

# 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 « 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
 <b>DANGER</b>	Indique un danger risquant d'entraîner la mort ou des blessures graves si les instructions données ne sont pas respectées.
 <b>AVERTISSEMENT</b>	Indique une situation moyennement ou faiblement dangereuse qui entraînera des blessures faibles ou modérées si les instructions données ne sont pas respectées.
 <b>ATTENTION</b>	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.
 <b>CONSEILS</b>	Fournit des instructions qui vous permettront de résoudre un problème ou de vous faire gagner du temps.
 <b>REMARQUE</b>	Fournit des informations supplémentaires en complément du texte.

## Historique des révisions

Version	Description de la révision	Date de publication
V1.0.0	Première publication.	Mars 2023

## 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

Avant-propos.....	I
Précautions et avertissements importants .....	III
1 Introduction.....	1
1.1 Caractéristiques .....	1
1.2 Apparence .....	1
2 Vue d'ensemble des ports .....	2
3 Installation.....	3
4 Invite sonore et lumineuse .....	4
5 Déverrouillage de la porte .....	5
5.1 Déverrouillage par carte à puce .....	5
5.2 Déverrouillage par Bluetooth .....	5
6 Mise à jour du système .....	16
6.1 Mise à jour via le contrôleur d'accès .....	16
6.2 Mise à jour via l'outil de config. ....	16
Annexe 1 – Recommandations en matière de cybersécurité .....	17

# 1 Introduction

## 1.1 Caractéristiques

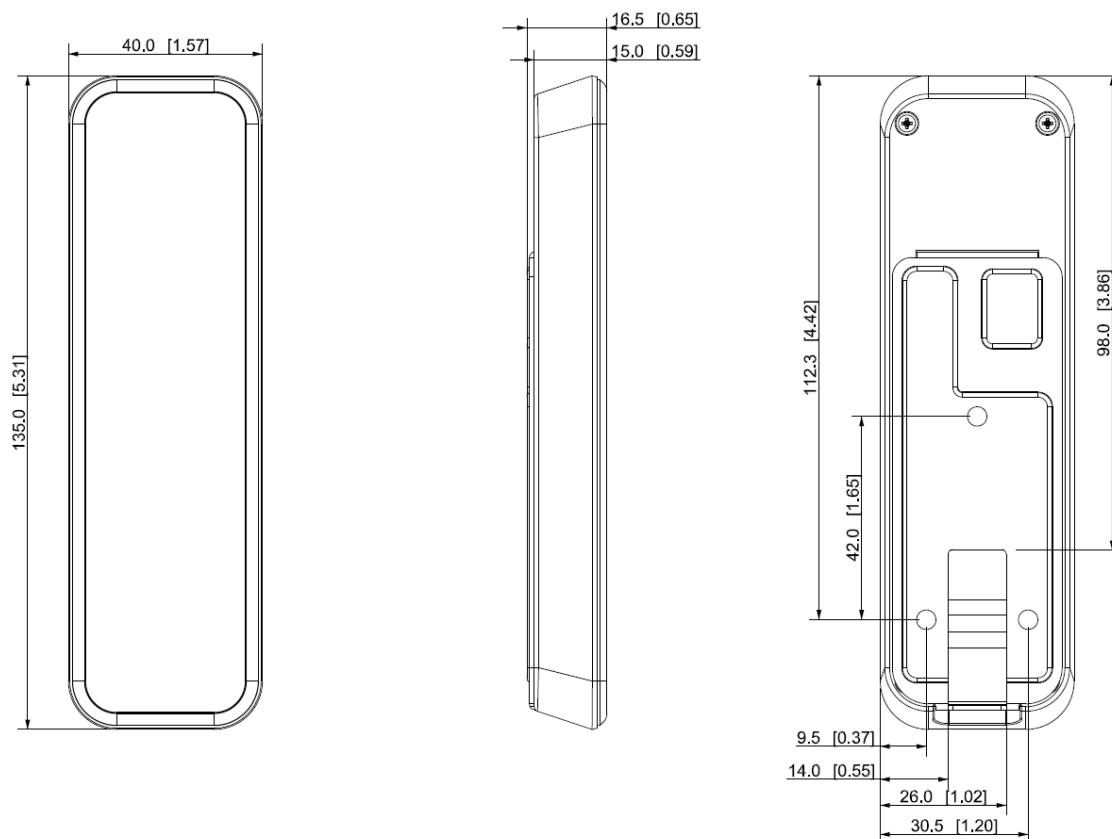
- Matériau PC, panneau en verre trempé et IP66, adapté à une utilisation intérieure et extérieure.
- Lecture de cartes sans contact pour les cartes à puce (cartes Mifare).
- Déverrouillage par glissement de carte et Bluebooth.
- Communication via le port RS-485, le port wiegand et le Bluetooth.
- Invite à l'aide d'un avertisseur sonore et d'un voyant lumineux.
- Prise en charge de l'alarme anti-sabotage.
- Le programme de chien de garde intégré peut détecter et contrôler l'état de fonctionnement anormal de l'équipement et effectuer un traitement de récupération pour assurer le fonctionnement à long terme de l'équipement.
- Tous les ports de connexion sont protégés contre les surintensités et les surtensions.
- Fonctionnement avec le client mobile DMSS et certains modèles de contrôleur d'accès (ASC3202B).



