# Clavier sans fil

## Manuel d’utilisation

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

# Avant-propos

## Général

Ce manuel présente l'installation, les fonctions et les opérations du clavier sans fil (ci-après dénommé « le clavier »). Lisez attentivement ce contenu avant d'utiliser l'appareil et conservez-le pour une future consultation.

## Modèle

DHI-ARK30T-W2 (868) ; DHI-ARK30T-W2

## Précautions d'emploi

Les mentions d'avertissement suivantes peuvent apparaître dans le manuel.

| Mentions d'avertissement | Signification |
|---|---|
| **DANGER** | Indique un danger risquant d'entraîner la mort ou des blessures graves si les instructions données ne sont pas respectées. |
| **AVERTISSEMENT** | Indique une situation moyennement ou faiblement dangereuse qui entraînera des blessures faibles ou modérées si les instructions données ne sont pas respectées. |
| **ATTENTION** | Indique une situation potentiellement dangereuse qui pourra entraîner des dommages de la propriété, des pertes de données, une performance moindre ou des résultats imprévisibles, si les instructions données ne sont pas respectées. |
| **CONSEILS** | Fournit des instructions qui vous permettront de résoudre un problème ou de vous faire gagner du temps. |
| **REMARQUE** | Fournit des informations supplémentaires en complément du texte. |

## Historique des révisions

| Version | Description de la révision | Date de publication |
|---|---|---|
| V1.0.0 | Date de sortie. | Avril 2022 |

## Avis de protection de la confidentialité

En tant qu'utilisateur de l'appareil ou responsable du traitement des données, vous êtes susceptible de recueillir les données personnelles d'autres personnes, telles que leur visage, leurs empreintes digitales et leur numéro de plaque d'immatriculation. Vous devez vous conformer aux lois et réglementations locales en matière de protection de la vie privée afin de protéger les droits et intérêts légitimes d'autrui en mettant en œuvre des mesures qui incluent, sans s'y limiter, les éléments suivants : La fourniture d'une identification claire et visible pour informer les gens de l'existence de la zone de surveillance et fournir les informations de contact requises.

# À propos du manuel

- Le manuel est donné uniquement à titre de référence. De légères différences peuvent être constatées entre le manuel et le produit.
- Nous ne sommes pas responsables des pertes encourues en raison d'une exploitation du produit de manière non conforme au manuel.
- Le manuel sera mis à jour en fonction des dernières lois et réglementations des juridictions concernées. Pour plus d'informations, consultez la version imprimée du manuel de l'utilisateur, utilisez notre CD-ROM, scannez le code QR ou visitez notre site Web officiel. Le manuel est donné uniquement à titre de référence. De légères différences peuvent apparaître entre la version électronique et la version papier.
- Tous les logiciels et toutes les interfaces présentés ici sont susceptibles d'être modifiés sans préavis écrit. Les mises à jour du produit peuvent apporter des différences entre le produit réel et le manuel. Veuillez contacter le service client pour être informé des dernières procédures et obtenir de la documentation supplémentaire.
- De légères variations ou des erreurs d'impression peuvent apparaître au niveau des caractéristiques techniques, des fonctions et de la description des opérations. En cas de doute ou d'incohérence, nous nous réservons le droit de fournir une explication définitive.
- Mettez à jour le logiciel de lecture ou essayez un autre logiciel de lecture grand public si le manuel (au format PDF) ne s'ouvre pas.
- Les marques de commerce, les marques déposées et les noms des sociétés dans ce manuel sont la propriété respective de leurs propriétaires.
- Veuillez visiter notre site Web, contacter le fournisseur ou le service après-vente si un problème survient pendant l'utilisation de l'appareil.
- En cas d'incertitude ou de controverse, nous nous réservons le droit de fournir une explication définitive.

# Précautions et avertissements importants

Le contenu de ce paragraphe aborde la bonne manipulation de l'appareil et la protection contre les risques et contre les dommages matériels. Lisez-le soigneusement avant d'utiliser l'appareil et respectez les directives lorsque vous l'utilisez.

## Conditions de fonctionnement

- Assurez-vous que le dispositif d'alimentation de l'appareil fonctionne correctement avant utilisation.
- Ne débranchez pas le câble d'alimentation de l'appareil lorsqu'il est allumé.
- N'utilisez l'appareil que dans la plage d'alimentation conseillé.
- Transportez, utilisez et stockez l'appareil dans les conditions d'humidité et de température autorisées.
- Évitez d'exposer l'appareil aux gouttes ou aux éclaboussures sur l'appareil. Veillez à ne placer aucun objet contenant du liquide sur l'appareil pour éviter qu'il ne se déverse dans l'appareil.
- Ne démontez pas l'appareil.

## Conditions d'installation requises

**AVERTISSEMENT**

- Connectez l'appareil à l'adaptateur d'alimentation avant de le mettre sous tension.
- Respectez strictement les normes de sécurité électrique locales et assurez-vous que la tension dans la région est stable et conforme aux conditions requises d'alimentation de l'appareil.
- Ne connectez pas l'appareil à plus d'un dispositif d'alimentation. Sinon, vous risquez d'endommager l'appareil.

- Respectez toutes les procédures de sécurité et portez les équipements de protection requis qui vous sont fournis lorsque vous travaillez en hauteur.
- N'exposez pas l'appareil aux rayons directs du soleil ou à des sources de chaleur.
- Évitez d'installer l'appareil dans une zone humide, poussiéreuse ou enfumée.
- Installez l'appareil dans un lieu bien ventilé et ne bloquez pas le ventilateur de l'appareil.
- Utilisez l'adaptateur ou le boîtier d'alimentation fournis par le fabricant de l'appareil.
- L'alimentation doit être conforme aux dispositions de la catégorie ES1 contenue dans la norme IEC 62368-1 et ne doit pas être supérieure à PS2. Notez que les informations relatives à l'alimentation électrique figurent sur l'étiquette de l'appareil.
- Branchez les appareils électriques de classe 1 à une prise d'alimentation équipée d'une mise à la terre.

