Manuel utilisateur Superior KeyPad Plus G3 Jeweller

Mis à jour November 21, 2025

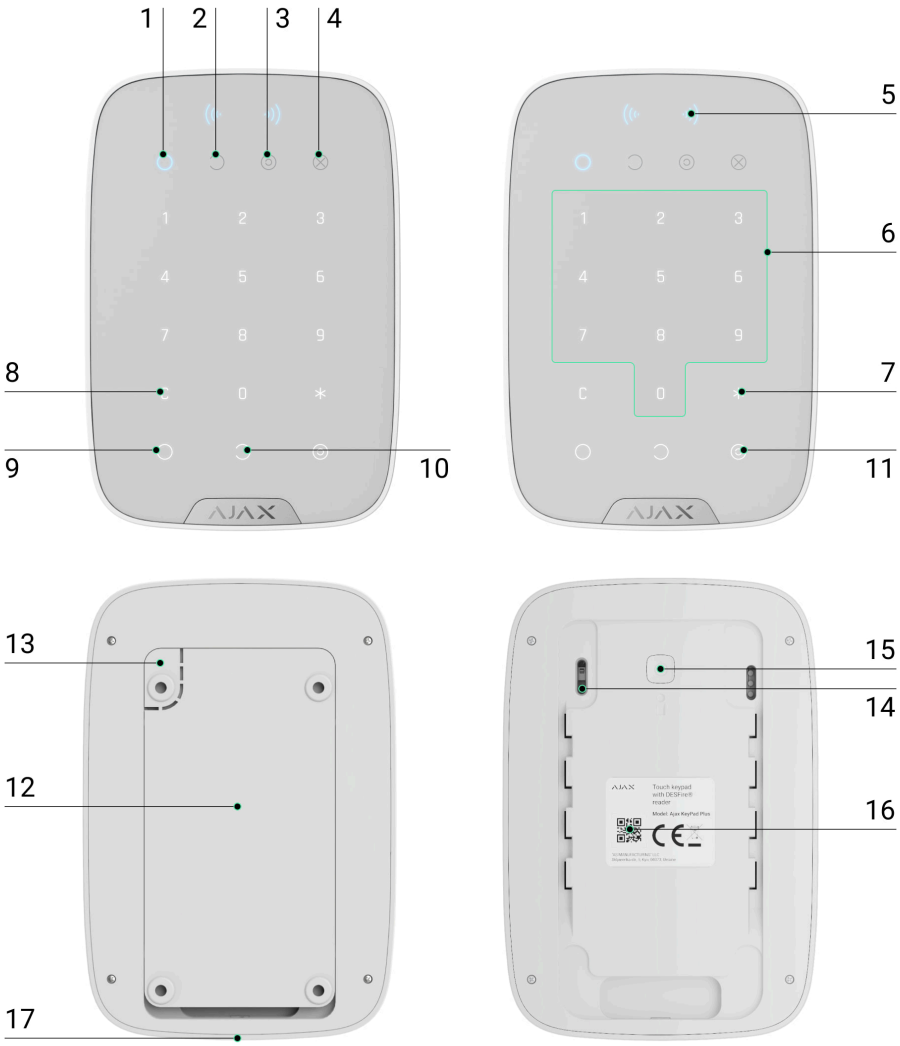
Superior KeyPad Plus G3 Jeweller est un clavier sans fil conçu pour gérer les systèmes Ajax. Les utilisateurs peuvent s'authentifier à l'aide de badges **Tag**, de cartes **Pass** et de codes d'accès. Le dispositif est destiné à être utilisé à l'intérieur uniquement.

Le clavier fait partie d'un système Ajax et échange des données avec la centrale en utilisant le protocole de communication radio sécurisé Jeweller.

Superior KeyPad Plus G3 Jeweller est un dispositif de la **ligne de produits Superior**. Seuls les partenaires accrédités d'Ajax Systems peuvent vendre, installer et entretenir des produits Superior.

Acheter Superior KeyPad Plus G3 Jeweller

Éléments fonctionnels



1. Indicateur **Armé**.

2. Indicateur **Désarmé**.

3. Indicateur **Mode nuit**.

4. Indicateur **Dysfonctionnement**.

5. Lecteur Pass/Tag.

6. Clavier numérique.

7. ✳ Bouton de **Fonction**.

8. C Bouton de **Réinitialisation**.

9. ◯ Bouton **Armer**.

10. Bouton **Désarmer**.
11. Bouton **Mode nuit**.
12. Panneau de montage SmartBracket. Pour enlever le panneau, dévissez la vis de fixation et faites glisser le panneau vers le bas.
13. Partie perforée du panneau de montage. Nécessaire pour déclencher le bouton anti-sabotage en cas de tentative de détacher le dispositif de la surface. Ne la cassez pas.
14. **Bouton anti-sabotage**.
15. Bouton d'alimentation.
16. QR code avec l'ID du dispositif. Il est utilisé pour ajouter le dispositif à la centrale.
17. Vis de fixation pour sécuriser le dispositif sur le SmartBracket.

Centrales compatibles

Une centrale Ajax avec **OS Malevich 2.35** et versions ultérieures est requise pour que le clavier fonctionne.

Vérifier la compatibilité du dispositif

Principe de fonctionnement

0:00 / 0:04

Superior KeyPad Plus G3 Jeweller est doté de grands touches tactiles, d'un lecteur pour l'autorisation sans contact et d'indicateurs LED. Le clavier est utilisé pour gérer les modes de sécurité, envoyer une alarme de panique ou couper l'alarme incendie.

Le Superior KeyPad Plus G3 Jeweller a des indicateurs LED montrant le mode de sécurité actuel et les dysfonctionnements du clavier (le cas échéant). L'état de la sécurité n'est affiché que lorsque le clavier est actif (le rétroéclairage du dispositif est allumé).

Le Superior KeyPad Plus G3 Jeweller peut être utilisé dans des conditions de faible luminosité car il dispose d'un rétroéclairage. L'appui sur les boutons est accompagné d'un signal sonore. La luminosité du rétroéclairage et le volume du clavier sont réglables dans les paramètres. Si le clavier n'est pas touché pendant 4 secondes, le Superior KeyPad Plus G3 Jeweller réduit la luminosité du rétroéclairage. Après 8 secondes d'inactivité, il entre en mode d'économie d'énergie et éteint l'écran.

Si la charge de la batterie est faible, le rétroéclairage s'allume au niveau minimum, indépendamment des paramètres.

Contrôle de sécurité

Superior KeyPad Plus G3 Jeweller peut armer et désarmer l'ensemble du site ou des groupes spécifiques et activer le **Mode nuit**. Vous pouvez gérer

la sécurité à l'aide du Superior KeyPad Plus G3 Jeweller en utilisant :

1. **Cartes ou badges**. Pour identifier rapidement et en toute sécurité les utilisateurs, Superior KeyPad Plus G3 Jeweller utilise la technologie DESFire ®. DESFire® est basé sur la norme internationale ISO 14443 et combine un chiffrement complet à 128 bits et une protection contre la copie. **Tag** et **Pass** prennent en charge cette technologie et sont compatibles avec Superior KeyPad Plus G3 Jeweller.
2. **Codes**. Superior KeyPad Plus G3 Jeweller prend en charge les codes généraux, les codes personnels et les codes pour les utilisateurs non enregistrés.

