
# Terminal de reconnaissance faciale de la série DS-K1T343

**Manuel de l'utilisateur**

# Informations juridiques



## À propos de ce manuel

Le manuel contient des instructions pour l'utilisation et la gestion du produit. Les photos, les graphiques, les images et toutes les autres informations ci-après sont uniquement des descriptions et des explications. Les informations contenues dans le manuel sont susceptibles d'être modifiées, sans préavis, en raison de mises à jour du micrologiciel ou pour d'autres raisons. Vous trouverez la dernière version de ce manuel sur le site Web de Hikvision ( ***https://www.hikvision.com/*** ).
Veuillez utiliser ce manuel avec les conseils et l'assistance de professionnels formés à l'utilisation du produit.

## Marques déposées

HIKVISION et les autres marques et logos d'Hikvision sont la propriété d'Hikvision dans diverses juridictions.
Les autres marques et logos mentionnés sont la propriété de leurs détenteurs respectifs.

## Clause de non-responsabilité

DANS TOUTE LA MESURE PERMISE PAR LA LOI APPLICABLE, CE MANUEL ET LE PRODUIT DÉCRIT, AVEC SON MATÉRIEL, SON LOGICIEL ET SON MICROLOGICIEL, SONT FOURNIS "EN L'ÉTAT" ET "AVEC TOUS LES DÉFAUTS ET TOUTES LES ERREURS". HIKVISION NE DONNE AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, Y COMPRIS, MAIS SANS S'Y LIMITER, LA QUALITÉ MARCHANDE, LA QUALITÉ SATISFAISANTE OU L'ADÉQUATION À UN USAGE PARTICULIER. VOUS UTILISEZ LE PRODUIT À VOS PROPRES RISQUES. EN AUCUN CAS HIKVISION NE POURRA ETRE TENU RESPONSABLE DE DOMMAGES SPECIAUX, CONSECUTIFS, ACCIDENTELS OU INDIRECTS, Y COMPRIS, ENTRE AUTRES, LES DOMMAGES POUR PERTE DE BENEFICES COMMERCIAUX, INTERRUPTION D'ACTIVITE, OU PERTE DE DONNEES, CORRUPTION DE SYSTEMES, OU PERTE DE DOCUMENTATION, QUE CE SOIT SUR LA BASE D'UNE RUPTURE DE CONTRAT, D'UN TORT (Y COMPRIS LA NEGLIGENCE), DE LA RESPONSABILITE DU PRODUIT, OU AUTRE, EN RELATION AVEC L'UTILISATION DU PRODUIT, MEME SI HIKVISION A ETE AVISE DE LA POSSIBILITE DE TELS DOMMAGES OU DE TELLES PERTES.
VOUS RECONNAISSEZ QUE LA NATURE DE L'INTERNET COMPORTE DES RISQUES DE SÉCURITÉ INHÉRENTS ET QU'HIKVISION N'ASSUME AUCUNE RESPONSABILITÉ EN CAS DE FONCTIONNEMENT ANORMAL, D'ATTEINTE À LA VIE PRIVÉE OU D'AUTRES DOMMAGES RÉSULTANT D'UNE CYBER-ATTAQUE, D'UNE ATTAQUE DE PIRATES INFORMATIQUES, D'UNE INFECTION PAR UN VIRUS OU D'AUTRES RISQUES LIÉS À LA SÉCURITÉ DE L'INTERNET ; TOUTEFOIS, HIKVISION FOURNIRA UNE ASSISTANCE TECHNIQUE EN TEMPS UTILE SI NÉCESSAIRE.
VOUS ACCEPTEZ D'UTILISER CE PRODUIT DANS LE RESPECT DE TOUTES LES LOIS APPLICABLES, ET VOUS ÊTES SEUL RESPONSABLE DE LA CONFORMITÉ DE VOTRE UTILISATION À LA LOI APPLICABLE. EN PARTICULIER, VOUS ÊTES RESPONSABLE DE L'UTILISATION DE CE PRODUIT D'UNE MANIÈRE QUI N'ENFREINT PAS LES DROITS DES TIERS, Y COMPRIS, MAIS SANS S'Y LIMITER, LES DROITS DE PUBLICITÉ, LES DROITS DE PROPRIÉTÉ INTELLECTUELLE OU LES DROITS DE PROTECTION DES DONNÉES ET AUTRES DROITS À LA VIE PRIVÉE. VOUS NE DEVEZ PAS UTILISER CE PRODUIT POUR DES UTILISATIONS FINALES INTERDITES, Y COMPRIS LES UTILISATIONS SUIVANTES

LE DÉVELOPPEMENT OU LA PRODUCTION D'ARMES DE DESTRUCTION MASSIVE, LE DÉVELOPPEMENT OU LA PRODUCTION D'ARMES CHIMIQUES OU BIOLOGIQUES, TOUTE ACTIVITÉ LIÉE À UN EXPLOSIF NUCLÉAIRE OU À UN CYCLE DE COMBUSTIBLE NUCLÉAIRE DANGEREUX, OU LE SOUTIEN À DES VIOLATIONS DES DROITS DE L'HOMME. EN CAS DE CONFLIT ENTRE CE MANUEL ET LA LOI APPLICABLE, CETTE DERNIÈRE PRÉVAUT.

## Protection des données

Lors de l'utilisation du dispositif, des données personnelles seront collectées, stockées et traitées. Pour protéger les données, le développement des appareils Hikvision intègre des principes de protection de la vie privée dès la conception. Par exemple, pour les appareils dotés de fonctions de reconnaissance faciale, les données biométriques sont stockées dans votre appareil avec une méthode de cryptage ; pour les appareils à empreintes digitales, seul le modèle d'empreinte digitale est sauvegardé, ce qui rend impossible la reconstitution d'une image d'empreinte digitale.

En tant que responsable du traitement des données, il vous est conseillé de collecter, stocker, traiter et transférer les données conformément aux lois et réglementations applicables en matière de protection des données, y compris, mais sans s'y limiter, d'effectuer des contrôles de sécurité pour sauvegarder les données à caractère personnel, tels que la mise en œuvre de contrôles de sécurité administratifs et physiques raisonnables, la réalisation d'examens et d'évaluations périodiques de l'efficacité de vos contrôles de sécurité.

# Conventions relatives aux symboles

Les symboles que l'on peut trouver dans ce document sont définis comme suit.

| Symbole | Description |
|---|---|
|  **Danger** | Indique une situation dangereuse qui, si elle n'est pas évitée, entraînera ou pourrait entraîner la mort ou des blessures graves. |
|  **Attention** | Indique une situation potentiellement dangereuse qui, si elle n'est pas évitée, peut entraîner des dommages à l'équipement, une perte de données, une dégradation des performances ou des résultats inattendus. |
|  **Note** | Fournit des informations supplémentaires pour souligner ou compléter des points importants du texte principal. |

# Informations réglementaires

## Informations sur la FCC

Veuillez noter que les changements ou modifications non expressément approuvés par la partie responsable de la conformité peuvent annuler l'autorité de l'utilisateur à faire fonctionner l'équipement.
Conformité FCC : Cet équipement a été testé et déclaré conforme aux limites imposées aux appareils numériques de classe B, conformément à la partie 15 des règles de la FCC. Ces limites sont conçues pour fournir une protection raisonnable contre les interférences nuisibles dans une installation résidentielle. Cet équipement génère, utilise et peut émettre des fréquences radio et, s'il n'est pas installé et utilisé conformément aux instructions, peut causer des interférences nuisibles aux communications radio. Cependant, il n'y a aucune garantie que des interférences ne se produiront pas dans une installation particulière. Si cet équipement provoque des interférences nuisibles à la réception de la radio ou de la télévision, ce qui peut être déterminé en éteignant et en allumant l'équipement, l'utilisateur est encouragé à essayer de corriger les interférences en prenant une ou plusieurs des mesures suivantes :

-Réorienter ou déplacer l'antenne de réception.

-Augmenter la distance entre l'équipement et le récepteur.

-Brancher l'appareil sur une prise de courant d'un circuit différent de celui sur lequel le récepteur est branché.

-Consulter le revendeur ou un technicien radio/TV expérimenté pour obtenir de l'aide

Cet appareil doit être installé et utilisé avec une distance minimale de 20 cm entre radiateur et votre corps.

Conditions FCC

Cet appareil est conforme à la partie 15 des règles de la FCC. Son fonctionnement est soumis aux deux conditions suivantes :

1. Cet appareil ne doit pas provoquer d'interférences nuisibles.
2. Cet appareil doit accepter toute interférence reçue, y compris les interférences susceptibles de provoquer un fonctionnement indésirable.

## Déclaration de conformité de l'UE

CE

Ce produit et, le cas échéant, les accessoires fournis sont marqués du sigle "CE" et sont donc conformes aux normes européennes harmonisées en vigueur.

en vertu de la directive CEM 2014/30/EU, de la directive RE 2014/53/EU, de la directive RoHS 2011/65/EU

2012/19/EU (directive DEEE) : Les produits marqués de ce symbole ne peuvent pas être éliminés comme des déchets municipaux non triés dans l'Union européenne. Pour un recyclage adéquat, renvoyez ce produit à votre fournisseur local lors de l'achat d'un nouvel équipement équivalent, ou déposez-le dans les points de collecte prévus à cet effet. Pour plus d'informations, voir : www.recyclethis.info

2006/66/CE (directive sur les piles) : Ce produit contient une batterie qui ne peut pas être éliminée comme un déchet municipal non trié dans l'Union européenne. Voir la documentation du produit pour des informations spécifiques sur la batterie. La batterie est marquée de ce symbole, qui peut inclure des lettres indiquant la présence de cadmium (Cd), de plomb (Pb) ou de mercure (Hg). Pour un recyclage correct, renvoyez la batterie à votre fournisseur ou à un point de collecte désigné. Pour plus d'informations, voir : www.recyclethis.info

Cet appareil est conforme à la (aux) norme(s) RSS exemptée(s) de licence d'Industrie Canada. Son utilisation est soumise deux conditions suivantes :

(1) cet appareil ne doit pas causer d'interférences, et

(2) cet appareil doit accepter toute interférence, y compris les interférences susceptibles d'entraîner un fonctionnement indésirable de l'appareil.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

# Consignes de sécurité

Ces instructions ont pour but d'assurer que l'utilisateur puisse utiliser le produit correctement afin d'éviter tout danger ou perte matérielle.

Les mesures de précaution sont divisées en deux catégories : les dangers et les mises en garde :

**Dangers :** Le non-respect de l'un des avertissements peut entraîner des blessures graves, voire mortelles.

**Précautions :** Le non-respect de l'une des mises en garde peut entraîner des blessures ou endommager l'équipement.

| ⚠ | ⚠ |
|---|---|
| **Dangers :** Respectez les consignes de sécurité suivantes afin d'éviter des blessures graves ou mortelles. | **Précautions :** Respectez ces précautions afin d'éviter tout risque de blessure ou de dommage matériel. |

### ⚠ Danger :

- Lors de l'utilisation du produit, vous devez vous conformer strictement aux règles de sécurité électrique du pays et de la région.
- Ne connectez pas plusieurs appareils à un seul adaptateur d'alimentation, car la surcharge de l'adaptateur peut entraîner une surchauffe ou un risque d'incendie.
- Si de la fumée, des odeurs ou des bruits s'échappent de l'appareil, éteignez-le immédiatement et débranchez le câble d'alimentation, puis contactez le centre de service.
- La prise de courant doit être installée à proximité de l'équipement et être facilement accessible.
- 1. Ne pas ingérer la batterie. Risque de brûlure chimique !
  2. Ce produit contient une  bouton. Si la pile bouton est avalée, elle peut provoquer de graves brûlures internes en seulement 2 heures et peut entraîner la mort.
  3. Conservez les piles neuves et usagées hors de portée des enfants.
  4. Si le compartiment à piles ne se ferme pas correctement, cessez d'utiliser le produit et tenez-le hors de portée des enfants.
  5. Si vous pensez que des piles ont été avalées ou placées à l'intérieur d'une partie du corps, consultez immédiatement un médecin.
  6. ATTENTION : Risque d'explosion si la batterie est remplacée par un type incorrect.
  7. Le remplacement de la batterie par un type de batterie incorrect peut mettre en échec une mesure de protection (par exemple, dans le cas de certains types de batteries au lithium).
  8. Ne jetez pas la au feu ou dans un four chaud, ne l'écrasez pas mécaniquement et ne la coupez pas, car cela pourrait provoquer une explosion.
  9. Ne laissez pas la batterie dans un environnement où la température est extrêmement élevée, ce qui pourrait entraîner une explosion ou une fuite de liquide ou de gaz inflammable.
  10. Ne soumettez pas la batterie à une pression d'air extrêmement basse, qui pourrait entraîner une explosion ou une fuite de liquide ou de gaz inflammable.
  11. Les piles usagées doivent être éliminées conformément aux instructions.

## ⚠ Précautions d'emploi :

- Ne faites pas tomber l'appareil, ne le soumettez pas à des chocs physiques et ne l'exposez pas à des radiations électromagnétiques élevées. Évitez d'installer l'appareil sur une surface vibrante ou dans un endroit soumis à des chocs (l'ignorance peut endommager l'appareil).
- Ne placez pas l'appareil dans des endroits extrêmement chauds (reportez-vous aux spécifications de l'appareil pour connaître la température de fonctionnement détaillée), froids, poussiéreux ou humides, et ne l'exposez pas à des radiations électromagnétiques élevées.
- Il est interdit d'exposer l'appareil à la lumière directe du soleil, à une faible ventilation ou à une source de chaleur telle qu'un chauffage ou un radiateur (l'ignorance peut entraîner un risque d'incendie).
- Le couvercle de l'appareil utilisé à l'intérieur doit être protégé de la pluie et de l'humidité.
- Il est interdit d'exposer l'appareil à la lumière directe du soleil, à une faible ventilation ou à une source de chaleur telle qu'un chauffage ou un radiateur (l'ignorance peut entraîner un risque d'incendie).
- Utilisez un chiffon doux et sec pour nettoyer les surfaces intérieures et extérieures du couvercle de l'appareil, n'utilisez pas de détergents alcalins.
- Les produits de reconnaissance biométrique ne sont pas totalement adaptés aux environnements de lutte contre l'usurpation d'identité. Si vous avez besoin d'un niveau de sécurité plus élevé, utilisez plusieurs modes d'authentification.
- Le port série de l'appareil est utilisé uniquement pour le débogage.
- Installez l'appareil conformément aux instructions de ce manuel. Pour éviter toute blessure, l'appareil doit être solidement fixé au sol ou au mur conformément aux instructions d'installation.
- L'utilisation ou le remplacement incorrect de la batterie peut entraîner un risque d'explosion. Remplacez-la uniquement par une pile du même type ou d'un type équivalent. Éliminez les piles usagées conformément aux instructions fournies par le fabricant de la pile.
- Ce support est destiné à être utilisé uniquement avec les appareils équipés. L'utilisation avec d'autres équipements peut entraîner une instabilité et des blessures.
- Cet appareil ne doit être utilisé qu'avec le support prévu à cet effet. L'utilisation d'autres supports (chariots, supports ou transporteurs) peut entraîner une instabilité et des blessures.

# Modèles disponibles

| Nom du produit | Modèle | Sans fil |
|---|---|---|
| Terminal de reconnaissance faciale | DS-K1T343MX | 13,56 MHz Fréquence de présentation des cartes |
| | DS-K1T343MWX | 13,56 MHz Fréquence de présentation des cartes, Wi-Fi |
| | DS-K1T343MFX | 13,56 MHz Fréquence de présentation de la carte |
| | DS-K1T343MFWX | 13,56 MHz Fréquence de présentation des cartes, Wi-Fi |
| | DS-K1T343EX | 125 KHz Fréquence de présentation des cartes |
| | DS-K1T343EWX | 125 KHz Fréquence de présentation des cartes, Wi-Fi |
| | DS-K1T343EFX | 125 KHz Fréquence de présentation des cartes |
| | DS-K1T343EFWX | 125 KHz Fréquence de présentation des cartes, Wi-Fi |

N'utilisez que les blocs d'alimentation indiqués dans le mode d'emploi :

| Modèle | Fabricant | Standard |
|---|---|---|
| ADS-12FG-12N 12012EPG | Shenzhen Honor Electronic Co. | PG |

# Contenu

# Chapitre 1 : Vue d'ensemble

## 1.1 Vue d'ensemble

Le terminal de reconnaissance faciale est un type de dispositif de contrôle d'accès par reconnaissance faciale, qui est principalement utilisé dans les systèmes de contrôle d'accès de sécurité, tels que les centres logistiques, les aéroports, les campus universitaires, les centrales d'alarme, les habitations, etc.

## 1.2 Caractéristiques

- Écran tactile LCD de 4,3 pouces
- Double objectif grand angle de 2 MP
- Anti-usurpation de visage
- Distance de reconnaissance des visages : 0,3 m à 1,5 m
- Hauteur suggérée pour la reconnaissance faciale : entre 1,4 m et 1,9 m
- Algorithme d'apprentissage profond
- Capacité 1 500 visages, 3 000 cartes et 150 000 événements
- Durée de la reconnaissance des visages < 0,2 s/Utilisateur ; taux de précision de la reconnaissance des visages≥ 99%.
- Lien de capture et stockage des images capturées
- Transmet les données relatives à la carte et à l'utilisateur depuis ou vers le logiciel client via le protocole TCP/IP et enregistre données sur le logiciel client.
- Importe des photos du lecteur flash USB vers l'appareil ou exporte des photos, des événements, de l'appareil vers le lecteur flash USB.
- Fonctionnement autonome
- Gérer, rechercher et définir les données de l'appareil après s'être connecté localement à l'appareil
- Connexion à un lecteur de cartes externe ou à un contrôleur d'accès via le protocole RS-485
- Se connecte à une unité de contrôle de porte sécurisée via le protocole RS-485 pour éviter que la porte ne s'ouvre lorsque le dispositif est détruit.
- Audio bidirectionnel
- Armes par plusieurs logiciels clients
- Conception de chien de garde et fonction d'autoprotection
- Prise en charge de l'anglais, de l'espagnol (Amérique du Sud), de l'arabe, du thaï, de l'indonésien, du russe, du vietnamien, du portugais (Brésil), du coréen et du japonais.

# Chapitre 2 Apparence

L'apparence de l'appareil avec empreinte digitale est la suivante :

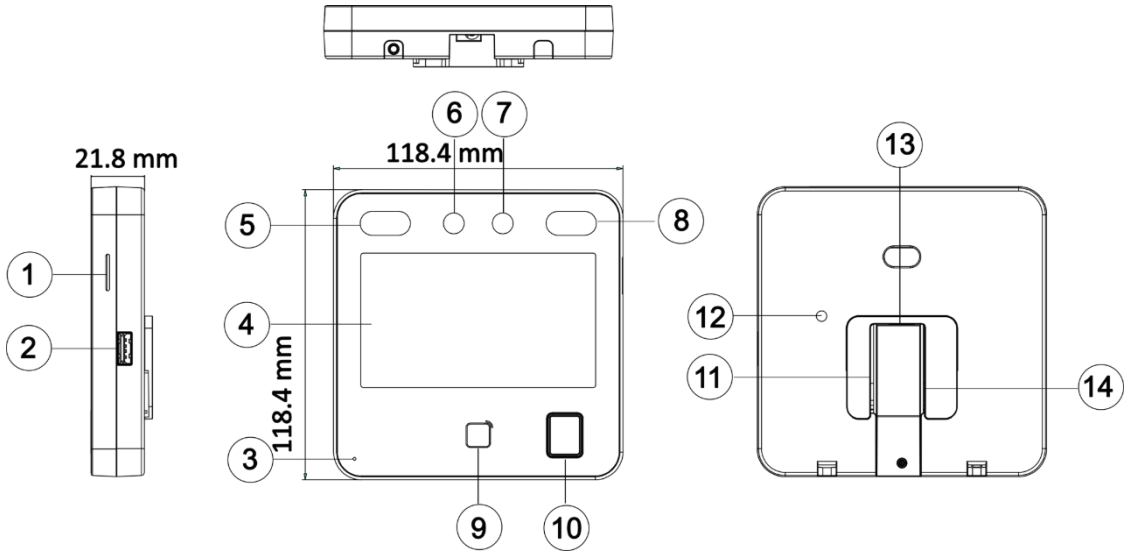



**Figure 2-1 Apparence（avec empreinte digitale)**

L'apparence de l'appareil sans empreinte digitale est la suivante :

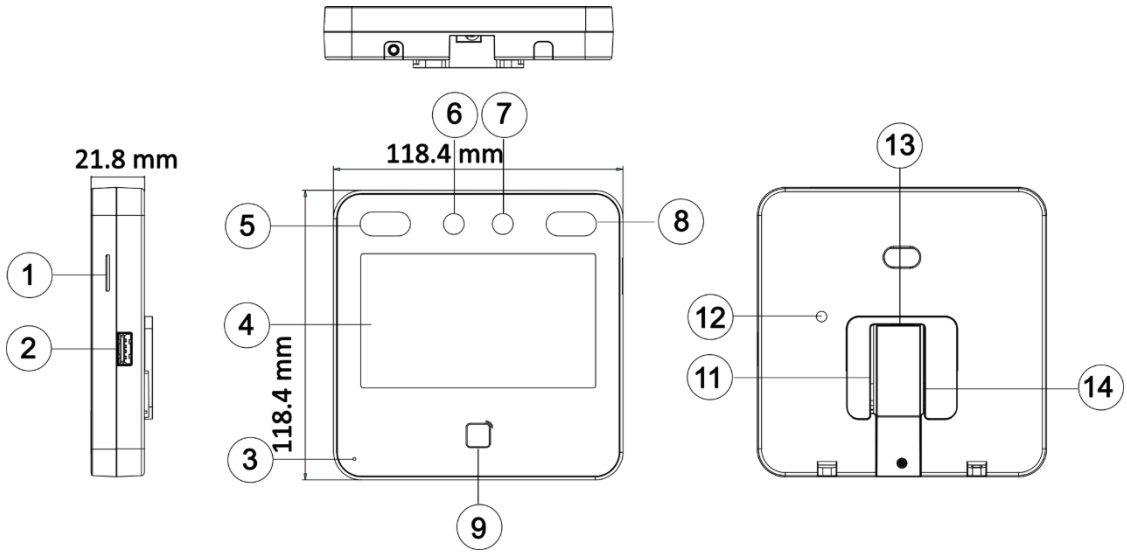



**Figure 2-2 Apparence（Sans empreinte digitale)**

**Tableau 2-1 Description de l'apparence**

| Non. | Nom |
|---|---|
| 1 | Haut-parleur |
| 2 | Interface USB |
| 3 | MIC |
| 4 | Écran tactile |
| 5 | Lumière IR |
| 6 | Appareil photo |
| 7 | Appareil photo |
| 8 | Lumière IR |
| 9 | Zone de présentation des cartes |
| 10 | Module d'empreintes digitales<br>**Note**<br>Seuls les appareils qui prennent en charge la fonction d'empreinte digitale contiennent un module d'empreinte digitale. |
| 11 | Borne de câblage (y compris l'interface d'alimentation) |
| 12 | TAMPER |
| 13 | Interface réseau |
| 14 | Port de débogage (pour le débogage uniquement) |

# Chapitre 3 Installation

## 3.1 Environnement d'installation

- Évitez le contre-jour, la lumière directe du soleil et la lumière indirecte du soleil.
- Pour une meilleure reconnaissance, une source lumineuse doit se trouver à l'intérieur ou à proximité de l'environnement d'installation.
- Le poids minimum du mur ou d'autres endroits doit être trois fois plus élevé que le poids de l'appareil.
- Il ne doit pas y avoir d'objets fortement réfléchissants (tels que portes/murs en verre, objets en acier inoxydable, acrylique et autres plastiques brillants, laques, carreaux de céramique, etc.) à moins de 1 m du champ de vision de l'appareil.
- Éviter la réflexion de l'appareil.
- La distance de reconnaissance des visages doit être supérieure à 30 cm.
- Gardez l'appareil photo propre.

