Manuel d’utilisateur de Hub 2

Mis à jour November 4, 2021

Ajax est un système de sécurité sans fil qui protège contre les **intrusions**, les **incendies** et les **inondations**, et il permet aux utilisateurs de **contrôler les appareils électriques** directement depuis une **application mobile**. Le système réagit immédiatement aux menaces en vous informant, vous et l’entreprise de sécurité, de tous les incidents. Conçu pour être utilisé à l’intérieur.

Hub 2 est un panneau de contrôle de système de sécurité intelligent qui prend en charge les détecteurs avec vérification photo des intrusions. Élément clé du

système de sécurité, il contrôle le fonctionnement des appareils Ajax et, en cas de menace, communique immédiatement les signaux d'alarme pour informer le propriétaire et le centre de télésurveillance de ces incidents.

Hub 2 nécessite une connexion Internet afin d'accéder au service Ajax Cloud pour la configuration et la gestion du système depuis n'importe quel endroit dans le monde via les applications Ajax, la communication des alarmes et des événements, et la mise à jour du firmware d'**OS Malevich**. Toutes les données sont stockées dans un système à plusieurs niveaux de sécurité et l'échange d'informations avec la centrale s'effectue via un canal sécurisé.

Afin de communiquer avec le service Ajax Cloud, la centrale utilise une connexion Internet filaire (Ethernet) et deux cartes SIM 2G. Il est recommandé d'utiliser tous les réseaux de communication afin d'assurer une connexion plus fiable avec le service Ajax Cloud et de se prémunir contre la défaillance de l'un des fournisseurs de services.

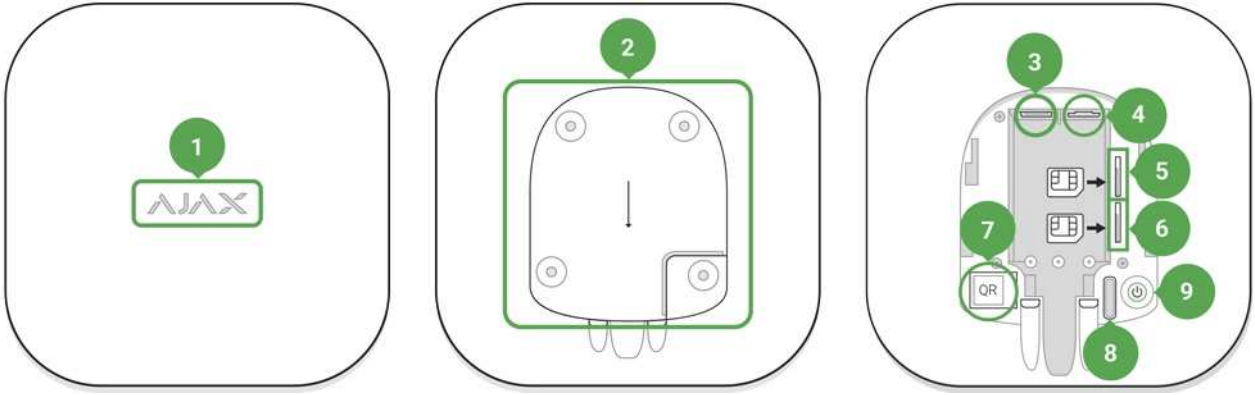
Les utilisateurs peuvent gérer le système de sécurité et répondre rapidement aux alarmes et aux notifications à l'aide d'**applications** conçues pour iPhone et smartphones fonctionnant sous Android, macOS et Windows. Le système notifie les alarmes et autres événements à l'aide de notifications directes, de SMS et d'appels téléphoniques.

Utilisez des scénarios pour automatiser le système de sécurité et réduire le nombre d'actions de routine. Réglez le système de sécurité, programmez les actions automatisées (Relay, WallSwitch ou Socket) en réponse à une alarme, en appuyant sur Button ou par programmation. Un scénario peut être créé à distance dans l'application Ajax.