Codes d'accès

- **Code clavier** est un code général configuré pour le clavier. Lorsqu'il est utilisé, tous les événements sont transmis aux applications Ajax par le biais du clavier.
- **Code utilisateur** est un code personnel défini 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 des claviers** sont des codes configurés pour des personnes qui ne sont pas enregistrées dans le système. Lorsqu'il est utilisé, les événements sont délivrés 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 personnels, codes d'accès des claviers et codes GIR dépend du modèle de centrale.

Vérifier la compatibilité du dispositif

Les droits d'accès et les codes peuvent être ajustés dans les applications Ajax. Si le code est compromis, il peut être modifié à distance, sans avoir besoin d'appeler un installateur sur le site. Si un utilisateur perd son Pass ou son Tag, un administrateur ou un PRO disposant de droits de configuration du système peut instantanément bloquer le dispositif dans l'application. En attendant, un utilisateur peut utiliser un code personnel pour gérer le système.

Contrôle de sécurité des groupes

Superior KeyPad Plus G3 Jeweller permet de contrôler la sécurité des groupes (si le **mode Groupe** est activé). Un administrateur ou un PRO ayant les droits de configuration du système peut également ajuster les **paramètres** du clavier pour déterminer quels groupes seront partagés (groupes de clavier). Pour en savoir plus sur la gestion de la sécurité des groupes, consultez **ce chapitre**.

Bouton de fonction

Superior KeyPad Plus G3 Jeweller a le ✳ **bouton de Fonction** qui fonctionne dans l'un des trois modes :

- **Off** – le bouton de **Fonction** ne marche pas : si l'utilisateur appuie dessus, rien ne se passe.
- **Panique** – après avoir appuyé sur le bouton de **Fonction**, le système envoie une alarme au centre de télésurveillance de l'entreprise de sécurité et à tous les utilisateurs.
- **Désactiver l'alarme incendie** – après avoir appuyé sur le bouton de **Fonction**, le système coupe l'alarme des détecteurs d'incendie Ajax. Disponible uniquement si la fonction **Alarme incendie interconnectée** est activée (Centrale → Paramètres ⚙ → Service → Paramètres des détecteurs d'incendie).

Code de contrainte

Le Superior KeyPad Plus G3 Jeweller prend en charge un **code de contrainte** qui permet à un utilisateur de simuler le désarmement du système. Dans ce cas, ni l'**application Ajax** ni les **sirènes** installées sur le site ne révèleront vos actions. Le centre de télésurveillance et les autres utilisateurs du système de sécurité seront néanmoins avertis de l'incident.

En savoir plus

Accès non autorisé. Auto-verrouillage

Si un code incorrect est saisi ou si un dispositif d'accès non vérifié est utilisé trois fois de suite en moins d'une minute, le clavier se verrouille pour la durée spécifiée dans ses **paramètres**. Pendant ce temps, la centrale ignore tous les codes et dispositifs d'accès, tout en informant les utilisateurs du système de sécurité de la tentative d'accès non autorisé.

Un PRO ou un utilisateur disposant de droits de configuration du système peut débloquer le clavier via l'application avant l'expiration du délai de verrouillage spécifié.

Armement en deux étapes

Superior KeyPad Plus G3 Jeweller peut participer à l'armement en deux étapes, mais ne peut pas être utilisé en tant que dispositif de deuxième étape. Le processus d'armement en deux étapes à l'aide de Tag ou Pass est similaire à l'utilisation d'un code personnel ou général sur le clavier.

En savoir plus

Silence de l'alarme incendie

Le Superior KeyPad Plus G3 Jeweller peut désactiver une alarme incendie interconnectée en appuyant sur le **bouton de Fonction** (si le paramètre requis est activé). La réponse du système à l'appui sur le bouton dépend des réglages et de l'état du système :

- **L’alarme de détecteur d’incendie interconnectée a déjà été propagée** – par la première pression du bouton, toutes les sirènes des détecteurs d’incendie sont désactivées, sauf celles qui ont enregistré l’alarme. En appuyant à nouveau sur le bouton, les détecteurs restants sont mis sous silence.

- **La temporisation de l’alarme interconnectée est en cours** – l’appui sur le bouton de **Fonction** coupe la sirène du détecteur incendie Ajax déclenché.

Rappelez-vous que l’option n’est disponible que si **Alarme incendie interconnectée** est activée.

En savoir plus

Protocole de transfert de données Superior Jeweller

Superior Jeweller est un protocole radio amélioré pour les dispositifs Superior, garantissant la conformité à la norme **Grade 3** (EN 50131). Il est doté d’un **chiffrement** avancé et d’un **saut de fréquence**. La protection par sauts de fréquence complète n’est disponible que si tous les dispositifs du système utilisent Superior Jeweller. Si au moins un dispositif fonctionne avec le protocole standard Jeweller, le système sera limité au **Grade 2** : le chiffrement est maintenu, mais les sauts de fréquence sont désactivés. Les dispositifs Superior sont également compatibles avec le protocole Jeweller standard, en fonction de la centrale.

En savoir plus

Communication chiffrée avancée

La communication entre Superior KeyPad Plus G3 Jeweller et la centrale est protégée par un système de chiffrement avancé qui garantit la confidentialité et l’intégrité des données. Cela veut dire que les informations importantes dans le message sont chiffrées, et que chaque message a une balise spéciale pour s’assurer que les données n’ont pas été changées en cours de route. Le système peut détecter les tentatives

de sabotage et rejeter les messages faux ou modifiés. Cela le protège efficacement contre les attaques, qu'elles soient discrètes ou directes. Cela garantit une communication sécurisée entre le dispositif et la centrale, ainsi qu'une protection fiable du système et des données.

Saut de fréquence

Pour se conformer aux exigences de la norme Grade 3, le clavier Superior KeyPad Plus G3 Jeweller utilise le **saut de fréquence** pour la communication radio avec la centrale (ou le prolongateur de portée du signal radio). Avec cette méthode, la centrale et les dispositifs connectés changent leur fréquence de fonctionnement en suivant un schéma précis. La séquence de saut utilise un groupe de fréquences prédéterminé, et les dispositifs changent de fréquence en même temps que la centrale. Même si certaines fréquences sont affectées par le brouillage, les messages peuvent être transmis avec succès via d'autres fréquences. Le saut de fréquence améliore la fiabilité et la performance du système, et garantit sa résistance aux interférences intentionnelles et aux tentatives de brouillage.

Le saut de fréquence ne cause pas de ralentissements ni de coupures durant la communication radio, et ne diminue pas la vitesse de transfert des données. Si des **prolongateurs de portée** sont ajoutés au système, le saut de fréquence est utilisé pour toutes les communications radio : « dispositif ↔ prolongateur de portée » et « prolongateur de portée ↔ centrale ».

Le système utilise le saut de fréquence pour les communications radio uniquement si tous les dispositifs sans fil prennent en charge cette méthode.

Si au moins un dispositif ajouté au système ne prend pas en charge le saut de fréquence, la centrale et tous les dispositifs passent aux fréquences de fonctionnement de ce dispositif et n'utilisent pas le saut de fréquence pour la communication radio.

En savoir plus sur le brouillage

Transmission d’événements au centre de télésurveillance

Le système de sécurité Ajax peut transmettre des alarmes à l’application de surveillance **Ajax PRO Desktop** et au centre de télésurveillance aux formats **SurGard (Contact ID), SIA (DC- 09), ADEMCO 685** et d’**autres protocoles**.