Les fonctions peuvent varier selon les modèles.

## 1.2 Apparence

Figure 1-1 Dimensions du modèle mince (mm [pouce])



## 2 Vue d'ensemble des ports



Utilisez RS-485 ou Wiegand pour connecter l'appareil.

Tableau 2-1 Description de la connexion par câble

Couleur	Port	Description
Rouge	RD+	PWR (12 V CC)
Noir	RD-	GND
Bleu	BOÎTIER	Signal d'alarme anti-sabotage
Blanc	D1	Signal de transmission Wiegand (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	

Tableau 2-2 Spécifications et longueur des câbles

Type d'appareil	Méthode de connexion	Longueur
Lecteur de carte RS485	Chaque fil doit avoir une longueur inférieure à 10 $\Omega$ .	100 m (328,08 pi)
Lecteur de carte Wiegand	Chaque fil doit avoir une longueur inférieure à 2 $\Omega$ .	80 m (262,47 pi)



# 3 Installation

## Procédure

Étape 1 : Percez 4 trous et une sortie de câble sur le mur.



Pour le câblage en saillie, la sortie de câble n'est pas nécessaire.

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

Étape 3 : Câblez le lecteur de carte et passez les fils dans la fente du support.

Étape 4 : Utilisez trois vis M3 pour fixer le support au mur.

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

Étape 6 : Serrez une vis M2 sur la partie inférieure du lecteur de carte.

Figure 3-1 Câblage encastré

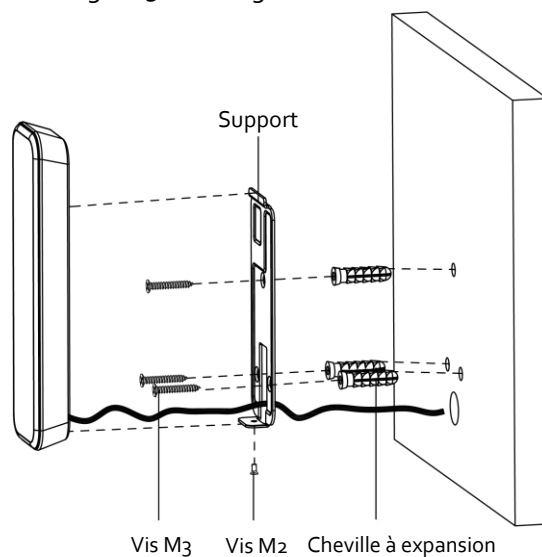
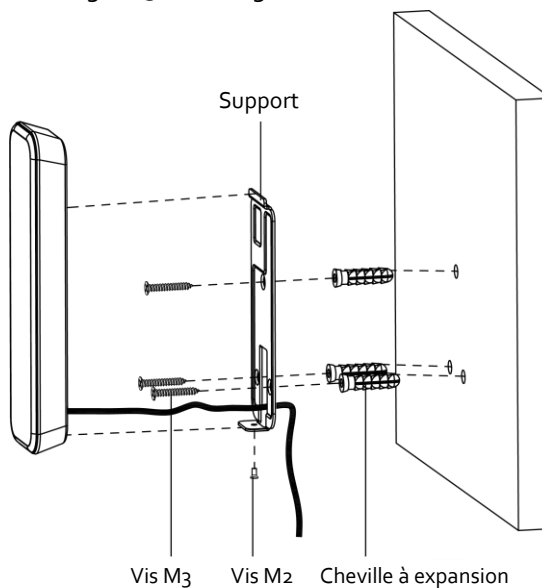