**Note**

Pour plus de détails sur l'environnement d'installation, voir *Conseils pour l'environnement d'installation*.

## 3.2 Installer avec le boîtier Gang

**Étapes**

1. Assurez-vous que la boîte de dérivation est installée sur le mur.

   **Note**

   Vous devez acheter la boîte de raccordement séparément.

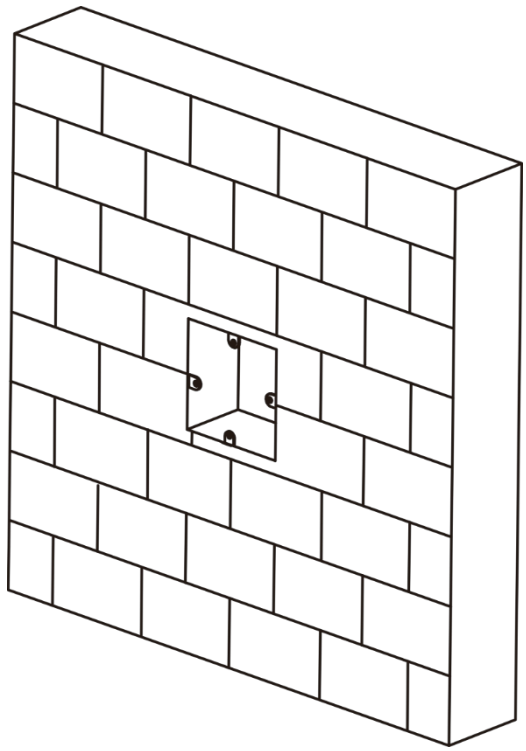


**Figure 3-1 Installation du boîtier d'encastrement**

**2.** Utilisez les 4 vis fournies (M4) pour fixer la plaque de montage sur la boîte de dérivation.

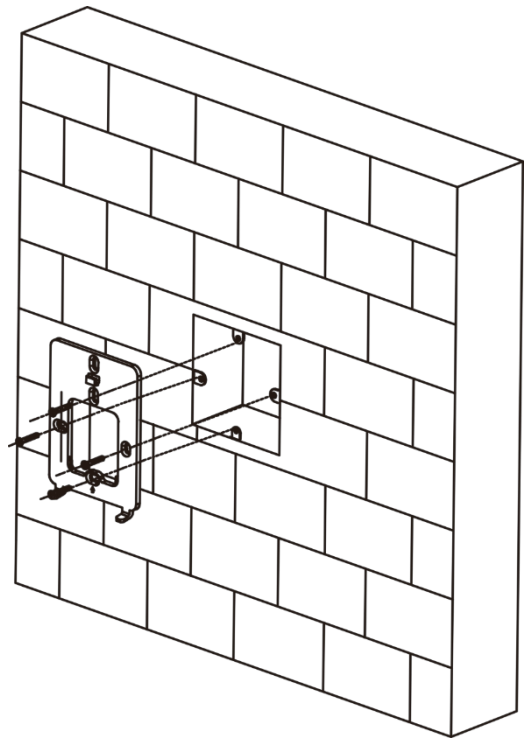


**Figure 3-2 Installation de la plaque de montage**

3. Faites passer les câbles par le trou de câble de la plaque de montage et connectez-les aux câbles des périphériques correspondants.
4. S'encliqueter dans la plaque de montage après avoir aligné l'appareil avec la plaque de montage. Utilisez une vis fournie (M3) pour fixer l'appareil sur la plaque de montage.

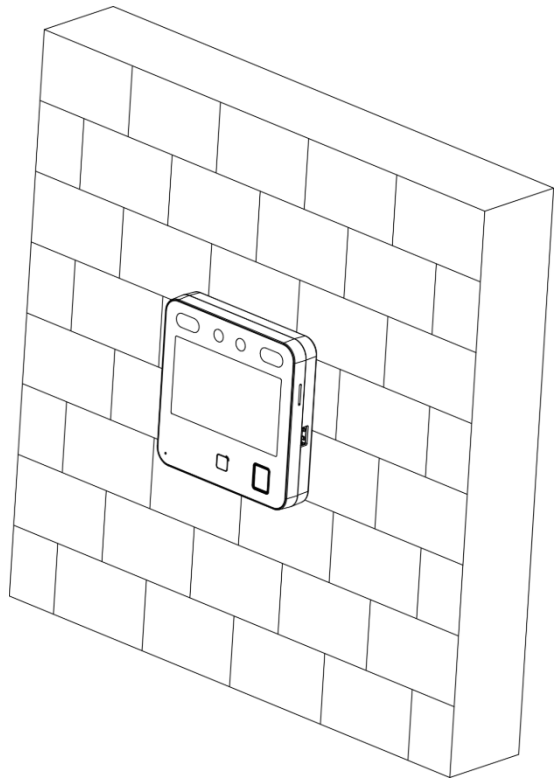


**Figure 3-3 Dispositif sécurisé**

## 3.3 Montage à la base

**Étapes**

1. Faites passer les câbles par le trou de câble du support et connectez les terminaux avec les câbles de périphériques. Placez le support près de la face arrière de l'appareil.

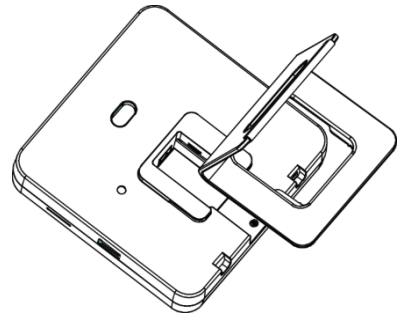


**Figure 3-4 Placer le support près de la face arrière de l'appareil**

2. Appuyez sur le support avec les deux mains et assurez-vous que la boucle du support s'adapte à face arrière de l'appareil. Fixez le support dans le sens de la flèche.

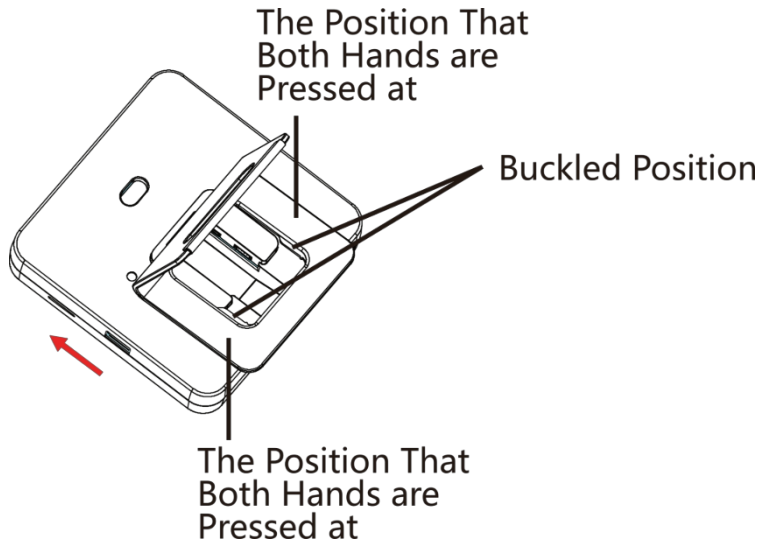



**Figure 3-5 Fixation du support**

**3.** Bouclez le support jusqu'à l'extrémité pour terminer l'installation.

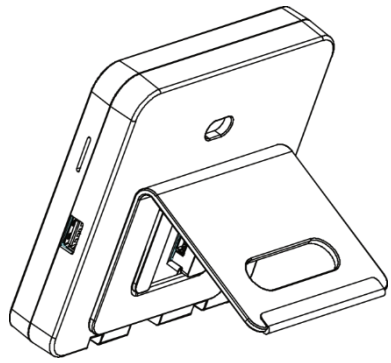


**Figure 3-6 Installation complète**

# Chapitre 4 Câblage

Vous pouvez connecter le terminal RS-485 au lecteur de cartes RS-485, connecter les terminaux NC/NO et COM à la serrure de la porte, connecter les terminaux SEN et GND au contact de la porte, le terminal BTN/GND au bouton de sortie et connecter le terminal Wiegand au contrôleur d'accès.

Si le terminal WIEGAND est connecté au contrôleur d'accès, le terminal de reconnaissance faciale peut transmettre les informations d'authentification au contrôleur d'accès et ce dernier peut décider d'ouvrir ou non la porte.

**Note**

- Si la taille du câble est de 18 AWG, vous devez utiliser une alimentation de 12 V. La distance entre lalimentation et l'appareil ne doit pas dépasser 20 m.
- Si la taille du câble est de 15 AWG, vous devez utiliser une alimentation de 12 V. La distance entre lalimentation et l'appareil ne doit pas dépasser 30 m.
- Si la taille du câble est de 12 AWG, vous devez utiliser une alimentation de 12 V. La distance entre lalimentation et l'appareil ne doit pas dépasser 40 m.
- Le lecteur de carte externe, la serrure de porte, le bouton de sortie et l'aimant de porte ont besoin d'une alimentation électrique individuelle.

## 4.1 Description du terminal

Les bornes contiennent l'entrée d'alimentation, RS-485, la sortie Wiegand et le

verrouillage de la porte. Les descriptions des terminaux sont les suivantes :

**Tableau 4-1 Descriptions des bornes**

| Groupe | Non. | Fonction | Couleur | Nom | Description |
|---|---|---|---|---|---|
| Groupe A | A1 | Entrée d'alimentation | Rouge | +12 V | Alimentation 12 VDC |
| | A2 | | Noir | GND | Sol |
| Groupe B | B1 | RS-485 | Jaune | 485+ | Câblage RS-485 |
| | B2 | | Bleu | 485- | |
| | B3 | | Noir | GND | Sol |
| Groupe C | C1 | Wiegand | Vert | W0 | Câblage Wiegand 0 |

| Groupe | Non. | Fonction | Couleur | Nom | Description |
|---|---|---|---|---|---|
| | C2 | | Blanc | W1 | Câblage Wiegand 1 |
| | C3 | | Noir | GND | Sol |
| Groupe D | D1 | Serrure de porte | Blanc/Pourpre | NC | Câblage de la serrure (NC) |
| | D2 | | Blanc/jaune | COM | Communs |
| | D3 | | Blanc/Rouge | NON | Câblage de la serrure (NO) |
| | D4 | | Jaune/vert | CAPTEUR | Contact de porte |
| | D5 | | Noir | GND | Sol |
| | D6 | | Jaune/Gris | BOUTON | Câblage de la porte de sortie |

## 4.2 Fil Dispositif normal

Vous pouvez connecter le terminal avec des périphériques normaux.

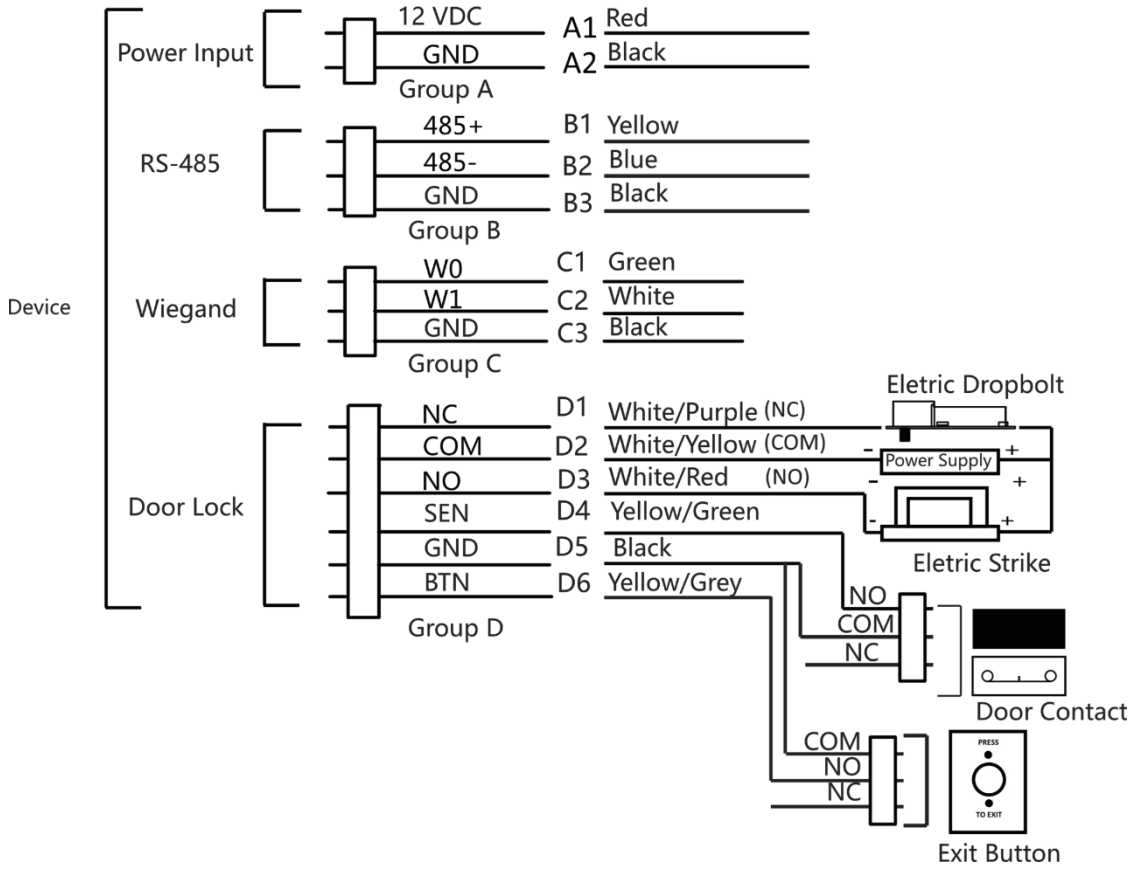



**Figure 4-1 Câblage de l'appareil**

**Note**

- En cas de connexion à un contrôleur d'accès, vous devez définir la direction Wiegand comme **Sortie** pour transmettre les informations d'authentification au contrôleur d'accès.
- Pour plus de détails sur les réglages de la direction Wiegand, voir ***Définir les paramètres Wiegand***.
- Ne pas brancher l'appareil directement sur l'alimentation électrique.

## 4.3 Unité de contrôle de porte sécurisée par fil

Vous pouvez connecter le terminal à l'unité de contrôle de la porte sécurisée. Le schéma de câblage est le suivant.

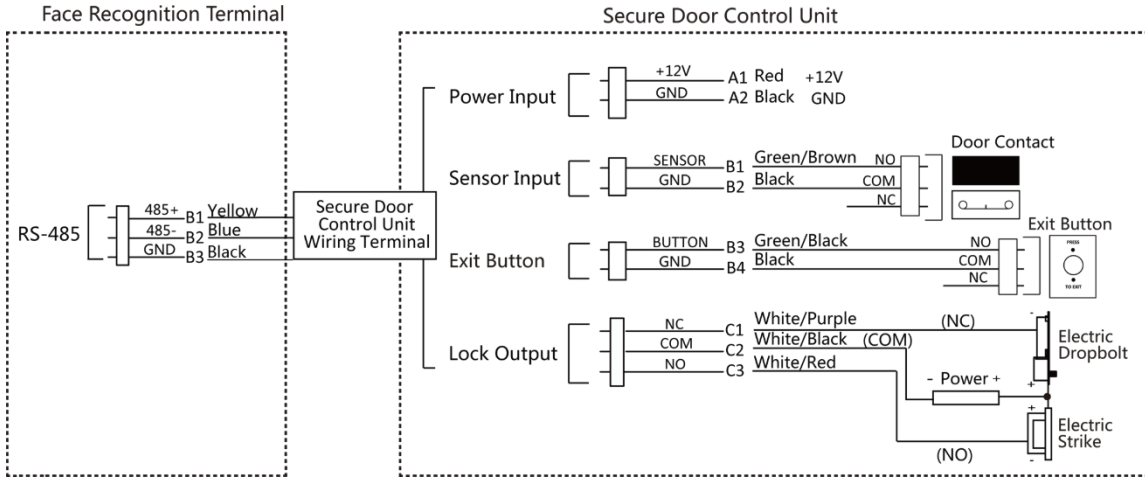



**Figure 4-2 Câblage de l'unité de contrôle des portes sécurisées**

**Note**

L'unité de contrôle des portes sécurisées doit être connectée à une alimentation électrique externe séparément. L'alimentation externe suggérée est de 12V, 0,5A.

## 4.4 Module d'incendie à fil

### 4.4.1 Schéma de câblage de la porte ouverte lors de la mise hors tension

Type de serrure : Verrouillage par anode, verrouillage magnétique et verrou électrique (NO) Type de sécurité : Porte ouverte lors de la mise hors tension

Scénario : installé dans l'accès aux véhicules d'incendie

#### Type 1

**Note**

Le système d'incendie contrôle l'alimentation électrique du système de contrôle d'accès.

