SÉCURITÉ ET VIE PRIVÉE

Votre système d'alarme Ajax est-il sûr ?

Un aperçu des mesures de sécurité du système d'alarme Ajax installé par Brepoels Security, et des règles qui déterminent qui a accès à votre système.

En bref

- La communication sans fil entre les détecteurs et la centrale est chiffrée et chaque appareil est vérifié à chaque contact.
- La centrale communique avec Ajax Cloud via une connexion chiffrée et peut utiliser plusieurs connexions à la fois.
- Le brouillage du signal radio et le sabotage sont détectés et signalés.
- Vous décidez vous-même qui peut utiliser le système et qui a accès aux paramètres.
- **Un installateur n'a accès aux paramètres qu'avec les droits que vous lui accordez.**

1. Communication sans fil chiffrée

Les détecteurs, sirènes et organes de commande communiquent avec la centrale (hub) via Jeweller, le protocole radio propre à Ajax :

- Les données sont chiffrées par un chiffrement par blocs. Une nouvelle clé est générée pour chaque session entre un appareil et la centrale.
- Chaque appareil est authentifié à chaque contact. La centrale ignore les signaux des appareils qui ne réussissent pas ce contrôle. Les appareils et les signaux ne peuvent donc pas être imités, par exemple avec une télécommande falsifiée.
- Un message est répété jusqu'à ce que la centrale confirme sa réception.
- Les appareils se signalent à la centrale à intervalle fixe (réglable de 12 à 300 secondes), avec leur niveau de batterie, leur température et la force du signal. Si un appareil ne répond plus, la centrale envoie une notification.

2. Connexion à Ajax Cloud et au centre de télésurveillance

- La centrale échange des données avec le serveur Ajax Cloud via un protocole de communication propriétaire chiffré. Le chiffrement AES-128 de cette connexion a été validé par le NIST, le National Institute of Standards and Technology américain. L'authentification protège le serveur contre les centrales usurpées.
- Selon Ajax, Ajax Cloud fonctionne dans plusieurs centres de données d'Amazon Web Services.
- Le serveur vérifie régulièrement que la centrale est toujours connectée. Avec les réglages les plus courts, les utilisateurs et la société de sécurité sont avertis environ 60 secondes après la perte de connexion.
- Si le système est raccordé à un centre de télésurveillance, l'alarme peut y être envoyée directement, sans passer par Ajax Cloud.

Brepoels Security · Bremakker 37, 3740 Bilzen · 089 39 08 99 · info@groupbrepoels.com · TVA BE 1021.926.276
Entreprise agréée par le SPF Intérieur pour les systèmes d'alarme et de vidéosurveillance n° 1021.926.276

3. Protection contre le brouillage et le sabotage

- La centrale et les appareils mesurent en permanence le bruit sur les fréquences radio. En cas de brouillage, les utilisateurs et la société de sécurité sont avertis et la centrale passe sur une fréquence moins perturbée.
- Selon le modèle, la centrale utilise plusieurs connexions : Ethernet, une ou deux cartes SIM et, pour certains modèles, le Wi-Fi. Si l'une tombe, la centrale continue via les autres.
- Si toutes les connexions tombent, la centrale enregistre les alarmes, déclenche les sirènes et envoie les événements enregistrés dès que la connexion est rétablie.
- La centrale dispose d'un contact d'autoprotection : si elle est retirée de sa plaque de montage, une notification est envoyée immédiatement, même lorsque le système est désarmé.
- En cas de coupure de courant, une batterie de secours prend le relais. Son autonomie dépend du modèle et de la configuration.

4. Logiciel de la centrale

- La centrale fonctionne avec OS Malevich, un système d'exploitation temps réel développé par Ajax. Selon Ajax, il est protégé contre les virus et les cyberattaques.
- Les mises à jour se font automatiquement via internet, uniquement lorsque le système est désarmé. Le fichier de mise à jour est chiffré ; selon Ajax, même le serveur n'en connaît pas les clés.

5. Vous décidez qui a accès

L'administrateur (admin) du système détermine qui peut utiliser le système et qui peut modifier les paramètres.

- Ajax distingue les administrateurs, les utilisateurs ordinaires (armer et désarmer, recevoir les alarmes) et les comptes PRO destinés aux installateurs et aux sociétés de sécurité.
- Un installateur n'a accès aux paramètres que si l'administrateur l'autorise : de façon permanente ou temporaire, pour 1, 2, 4 ou 8 heures. Passé ce délai, les droits sont retirés automatiquement.
- Les photos prises par les détecteurs avec caméra (par ex. pour vérifier une alarme) relèvent des paramètres de confidentialité. Ceux-ci sont gérés par l'administrateur ; un installateur ne peut pas les modifier.
- Ajax déconseille d'accorder des droits d'administrateur complets à des tiers, même temporairement. Ajax ne peut pas rétablir un accès perdu par négligence.
- L'application Ajax prend en charge la double authentification (2FA).

