

Manuel utilisateur KeyPad Plus

Mis à jour September 13, 2024



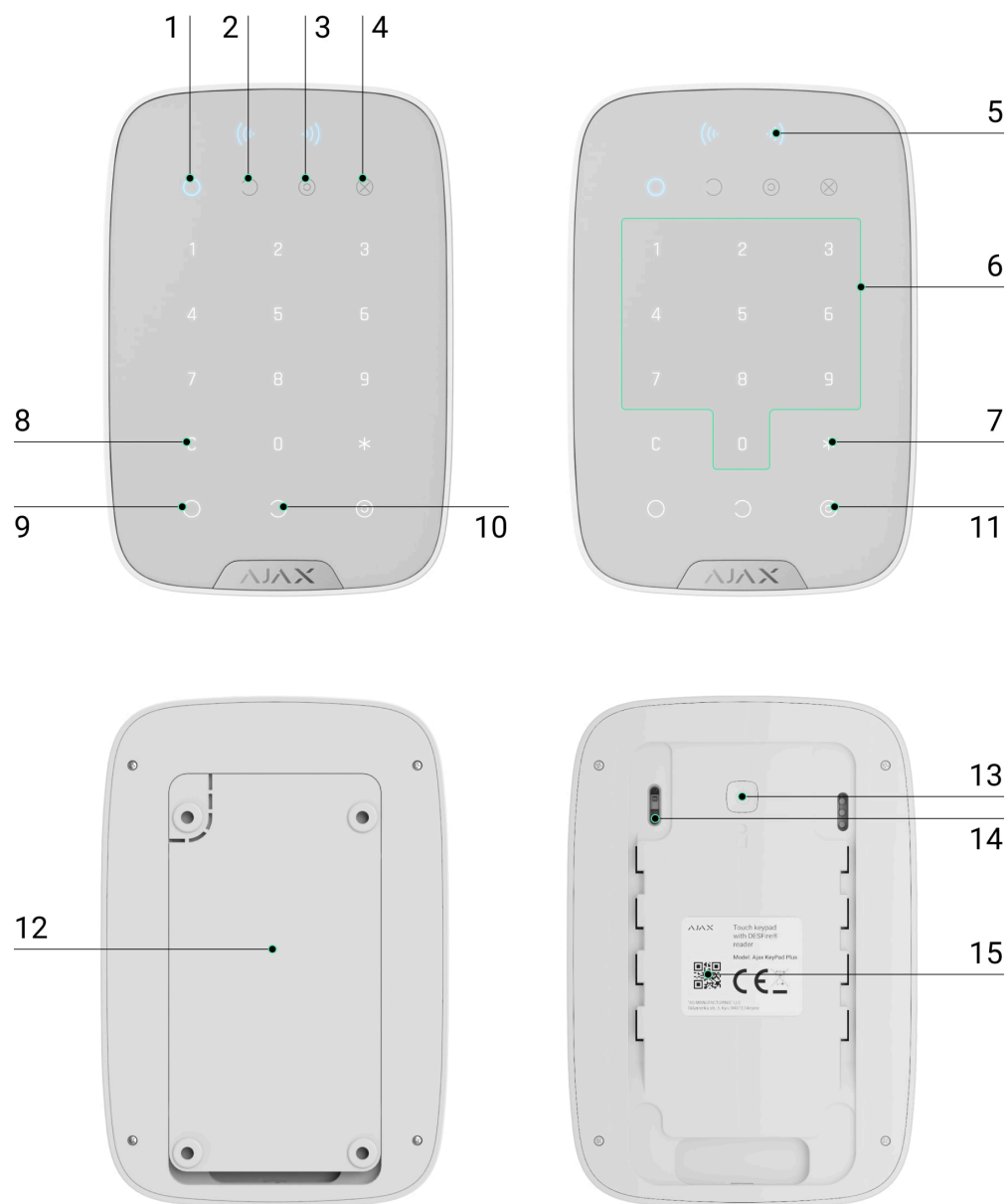
KeyPad Plus est un clavier tactile sans fil pour une installation à l'intérieur et permettant la gestion du système Ajax 'avec des cartes sans contact et des porteclés chiffrés. Il prend en charge une alarme silencieuse, lors de la saisie du code de contrainte. L'éclairage LED indique le mode de sécurité actuel.



Le clavier ne fonctionne qu'avec le Hub (4G) Jeweller, le Hub Plus Jeweller, le Hub 2 Jeweller, le Hub Hybrid et le Hub 2 Plus Jeweller utilisé OS Malevich 2.11 et les versions ultérieures. La connexion au Hub (2G) Jeweller et aux modules d'intégration ocBridge Plus et uartBridge n'est pas prise en charge.

Le clavier fonctionne comme une partie du système Ajax en se connectant à la centrale via le protocole de communication radio sécurisé Jeweller. La portée de communication en champ ouvert peut atteindre 1 700 mètres. La durée de vie de la batterie préinstallée peut atteindre 4,5 ans.

Éléments fonctionnels



1. Indicateur **Armé**

2. Indicateur **Désarmé**

3. Indicateur de **mode Nuit**

4. Indicateur de **dysfonctionnement**

5. **Lecteur du Pass/Tag**

6. Bloc boutons tactiles numériques

- 7. Bouton **Fonction**
- 8. Bouton **Effacer**
- 9. Bouton **Armer** 
- 10. Bouton **Désarmer** 
- 11. Bouton du **mode Nuit** 
- 12. Panneau de montage du SmartBracket (pour retirer la plaque, faites-la glisser vers le bas)



N'enlevez pas la partie perforée du support. Elle est nécessaire pour actionner l'anti-sabotage en cas de tentative de démontage du clavier.

- 13. Bouton marche/arrêt
- 14. Bouton anti-sabotage
- 15. Code QR

Principe de fonctionnement

1. **Codes d'accès.** Le clavier prend en charge les codes communs et personnels, ainsi que l'armement sans saisie de code.
2. **Cartes ou portecclés.** Vous pouvez connecter des portecclés Tag et des cartes Pass au système. Pour identifier rapidement et en toute sécurité les utilisateurs, KeyPad Plus utilise la technologie DESFire®. DESFire® est basé sur la norme internationale ISO 14443 et combine un chiffrement 128 bits et une protection contre l'usurpation des données.

Le KeyPad Plus prend en charge les types de codes suivants :

- **Code clavier** est un code commun, configuré pour le clavier. Lorsqu'il est utilisé, tous les événements sont transmis aux applications Ajax au nom du clavier.
- **Code utilisateur** est un code personnel, configuré pour les utilisateurs connectés à la centrale. Lorsqu'il est utilisé, tous les événements sont transmis aux applications Ajax au nom de l'utilisateur.
- **Codes d'accès** est un configuré pour les personnes qui ne sont pas enregistrées dans le système. Lorsqu'il est utilisé, les événements sont transmis aux applications Ajax avec un nom associé à ce code.
- **Code GIR** est un code d'accès pour les groupes d'intervention rapide (GIR) qui est activé après une alarme et qui est valable pour une durée déterminée. Lorsque le code est activé et utilisé, les événements sont envoyés aux applications Ajax avec un nom associé à ce code.



Le nombre de codes d'accès personnels, codes d'accès et codes GIR dépend du modèle de centrale.

Le panneau de contrôle Hub (2G) Jeweller ne prend pas en charge les codes d'accès.

Avant de saisir un code ou d'utiliser Tag/Pass, vous devez activer (réveiller) le KeyPad Plus, en faisant glisser votre main sur l'écran tactile de haut en bas. Lorsqu'il est activé, il déclenche le rétro-éclairage des touches et le clavier émet des bips.



La fonction **Auto-réveil en cas de Temporisation au désarmement** permet d'activer automatiquement le clavier lorsque la Temporisation au désarmement est configurée. Cette fonction est compatible avec KeyPad Plus Jeweller avec la version 5.60.7.0 du firmware ou une version ultérieure et les centrales avec OS Malevich 2.19 ou une version ultérieure.