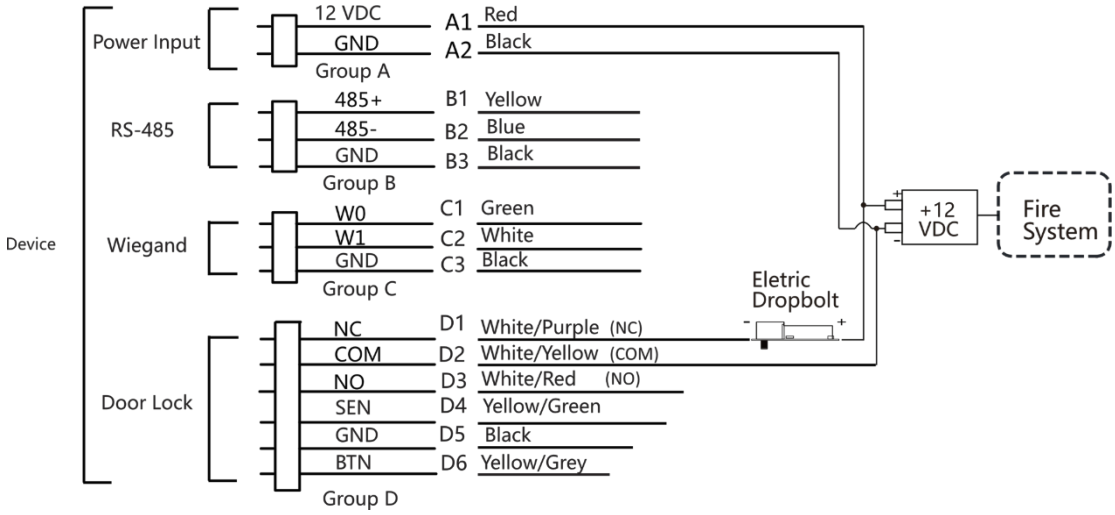



**Figure 4-3 Dispositif de câblage**

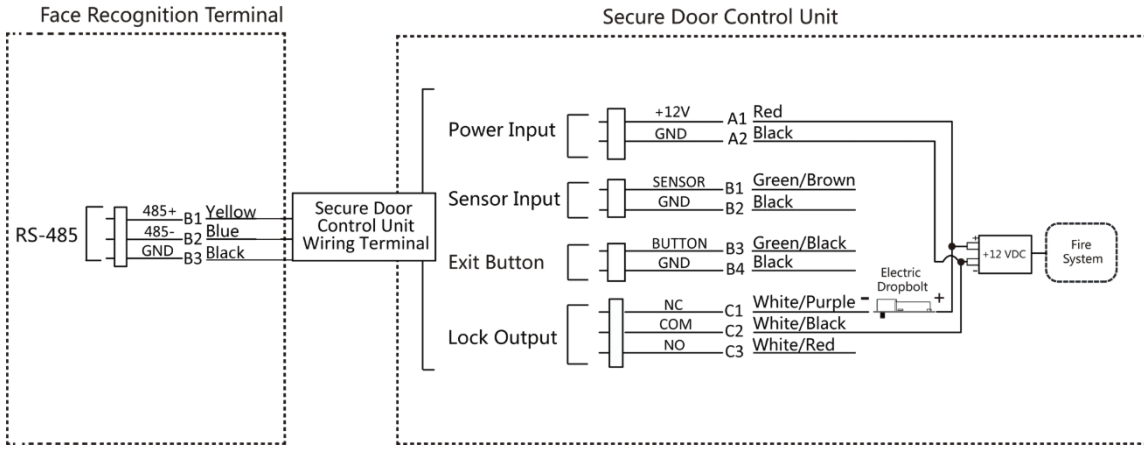



**Figure 4-4 Sécurisation du câblage de l'unité de contrôle des portes**

## Type 2

**Note**

Le système anti-incendie (NO et COM, normalement ouvert lors de la mise hors tension) est connecté en série à la serrure et à l'alimentation électrique. Lorsqu'une alarme incendie est déclenchée, la porte reste ouverte. En temps normal, NO et COM sont fermés.

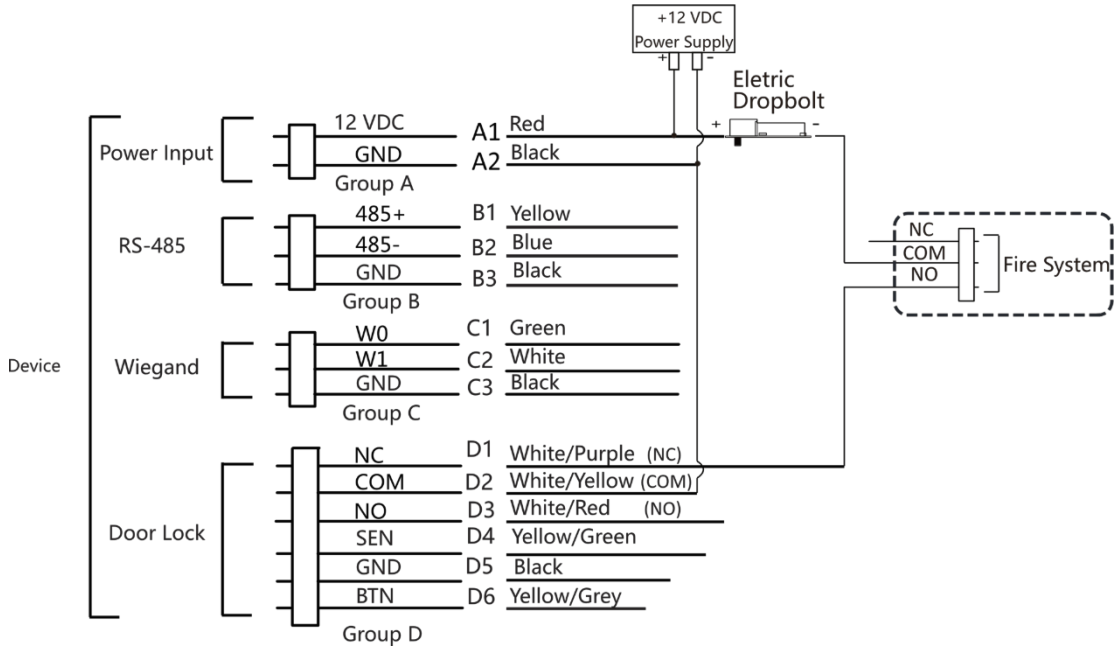



**Figure 4-5 Dispositif de câblage**

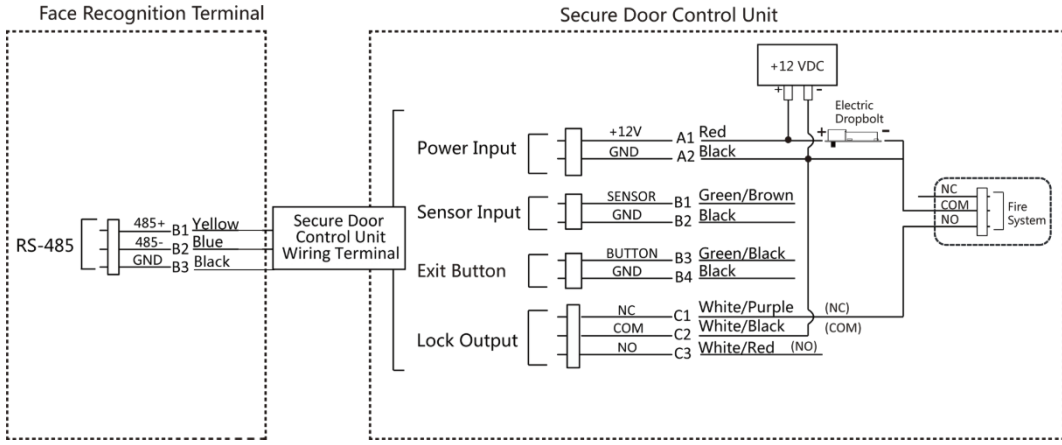



**Figure 4-6 Câblage de l'unité de commande de porte sécurisée**

## 4.4.2 Schéma de câblage de la porte verrouillée lors de la mise hors tension

Type de serrure : Serrure cathodique, serrure électrique et pêne électrique

(NC) Type de sécurité : Verrouillage de la porte lors de la mise hors tension

Scénario : Installation dans l'entrée/sortie avec liaison incendie

**Note**

- Le bloc d'alimentation ininterprétable (UPS) est nécessaire.
- Le système anti-incendie (NC et COM, normalement fermé lors de la mise hors tension) est connecté en série à la serrure et à l'alimentation électrique. Lorsqu'une alarme incendie est déclenchée, la porte reste ouverte. En temps normal, NC et COM sont ouverts.

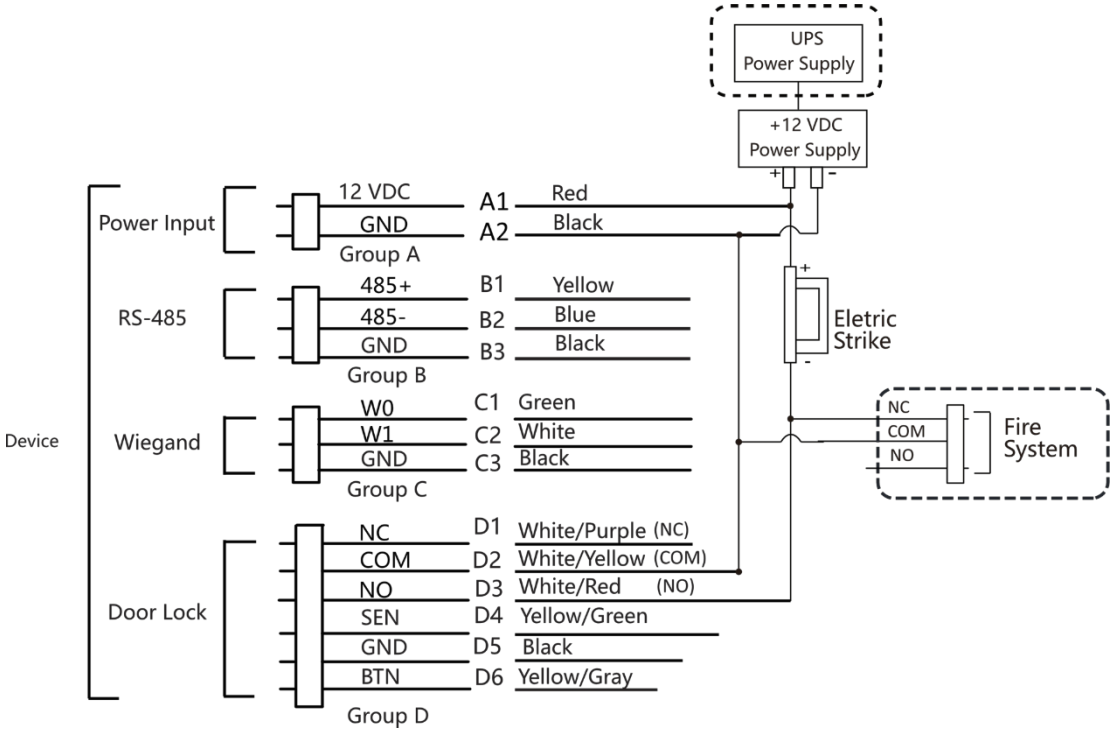



**Figure 4-7 Câblage de l'appareil**

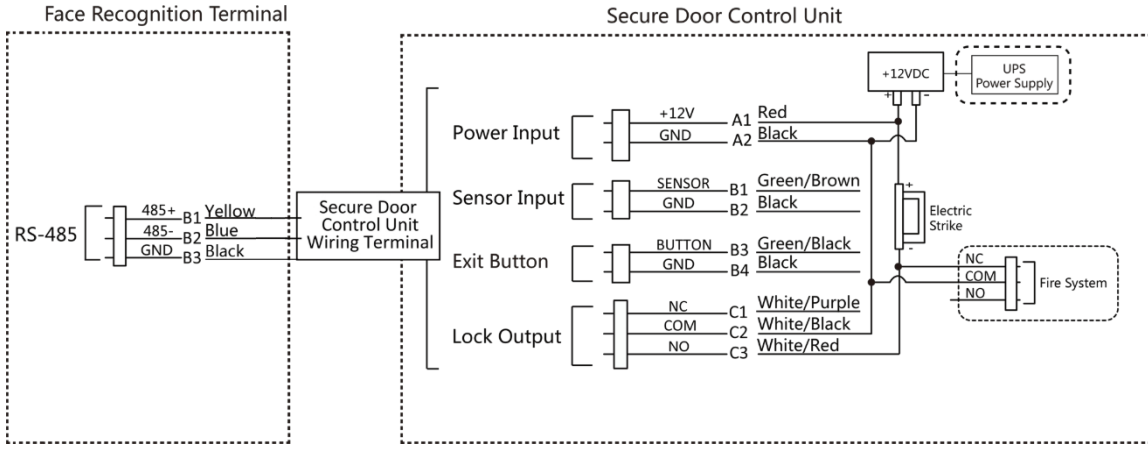



**Figure 4-8 Schéma de câblage**

# Chapitre 5 Activation

Vous devez activer l'appareil avant la première connexion. Après la mise sous tension de l'appareil le système passe à la page d'activation de l'appareil.

L'activation via l'appareil, l'outil SADP et le logiciel client sont pris en charge. Les valeurs par défaut de l'appareil sont les suivantes :

- L'adresse IP par défaut : 192.0.0.64
- Numéro de port par défaut : 8000
- Le nom d'utilisateur par défaut : admin

## 5.1 Activation par l'intermédiaire d'un dispositif

Si l'appareil n'est pas activé, vous pouvez l'activer après l'avoir mis  tension.

Sur la page Activer l'appareil, créez un mot de et confirmez-le. Appuyez sur **Activer** et lappareil sera activé.

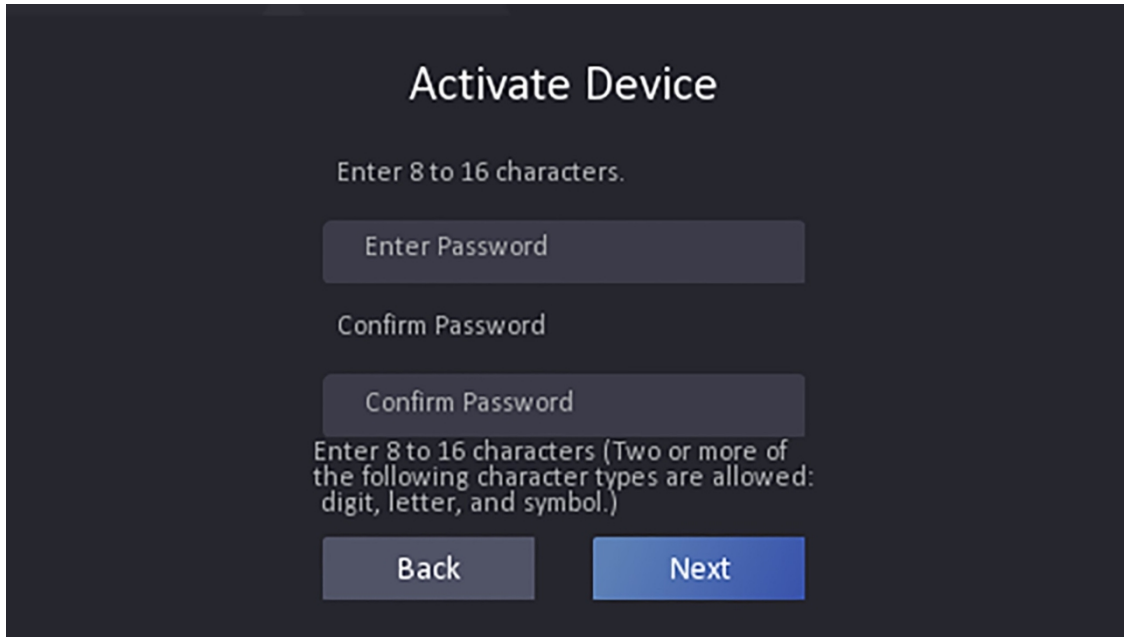



**Figure 5-1 Page d'activation**

**Attention**

La force du mot de passe de l'appareil peut être automatiquement vérifiée. Nous vous recommandons vivement de modifier le mot de passe de votre choix (en utilisant un minimum de 8 caractères, dont au moins trois des catégories suivantes : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux).

caractères) afin d'accroître la sécurité de votre produit. Nous vous recommandons de modifier régulièrement votre mot de passe, en particulier dans le cas d'un système de haute sécurité. Un changement de mot de passe mensuel ou hebdomadaire permet de mieux protéger votre produit.
La configuration correcte de tous les mots de passe et autres paramètres de sécurité relève de la responsabilité de 'installateur et/ou de l'utilisateur final.

**Note**
Les caractères contenant admin et nimda ne peuvent pas être définis comme mot de passe d'activation.

- Après l'activation, vous devez sélectionner une langue en fonction de vos besoins réels.
- Après l'activation, vous devez sélectionner un mode d'application. Pour plus de détails, voir ***Définir le mode d'application***.
- Après l'activation, vous devez définir le réseau. Pour plus de détails, voir ***Définir les paramètres du réseau***.
- Après l'activation, vous pouvez ajouter l'appareil à la plate-forme. Pour plus de détails, voir ***Accès à la plateforme***.
- Après l'activation, si vous avez besoin de définir la confidentialité, vous devez vérifier l'élément. Pour plus d'informations, reportez-vous à la section ***Paramètres de confidentialité***.
- Après l'activation, si vous devez ajouter un administrateur pour gérer les paramètres de l'appareil, vous devez définir l'administrateur. Pour plus de détails, voir ***Ajouter un administrateur***.

## 5.2 Activation via le navigateur web

Vous pouvez activer l'appareil via le navigateur web.

**Étapes**

1. Saisissez l'adresse IP par défaut de l'appareil (192.0.0.64) dans la barre d'adresse du navigateur Web et appuyez sur
   **Entrer**.

   **Note**
   Assurez-vous que l'adresse IP de l'appareil et celle de l'ordinateur se trouvent dans le même segment IP.
2. Créez un nouveau mot de passe (mot de passe administrateur) et confirmez le mot de passe.

   **Attention**
   Nous vous recommandons vivement de créer un mot de passe fort de votre choix (utilisant un minimum de 8 caractères, comprenant des lettres majuscules, des lettres minuscules, des chiffres et des caractères spéciaux) afin d'accroître la sécurité de votre produit. Nous vous recommandons également de réinitialiser votre mot de passe régulièrement, en particulier dans le cas d'un système de haute sécurité, la réinitialisation du mot de passe une fois par mois ou une fois par semaine permet de mieux protéger votre produit.

   **Note**
   Les caractères contenant admin et nimda ne peuvent pas être définis comme mot de passe d'activation.
3. Cliquez sur **Activer**.
4. Modifier l'adresse IP de l'appareil. Vous pouvez modifier l'adresse IP via l'outil SADP, l'appareil et logiciel client.

## 5.3 Activer via SADP

SADP est un outil permettant de détecter, d'activer et de modifier l'adresse IP d'un appareil sur le réseau local.

**Avant de commencer**

- Procurez-vous le logiciel SADP sur le disque fourni ou sur le site officiel ***http://www.hikvision.com/en/*** , et installez le SADP en suivant les instructions.
- L'appareil et le PC qui exécute l'outil SADP doivent se trouver dans le même sous-réseau.

Les étapes suivantes montrent comment activer un appareil et modifier son adresse IP. Pour l'activation par lots et la modification des adresses IP, se référer au *manuel d'utilisation de SADP* pour plus de détails.

**Étapes**

1. Lancez le logiciel SADP et recherchez les dispositifs en ligne.
2. Recherchez et sélectionnez votre appareil dans la liste des appareils en ligne.
3. Saisir le nouveau mot de passe (mot de passe administrateur) et confirmer le mot de passe.

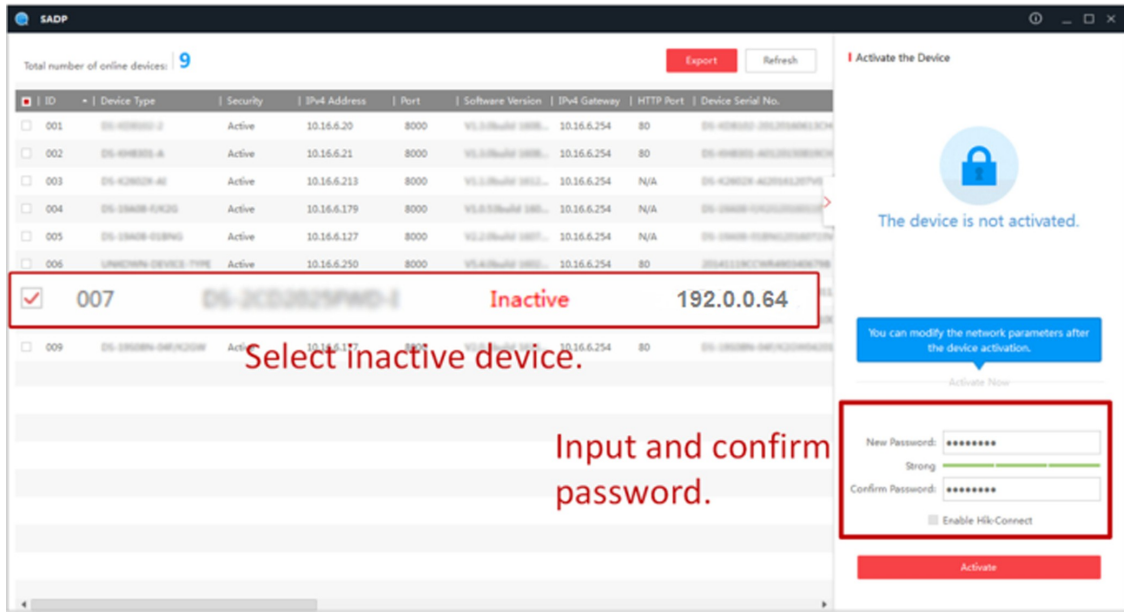
**Attention**

Nous vous recommandons vivement de créer un mot de passe fort de votre choix (avec un minimum de 8 caractères, comprenant des lettres majuscules, des lettres minuscules, des chiffres et des caractères spéciaux) afin d'accroître la sécurité de votre produit. Nous vous recommandons également de réinitialiser votre mot de passe régulièrement, en particulier dans le cas d'un système de haute sécurité, la réinitialisation du mot de passe une fois par mois ou une fois par semaine permet de mieux protéger votre produit.

**Note**

Les caractères contenant admin et nimda ne peuvent pas être définis comme mot de passe d'activation.

4. Cliquez sur **Activer** pour lancer l'activation.




L'état de l'appareil devient **actif** après une activation réussie.

5. Modifier l'adresse IP de l'appareil.
   1) Sélectionnez l'appareil.
   2) Modifiez l'adresse IP de l'appareil pour qu'elle corresponde au même sous-réseau que votre ordinateur, soit en modifiant l'adresse IP manuellement, soit en cochant la case **Activer DHCP**.
   3) Saisissez le mot de passe administrateur et cliquez sur **Modifier** pour activer la modification de votre adresse IP.