Superior KeyPad Plus G3 Jeweller peut transmettre les événements suivants :

1. Armement/désarmement du système.
2. Saisie du code de contrainte.
3. Appui sur le bouton de panique.
4. Verrouillage du clavier suite à une tentative d’accès non autorisé.
5. Tentative infructueuse d’armer le système de sécurité (avec **vérification de l’intégrité du système** activée).
6. Alarme du bouton anti-sabotage. Récupération du bouton anti-sabotage.
7. Perte/rétablissement de la connexion avec la centrale.
8. Désactivation forcée / activation du dispositif.
9. Désactivation unique / activation du dispositif.

Lorsqu’une alarme est reçue, l’opérateur du centre de télésurveillance sait exactement ce qui s’est passé et où envoyer l’équipe d’intervention rapide. L’adressage des dispositifs Ajax permet d’envoyer des événements à **Ajax PRO Desktop** ou au centre de télésurveillance, y compris le type de dispositif, son prénom, le groupe de sécurité et la pièce virtuelle. La liste des paramètres transmis peut différer selon le type de centre de télésurveillance et le protocole de communication sélectionné.

Vous pouvez trouver l’ID du dispositif et le numéro de boucle (zone) dans ses états.

Sélection de l’emplacement

Lorsque vous choisissez l’endroit où installer votre Superior KeyPad Plus G3 Jeweller, tenez compte des paramètres qui affectent son fonctionnement :

- **Intensité du signal Jeweller**

Tenez compte des recommandations de l’emplacement lors de l’élaboration d’un projet pour le système de sécurité du site. Le système Ajax doit être conçu et installé par des spécialistes. Une liste des partenaires officiels autorisés d’Ajax est **disponible ici**.

Il est préférable d’installer le Superior KeyPad Plus G3 Jeweller à l’intérieur, à proximité de l’entrée. Cela permet aux utilisateurs de désarmer le site avant d’entrer dans les locaux ou jusqu’à ce que les temporisations au désarmement expirent. Les utilisateurs peuvent également armer rapidement le site lorsqu’ils quittent les lieux.

La hauteur d’installation recommandée est de 1,3–1,5 m au-dessus du sol. Installez le clavier sur une surface plane et verticale. Cela garantit que votre Superior KeyPad Plus G3 Jeweller est solidement fixé à la surface et permet d’éviter les déclenchements intempestifs du bouton anti-sabotage.

Lorsque vous tenez le Superior KeyPad Plus G3 Jeweller dans vos mains ou que vous l'utilisez sur une table, nous ne pouvons pas garantir que les touches tactiles fonctionneront correctement.

Intensité du signal

Le niveau du signal est déterminé par le nombre de paquets de données non livrés ou endommagés sur une période de temps donnée. L'icône dans l'onglet **Dispositifs** dans les applications Ajax indique l'intensité du signal :

- **trois barres** – excellente intensité du signal ;
- **deux barres** – bonne intensité du signal ;
- **une barre** – intensité du signal faible, le fonctionnement stable n'est pas garanti ;
- **icône barrée** – pas de signal.

Vérifiez l'intensité du signal Jeweller avant l'installation permanente. Avec une intensité du signal d'une ou zéro barre, nous ne garantissons pas que le dispositif fonctionnera de manière stable. Envisagez de déplacer le dispositif, car un ajustement de sa position, même de 20 cm, peut améliorer considérablement l'Intensité du signal. Si le signal reste faible ou instable après le déplacement, envisagez d'utiliser un prolongateur de portée du signal radio.

Reportez-vous à la section **Tests de fonctionnalité** pour savoir comment exécuter le test d'intensité du signal Jeweller.

Quel est le test d'intensité du signal Jeweller

Où ne pas installer le clavier

1. À l'extérieur. Cela peut entraîner une défaillance du dispositif.

2. Dans les endroits où des câbles d'alimentation ou Ethernet, des objets décoratifs ou autres peuvent obstruer le clavier.
3. Dans les endroits où la température et l'humidité dépassent les limites autorisées. Cela pourrait endommager le dispositif.
4. À une distance inférieure à 1 m de la centrale ou du prolongateur de portée du signal radio.
5. Dans les endroits où la puissance du signal Jeweller est faible ou instable.

Installation

Avant d'installer votre Superior KeyPad Plus G3 Jeweller, assurez-vous que vous avez choisi l'emplacement optimal et qu'il est conforme aux directives de ce manuel.

Pour installer le dispositif :

1. Dévissez la vis de fixation située au bas du dispositif et retirez le panneau de montage SmartBracket du clavier.
2. **Ajoutez le dispositif au système**.
3. Fixez temporairement le panneau SmartBracket à une surface verticale ou à un coin à l'aide d'une bande adhésive double face ou d'autres fixations temporaires.

Le ruban adhésif double-face ne peut être utilisé que pour une installation temporaire. Le dispositif fixé par le ruban adhésif peut se décoller de la surface à tout moment. Lorsque le dispositif est fixé avec le ruban, le bouton anti-sabotage ne de déclanchera pas lorsque le dispositif se détache de la surface.

4. Placez le clavier sur le panneau de montage SmartBracket. L'indicateur LED **X** du dispositif clignotera, indiquant que le boîtier du

dispositif est fermé.

5. Exécutez les **tests de fonctionnalité**.
6. Si les tests sont réussis, retirez le clavier du SmartBracket.
7. Fixez le SmartBracket sur la surface à l'aide des vis fournies. Utilisez tous les points de fixation.

> Lorsque vous utilisez d'autres éléments de fixation, assurez-vous qu'ils n'endommagent pas ou ne déforment pas le panneau.

8. Placez le clavier sur le panneau de montage SmartBracket.
9. Serrez la vis de fixation située sous le boîtier du clavier. La vis est nécessaire pour une fixation plus fiable et pour protéger le clavier du démontage rapide.

Ajout au système

> La centrale et le dispositif fonctionnant à des fréquences radio différentes sont incompatibles. La portée de la fréquence radio de l'appareil peut varier selon les régions. Nous recommandons d'acheter et d'utiliser des dispositifs Ajax dans le même pays. Vous pouvez vérifier la gamme des fréquences radio opérationnelles auprès du service d'assistance technique.
>
> Vérifiez la compatibilité des dispositifs avant que le dispositif ne soit ajouté au système. Seuls les partenaires vérifiés peuvent ajouter et configurer les dispositifs Superior dans les applications Ajax PRO.
>
> Types de comptes et leurs droits

Avant d'ajouter un dispositif

1. Installez une **application Ajax PRO**.
2. Connectez-vous à un **compte PRO** ou créez-en un nouveau.

3. Sélectionnez un **espace** ou créez-en un nouveau.
4. Ajoutez au moins une **pièce virtuelle**.
5. Ajoutez une **centrale compatible** à l'espace. Assurez-vous que la centrale est allumée et qu'elle dispose d'un accès Internet via Ethernet, Wi-Fi et/ou réseau mobile.
6. Vérifiez les états dans l'application Ajax pour vous assurer que l'espace est désarmé et que la centrale ne démarre pas de mise à jour.

Ajout à la centrale

1. Ouvrez une **application Ajax PRO**. Sélectionnez un **espace** auquel vous souhaitez ajouter le dispositif.
2. Allez dans l'onglet **Dispositifs** et appuyez sur **Ajouter un dispositif**.
3. Attribuez un nom au dispositif.
4. Scannez le QR code ou saisissez manuellement l'ID du dispositif. Le QR code avec l'identifiant est placé sur le boîtier du dispositif. Il est également reproduit sur l'emballage du dispositif.
5. Sélectionnez une pièce virtuelle et un groupe de sécurité (si le **Mode groupe** est activé).
6. Cliquez sur **Ajouter** et le compte à rebours va commencer.
7. Allumez le dispositif en maintenant le bouton d'alimentation pendant 3 secondes.