Figure 3-2 Câblage en saillie



## 4 Invite sonore et lumineuse

Tableau 4-1 Description de l'invite sonore et lumineuse

Situation	Invite sonore et lumineuse
Mise sous tension.	Sonne une fois. L'indicateur est bleu fixe.
Retrait de l'appareil.	Sonne longuement pendant 15 secondes.
Appui sur les boutons.	Sonne brièvement une fois.
Alarme déclenchée par le contrôleur.	Sonne longuement pendant 15 secondes.
Communication RS-485 et glissement d'une carte autorisée.	Sonne une fois. L'indicateur clignote une fois en vert, puis devient bleu fixe en mode veille.
Communication RS-485 et glissement d'une carte non autorisée.	Sonne quatre fois. L'indicateur clignote une fois en rouge, puis devient bleu fixe en mode veille.
Communication RS-485 anormale et glissement d'une carte autorisée/non autorisée.	Sonne trois fois. L'indicateur clignote une fois en rouge, puis devient bleu fixe en mode veille.
Communication Wiegand et glissement d'une carte autorisée.	Sonne une fois. L'indicateur clignote une fois en vert, puis devient bleu fixe en mode veille.
Communication Wiegand et glissement d'une carte non autorisée.	Sonne trois fois. L'indicateur clignote une fois en rouge, puis devient bleu fixe en mode veille.
Mise à jour du logiciel ou attente de mise à jour dans BOOT.	L'indicateur clignote en bleu jusqu'à ce que la mise à jour soit terminée.

# 5 Déverrouillage de la porte

Déverrouillez la porte à l'aide de la carte à puce et de la carte Bluetooth.

## 5.1 Déverrouillage par carte à puce

Déverrouillez la porte en glissant la carte à puce.

## 5.2 Déverrouillage par Bluetooth

Déverrouillez la porte à l'aide des cartes Bluetooth. Le lecteur de carte doit fonctionner avec le contrôleur d'accès (ASC3202B) pour réaliser le déverrouillage par Bluetooth. Pour plus de détails, consultez le manuel d'utilisation du contrôleur d'accès.