Le KeyPad Plus est équipé d'indicateurs LED qui indiquent le mode de sécurité actuel et les dysfonctionnements du clavier (le cas échéant). L'état de sécurité est affiché uniquement lorsque le clavier est actif (le rétroéclairage du dispositif est allumé).



Vous pouvez utiliser le KeyPad Plus sans éclairage ambiant car le clavier dispose d'un rétroéclairage. Un signal sonore retentit lorsque les boutons sont enfoncés. La luminosité du rétroéclairage et le volume du clavier sont réglables dans les paramètres. Si vous ne touchez pas le clavier pendant 4 secondes, le KeyPad Plus réduit la luminosité du rétroéclairage, et 8 secondes plus tard, il passe en mode d'économie d'énergie et l'écran s'éteint.



Si les batteries sont déchargées, le rétroéclairage s'allume au niveau minimum, quels que soient les réglages.

Le bouton de fonction

Le KeyPad Plus dispose d'un **bouton de fonction** qui fonctionne selon 3 modes :

- **Off** — le bouton est désactivé et rien ne se passe après avoir appuyé dessus.
- **Alarme** — après avoir appuyé sur le **bouton de fonction**, le système envoie une alarme au centre de télésurveillance et à tous les utilisateurs.
- **Désactiver l'alarme incendie interconnectée** — après avoir appuyé sur le **bouton de fonction**, le système coupe l'alarme des détecteurs d'incendie Ajax. Cette fonctionnalité est disponible uniquement si les Alarmes incendie interconnectées sont activées (Centrale → Paramètres ⚙️ → Service → Paramètres des détecteurs d'incendie).

[En savoir plus](#)

Code de contrainte

KeyPad Plus prend en charge le code de contrainte. Il permet de simuler la désactivation de l'alarme. L'application Ajax et les sirènes installées dans l'installation ne vous trahiront pas, et le centre de télésurveillance et les autres utilisateurs du système Ajax seront avertis de l'incidence.

[En savoir plus](#)

Armement en deux étapes

Le KeyPad Plus peut participer à l'armement en deux étapes, mais ne peut pas être utilisé comme un dispositif de deuxième étape. Le processus d'armement en deux étapes à l'aide de Tag ou Pass est similaire à l'armement à l'aide d'un code personnel ou commun sur le clavier.

Transmission des événements au centre de télésurveillance

Le système Ajax peut se connecter au centre de télésurveillance et transmettre des événements et des alarmes à ce dernier sous les formats **SurGard (Contact ID)**, **ADEMCO 685**, **SIA (DC-09)** et d'autres protocoles propriétaires. Une liste complète des protocoles pris en charge est [disponible ici](#). L'ID du dispositif et le numéro de la boucle (zone) peuvent être trouvés dans [ses états](#).

Connexion



Le KeyPad Plus est incompatible avec le Hub (2G) Jeweller, les unités centrales de sécurité tierces et les modules d'intégration ocBridge Plus et uartBridge.

Avant de commencer la connexion

1. Installez l'application Ajax et créez un [compte](#). Ajoutez une centrale et créez au moins une pièce.
2. Assurez-vous que la centrale est allumée et qu'elle dispose d'un accès à Internet (via un câble Ethernet, un réseau Wi-Fi et/ou un réseau mobile). Pour se faire, ouvrez l'application Ajax ou regardez le logo de la centrale sur la plaque frontale — il s'allume en blanc ou en vert si la centrale est connectée au réseau.
3. Assurez-vous que la centrale ne soit pas en mode armé et que les mises à jour ne soient pas en cours, en vérifiant son état dans l'application.



Seul un utilisateur ou un PRO ayant des droits d'administrateur complets peut ajouter un dispositif à la centrale.

Pour connecter le KeyPad Plus

1. Ouvrez l'application Ajax. Si votre compte a accès à plusieurs centrales, sélectionnez celle à laquelle vous souhaitez connecter le KeyPad Plus.
2. Allez dans le menu **Dispositifs**  et cliquez sur **Ajouter un dispositif**.
3. Nommez le clavier, scannez ou saisissez le code QR (situé sur l'emballage et sous le panneau de montage SmartBracket), puis sélectionnez une pièce.
4. Cliquez sur **Ajouter** ; le compte à rebours commencera.
5. Allumez le clavier en appuyant sur le bouton d'alimentation pendant 3 secondes. Une fois connecté, le KeyPad Plus apparaît dans la liste des dispositifs de la centrale dans l'application. Pour se connecter, placez le clavier dans la même installation protégée que le système (dans la zone de couverture du réseau radio de la centrale). Si la connexion est interrompue, réessayez dans 10 secondes.



Le clavier ne peut fonctionner qu'avec une seule centrale. Lorsqu'il est connecté à une nouvelle centrale, le dispositif cesse d'envoyer des commandes à l'ancienne centrale. Une fois ajouté à une nouvelle centrale, le KeyPad Plus n'est pas supprimé de la liste des dispositifs de l'ancienne centrale. Ceci doit être fait manuellement via l'application Ajax.

Le KeyPad Plus s'éteint automatiquement 6 secondes après avoir été allumé si le clavier ne parvient pas à se connecter à la centrale. Par conséquent, vous n'avez pas besoin d'éteindre le dispositif pour réessayer la connexion.

La mise à jour des états des dispositifs de la liste dépend des paramètres du Jeweller ; la valeur par défaut est de 36 secondes.

Icônes

Les icônes représentent certains des états du KeyPad Plus. Vous pouvez les voir dans l'onglet **Dispositifs** , dans l'application Ajax.

Icône	Valeur
-------	--------

	Intensité du signal Jeweller — Affiche l'intensité du signal entre la centrale ou le prolongateur de portée et le KeyPad Plus
	Niveau de charge de la batterie du KeyPad Plus
	Le KeyPad Plus fonctionne via un <u>prolongateur de portée du signal radio</u>
	Les notifications d'état corporel de KeyPad Plus sont désactivées <u>En savoir plus</u>
	KeyPad Plus est désactivé <u>En savoir plus</u>
	Lecture du pass/tag est activée dans les paramètres du KeyPad Plus
	Lecture du pass/tag est désactivée dans les paramètres du KeyPad Plus
	Le dispositif n'a pas été transféré à la nouvelle centrale. <u>En savoir plus</u>

États

Les états incluent des informations sur le dispositif et ses paramètres de fonctionnement. Les états du KeyPad Plus peuvent être trouvés dans l'application Ajax :

1. Allez dans l'onglet **Dispositifs** .
2. Sélectionnez KeyPad Plus dans la liste.

Paramètre	Valeur
Dysfonctionnement	En appuyant sur  , vous ouvrez la liste des dysfonctionnements du KeyPad Plus.

	Ce champ est uniquement affiché si un dysfonctionnement est détecté.
Température	Température du clavier. Elle est mesurée sur le processeur et évolue progressivement. L'erreur acceptable entre la valeur dans l'application et la température ambiante est de 2°C. La valeur est mise à jour dès que le dispositif identifie un changement de température d'au moins 2°C. Un scénario par température peut être défini pour contrôler les dispositifs d'automatisation. <u>En savoir plus</u>
Intensité du signal Jeweller	Intensité du signal Jeweller entre la centrale (ou prolongateur de portée) et le clavier. Les valeurs recommandées sont de 2 à 3 barres.
Connexion	État de la connexion entre la centrale ou le prolongateur de portée et le clavier : • En ligne — le clavier est en ligne. • Hors ligne — aucune connexion au clavier.
Charge de la batterie	Le niveau de charge de la batterie du dispositif. Deux états sont disponibles : • OK. • Batterie faible. Lorsque les batteries sont déchargées, les applications Ajax et le centre de télésurveillance reçoivent les notifications appropriées. Après une notification de batterie faible, le clavier peut fonctionner jusqu'à 2 mois.