# Table des matières

Avant-propos ..... I
Précautions et avertissements importants ..... III
1 Introduction ..... 1
1.1 Présentation ..... 1
1.2 Caractéristiques Techniques ..... 1
2 Liste de contrôle ..... 3
3 Apparence ..... 4
4 Ajout du clavier à la centrale d'alarme ..... 3
5 Installation ..... 4
6 Configuration ..... 6
6.1 Afficher l'état ..... 6
6.2 Configuration du clavier ..... 7
7 Gestion des Utilisateurs ..... 10
7.1 Ajout d'utilisateurs ..... 10
7.2 Ajout d'une carte ..... 11
7.2.1 Ajout de la carte sur le Gestionnaire des utilisateurs ..... 11
7.2.2 Ajout de la carte dans la liste des accessoires ..... 11
8 Opérations ..... 13
8.1 Commandes fréquemment utilisées ..... 13
8.2 Réveil du clavier ..... 13
8.3 Armement ..... 14
8.4 Désarmement ..... 14
8.5 Recherche de l'état de la pièce ..... 15
Annexe 1 – Recommandations en matière de cybersécurité ..... 16

# 1 Introduction

## 1.1 Présentation

Le clavier sans fil est utilisé avec la centrale d'alarme et prend en charge plusieurs utilisateurs, permettant à chacun d'accéder au système d'alarme et de sécurité avec son propre code privé. Le système conserve également de manière pratique un journal des opérations effectuées par chaque utilisateur, ce qui facilite l'examen et l'analyse de l'historique d'utilisation. Il est idéal pour une utilisation dans les villas, les magasins, les appartements, etc.

## 1.2 Caractéristiques Techniques

Cette section contient les spécifications techniques du clavier. Veuillez vous référer à celles qui correspondent à votre modèle.

Tableau 1–1 Spécifications techniques

| Type | Paramètre | Description | |
|---|---|---|---|
| Fonction | Voyant d'état | 4 indicateurs (communication, armement et désarmement, défaut et alarme) | |
| | Clé | 15 touches (0-9, *, #, armer, désarmer et armement de la maison) | |
| | Sonnette | 1 sonnette intégrée | |
| | Armer et Désarmer | Mot de passe ; carte IC | |
| | Mise à Jour à Distance | Mise à jour du cloud | |
| | Détection de batterie faible | Oui | |
| | Antisabotage | Oui | |
| | Plage de Mesure (Température) | De -15 à 65 °C (de 5 à 149 °F) (intérieur) | |
| | Précision de la mesure | 1 °C (33,8 °F) | |
| Sans fil | Fréquence Porteuse | DHI-ARK30T-W2 (868) : 868,0 MHz à 868,6 MHz | DHI-ARK30T-W2 : 433,1 MHz à 434,6 MHz |
| | Distance de Communication | DHI-ARD821-W2 (868) : Jusqu'à 1 600 m (5 249,34 pieds) dans un espace ouvert | DHI-ARD821-W2 : Jusqu'à 1 200 m (3 937,01 pieds) dans un espace ouvert |
| | Consommation Électrique | 2,3 W max. | |
| | Mécanisme de Communication | Bidirectionnelle | |

| Type | Paramètre | Description |
|---|---|---|
| | Mode Chiffrement | AES128 |
| | Saut de Fréquence | Oui |
| Général | Température de Fonctionnement | De -10 à 55 °C (de 14 à 131 °F) (Intérieur) |
| | Humidité de Fonctionnement | 10 à 90 % (HR) |
| | Alimentation Électrique | 4 piles AA |
| | Durée de Vie de la Batterie | 3 ans (si l'appareil est utilisé pour l'armement et le désarmement une fois par jour) |
| | Dimensions du Produit | 146 × 82 × 22,6 mm (5,75 × 3,23 × 0,89 po) |
| | Dimensions de l'Emballage | 180 × 104 × 58 mm (7,07 × 4,09 × 2,28 po) |
| | Installation | Montage mural |
| | Poids Net | 240 g (0,529 livre) (avec batterie)<br>145 g (0,32 livre) (sans batterie) |
| | Poids Brut | 370 g (0,816 livre) |
| | Certifications | CE |

# 2 Liste de contrôle

Figure 2–1 Liste de contrôle

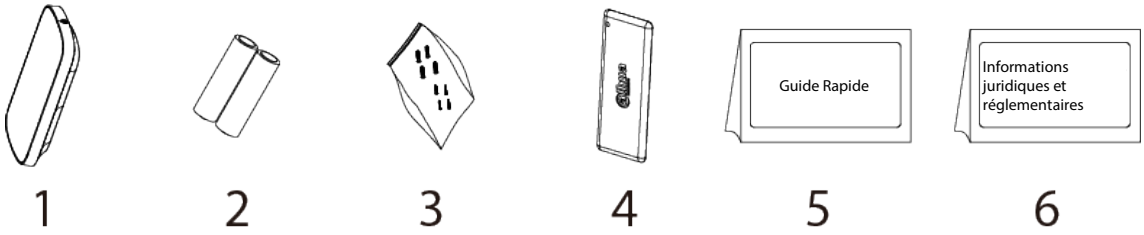



Tableau 2–1 Liste de contrôle

| N° | Nom de l'article | Quantité | N° | Nom de l'article | Quantité |
|---|---|---|---|---|---|
| 1 | Clavier | 1 | 4 | Carte IC | 2 |
| 2 | Batterie | 4 | 5 | Guide Rapide | 1 |
| 3 | Paquet de vis | 1 | 6 | Informations juridiques et réglementaires | 1 |

