hub 2 Plus. 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 :

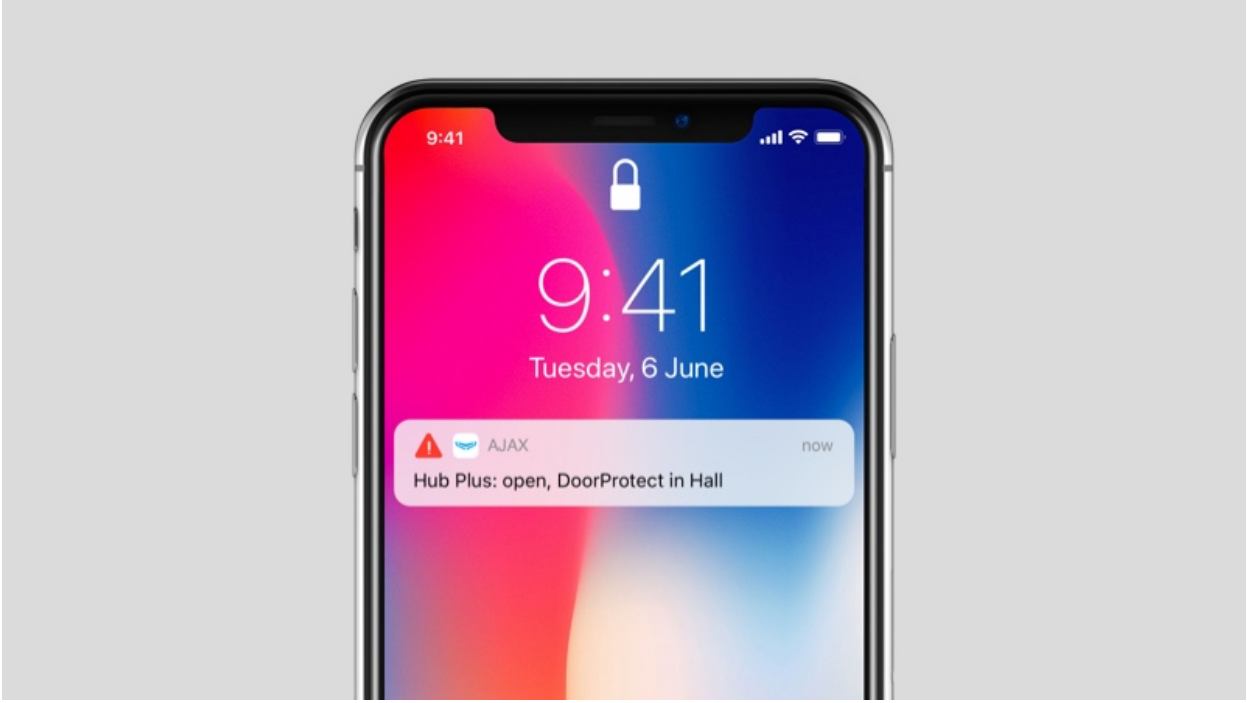
	• Fermé — le couvercle du hub est fermé • Ouvert — le hub a été retiré du support du SmartBracket **Qu'est-ce qu'un anti-sabotage ?**
Alimentation externe	État de la connexion de l'alimentation externe : • Connecté — le hub est connecté à une alimentation externe • Déconnecté — pas d'alimentation électrique 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
Actif	Affiche la carte SIM active : Carte SIM 1 ou carte SIM 2

Carte SIM 1	Le numéro de la carte SIM installée dans le premier emplacement. Copiez le numéro en cliquant dessus
Carte SIM 2	Le numéro de la carte SIM installée dans le deuxième emplacement. Copiez le numéro en cliquant dessus
Wi-Fi	État de la connexion Internet du hub via Wi-Fi. Pour une plus grande fiabilité, il est recommandé d'installer le hub dans des endroits où l'intensité du signal est de 2 à 3 bars
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)	Niveau de puissance sonore sur le site d'installation du hub. Les deux premières valeurs indiquent le niveau selon les fréquences de Jeweller, et la troisième — selon les fréquences de Wings. La valeur acceptable est de -80 dBm 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

Pièces

Avant de relier un détecteur ou un appareil à un hub, créez au moins une pièce. Les pièces sont utilisées pour regrouper les détecteurs et les appareils, ainsi que pour augmenter le contenu informatif des notifications. Le nom de l'appareil et de la pièce sera affiché dans le texte de l'événement ou de l'alarme du système de sécurité.