	<u>Comment la charge de la batterie est affichée dans les applications Ajax</u>
Couvercle	L'état du bouton anti-sabotage du dispositif qui réagit au détachement ou à l'endommagement du boîtier : • Ouvert. • Fermé. <u>Qu'est-ce qu'un bouton anti-sabotage</u>
Fonctionne via *nom du prolongateur de portée*	Affiche l'état de l'utilisation du prolongateur de portée. Ce champ n'est pas affiché si le clavier fonctionne directement avec la centrale.
Lecture du pass/tag	Affiche si le lecteur de cartes et de badges est activé
Gestion facile de groupe assignée	Affiche si oui ou non le mode de sécurité peut être changé avec Pass ou Tag et sans confirmation par les boutons de contrôle.
Changement facile du mode de sécurité	 Ce paramètre remplace Gestion facile du groupe assigné sur KeyPad Plus Jeweller avec la version 5.60.7.0 du firmware ou une version ultérieure, fonctionnant avec les centrales avec <u>OS Malevich 2.19</u> ou une version ultérieure. Affiche le réglage de la fonction Changement facile du mode de sécurité : • Off – chaque tentative d'armement ou de désarmement doit être confirmée en entrant le

	code d'accès ou en présentant le dispositif d'accès. • Armer/désarmer à l'aide d'un dispositif d'accès sans confirmer l'action par les touches – permet aux utilisateurs de changer les modes de sécurité du système à l'aide des dispositifs d'accès sans confirmation par l'appui sur les touches du clavier. • Désarmement sans confirmation par touche – le système ou ses groupes, dont la sécurité est gérée par un code d'accès ou des dispositifs d'accès, seront désarmés sans confirmation par l'appui sur les touches du clavier.  Une longueur de code fixe doit être définie pour le système dans les paramètres de la centrale à l'aide de l'application Ajax PRO.
Désactivation forcée	Indique l'état du dispositif : • Non – le dispositif fonctionne normalement et transmet tous les événements. • Couvercle seulement – l'administrateur de la centrale a désactivé les notifications concernant l'ouverture du boîtier. • Entièrement – l'administrateur de la centrale a entièrement exclu le clavier du système. Le dispositif n'exécute pas les commandes du système et ne signale pas les alarmes ou autres événements. <u>En savoir plus</u>
Désactivation unique	Indique l'état du réglage de la désactivation unique du clavier : • Non – le clavier fonctionne normalement.

	• Couvercle seulement – les notifications sur le déclenchement du bouton anti-sabotage du clavier sont désactivées jusqu’au premier désarmement. • Entièrement – le clavier est entièrement exclu du fonctionnement du système jusqu’au premier désarmement. Le dispositif n’exécute pas les commandes du système et ne signale pas les alarmes ou autres événements. <u>En savoir plus</u>
Firmware	Version du firmware du KeyPad Plus.
ID	Identifiant du dispositif.
N° du dispositif	Numéro de la boucle du dispositif (zone).

Paramètres

KeyPad Plus est configuré dans l’application Ajax :

1. Allez dans l’onglet **Dispositifs** .
2. Sélectionnez KeyPad Plus dans la liste.
3. Accédez aux **Paramètres** en cliquant sur l’icône engrenage .



Pour appliquer les paramètres après la modification, cliquez sur le bouton **Retour**.

Paramètre	Signification
Nom	Nom du dispositif. Affiché dans la liste des dispositifs de la centrale, texte SMS et notifications dans l’historique des événements.

	Pour modifier le nom du dispositif, cliquez sur l'icône en forme de crayon . Le nom peut contenir jusqu'à 12 caractères cyrilliques ou jusqu'à 24 caractères latins.
Pièce	Sélection de la pièce virtuelle à laquelle KeyPad Plus est assigné. Le nom de la pièce est affiché dans le texte des SMS et des notifications dans l'historique des événements.
Gestion du groupe	Sélection du groupe de sécurité contrôlé par le dispositif. Il est possible de sélectionner tous les groupes ou un seul. Ce champ s'affiche lorsque le <u>mode Groupe</u> est activé.
Options d'accès	Sélection de la méthode armer/désarmer : • Code des clavier uniquement. • Code d'utilisateur uniquement. • Code des claviers et de l'utilisateur.  Pour activer les codes d'accès, configurés pour les personnes qui ne sont pas enregistrées dans le système, sélectionnez les options sur le clavier : Code des claviers uniquement ou Code des claviers et de l'utilisateur
Code clavier	Sélection d'un code commun pour le contrôle de la sécurité. Contient 4 à 6 chiffres.
Code de contrainte	Sélection d'un code de contrainte commun pour l'alarme silencieuse. Il contient 4 à 6 chiffres. <u>En savoir plus</u>

Bouton de fonction	Sélection de la fonction du * bouton (bouton de fonction) : • Off — le bouton de fonction est désactivé et ne permet pas d'exécuter des commandes lorsqu'il est pressé. • Alarmer — Après avoir pressé sur le bouton de fonction, le système envoie une alarme au centre de télésurveillance et à tous les utilisateurs. • Désactiver l'alarme incendie interconnectée — lorsqu'elle est enfoncée. Désactiver l'alarme des détecteurs d'incendie Ajax. Disponible uniquement si l'alarme incendie interconnectée est activée. <u>En savoir plus</u>
Accès non autorisé auto-verrouillage	S'il est actif, le clavier est verrouillé pour la durée prédéfinie si un code incorrect est saisi ou si les passes/tags non vérifiés sont utilisés plus de 3 fois de suite en 1 minute. Il est impossible de désarmer le système via le clavier pendant cette période. Vous pouvez déverrouiller le clavier via l'application Ajax.
Temps auto-verrouillage (min)	Sélection de la période de verrouillage du clavier après des tentatives de code erroné : • 3 minutes. • 5 minutes. • 10 minutes. • 20 minutes. • 30 minutes. • 60 minutes. • 90 minutes.

	• 180 minutes.
Luminosité	Sélection de la luminosité du rétro-éclairage des touches du clavier. Le rétro-éclairage ne fonctionne que lorsque le clavier est actif. Cette option n'affecte pas le niveau de luminosité des indicateurs pass/tag reader et des modes de sécurité.
Volume	Sélection du niveau de volume des boutons du clavier lorsqu'ils sont enfoncés.
Lecture du pass/tag	Lorsqu'il est activé, le mode de sécurité peut être contrôlé par des dispositifs d'accès de type Pass et Tag.
Confirmation de l'autorisation avec un code d'accès	Si ce paramètre est activé, l'autorisation d'accès au système à l'aide de dispositifs d'accès nécessite la confirmation de l'action par le code utilisateur ou le code clavier. Disponible si le commutateur Lecture du pass/tag est activé. Ce paramètre est pris en charge lorsque le KeyPad Plus Jeweller est connecté à une centrale dont la version du firmware est <u>OS Malevich 2.20</u> ou supérieure.
Délai de confirmation	Sélection du délai maximum pour confirmer l'autorisation avec un code d'accès après la confirmation des dispositifs d'accès. Disponible si la bascule Confirmation de l'autorisation par un code d'accès est activée. Ce paramètre est pris en charge lorsque le KeyPad Plus Jeweller est connecté à une centrale dont la version du firmware est <u>OS Malevich 2.21</u> ou supérieure.
Gestion facile de groupe assignée	Lorsqu'il est activé, le changement de mode de sécurité avec Tag et Pass ne nécessite pas de confirmation en appuyant sur le boutons armer , désarmer ou du mode Nuit . Le mode de sécurité est automatiquement activé.

Cette option est disponible si la **lecture du pass/tag** est activée dans les paramètres du clavier.