# 3 Apparence

Figure 3–1 Apparence

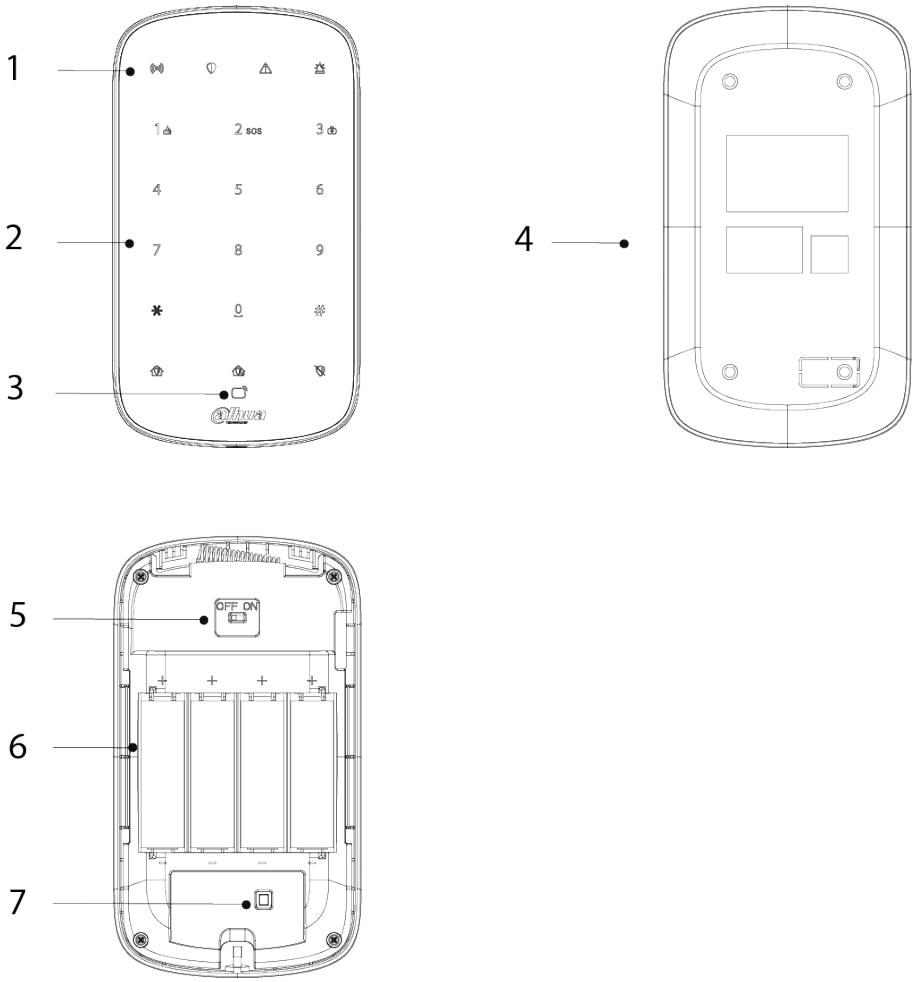


Tableau 3–1 Structure

| N° | Nom | Description |
|---|---|---|
| 1 | Voyant | Il existe quatre voyants, à savoir les voyants de communication, d'armement et de désarmement, de défaut et d'alarme.<br>● Tous les voyants sont fixes pendant 2 secondes : Sous tension.<br>● Tous les voyants sont éteints : Ne pas entrer en mode de couplage.<br>● Statut du voyant de communication :<br>◇ Vert clignotant rapidement : Mode d'appariement.<br>◇ Vert fixe pendant 2 secondes : Couplage réussi.<br>◇ Vert clignotant 3 fois : Échec du couplage.<br>◇ Éteint : En ligne.<br>◇ Vert clignotant lentement et les autres voyants éteints : Hors cnx.<br>◇ Vert clignotant lentement et les autres voyant en statut normal : Entre en mode de sensibilité réduite.<br>● État des voyants d'armement et de désarmement :<br>◇ Bleu fixe : Une seule ou plusieurs pièces sont armées.<br>◇ Vert clignotant 3 fois puis extinction : Toutes les pièces sont désarmées.<br>● Statut du voyant de défaut :<br>◇ Jaune clignotant : Les alarmes de défaut sont déclenchées.<br>◇ Éteint : Une seule ou plusieurs pièces sont armées ou aucun défaut ne se produit.<br>● Indicateur d'alarme clignotant en rouge : Les alarmes sont déclenchées. |
| 2 | Clé | 15 touches.<br>● Touches numériques : 0-9.<br>1 est également la touche d'alarme incendie, 2 la touche d'alarme d'urgence et 3 la touche d'alarme médicale.<br>● # : Recherche.<br>● * : Espace.<br>● Armement à domicile.<br>● : Armement à distance.<br>● : Désarmement. |
| 3 | Section du lecteur de carte | Prend en charge l'ouverture par carte à circuit intégré. Vous pouvez faire glisser votre carte ici. |

| N° | Nom | Description |
|---|---|---|
| 4 | Capot arrière | Lorsque le contact anti-sabotage est relâché, l'alarme anti-sabotage se déclenche. |
| 5 | Interrupteur marche/arrêt | Activez ou désactivez le clavier. |
| 6 | 4 piles | Insérez des piles pour mettre le clavier sous tension. |
| 7 | Contact Antisabotage | Lorsque le contact anti-sabotage est relâché, l'alarme anti-sabotage se déclenche. |

# 4 Ajout du clavier à la centrale d'alarme

Avant de le connecter à la centrale, installez l'application DMSS sur votre téléphone. Ce manuel utilise iOS comme exemple.

- Assurez-vous que la version de l'application DMSS est égale ou supérieure à 1.98 et que celle de la Centrale est égale ou supérieure à v 1.001.0000000.8.R.220319.
- Assurez-vous que la centrale dispose d'une connexion Internet stable.
- Assurez-vous que la centrale n'est pas désarmée.

Étape 1 : Allez sur l'écran de la centrale, puis appuyez sur Accessory pour ajouter le clavier.

Étape 2 : Appuyez sur ⊕ pour scanner le code QR en bas du clavier, puis appuyez sur **Suivant** (Next).

Étape 3 : Appuyez sur **Suivant** (Next) après avoir trouvé le clavier.

Étape 4 : Suivez les instructions à l'écran et activez le clavier, puis appuyez sur **Suivant** (Next).

Étape 5 : Attendez le couplage.