## 5.4 Activer l'appareil via le logiciel client iVMS-4200

Pour certains appareils, vous devez créer un mot de passe pour les activer avant qu'ils puissent être ajoutés au logiciel iVMS-4200 et fonctionner correctement.

**Étapes**

**Note**
Cette fonction doit être prise en charge par l'appareil.

1. Accédez à la page Gestion des appareils.
2. Cliquez sur à droite de **Device Management** et sélectionnez **Device**.
3. Cliquez sur **Appareil en ligne** pour afficher la zone des appareils en ligne. Les appareils en ligne recherchés sont affichés dans la liste.
4. Vérifiez l'état de l'appareil (indiqué dans la colonne **Niveau de sécurité**) et sélectionnez un appareil inactif.
5. Cliquez sur **Activer** pour ouvrir la boîte de dialogue d'activation.
6. Créez un mot de passe dans le champ du mot de passe et confirmez le mot de passe.

**Attention**

La force du mot de passe de l'appareil peut être automatiquement vérifiée. Nous vous recommandons vivement de modifier le mot de passe de votre choix (en utilisant un minimum de 8 caractères, dont au moins trois des catégories suivantes : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) afin d'accroître la sécurité de votre produit. Nous vous recommandons également de modifier votre mot de passe régulièrement, en particulier dans le cas d'un système de haute sécurité, un changement de mot de passe mensuel ou hebdomadaire permet de mieux protéger votre produit.
La configuration correcte de tous les mots de passe et autres paramètres de sécurité relève de la responsabilité de 'installateur et/ou de l'utilisateur final.

**Note**

Les caractères contenant admin et nimda ne peuvent pas être définis comme mot de passe d'activation.

**7.** Cliquez sur **OK** pour activer l'appareil.

# Chapitre 6 Fonctionnement rapide

## 6.1 Sélectionner la langue

Vous pouvez sélectionner une langue pour le système de l'appareil.

Après l'activation de l'appareil, vous pouvez sélectionner une langue pour le système de l'appareil.

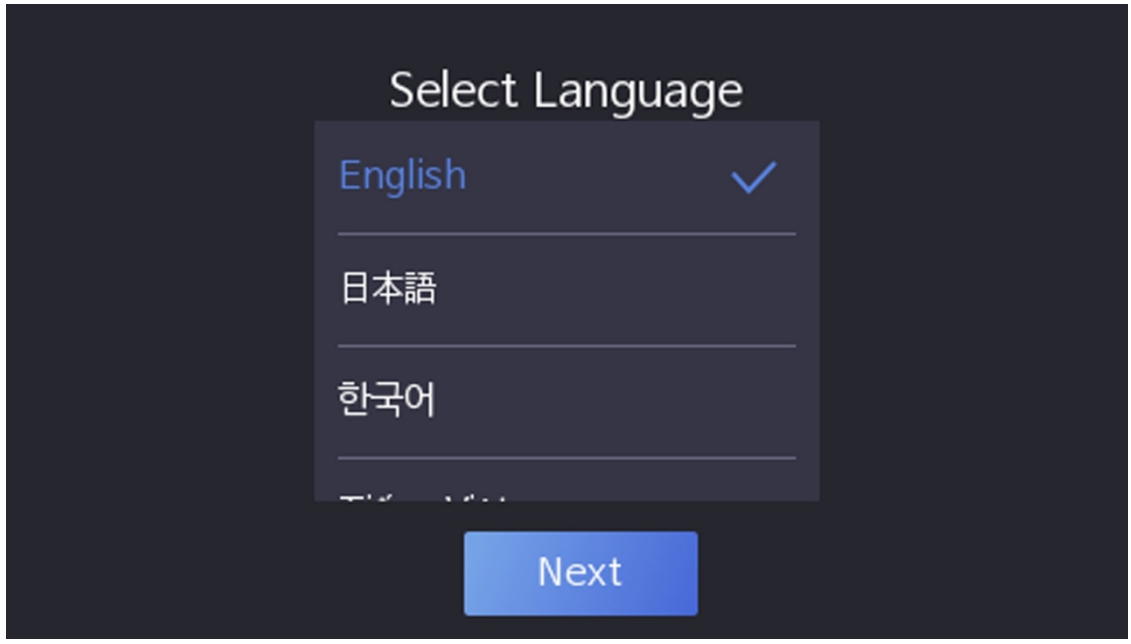



**Figure 6-1 Sélection de la langue du système**

Par défaut, la langue du système est l'anglais.

**Note**

Après avoir changé la langue du système, l'appareil redémarre automatiquement.

## 6.2 Définir le mode d'application

Après avoir activé l'appareil, vous devez sélectionner un mode d'application pour une meilleure utilisation de l'appareil.

**Étapes**

**1.** Sur la page d'accueil, sélectionnez **Intérieur** ou **Autres** dans la liste déroulante.

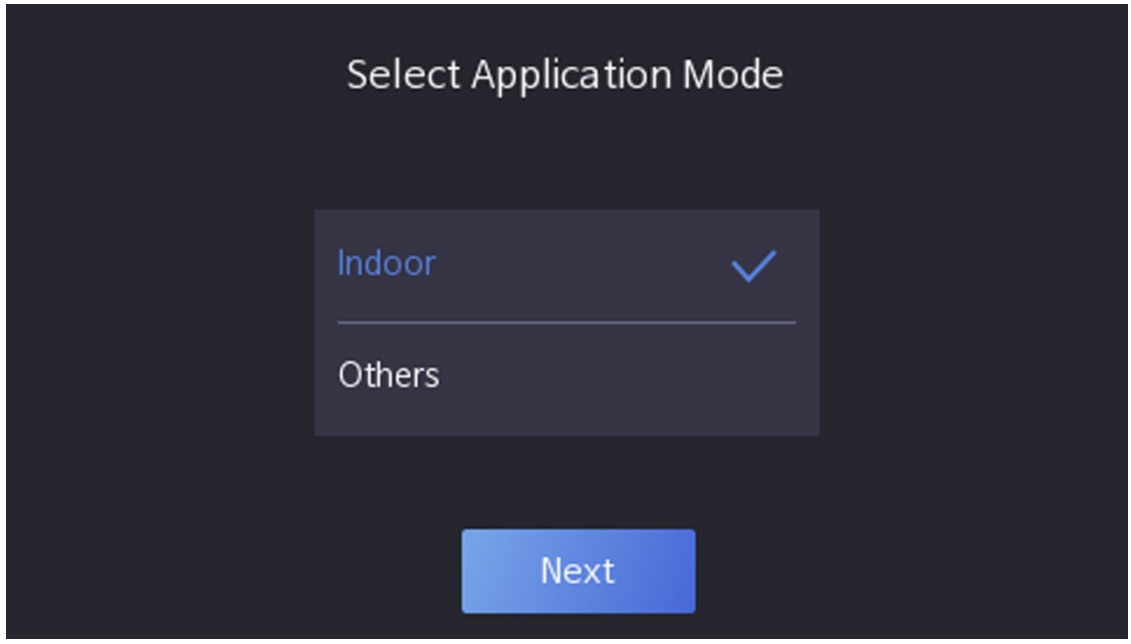



**Figure 6-2 Page d'accueil**

**2.** Appuyez sur **OK** pour enregistrer.

**Note**

- Vous pouvez également modifier les paramètres dans les *Paramètres du système*.
- Si vous installez l'appareil à l'intérieur, près d'une fenêtre, ou si la fonction de reconnaissance faciale ne fonctionne pas correctement, sélectionnez **Autres**.
- Si vous ne configurez pas le mode d'application et que vous appuyez sur **Suivant**, le système sélectionnera **Intérieur** par défaut.
- Si vous activez le dispositif à distance à l'aide d'autres outils, le système par défaut **Indoor** comme mode d'application.

## 6.3 Régler les paramètres du réseau

Après l'activation et la sélection du mode d'application, vous pouvez définir le réseau de l'appareil.

**Étapes**

**1.** Lorsque vous accédez à la page Sélectionner un réseau, appuyez sur **Réseau câblé** ou **Wi-Fi** en fonction de vos besoins.

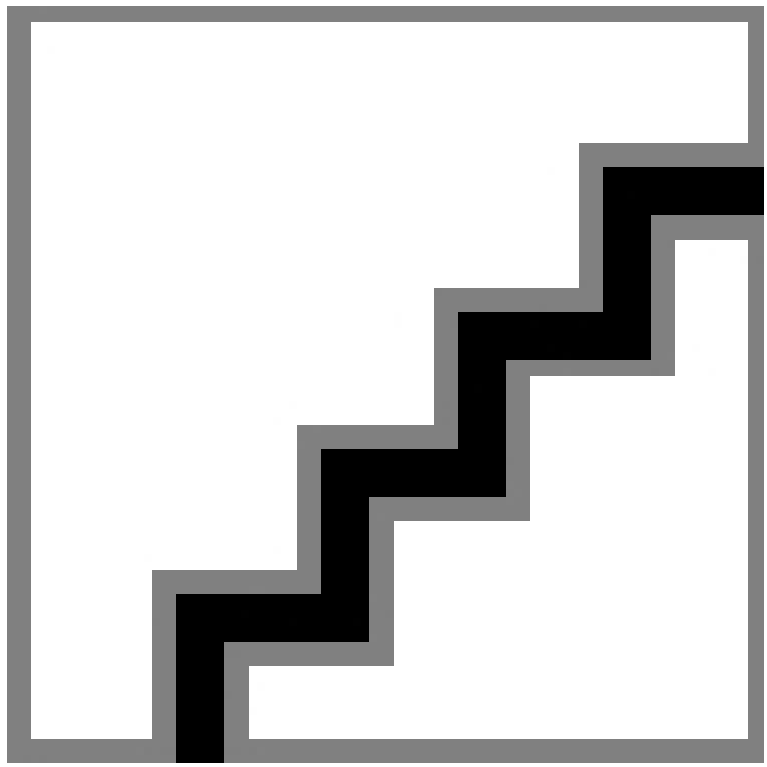


**Figure 6-3 Sélection du réseau**

**Note**

Déconnectez le réseau câblé avant de connecter un réseau Wi-Fi.

**2.** Appuyez sur **Suivant**. **Réseau câblé**

**Note**

Assurez-vous que l'appareil est connecté à un réseau.

Si **la fonction DHCP** est activée, le système attribue automatiquement l'adresse IP et d'autres paramètres. Si vous désactivez le **DHCP**, vous devez définir l'adresse IP, le masque de sous-réseau et la passerelle.

**Wi-Fi**

Sélectionnez un et entrez son mot de passe pour vous connecter.

Ou appuyez sur **Ajouter un Wi-Fi** et entrez le nom du Wi-Fi et le mot de passe pour vous connecter.

**3. Facultatif :** Appuyez sur **Sauter** pour ignorer les paramètres du réseau.

## 6.4 Accès à la plate-forme

Activez la fonction et le dispositif peut communiquer via Hik-Connect. Vous pouvez ajouter le dispositif au client modulaire Hik-Connect, etc.

**Étapes**

1. Activez l'**accès à Hik-Connect** et définissez l'IP du serveur et le code de vérification.

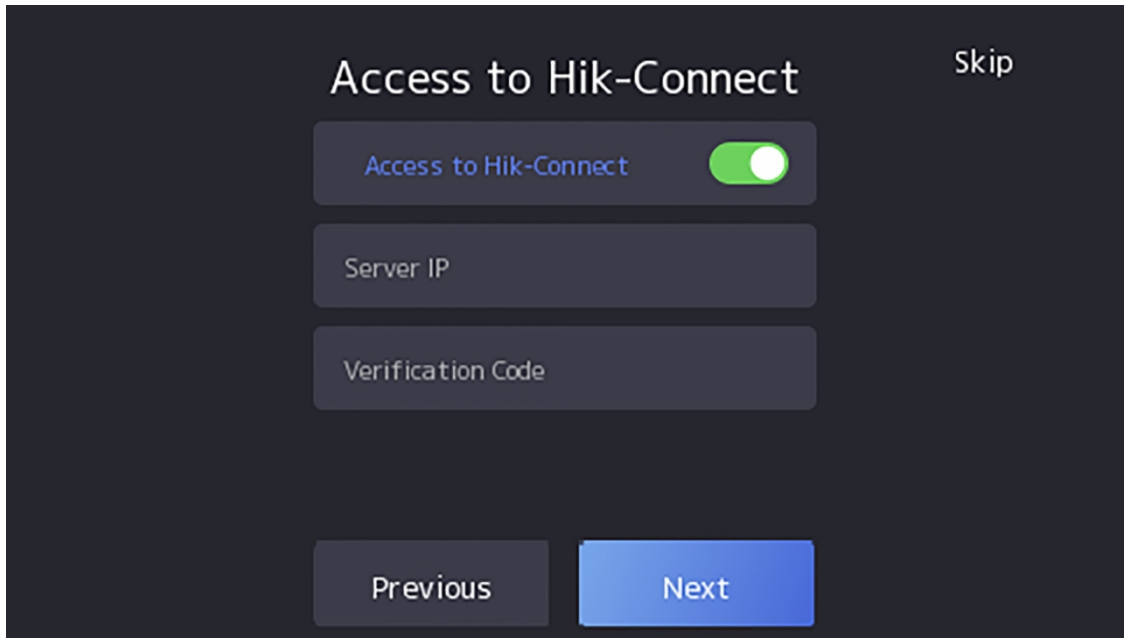



**Figure 6-4 Accès à Hik-Connect**

2. Appuyez sur **Suivant**.

**Note**

Si vous appuyez sur **Précédent** pour revenir à la page de configuration Wi-Fi, vous devez appuyer sur le Wi-Fi connecté ou connecter un autre Wi-Fi pour accéder à nouveau à la page de la plateforme.

## 6.5 Paramètres de confidentialité

Après l'activation, la sélection du mode d'application et la sélection du réseau, vous devez définir les paramètres de confidentialité, y compris le téléchargement et le stockage des photos.

Sélectionnez les paramètres en fonction de vos besoins réels.

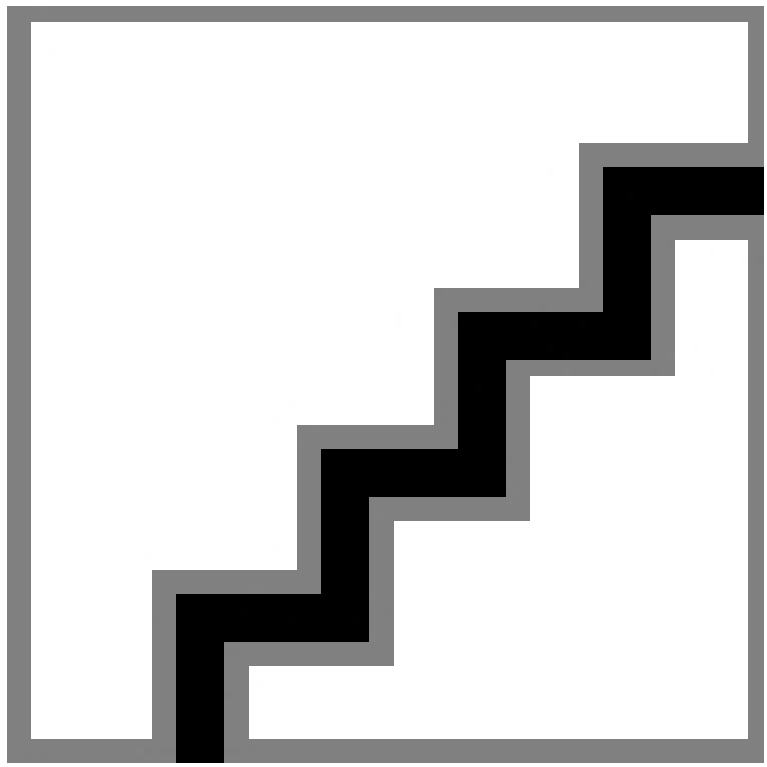


**Figure 6-5 Confidentialité**

**Upload Captured Pic. (Télécharger l'image capturée lors de l'authentification)**

Télécharger automatiquement les photos prises lors de l'authentification sur la plateforme.

**Save Captured Pic. (Enregistrer l'image capturée lors de l'authentification)**

Si vous activez cette fonction, vous pouvez enregistrer l'image lors de l'authentification à l'appareil.

**Sauvegarder l'image enregistrée (Sauvegarder l'image enregistrée)**

L'image du visage enregistrée sera sauvegardée dans le système si vous activez la fonction.

**Upload Pic. Après la capture liée (Télécharger une image après la capture liée)**

Téléchargez automatiquement sur la plateforme les images capturées par l'appareil photo relié.

**Enregistrer Pic. après la capture liée (Enregistrer les images après la capture liée)**

Si vous activez cette fonction, vous pouvez enregistrer l'image capturée par l'appareil photo lié sur l'appareil.

Appuyez sur **Suivant** pour terminer les réglages.

## 6.6 Définir l'administrateur

Après l'activation de l'appareil, vous pouvez ajouter un administrateur pour gérer les paramètres de l'appareil.

**Avant de commencer**

Activez l'appareil et sélectionnez un mode d'application.

**Étapes**

1. **Facultatif :** Appuyez sur **Sauter** pour ignorer l'ajout d'un administrateur si nécessaire.
2. Saisissez le nom de l'administrateur (facultatif) et appuyez sur **Suivant**.

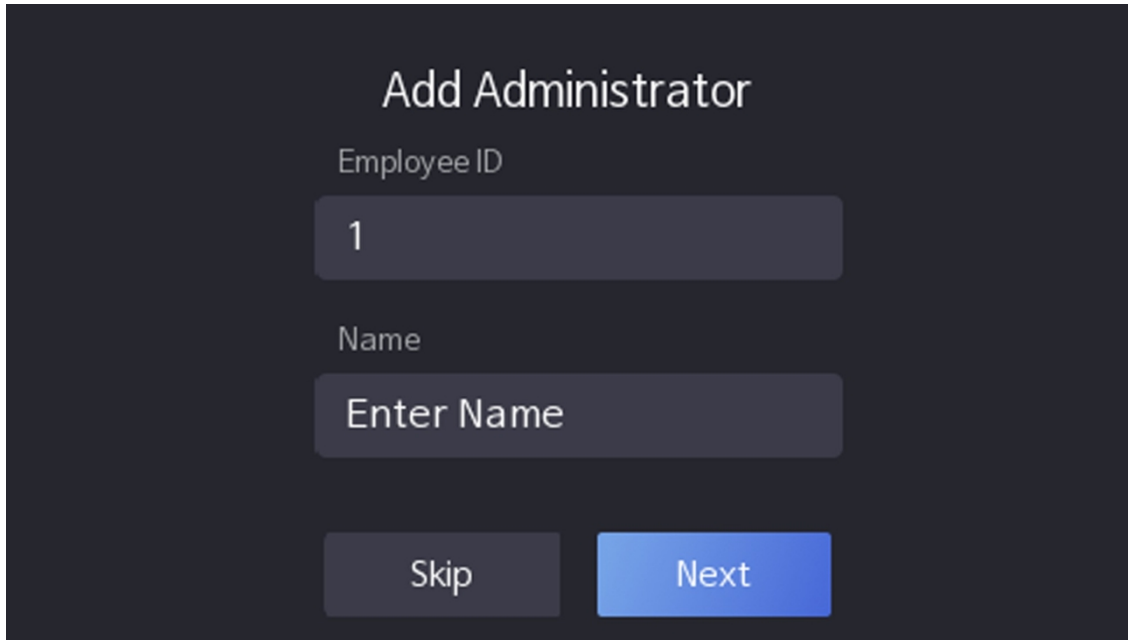



**Figure 6-6 Page d'ajout d'un administrateur**

3. Sélectionnez un titre à ajouter.

**Note**

Il convient d'ajouter jusqu'à un seul titre de compétence.

- : Faites face à l'appareil photo. Assurez-vous que le visage se trouve dans la zone de reconnaissance des visages. Cliquez sur pour capturer et sur pour confirmer.
- : Appuyez sur votre doigt en suivant les instructions sur l'écran de l'appareil. Cliquez sur pour confirmer.
- : Saisissez le numéro de la carte ou présentez la carte dans la zone de présentation des cartes. Cliquez sur **OK**.

4. Cliquez sur **OK**.

Vous accédez à la page d'authentification.

**Icône d'état Description**

/

L'appareil est armé/non armé.

/

Hik-Connect est activé/désactivé.

/ /

Le réseau câblé de l'appareil est connecté/pas connecté/échec de la connexion.

/ /

Le Wi-Fi de l'appareil est activé et connecté/non connecté/activé mais non connecté.

**Description des touches de raccourci**

**Note**

Vous pouvez configurer les touches de raccourci affichées à l'écran. Pour plus d'informations, voir ***Sélections de base***.

- Saisissez le numéro de pièce de l'appareil et appuyez sur **OK** pour appeler.
- Tapez sur pour appeler le centre.

**Note**

Le dispositif doit être ajouté au centre, sinon l'opération d'appel échouera.

Saisir le code PIN pour s'authentifier.

# Chapitre 7 Fonctionnement de base

## 7.1 Connexion

Se connecter à l'appareil pour définir les paramètres de base de l'appareil.

### 7.1.1 Connexion par l'administrateur

Si vous avez ajouté un administrateur pour l'appareil, seul l'administrateur peut se connecter à l'appareil pour le faire fonctionner.