Si le mode groupe est activé, l'option est disponible lorsque le clavier est affecté à un groupe particulier – le champ **Gestion de groupes** dans les paramètres du clavier.

En savoir plus

Changement facile du mode de sécurité



Ce paramètre remplace **Gestion facile du groupe assigné** sur KeyPad Plus Jeweller avec la version 5.60.7.0 du firmware ou une version ultérieure, fonctionnant avec les centrales avec OS Malevich 2.19 ou une version ultérieure.

Permet aux utilisateurs d'armer/désarmer le système sans confirmation en appuyant sur les touches du clavier.

Trois options sont disponibles :

- **Off** – chaque tentative d'armement ou de désarmement doit être confirmée en entrant le code d'accès ou en présentant le dispositif d'accès.
- **Armer/désarmer à l'aide d'un dispositif d'accès sans confirmer l'action par les touches** – permet aux utilisateurs de changer les modes de sécurité du système à l'aide des dispositifs d'accès sans confirmation par l'appui sur les touches du clavier.
- **Désarmement sans confirmation par touche** – le système ou ses groupes, dont la sécurité est gérée par un code d'accès ou des dispositifs d'accès, seront désarmés sans

	confirmation par l'appui sur les touches du clavier.  Une longueur de code fixe doit être définie pour le système dans les paramètres de la centrale à l'aide de l'application Ajax PRO.
Armement sans code	Cette option vous permet d'armer le système sans saisir de code. Pour ce faire, il suffit de cliquer sur le bouton  Armer ou  Mode nuit.
Auto-réveil en cas de Temporisation au désarmement	 La fonction est disponible sur KeyPad Plus Jeweller avec la version 5.60.7.0 du firmware ou une version plus récente, fonctionnant avec les centrales avec <u>OS Malevich 2.19</u> ou une version plus récente. Active le clavier après que la <u>Temporisation au désarmement</u> ait été lancée par un dispositif de sécurité. La fonction d'Auto-réveil peut également réduire la durée de vie de la batterie du clavier.
Alerte avec une sirène si le bouton de panique est pressé	Ce champ s'affiche si l'option Alarme est sélectionnée pour le bouton de fonction. Lorsque l'option est activée, les sirènes connectées au système Ajax émettent une alerte lorsque l'on appuie sur le * bouton (bouton de fonction).
Test d'intensité du signal Jeweller	Basculer le clavier en mode test d'intensité du signal Jeweller. <u>En savoir plus</u>

Test d'atténuation du signal	Basculer le clavier en mode test d'atténuation. <u>En savoir plus</u>
Réinitialiser du pass/tag	Permet de supprimer toutes les centrales associées à Tag ou Pass, de la mémoire du dispositif. <u>En savoir plus</u>
Manuel de l'utilisateur	Ouvre le Manuel de l'utilisateur du KeyPad Plus dans l'application Ajax
Désactivation forcée	Permet à l'utilisateur de désactiver le dispositif sans le retirer du système. Trois options sont disponibles : • Non — le dispositif fonctionne normalement et transmet tous les événements. • Entièrement — le dispositif n'exécutera pas les commandes du système ou ne participera pas aux scénarios d'automatisation, et le système ignorera les alarmes du dispositif et autres notifications. • Couvercle seulement — le système ignorera uniquement les notifications relatives au déclenchement du bouton anti-sabotage du dispositif. <u>En savoir plus</u>
Désactivation unique	Indique l'état du réglage de la désactivation unique du clavier. Trois options sont disponibles : • Non — le clavier fonctionne normalement. • Couvercle seulement — les notifications sur le déclenchement du bouton anti-sabotage du clavier sont désactivées jusqu'au premier désarmement. • Entièrement — le clavier est entièrement exclu du fonctionnement du système jusqu'au premier désarmement. Le dispositif n'exécute pas les commandes du système et ne signale pas les alarmes ou autres événements.

	En savoir plus
Dissocier le dispositif	Déconnectez le KeyPad Plus de la centrale et supprimez ses paramètres.



Les retards d'entrée et de sortie sont définis dans les paramètres des détecteurs correspondants, et non dans les paramètres du clavier.

[En savoir plus sur les retards d'entrée et de sortie](#)

Configuration des codes

Le système Ajax vous permet de configurer un code de clavier, ainsi que des codes personnels pour les utilisateurs ajoutés à la centrale.

Avec la mise à jour de l'[OS Malevich 2.13.1](#), nous avons également ajouté la possibilité de créer des codes pour les personnes qui ne sont pas connectées à la centrale. Ceci est pratique, par exemple, pour permettre à une entreprise de nettoyage d'accéder à la gestion de la sécurité.

Avec la mise à jour de l'**OS Malevich 2.17**, des codes pour les groupes d'intervention rapide sont disponibles. Les codes GIR sont des codes d'accès activés après l'alarme et valables pour une période déterminée. Découvrez ci-dessous comment configurer et utiliser chaque type de code.

Pour configurer un code de clavier

1. Allez dans les paramètres du clavier.
2. Sélectionnez **Code du clavier**.
3. Définissez le code du clavier que vous souhaitez.

Pour définir un code de contrainte du clavier

1. Allez dans les paramètres du clavier.

2. Sélectionnez **Code de contrainte**.

3. Définissez le code de contrainte du clavier que vous souhaitez.

Pour configurer un code d'accès personnel dans l'application Ajax

1. Accédez aux paramètres du profil utilisateur (**Centrale** → **Paramètres**  → **Utilisateurs** → **Vos paramètres de profil**).
2. Sélectionnez **Paramètres code d'accès** (l'ID utilisateur est également visible dans ce menu).
3. Définir le **Code utilisateur** et le **Code de contrainte**.



Chaque utilisateur définit individuellement un code personnel. L'administrateur ne peut pas définir un code pour tous les utilisateurs.

Pour définir un code d'accès pour une personne non enregistrée dans le système

1. Accédez aux paramètres de la centrale (**Centrale** → **Paramètres** ).
2. Sélectionnez **Codes d'accès des claviers**.
3. Configurez le **Nom d'utilisateur** et le **Code d'accès**.

Si vous souhaitez configurer un code de contrainte, modifier les paramètres d'accès aux groupes, au mode Nuit, à l'ID du code, désactiver temporairement ou supprimer ce code, sélectionnez-le dans la liste et effectuez les modifications.



Un utilisateur PRO ou un utilisateur disposant de droits d'administrateur peut configurer un code d'accès ou modifier ses paramètres. Cette fonction est prise en charge par les centrales avec OS Malevich 2.13.1 et supérieur. Les codes d'accès ne sont pas pris en charge par le panneau de contrôle Hub (2G) Jeweller.

Pour définir le code GIR

Seul un PRO ayant les permissions de configurer le système peut créer et configurer les codes GIR dans les [applications Ajax PRO](#). De plus amples informations sur la configuration de cette fonction sont disponibles dans [cet article](#).



Les codes GIR sont pris en charge par les centrales (sauf le modèle Hub (2G) Jeweller) avec OS Malevich 2.17 et les versions ultérieures.

Ajout des cartes et portecclés

Le KeyPad Plus peut fonctionner avec les [portescclés Tag](#), les [cartes Pass](#) et les portescclés et cartes tiers qui utilisent le protocole DESFire®.



Avant d'ajouter des dispositifs tiers compatibles avec DESFire®, assurez-vous qu'ils disposent de suffisamment de mémoire libre pour utiliser le nouveau clavier. Il est conseillé que le périphérique tiers soit pré-formaté.

Le nombre maximum de pass/tags connecté dépend du modèle de centrale. En même temps, les cartes et portecclés n'affectent pas la limite totale d'appareils de la centrale.

Modèle de centrale	Nombre des dispositifs Tag ou Pass
Hub (4G) Jeweller	50
Hub Plus Jeweller	99
Hub 2 Jeweller	50
Hub 2 Plus Jeweller	200
Hub Hybrid	50

La procédure de connexion des Tag, Pass et des dispositifs tiers est la même. Voir les instructions de connexion [ici](#).