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

Achetez le panneau de contrôle de sécurité intelligent Hub 2

Éléments fonctionnels



1. Logo Ajax avec indicateur lumineux
2. Panneau de montage SmartBracket (glissez avec force vers le bas pour ouvrir ; la section perforée est nécessaire pour déclencher l'anti-sabotage lors des tentatives d'arrachement de la centrale de la surface. Ne le cassez pas !)
3. Connecteur de câble d'alimentation
4. Connecteur de câble Ethernet
5. Emplacement pour l'installation d'une carte micro-SIM
6. Emplacement pour l'installation d'une carte micro-SIM
7. Code QR
8. Bouton anti-sabotage
9. Bouton d'alimentation

Principes de fonctionnement de Hub 2

La centrale recueille les informations relatives au fonctionnement des appareils connectés sous forme sécurisée, analyse les données et, en cas d'alarme, informe le propriétaire du système du danger en moins d'une seconde et communique l'alarme directement au centre de télésurveillance de l'entreprise de sécurité.

Afin de communiquer avec les appareils, de surveiller leur fonctionnement et de réagir rapidement aux menaces, Hub 2 utilise la technologie radio **Jeweller**. Pour la transmission visuelle de données, Hub 2 utilise le protocole radio Ajax Wings. Il s'agit d'un protocole haut débit basé sur la technologie Jeweller. Wings utilise également une antenne dédiée pour améliorer la fiabilité du canal.

Tous les appareils Ajax

Indicateur LED de la centrale

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 réseau de communication est connecté	S'allume en vert
La centrale n'est pas connectée 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 10 secondes. La couleur de l'indicateur dépend du nombre de réseaux de communication connectés.

Compte Ajax

Le système de sécurité est configuré et géré via des applications Ajax conçues pour iPhone et smartphones fonctionnant sous Android, macOS et Windows.

Pour configurer le système, installez l'**application Ajax** et créez un compte. Nous vous recommandons d'utiliser l'application Ajax Security System pour gérer un ou plusieurs centrales. Si vous envisagez de gérer plus d'une centaine de centrales, nous vous recommandons d'utiliser l'application **Ajax PRO: Tool for Engineers** (pour iPhone et smartphones fonctionnant sous Android) ou **Ajax PRO Desktop** (pour les ordinateurs de bureau et les ordinateurs portables fonctionnant sous Windows et macOS). Vous devrez confirmer votre adresse électronique et votre numéro de téléphone dans le cadre du processus. Notez que vous pouvez utiliser votre numéro de téléphone et votre adresse électronique pour créer un seul compte Ajax! Vous n'avez pas besoin de créer un nouveau compte pour chaque centrale, vous pouvez ajouter plusieurs centrales à un seul compte.

Un compte contenant des informations sur les centrales ajoutés est téléchargé vers le service Ajax Cloud basé sur le cloud sous une forme sécurisée.