**Étapes**

1. Appuyez longuement sur la page initiale pendant 3 secondes et faites glisser vers la gauche/droite en suivant le geste pour accéder à la page de connexion de l'administrateur.


**Figure 7-1 Connexion admin.**

2. Authentifier le visage, l'empreinte digitale ou la carte de l'administrateur pour accéder à la page d'accueil.

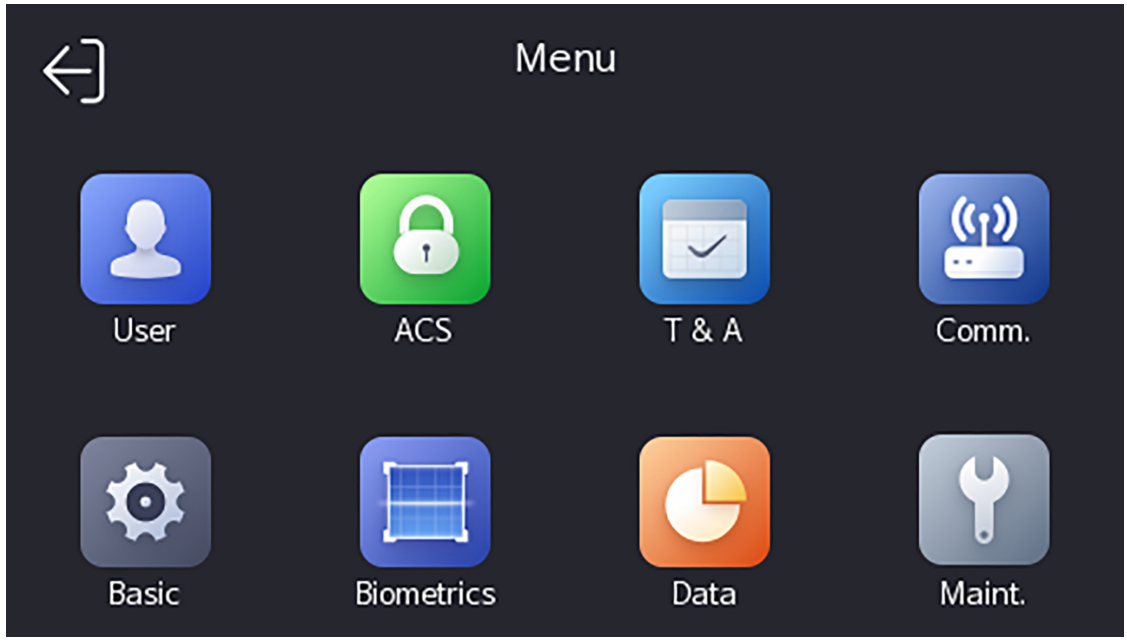



**Figure 7-2 Page d'accueil**

**Note**

L'appareil sera verrouillé pendant 30 minutes après 5 tentatives infructueuses de saisie d'empreinte digitale ou de carte.

3. **Optionnel :** Appuyez sur et vous pouvez saisir le mot de passe d'activation de l'appareil pour vous connecter.
4. **Facultatif :** Tapez sur pour quitter la page de connexion de l'administrateur.

### 7.1.2 Connexion par mot de passe d'activation

Vous devez vous connecter au système avant d'effectuer d'autres opérations sur l'appareil. Si vous n'avez pas configuré d'administrateur, vous devez suivre les instructions ci-dessous pour vous connecter.

**Étapes**

1. Appuyez longuement sur la page initiale pendant 3 secondes et faites glisser vers la gauche/droite en suivant le geste pour accéder à la page de saisie du mot de passe.
2. Saisissez le mot de passe.
   - Si vous avez ajouté un administrateur pour l'appareil, appuyez sur et saisissez le mot de passe.
   - Si vous n'avez pas ajouté d'administrateur pour l'appareil, saisissez le mot de passe.
3. Appuyez sur **OK** pour accéder à la page d'accueil.

**Note**

L'appareil sera verrouillé pendant 30 minutes après 5 tentatives infructueuses de saisie du mot de passe.

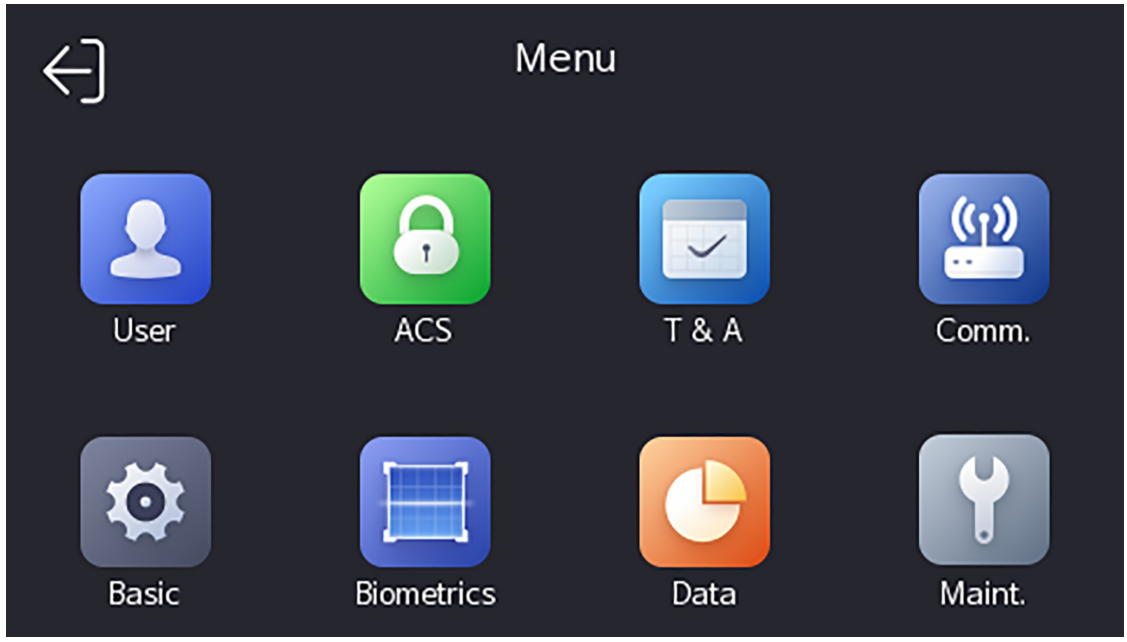



**Figure 7-3 Page d'accueil**

### 7.1.3 Mot de passe oublié

Si vous oubliez le mot de passe lors de l'authentification, vous pouvez le réinitialiser en important la clé.

**Étapes**

1. Appuyez longuement sur la page initiale pendant 3 secondes et glissez vers la gauche/droite en suivant le geste et connectez-vous à la page.
2. Appuyez sur dans la page d'authentification de l'administrateur qui s'affiche.
3. Brancher la clé USB dans l'interface USB.

**Note**

- Les formats de clés USB pris en charge sont FAT32 et exfat.
- L'appareil prend en charge les clés USB de 1 G à 32 G (y compris 1 G et 32 G). Assurez-vous que l'espace libre de la clé USB est supérieur à 512 M.

4. Appuyez sur **Exporter le fichier**, puis contactez le technicien pour obtenir la clé et entrez la clé dans le fichier d'exportation.
5. Appuyez sur **Importer un fichier** pour importer le fichier contenant la clé sur l'appareil.
6. Suivez les instructions pour réinitialiser le mot de passe.

## 7.2 Paramètres de communication

Vous pouvez définir le réseau câblé, le paramètre Wi-Fi, les paramètres RS-485, les paramètres Wiegand, l'ISUP et l'accès à Hik-Connect sur la page des paramètres de communication.

### 7.2.1 Paramètres du réseau câblé

Vous pouvez définir les paramètres du réseau câblé de l'appareil, notamment l'adresse IP, le masque de sous-réseau, passerelle et les paramètres DNS.

**Étapes**

1. Appuyez sur **Comm.** (Paramètres de communication) sur la page d'accueil pour accéder à la page Paramètres de communication.
2. Sur la page Paramètres de communication, appuyez sur **Réseau câblé**.

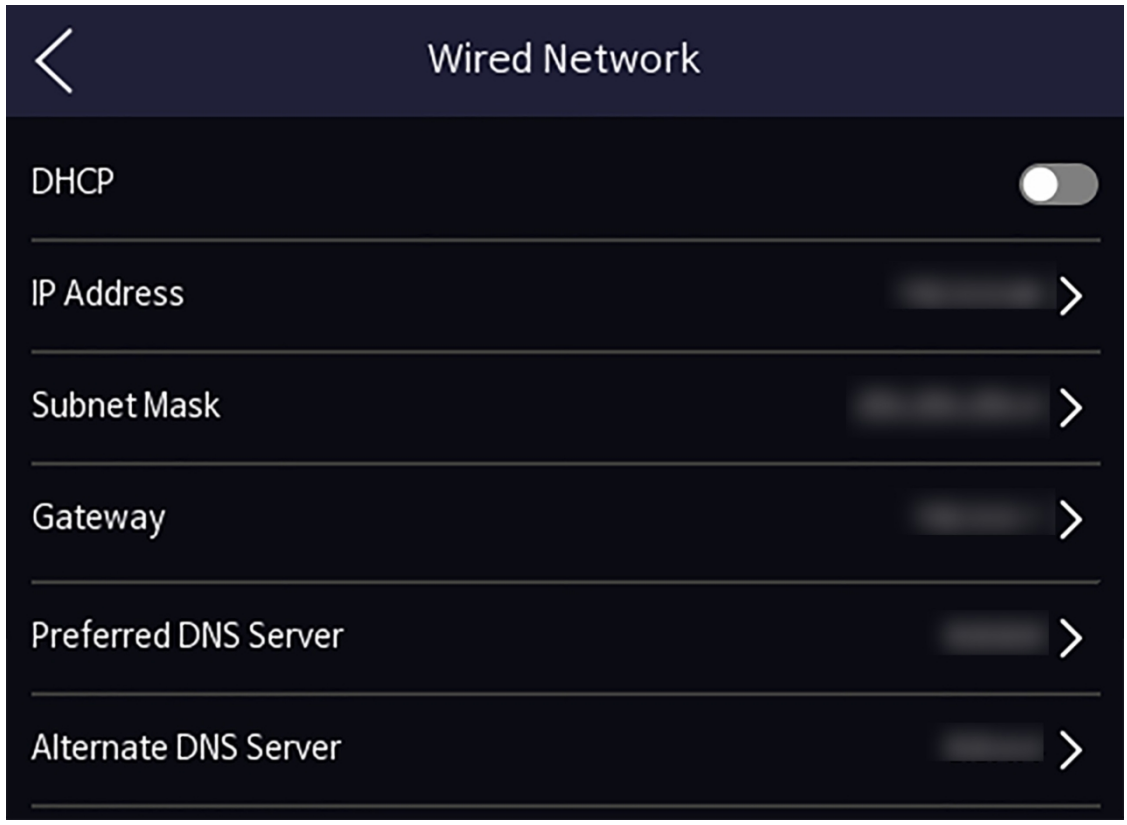



**Figure 7-4 Paramètres du réseau câblé**

3. Définir l'adresse IP, le masque de sous-réseau et la passerelle.
   - Activer **DHCP**, le système attribue automatiquement l'adresse IP, le masque de sous-réseau et la passerelle.
   - Désactivez le **DHCP** et définissez manuellement l'adresse IP, le masque de sous-réseau et la passerelle.

   **Note**

   L'adresse IP de l'appareil et l'adresse IP de l'ordinateur doivent se trouver dans le même segment IP.
4. Définissez les paramètres DNS. Vous pouvez activer l'**obtention automatique de DNS**, définir le serveur DNS préféré et serveur DNS alternatif.

### 7.2.2 Définir les paramètres Wi-Fi

Vous pouvez activer la fonction Wi-Fi et définir les paramètres liés au Wi-Fi.

**Étapes**

**Note**

La fonction doit être prise en charge par l'appareil.

1. Appuyez sur **Comm.** (Paramètres de communication) sur la page d'accueil pour accéder à la page Paramètres de communication.
2. Sur la page Paramètres de communication, appuyez sur .

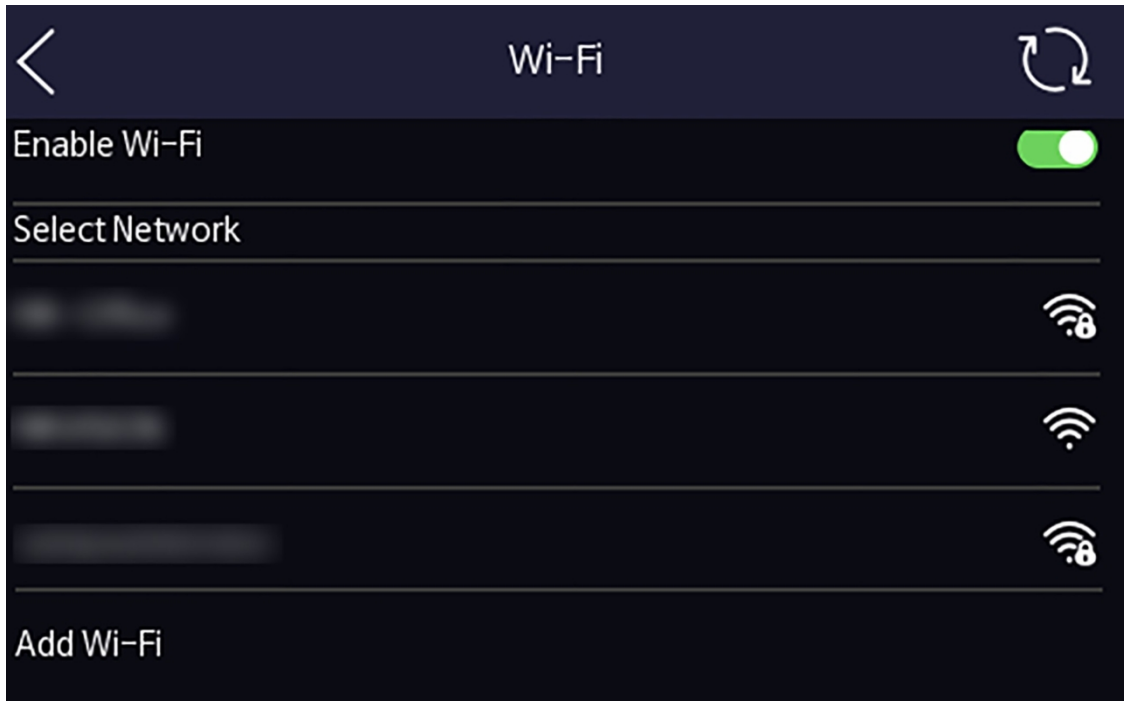



**Figure 7-5 Paramètres Wi-Fi**

3. Activer la fonction Wi-Fi.
4. Configurer les paramètres Wi-Fi.
   - Sélectionnez un Wi-Fi dans la liste et entrez le mot de passe du Wi-Fi. Appuyez sur **OK**.
   - Si le Wi-Fi cible ne figure pas dans la liste, appuyez sur **Ajouter un Wi-Fi**. Saisissez le nom et le mot de passe du Wi-Fi. Puis appuyez sur **OK**.

   **Note**

   Seuls les chiffres, les lettres et les caractères spéciaux sont autorisés dans le mot de passe.
5. Régler les paramètres du Wi-Fi.

- Par défaut, le protocole DHCP est activé. Le système attribue automatiquement l'adresse IP, le masque de sous-réseau et la passerelle.
- Si vous désactivez le DHCP, vous devez saisir manuellement l'adresse IP, le masque de sous-réseau et la passerelle.

6. Appuyez sur **OK** pour enregistrer les paramètres et revenir à l'onglet Wi-Fi.
7. Tapez sur ✓ pour enregistrer les paramètres du réseau.

### 7.2.3 Réglage des paramètres RS-485

Le terminal de reconnaissance faciale peut connecter un contrôleur d'accès externe, une unité de contrôle de porte sécurisée ou un lecteur de carte via le terminal RS-485.

**Étapes**

1. Appuyez sur **Comm.** (Paramètres de communication) sur la page d'accueil pour accéder à la page Paramètres de communication.
2. Sur la page Paramètres de communication, appuyez sur **RS-485** pour accéder à l'onglet RS-485.

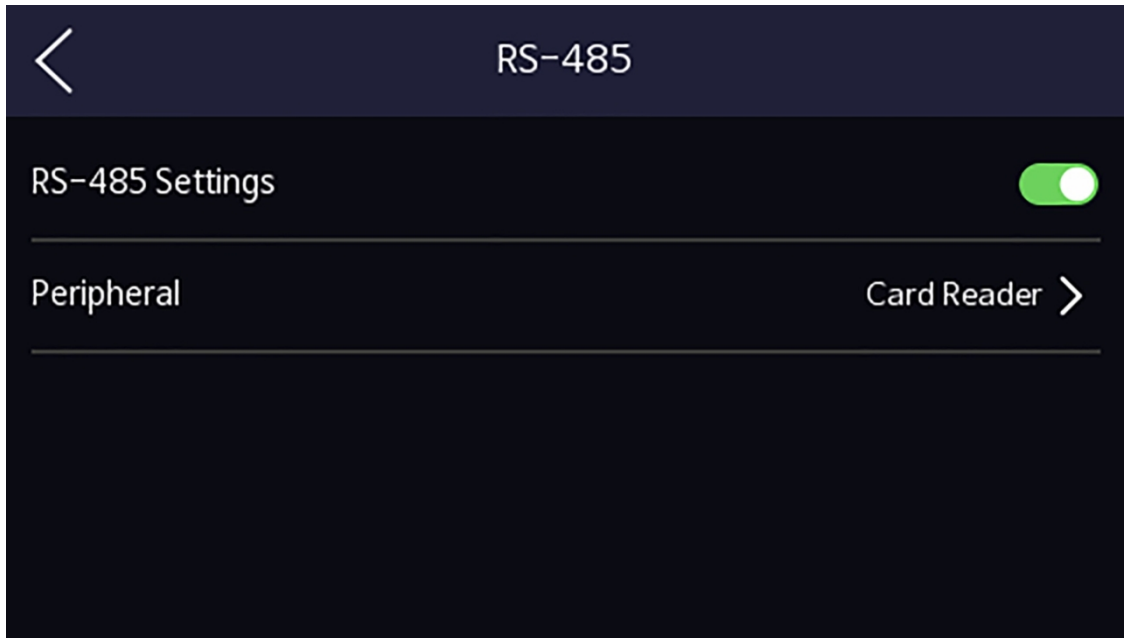



**Figure 7-6 Réglage des paramètres RS-485**

3. Sélectionnez un type de périphérique en fonction de vos besoins réels.

**Note**

Si vous sélectionnez **Contrôleur d'accès** : Si vous connectez l'appareil à un terminal via l'interface RS-485, réglez l'adresse RS-485 sur 2. Si vous connectez l'appareil à un contrôleur, réglez l'adresse RS-485 en fonction du numéro de porte.

4. Appuyez sur l'icône de retour dans le coin supérieur gauche et vous devrez redémarrer l'appareil si vous modifiez les paramètres.

### 7.2.4 Paramètres Wiegand

Vous pouvez définir la direction de la transmission Wiegand.

**Étapes**

1. Appuyez sur **Comm.** (Paramètres de communication) sur la page d'accueil pour accéder à la page Paramètres de communication.
2. Sur la page Paramètres de communication, appuyez sur **Wiegand** pour accéder à l'onglet Wiegand.


**Figure 7-7 Paramètres Wiegand**

3. Activer la fonction Wiegand.
4. Sélectionnez une direction de transmission.
   - Sortie : Un terminal de reconnaissance faciale peut connecter un contrôleur d'accès externe. Les deux appareils transmettent le numéro de carte via Wiegand 26 ou Wiegand 34.
5. Tapez sur ✓ pour enregistrer les paramètres du réseau.

**Note**

Si vous modifiez l'appareil externe, et après avoir enregistré les paramètres de l'appareil, lappareil redémarre automatiquement.

### 7.2.5 Paramètres ISUP

Réglez les paramètres ISUP et l'appareil peut télécharger des données via le protocole ISUP.

**Avant de commencer**

Assurez-vous que votre appareil est connecté à un réseau.

