Lecteur d’accès

Manuel d’utilisation

V1.0.0

Avant-propos

Généralités

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

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	Première Publication.	Novembre 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 du lecteur de carte, la prévention des risques et la prévention des dommages matériels. Lisez attentivement ce contenu avant d'utiliser le lecteur de carte et respectez les consignes lorsque vous l'utilisez.

Conditions de transport requises

Transportez, utilisez et stockez le lecteur de carte dans les conditions d'humidité et de température autorisées.

Conditions requises pour le stockage

Stockez le lecteur de carte dans les conditions d'humidité et de température autorisées.

Conditions d'installation requises

 **AVERTISSEMENT**

- Ne connectez pas l'adaptateur d'alimentation au lecteur de carte alors que l'adaptateur est sous tension.
- Veillez à respecter strictement les codes et normes locales de sécurité électrique. Assurez-vous que la tension ambiante est stable et répond aux exigences du contrôleur d'accès.
- Ne connectez pas le lecteur de carte à deux ou plusieurs sources d'alimentation électrique pour éviter d'endommager le lecteur de carte.
- Toute utilisation inappropriée de la batterie peut entraîner un incendie ou une explosion.

- Le personnel travaillant en hauteur doit prendre toutes les mesures nécessaires pour assurer sa propre sécurité, notamment porter un casque et des ceintures de sécurité.
- Ne placez pas le lecteur de carte à un endroit exposé à la lumière du soleil ou proche de sources de chaleur.
- Gardez le lecteur de carte à l'écart de l'humidité, de la poussière et de la suie.
- Installez le lecteur de carte sur une surface stable afin d'éviter toute chute.
- Installez le lecteur de carte à un endroit bien ventilé et empêchez toute obstruction des orifices de ventilation.
- Utilisez un adaptateur ou un boîtier d'alimentation fourni par le fabricant.
- Utilisez les cordons d'alimentation recommandés dans votre région et conformez-vous aux spécifications d'alimentation nominales.
- 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. Veuillez noter que l'exigence relative à l'alimentation électrique est soumise à l'étiquette du lecteur de carte.
- Le lecteur de carte est un équipement électrique de classe I. Assurez-vous que le bloc d'alimentation du lecteur de carte est connecté à une prise électrique munie d'une mise à la terre de protection.

Conditions de fonctionnement

- Assurez-vous que l'alimentation électrique est correcte avant utilisation.
- Ne débranchez pas le cordon d'alimentation sur le côté du lecteur de carte alors que l'adaptateur est sous tension.
- Utilisez le lecteur de carte dans la plage nominale d'entrée et de sortie d'alimentation.
- Utilisez le lecteur de carte dans les conditions d'humidité et de température autorisées.
- Évitez d'exposer le lecteur de carte aux gouttes ou aux éclaboussures de liquides. Ne placez aucun objet contenant un liquide sur le lecteur de carte afin d'éviter que ce liquide n'y pénètre.
- Ne démontez pas le lecteur de carte sans instructions d'un professionnel.