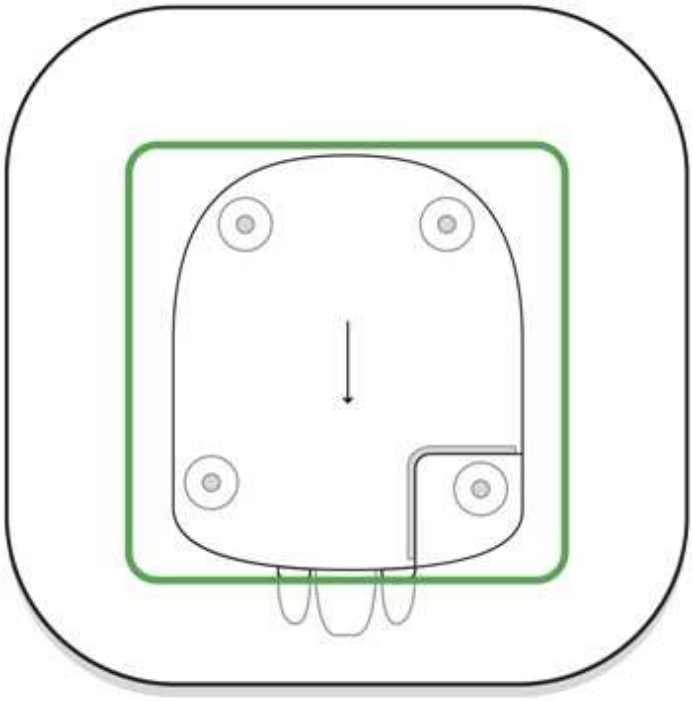
Exigences de sécurité

Lors de l'installation et de l'utilisation de Hub 2, respectez les règles générales de sécurité électrique pour l'utilisation des appareils électriques ainsi que les exigences des prescriptions de sécurité électrique.

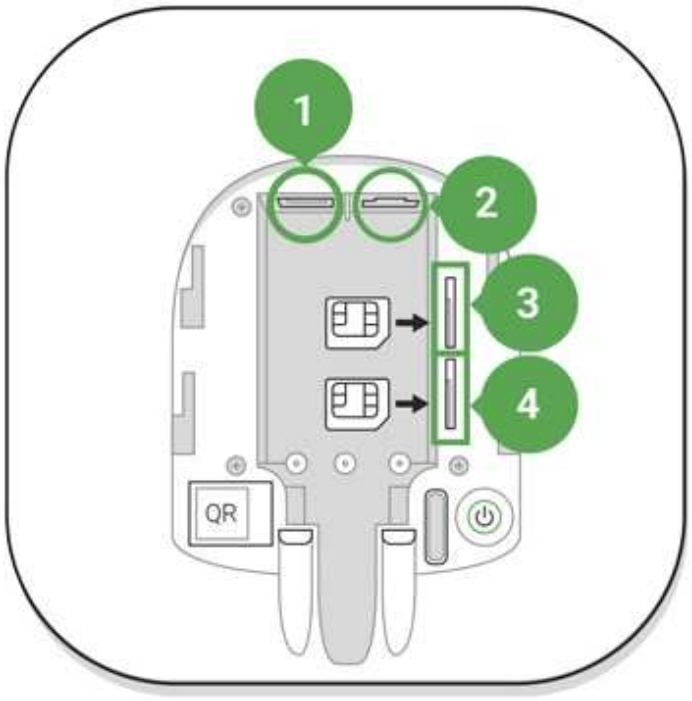
Il est strictement interdit de démonter l'appareil raccordé à l'alimentation électrique ! De plus, n'utilisez pas l'appareil avec un cordon d'alimentation endommagé.

Raccordement de la centrale

1. Retirez le couvercle de la centrale en le faisant glisser de force vers le bas. N'endommagez pas la partie perforée qui est nécessaire pour déclencher le bouton anti-sabotage lors d'une tentative de sabotage de la centrale!



2. Branchez le cordon d’alimentation et le câble Ethernet sur les connecteurs correspondants.



1 — Connecteur de cordon d’alimentation
2 — Connecteur Ethernet
3, 4 — Fentes pour 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 jusqu’à 2 minutes à la centrale pour mettre à jour la dernière version du firmware et accéder à

Internet. La couleur verte ou blanche du logo indique que la centrale fonctionne et qu'il est connecté au service Ajax Cloud.

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

4. Pour vous connecter via GSM, vous avez besoin d'une carte micro SIM émise par un opérateur mobile dont la demande de code PIN est désactivée (vous pouvez la désactiver avec un téléphone portable) et d'un solde suffisant sur le compte pour payer les services de l'opérateur mobile. Si la centrale n'est pas connectée via GSM, utilisez Ethernet pour configurer les réglages de l'opérateur réseau (réglages d'itinérance, points d'accès APN, nom d'utilisateur et mot de passe). Pour connaître les réglages de votre opérateur de téléphonie mobile, contactez le service d'assistance de votre fournisseur de services.