Pour créer une pièce dans l'app Ajax :

1. Allez à l'onglet **Pièces** .
2. Cliquez sur **Ajouter pièce**.
3. Attribuez un nom à la pièce, et éventuellement joignez ou prenez une photo : cela permet de trouver rapidement la pièce nécessaire dans la liste.
4. Cliquez sur **Enregistrer**.

Pour supprimer la pièce ou changer son avatar ou son nom, allez dans **paramètres Pièce** en appuyant sur ⚙.

Connexion de détecteurs et d'appareils

Hub n’est pas compatible avec les modules d’intégration uartBridge et ocBridge Plus.

Lorsque vous ajoutez un hub à votre compte à l’aide du guide étape par étape, vous serez invité à connecter des appareils au hub. Cependant, vous pouvez refuser et revenir à cette étape plus tard.

Pour ajouter un appareil au hub, dans l’app Ajax :

1. Ouvrez la pièce et sélectionnez **Ajouter appareil**.
2. Nommez l’appareil, scannez son code QR (ou saisissez-le manuellement), sélectionnez un groupe (si le mode groupe est activé).
3. Cliquez sur **Ajouter** — le compte à rebours pour l’ajout d’un appareil commence.
4. Suivez les instructions de l’app pour connecter l’appareil.

Veuillez noter que pour être relié au hub, l’appareil doit être situé dans la portée de communication radio du hub (au même endroit que l’objet protégé).

Réglages du hub

Les paramètres peuvent être modifiés dans **app Ajax** :

1. Aller à l’onglet **Appareils** .
2. Sélectionnez Hub 2 Plus 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

Wi-Fi — paramètres de la connexion Internet Wi-Fi. La liste générale affiche tous les réseaux disponibles pour le hub.

- Wi-Fi — vous permet d'activer et de désactiver le Wi-Fi sur le hub. Après avoir appuyé sur le [i] bouton, les paramètres du réseau s'ouvrent :

- 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
- Oubliez ce réseau — après avoir appuyé sur la touche, le hub supprime les paramètres du réseau et ne se connecte plus à celui-ci

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
- Carte SIM 2 — 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 (8 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 s	39 appareils
24 s	79 appareils
36 s	119 appareils
48 s	159 appareils
72 s	200 appareils

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

Le **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
- Wi-Fi
- 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 alarme Processus d'armement/désarmement 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 (sec).** 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 (sec).** 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 lorsque la connexion avec le serveur est perdue**. 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 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'armement/désarmement

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**, **UMTS/LTE** et **Wi-Fi**. 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.
- **Wi-Fi** — permet la transmission d’événements et d’alarmes par Wi-Fi.
- **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 2 Plus.

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

Réinitialisation du hub aux réglages d'usine :

1. Allumez le hub s'il est éteint.
2. Retirez tous les utilisateurs et installateurs du hub.
3. Maintenez le bouton d'alimentation enfoncé pendant 30 s, le logo Ajax sur le hub commence alors à clignoter en rouge.
4. Supprimez le hub de votre compte.



La réinitialisation du hub ne supprime pas les utilisateurs connectés !