Table des matières

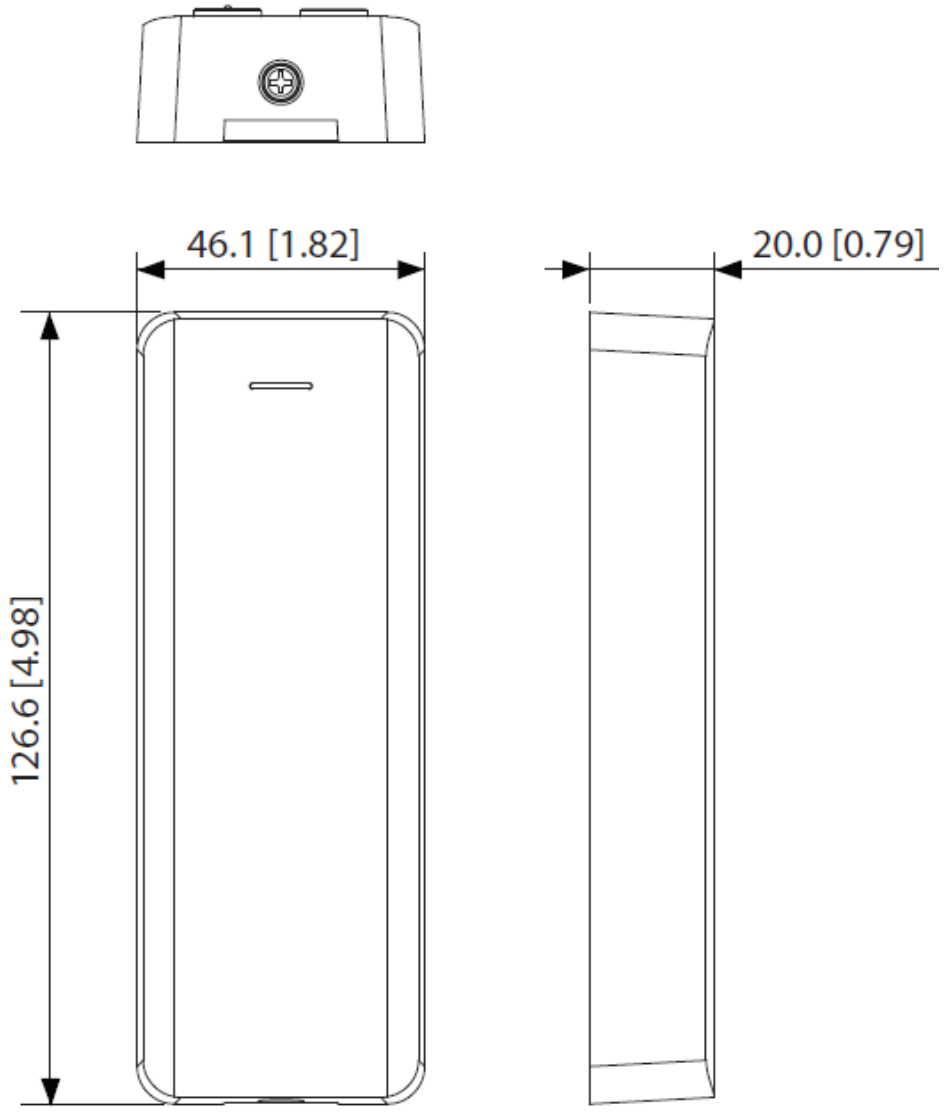
1 Présentation du produit

1.1 Introduction

Dans la plupart des systèmes de contrôle d'accès, un lecteur de carte de contrôle d'accès est un système de sécurité qui nécessite le glissement d'une carte d'identité pour vérifier que la personne qui entre dans la pièce ou l'espace est autorisée. Il convient à une grande variété de lieux tels que les immeubles de bureaux, les écoles, les complexes, les communautés, les usines, les lieux publics, les centres d'affaires et les bâtiments gouvernementaux.

1.2 Dimensions

Figure 1-1 Dimensions du lecteur de carte (unité : mm [pouce])



2 Câblage et installation

2.1 Vue d'ensemble des ports

Tableau 2-1 Vue d'ensemble des ports

Couleur	Port	Description
Rouge	RD+	PWR (12 V CC)
Noir	RD–	GND
Bleu	BOÎTIER	Signal d'alarme anti-sabotage
Blanc	D1	Signal de transmission Wiegands (efficace uniquement lors de l'utilisation du protocole Wiegand)
Vert	Do	
Marron	LED	Signal de réponse Wiegand (efficace uniquement lors de l'utilisation du protocole Wiegand)
Jaune	RS–485_B	
Violet	RS–485_A	