### Conditions préalables

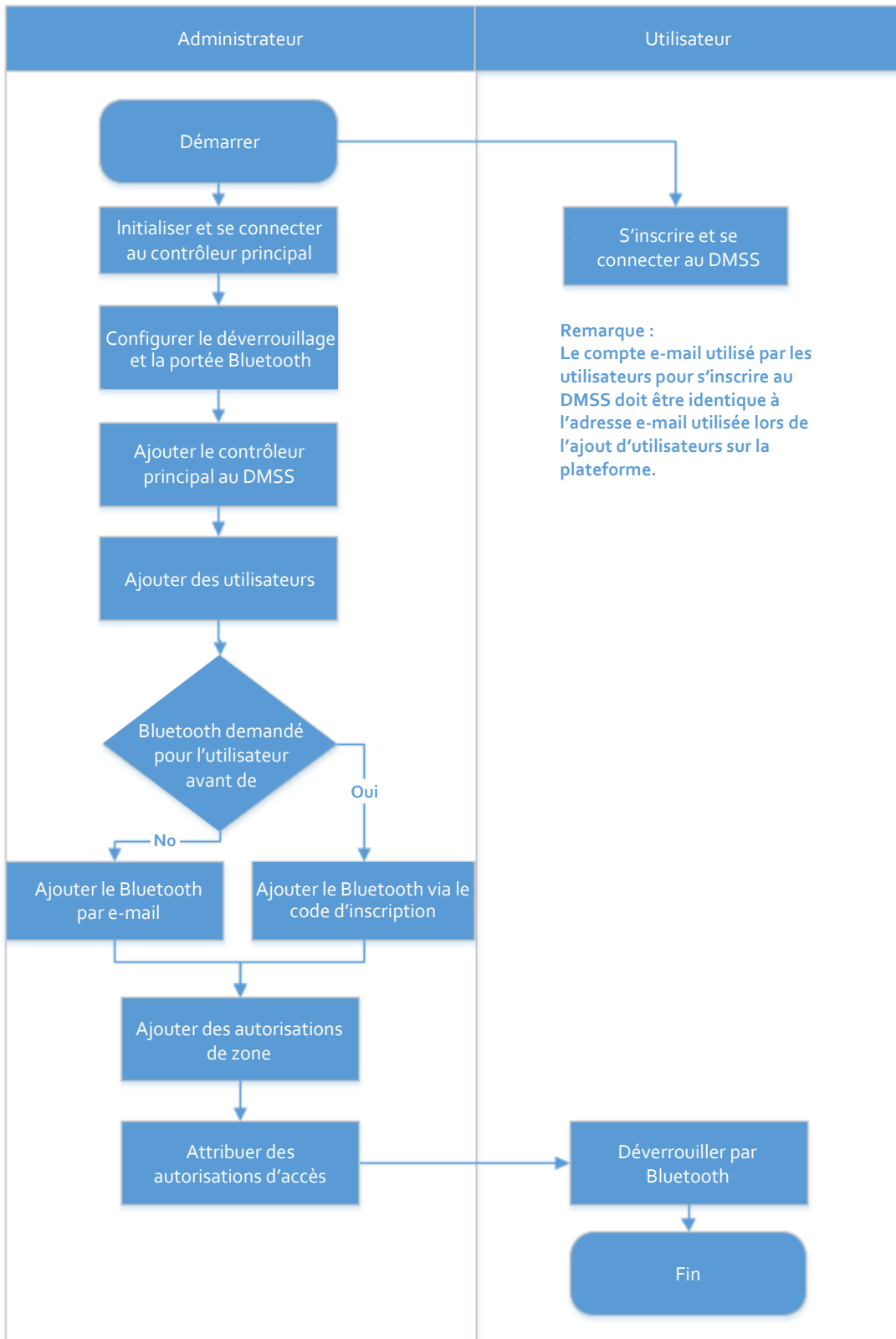
Les utilisateurs généraux, comme les employés d'une entreprise, se sont inscrits au DMSS avec leur e-mail.

### Préambule

Reportez-vous à l'organigramme de la configuration du déverrouillage par Bluetooth.

L'administrateur et les utilisateurs généraux doivent effectuer des opérations différentes comme indiqué ci-dessous. Les utilisateurs généraux, comme les employés de l'entreprise, ne doivent que s'inscrire et se connecter au DMSS via leur e-mail, puis ils peuvent déverrouiller les cartes Bluetooth qui leur ont été délivrées.

Figure 5-1 Organigramme de la configuration du déverrouillage par Bluetooth



L'administrateur doit effectuer Étape 1 à Étape 7, et les utilisateurs généraux doivent effectuer Étape 8.

## Procédure

Étape 1 : L'nitialisez et connectez-vous au contrôleur d'accès principal.

Étape 2 : Activez la fonction de la carte Bluetooth et configurez la portée Bluetooth.

Figure 5-2 Paramètres de verrouillage

The screenshot shows the 'Unlock Settings' interface with the following configurations:

- Unlock Mode:** Combination Unlock
- Combination Method:** Or (selected), And
- Unlock Method (Multi-select):** Card, Fingerprint, Password, Bluetooth Card (all selected)
- Bluetooth Mode:** Short-range, Mid-range (selected), Long-range
- Door Unlocked Duration:** 3.0 s (range 0.2-600)
- Unlock Timeout:** 60 s (range 1-9999)

La carte Bluetooth doit se trouver à une certaine distance du dispositif de contrôle d'accès pour échanger des données et déverrouiller la porte. Les plages suivantes sont les plus appropriées.

- Courte portée : La portée de déverrouillage Bluetooth est inférieure à 0,2 m.
- Moyenne portée : La portée de déverrouillage Bluetooth est inférieure à 2 m.
- Longue portée : La portée de déverrouillage Bluetooth est inférieure à 10 m.



La portée de déverrouillage Bluetooth peut varier en fonction des modèles de votre téléphone et de l'environnement.

Étape 3 : Téléchargez DMSS et inscrivez-vous avec un compte e-mail, puis scannez le code QR avec le DMSS pour ajouter le contrôleur d'accès.