Ajout d'une centrale à l'application Ajax

1. Entrez dans l'application Ajax. Assurez-vous de lui accorder l'accès à toutes les fonctions système demandées, en particulier les autorisations d'afficher les notifications. Si vous utilisez un smartphone fonctionnant sous Android, nous vous recommandons d'utiliser les **instructions de configuration des notifications directes**.
2. Connectez-vous à votre compte et cliquez sur **Ajouter une centrale**. Choisissez une méthode appropriée, manuellement ou à l'aide d'un guide étape par étape. Si vous configurez le système pour la première fois, nous vous recommandons d'utiliser le guide étape par étape.
3. Spécifiez le nom de la centrale et scannez le code QR situé sous le couvercle ou saisissez-le manuellement.
4. Attendez que le processus d'ajout de la centrale soit terminé. Après la liaison, la centrale sera affichée dans l'onglet **Appareils** .

Utilisateurs du système de sécurité

Lorsque vous ajoutez une centrale à votre compte, vous devenez l'administrateur de cet appareil. Une seule centrale peut accueillir jusqu'à 50

utilisateurs/administrateurs. L'administrateur invite les utilisateurs à utiliser le système de sécurité et détermine leurs droits.

Changer l'administrateur du système de sécurité et le retirer de la centrale n'entraînera pas la réinitialisation des appareils qui y sont connectés.

Droits des utilisateurs du système de sécurité Ajax

États de la centrale

Icônes

Les icônes affichent certains des états de Hub 2. Vous pouvez les voir dans l'application 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 2. Affichage par tranches de 5%
	Le dysfonctionnement du Hub 2 est détecté. La liste est disponible dans la liste des États du Hub
	La centrale est directement relié au centre de télésurveillance de l'organisme de sécurité
	La centrale 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'**application Ajax** :

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

Paramètre	Signification
Dysfonctionnement	Cliquez (i) pour ouvrir la liste des dysfonctionnements de Hub 2. 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 la centrale dans des endroits où l'intensité du signal est de 2 à 3 barres. Si l'intensité du signal est faible, la centrale ne pourra pas appeler ou envoyer un SMS concernant un événement ou une alarme
Charge de la batterie	Niveau de charge de la batterie d'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 de la centrale : • **Fermé** — le couvercle de la centrale est fermé • **Ouvert** — la centrale a été retirée du support du SmartBracket **Qu'est-ce qu'un bouton anti-sabotage ?**
Alimentation externe	État de la connexion de l'alimentation externe : • **Connecté** — la centrale est connectée à une alimentation externe • **Déconnecté** — pas d'alimentation électrique externe
Connexion	État de connexion entre la centrale et Ajax Cloud : • **En ligne** — la centrale est connecté à Ajax Cloud

	• **Hors ligne** — la centrale n'est pas connecté à Ajax Cloud
Réseau Mobile	L'état de la connexion de la centrale à l'Internet mobile : • **Connecté** — la centrale est connectée à Ajax Cloud via l'Internet mobile • **Déconnecté** — la centrale n'est pas connectée à Ajax Cloud via l'Internet mobile Si la centrale 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
Ethernet	État de la connexion Internet de la centrale via Ethernet : • **Connecté** — la centrale est connectée à Ajax Cloud via Ethernet • **Déconnecté** — la centrale n'est pas connectée à Ajax Cloud via Ethernet
Bruit moyen (dBm)	Niveau de puissance sonore sur le site d'installation de la centrale. 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 de la centrale au centre de télésurveillance de l'organisme de sécurité :

	• **Connecté** — la centrale est directement reliée au centre de télésurveillance de l'organisme de sécurité • **Déconnecté** — la centrale n'est pas directement connectée 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 de la centrale	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

Ajouter une pièce

Avant de lier l'appareil à la centrale, créez au moins une pièce.