Étape 6 : Personnalisez le nom du clavier et sélectionnez la zone, puis appuyez sur **Terminé** (Completed).

# 5 Installation

Avant l'installation, ajoutez le clavier à la centrale et vérifiez la force du signal sur l'emplacement d'installation. Nous recommandons d'installer le clavier dans un endroit avec une force de signal d'au moins 2 barres.

Le clavier peut être fixé au mur.

Étape 1 : Desserrez la vis pour ouvrir le clavier.

Figure 5–1 Desserrage de la vis

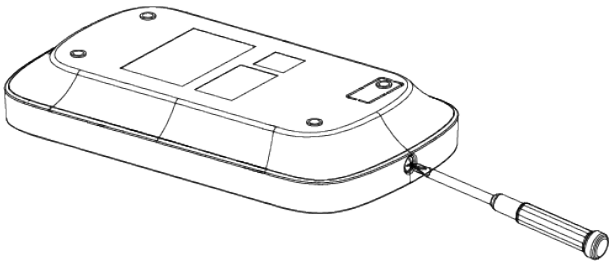
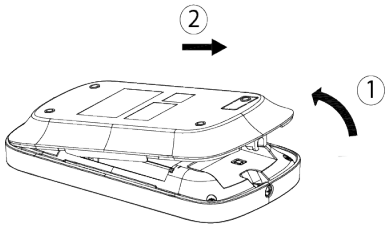


Figure 5–2 Ouverture du clavier

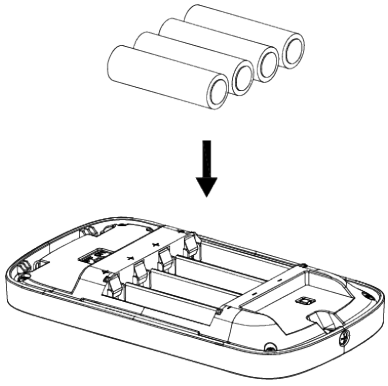



Étape 2 : Insertion de quatre piles dans le clavier.

- Si la batterie est vide, vous devez la remplacer.
- Lorsque vous remplacez la batterie, assurez-vous que le côté marqué « + » est tourné vers le couvercle arrière du clavier.

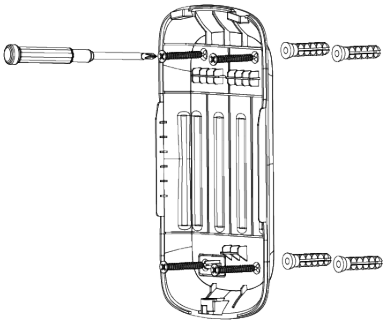
- Veillez à utiliser le même modèle lors du remplacement de la batterie pour éviter tout risque d'incendie ou d'explosion.
- Veillez à ne pas mélanger les anciennes piles avec les nouvelles.

Figure 5–3 Installation des piles



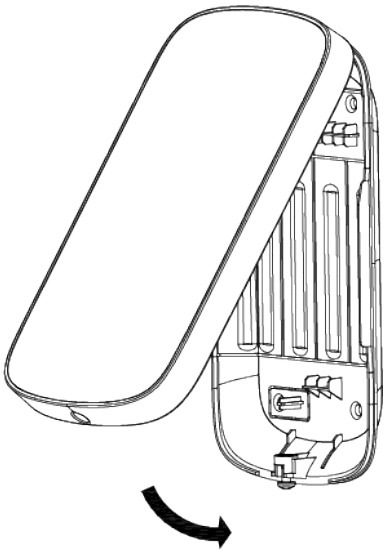
Étape 3 : Percez quatre trous dans le mur en fonction des positions de trou du clavier, puis insérez les chevilles à expansion dans les trous.

Figure 5–4 Perçage des trous



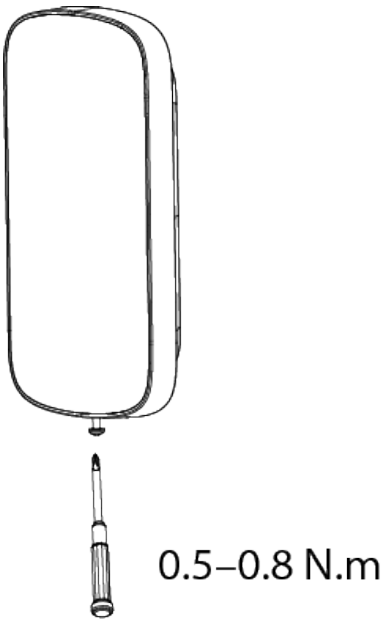
Étape 4 : Fermez le clavier.

Figure 5–5 Fermeture du clavier



Étape 5 : Fixez le clavier à l'aide de la vis.

Figure 5–6 Fixation du clavier



# 6 Configuration

Vous pouvez visualiser et modifier les informations générales du clavier.

## 6.1 Afficher l'état

Sur l'écran de la centrale, sélectionnez le clavier dans la liste des accessoires pour pouvoir afficher l'état du clavier.

Tableau 6–1 État

| Paramètre | Valeur |
|---|---|
| Désactiver temporairement | L'état indique si les fonctions du clavier sont activées ou désactivées.<br>● : Activer.<br>● : Désactiver uniquement l'alarme anti-sabotage.<br>● : Désactiver. |
| Température | La température moyenne de l'environnement. |
| Force du signal | La force du signal entre la centrale et le clavier.<br>● : Faible.<br>● : Faible.<br>● : Bon.<br>● : Excellent.<br>● : N° |
| Niveau de la batterie | Le niveau de la batterie du clavier.<br>● : Complètement chargée.<br>● : Suffisant.<br>● : Modéré.<br>● : Insuffisant.<br>● : Faible. |
| État anti-sabotage | L'état anti-sabotage du clavier, qui réagit au détachement du corps. |
| État en ligne | État en ligne et hors ligne du clavier.<br>● : En ligne.<br>● : Hors cnx. |
| État de verrouillage | L'état pour savoir si le clavier est verrouillé ou non.<br>● : Verrouillé.<br>● : Déverrouillé. |
| Transmission par Répéteur | Indique si le clavier transmet les messages à la centrale via le répéteur. |
| Version du programme | La version du programme du clavier. |

## 6.2 Configuration du clavier

Sur l'écran de la centrale, sélectionnez un clavier dans la liste des accessoires, puis appuyez sur

 pour configurer les paramètres du clavier.