Si la connexion échoue, réessayez dans 5 secondes. Si le nombre maximum de dispositifs a déjà été ajouté à la centrale, vous recevrez une notification d'erreur lorsque vous essayez d'ajouter plus.

Une fois ajouté à la centrale, le dispositif apparaîtra dans la liste des dispositifs de la centrale dans l'application Ajax. La mise à jour des états des dispositifs de la liste dépend des paramètres **Jeweller** ou **Jeweller/Fibra** et est de 36 secondes par défaut.

Superior KeyPad Plus G3 Jeweller ne fonctionne qu'avec une seule centrale. Lorsqu'il est connecté à une nouvelle centrale, le clavier cesse d'envoyer des événements à l'ancienne. Une fois ajouté à une nouvelle centrale, le clavier n'est pas automatiquement supprimé de la liste des dispositifs de l'ancienne centrale. Cela doit être fait manuellement dans l'application Ajax.

Test de fonctionnalité

Le système de sécurité Ajax propose plusieurs types de tests pour vous aider à choisir le bon endroit pour installer les dispositifs. Les tests suivants sont disponibles pour Superior KeyPad Plus G3 Jeweller :

- **Test d'intensité du signal Jeweller** – pour déterminer l'intensité du signal et sa stabilité entre la centrale (ou le prolongateur de portée du signal radio) et le dispositif via le protocole de transfert de données Jeweller sans fil sur le site d'installation du dispositif.
- **Test d'atténuation du signal** – pour diminuer ou augmenter la puissance du transmetteur radio ; pour vérifier la stabilité de la communication entre le dispositif et la centrale, l'environnement changeant sur le site est simulé.

Icônes

Les icônes dans l'application Ajax affichent certains des états du Superior KeyPad Plus G3 Jeweller. Les icônes peuvent être vérifiées dans l'onglet **Dispositifs** .

Icône	Signification
	Intensité du signal Jeweller. Affiche l'intensité du signal entre la centrale et le dispositif. Valeurs recommandées de 2 à 3 barres. En savoir plus

	Niveau de charge de batterie du dispositif. **En savoir plus**
	Le dispositif fonctionne via le prolongateur de portée du signal radio. **En savoir plus**
	Lecture du Pass/Tag est activée dans les paramètres du clavier.
	Le dispositif est en mode de test d'atténuation du signal. **En savoir plus**
	Le dispositif est désactivé de façon permanente. **En savoir plus**
	Les notifications d'alarme anti-sabotage sont désactivées de manière permanente. **En savoir plus**
	Le dispositif est désactivé jusqu'au premier désarmement du système. **En savoir plus**
	Les notifications d'alarme du bouton anti-sabotage sont désactivées jusqu'à ce que le site soit désarmé pour la première fois. **En savoir plus**
	Le dispositif a perdu la connexion avec la centrale ou la centrale a perdu la connexion avec le serveur Ajax Cloud.
	Le dispositif n'a pas été transféré à la nouvelle centrale. **En savoir plus**

États

Les états comprennent des informations sur le dispositif et ses paramètres de fonctionnement. Les états du Superior KeyPad Plus G3 Jeweller se trouvent dans les applications Ajax :

1. Allez dans l'onglet **Dispositifs** .
2. Sélectionnez **Superior KeyPad Plus G3 Jeweller** dans la liste.

Paramètre	Signification
Importation de données	Affiche l'erreur lors du transfert de données vers la nouvelle centrale : • **Échoué** – le dispositif n'a pas été transféré vers la nouvelle centrale. En savoir plus
Dysfonctionnement	Un clic sur ⓘ ouvre la liste des dysfonctionnements. Ce champ s'affiche si un dysfonctionnement est détecté.
Température	Température du dispositif. Elle est mesurée par le processeur et varie en fonction de la température ambiante. Vous pouvez configurer un scénario par température pour contrôler les dispositifs d'automatisation. En savoir plus

Intensité du signal Jeweller	Intensité du signal Jeweller entre le dispositif et la centrale (ou le prolongateur de portée du signal radio). Valeurs recommandées de 2 à 3 barres. Jeweller est un protocole de transmission des événements et des alarmes.
Connexion via Jeweller	État de la connexion via le canal Jeweller entre le dispositif et la centrale (ou le prolongateur de portée) : • **En ligne** – le dispositif est connectée à la centrale ou au prolongateur de portée). État normal. • **Hors ligne** – le dispositif n'est pas connecté à la centrale ou au prolongateur de portée). Vérifiez la connexion du dispositif.
Puissance de l'émetteur	Affiche la puissance sélectionnée de l'émetteur. Ce paramètre apparaît lorsque l'option **Max** ou **Atténuation** est sélectionnée dans le menu **Test d'atténuation du signal**. En savoir plus
<Range extender name>	État de la connexion du dispositif au prolongateur de portée du signal radio : • **En ligne** – le dispositif est connectée au prolongateur de portée. • **Hors ligne** – le dispositif n'est pas connecté au prolongateur de portée. Ce champ est affiché si le dispositif fonctionne via un prolongateur de portée de signal radio.

Charge de la batterie	Niveau de charge de batterie du dispositif. Deux états sont disponibles : • **OK**. • **Batterie faible**. Lorsque les batteries sont faibles, les utilisateurs et le centre de télésurveillance reçoivent des notifications appropriées. ## En savoir plus
Couvercle	L'état du bouton anti-sabotage du dispositif qui réagit à l'arrachement ou à l'ouverture du boîtier : • **Ouvert** – le dispositif a été retiré du panneau de montage SmartBracket ou l'intégrité de son boîtier a été compromise. Vérifiez la fixation du dispositif. • **Fermé** – le dispositif est installé sur le panneau de montage SmartBracket. L'intégrité du boîtier du dispositif et du panneau de montage n'est pas compromise. État normal. ## En savoir plus
Lecture du Pass/Tag	Indique si le lecteur de cartes et de badges est activé.
Changement facile du mode de sécurité	Affiche le réglage de la fonction **Changement facile du mode de sécurité** : • **Off** – chaque tentative d'armement ou de désarmement doit être confirmée par la saisie du code d'accès ou la présentation du 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 en utilisant des dispositifs

	d'accès sans confirmation en appuyant sur les boutons du clavier. • **Désarmement sans confirmation par touche** – le système ou ses groupes, dont la sécurité est gérée avec un code d'accès ou des dispositifs d'accès, sera désarmé sans confirmation en appuyant sur les boutons du clavier. Une longueur de code d'accès fixe doit être définie dans les paramètres de la centrale dans l'application Ajax PRO.
Désactivation forcée	L'état du réglage de la désactivation forcée du dispositif : • **Non** – le dispositif fonctionne normalement et transmet tous les événements. • **Entièrement** – le dispositif est complètement exclu du fonctionnement du système. Le dispositif ne réagit pas aux commandes du système et ne signale pas les alarmes ou autres événements. • **Couvercle seulement** – l'administrateur de la centrale a désactivé les notifications relatives aux alarmes anti-sabotage. En savoir plus
Désactivation unique	Indique l'état du réglage de la désactivation unique du dispositif : • **Non** – le dispositif fonctionne normalement.

	• **Entièrement** – le dispositif est entièrement exclu du fonctionnement du système pendant que le mode armé est actif. Le dispositif ne réagit pas aux commandes du système et ne signale pas les alarmes ou autres événements. • **Couvercle seulement** – les notifications concernant le déclenchement de l'alarme anti-sabotage sont désactivées pendant que le mode armé est actif. En savoir plus
Firmware	Version firmware du dispositif.
ID du dispositif	ID du dispositif. Également disponible sur le QR code figurant sur le boîtier du dispositif et son emballage.
Dispositif n°	Numéro du dispositif. Ce numéro est transmis au centre de télésurveillance en cas d'alarme ou d'événement.