2.2 Exigences en matière de câblage

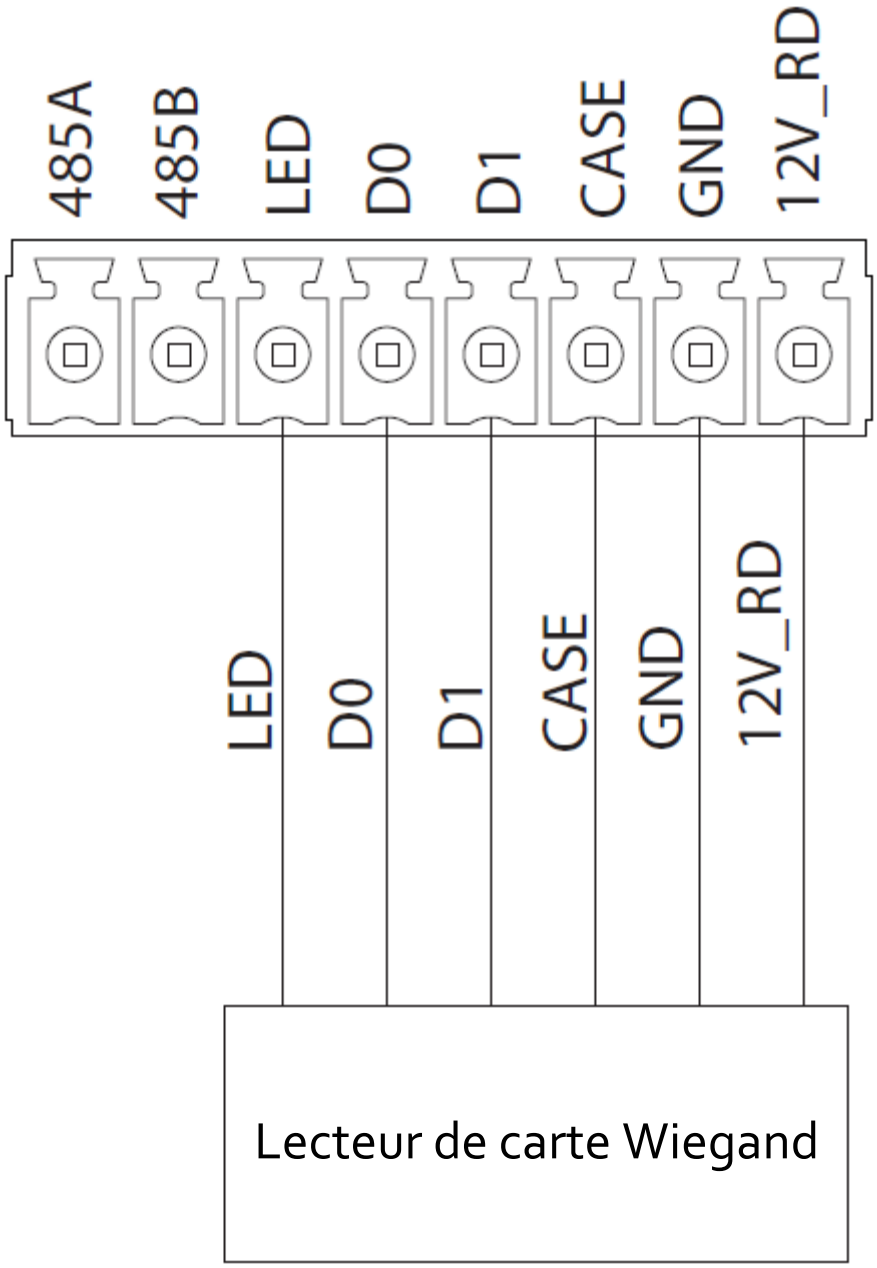
- Connectez le lecteur de carte aux ports Wiegand ou aux ports RS-485 en fonction du type de lecteur de carte.
- Sélectionnez les fils appropriés en fonction des exigences relatives aux fils.

Tableau 2-2 Exigences de câblage du lecteur de carte

Type	Exigences en matière d'impédance	Exigences en matière de longueur
Lecteur de carte RS-485	Connecte des fils RS-485, et l'impédance d'un seul fil doit être ≤ 10 Ω.	≤ 100 m. Au-dessus de UL1061, des fils blindés 24AWG sont recommandés.
Lecteur de carte Wiegand	Connecte des fils Wiegand, et l'impédance d'un seul fil doit être ≤ 2 Ω.	≤ 80 m. Au-dessus de UL1061, des fils blindés 18AWG sont recommandés.