Assurez-vous que le service cloud est activé.


Figure 5-3 Service cloud

Enable

After enabling the function and connecting Internet, we will collect device information such as IP address, MAC address, name and serial number. The collected information is only used for remote access of the device. If you do not agree to enable the function, please cancel the selection of check box.

Status

SN



Étape 4: Ajoutez des utilisateurs au contrôleur principal.



L'adresse e-mail que vous avez saisie lors de l'ajout d'utilisateurs au contrôleur principal doit être identique au compte e-mail que les utilisateurs utilisent pour s'inscrire au DMSS.

Figure 5- 4 Informations de base sur l'utilisateur

The screenshot shows a window titled "Edit" with a close button (X) in the top right corner. Below the title bar, there are three tabs: "Basic Info" (selected), "Authentication", and "Permission" (with a help icon). The "Basic Info" tab contains the following fields:

User ID	test001	* User Name	test wy
* Department	Default Company	* User Type	General User
Validity Period	2023-03-01 00:00:00	To	2037-12-31 23:59:59
Email	1182...387@qq.com		
* Unlock Attempts	Unlimited		

At the bottom right of the window, there are two buttons: "OK" (blue) and "Cancel" (white).

**Étape 5:** Dans l'onglet, cliquez sur **Carte Bluetooth** (Bluetooth Card).

3 méthodes sont disponibles pour l'ajout de cartes Bluetooth.

- Demande par e-mail, une par une : Cliquez sur **Demande par e-mail** (Request through Email).

Une carte Bluetooth est générée automatiquement. Vous pouvez générer jusqu'à 5 cartes pour chaque utilisateur.

Figure 5-5 Demande par e-mail

The screenshot shows a window titled "Edit" with a close button (X) in the top right corner. Below the title bar are three tabs: "Basic Info", "Authentication" (which is selected and underlined), and "Permission" with a help icon. The main content area is divided into sections. The first section lists authentication methods: "Password" (Not Added), "Card" (Not Added), "Fingerprint" (Not Added), and "Bluetooth Card" (Added: 4). The "Bluetooth Card" section is expanded to show four individual cards with IDs: 47\*\*\*\*41, 82\*\*\*\*3D, 76\*\*\*\*E3, and 9C\*\*\*\*E2. Each card has a trash icon at the bottom. Below the cards is a container with two buttons: "Request through Email" (highlighted with an orange border) and "Request through Registration Code". At the bottom right of the dialog are "OK" and "Cancel" buttons.

- Demande via e-mail par lots.
  1. Dans la page **Gestion des personnes** (Person Management), cliquez sur **Émission des cartes par lots** (Batch Issue Cards).



L'émission des cartes par lots ne prend en charge que les demandes par e-mail.

- ◇ Émettre des cartes Bluetooth à tous les utilisateurs de la liste : Cliquez sur **Émission des cartes à tous les utilisateurs** (Issue Cards to All Users).
  - ◇ Émettre des cartes Bluetooth aux utilisateurs sélectionnés : Sélectionnez des utilisateurs, puis cliquez sur **Émission des cartes aux utilisateurs sélectionnés** (Issue Cards to Selected Users).
2. Cliquez sur **Carte Bluetooth** (Bluetooth Card).
  3. Cliquez sur **Demande par e-mail** (Request through Email).





- ◇ Les utilisateurs qui ne disposent pas d'e-mail ou qui possèdent déjà 5 cartes Bluetooth seront affichés dans la liste des utilisateurs ne pouvant pas faire de demande.
- ◇ Exporter les utilisateurs n'ayant pas d'e-mail : Cliquez sur **Exporter** (Export), entrez les e-mails dans le format correct, puis cliquez sur **Importer** (Import). Ils seront déplacés vers la liste des utilisateurs pouvant faire de demande.