Paramètres

Pour modifier les paramètres de votre Superior KeyPad Plus G3 Jeweller dans les applications Ajax :

1. Allez dans l'onglet **Dispositifs** .
2. Sélectionnez **Superior KeyPad Plus G3 Jeweller** dans la liste.
3. Allez dans **Paramètres** .
4. Définissez les paramètres requis.
5. Cliquez sur **Retour** pour enregistrer les paramètres.

Paramètres	Signification

Nom	Nom du dispositif. Il est affiché dans la liste des dispositifs de la centrale, dans le texte SMS et dans les notifications du flux d'événements. Pour changer le nom du dispositif, cliquez sur le texte du nom. Le nom peut contenir 24 caractères cyrilliques ou 12 caractères latins.
Pièce	Sélection de la pièce virtuelle à laquelle votre Superior KeyPad Plus G3 Jeweller est assigné. Le nom de la pièce est affiché dans le texte SMS et les notifications dans le flux d'événement.
Gestion des groupes	Sélection des groupes de sécurité contrôlés par le dispositif. Vous pouvez sélectionner tous les groupes ou juste un seul groupe. Ce champ est affiché lorsque le **Mode groupe** est activé. Si la fonction Groupes suivis est configurée pour les groupes, leur état de sécurité peut automatiquement changer en fonction de leurs paramètres et de l'état des initiateurs.
Options d'accès	Sélection de la méthode d'armement/désarmement : • Codes clavier uniquement. • Codes utilisateur uniquement. • Codes clavier et codes utilisateur.

	Pour activer les **Codes d'accès des claviers** configurés pour les personnes qui ne sont pas enregistrées dans le système, sélectionnez les options sur le clavier : **Codes clavier uniquement** ou **Codes clavier et codes utilisateur**.
Code clavier	Sélection d'un code général pour le contrôle de sécurité. Contient 4 à 6 chiffres.
Code de contrainte	Sélection d'un code de contrainte générale pour l'alarme silencieuse. Contient 4 à 6 chiffres. En savoir plus
Bouton de Fonction	Sélection de la fonction du ✳ bouton (bouton de **Fonction**) : • **Off** – le bouton de fonction est désactivé et n'exécute aucune commande lorsqu'il est pressé. • **Panique** – 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** – en appuyant sur le bouton, l'alarme des détecteurs d'incendie Ajax est mise en sourdine. Disponible uniquement si la fonction **Alarme incendie interconnectée** est activée. En savoir plus
Protection contre la pression accidentelle	Une fois l'option activée, le bouton **Fonction** doit être pressé deux fois pour déclencher une alarme panique. Ce réglage est disponible si le **Bouton de fonction** est réglé sur **Panique**.
Accès non autorisé. Auto-verrouillage	Lorsque cette fonction est activée, le clavier est verrouillé pendant une durée prédéfinie

	si un code incorrect est saisi ou si des dispositifs d'accès non vérifiés sont utilisés plus de trois fois de suite en l'espace d'une minute. Un PRO ou un utilisateur disposant de droits de configuration du système peut débloquer le clavier via l'application avant l'expiration du délai de verrouillage spécifié.
Temps de verrouillage automatique, min	Sélection de la période de verrouillage du clavier après des tentatives d'accès non autorisées : • 3 minutes • 5 minutes • 10 minutes • 20 minutes • 30 minutes • 60 minutes • 90 minutes • 180 minutes Disponible si la bascule **Accès non autorisé auto-verrouillage** est activée.
Luminosité	Réglage de la luminosité du rétroéclairage des touches du clavier. Le rétroéclairage ne fonctionne que lorsque le clavier est actif. Cette option n'affecte pas le niveau de luminosité des indicateurs des modes de sécurité et du lecteur Pass/Tag.
Volume des boutons	Sélection du volume des touches du clavier lorsqu'on appuie dessus.
Lecture du pass/tag	Lorsque cette option est activée, le mode de sécurité peut être contrôlé par les dispositifs d'accès **Pass** et **Tag**.

Confirmation de l’autorisation avec un code d’accès	Lorsque cette fonction est activée, les utilisateurs ne peuvent armer ou désarmer le système que s’ils ont été autorisés avec succès à l’aide de deux formes d’identification, c’est-à-dire en utilisant les dispositifs Pass ou Tag et en saisissant le code d’accès approprié. **En savoir plus**
Délai de confirmation	Sélection du délai maximum pour confirmer l’autorisation avec un mot de passe après la confirmation du dispositif d’accès. Disponible si la **Confirmation de l’autorisation avec un code d’accès** est activé.
Changement facile du mode de sécurité	Permet aux utilisateurs d’armer/désarmer le système sans confirmation en appuyant sur les boutons du clavier. Trois options sont disponibles : • **Off** – chaque tentative d’armement ou de désarmement doit être confirmée par la saisie du code d’accès ou la présentation du dispositif d’accès. • **Armer/désarmer en utilisant un dispositif d’accès sans confirmation de l’action par les boutons** – permet aux utilisateurs de basculer les modes de sécurité du système en utilisant des dispositifs d’accès sans confirmation avec les boutons du clavier. • **Désarmement sans confirmation par touche** – le système ou ses groupes, dont la sécurité est gérée avec un code d’accès ou des dispositifs d’accès, sera désarmé sans confirmation en appuyant sur les boutons du clavier.  Une longueur de code d’accès fixe doit être définie

	dans les paramètres de la centrale dans l'application Ajax PRO.
Armement sans code	Lorsque cette fonctionnalité est activée, l'utilisateur peut armer le site sans saisir de code ni présenter son dispositif d'accès. Si cette fonction est désactivée, saisissez un code ou présentez le dispositif d'accès pour armer le système. L'écran pour saisir le code apparaît après avoir appuyé sur le bouton ◯ **Armer**.
Auto-réveil lors de Temporisation désarm	Active le clavier après qu'un dispositif de sécurité commence la **Temporisation au désarmement**. La fonction d'activation automatique peut également réduire l'autonomie de la batterie du clavier.
Alerte par sirène si un bouton de panique est appuyé	Le réglage s'affiche si l'option **Panique** est sélectionnée pour le bouton de **Fonction**. Lorsque l'option est activée, les sirènes connectées au système de sécurité donnent une alerte lorsque le ✳ bouton (**bouton de Fonction**) est pressé.
Test d'intensité du signal Jeweller	Bascule le dispositif en mode test d'intensité du signal Jeweller. Le test permet de vérifier l'intensité du signal entre la centrale (ou le prolongateur de portée du signal radio) et le dispositif via le protocole de transfert de données sans fil Jeweller, afin de sélectionner le site d'installation optimal. **En savoir plus**

Test d’atténuation du signal	Bascule le dispositif en mode de test d’atténuation du signal. **En savoir plus**
Réinitialisation du pass/tag	Permet de supprimer de la mémoire du dispositif toutes les centrales associées au dispositif Tag ou Pass. **En savoir plus**
Manuel de l’utilisateur	Ouvre le manuel utilisateur du Superior KeyPad Plus G3 Jeweller 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 et ne participera pas aux scénarios, et le système ignorera les alarmes et autres notifications du dispositif. • **Couvercle seulement** – le système ignorera uniquement des notifications relatives au déclenchement de l’alarme anti-sabotage du dispositif. **En savoir plus**
Désactivation unique	Permet à l’utilisateur de désactiver les événements du dispositif jusqu’au premier désarmement. Trois options sont disponibles : • **Non** – le dispositif fonctionne normalement et transmet tous les événements.