Gestion de la sécurité par codes d'accès

En utilisant un code commun, personnel ou GIR, vous pouvez contrôler le **Mode nuit** et la sécurité du site entier ou de groupes séparés. Le clavier vous permet d'utiliser des codes de 4 à 6 chiffres. Les numéros saisis de manière incorrecte peuvent être effacés à l'aide de la touche **C**.

Restrictions de longueur de code pour le clavier



Si un code d'accès ou un code personnel est utilisé, le nom de l'utilisateur qui a armé ou désarmé le système est affiché dans l'historique d'événements de la centrale et dans la liste des notifications. Si un code commun est utilisé, le nom de l'utilisateur qui a changé le mode de sécurité n'est pas affiché.

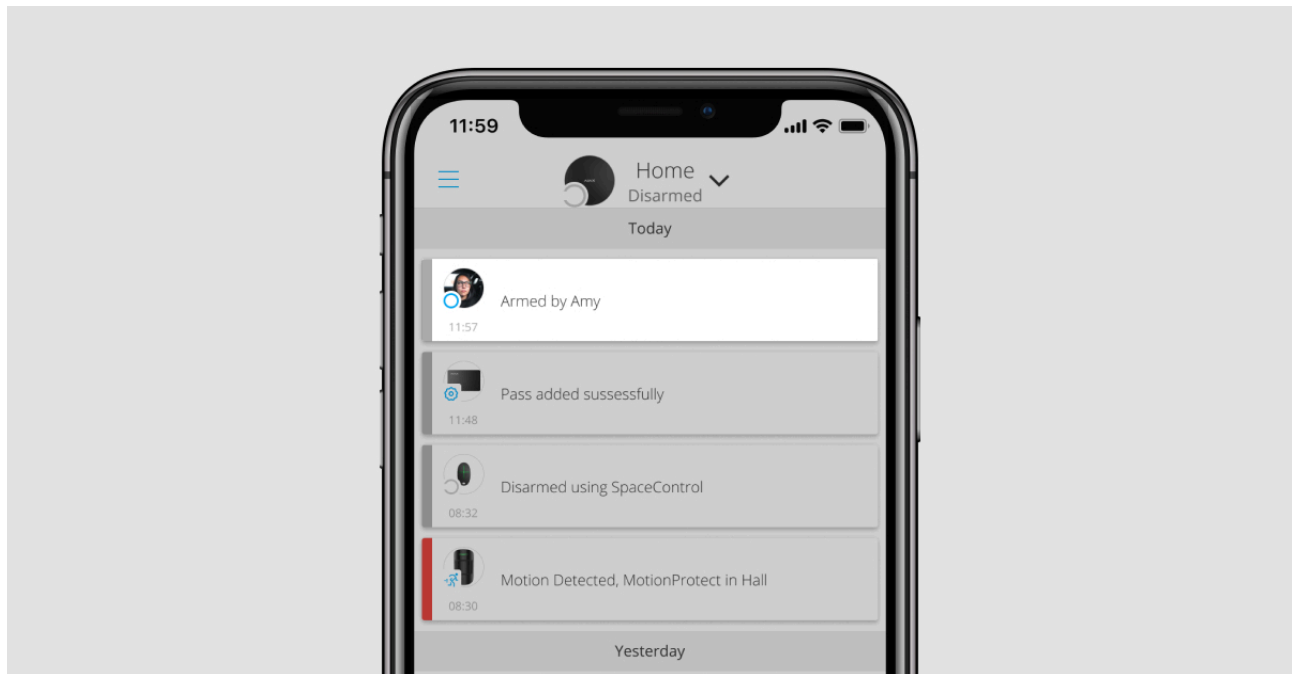


Les **codes d'accès des claviers** sont compatibles avec les centrales (sauf le modèle [Hub \(2G\) Jeweller](#)) avec OS Malevich 2.13.1 et supérieur.

Les **codes GIR** sont pris en charge par les centrales (sauf le modèle [Hub \(2G\) Jeweller](#)) avec OS Malevich 2.17 et les versions ultérieures.

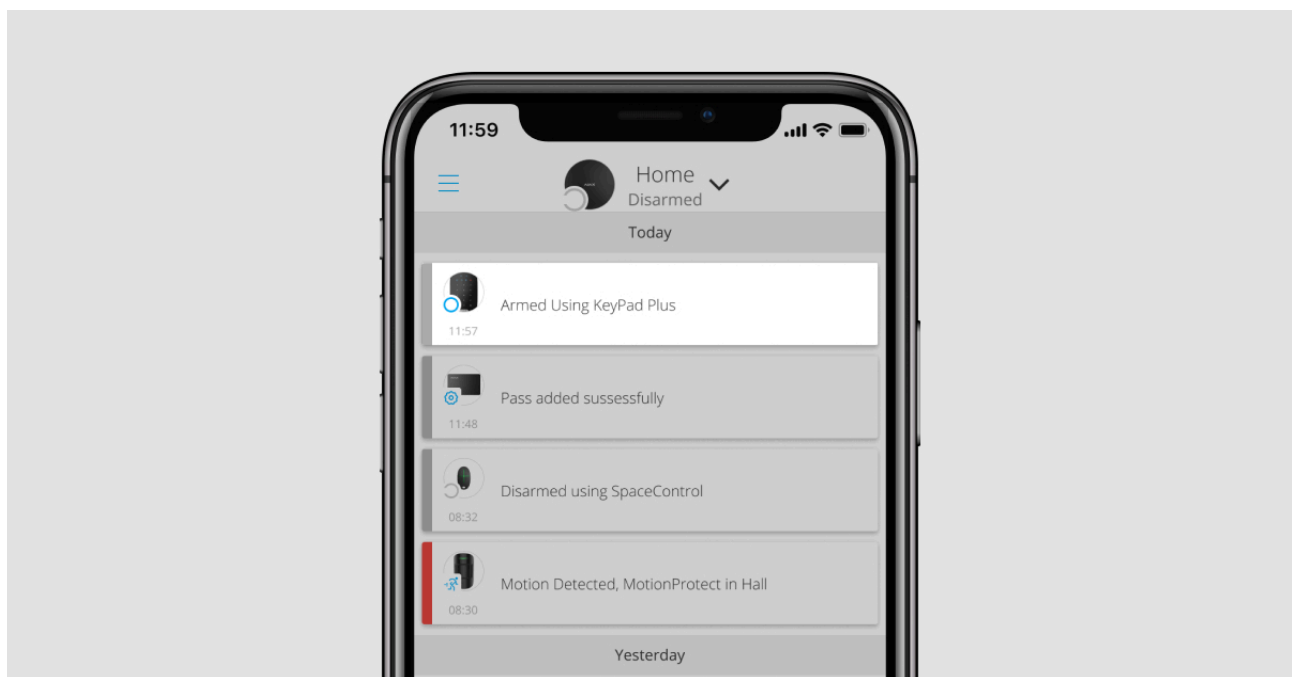
Armement avec un code personnel

Le nom de l'utilisateur est affiché dans la liste des notifications et des événements



Armement avec un code commun

Le nom du dispositif est affiché dans la liste des notifications et des événements



Le KeyPad Plus est verrouillé pour la durée spécifiée dans les paramètres si un code incorrect est saisi trois fois de suite en l'espace d'une (1) minute. Les notifications correspondantes sont envoyées aux utilisateurs et au centre de télésurveillance. Un utilisateur ou PRO ayant des droits d'administrateur peut déverrouiller le clavier dans l'application Ajax.