Figure 5-6 Émission des cartes par lots

### Batch Issue Cards

Card **Bluetooth Card**

**i** Bluetooth cards can only be generated in batches through emails.

**Issue Cards**

**Requestable (3)** Non-Requestable (1) [Export Users that Lack Emails](#) [Import](#)

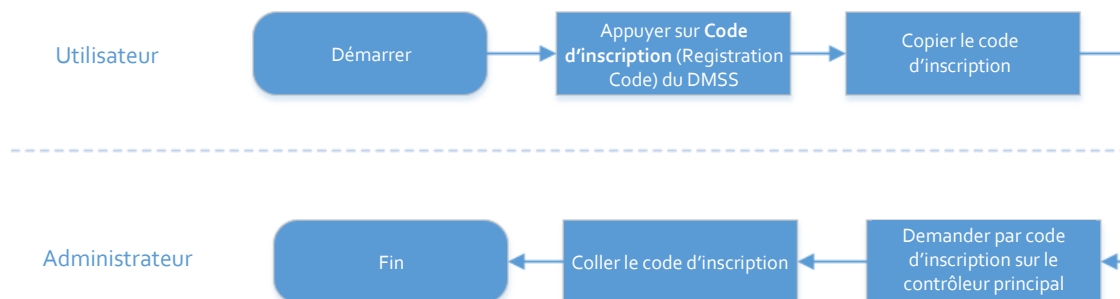
User ID	User Name	Email	Bluetooth Card No.	Status	Operation
001	001	118[redacted].com	0		⊖
002	002	118[redacted].com	0		⊖
003	003	11[redacted].com	0		⊖

User ID: 001      User Name: 001  
User Type: General User      Email: 118[redacted].com  
Department: Default Company  
Effective Time: 2023-06-15 00:00:00~2037-12-31 23:59:59

**Request through Email**

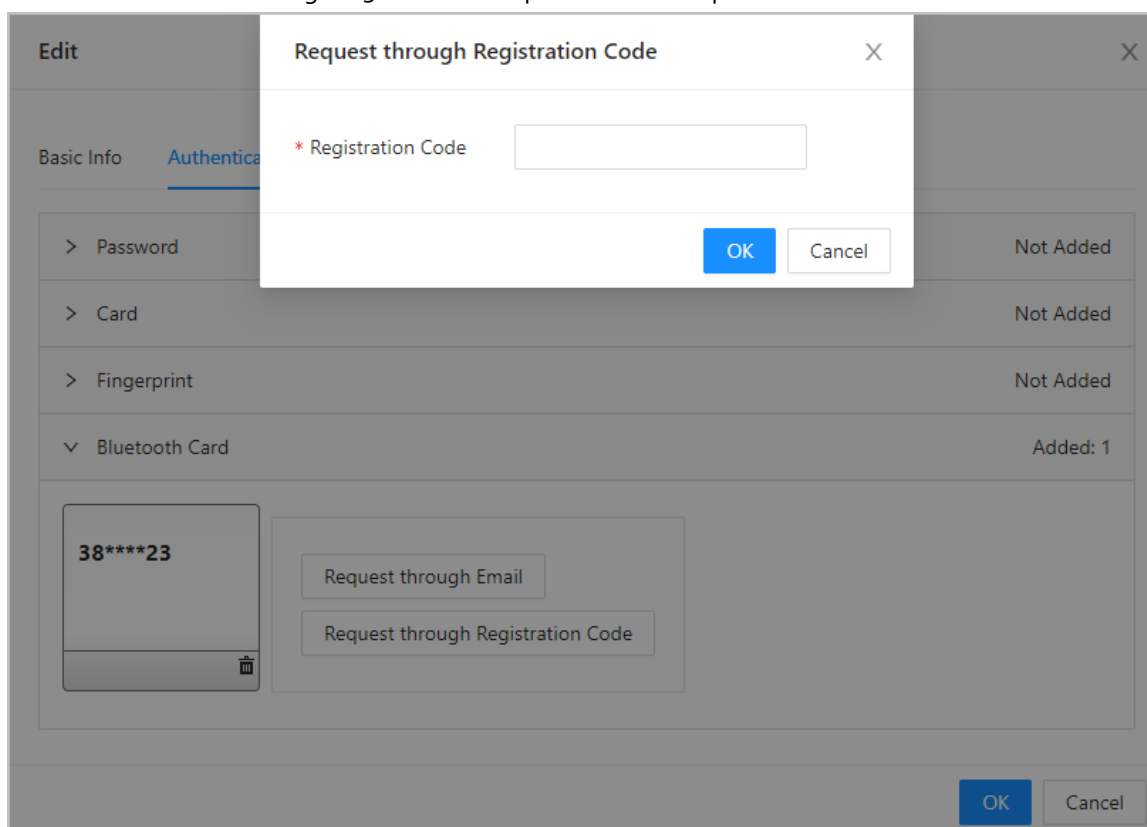
- Si vous avez déjà demandé des cartes Bluetooth pour l'utilisateur, vous pouvez ajouter les cartes Bluetooth à l'aide d'un code d'inscription en utilisant des codes d'inscription.