La description de l'événement de l'appareil spécifie la pièce dans laquelle l'appareil est situé:

Pour créer une pièce, allez dans l'onglet **Pièces** puis cliquez sur **Ajouter une pièce**. Attribuez-lui un nom et, si nécessaire, joignez (ou prenez) une photo, il sera alors plus facile de trouver une pièce dans la liste.

Pour supprimer une pièce, ou changer son avatar ou son nom, allez dans les réglages de la pièce (cliquez sur l'icône d'engrenage).

Connexion de détecteurs et d'appareils

Centrale n'est pas compatible avec les modules d'intégration uartBridge et ocBridge Plus.

Lors de l'ajout d'une centrale à l'aide d'un guide étape par étape, vous êtes invité à ajouter des appareils qui protégeront les lieux. Mais vous pouvez refuser et revenir à cette étape plus tard.

Pour ajouter un appareil à la centrale:

1. Dans l'application Ajax, ouvrez la pièce et sélectionnez **Ajouter un appareil**.
2. Attribuez un nom à l'appareil, scannez son code QR (ou saisissez-le manuellement), sélectionnez un Groupe (si le mode groupe est activé).
3. Cliquez sur **Ajouter** et le compte à rebours pour ajouter un appareil démarre.

4. Allumez l'appareil pendant le compte à rebours et sa LED s'allume une fois. Pour lier un appareil à la centrale, celui-ci doit être situé dans la zone de communication radio de la centrale (dans les mêmes locaux sécurisés).

En cas d'échec de la connexion, éteignez l'appareil pendant 5 secondes puis réessayez.

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

Vidéosurveillance

Vous pouvez connecter des caméras tierces au système de sécurité : une intégration transparente avec les caméras et enregistreurs vidéo IP Dahua, Hikvision et Safire a été mise en œuvre, et vous pouvez aussi connecter des caméras tierces supportant le protocole RTSP. Vous pouvez connecter jusqu'à 25 appareils de vidéosurveillance au système.

> **Comment ajouter une caméra Dahua ou un enregistreur vidéo à la centrale**

> **Comment ajouter une caméra Hikvision/Safire ou un enregistreur vidéo à la centrale**

Paramètres de centrale

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

1. Aller à l'onglet **Appareils** .
2. Sélectionnez Hub 2 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 de la centrale 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 de la centrale. 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 saisissez le nom souhaité de la centrale.

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 à la centrale**

Ethernet — paramètres de la connexion Internet filaire.

- Ethernet — vous permet d'activer et de désactiver Ethernet sur la centrale

- DHCP / Statique — sélection du type d'adresse IP de la centrale à recevoir : dynamique ou statique
- Adresse IP — Adresse IP de la centrale
- Masque de sous-réseau — masque de sous-réseau dans lequel la centrale fonctionne
- Routeur — passerelle utilisée par la centrale
- DNS — DNS de la centrale

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

- Données mobiles — désactivation et activation des cartes SIM sur la centrale
- Itinérance — si elle est activée, les cartes SIM installées dans la centrale peuvent fonctionner en itinérance
- Ignorer l'erreur d'enregistrement du réseau — lorsque ce paramètre est activé, la centrale 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, la centrale 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 la centrale

Utilisation de données mobiles

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

> N'oubliez pas que les données dépendent de la centrale 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 crédit** pour envoyer une demande. Le résultat sera affiché sous le bouton.

Géorepérage — 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'un géorepérage et comment fonctionne-t-il ?

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.

> **Comment activer et configurer le mode Groupe dans le système de sécurité Ajax**

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 la période d'interrogation pour la centrale et les appareils connectés. Les réglages déterminent à quelle fréquence la centrale échange des données avec les appareils et à quelle vitesse la perte de communication est détectée.

En savoir plus

- **Intervalle de ping du détecteur, sec** — la fréquence d'interrogation des appareils connectés par la centrale 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, sec** — un compteur de paquets non livrés (8 paquets par défaut).