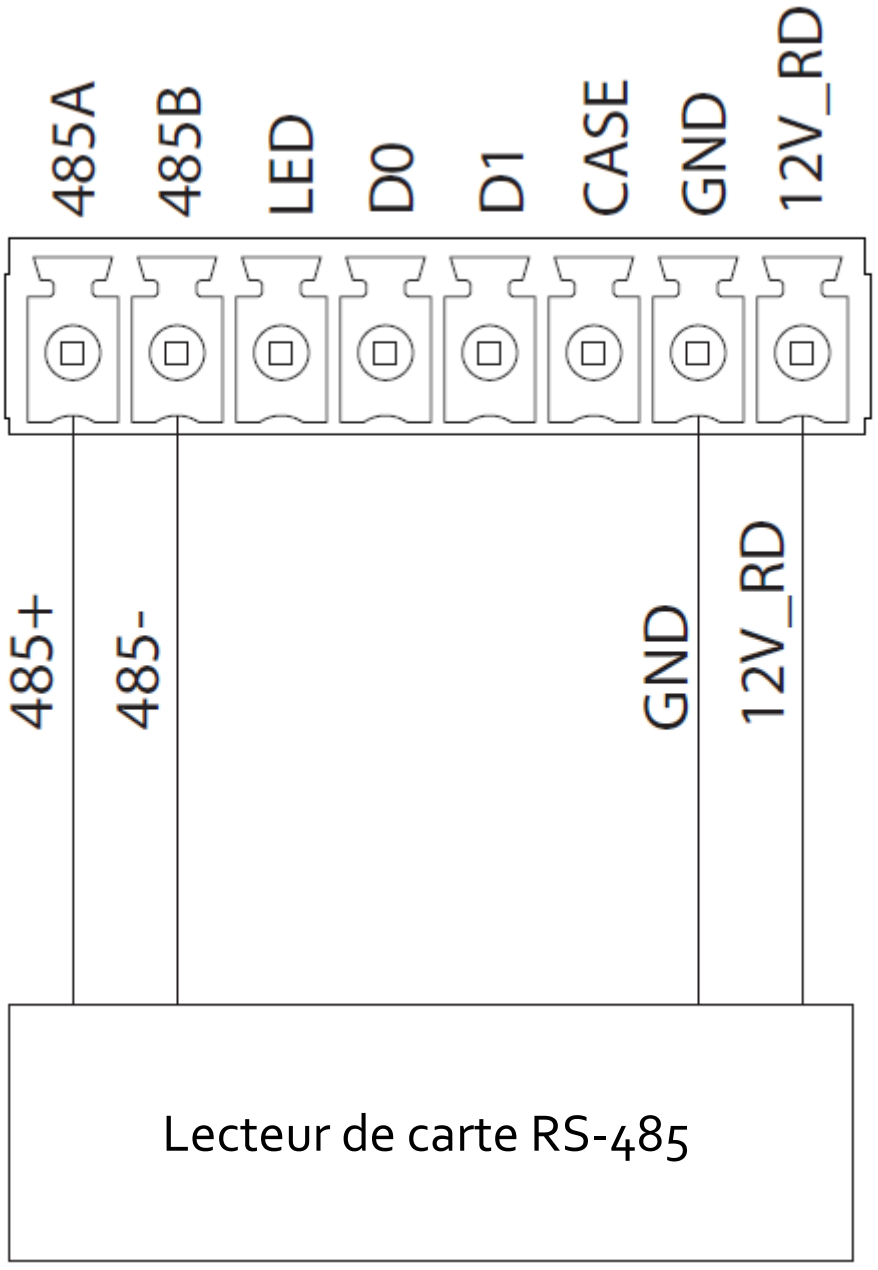
2.3 Câblage

Figure 2-1 Câblage du lecteur de carte Wiegand



- Pour le lecteur de carte Wiegand sans clavier, Wiegand 34 est pris en charge par défaut et Wiegand 26 est personnalisable.
- Pour les lecteurs de carte Wiegand avec clavier, appuyez sur ******0034****** pour passer au format Wiegand 34 et sur ******0026****** pour passer au format Wiegand 26.