**Étapes**

1. Tap **Comm.** → **ISUP** .

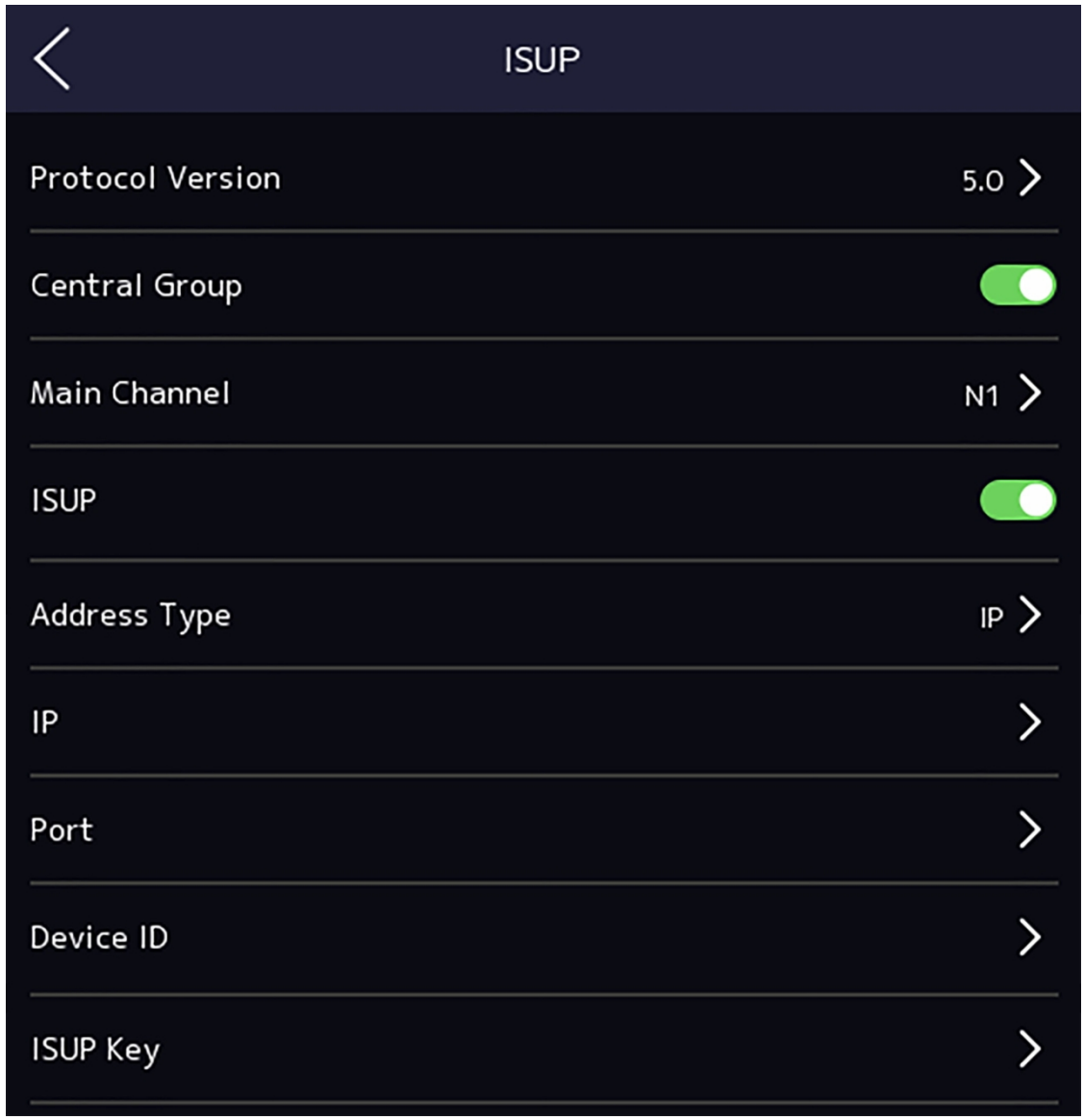



**Figure 7-8 Paramètres ISUP**

2. Activer la fonction ISUP et définir les paramètres du serveur ISUP.

**Version de l'ISUP**

Réglez la version de l'ISUP en fonction de vos besoins réels.

**Groupe central**

Activez le groupe central et les données seront téléchargées vers le groupe central.

**Canal principal**

Support N1 ou None.

**GISUP**

Activez la fonction ISUP et les données seront téléchargées via le protocole EHome.

**Type d'adresse**

Sélectionnez un type d'adresse en fonction de vos besoins réels.

**Adresse IP**

Définir l'adresse IP du serveur ISUP.

**N° de port**

Définir le numéro de port du serveur ISUP.

**Note**

Numéro de port Plage : 0 à 65535.

**ID de l'appareil**

Définir le numéro de série de l'appareil.

**Mot de passe**

Si vous choisissez la V5.0, vous devez créer un compte et une clé ISUP. Si vous choisissez une autre version, vous devez créer un compte ISUP uniquement.

**Note**

- N'oubliez pas le compte ISUP et la clé ISUP. Vous devez saisir le nom du compte ou la clé lorsque l'appareil doit communiquer avec d'autres plates-formes via le protocole ISUP.
- Gamme de clés ISUP : 8 à 32 caractères.

### 7.2.6 Accès à la plate-forme

Vous pouvez modifier le code de vérification de l'appareil et définir l'adresse du serveur avant d'ajouter l'appareil au client mobile Hik-Connect.

**Avant de commencer**

Assurez-vous que votre appareil est connecté à un réseau.

**Étapes**

1. Appuyez sur **Comm.** (Paramètres de communication) sur la page d'accueil pour accéder à la page Paramètres de communication.
2. Sur la page Paramètres de communication, appuyez sur **Accès à Hik-Connect**.
3. Permettre l'**accès à Hik-Connect**
4. Entrez l'**IP du serveur**.
5. Créez le **code de** vérification, et vous devez saisir le code de vérification lorsque vous gérez les dispositifs via **Hik-Connect**.

## 7.3 Gestion des utilisateurs

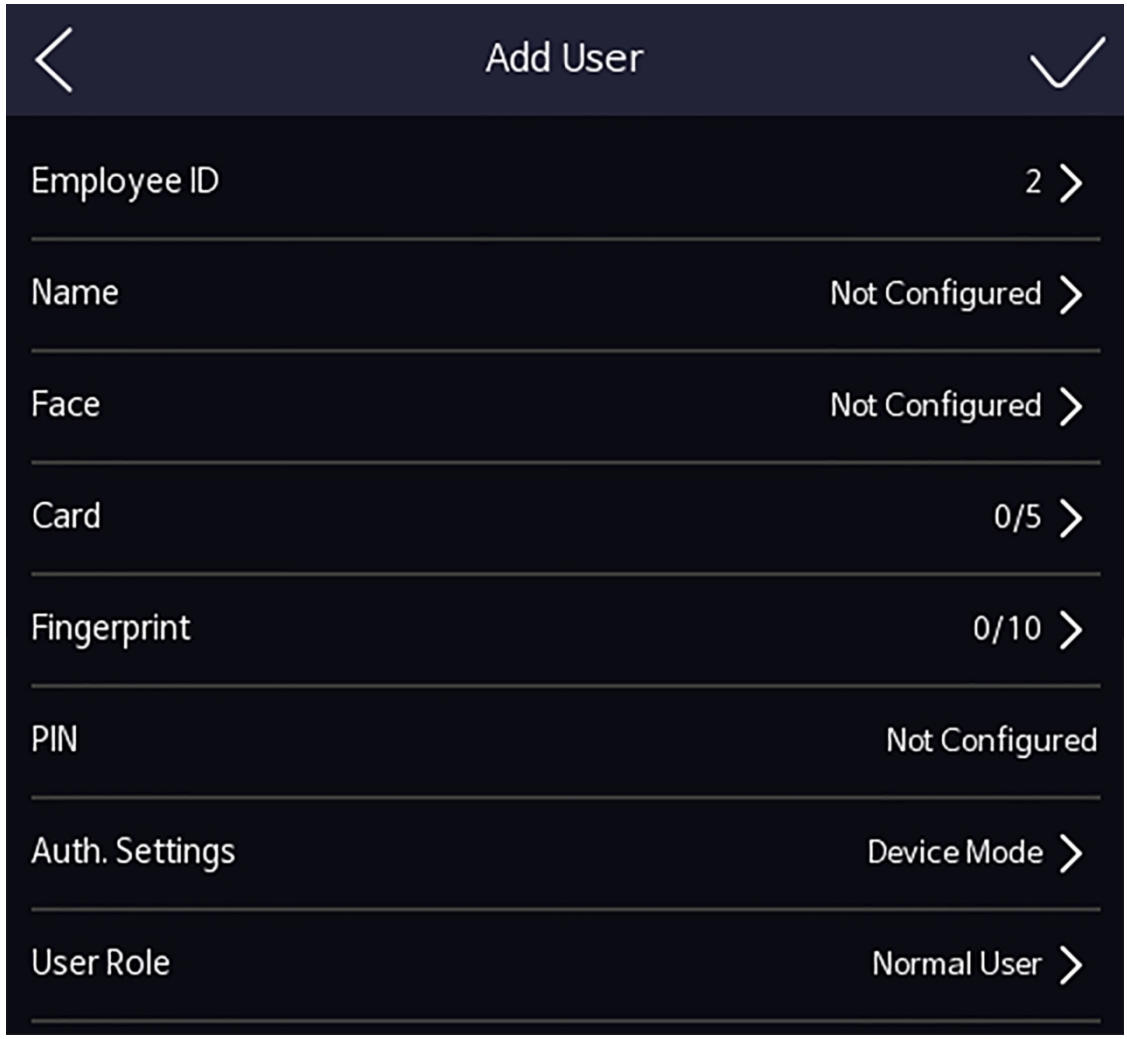
L'interface de gestion des utilisateurs permet d'ajouter, de modifier, de supprimer et de rechercher un utilisateur.

### 7.3.1 Ajouter un administrateur

L'administrateur peut se connecter au backend de l'appareil et configurer les paramètres de l'appareil.

**Étapes**

1. Appuyez longuement sur la page initiale et connectez-vous au backend.
2. Appuyez sur **Utilisateur →+**pour accéder à la page Ajouter un utilisateur.




3. Modifiez l'ID de l'employé.

**Note**

- L'identifiant de l'employé doit comporter moins de 32 caractères. Il peut s'agir d'une combinaison de lettres minuscules, de lettres majuscules et de chiffres.
- L'ID de l'employé ne doit pas être dupliqué.

4. Appuyez sur le champ Nom et saisissez le nom de l'utilisateur sur le clavier souple.

**Note**

- Les chiffres, les lettres majuscules, les lettres minuscules et les caractères spéciaux sont autorisés dans le nom d'utilisateur.
- Le nom de l'utilisateur peut comporter jusqu'à 32 caractères.

5. **Facultatif :** Ajoutez une photo de face, des empreintes digitales, des cartes ou un code PIN pour l'administrateur.

**Note**

- Pour plus d'informations sur l'ajout d'une photo de visage, voir ***Ajouter une photo de visage***.
- **Note**
  Pour plus d'informations sur l'ajout d'une empreinte digitale, voir ***Ajouter une empreinte digitale***.
- Pour plus d'informations sur l'ajout d'une carte, voir ***Ajouter une carte***.
- Pour plus d'informations sur l'ajout d'un mot de passe, voir ***Afficher le code PIN***.

6. **Facultatif :** Définissez le type d'authentification de l'administrateur.

**Note**

Pour plus d'informations sur la définition du type d'authentification, voir ***Définir le mode d'authentification***.

7. Activer la fonction d'autorisation de l'administrateur.

   **Activer l'autorisation de l'administrateur**

   L'utilisateur est l'administrateur. Outre la fonction de présence normale, l'utilisateur peut également accéder à la page d'accueil pour opérer après avoir authentifié l'autorisation.

8. Appuyez sur ✓ pour enregistrer les paramètres.

## 7.3.2 Ajouter une photo de face

Ajouter la photo du visage de l'utilisateur à l'appareil. L'utilisateur peut utiliser la photo de son visage pour s'authentifier.

**Étapes**

**Note**

Il est possible d'ajouter jusqu'à 1500 photos de visage.

1. Appuyez longuement sur la page initiale pendant 3 secondes et glissez vers la gauche/droite en suivant le geste et connectez-vous au backend.
2. Appuyez sur **Utilisateur →+**pour accéder à la page Ajouter un utilisateur.
3. Modifiez l'ID de l'employé.

**Note**

- L'identifiant de l'employé doit comporter moins de 32 caractères. Il peut s'agir d'une combinaison de lettres minuscules, de lettres majuscules et de chiffres.
- L'ID de l'employé ne doit pas être dupliqué.

4. Appuyez sur le champ Nom et saisissez le nom de l'utilisateur sur le clavier souple.

**Note**

- Les chiffres, les lettres majuscules, les lettres minuscules et les caractères spéciaux sont autorisés dans le nom d'utilisateur.
- Le nom d'utilisateur suggéré ne doit pas dépasser 32 caractères.

5. Appuyez sur le champ Image de visage pour accéder à la page d'ajout d'image de visage.

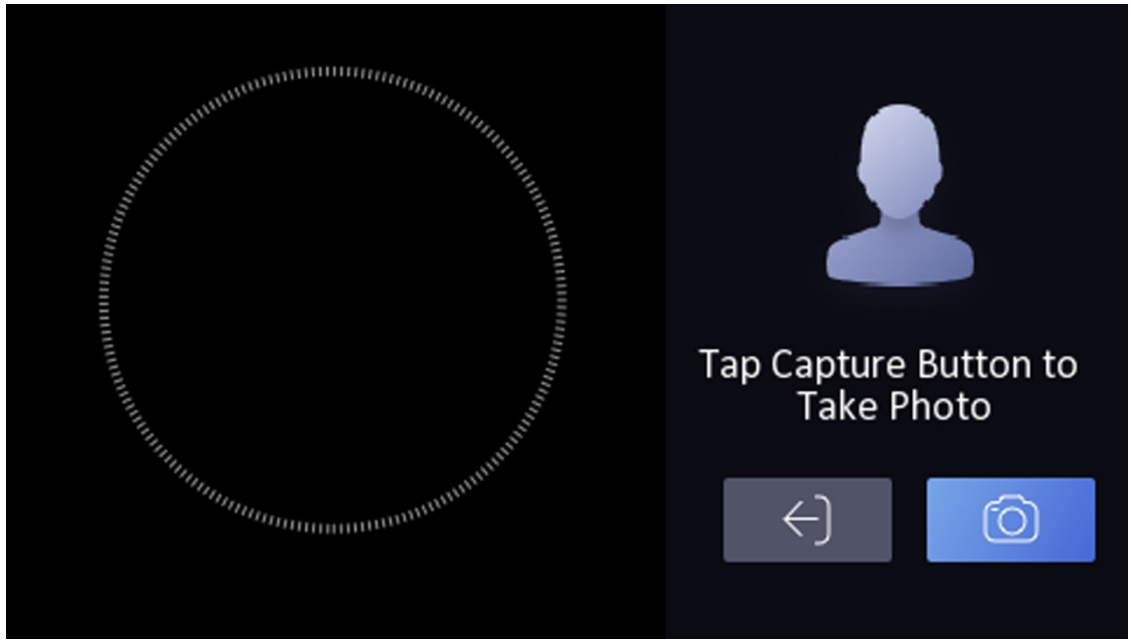



**Figure 7-9 Ajouter une image de visage**

6. Regardez l'appareil photo.

**Note**

- Assurez-vous que l'image de votre visage se trouve dans le contour de l'image du visage lorsque vous ajoutez l'image du visage.
- Assurez-vous que la photo du visage capturée est de bonne qualité et qu'elle est exacte.
- Pour plus d'informations sur les instructions relatives à l'ajout d' de visages, voir ***Conseils pour la collecte/comparaison d'images de visages*** .

Après avoir ajouté la photo du visage, une photo du visage capturé s'affiche dans le coin supérieur droit de la page.

7. Appuyez sur **Enregistrer** pour enregistrer l'image du visage.
8. **Facultatif :** Appuyez sur **Réessayer** et ajustez la position de votre visage pour ajouter à nouveau la photo du visage.

**9.** Définir le rôle de l'utilisateur.

**Administrateur**

L'utilisateur est l'administrateur. Outre la fonction de présence normale, l'utilisateur peut également accéder à la page d'accueil pour opérer après avoir authentifié l'autorisation.

**Utilisateur normal**

L'utilisateur est l'utilisateur normal. L'utilisateur ne peut s'authentifier ou prendre des présences que sur la page initiale.

**10.** Appuyez sur ✓ pour enregistrer les paramètres.

### 7.3.3 Ajouter une empreinte digitale

Ajouter une empreinte digitale pour l'utilisateur et l'utilisateur peut s'authentifier via l'empreinte digitale ajoutée.

**Étapes**

**Note**

- La fonction doit être prise en charge par l'appareil.
- Il est possible d'ajouter jusqu'à 3000 empreintes digitales.

**1.** Appuyez longuement sur la page initiale pendant 3 secondes et glissez vers la gauche/droite en suivant le geste et entrez dans le backend de l'appareil.

**2.** Appuyez sur **Utilisateur →+**pour accéder à la page Ajouter un utilisateur.

**3.** Appuyez sur le champ ID de l'employé et modifiez l'ID de l'employé.

**Note**

- L'identifiant de l'employé doit comporter moins de 32 caractères. Il peut s'agir d'une combinaison de lettres minuscules, de lettres majuscules et de chiffres.
- L'ID de l'employé ne doit pas commencer par 0 et ne doit pas être dupliqué.

**4.** Appuyez sur le champ Nom et saisissez le nom de l'utilisateur sur le clavier souple.

**Note**

- Les chiffres, les lettres majuscules, les lettres minuscules et les caractères spéciaux sont autorisés dans le nom d'utilisateur.
- Le nom d'utilisateur suggéré ne doit pas dépasser 32 caractères.

**5.** Appuyez sur le champ Empreinte digitale pour accéder à la page Ajouter une empreinte digitale.

**6.** Suivez les instructions pour ajouter une empreinte digitale.

**Note**

- Il n'est pas possible d'ajouter plusieurs fois la même empreinte digitale.
- Il est possible d'ajouter jusqu'à 10 empreintes digitales pour un utilisateur.
- Vous pouvez également utiliser le logiciel client ou l'enregistreur d'empreintes digitales pour enregistrer les empreintes digitales.

Pour plus de détails sur les instructions de numérisation des ***empreintes Conseils pour la numérisation des empreintes digitales*** digitales, voir .

**7.** Définir le rôle de l'utilisateur.

**Administrateur**

L'utilisateur est l'administrateur. Outre la fonction de présence normale, l'utilisateur peut également accéder à la page d'accueil pour opérer après avoir authentifié l'autorisation.

**Utilisateur normal**

L'utilisateur est l'utilisateur normal. L'utilisateur ne peut s'authentifier ou prendre des présences que sur la page initiale.

**8.** Appuyez sur pour enregistrer les paramètres.

### 7.3.4 Ajouter une carte

Ajouter une carte pour l'utilisateur et l'utilisateur peut s'authentifier via la carte ajoutée.

**Étapes**

**Note**

Il est possible d'ajouter jusqu'à 3000 cartes.

**1.** Appuyez longuement sur la page initiale pendant 3 secondes et glissez vers la gauche/droite en suivant le geste et connectez-vous au backend.

**2.** Appuyez sur **Utilisateur →+**pour accéder à la page Ajouter un utilisateur.

**3.** Connectez un lecteur de cartes externe conformément au schéma de câblage.

**4.** Appuyez sur le champ ID de l'employé et modifiez l'ID de l'employé.

**Note**

- L'identifiant de l'employé doit comporter moins de 32 caractères. Il peut s'agir d'une combinaison de lettres minuscules, de lettres majuscules et de chiffres.
- L'ID de l'employé ne doit pas être dupliqué.

**5.** Appuyez sur le champ Nom et saisissez le nom de l'utilisateur sur le clavier souple.

**Note**

- Les chiffres, les lettres majuscules, les lettres minuscules et les caractères spéciaux sont autorisés dans le nom d'utilisateur.
- Le nom d'utilisateur suggéré ne doit pas dépasser 32 caractères.

**6.** Appuyez sur le champ Carte et appuyez sur .**+**

**7.** Configurer le numéro de carte

- Saisir manuellement le numéro de la carte.
- Présentez la carte sur la zone de présentation des cartes pour obtenir le numéro de carte.

**Note**

- Le numéro de carte ne peut pas être vide.
- Le numéro de carte peut comporter jusqu'à 20 caractères.
- Le numéro de la carte ne peut être dupliqué.

8. Configurer le type de carte.
9. Définir le rôle de l'utilisateur.

**Administrateur**

L'utilisateur est l'administrateur. Outre la fonction de présence normale, l'utilisateur peut également accéder à la page d'accueil pour opérer après avoir authentifié l'autorisation.

**Utilisateur normal**

L'utilisateur est l'utilisateur normal. L'utilisateur ne peut s'authentifier ou prendre des présences que sur la page initiale.

10. Appuyez sur pour enregistrer les paramètres.

### 7.3.5 Afficher le code PIN

Ajoutez un code PIN pour l'utilisateur et l'utilisateur peut s'authentifier via le code PIN.

**Étapes**

1. Appuyez longuement sur la page initiale pendant 3 secondes et glissez vers la gauche/droite en suivant le geste et connectez-vous au backend.
2. Appuyez sur **Utilisateur →+**pour accéder à la page Ajouter un utilisateur.
3. Appuyez sur le champ ID de l'employé et modifiez l'ID de l'employé.

**Note**

- L'identifiant de l'employé doit comporter moins de 32 caractères. Il peut s'agir d'une combinaison de lettres minuscules, de lettres majuscules et de chiffres.
- L'ID de l'employé ne doit pas être dupliqué.

4. Appuyez sur le champ Nom et saisissez le nom de l'utilisateur sur le clavier souple.

**Note**

- Les chiffres, les lettres majuscules, les lettres minuscules et les caractères spéciaux sont autorisés dans le nom d'utilisateur.
- Le nom d'utilisateur suggéré ne doit pas dépasser 32 caractères.

5. Appuyez sur le code PIN pour afficher le code PIN.

**Note**

Le code PIN ne peut pas être modifié. Il ne peut être appliqué que par la plate-forme.