Tableau 6–2 Description des paramètres du clavier

| Paramètre | Description |
|---|---|
| Configuration de l'appareil | • Affichez le nom, le type, le numéro de série et le modèle du clavier.<br>• Modifiez le nom du clavier, puis appuyez sur **Enregistrer** (Save) pour enregistrer la configuration. |
| Zone | Sélectionnez la zone à laquelle le clavier est affecté. |
| Autorisations de contrôle | est utilisées pour définir la zone dans laquelle le clavier peut fonctionner. |
| Désactiver temporairement | Permet d'envoyer des commandes à la centrale d'alarme.<br>• Appuyez sur **Activer** (Enable) pour que le clavier envoie des commandes à la centrale d'alarme. L'option réglée par défaut est **Activer** (Enable).<br>• Appuyez sur **Désactiver uniquement l'alarme anti-sabotage** (Only Disable Tamper Alarm) pour que le système ignore uniquement les messages d'alarme anti-sabotage.<br>• Appuyez sur **Désactiver** (Disable) pour que le clavier envoie des commandes à la centrale d'alarme. |

| Paramètre | Description |
| --- | --- |
| Configuration du clavier | Activez d'abord les touches du clavier et définissez si un événement se produit.<br>• **Alarme incendie :** Activé par défaut. Après avoir activé la fonction **Alarme incendie** (Fire Alarm), lorsqu'un incendie est détecté, vous devez appuyer sur la touche incendie du clavier et la maintenir enfoncée pendant 3 secondes pour déclencher l'alarme incendie.<br>• **Liaison entre l'alarme incendie et la sirène :** Activé par défaut. Après avoir activé cette fonction, la sirène et la sonnette seront liées lorsque les alarmes incendie seront déclenchées.<br>• **Alarme urgence :** Activé par défaut. Après avoir activé la fonction **Alarme urgence** (Emergency Alarm), lorsqu'une urgence est détectée, vous devez appuyer sur la touche urgence du clavier et la maintenir enfoncée pendant 3 secondes pour déclencher l'alarme urgence.<br>• **Liaison entre l'alarme urgence et la sirène :** Activé par défaut. Après avoir activé la fonction, la sirène et la sonnette seront liées lorsque les alarmes urgence seront déclenchées.<br>• **Alarme médicale :** Activé par défaut. Après avoir activé la fonction **Alarme médicale**(Medical Alarm), lorsqu'un incendie est détecté, vous devez appuyer sur la touche incendie du clavier et la maintenir enfoncée pendant 3 secondes pour déclencher l'alarme médicale.<br>• **Liaison entre l'alarme médicale et la sirène :** Activé par défaut. Après avoir activé la fonction, la sirène et la sonnette seront liées lorsque les alarmes médicales seront déclenchées. |
| État de verrouillage du clavier | Réglez le nombre de tentatives de saisie d'un code d'accès erroné et le temps de verrouillage du clavier.<br>• Activez d'abord la fonction de verrouillage du clavier.<br>• Pour le nombre de tentatives de saisie d'un code d'accès erroné dans les 30 minutes, vous pouvez choisir entre 3 et 10 fois. L'option réglée par défaut est 5.<br>• Pour la durée de verrouillage, vous pouvez choisir entre 3, 5, 10, 20, 30, 60, 90 et 180 minutes. L'option réglée par défaut est 3 minutes. |
| Armement sans code d'accès | Définissez si vous pouvez utiliser le clavier pour armer le système sans code d'accès. Désactivé par défaut.<br>L'activation de la fonction **Armement sans code d'accès** (No Passcode Arming) ne répond pas aux certifications EN50131-1. |

| Paramètre | Description |
| --- | --- |
| Puissance de transmission | Choisissez entre élevée, faible et automatique.<br>Plus les niveaux de puissance de transmission sont élevés, plus les transmissions peuvent aller loin, mais la consommation d'énergie augmente.<br>Si vous sélectionnez **Faible** (Low), le clavier passe en mode de sensibilité réduite. |
| Configuration de lecteur de carte | Activez la fonction de lecteur de carte et la fonction de cryptage logiciel sur le clavier.<br>• **Lecteur de carte :** Activé par défaut. Si cette option est activée, le clavier prend en charge la fonction de reconnaissance de carte. Si elle est désactivée, la fonction de lecteur de cartes sera désactivée.<br>• **Cryptage logiciel :** Activé par défaut. Si cette option est activée, les informations sur la carte seront cryptées lors de l'émission de la carte. |
| Luminosité de rétroéclairage | Réglez la luminosité du clavier rétroéclairé. Vous pouvez choisir entre **Désactivée** (Off), **Faible** (Low) et **Élevée** (High).<br>Lorsque le niveau de la batterie est faible, la luminosité du rétroéclairage passe automatiquement à **Faible** (Low). |
| Volume de la sonnette | Configurez le niveau de volume de la sonnette. Choisissez entre **Désactivée**(Off), **Faible** (Low) et **Élevée** (High). |
| Détection de la force du signal | Testez la force du signal actuelle.<br>Le test de puissance du signal n'est pas pris en charge lorsque le clavier est en mode veille. Vous pouvez appuyer sur n'importe quelle touche pour réveiller le clavier. |
| Mise à jour du cloud | Mise à jour en ligne. |
| Supprimer | Supprimez le clavier.<br>Accédez à l'écran de la centrale, sélectionnez le clavier dans la liste des accessoires, puis balayez vers la gauche pour le supprimer. |

# 7 Gestion des Utilisateurs

## 7.1 Ajout d'utilisateurs

Vous pouvez ajouter, modifier ou supprimer des utilisateurs du clavier lorsqu'il est désarmé.