Le délai avant le déclenchement de l'alarme par la perte de communication entre la centrale 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 la centrale 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 ou plus	100 appareils

Quels que soient les paramètres, la centrale supporte 10 sirènes connectées au maximum !

Le **Service** est un groupe de paramètres de service de la centrale. Ils sont divisés en 2 groupes : les paramètres généraux et les paramètres avancés.

Paramètres généraux

Fuseau horaire

Sélection du fuseau horaire dans lequel fonctionne la centrale. 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 de la centrale. 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'application proposera de mettre à jour l'OS Malevich.

En quoi consistent les mises à jour d'OS Malevich

Logs de la centrale

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 réseau de transmission pour les journaux de la centrale 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 de la centrale dépend du type d'application : standard ou PRO.

Ajax Security System	Ajax PRO
Connexion au serveur Paramètres des sirènes Paramètres des détecteurs d'incendie Vérification de l'intégrité du système	Assistant de configuration PD 6662 Connexion au serveur Paramètres des sirènes Paramètres des détecteurs d'incendie Vérification de l'intégrité du système Confirmation d'alarme Restauration 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 au serveur

Le menu contient les paramètres de communication entre la centrale et Ajax Cloud :

- **Intervalle de ping du serveur, sec.** Fréquence d'envoi des pings depuis la centrale vers le serveur Ajax Cloud. Il est fixé dans une plage de 10 à 300 secondes. La valeur par défaut recommandée est de 60 secondes.
- **Temporisation d'alarme concernant l'échec de connexion au serveur, 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 secondes. La valeur par défaut recommandée est de 300 secondes.

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

*(Intervalle ping * 4) + Filtre temporel*

Avec les paramètres par défaut, Ajax Cloud signale la perte de la centrale en 9 minutes :

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

- **Recevoir des notifications de perte de connexion au serveur sans alarme**. Les applications Ajax peuvent avertir de la perte de communication entre la centrale et le serveur de deux façons : par un signal standard de notification push ou par un son de la sirène (activé par défaut). Lorsque l'option est active, la notification est accompagnée d'un signal standard de notification push.
- **Notifier de perte de connexion sur un réseau**. Le système de sécurité Ajax peut notifier la perte de connexion même via un seul réseau de communication : aux utilisateurs et au centre de télésurveillance à la fois.

Dans ce menu, vous pouvez choisir les réseaux de communication via lesquels le système notifiera la perte de connexion, ainsi que la temporisation d'envoi de ces notifications :

  - Ethernet
  - Réseau cellulaire

- **Temporisation à l'envoi d'une notification, min** – délai avant l'envoi d'une notification de perte de connexion via l'un des réseaux de communication. Elle peut être définie dans la plage de 3 à 30 minutes.

Le temps d'envoi d'une notification de perte de connexion avec un des réseaux de télécommunication est calculé à l'aide de la formule :

*(Intervalle ping * 4) + Filtre temporel + Temporisation à l'envoi d'une notification*

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 la centrale ou le boîtier du détecteur est ouvert. S'il est activé, la centrale active les **sirènes** connectées si le boîtier de la centrale, du détecteur ou de tout autre appareil Ajax est ouvert.

Si un bouton panique est appuyé dans l'app. Lorsque la fonction est active, la centrale active les sirènes connectées si le bouton de panique a été appuyé dans l'application 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 applications Ajax PRO

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'alarme des détecteurs d'incendie FireProtect.

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/KeyPad Plus.

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 applications Ajax PRO

La **Confirmation d’alarme** est un événement spécial que la centrale 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 d’interventions sur les fausses alarmes.

En savoir plus

Restauration après alarme

Ce paramètre n’est disponible que dans les applications Ajax PRO

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 applications Ajax PRO

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 applications Ajax PRO

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 minuteur 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 de la centrale.