Figure 2-2 Câblage du lecteur de carte RS-485



2.4 Procédure d'installation

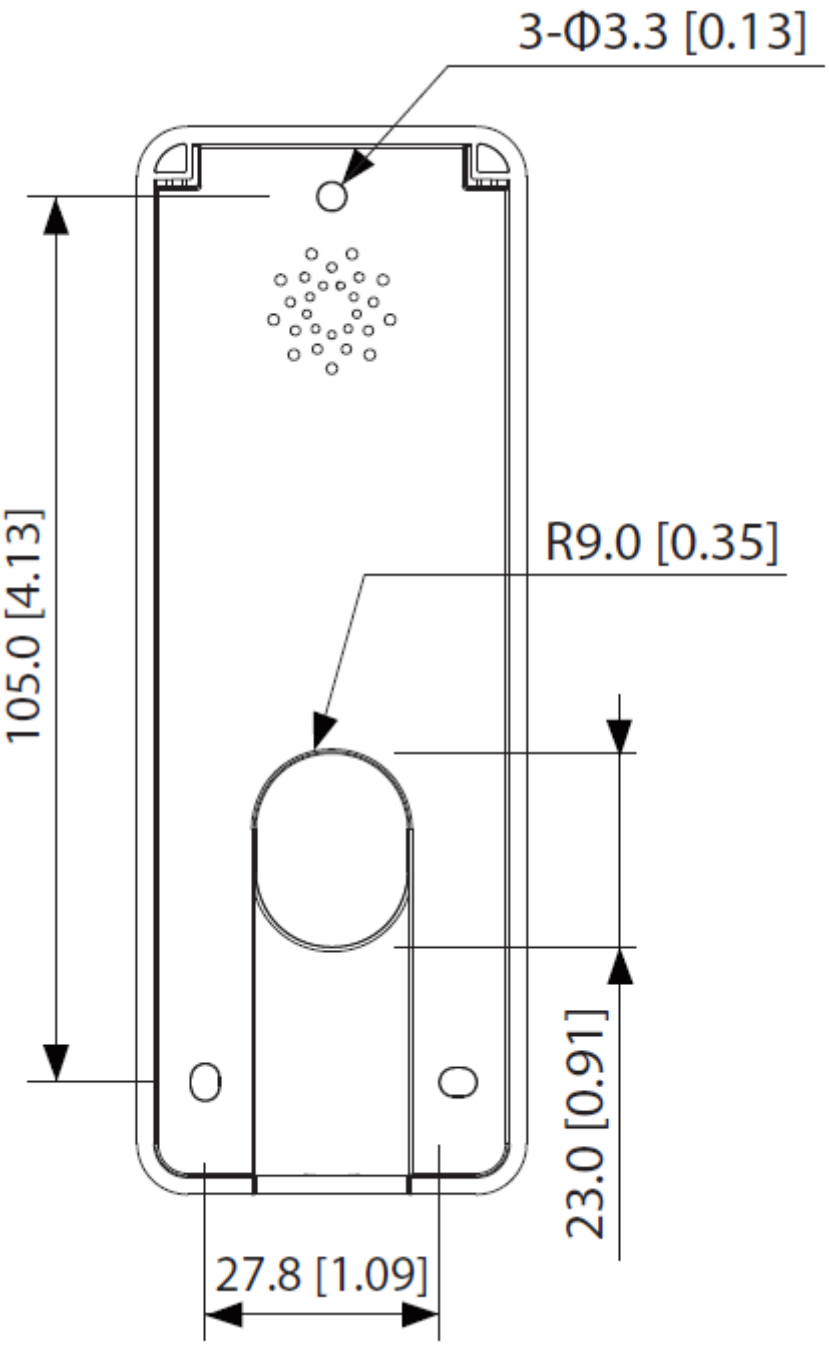
La hauteur d'installation recommandée est de 1,3 m à 1,5 m (du centre de l'appareil au sol) et ne doit pas dépasser 2 m.

Procédure

Étape 1 : Percez les 3 trous d'installation dans le mur en fonction de la position des trous présents sur le support.

Étape 2 : Insérez les 3 chevilles à expansion dans les trous.