	• **Entièrement** – le dispositif est entièrement exclu du fonctionnement du système jusqu'au premier désarmement. Le dispositif ne réagit pas aux commandes du système et ne signale pas les alarmes ou autres événements. • **Couvercle seulement** – les notifications concernant le déclenchement de l'alarme anti-sabotage sont désactivées jusqu'au premier désarmement. En savoir plus
Supprimer le dispositif	Dissocie le dispositif, le déconnecte de la centrale et supprime ses paramètres.

Configuration des codes

Dans les applications Ajax PRO, dans les paramètres de la centrale, vous pouvez définir les exigences relatives à la longueur des codes d'accès utilisés pour l'autorisation de l'utilisateur et l'accès au système. Vous pouvez sélectionner l'option **Flexible (4 à 6 caractères)** ou définir la longueur de code fixe : **4 symboles**, **5 symboles**, ou **6 symboles**.

La définition d'une longueur de code fixe réinitialise tous les codes d'accès précédemment configurés.

La longueur de code fixe est requise pour la fonction **Changement facile du mode de sécurité**, qui permet de désarmer le système sans appuyer sur le bouton **Désarmer** du clavier après avoir saisi un code d'accès ou utilisé un dispositif d'accès.

Codes d'accès des claviers

Pour définir le code clavier et le code de contrainte du clavier :

1. Dans l'application Ajax, allez dans l'onglet **Dispositifs** .

2. Sélectionnez le clavier pour lequel vous souhaitez configurer un code d’accès.
3. Allez dans **Paramètres** ⚙.
4. Sélectionnez l’option **Codes des claviers uniquement** ou **Codes des claviers et de l’utilisateur** dans le menu **Options d’accès**.
5. Allez dans le menu **Codes d’accès des claviers**.
6. Définissez le code du clavier. Contient de 4 à 6 chiffres.
7. Appuyez sur **Terminé**.
8. Allez au menu **Code de contrainte**.
9. Définissez le code de contrainte du clavier. Contient de 4 à 6 chiffres.
10. Appuyez sur **Terminé**.

Codes utilisateur

Pour définir un code personnel et un code de contrainte personnel :

1. Sélectionnez un espace dans l’application Ajax.
2. Allez dans l’onglet **Paramètres** ⚙.
3. Ouvrez le menu **Utilisateurs**.
4. Trouvez votre compte dans la liste et cliquez dessus.
5. Allez dans **Paramètres code d’accès**.
6. Saisissez le **Code utilisateur**. Contient de 4 à 6 chiffres.
7. Appuyez sur **Enregistrer**.
8. Définissez le **Code de contrainte**. Contient de 4 à 6 chiffres.
9. Appuyez sur **Enregistrer**.
10. Cliquez sur **Retour** pour enregistrer les paramètres.

Codes pour les utilisateurs non enregistrés

Pour définir un code d'accès pour un utilisateur sans compte :

1. Sélectionnez une centrale dans l'application Ajax.
2. Allez dans l'onglet **Paramètres** ⚙.
3. Allez dans le menu **Codes d'accès des claviers**.
4. Appuyez sur **Ajouter** un code. Configurez le **Nom** et le **Code d'accès**. Contient de 4 à 6 chiffres.
5. Cliquez sur **Ajouter** pour enregistrer les données.

Pour définir un code de contrainte pour un utilisateur sans compte :

1. Sélectionnez le menu **Codes d'accès des claviers** dans les paramètres de la centrale.
2. Sélectionnez l'utilisateur non enregistré requis.
3. Appuyez sur **Ajouter un code de contrainte**. Définissez le code. Contient de 4 à 6 chiffres.
4. Appuyez sur **Terminé**.

> Pour les utilisateurs non enregistrés, un administrateur ou un PRO ayant les droits de configurer le système peut ajuster l'accès à la gestion de la sécurité. Tout d'abord, activez le Mode groupe. Ensuite, sélectionnez le menu **Codes d'accès des claviers** dans les paramètres de la centrale, trouvez l'utilisateur requis et définissez les paramètres appropriés dans le menu **Gestion de la sécurité**.

Code GIR

Seul un PRO ayant les droits de configuration du système peut créer et configurer les codes GIR dans l'**application Ajax PRO**. Vous trouverez plus d'informations sur la configuration de cette fonctionnalité dans **cet article**.

Cartes et badges

Le Superior KeyPad Plus G3 Jeweller peut fonctionner avec des badges **Tag**, des cartes **Pass** et des dispositifs tiers qui prennent en charge la technologie DESFire®.

> Avant d'ajouter des dispositifs tiers prenant en charge DESFire®, assurez-vous qu'ils disposent de suffisamment de mémoire libre pour prendre en charge le nouveau clavier. De préférence, le dispositif tiers doit être formaté à l'avance.
>
> Cet article fournit des informations sur la manière de réinitialiser le dispositif **Tag** ou **Pass**.

Le nombre maximum de dispositifs Pass et Tag ajoutés dépend du modèle de la centrale. Les dispositifs Pass et Tag ajoutés n'affectent pas la limite totale de dispositifs liés à la centrale.

Vérifier la compatibilité du dispositif

Ajout de Tag ou Pass

1. Ouvrez l'application Ajax.
2. Sélectionnez l'espace à laquelle vous souhaitez ajouter un badge Tag ou une carte Pass.
3. Allez dans l'onglet **Dispositifs** .

> Assurez-vous que la fonction **Lecture du pass/tag** est activée dans les paramètres d'au moins un clavier.

4. Appuyez sur **Ajouter un dispositif**.
5. Sélectionnez **Ajouter un pass/tag**.

6. Spécifiez le type (Tag ou Pass), la couleur, le nom du dispositif et l'utilisateur (si nécessaire).
7. Appuyez sur **Suivant**. Ensuite, la centrale passe en mode d'enregistrement des dispositifs.
8. Accédez à n'importe quel clavier compatible avec la **Lecture du pass/tag**. Appuyez sur le bouton **Désarmer** pour basculer le clavier en mode d'enregistrement des dispositifs d'accès.
9. Approchez la carte Pass ou le badge Tag avec le côté large contre le lecteur de clavier pendant quelques secondes. Si l'ajout est réussi, vous recevrez une notification dans l'application Ajax.

Si la connexion échoue, réessayez dans 5 secondes. Veuillez noter que si le nombre maximum de dispositifs Tag ou Pass a déjà été ajouté à la centrale, vous recevrez une notification correspondante dans l'application Ajax lors de l'ajout d'un nouveau dispositif.

Tag et Pass peuvent fonctionner avec plusieurs centrales en même temps. Le nombre maximal de centrales est de 13. Si vous essayez de lier un badge Tag ou une carte Pass à une centrale qui a déjà atteint sa limite, vous recevrez une notification correspondante. Pour ajouter un badge / une carte à une nouvelle centrale, vous devrez les réinitialiser.

Si vous avez besoin d'ajouter un autre Tag ou Pass, cliquez sur **Ajouter un autre dispositif Pass/Tag** dans l'application. Répétez les étapes 6 à 9.