Seuls les utilisateurs installateurs et administrateurs sont autorisés à ajouter des utilisateurs.

### Procédure

Étape 1 : Allez à l'écran accueil.

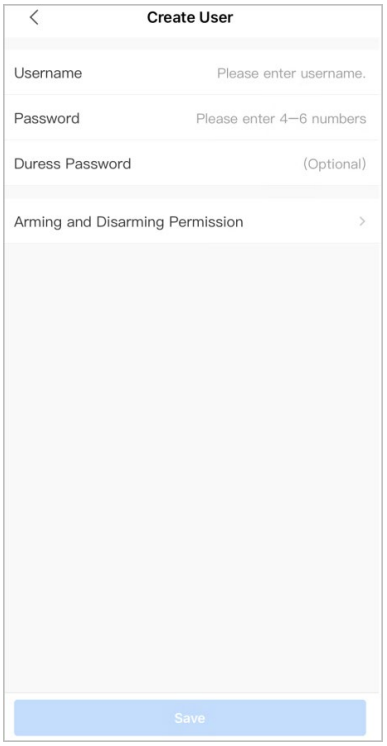
Étape 2 : Sélectionnez une centrale, puis [redacted] **> Détails appareil > Paramètres de centrale > Gestionnaire des utilisateurs** ([redacted] > Device Details > Hub Setting > User Manager).

Étape 3 : Appuyez sur ⊕ pour ajouter un utilisateur.

Étape 4 : Saisissez votre nom d'utilisateur, votre code d'accès et votre code d'accès sous contrainte, puis sélectionnez les autorisations d'armement et de désarmement pour la pièce.

- Le code d'accès et le code sous contrainte doivent être composés de 4 à 6 chiffres.
- Le code d'accès sous contrainte est facultatif.
- Jusqu'à 32 utilisateurs peuvent être créés. Le premier utilisateur créé est l'utilisateur admin par défaut. Il dispose de toutes les autorisations.

Figure 7–1 Ajout d'un utilisateur




Étape 5 : Appuyez sur **Enregistrer** (Save).

Opérations connexes

- Suppression d'un utilisateur
  Dans l'écran **Gestionnaire des utilisateurs** (User Manager), sélectionnez l'utilisateur, puis faites-le glisser vers la gauche pour le supprimer.

  L'utilisateur admin doit être le dernier à être supprimé.
- Modification des informations de l'utilisateur
  Sur l'écran **Gestionnaire des utilisateurs** (User Manager), sélectionnez l'utilisateur, puis vous pouvez modifier les informations de l'utilisateur, y compris le nom d'utilisateur, le code d'accès, le code sous contrainte et les autorisations d'armement et de désarmement.

# 7.2 Ajout d'une carte

Vous pouvez ajouter, modifier ou supprimer la carte lorsque le clavier est désarmé. Il existe 2 manières d'ajouter manuellement la carte.

- Ajout de la carte sur le **Gestionnaire des utilisateurs**(User Manager).
- Ajout de la carte dans la liste des accessoires.

Seuls les utilisateurs installateurs et administrateurs sont autorisés à ajouter la carte.

## 7.2.1 Ajout de la carte sur le Gestionnaire des utilisateurs

Étape 1 : Allez à l'écran accueil.
Étape 2 : Sélectionnez une centrale, puis [redacted] **> Détails appareil > Paramètres de centrale > Gestionnaire des utilisateurs** ([redacted] > Device Details > Hub Setting > User Manager).
Étape 3 : Sélectionnez l'utilisateur vers lequel vous souhaitez lier la carte.
Étape 4 : Appuyez sur ⊕.
Étape 5 : Appuyez sur n'importe quelle touche pour réveiller le clavier, puis placez la carte à proximité de la section du lecteur de carte du clavier pour lancer le processus de liaison dans les 30 secondes.
Si les informations de la carte sont reconnues, l'ID de carte s'affiche sur l'application et le clavier émet un bip. Après avoir enregistré les configurations, la carte aura les autorisations de l'utilisateur.

Jusqu'à 8 cartes peuvent être liées à un utilisateur.

## 7.2.2 Ajout de la carte dans la liste des accessoires

Étape 1 : Allez à l'écran de la centrale.
Étape 2 : Sélectionnez **Accessoire** (Accessory).
Étape 3 : Touchez ⊕, puis sélectionnez **Ajouter une carte** (Add Card).
Étape 4 : Appuyez sur n'importe quelle touche pour réveiller le clavier.

Étape 5 : Placez la carte à proximité de la section du lecteur de carte du clavier pour lancer le processus de liaison.

Étape 6 : Sur l'écran **Utilisateur lié** (Linked User), vous pouvez choisir de créer un nouvel utilisateur ou de lier la carte à l'utilisateur ajouté.

Si vous choisissez de créer un nouvel utilisateur, appuyez sur **Créer un utilisateur** (Create User).

Pour des détails sur l'ajout d'un utilisateur, voir « 7.1Ajout d'utilisateurs ».

Étape 7 : Appuyez sur **Terminé** (Completed).

# 8 Opérations

## 8.1 Commandes fréquemment utilisées

Voici les commandes fréquemment utilisées pour le clavier.

Avant d'utiliser le clavier, assurez-vous d'avoir créé des comptes sur l'application DMSS ou COS.

Tableau 8–1 Commande

| Fonction | Commande |
|---|---|
| Armement à distance global | Saisissez le mot de passe+ + #. |
| Armement à domicile global | Saisissez le mot de passe+ + #. |
| Armement sans code d'accès | Appuyez sur ou sur et maintenez enfoncé. |
| Désarmement global | Saisissez le mot de passe+ + #. |
| Armement à distance d'une seule pièce | Saisissez le mot de passe + * + Pièce n° + + #. |
| Armement à domicile d'une seule pièce | Saisissez le mot de passe + * + Pièce n° + + #. |
| Désarmement d'une seule pièce | Saisissez le mot de passe + * + Pièce n° + + #. |
| Recherche de l'état de la pièce | Saisissez le mot de passe + * + Pièce n° + #. |
| Effacer | Appuyez sur # et maintenez enfoncé. |

## 8.2 Réveil du clavier

Appuyez sur n'importe quelle touche et maintenez-la enfoncée pendant plus de 0,1 seconde pour réveiller le clavier. Lorsque vous entendez un bip court et que tous les voyants lumineux sont allumés, vous pouvez l'utiliser.