Figure 2-3 Perçage des trous (unité : mm [pouce])



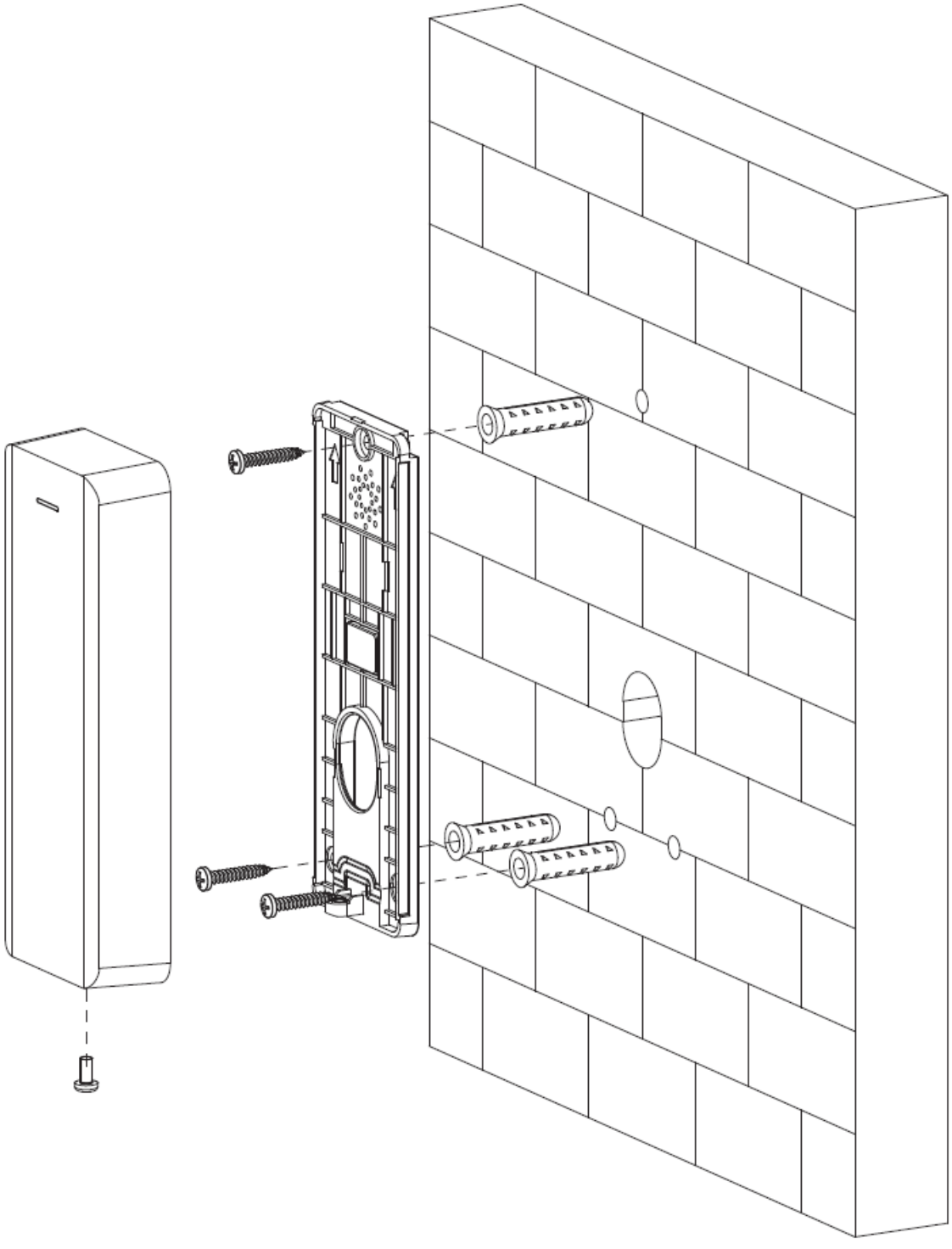
Étape 3 : Faites passer les fils du lecteur de carte dans la fente du support.

Étape 4 : Fixez le support au mur à l'aide de 3 vis.

Étape 5 : Fixez le lecteur de carte au support de bas en haut.

Étape 6 : Vissez une vis en bas pour fixer le lecteur de carte.

Figure 2-4 Perçage de trous (unité : mm [pouce])



3 Déverrouillage de la porte

Glissez la carte dans le lecteur de carte pour ouvrir la porte. Pour le lecteur de carte avec clavier, vous pouvez également déverrouiller la porte en entrant le mot de passe.