Brepoels Security · Bremakker 37, 3740 Bilzen · 089 39 08 99 · info@groupbrepoels.com · TVA BE 1021.926.276
Entreprise agréée par le SPF Intérieur pour les systèmes d'alarme et de vidéosurveillance n° 1021.926.276

6. Normes et certificats

NORME / CERTIFICAT	SIGNIFICATION
EN 50131 (Grade 2)	Norme européenne pour les systèmes d'alarme intrusion. Selon Ajax, tous les produits de détection intrusion des gammes Baseline et Superior sont certifiés Grade 2.
EN 50131 (Grade 3)	Niveau de sécurité supérieur, notamment pour les banques et les bijouteries. Une série d'appareils Ajax Superior, dont la Superior Hub Hybrid, est certifiée à ce niveau.
Validation NIST AES-128	Validation du chiffrement entre la centrale Ajax et Ajax Cloud.
ETSI EN 303 645	Norme européenne de cybersécurité pour les objets connectés. La Superior Hub Hybrid (4G) a été certifiée après des tests réalisés par le laboratoire Kiwa.
EN 18031	Normes européennes de cybersécurité pour les équipements radio. Selon Ajax, tous les équipements radio Ajax connectés à internet sur le marché européen y sont conformes.

Le grade atteint par votre installation dépend des appareils installés et de la configuration. Les certificats applicables à chaque appareil sont repris sur ajax.systems/standards.

7. Rôle de Brepoels Security

Brepoels Security installe et configure votre système selon les directives du fabricant. Après la réception, la gestion des utilisateurs et de leurs droits vous appartient.

> **Accès uniquement avec votre autorisation**
>
> Si nous avons besoin d'accéder aux paramètres pour un entretien ou une panne, nous le faisons avec les droits que vous nous accordez. Vous pouvez donner cet accès temporairement et le retirer à tout moment.

8. Votre responsabilité en tant qu'utilisateur

La sécurité technique n'est efficace que si les accès sont bien gérés. L'utilisateur est responsable des mots de passe, codes et droits qu'il gère et attribue lui-même. Nous vous conseillons :

- Choisir un mot de passe fort et unique pour votre compte Ajax et activer la double authentification.
- Ne partager votre mot de passe et les codes du clavier avec personne et choisir des codes difficiles à deviner.
- N'accorder aux utilisateurs que les droits dont ils ont réellement besoin et supprimer les utilisateurs qui ne doivent plus avoir accès.
- Supprimer immédiatement du système un badge, un tag ou une télécommande perdu(e).
- Toujours conserver vous-même les droits d'administrateur de votre système.
- Protéger les smartphones et ordinateurs sur lesquels l'application est installée par un code ou la biométrie.

Brepoels Security n'est pas responsable d'un accès au système résultant de mots de passe ou de codes partagés ou faibles, ou de droits que l'utilisateur a lui-même accordés à des tiers.

Brepoels Security · Bremakker 37, 3740 Bilzen · 089 39 08 99 · info@groupbrepoels.com · TVA BE 1021.926.276
Entreprise agréée par le SPF Intérieur pour les systèmes d'alarme et de vidéosurveillance n° 1021.926.276

9. Remarque importante

Ce document décrit les mesures de sécurité d'Ajax sur la base des informations publiées par le fabricant. Les fonctions disponibles peuvent varier selon le modèle de centrale. Les systèmes Ajax sont conçus avec un niveau de sécurité élevé, mais aucun système ne peut garantir une invulnérabilité absolue. Brepoels Security assure une installation et une configuration correctes selon les directives du fabricant.

Sources

1. Ajax Systems Support, "Jeweller radio protocol: technology and capabilities": ajax.systems/support/posts/jeweller-radio-protocol
2. Ajax Systems Support, "Hub encryption" (FAQ): ajax.systems/support/faqs/hub-encryption
3. Ajax Systems, "Ajax Systems' AES-128 encryption is now NIST-validated": ajax.systems/blog/nist-validation
4. Ajax Systems, "How OS Malevich updates": ajax.systems/blog/ajax-updating-procedure
5. Ajax Systems, "What is jamming of a wireless security system and how to resist it": ajax.systems/blog/what-is-jamming
6. Ajax Systems, Hub 2 user manual: ajax.systems/support/manuals/hub-2
7. Ajax Systems Support, "Accounts and permissions": ajax.systems/support/posts/accounts-and-permissions
8. Ajax Systems, "What is a security grade": ajax.systems/blog/what-is-a-security-grade
9. Ajax Systems, "Grade 3 certification": ajax.systems/blog/grade-3-certification
10. Ajax Systems, "Superior Hub Hybrid certified to ETSI EN 303 645": ajax.systems/blog/superior-hub-hybrid-certified-etsi-standard
11. Ajax Systems, "Ajax complies with the EN 18031 series of standards": ajax.systems/blog/ajax-complies-with-the-en-18031-series-of-standards

Brepoels Security · Bremakker 37, 3740 Bilzen · 089 39 08 99 · info@groupbrepoels.com · TVA BE 1021.926.276
Entreprise agréée par le SPF Intérieur pour les systèmes d'alarme et de vidéosurveillance n° 1021.926.276