Gestion de la sécurité de l'installation à l'aide d'un code commun

1. Activez le clavier en faisant glisser votre main dessus. Apportez le badge Tag ou la carte Pass au lecteur de Pass/Tag du clavier si la fonction **Confirmation de l'autorisation avec un code d'accès** est activée.
2. Entrez le **code commun**.
3. Appuyez sur la touche d'**armer**  / **désarmer**  / **mode Nuit** .

Par exemple : 1234 → 

Gestion de la sécurité du groupe avec un code commun

1. Activez le clavier en faisant glisser votre main dessus. Apportez le badge Tag ou la carte Pass au lecteur de Pass/Tag du clavier si la fonction **Confirmation de l'autorisation avec un code d'accès** est activée.
2. Entrez le **code commun**.
3. Appuyez le * (**bouton de fonction**).
4. Entrez l'**ID du groupe**.
5. Appuyez sur la touche d'**armer**  / **désarmer**  / **mode Nuit** .

Par exemple : 1234 → * → 2 → 

Qu'est-ce que l'ID du groupe

Si un groupe de sécurité est attribué au KeyPad Plus (dans le champ Gestion des groupes des paramètres du clavier), vous n'avez pas besoin de saisir l'ID du groupe. Pour gérer le mode de sécurité de ce groupe, il suffit de saisir un code commun ou personnel.



Si un groupe est attribué au KeyPad Plus, vous ne pourrez pas gérer le **mode Nuit** à l'aide d'un code commun. Dans ce cas, le **mode Nuit** ne peut être contrôlé à l'aide d'un code personnel que si l'utilisateur dispose des droits appropriés.

Gestion de la sécurité de l'installation à l'aide d'un code personnel

1. Activez le clavier en faisant glisser votre main dessus. Apportez le badge Tag ou la carte Pass au lecteur de Pass/Tag du clavier si la fonction **Confirmation de l'autorisation avec un code d'accès** est activée.
2. Entrez l'**ID d'utilisateur**.
3. Appuyez le * (**bouton de fonction**).
4. Entrez votre **code personnel**.
5. Appuyez sur la touche d'**armer**  / **désarmer**  / **mode Nuit** .

Par exemple : 2 → * → 1234 → 

Qu'est-ce que l'ID utilisateur

Gestion de la sécurité du groupe avec un mot de passe personnel

1. Activez le clavier en faisant glisser votre main dessus. Apporter le badge Tag ou la carte Pass au lecteur de pass/tag du clavier si la fonction **Confirmation de l'autorisation avec un code d'accès** est activée.
2. Entrez l'**ID d'utilisateur**.
3. Appuyez le * (**bouton de fonction**).
4. Entrez votre **code personnel**.
5. Appuyez le * (**bouton de fonction**).
6. Entrez l'**ID du groupe**.
7. Appuyez sur l'activation du bouton **armer**  / **désarmer**  / **mode Nuit** .

Par exemple : 2 → * → 1234 → * → 5 → 

Si un groupe est attribué au KeyPad Plus (dans le champ **Gestion des groupes** des paramètres du clavier), vous n'avez pas besoin de saisir l'ID du groupe. Pour gérer le mode de sécurité de ce groupe, il suffit de saisir un code personnel.

Qu'est-ce que l'ID du groupe

Qu'est-ce que l'ID utilisateur

Gestion de la sécurité de l'installation à l'aide d'un code d'accès

Saisissez le **code d'accès** et appuyez sur la touche d'**armer**  / **désarmer**  / **mode Nuit** .

Par exemple : 1234 → 

Gestion de la sécurité du groupe à l'aide d'un code d'accès

Saisissez le **code d'accès**, appuyez sur l'icône *звезда*, saisissez l'**ID du groupe** et appuyez sur la touche d'**armer**  / **désarmer**  / **mode Nuit** .

Par exemple : 1234 → * → 2 → 

Qu'est-ce que l'ID du groupe

Utilisation d'un code de contrainte

Un code de contrainte vous permet de simuler la désactivation de l'alarme. L'application Ajax et les sirènes installées dans l'installation ne trahiront pas l'utilisateur dans ce cas, et le centre de télésurveillance ainsi que les autres utilisateurs seront avertis de l'incidence. Vous pouvez utiliser à la fois un code de contrainte personnel et un code de contrainte commun.



Les scénarios et les sirènes réagissent au désarmement de contrainte de la même manière qu'au désarmement normal.

En savoir plus

Pour utiliser un code de contrainte commun

1. Activez le clavier en faisant glisser votre main dessus. Apportez le badge Tag ou la carte Pass au lecteur de Pass/Tag du clavier si la fonction **Confirmation de l'autorisation avec un code d'accès** est activée.
2. Entrez le **code de contrainte commun**.
3. Appuyez sur la touche de désarmer .

Par exemple : 4321 → 

Pour utiliser un code de contrainte personnel

1. Activez le clavier en faisant glisser votre main dessus. Apportez le badge Tag ou la carte Pass au lecteur de Pass/Tag du clavier si la fonction **Confirmation de l'autorisation avec un code d'accès** est activée.
2. Entrez l'**ID d'utilisateur**.
3. Appuyez le * (**bouton de fonction**).
4. Entrez le **code de contrainte personnel**.
5. Appuyez sur la touche de désarmer .

Par exemple : 2 → * → 4422 → 

Pour utiliser un code de contrainte

Saisissez le **code de contrainte** et appuyez sur la touche de **désarmement** .

Par exemple : 4567 → 

Utilisation du code GIR

Le code GIR est activé après le déclenchement de l'alarme pendant la durée configurée dans les paramètres de la centrale et il est valable pendant une période déterminée. Cela garantit que ces codes ne seront utilisés qu'en cas de risque, contrairement aux codes clavier ou utilisateur.

Comment configurer le code GIR

Contrôle de sécurité du site à l'aide du code GIR :

Saisissez le **code GIR** et appuyez sur la touche pour **armer**  / **désarmer**  / **mode Nuit** .

Par exemple: 1234 → 

Contrôle de sécurité du groupe à l'aide du code GIR :

Saisissez le **code GIR**, appuyez sur *****, entrez l'ID du groupe et appuyez sur **armer**  / **désarmer**  / **mode Nuit** .

Par exemple: 1234 → ***** → 2 → 

Gestion de la sécurité à l'aide de Tag ou Pass

1. Activez le clavier en faisant glisser votre main dessus. KeyPad Plus émet un signal sonore (s'il est activé dans les paramètres) et allume le rétroéclairage.



Notez que le clavier peut être activé automatiquement avec la fonction **Auto-réveil en cas de Temporisation au désarmement** si la Temporisation au désarmement est configurée. Cette fonction est compatible avec le KeyPad Plus Jeweller avec la version 5.60.7.0 du firmware ou une version ultérieure et les centrales avec OS Malevich 2.19 ou une version ultérieure.

2. Approcher Tag ou Pass au lecteur du pass/tag. Il est marqué par des icônes de vagues.
3. Saisissez le code requis si la fonction **Confirmation de l'autorisation avec un code d'accès** est activée.
4. Appuyez sur la touche **armer, désarmer** ou **mode Nuit** du clavier.



Notez que si l'option Changement facile du mode de sécurité est activée dans les paramètres du KeyPad Plus, il n'est pas nécessaire d'appuyer sur la touche **armer, désarmer** ou de **mode Nuit**. Le mode de sécurité passe à l'inverse après avoir appuyé sur Tag ou Pass.

Fonction de mise en sourdine de l'alarme d'incendie interconnectée

Le KeyPad Plus peut mettre sous silence une alarme d'incendie interconnectée en appuyant sur le **bouton de fonction** (si le paramètre requis est activé). La réponse du système à une pression sur un bouton dépend des réglages et de l'état du système :

- **L'alarme incendie interconnectée s'est déjà propagée** — au premier appui sur le bouton, toutes les sirènes des détecteurs d'incendie sont mises sous silence, sauf celles qui ont enregistré l'alarme. En appuyant à nouveau sur le bouton, les autres sirènes des détecteurs restent sous silence.
- **Temps de retard d'interconnexion des alarmes** — en appuyant sur le **bouton de fonction**, la sirène des détecteurs d'incendie Ajax déclenché est mise sous silence.