6. Définir le rôle de l'utilisateur.

**Administrateur**

L'utilisateur est l'administrateur. Outre la fonction de présence normale, l'utilisateur peut également accéder à la page d'accueil pour opérer après avoir authentifié l'autorisation.

**Utilisateur normal**

L'utilisateur est l'utilisateur normal. L'utilisateur ne peut s'authentifier ou prendre des présences que sur la page initiale.

**7.** Appuyez sur pour enregistrer les paramètres.

### 7.3.6 Définir le mode d'authentification

Après avoir ajouté la photo du visage de l'utilisateur, son mot de passe ou d'autres informations d'identification, vous devez définir mode d'authentification et l'utilisateur peut authentifier son identité via le mode d'authentification configuré.

**Étapes**

**1.** Appuyez longuement sur la page initiale pendant 3 secondes et glissez vers la gauche/droite en suivant le geste et connectez-vous au backend.

**2.** Appuyez sur **Utilisateur→ Ajouter un utilisateur/Modifier un utilisateur→ Mode d'authentification** .

**3.** Sélectionnez Device ou Custom comme mode d'authentification.

**Dispositif**

Si vous souhaitez sélectionner le mode périphérique, vous devez d'abord définir le mode d'authentification du terminal dans la page Paramètres de contrôle d'accès. Pour plus d'informations, voir *Configuration des paramètres de contrôle d'accès*.

**Sur mesure**

Vous pouvez combiner différents modes d'authentification en fonction de vos besoins réels.

**4.** Appuyez sur pour enregistrer les paramètres.

### 7.3.7 Rechercher et modifier un utilisateur

Après avoir ajouté un utilisateur, vous pouvez le rechercher et le modifier.

#### Recherche d'un utilisateur

Sur la page Gestion des utilisateurs, appuyez sur la zone de recherche pour accéder à la page Rechercher un utilisateur. Appuyez sur **Carte à** gauche de la page et sélectionnez un type de recherche dans la liste déroulante. Saisissez l'ID de l'employé, le numéro de carte ou le nom de l'utilisateur à rechercher. Tapez sur pour effectuer la recherche.

#### Modifier l'utilisateur

Sur la page Gestion des utilisateurs, sélectionnez un utilisateur dans la liste des utilisateurs pour accéder à la page Modifier l'utilisateur. Suivez les étapes de la section ***Gestion des utilisateurs*** pour modifier les paramètres de l'utilisateur. Tapez sur pour enregistrer les paramètres.

**Note**

L'ID de l'employé ne peut pas être modifié.

## 7.4 Gestion des données

Vous pouvez supprimer des données, les importer et les exporter.

### 7.4.1 Supprimer les données

Supprimer les données de l'utilisateur.

Sur la page d'accueil, appuyez sur **Données→ Supprimer les données→ Données utilisateur** . Toutes les données utilisateur ajoutées dans l'appareil seront supprimées.

### 7.4.2 Importer des données

**Étapes**

1. Branchez une clé USB dans l'appareil.
2. Sur la page d'accueil, appuyez sur **Données→ Importer des données** .
3. Appuyez sur **Données de l'utilisateur**, **Données du visage** ou **Paramètres de contrôle d'accès** .

**Note**

Les paramètres de contrôle d'accès importés sont des fichiers de configuration de l'appareil.

4. Saisissez le mot de passe créé lors de l'exportation des données. Si vous n'avez pas créé de mot de passe lors de l'exportation des données, laissez un blanc dans la zone de saisie et appuyez immédiatement sur **OK.**

**Note**

- Si vous souhaitez transférer toutes les informations relatives à l'utilisateur d'un appareil (appareil A) à un autre (appareil B), vous devez exporter les informations de l'appareil A vers la clé USB, puis les importer de la clé USB vers l'appareil B. Dans ce , vous devez importer les données relatives à l'utilisateur avant d'importer la photo de profil.
- Le format de clé USB pris en charge est FAT32.
- Les images importées doivent être sauvegardées dans le dossier (nommé enroll_pic) du répertoire racine et le nom de l'image doit suivre la règle ci-dessous :
  N° de carte _Nom_Département_Identification du salarié_Genre.jpg
- Si le dossier enroll_pic ne peut pas contenir toutes les images importées, vous pouvez créer d'autres dossiers, nommés enroll_pic1, enroll_pic2, enroll_pic3, enroll_pic4, sous le répertoire racine.
- L'identifiant de l'employé doit comporter moins de 32 caractères. Il peut s'agir d'une combinaison de minuscules, de lettres majuscules et de chiffres. Il ne doit pas être dupliqué et ne doit pas commencer par 0.
- La photo de face doit respecter les règles suivantes : Elle doit être prise de face, en faisant directement face à l'appareil photo. Ne pas porter de chapeau ou de couvre-chef lors de la prise de la photo de face. Le format doit être JPEG ou JPG. La résolution doit être de 640× 480 pixels ou plus de 640 × 480 pixels. La taille de l'image doit être comprise entre 60 KB et 200 KB.

### 7.4.3 Exportation de données

**Étapes**

1. Branchez une clé USB dans l'appareil.
2. Sur la page d'accueil, appuyez sur **Données→ Exporter les données** .
3. Appuyez sur **Données de visage**, **Données d'événement**, **Données utilisateur** ou **Paramètres de contrôle d'accès**.

**Note**

Les paramètres de contrôle d'accès exportés sont des fichiers de configuration de l'appareil.

4. **Optionnel :** Créez un mot de passe pour l'exportation. Lorsque vous importez ces données vers un autre appareil, vous devez saisir le mot de passe.

**Note**

- Le format de clé USB pris en charge est DB.
- Le système prend en charge les clés USB d'une capacité de stockage de 1G à 32G. Assurez-vous que l'espace libre de la clé USB est supérieur à 512M.
- Les données utilisateur exportées sont un fichier DB, qui ne peut pas être modifié.

## 7.5 Authentification de l'identité

Après la configuration du réseau, la configuration des paramètres du système et la configuration de l'utilisateur, vous pouvez retourner à la page initiale pour l'authentification de l'identité. Le système authentifie la personne fonction du mode d'authentification configuré.

### 7.5.1 Authentification via un justificatif unique

Définissez le type d'authentification de l'utilisateur avant l'authentification. Pour plus de détails, voir ***Définir le mode d'authentification*** . Authentifier le visage, l'empreinte digitale ou la carte.

**Visage**

Faites face à la caméra et commencez l'authentification par le visage.

**Empreinte digitale**

Placez l'empreinte digitale enregistrée sur le module d'empreintes digitales et démarrez l'authentification par empreinte digitale.

**Carte**

Présenter la carte dans la zone de présentation des cartes et commencer l'authentification par carte.

**Note**

La carte peut être une carte à puce normale ou une carte cryptée.

**Code PIN**

Saisissez le code PIN pour vous authentifier via le code PIN.

Si l'authentification est terminée, le message "Authentifié" s'affiche.

### 7.5.2 Authentification via des justificatifs multiples

**Avant de commencer**

Définissez le type d'authentification de l'utilisateur avant l'authentification. Pour plus de détails, voir ***Définir le mode d'authentification*** .

**Étapes**

1. Si le mode d'authentification est Carte et Face, Mot de passe et Face, Carte et Mot de passe, Carte et Face et Empreinte digitale, authentifiez n'importe quelle pièce d'identité conformément aux instructions de la page de visualisation en direct.

**Note**

- La carte peut être une carte à puce normale ou une carte cryptée.

2. Après l'authentification de l'identifiant précédent, poursuivre l'authentification des autres identifiants.

**Note**

- Pour plus d'informations sur la numérisation des empreintes digitales, voir *Conseils pour la numérisation des empreintes digitales*.
- Pour des informations détaillées sur l'authentification des visages, voir *Conseils pour la collecte et la comparaison de photos de visages*.

Si l'authentification a réussi, le message "Authentifié" s'affiche.

## 7.6 Paramètres de base

Vous pouvez définir la touche de raccourci, le thème, la voix, l'heure, le temps de sommeil (s), le temps d'attente avant la déconnexion (s), la langue, le numéro de communauté, le numéro de bâtiment et le numéro d'unité.

Appuyez longuement sur la page initiale pendant 3 s et faites glisser vers la gauche/droite en suivant le geste et connectez-vous à la page d'accueil de l'appareil. Tapez sur **Basique**.

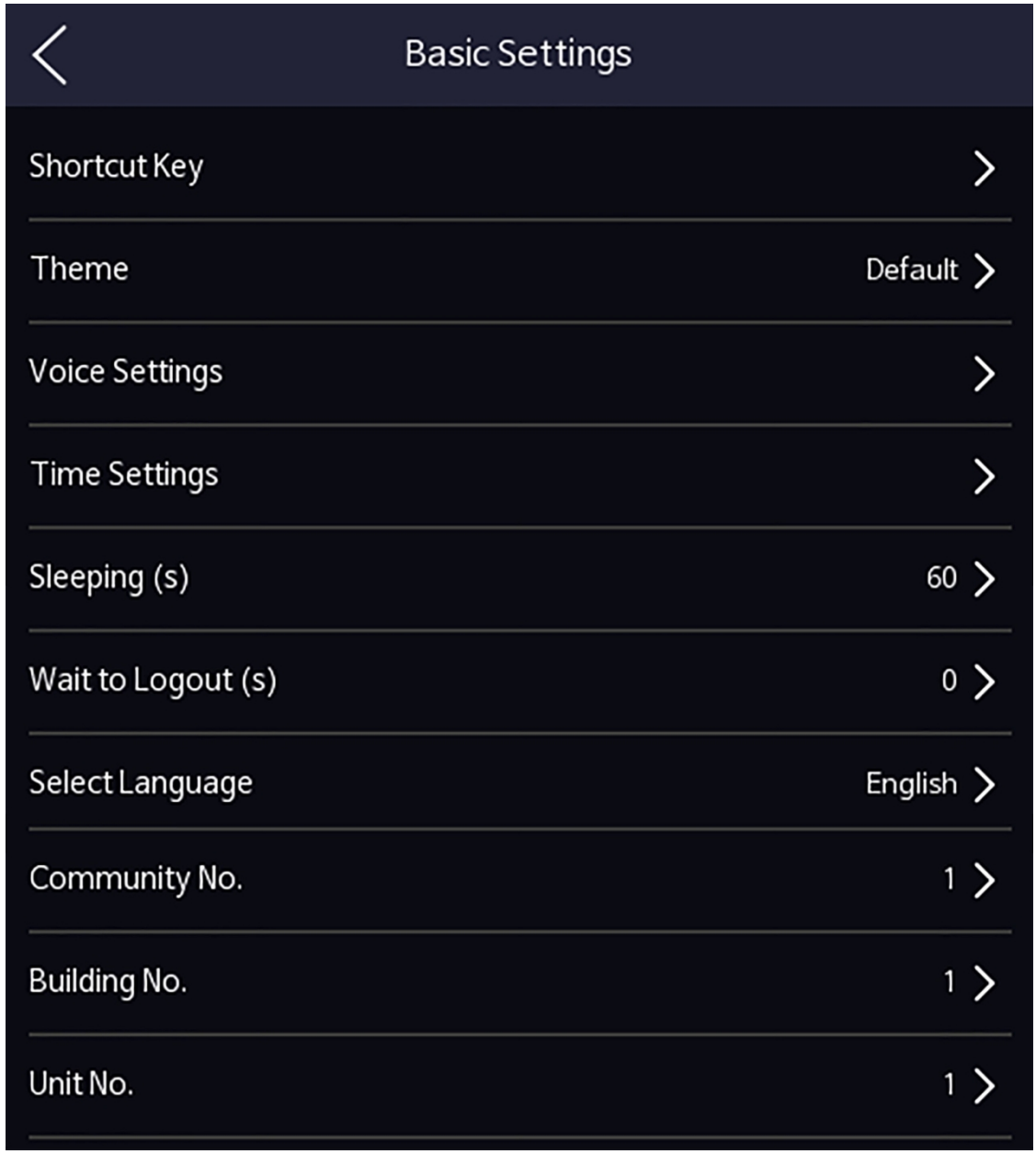



**Figure 7-10 Page des paramètres de base**

**Touche de raccourci**

Choisissez la touche de raccourci affichée sur la page d'authentification, y compris la fonction de code QR, la fonction d'appel, le type d'appel et la fonction de saisie du mot de passe.

**Note**

- Si l'authentification combinée du visage et du code QR est prise en charge et que la clé de raccourci du code QR est désactivée (il n'y a pas d'icône de clé de raccourci du code QR sur la page d'authentification), vous pouvez scanner le code QR au milieu de la page d'authentification pour vous authentifier.
- Vous pouvez sélectionner le type d'appel parmi **Salle d'appel**, **Centre d'appel** et **Numéro de salle spécifié. Salle d'appel**

  Lorsque vous appuyez sur le bouton d'appel sur la page d'authentification, vous devez composer le numéro de la pièce à appeler.

  **Centre d'appel**

  Lorsque vous appuyez sur le bouton d'appel de la page d'authentification, vous pouvez appeler directement le centre.

  **Appeler le numéro de chambre spécifié**

  Lorsque vous appuyez sur le bouton d'appel sur la page d'authentification, vous pouvez appeler directement la salle configurée sans composer de numéro.

**Thème**

Vous pouvez définir le thème de la fenêtre d'invite sur la page d'authentification. Vous pouvez sélectionner **Thème par défaut/Simple**. Si vous sélectionnez **Simple**, l'affichage en direct de la page d'authentification sera désactivé et, dans le même temps, le nom de la personne, l'identifiant de l'employé et les photos du visage seront tous masqués.

**Paramètres vocaux**

Vous pouvez activer/désactiver la fonction d'invite vocale et régler le volume de la voix.

**Note**

Vous pouvez régler le volume de la voix entre 0 et 10.

**Réglages de l'heure**

Régler le fuseau horaire, l'heure de l'appareil et l'heure d'été.

**Dormir (s)**

Réglez le temps d'attente de mise en veille de l'appareil (en minutes). Lorsque vous êtes sur la page initiale et que vous réglez le temps de sommeil sur 30 min, l'appareil se mettra en veille après 30 min sans aucune opération.

**Note**

Si vous réglez le temps de sommeil sur 0, l'appareil n'entrera pas en mode sommeil.

**Attente de la déconnexion (s)**

Si aucune opération n'est effectuée dans le délai configuré, le système se déconnecte.

**Sélectionner la langue**

Sélectionnez la langue en fonction de vos besoins.

**No. de la communauté**

Définir le numéro de communauté du dispositif installé.

**Bâtiment n°.**

Définir le numéro de bâtiment installé sur l'appareil.

**N° d'unité**

Définir le numéro de l'unité installée sur l'appareil.

## 7.7 Paramètres biométriques

Vous pouvez personnaliser les paramètres du visage afin d'améliorer les performances de la reconnaissance faciale. Les paramètres configurables comprennent la sélection du mode d'application, le niveau de vivacité des visages, la distance de reconnaissance des visages, l'intervalle de reconnaissance des visages, le niveau de sécurité des visages 1:N, le niveau de sécurité des visages 1:1, les paramètres ECO et la détection des visages avec masque.

Appuyez longuement sur la page initiale pendant 3 secondes et connectez-vous à la page d'accueil. Appuyez sur **Biométrie**.

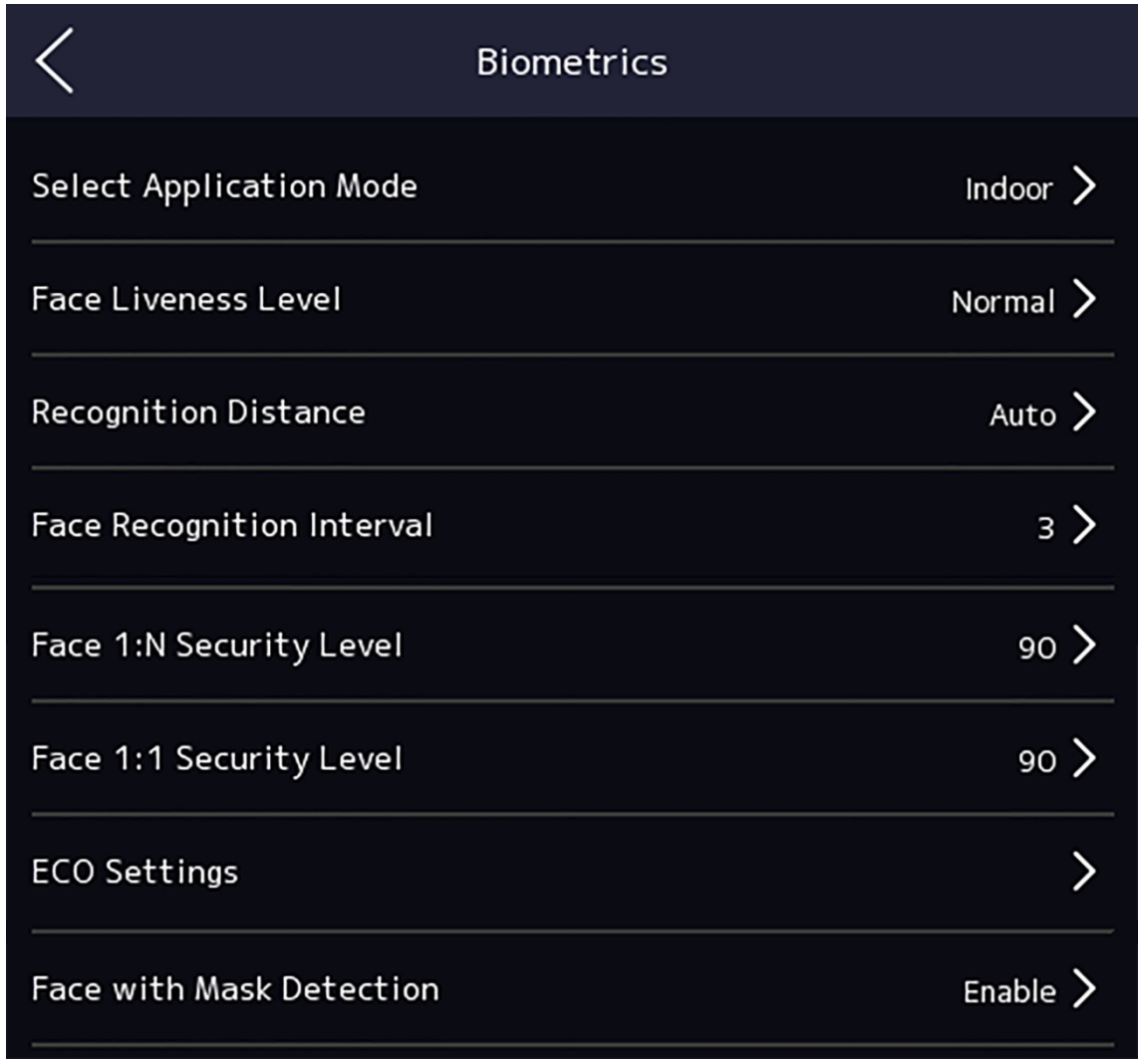



**Figure 7-11 Page des paramètres biométriques**

**Tableau 7-1 Paramètres de l'image de face**

| Paramètres | Description |
|---|---|
| Sélectionner le mode d'application | Sélectionnez "autres" ou "intérieur" en fonction de l'environnement réel. |
| Niveau de vivacité du visage | Après avoir activé la fonction anti-falsification des visages, vous pouvez définir le niveau de sécurité correspondant lors de l'authentification des visages en direct. |
| Distance de reconnaissance des visages | Définir la distance valide entre l'utilisateur et la caméra lors de l'authentification. |

| Paramètres | Description |
|---|---|
| Intervalle de reconnaissance des visages | Intervalle de temps entre deux reconnaissances continues du visage lors de l'authentification.<br>**Note**<br>Vous pouvez saisir un nombre de 1 à 10. |
| Face 1:N Niveau de sécurité | Définir le seuil de correspondance lors de l'authentification en mode de correspondance 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est important. |
| Niveau de sécurité face 1:1 | Définit le seuil de correspondance lors de l'authentification en mode de correspondance 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est important. |
| Réglages ECO | Après avoir activé le mode ECO, l'appareil utilisera la caméra IR pour authentifier les visages dans un environnement sombre ou faiblement éclairé. Vous pouvez définir le seuil du mode ECO, le mode ECO (1:N), le mode ECO (1:1), Face with mask & face (1:1 ECO) et Face with mask & face (1:N ECO).<br>**Seuil ECO**<br>Lorsque vous activez le mode ECO, vous pouvez définir le seuil du mode ECO. Plus la valeur est élevée, plus l'appareil passe facilement en mode ECO.<br>**Mode ECO (1:1)**<br>Définir le seuil de correspondance lors de l'authentification en mode ECO 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.<br>**Mode ECO (1:N)**<br>Définir le seuil de correspondance lors de l'authentification en mode ECO 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.<br>**Face avec Mask & Face (1:1 ECO)**<br>Définir la valeur de correspondance lors de l'authentification avec un masque facial en mode ECO 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.<br>**Visage avec masque et visage (1:N ECO)** |

| Paramètres | Description |
|---|---|
| | Définit la valeur de correspondance lors de l'authentification avec un masque facial via le mode ECO 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé. |
| Détection de visage avec masque | Après avoir activé la détection de visage avec masque, le système reconnaîtra le visage capturé avec l'image du masque. Vous pouvez définir le niveau et la stratégie de détection des visages avec masque et des visages 1:N.<br>**Stratégie**<br>Définir la stratégie **Aucun**, **Rappel du port** et **Doit être porté.**<br>**Rappel du port**<br>Si la personne ne porte pas de masque facial lors de l'authentification, l'appareil émet une notification et la porte s'ouvre.<br>**Must Wear**<br>Si la personne ne porte pas de masque facial lors de l'authentification, dispositif émet une notification et la porte reste fermée.<br>**Aucun**<br>Si la personne ne porte pas de masque facial lors de l'authentification, l'appareil n'émettra pas de notification.<br>**Visage avec masque et visage (1:1)**<br>Définir la valeur de correspondance lors de l'authentification par masque facial en mode de correspondance 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.<br>**Visage avec masque et visage (1:N)**<br>Définir la valeur de correspondance lors de l'authentification par masque facial en mode de correspondance 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé. |

## 7.8 Paramètres de contrôle d'accès

Vous pouvez définir les autorisations de contrôle d'accès, y compris les fonctions de mode d'authentification, d'activation de la carte NFC, d'activation de la carte M1, de contact de porte, de durée d'ouverture (s) et d'intervalle d'authentification (s).