Figure 5-7 Organigramme de la demande par code d'inscription



1. Sur le DMSS, appuyez sur **Code d'inscription** (Registration Code) d'une carte Bluetooth.  
Le code d'inscription est automatiquement généré par le DMSS.
2. Copiez le code d'inscription.
3. Dans l'onglet **Carte Bluetooth** (Bluetooth Card), cliquez sur **Demander par code d'inscription** (Request through Registration Code), collez le code d'inscription, puis cliquez sur **OK**.

Figure 5-8 Demande par code d'inscription



4. Cliquez sur **OK**.  
La carte Bluetooth est ajoutée.

**Étape 6 :** Ajoutez des autorisations de zone.

Créez un groupe d'autorisation, puis associez des utilisateurs au groupe afin que les utilisateurs se voient attribuer les autorisations d'accès définies pour le groupe.

Figure 5-9 Création de groupes d'autorisation de zone

\* Area Name:  Remarks:

\* Time Templates:

**Device List**

Search

- Main Control
  - 8D00E71YAJE2232
    - Door1
    - Door2

>

**Selected 2 items.**

No.	Device Name	Operation
1	90_12_43_6d_88-Door1	
2	90_12_43_6d_88-Door2	

OK Cancel

**Étape 7 :** Ajoutez des autorisations d'accès aux utilisateurs.

Attribuez des autorisations d'accès aux utilisateurs en les associant au groupe d'autorisation de zone. Cela permettra aux utilisateurs d'accéder aux zones sécurisées.

Figure 5-10 Sélection des utilisateurs

Area Permission +

Search

Area Permission	Operation
Area Permission	
Area Permission1	

**Étape 8 :** Une fois que les utilisateurs se sont inscrits et connectés à DMSS avec leur adresse e-mail, ils doivent ouvrir DMSS pour déverrouiller la porte à l'aide des cartes Bluetooth. Pour plus de détails, consultez le manuel d'utilisation du DMSS.