Suppression du badge Tag ou de la carte Pass

La réinitialisation efface tous les réglages et toutes les connexions des badges et des cartes. Dans ce cas, le badge Tag et la carte Pass réinitialisés ne sont retirés que de la centrale depuis laquelle la réinitialisation a été effectuée. Sur d'autres centrales, le Tag ou la Pass sont toujours affichés dans l'application, mais ne peuvent pas être utilisés pour gérer les modes de sécurité. Ces dispositifs doivent être supprimés manuellement.

1. Ouvrez l’application Ajax.
2. Sélectionnez l’espace.
3. Allez dans l’onglet **Dispositifs** .
4. Sélectionnez un clavier compatible dans la liste des dispositifs.

> Assurez-vous que la fonction **Lecture du pass/tag** est activée dans les paramètres de clavier.

5. Accédez aux paramètres du clavier en cliquant sur l’icône .
6. Tapez sur **Réinitialisation du pass/tag**.
7. Cliquez sur **Continuer**.
8. Accédez à n’importe quel clavier compatible avec la **Lecture du pass/tag**. Appuyez sur le bouton **Désarmer** pour faire passer le clavier en mode de réinitialisation des dispositifs d’accès.
9. Approchez la carte Pass ou le badge Tag avec le côté large contre le lecteur de clavier pendant quelques secondes. Si le formatage est réussi, vous recevrez une notification dans l’application Ajax. Si le formatage échoue, veuillez réessayer.

Si vous devez réinitialiser un autre Pass ou une autre Tag, cliquez sur **Réinitialiser un autre dispositif Pass/Tag** dans l’application. Répétez l’étape 9.

Gestion de la sécurité

En utilisant des codes, Tag, ou Pass, vous pouvez gérer le **Mode nuit** et la sécurité de l’ensemble du site ou de groupes séparés. L’utilisateur ou le PRO ayant les droits de configuration du système peut configurer les codes d’accès. **Ce chapitre** fournit des informations sur la manière d’ajouter un badge Tag ou une carte Pass à la centrale.

Si un code personnel ou d'accès, un Tag ou un Pass est utilisé, le nom de l'utilisateur qui a modifié le mode de sécurité est affiché dans le flux d'événements de la centrale et dans la liste des notifications. Lorsqu'un code général est utilisé, le nom du clavier à partir duquel la modification du mode de sécurité a été effectuée s'affiche.

> Superior KeyPad Plus G3 Jeweller est verrouillé pour la durée spécifiée dans les paramètres si un code incorrect est saisi ou si un dispositif d'accès non vérifié est présenté trois fois de suite en l'espace d'une minute. Les notifications correspondantes sont envoyées aux utilisateurs et au centre de télésurveillance. Un utilisateur ou un PRO disposant des droits de configuration du système peut déverrouiller Superior KeyPad Plus G3 Jeweller dans l'application Ajax.

La séquence des étapes pour changer le mode de sécurité avec le clavier dépend de l'activation des options **Armement sans code**, **Confirmation de l'autorisation avec un code d'accès** et **Changement facile du mode de sécurité** dans les paramètres du Superior KeyPad Plus G3 Jeweller.

Utilisation d'un badge Tag ou d'une carte Pass

1. Activez le clavier en approchant votre main devant lui.
2. Approchez votre Tag ou votre Pass du lecteur du clavier.
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.

Si l'option **Changement facile du mode de sécurité** est activée, vous n'avez pas besoin d'appuyer sur le bouton **Armer**, **Désarmer** ou **Mode nuit** après que le dispositif d'accès ait été lu.

Utilisation des codes d'accès

Les codes saisis de manière incorrecte peuvent être effacés en appuyant sur le bouton **Réinitialisation**.

Code	Exemple	Remarque
Gestion des modes de sécurité du site		
Code clavier Code de contrainte du clavier	1234 → ◯ / ◯ / ◎	
Code utilisateur Code de contrainte de l'utilisateur	5 → ✳ → 1234 → ◯ / ◯ / ◎	**5** est un identifiant de l'utilisateur
Code de l'utilisateur non enregistré Code de contrainte de l'utilisateur non enregistré	1234 → ◯ / ◯ / ◎	
Code GIR	1234 → ◯ / ◯ / ◎	
Gestion des modes de sécurité du groupe		
Code clavier Code de contrainte du clavier	1234 → ✳ → 2 → ◯ / ◎	**2** est un identifiant du groupe
Code utilisateur Code de contrainte de l'utilisateur	5 → ✳ → 1234 → ✳ → 2 → ◯ / ◎	**5** est un identifiant de l'utilisateur **2** est un identifiant du groupe
Code de l'utilisateur non enregistré	1234 → ✳ → 2 → ◯ / ◎	**2** est un identifiant du groupe

Code de contrainte de l'utilisateur non enregistré		
Code GIR	1234 → ✱ → 2 → ◯/ ◎	**2** est un identifiant du groupe

En savoir plus sur l'identifiant de l'utilisateur

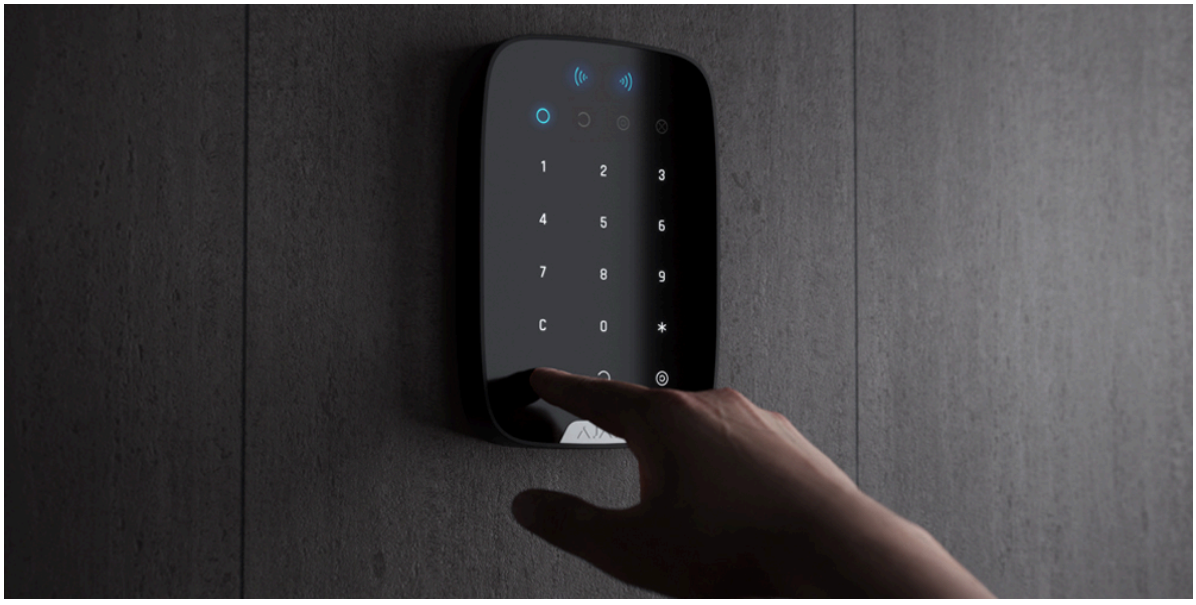
En savoir plus sur l'identifiant du groupe

Confirmation de l'autorisation avec un code d'accès

Confirmation de l'autorisation avec un code d'accès est une fonctionnalité qui permet de mettre en place une authentification à deux facteurs pour les utilisateurs lorsqu'ils contrôlent les modes de sécurité du système. Cela signifie que les utilisateurs doivent d'abord utiliser un dispositif d'accès (Pass ou Tag), puis saisir un code d'accès pour confirmer leur autorisation d'accès au système.