Centre de télésurveillance — les réglages pour une connexion directe au centre de télésurveillance. Les paramètres sont fixés par les ingénieurs du

centre de 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 la centrale 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 (centrale).

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.

Réseaux d'envoi d'alarme

Dans ce menu, les réseaux d'envoi des alarmes et des événements au centre de télésurveillance sont sélectionnés. Hub 2 peut envoyer des alarmes et des événements au centre de télésurveillance via **Ethernet** et **EDGE**. Nous vous recommandons d'utiliser tous les réseaux 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, la centrale envoie des rapports de test avec une période donnée au 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 sécurisés.
- **Clé de cryptage** — clé de chiffrement 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 à la centrale

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.

Importation des données — un menu permettant de transférer automatiquement des appareils et des paramètres depuis une autre centrale. **Notez que vous êtes dans les paramètres de centrale dans laquelle vous voulez importer des données.**

En savoir plus sur l'importation des données

Dissocier la centrale — supprime votre compte de la centrale. Indépendamment de cela, tous les réglages et les détecteurs connectés restent enregistrés.

Réinitialisez les réglages de la centrale

Réinitialisez la centrale sur les réglages d'usine:

1. Allumez la centrale si elle est éteinte.
2. Retirez tous les utilisateurs et installateurs de la centrale.
3. Maintenez le bouton d'alimentation enfoncé pendant 30 secondes, le logo Ajax sur la centrale commence alors à clignoter en rouge.
4. Supprimez la centrale de votre compte.

Alerte sur les événements et les alarmes

Le système de sécurité Ajax informe l'utilisateur des alertes et des événements à l'aide de trois types de notifications: notifications push, SMS et appels téléphoniques. Les réglages d'alerte ne peuvent être modifiés que pour les utilisateurs enregistrés.

Types de événements	Objectif	Types de notifications
Dysfonctionnements	• Perte de connexion entre l'appareil et la centrale • Brouillage • Charge de batterie faible dans l'appareil ou dans la centrale • Masquage • Sabotage du boîtier du détecteur	Notifications push SMS
Alarme	• Intrusion • Incendie • Inondation • La central a perdu la connexion avec le service Ajax Cloud	Appels Notifications push SMS
Événements	• Mise en marche/arrêt de	Notifications push

	WallSwitch, Relay, Socket	SMS
Armer/Désarmer	• Armer/désarmer l'ensemble des locaux ou du groupe • Activation du mode Nuit	Notifications push SMS

Comment Ajax informe les utilisateurs des alarmes

La centrale n'informe pas les utilisateurs du déclenchement des détecteurs d'ouverture en mode Désarmé, lorsque la fonction Carillon d'entrée est activée et configurée. Seules les sirènes connectées au système avertiront de l'ouverture.

Qu'est que le Carillon d'entrée

Se connecter à une entreprise de sécurité

La liste des organisations qui connectent le système aux centrales de télésurveillance des organisations se trouve dans le menu **Entreprises de sécurité** (**Appareils** → **Centrale** → **Réglages** → **Entreprises de sécurité**).

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

La connexion à la centrale de télésurveillance est réalisée via le protocole Contact ID ou SIA.

Montage

Avant d'installer la centrale, assurez-vous que vous avez choisi l'emplacement optimal et qu'il est conforme aux exigences de ces instructions ! Veillez à ce que la centrale soit à l'abri des regards indiscrets.

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

Assurez-vous que l'intensité du signal de la centrale est stable avec tous les appareils connectés. Si l'intensité du signal est faible (une seule barre), nous ne garantissons pas un fonctionnement stable du système de sécurité. Appliquez des mesures potentielles pour améliorer la qualité du signal ! Au minimum, déplacez la centrale, car même un repositionnement de 20 cm peut améliorer considérablement la réception du signal.

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

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

Installation de la centrale:

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

   Il n'est pas recommandé d'utiliser du ruban adhésif double face pour le montage. Cela peut entraîner la chute d'une centrale et la défaillance de l'appareil en cas d'impact.