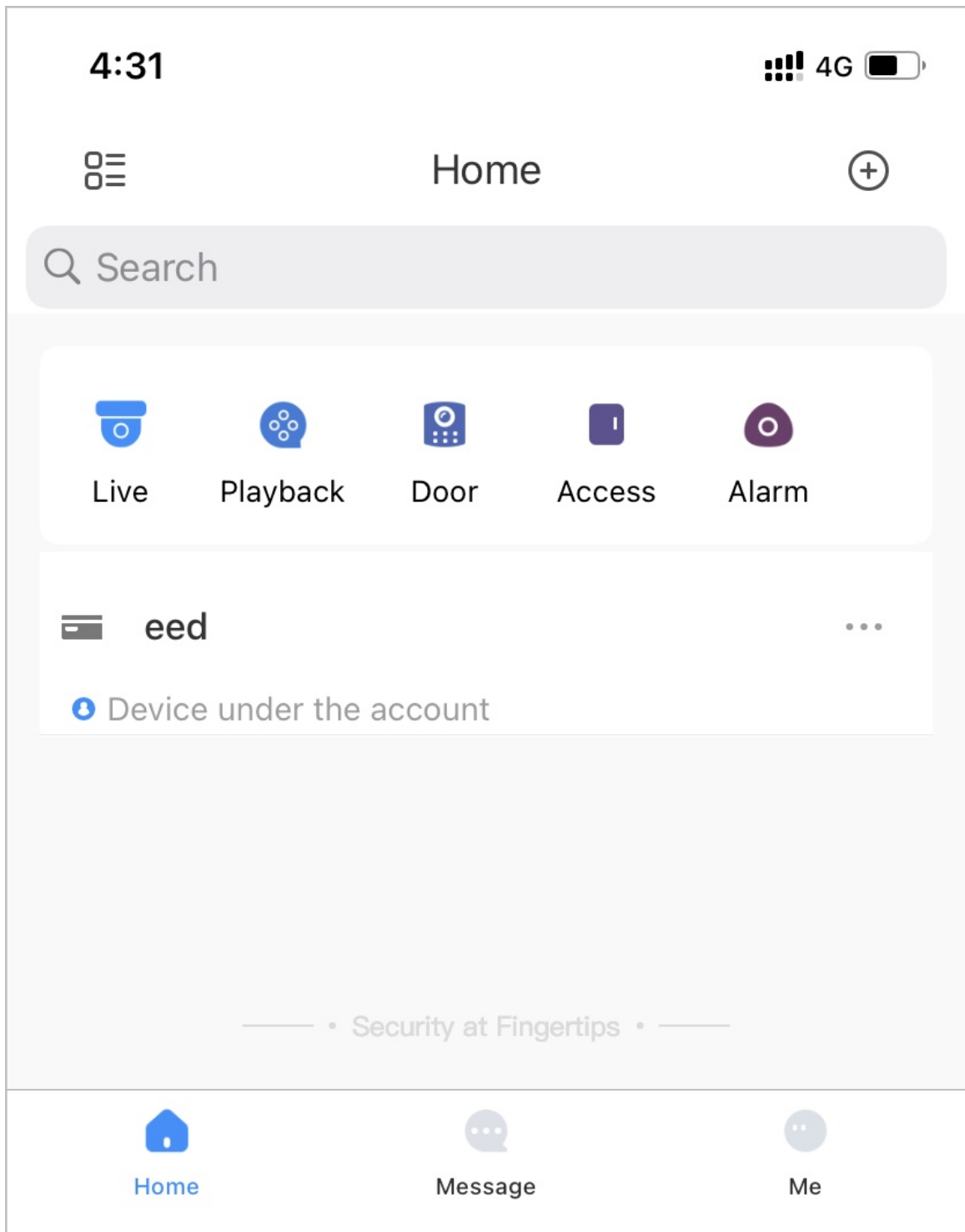
- Déverrouillage automatique : La porte se déverrouille automatiquement lorsque vous vous trouvez dans la zone Bluetooth définie, ce qui permet à la carte Bluetooth de transmettre des signaux au lecteur de carte.



En mode de déverrouillage automatique, la carte Bluetooth déverrouillera fréquemment la porte si vous vous trouvez toujours dans la zone Bluetooth, ce qui peut entraîner une panne. Veuillez désactiver le Bluetooth sur le téléphone et le réactiver.

- Secouer pour déverrouiller : La porte se déverrouille lorsque vous secouez votre téléphone pour permettre à la carte Bluetooth de transmettre des signaux au lecteur de carte.

Figure 5-11 Déverrouillage de la porte à l'aide des cartes Bluetooth



## Résultat

- Déverrouillage réussi : Le voyant vert clignote et l'avertisseur sonore retentit une fois.
- Échec du déverrouillage : Le voyant rouge clignote et l'avertisseur sonore retentit 4 fois.

# 6 Mise à jour du système

Mettez à jour le système du lecteur de carte via le contrôleur d'accès ou Configtool.

## 6.1 Mise à jour via le contrôleur d'accès

### Conditions préalables

Connectez le lecteur de carte au contrôleur d'accès (ASC3202B) via RS-485.

### Préambule



- Utilisez le fichier de mise à jour correct. Assurez-vous d'obtenir le fichier de mise à jour correct auprès du support technique.
- Ne déconnectez pas l'alimentation électrique ou le réseau, et ne redémarrez pas ou n'arrêtez pas le contrôleur d'accès pendant la mise à jour.

### Procédure

Étape 1 : Sur la page d'accueil du contrôleur d'accès, sélectionnez **Config. de l'appareil local > Mise à jour système** (Device Config > System Update).

Étape 2 : Dans **Mise à jour du fichier** (File Update), cliquez sur **Parcourir** (Browse), puis téléchargez le fichier de mise à jour.



Le fichier de mise à jour doit être un fichier « .bin ».

Étape 3 : Cliquez sur **Mettre à jour** (Update).

Une fois le système du lecteur de carte mis à jour avec succès, le contrôleur d'accès et le lecteur de carte redémarrent.



## 6.2 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

Veillez 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, GARP 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.