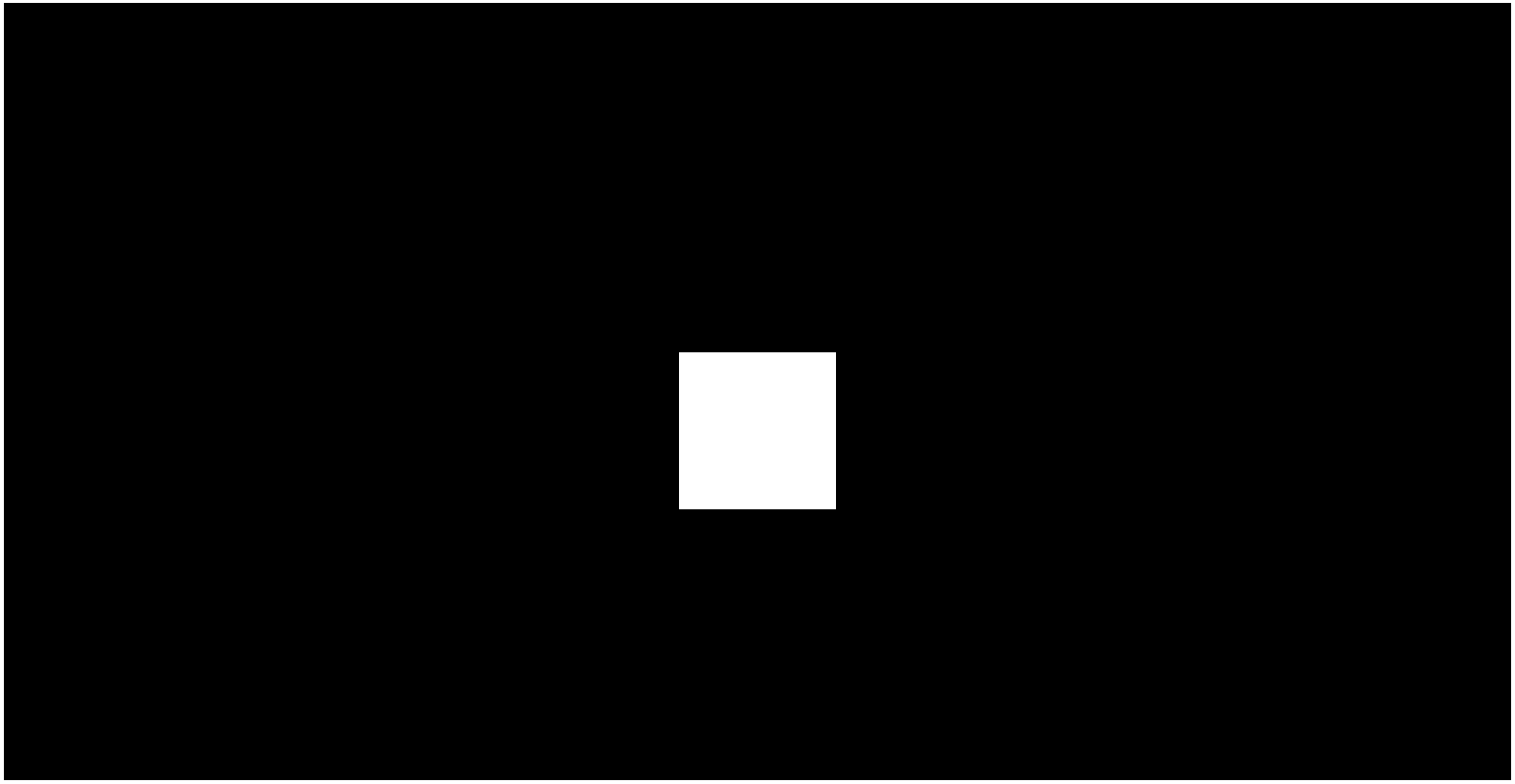
Notifications d'événements et d'alarmes

Le système de sécurité Ajax informe l'utilisateur des alarmes et des événements de trois manières : notifications push, SMS et appels téléphoniques. Les paramètres de notification ne peuvent être modifiés que pour les utilisateurs enregistrés.