- Si vous n'utilisez pas le clavier pendant plus de 4 secondes, l'écran LCD rétroéclairé sera faible et l'état des voyants lumineux restera le même.
- Si vous n'utilisez pas le clavier pendant plus de 12 secondes, le clavier émet deux bips, tous les voyants lumineux s'éteignent et le clavier passe en mode veille.
- Pour réveiller le clavier lorsqu'il est hors ligne, le voyant de communication clignote lentement en vert et les autres voyants lumineux, y compris les voyants d'armement et de désarmement, de défaut et d'alarme, s'éteignent.

## 8.3 Armement

- Pour armer toutes les pièces, vous pouvez entrer les commandes d'armement ou faire glisser la carte.

  Pour armer le système sans code d'accès, vous pouvez d'abord activer la fonction **Armement sans code d'accès** (No Passcode Arming), puis appuyer et maintenir enfoncée ou .
- Pour armer une seule pièce, vous pouvez saisir la commande d'armement correspondante.

  ◇ Si l'armement est réussi, le voyant lumineux d'armement et de désarmement clignote lentement 3 fois en bleu, puis reste fixe et émet un bip court.

  ◇ Si l'armement échoue à cause d'une erreur potentielle, le voyant d'armement et de désarmement clignote rapidement deux fois en vert, puis revient à l'état normal en émettant un long bip. Et si vous entrez à nouveau la même commande d'armement dans les 30 secondes ou si vous passez à nouveau la même carte dans les 10 secondes, vous pouvez forcer l'armement de la pièce.

  ◇ Si l'armement échoue pour des raisons telles que l'utilisation d'un code d'accès erroné ou d'une carte non valide ou si vous autorisez des personnes non autorisées à utiliser le clavier, le voyant rétroéclairé clignote deux fois rapidement et un long bip est émis.

  En glissant la carte, vous pouvez uniquement utiliser l'armement à distance global.

## 8.4 Désarmement

- Si le désarmement global est réussi, le voyant lumineux d'armement et de désarmement clignote lentement 3 fois en vert, puis s'éteint et émet 2 bips courts.

  Après avoir réussi à désarmer le système, si le système présente des défauts, le voyant de défaut clignote lentement en jaune.
- Si le désarmement d'une seule pièce est réussi, le voyant d'armement et de désarmement clignote lentement 3 fois en vert, puis revient à l'état normal en émettant 2 bips courts.
- Si le désarmement échoue pour des raisons telles que l'utilisation d'un code d'accès erroné ou d'une carte non valide ou si vous autorisez des personnes non autorisées à utiliser le clavier, le voyant rétroéclairé clignote deux fois rapidement et un long bip est émis.

  ◇ Si une ou plusieurs pièces associées à la carte sont en état d'armement, alors toutes les pièces associées seront désarmées si vous glissez la carte.

  ◇ Si toutes les pièces associées à la carte sont en état de désarmement, alors toutes les pièces associées seront armées si vous glissez la carte.

# 8.5 Recherche de l'état de la pièce

Vous n'êtes autorisé qu'à rechercher l'état d'une seule pièce.

- Si votre recherche est fructueuse, le clavier émet un bip et des voyants lumineux indiquent l'état de la pièce.
  - ◇ Le voyant d'armement et de désarmement s'allume en bleu pendant 6 secondes si la pièce est armée.
  - ◇ Le voyant d'armement et de désarmement clignote lentement en vert pendant 3 secondes si la pièce est désarmée.
  - ◇ Le voyant de défaut est allumé en continu pendant 6 secondes en cas de défaut sur les périphériques et la centrale.
  - ◇ Le voyant d'alarme est allumé pendant 6 secondes si des événements d'alarme se produisent dans la pièce.
- Si la recherche échoue pour des raisons telles que l'utilisation d'un code d'accès erroné ou d'une carte non valide, ou la recherche d'une pièce qui n'est pas associée à la carte, les voyants rétroéclairés clignotent 3 fois rapidement et un long bip est émis. Lorsque le bip s'arrête, le voyant lumineux revient à son état normal.

# Annexe 1 – Recommandations en matière de cybersécurité

La cybersécurité est plus qu'un mot à la mode : c'est quelque chose qui concerne chaque appareil connecté à Internet. La vidéosurveillance sur IP n'est pas à l'abri des cyberrisques, mais la mise en place de mesures élémentaires pour protéger et renforcer les réseaux et les appareils en réseau les rendra moins vulnérables à des attaques. Nous donnons, ci-après, des conseils et des recommandations de Dahua pour créer un système de sécurité plus sûr.

**Actions obligatoires à prendre pour la sécurité réseau d'un équipement de base :**

1. **Utiliser des mots de passe robustes**

   Veuillez vous référer aux recommandations suivantes pour définir les mots de passe :

   - La longueur du mot de passe doit être d'au moins 8 caractères.
   - Ils doivent être composés de deux types de caractères comprenant des lettres majuscules et minuscules, des chiffres et des symboles.
   - Ils ne doivent pas être composés du nom du compte dans l'ordre normal ou inversé.
   - Les caractères ne doivent pas se suivre, p. ex. 123, abc, etc.
   - Les caractères ne doivent pas se répéter, par ex. 111, aaa, etc.

2. **Mettre à jour le micrologiciel et le logiciel client à temps**

   - Conformément à la procédure standard de l'industrie technologique, nous vous recommandons de maintenir à jour le micrologiciel de votre équipement (enregistreurs NVR et DVR, caméra IP, etc.) afin de garantir que votre système est doté des correctifs de sécurité les plus récents. Lorsque l'équipement est connecté au réseau public, il est recommandé d'activer la fonction de vérification automatique de la disponibilité de mises à jour afin d'obtenir rapidement les informations sur les mises à jour du micrologiciel fournies par le fabricant.
   - Nous vous conseillons de télécharger et d'utiliser la version du logiciel client la plus récente.