En savoir plus sur la Confirmation de l'autorisation avec un code d'accès

Indication



Le clavier Superior KeyPad Plus G3 Jeweller utilise des lumières (LED) et des sons pour vous informer du mode de sécurité actif, des touches que vous pressez, des problèmes éventuels, et de son état général. Le rétroéclairage affiche le mode de sécurité actuel après l'activation du clavier. Les informations sur le mode de sécurité actuel sont pertinentes même si le mode de sécurité est changé par un autre dispositif : une télécommande, un autre clavier ou une application.

Vous pouvez activer le clavier en passant votre main sur le panneau tactile de haut en bas. Lorsqu'il est activé, le rétroéclairage du clavier s'allume et un signal sonore retentit (s'il est activé).

Événement	Indication	Remarque
Mise en marche du dispositif	Tous les indicateurs et le rétroéclairage du pavé numérique s'allument brièvement. Ensuite, un bip à trois tons retentit et la LED du mode de sécurité du système actuel ainsi que le rétroéclairage du pavé numérique s'allument. Après cela, le rétroéclairage du pavé numérique s'éteint progressivement, et un double bip retentit	
Mise en marche du dispositif qui n'a pas été ajouté à la centrale	Tous les indicateurs et le rétroéclairage du pavé numérique s'allument brièvement. Après cela, la LED **X** clignote 6 fois et ensuite clignote 3 fois rapidement	Le clavier s'éteint après la fin de l'indication
Mise en arrêt du dispositif	La LED **X** s'allume pendant environ 1 s, puis clignote 3 fois	Le système envoie une notification lorsque le clavier est éteint à l'aide du bouton d'alimentation
Le dispositif est supprimé de la centrale	La LED **X** clignote 6 fois puis clignote 3 fois rapidement	Le clavier s'éteint après la fin de l'indication

Pas de connexion avec la centrale ou avec le prolongateur de portée du signal radio	La LED **X** clignote	
Le couvercle du dispositif est ouvert (le panneau de montage SmartBracket est enlevé)	La LED **X** clignote brièvement une fois	
Appui sur un bouton tactile	Bip court, la LED d'état du système clignote une fois	Le volume dépend des paramètres du clavier
Le système est armé	Bip court, les LED **Armé** ou **Mode nuit** s'allument	
Le système est désarmé	Deux bips courts, la LED **Désarmé** s'allume	
Un code incorrect a été saisi, ou une tentative de changement de mode de sécurité a été faite par un badge/carte déconnecté(e) ou désactivé(e)	Bip long, le rétroéclairage du pavé numérique clignote 3 fois	
Le mode de sécurité ne peut pas être activé (**Vérification de l'intégrité du système** échoue)	Bip long, la LED d'état de sécurité clignote 3 fois	
Le système nécessite de confirmer l'autorisation avec un mot de passe après la confirmation du dispositif d'accès. Disponible si l'option Confirmation de l'autorisation avec un code d'accès est activée	La LED d'état de sécurité clignote pendant la durée configurée pour la confirmation	
Le clavier est verrouillé en raison d'une tentative de code incorrect ou d'une tentative d'utiliser un badge/carte non autorisé(e)	Bip long, pendant lequel la LED d'état de sécurité et le rétroéclairage du clavier clignotent 3 fois	
La centrale ne répond pas	Bip long, la LED **X** s'allume	
Le niveau de charge de la batterie est faible	Après avoir changé le mode de sécurité, la LED **X** s'allume. Les boutons	## Comment remplacer les batteries

	tactiles sont verrouillés pendant ce temps. Lorsque vous essayez d'allumer le clavier avec des batteries déchargées, il émet un long bip, la LED **X** s'éclaire progressivement et s'éteint, puis le clavier s'éteint.	

Notifications sonores des dysfonctionnements

Le Superior KeyPad Plus G3 Jeweller peut informer les utilisateurs du système par un signal sonore si un dispositif est hors ligne ou si sa batterie est faible. La LED **X** du clavier clignote. Les notifications de dysfonctionnement seront affichées dans le flux d'événements, le texte SMS ou les notifications push.

Pour activer les notifications sonores de dysfonctionnements, allez dans une application Ajax PRO :

1. Allez dans l'onglet **Dispositifs** .
2. Sélectionnez la centrale, et allez dans ses paramètres .
3. Allez à **Service** → **Sons et alertes**.
4. Activez les commutateurs : **Si la batterie d'un dispositif est faible** et **Si un dispositif est hors ligne**.
5. Appuyez sur **Retour** pour enregistrer les paramètres.

Événement	Indication	Remarque
Si un dispositif est hors ligne	Deux signaux sonores courts, la LED **X** clignote deux fois.	Les utilisateurs peuvent temporiser l'indication sonore pendant 12 heures

	Bip une fois par minute jusqu'à ce que tous les dispositifs du système soient en ligne.	
Si le Superior KeyPad Plus G3 Jeweller est hors ligne	Deux signaux sonores courts, la LED **X** clignote deux fois. Bip une fois par minute 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 signaux sonores brefs, la LED **X** clignote trois fois. Bip une fois par minute jusqu'à ce que la batterie soit rétablie 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 notifiera d'abord la perte de connexion entre le dispositif et la centrale.

Dysfonctionnements

Lorsque le dispositif détecte un dysfonctionnement (par exemple, il n'y a pas de communication via le protocole Jeweller), un compteur de dysfonctionnement s'affiche dans l'application Ajax dans le coin supérieur gauche de l'icône du dispositif.

Tous les dysfonctionnements sont visibles dans les **états** du dispositif. Les champs présentant des dysfonctionnements seront mis en évidence en rouge.

Un dysfonctionnement est affiché si :

- La température du dispositif dépasse les limites admissibles.

- Le couvercle du dispositif est ouvert (l'alarme anti-sabotage s'est déclenchée).
- Pas de connexion avec la centrale ou le prolongateur de portée du signal radio via Jeweller.
- La batterie du dispositif est faible.

Maintenance

Vérifiez régulièrement le fonctionnement du dispositif. La fréquence optimale des contrôles est d'une fois tous les trois mois. Nettoyez la poussière, les toiles d'araignée et d'autres contaminants sur le boîtier du dispositif dès leur apparition. Utilisez un chiffon sec et doux, adapté à l'entretien du matériel.

N'utilisez pas de substances contenant de l'alcool, de l'acétone, de l'essence ou d'autres solvants actifs pour nettoyer le dispositif.

Si la batterie du clavier est faible, le système envoie des notifications appropriées, et la LED e **X Dysfonctionnement** s'allume et s'éteint après chaque saisie de code réussie.

Le Superior KeyPad Plus G3 Jeweller peut fonctionner pendant jusqu'à 2 mois après le signal de batterie faible. Toutefois, nous vous recommandons de remplacer les batteries dès que vous en êtes informé. Il est conseillé d'utiliser des batteries au lithium. Elles ont une grande capacité et sont moins affectés par les températures.

> **Comment remplacer les batteries dans le Superior KeyPad Plus G3 Jeweller**

Spécifications techniques

> **Toutes les caractéristiques techniques**

> **Conformité aux normes**

Configuration conformément aux exigences de la norme EN 50131

Garantie

La garantie des produits de la Limited Liability Company « Ajax Systems Manufacturing » est valable pendant 2 ans à compter de la date d'achat.

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

Obligations de garantie

Accord d'utilisation

Contacter l'assistance technique :

- e-mail
- Telegram

Fabriqué par « AS Manufacturing » LLC