Gardez à l'esprit que l'option n'est disponible que si la fonction d'Alarme incendie interconnectée est activée.

En savoir plus



Avec la mise à jour d'OS Malevich 2.12, les utilisateurs peuvent désactiver les alarmes des détecteurs d'incendie de leurs groupes, sans affecter le fonctionnement des détecteurs

dans des groupes auxquels ils n'ont pas accès.

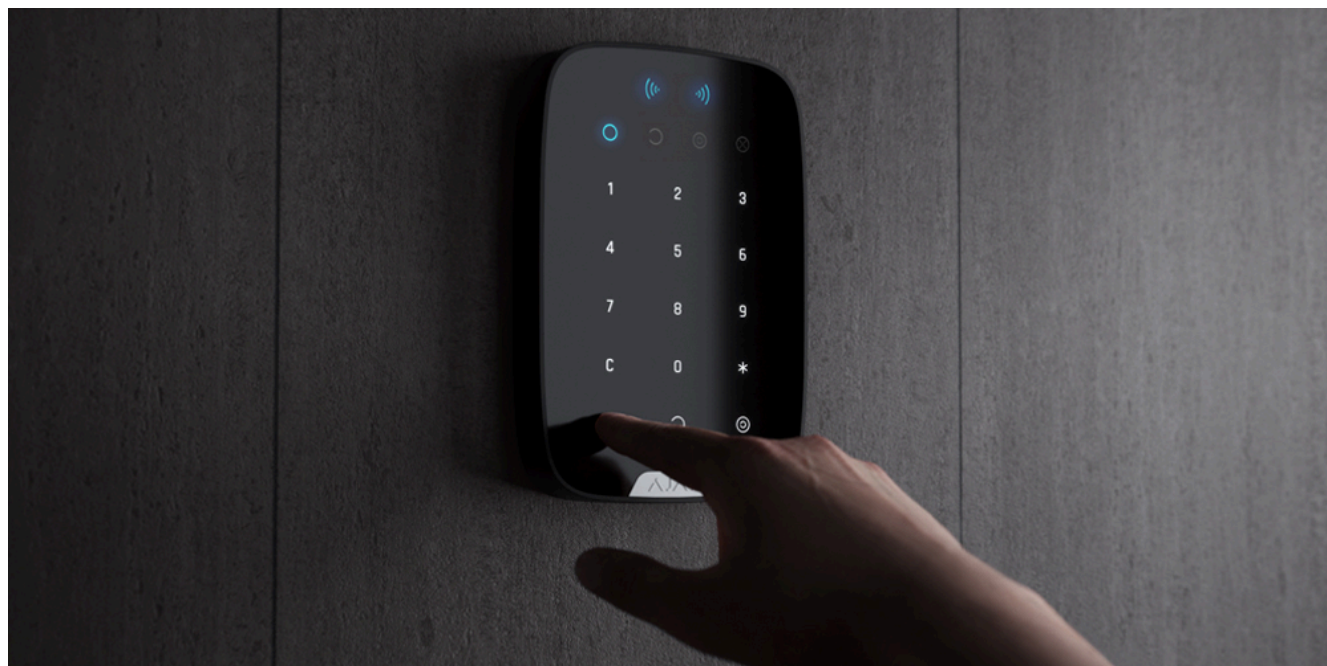
[En savoir plus](#)

Indication

KeyPad Plus peut signaler le mode de sécurité actuel, les frappes au clavier, les dysfonctionnements et son état par un indicateur LED et un son. Le mode de sécurité actuel est affiché par le rétroéclairage après l'activation du clavier. Les informations sur le mode de sécurité actuel sont pertinentes même si le mode armé est modifié par un autre dispositif : une télécommande, un autre clavier ou une application.



La fonction **Auto-réveil en cas de Temporisation au désarmement** permet d'activer automatiquement le clavier lorsque la [Temporisation au désarmement](#) est configurée. Cette fonction est compatible avec KeyPad Plus Jeweller avec la version 5.60.7.0 du firmware ou une version ultérieure et les centrales avec [OS Malevich 2.19](#) ou une version ultérieure.



Vous pouvez activer le clavier en faisant glisser votre main sur l'écran tactile de haut en bas. Lorsqu'il est activé, le rétroéclairage du clavier s'allume et un bip sonore retentit (s'il est activé).

Événement	Indication
Il n'y a pas de connexion à la centrale ou au prolongateur de portée	Clignotement de la LED X
Le boîtier du KeyPad Plus est ouvert (le support SmartBracket est retiré)	Clignotement de la LED X Brièvement en une fois
Bouton tactile appuyé	Bip court, la LED d'état de sécurité du système Ajax actuel clignote une fois. Le volume dépend des réglages du clavier
Le système est armé	Bip court, la LED du mode Armé ou mode Nuit s'allume
Le système est désarmé	Deux bips courts, la LED Désarmée s'allume
Un code incorrect a été saisi ou une tentative de changement de mode de sécurité a été effectuée par un pass/tag non connecté ou désactivé	Bip long, le rétroéclairage de l'unité numérique clignote 3 fois
Le mode de sécurité ne peut pas être activé (par exemple, une fenêtre est ouverte et le Vérification de l'intégrité du système est activé)	Bip long, le statut de sécurité actuel clignote 3 fois
La centrale ne répond pas à la commande — la connexion n'est pas établie	Bip long, la LED X (Dysfonctionnement) s'allume
Le clavier est verrouillé en raison d'une tentative de code erroné ou d'un essaie d'utilisation d'un pass/tag non autorisé	Bip long, pendant lequel les LED d'état de sécurité et le rétroéclairage du clavier clignent 3 fois
Les batteries sont faibles	Après avoir changé le mode de sécurité, la LED X s'allume. Les boutons tactiles sont verrouillés pour le moment. Lorsque vous essayez d'allumer le clavier avec des batteries déchargées, il émet un long bip, la LED X s'allume doucement et s'éteint, puis le clavier s'éteint <u>Comment remplacer les batteries du KeyPad Plus</u>
Le système exige de confirmer l'autorisation avec un code d'accès après la confirmation des dispositifs d'accès. Disponible si la fonction	Le voyant de l'état de sécurité actuel clignote pendant la durée programmée pour confirmation

Notifications sonores en cas de dysfonctionnement

Si un dispositif quelconque est hors ligne ou si la batterie est faible, le KeyPad Plus peut en informer les utilisateurs du système par un son audible. Les LED **X** des claviers clignotent. Les notifications de dysfonctionnement seront affichées dans le flux d'événements, dans le texte SMS ou dans la notification push.

Pour activer les notifications sonores de dysfonctionnements, utilisez les applications Ajax PRO et PRO Desktop :

1. Cliquez sur **Dispositifs** , choisissez la centrale et ouvrez ses paramètres  : Cliquez sur **Service** → **Sons et alertes**
2. Activez les interrupteurs : **Si la batterie d'un dispositif est faible** et **Si un dispositif est hors ligne**.
3. Cliquez sur **Retour** pour enregistrer les paramètres.



Les notifications sonores des dysfonctionnements sont disponibles pour toutes les centrales avec la version du firmware OS Malevich 2.15 ou plus.

Les notifications sonores des dysfonctionnements sont prises en charge par KeyPad Plus avec la version 5.57.5.0 du firmware ou une version plus récente.