**Recommandations à suivre pour améliorer la sécurité réseau de votre équipement :**

1. **Protection matérielle**

   Nous vous suggérons de fournir une protection matérielle à vos équipements, en particulier les dispositifs de stockage. Par exemple, placez l'équipement dans une armoire ou une salle informatique spéciale, et appliquez des autorisations de contrôle d'accès et une gestion des clés sur mesure afin d'empêcher tout personnel non autorisé d'entrer en contact physique avec les équipements pour éviter p. ex. d'endommager le matériel, des connexions non autorisées à des équipements amovibles (disque flash USB, port série, etc.).

2. **Modifier régulièrement votre mot de passe**

   Nous vous conseillons de modifier régulièrement vos mots de passe pour réduire les risques qu'ils soient devinés ou déchiffrés.

3. **Définir et mettre à jour les informations de réinitialisation des mots de passe à temps**

   L'équipement prend en charge la fonction de réinitialisation du mot de passe. Veuillez définir les informations relatives à la réinitialisation du mot de passe à temps, y compris l'adresse électronique de l'utilisateur final et les questions de protection du mot de passe. Si les informations changent, veuillez les modifier à temps. Lors de la configuration des questions de

protection du mot de passe, il est conseillé de ne pas utiliser des questions (réponses) trop faciles à deviner.

4. **Activer le blocage de compte**
   La fonction de blocage de compte est activée par défaut. Nous vous recommandons de la laisser activée pour garantir la sécurité des comptes. Si un pirate tente de se connecter plusieurs fois avec un mot de passe incorrect, le compte concerné et l'adresse IP de la source seront bloqués.
5. **Modifier les ports par défaut des services HTTP et d'autres services**
   Nous vous conseillons de modifier les ports par défaut du service HTTP et des autres services en les choisissant dans la plage numérique allant de 1 024 à 65 535, ce qui permet de réduire le risque que des étrangers puissent deviner les ports utilisés.
6. **Activer HTTPS**
   Nous vous conseillons d'activer le protocole HTTPS. Vous accéderez ainsi au service Web au moyen d'un canal de communication sécurisé.
7. **Liaison d'adresse MAC**
   Nous vous recommandons de lier l'adresse IP et l'adresse MAC de la passerelle à l'équipement, réduisant ainsi le risque d'usurpation ARP.
8. **Assigner raisonnablement les comptes et les privilèges**
   En fonction des besoins d'activité et de gestion, ajoutez de manière raisonnable des utilisateurs et attribuez-leur un ensemble d'autorisations minimales.
9. **Désactiver les services inutiles et choisir les modes sécurisés**
   S'ils ne sont pas nécessaires et pour réduire les risques, désactivez certains services, tels que SNMP, SMTP, UPnP, etc.
   En cas de besoin, il est fortement recommandé d'utiliser les modes sécurisés, y compris, mais sans limitation, les services suivants :
   - SNMP : Choisissez SNMP v3 et configurez des mots de passe de chiffrement et d'authentification robustes.
   - SMTP : Choisissez le protocole TLS pour accéder aux serveurs de messagerie.
   - FTP : Choisissez le protocole SFTP et définissez des mots de passe robustes.
   - Point d'accès : Choisissez le mode de chiffrement WPA2-PSK et définissez des mots de passe robustes.
10. **Chiffrement de la transmission audio et vidéo**
    Si vos contenus de données audio et vidéo sont très importants ou sensibles, nous vous recommandons d'utiliser la fonction de chiffrement de la transmission, afin de réduire les risques de vol des données audio et vidéo durant la transmission.
    Rappel : Le chiffrement de la transmission entraînera une certaine baisse de l'efficacité de la transmission.
11. **Contrôle sécurisé**
    - Vérifier les utilisateurs connectés : Nous vous conseillons de vérifier régulièrement les utilisateurs connectés afin de savoir si la connexion à l'appareil s'effectue sans autorisation.
    - Consulter le journal de l'équipement : En examinant les journaux, vous pouvez connaître les adresses IP utilisées pour la connexion à vos appareils et les principales opérations effectuées.
12. **Journal réseau**
    Comme la capacité de stockage de l'équipement est limitée, le journal stocké sera limité. Si vous devez conserver le journal pour longtemps, il est recommandé d'activer la fonction de journal

réseau afin de veiller à ce que les journaux essentiels soient synchronisés avec le serveur de journal réseau pour suivi.

13. **Construire un environnement réseau sécurisé**

    Afin de garantir au mieux la sécurité des équipements et de réduire les cyberrisques, nous vous recommandons de :

    - Désactiver la fonction de mappage de ports du routeur pour éviter les accès directs aux appareils Intranet à partir du réseau externe.
    - Compartimenter et isoler le réseau en fonction des besoins réseau réels. Si la communication n'est pas nécessaire entre deux sous-réseaux, il est conseillé d'utiliser les technologies de réseau VLAN, GAP et d'autres pour compartimenter le réseau de sorte à obtenir une isolation réseau effective.
    - Mettre en place le système d'authentification d'accès 802.1x pour réduire le risque d'accès non autorisés aux réseaux privés.
    - Activer le filtrage des adresses IP/MAC pour limiter le nombre d'hôtes autorisés à accéder à l'équipement.

## En savoir plus

Veuillez visiter le centre de réponse d'urgence de sécurité du site officiel de Dahua pour les annonces de sécurité et les dernières recommandations en matière de sécurité.

POUR UNE SOCIÉTÉ PLUS SÛRE ET UNE VIE PLUS INTELLIGENTE

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Adresse : No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. Chine | Site Web : www.dahuasecurity.com | Code postal : 310053
E-mail : overseas@dahuatech.com | Fax : +86-571-87688815 | Tél. : +86-571-87688883