- Déverrouillez la porte en entrant le mot de passe public : Saisissez le mot de passe public, puis cliquez sur **#**.
- Déverrouillez la porte en entrant le mot de passe utilisateur : Saisissez l'ID utilisateur et tapez sur **#**, puis saisissez le mot de passe utilisateur et appuyez sur **#**.
- Déverrouillez la porte à l'aide de la carte et du mot de passe : Glissez la carte, entrez le mot de passe, puis appuyez sur **#**.

Si le mot de passe est correct, l'indicateur est vert et l'avertisseur sonore retentit une fois. Si le mot de passe est incorrect, l'indicateur est rouge et l'avertisseur sonore retentit 4 fois (communication RS-485) ou 3 fois (communication Wiegand ou aucune ligne de signal n'est connectée).

4 Invite lumineuse et vocale

Une fois le lecteur de carte mis sous tension, il émet un bip et le voyant LED est bleu fixe, ce qui signifie qu'il a été démarré avec succès.

Ne glissez qu'une seule carte à la fois. Ne glissez pas plusieurs cartes simultanément.

Tableau 4-1 Invites lumineuse et vocale

Fonction	Invites
Le lecteur de carte est sous tension.	Émet un bip et l'indicateur est bleu fixe.
Anti-sabotage	Émet un bip et dure 15 secondes.
Son du clavier	Émet un bip.
Association d'alarme	Émet un bip et dure 15 secondes.
Glisser la carte authentifiée (communication RS-485).	Émet un bip et l'indicateur devient vert.
Glisser la carte non authentifiée (communication RS-485)	Émet 4 bips et l'indicateur devient rouge.
Erreur de communication RS-485 et glisser la carte authentifiée/non authentifiée.	Émet 3 bips et l'indicateur devient rouge.
Glisser la carte authentifiée (communication Wiegand).	Émet un bip et l'indicateur devient vert.
Glisser la carte non authentifiée (communication Wiegand)	Émet un bip et l'indicateur devient rouge.
Le programme principal est en cours de mise à jour ou en état BOOT pour la mise à jour.	L'indicateur clignote en bleu jusqu'à ce que la mise à jour soit terminée.

5 Mise à jour du système

5.1 Mise à jour par SmartPSS Lite

Conditions préalables

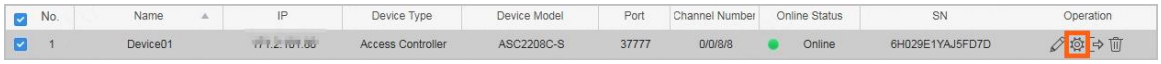
- Le lecteur de carte a été ajouté au contrôleur d'accès via des fils RS-485.
- Le contrôleur d'accès et le lecteur de carte sont sous tension.

Procédure

Étape 1 : Installez et connectez-vous à SmartPSS Lite, puis sélectionnez **Gestionnaire des appareils** (Device Manager).

Étape 2 : Cliquez sur .

Figure 5-1 Sélection du contrôleur d'accès



Étape 3 : Cliquez sur et pour sélectionner le fichier de mise à jour.

Étape 4 : Cliquez sur **Mettre à niveau** (Upgrade).

L'indicateur du lecteur de carte clignote en bleu jusqu'à ce que la mise à jour soit terminée, puis le lecteur de carte redémarre automatiquement.

5.2 Mise à jour via l'outil de config.

Conditions préalables

- Le lecteur de carte a été ajouté au contrôleur d'accès via des fils RS-485.
- Le contrôleur d'accès et le lecteur de carte sont sous tension.

Procédure

Étape 1 : Installez et ouvrez Configtool, puis sélectionnez **Mise à niveau de l'appareil** (Device upgrade).

Étape 2 : Cliquez sur d'un contrôleur d'accès, puis sur .

Étape 3 : Cliquez sur **Mettre à niveau** (Upgrade).

L'indicateur du lecteur de carte clignote en bleu jusqu'à ce que la mise à jour soit terminée, puis le lecteur de carte redémarre automatiquement.

Annexe 1 – Recommandations en matière de cybersécurité

Actions obligatoires à prendre pour la sécurité réseau d'équipements 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, p. 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 potentiels, 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.