Event	Indication	Note
Si un dispositif est hors ligne.	Deux courts signaux sonores, l'indicateur de dysfonctionnement X clignote deux fois. Émet un bip toutes les minutes jusqu'à ce que tous les	Les utilisateurs peuvent temporiser l'indication sonore pendant 12 heures.

	dispositifs du système soient en ligne.	
Si le KeyPad Plus est hors ligne.	Deux courts signaux sonores, l'indicateur de dysfonctionnement X clignote deux fois. Émet un bip toutes les minutes jusqu'à ce que le clavier du système soit en ligne.	Il est impossible de temporiser l'indication sonore.
Si la batterie d'un dispositif est faible.	Trois courts signaux sonores, l'indicateur de dysfonctionnement X clignote trois fois. Émet un bip une fois par minute jusqu'à ce que la batterie soit rechargée ou que le dispositif soit retiré.	Les utilisateurs peuvent temporiser l'indication sonore pendant 4 heures.

Les notifications sonores des dysfonctionnements apparaissent lorsque l'indication du clavier est terminée. Si plusieurs dysfonctionnements se produisent dans le système, le clavier signale d'abord la perte de connexion entre le dispositif et la centrale.

Test de fonctionnalité

Le système Ajax fournit plusieurs types de tests qui vous aident à vous assurer que les points d'installation des dispositifs sont sélectionnés correctement.

Les tests de fonctionnalité du KeyPad Plus ne démarrent pas immédiatement, mais au plus tard après une période de ping entre le détecteur et la centrale(36 secondes avec les paramètres standard de la centrale). Vous pouvez modifier la période de ping des dispositifs dans le menu **Jeweller** des paramètres de la centrale.

Les tests sont disponibles dans le menu des paramètres du dispositif (Application Ajax → Dispositifs  → KeyPad Plus → Paramètres 

- Test d'intensité du signal Jeweller
- Test d'atténuation du signal

Choix d'un emplacement



Il est préférable de placer le KeyPad Plus à l'intérieur, près de l'entrée. Cela permet de désarmer le système avant que les retards d'entrée n'aient expiré, ainsi que d'armer rapidement le système lorsque l'on quitte les lieux.



Lorsque vous tenez le KeyPad Plus dans vos mains ou que vous l'utilisez sur une table, nous ne pouvons pas garantir le bon fonctionnement des touches tactiles.

Pour des raisons de commodité, il est recommandé d'installer le clavier à une hauteur de 1,3 à 1,5 mètre au-dessus du sol. Installez le clavier sur une surface plane et verticale. Cela permet au KeyPad Plus d'être fermement fixé à la surface et d'éviter les faux déclenchements d'anti-sabotage.

En outre, l'emplacement du clavier est déterminé par la distance qui le sépare de la centrale ou du prolongateur de portée, et par la présence d'obstacles entre eux qui empêchent le passage du signal radio : murs, sols et autres objets.

Qu'est-ce qui affecte la portée de communication radio



Veillez à vérifier l'intensité du signal Jeweller sur le site d'installation. Si l'intensité du signal est faible (une seule barre), nous ne pouvons pas garantir un fonctionnement stable du système de sécurité. Au minimum, déplacez le dispositif car un repositionnement, même de 20 cm, peut améliorer considérablement la réception du signal.

Si une intensité de signal faible ou instable est toujours signalée après le déplacement du dispositif, utilisez le prolongateur de portée du signal radio.

Ne pas installer le clavier :

- Dans les endroits où des compartiments de vêtements (par exemple, à côté du cintre), des câbles d'alimentation ou des câbles Ethernet peuvent obstruer le clavier. Cela peut entraîner un faux déclenchement du clavier.
- L'intérieur des locaux dont la température et l'humidité sont en dehors des limites autorisées. Cela pourrait endommager le dispositif.
- Dans les endroits où le KeyPad Plus a une puissance de signal instable ou faible avec la centrale ou le prolongateur de portée.
- A moins un (1) mètre d'une centrale ou d'un prolongateur de portée. Cela pourrait entraîner une perte de connexion avec le clavier.
- Près du câblage électrique. Cela peut provoquer des interférences de communication.
- A l'extérieur. Cela pourrait endommager le dispositif.

Installation du clavier



Avant d'installer le KeyPad Plus, assurez-vous de choisir l'emplacement optimal en respectant les exigences de ce manuel.

1. Fixez le clavier sur la surface à l'aide d'une bande adhésif double face et effectuez des **tests d'atténuation** et d'**intensité du signal**. Si l'intensité du signal est instable ou si une seule barre est affichée, déplacez le clavier ou utilisez le prolongateur de portée.



La bande adhésive double face ne peut être utilisée que pour la fixation temporaire du clavier. Le dispositif fixé avec du ruban adhésif peut à tout moment se détacher de la surface et tomber, ce qui peut entraîner une défaillance. Veuillez noter que si le dispositif est fixé avec une bande adhésive, le bouton anti-sabotage ne se déclenchera pas lorsqu'on essaiera de le détacher.

2. Vérifiez la commodité de la saisie du code, ainsi que de l'utilisation du Tag ou Pass, pour gérer les modes de sécurité. S'il n'est pas pratique de gérer la sécurité à l'endroit choisi, déplacez le clavier.
3. Retirez le clavier du panneau de montage du SmartBracket.
4. Fixez le panneau de montage du SmartBracket à la surface à l'aide des vis jointes. Lors du montage, utilisez au moins deux points de fixation. Veillez à fixer le coin perforé sur la plaque du SmartBracket afin que l'anti-sabotage réagisse à une tentative de détachement.



5. Faites glisser le KeyPad Plus sur le panneau de montage et serrez la vis de montage située au bas du boîtier. La vis est nécessaire pour une fixation plus fiable et pour protéger le clavier d'un démontage rapide.

6. Dès que le clavier est fixé sur le SmartBracket, la LED **X** clignote une fois — c'est le signal que l'anti-sabotage a été déclenché. Si la LED ne clignote pas après l'installation sur le SmartBracket, vérifiez l'état de l'anti-sabotage dans l'application Ajax, puis assurez-vous que la plaque soit bien fixée.

Maintenance



Vérifiez régulièrement le fonctionnement de votre clavier. Cela peut être fait une ou deux fois par semaine. 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 contenant de l'alcool, de l'acétone, de l'essence ou d'autres solvants actifs pour nettoyer le détecteur. Essuyez délicatement le clavier tactile : les rayures peuvent réduire la sensibilité du clavier.

Les batteries installées dans le clavier assurent jusqu'à 3,5 ans de fonctionnement autonome avec les réglages par défaut. Si la batterie est faible, le système envoie des notifications appropriées, et l'indicateur **X (Dysfonctionnement)** s'allume en douceur et s'éteint après chaque saisie réussie du code.

KeyPad Plus peut fonctionner jusqu'à 2 mois après le signal de batterie faible. Cependant, nous vous recommandons de remplacer les batteries dès qu'elles vous

sont signalées. Il est conseillé d'utiliser des batteries au lithium. Ils ont une grande capacité et sont moins soumis aux températures.

Combien de temps les dispositifs Ajax fonctionnent-ils avec des batteries, et qu'est-ce qui influe sur cela

Comment remplacer les batteries du KeyPad Plus

Kit complet

1. KeyPad Plus
2. Panneau de montage SmartBracket
3. 4 batteries au lithium préinstallées AA (FR6)
4. Kit d'installation
5. Guide rapide

Caractéristiques techniques

Toutes les spécifications techniques de KeyPad Plus Jeweller

Conformité aux normes

Garantie

La garantie des produits de la Limited Liability Company "Ajax Systems Manufacturing" est valable 2 ans après l'achat et ne s'étend pas aux batteries groupées.

Si le dispositif ne fonctionne pas correctement, nous vous recommandons de contacter d'abord le service d'assistance, car la moitié des problèmes techniques peuvent être résolus à distance.

[Obligations de garantie](#)

[Accord utilisateur](#)

Contacter l'assistance technique :

- [e-mail](#)
- [Telegram](#)

Abonnez-vous à nos e-mails et découvrez nos derniers conseils sécurité. Aucun spam

S'abonner