Types d'événements	Objectif	Types de notifications
Dysfonctionnements	• Perte de connexion entre l'appareil et le hub • Brouillage • Charge de batterie faible dans l'appareil ou le hub • Masquage • Alarme anti-sabotage	Notifications push SMS
Alarme	• Intrusion • Incendie • Inondation • Perte de connexion entre le hub et le serveur Ajax Cloud	Appels Notifications push SMS
Événements	• Activation de **WallSwitch**, **Relay**, **Socket**	Notifications push SMS
Armer/Désarmer	• Armer/désarmer un objet ou un groupe entier • Activation du **mode Nuit**	Notifications push SMS

Comment Ajax informe les utilisateurs des alertes

Vidéosurveillance

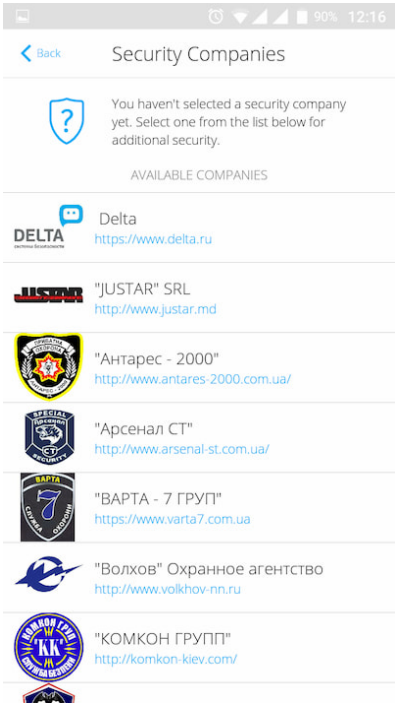


Vous pouvez connecter des caméras tierces au système de sécurité : une intégration transparente avec les caméras IP et les enregistreurs vidéo Dahua, Hikvision et Safire a été mise en place. Vous pouvez également connecter des caméras tierces supportant le protocole RTSP. Vous pouvez connecter jusqu'à 100 appareils de vidéosurveillance au système.

Comment ajouter une caméra au système de sécurité Ajax

Se connecter à un centre de télésurveillance

La liste des compagnies qui acceptent le système du centre de télésurveillance se trouve dans le menu **Centre de télésurveillance** (**Appareils** **Hub** **Paramètres** **Entreprises de sécurité**):



Sélectionnez un centre de télésurveillance et cliquez sur **Envoyer la demande de télésurveillance**. Ensuite, le centre de télésurveillance vous contactera et discutera des conditions de connexion. Ou vous pouvez les contacter vous-même (les contacts sont disponibles dans l'app) pour convenir d'une connexion.

La connexion au Centre de Télésurveillance (CMS) se fait via le protocole Contact ID ou SIA.

Installation

Avant d'installer le hub, assurez-vous que vous avez choisi l'emplacement optimal et qu'il est conforme aux exigences de ce manuel ! Il est souhaitable que le hub soit caché de la vue

directe.

Assurez-vous que la communication entre le hub et tous les appareils connectés est stable. Si l'intensité du signal est faible (une seule barre), nous ne pouvons pas garantir un fonctionnement stable du système de sécurité. Mettez en œuvre toutes les mesures possibles pour améliorer la qualité du signal ! Quoi qu'il en soit, déplacez le hub, car même un repositionnement de 20 cm peut améliorer considérablement la réception du signal.

Si l'intensité du signal est toujours faible ou instable après la relocalisation, utilisez **le prolongateur de portée du signal radio ReX**.

Lors de l'installation et de l'utilisation de l'appareil, suivez les règles générales de sécurité électrique pour l'utilisation des appareils électriques, ainsi que les exigences des lois 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.

Installation du hub :

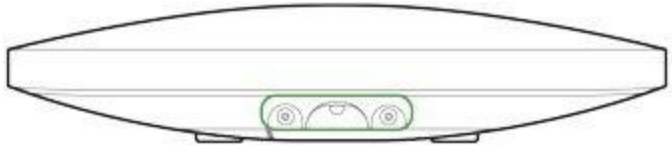
1. Fixez le panneau de montage SmartBracket à l'aide des vis groupées. Lorsque vous utilisez d'autres éléments de fixation, assurez-vous qu'ils n'endommagent pas ou ne déforment pas le panneau.