2. Fixez la centrale au panneau de montage. Après l'installation, vérifiez le mode Sabotage dans l'application Ajax, puis vérifiez si le panneau est bien fixé.
3. Afin d'assurer une plus grande fiabilité, fixez la centrale à la plaque à l'aide des vis fournies.

Ne retournez pas la centrale lorsqu'une installation verticale (par exemple, sur un mur). Avec une bonne fixation, le logo Ajax se lit horizontalement.

Vous recevez une notification si vous tentez de retirer la centrale de la surface ou de la retirer du panneau de montage.

Il est strictement interdit de démonter l'appareil raccordé à l'alimentation électrique ! N'utilisez pas l'appareil avec un cordon d'alimentation endommagé.

Ne démontez pas ou ne modifiez pas la centrale ou l'une de ses pièces individuelles – cela pourrait interférer avec le fonctionnement normal de l'appareil ou le faire tomber en panne.

Ne placez pas la centrale:

- En dehors de la pièce (à l'extérieur).
- Près d'objets métalliques et de miroirs qui atténuent ou masquent les signaux radio.
- Dans les 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 des pièces où l'humidité et la température dépassent les limites autorisées.

Maintenance du système Ajax

Vérifiez régulièrement le fonctionnement du système de sécurité Ajax. Nettoyez le boîtier de la poussière, des toiles d'araignée et d'autres contaminants à mesure qu'ils se produisent. Utilisez un chiffon doux et sec qui convient à l'entretien de l'équipement.

N'utilisez pas de substances qui contiennent de l'alcool, de l'acétone, de l'essence ou d'autres solvants actifs.

Comment remplacer la batterie de la centrale

Le kit comprend

1. Hub 2
2. Câble alimentation

3. Câble Ethernet
4. Kit d’installation
5. Carte SIM (pas disponible dans tous les pays)
6. Guide rapide

Caractéristiques techniques

Classification	Panneau de contrôle du système de sécurité intelligent prenant en charge Ethernet et deux cartes SIM
Nombre maximum d’appareils connectés	Jusqu’à 100
ReX connectés	Jusqu’à 5
Nombre de sirènes connectées	jusqu’à 10
Groupes de sécurité	Jusqu’à 9
Utilisateurs du système de sécurité	Jusqu’à 50
Vidéosurveillance	Jusqu’à 25 caméras ou enregistreurs vidéo
Pièces	Jusqu’à 50
Scénarios	Jusqu’à 32 **En savoir plus**
Protocoles de communication du centre de télésurveillance	Contact ID, SIA (DC-09) **Centres de télésurveillances prenant en charge la vérification visuelle des alarmes**
Alimentation	110-240 V avec batterie préinstallée 12 V avec source d’alimentation alternative **12V PSU** 6 V avec source d’alimentation alternative **6V PSU**Consommation d’énergie du réseau — 10 W
Batterie de secours intégrée	Li-Ion 2 A·h Fournit jusqu’à 16 heures d’autonomie sur une carte SIM

Consommation d’énergie du réseau	10 W
Protection anti-sabotage	Disponible, bouton anti-sabotage
Bande de fréquences de fonctionnement	868,0 – 868,6 MHz ou 868,7 – 869,2 MHz, selon la région de vente
Puissance du signal radio	8.20 dBm / 6.60 mW (limite 25 mW)
Modulation du signal radio	GFSK
Portée du signal radio	Jusqu’à 2000 m (en champ ouvert) **En savoir plus**
Réseaux de communication	• 2 cartes SIM (GSM 850/900/1800/1900 MHz GPRS) • Ethernet
Installation	Intérieur
Température d’exploitation	De -10°C à +40°C
Humidité admissible	Jusqu’à 75%
Dimensions	163 × 163 × 36 mm
Poids	362 g
Durée de vie	10 années

Conformité aux normes

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 préinstallé.

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!

Garantie

Contrat d’utilisation

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