> ⚠ Nous ne recommandons pas d'utiliser une bande adhésif double face pour l'installation : elle peut provoquer la chute du hub en cas de choc.

2. Fixez le hub au panneau de montage. Après l'installation, vérifiez le mode tamper dans l'application Ajax et ensuite la qualité de la fixation du panneau. Vous recevrez une

notification si une tentative est faite pour arracher le hub de la surface ou le retirer du panneau de montage.

3. Fixez le hub sur le panneau du SmartBracket avec des vis groupées.



Ne retournez pas le hub lorsque vous le fixez verticalement (par exemple, sur un mur). Lorsqu'il est bien fixé, le logo Ajax peut être lu horizontalement.

Ne placez pas le hub :

- À l'extérieur des locaux (extérieur).
- A proximité ou à l'intérieur de tout objet métallique ou miroir provoquant l'atténuation et le filtrage du signal.
- Dans les endroits où le niveau d'interférence radio est élevé.
- Près des sources d'interférences radio : à moins d'un mètre (1) du routeur et des câbles électriques.
- A l'intérieur de tout local dont la température et l'humidité dépassent les limites autorisées.

Maintenance

Vérifiez régulièrement la capacité opérationnelle du système de sécurité Ajax. Nettoyez le boîtier du hub de la poussière, des toiles d'araignées et des autres contaminants dès leur apparition.

Utilisez une serviette douce et sèche adaptée 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 hub.

Comment remplacer la batterie du hub

Le paquet comprend

1. Hub 2 Plus
2. Panneau de montage SmartBracket
3. Câble d’alimentation
4. Câble Ethernet
5. Kit d’installation
6. Pack de démarrage – non disponible dans tous les pays
7. Guide rapide

Caractéristiques techniques

Classification	Panneau de contrôle du système de sécurité avec support Ethernet, Wi-Fi et double carte SIM
Prise en charge des détecteurs avec vérification photographique des alarmes	Disponible

Nombre d’appareils connectés	Jusqu’à 200
Nombre de ReX connectés	Jusqu’à 5
Nombre de groupes de sécurité	Jusqu’à 25
Nombre d’utilisateurs	Jusqu’à 200
Vidéosurveillance	Jusqu’à 100 caméras ou DVRs
Nombre de pièces	Jusqu’à 50
Nombre de scénarios	Jusqu’à 64 (Les réponses lors de l’armement et du désarmement du système ne sont pas comprises dans la limite générale des scénarios du hub)
Protocoles de communication du Centre de Télésurveillance	Contact ID, SIA Vérification photo intégrée dans Manitou, ABsistemDC(NG), WBB, Horus, V1/F1, Kronos, eLipse, Sentinel et SBN
Alimentation	110-240 V avec batterie préinstallée 6 V avec source d’alimentation alternative **6V PSU** Consommation d’énergie du réseau — 10 W
Batterie de secours intégrée	Li-Ion 3 A·h Fournit jusqu’à 15 heures d’autonomie sur une carte SIM
Consommation d’énergie du réseau	Jusqu’à 10 W
Protection anti-sabotage	Disponible, anti-sabotage
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	10,4 mW (max 25 mW)
Portée du signal radio	Jusqu'à 2000 m
Canaux de communication	2 cartes SIM • 2G (GSM900/DCS1800 (B3/B8)) • 3G (WCDMA 850/900/2100 (B1/B5/B8)) • LTE (FDD B1/B3/B5/B7/B8/B20/B28) Wi-Fi (802.11 b/g/n) Ethernet
Plage de températures de fonctionnement	De -10°C à +40°C
Humidité de fonctionnement	Jusqu'à 75%
Dimensions	163 × 163 × 36 mm
Poids	367 g

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 au batterie rechargeable groupée.

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

Obligations de garantie

Contrat d’utilisateur

Support technique : **support@ajax.systems**