Sur la page d'accueil, appuyez sur **ACS** (Access Control Settings) pour accéder à la page Access Control Settings. Modifiez les paramètres de contrôle d'accès sur cette page.

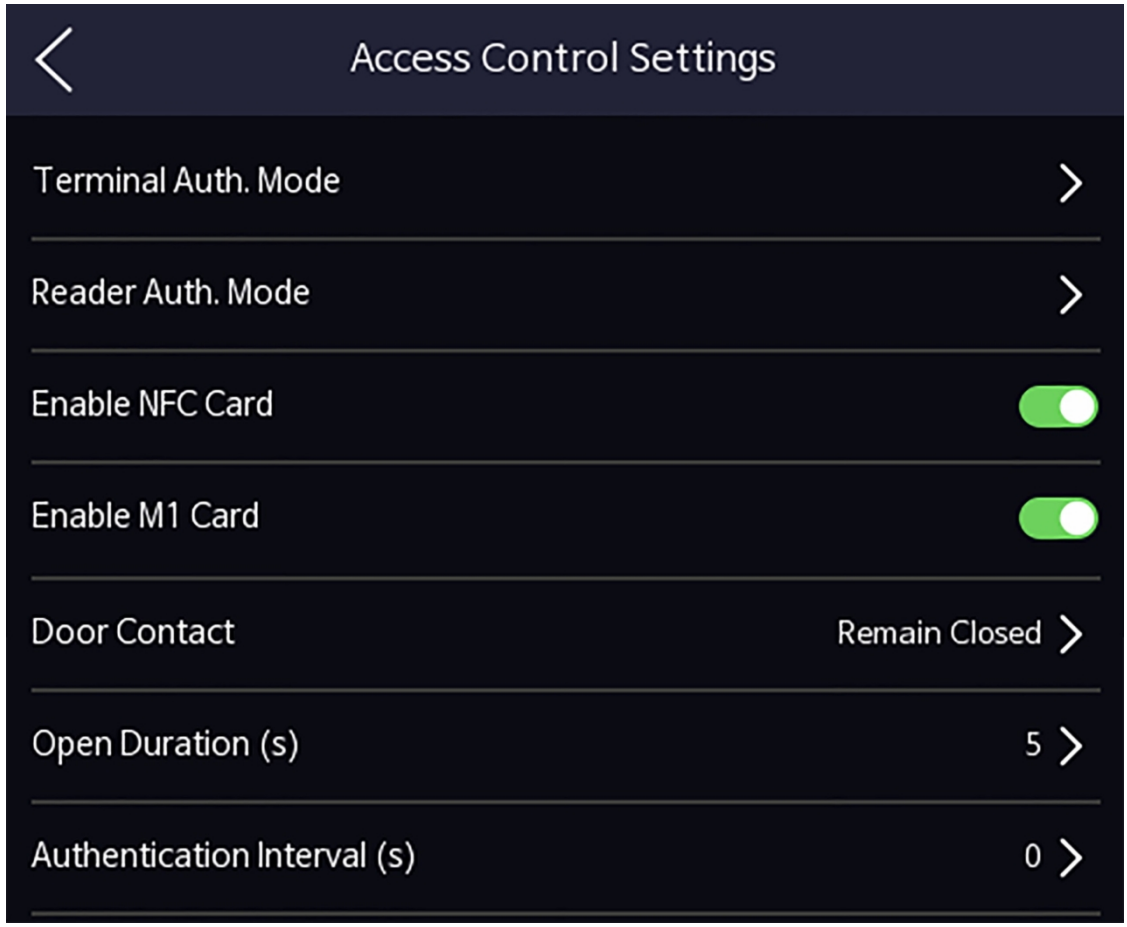



**Figure 7-12 Paramètres de contrôle d'accès**

Les descriptions des paramètres disponibles sont les suivantes :

**Tableau 7-2 Description des paramètres de contrôle d'accès**

| Paramètres | Description |
|---|---|
| Mode Auth. (Mode d'authentification du terminal) | Sélectionnez le mode d'authentification du terminal de reconnaissance faciale. Vous pouvez également personnaliser le mode d'authentification. |

| Paramètres | Description |
|---|---|
| | **Note**<br>• Seul l'appareil équipé d'un module d'empreintes digitales prend en charge fonction liée aux empreintes digitales.<br>• Les produits de reconnaissance biométrique ne sont pas totalement adaptés aux environnements de lutte contre l'usurpation d'identité. Si vous avez besoin d'un niveau de sécurité plus élevé, utilisez plusieurs modes d'authentification.<br>• Si vous adoptez plusieurs modes d'authentification, vous devez authentifier les autres méthodes avant d'authentifier le visage. |
| Reader Auth. (Mode d'authentification du lecteur de cartes) | Sélectionnez le mode d'authentification du lecteur de cartes. |
| Activer la carte NFC | Activez la fonction et vous pourrez présenter la carte NFC pour vous authentifier. |
| Activer la carte M1 | Activez la fonction et vous pourrez présenter la carte M1 pour vous authentifier. |
| Contact de porte | Vous pouvez sélectionner "Ouvrir (rester ouvert)" ou "Fermer (fermer)" en fonction de vos besoins réels. Par défaut, il s'agit de "Fermer" (Remian Closed). |
| Ouvert Durée | Régler la durée de déverrouillage de la porte. Si la porte n'est pas ouverte pendant la durée définie, elle est verrouillée. Plage de temps disponible pour le verrouillage de la porte : 1 à 255 s. |
| Intervalle d'authentification | Définir l'intervalle d'authentification de l'appareil. Intervalle d'authentification disponible : 0 à 65535. |

## 7.9 Réglages du statut des heures et des présences

Vous pouvez définir le mode de présence comme l', la sortie, la pause, l'enregistrement, les heures supplémentaires, l'enregistrement et la sortie en fonction de votre situation réelle.

**Note**
Cette fonction doit être utilisée en coopération avec la fonction de gestion du temps et des présences du logiciel client.

### 7.9.1 Désactiver le mode présence via l'appareil

Désactivez le mode de présence et le système n'affichera pas l'état de la présence sur la page initiale.

Tapez sur **Statut** T&A pour accéder à la page Statut T&A.

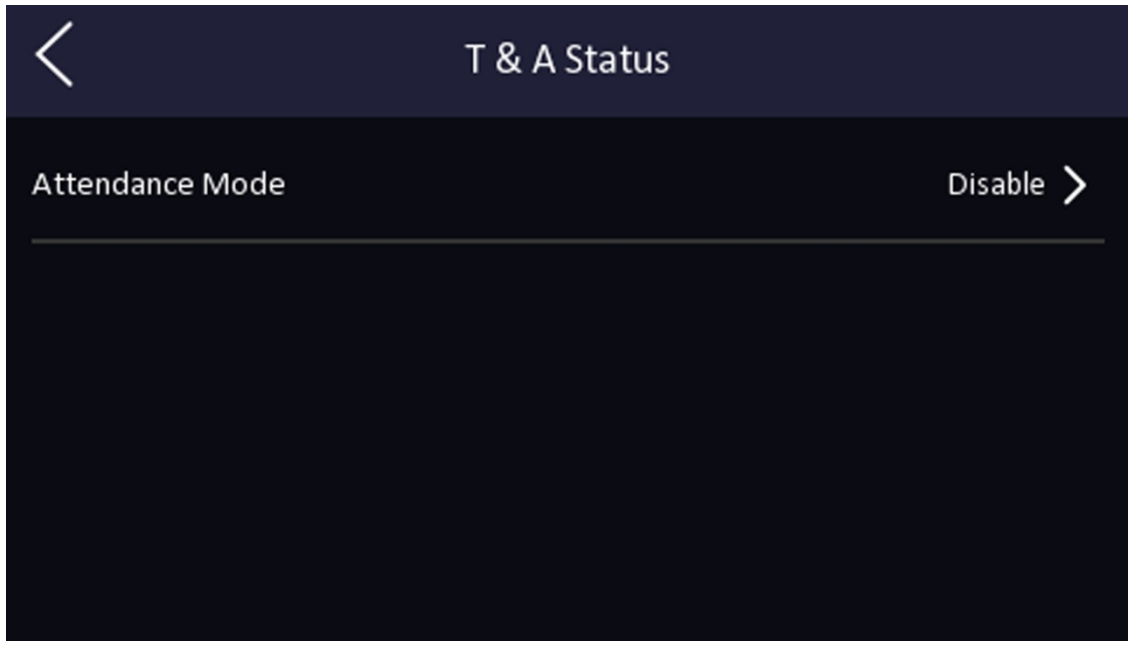



**Figure 7-13 Désactiver le mode présence**

Réglez **le mode de présence** sur **Désactivé**.

Vous ne verrez ni ne configurerez l'état des présences sur la page initiale. Le système suivra la règle de présence configurée sur la plateforme.

### 7.9.2 Régler la participation manuelle via le dispositif

Définissez le mode de présence comme étant manuel, et vous devrez sélectionner un statut manuellement lorsque vous prendrez des présences.

**Avant de commencer**

Ajoutez au moins un et définissez son mode d'authentification. Pour plus de détails, voir *Gestion des utilisateurs*.

**Étapes**

1. Tapez sur **Statut** T&A pour accéder à la page Statut T&A.
2. Réglez **le mode de participation** sur **Manuel**.

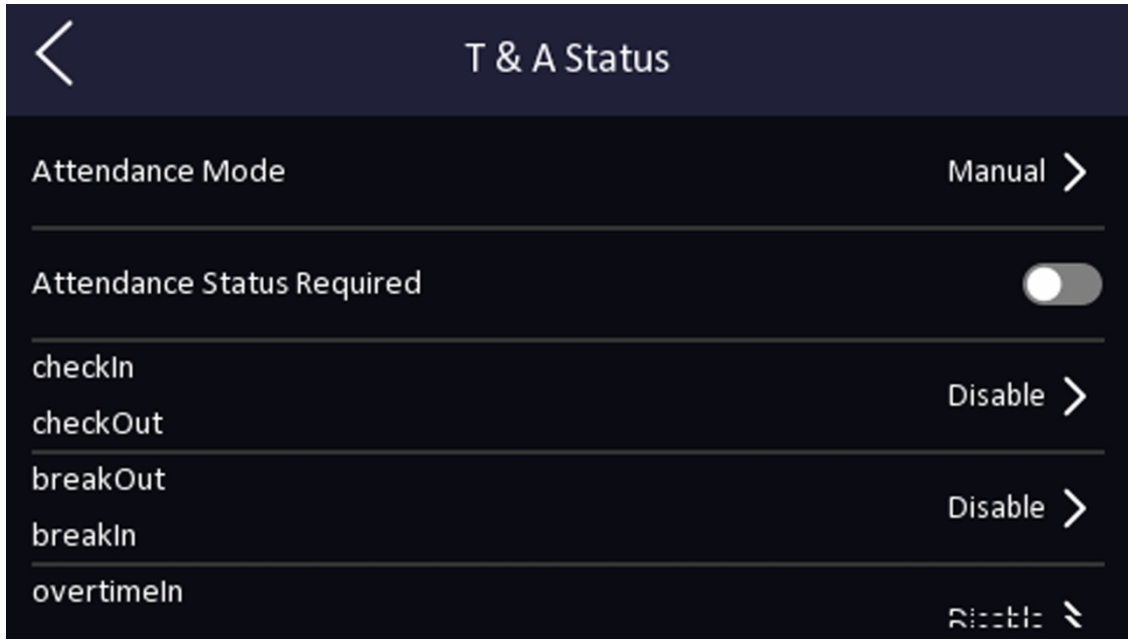



**Figure 7-14 Mode de participation manuelle**

3. Activer le **statut de présence requis**.
4. Activer un groupe de statuts de présence.

**Note**

La propriété de l'assiduité ne sera pas modifiée.

5. **Optionnel :** Sélectionnez un statut et modifiez son nom si nécessaire.

   Le nom sera affiché sur la page de statut T & A et sur la page de résultat de l'authentification.

**Résultat**

Vous devez sélectionner manuellement un statut de présence après l'authentification.

**Note**

Si vous ne sélectionnez pas de statut, l'authentification échouera et ne sera pas marquée comme une présence valide.

### 7.9.3 Régler la présence automatique via l'appareil

Définissez le mode de présence comme automatique, et vous pouvez définir le statut de présence et son horaire disponible. Le système modifie automatiquement le statut de présence en fonction de l'horaire configuré.

**Avant de commencer**

Ajoutez au moins un et définissez son mode d'authentification. Pour plus de détails, voir *Gestion des utilisateurs*.

**Étapes**

1. Tapez sur **Statut** T&A pour accéder à la page Statut T&A.
2. Réglez **le mode de participation** sur **Auto**.

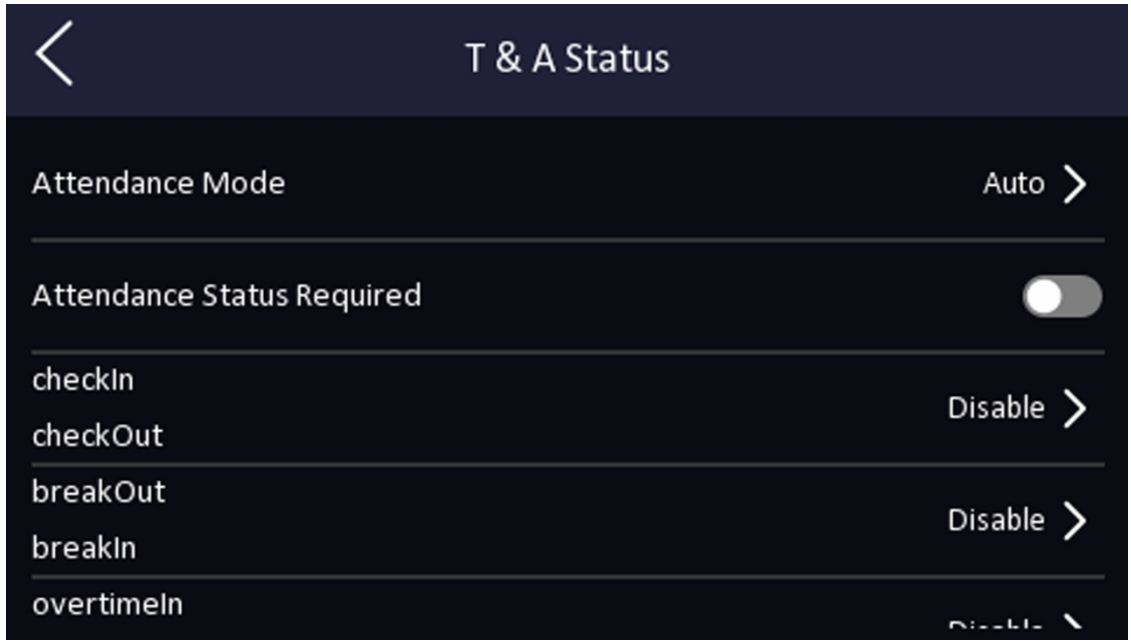



**Figure 7-15 Mode de présence automatique**

3. Activer la fonction **Statut de présence.**
4. Activer un groupe de statuts de présence.

**Note**

La propriété de l'assiduité ne sera pas modifiée.

5. **Optionnel :** Sélectionnez un statut et modifiez son nom si nécessaire.

   Le nom sera affiché sur la page de statut T & A et sur la page de résultat de l'authentification.
6. Fixer le calendrier du statut.
   1) Appuyez sur **Calendrier des présences**.
   2) Sélectionnez **lundi**, **mardi**, **mercredi**, **jeudi**, **vendredi**, **samedi** ou **dimanche**.
   3) Définir l'heure de début de journée du statut de présence sélectionné.
   4) Appuyez sur **Confirmer**.
   5) Répétez les étapes 1 à 4 en fonction de vos besoins réels.

**Note**

L'état de présence sera valide dans le cadre de l'horaire configuré.

**Résultat**

Lorsque vous vous authentifiez sur la page initiale, l'authentification est marquée comme l'état de présence configuré selon le calendrier configuré.

**Exemple**
Si l'on fixe l'**heure de sortie** au lundi 11:00 et l'heure **d'entrée au** lundi 12:00, l'authentification de l'utilisateur valide entre le lundi 11:00 et le lundi 12:00 sera marquée comme une interruption.

### 7.9.4 Régler la présence manuelle et automatique via l'appareil

Définissez le mode de présence comme **Manuel et Auto**, et le système changera automatiquement statut de présence selon le calendrier configuré. En même temps, vous pouvez modifier manuellement le statut de présence après l'authentification.

**Avant de commencer**
Ajoutez au moins un et définissez son mode d'authentification. Pour plus de détails, voir *Gestion des utilisateurs*.

**Étapes**
1. Tapez sur **Statut** T&A pour accéder à la page Statut T&A.
2. Réglez **le mode de présence** sur **Manuel et Auto**.

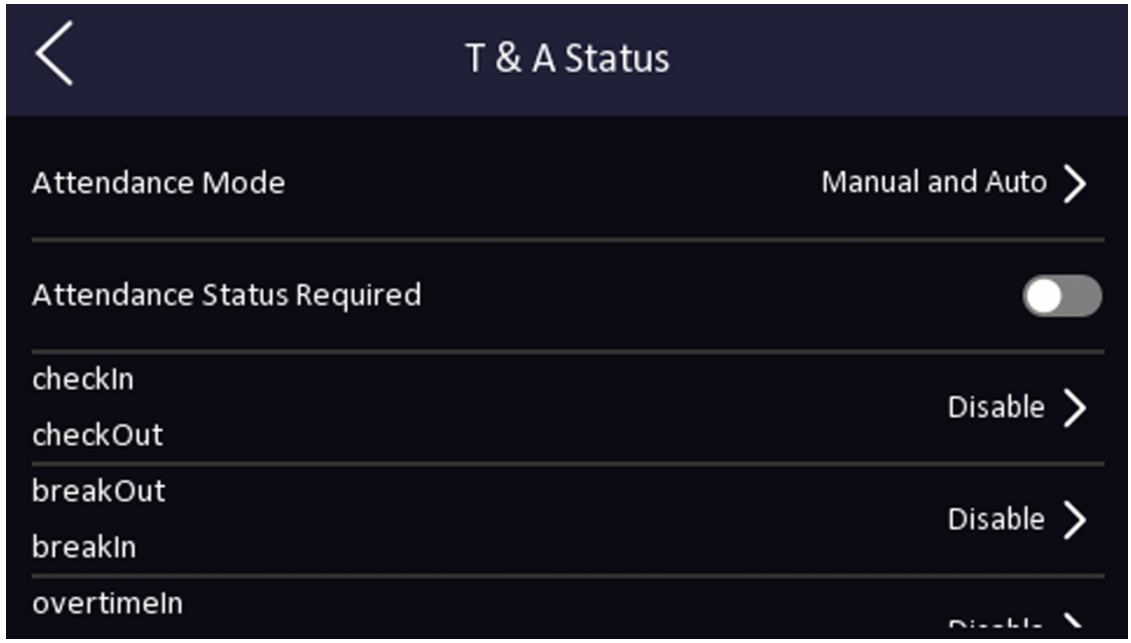



**Figure 7-16 Mode manuel et mode automatique**

3. Activer la fonction **Statut de présence.**
4. Activer un groupe de statuts de présence.

**Note**
La propriété de l'assiduité ne sera pas modifiée.

5. **Optionnel :** Sélectionnez un statut et modifiez son nom si nécessaire.
   Le nom sera affiché sur la page de statut T & A et sur la page de résultat de l'authentification.
6. Fixer le calendrier du statut.

1) Appuyez sur **Calendrier des présences**.
2) Sélectionnez **lundi**, **mardi**, **mercredi**, **jeudi**, **vendredi**, **samedi** ou **dimanche**.
3) Définir l'heure de début de journée du statut de présence sélectionné.
4) Appuyez sur **OK**.
5) Répétez les étapes 1 à 4 en fonction de vos besoins réels.

**Note**

L'état de présence sera valide dans le cadre de l'horaire configuré.

**Résultat**

Sur la page initiale et s'authentifier. L'authentification sera marquée comme l'état de présence configuré selon le calendrier. Si vous appuyez sur l'icône de modification dans l'onglet des résultats, vous pouvez sélectionner un statut pour prendre des présences manuellement, l'authentification sera marquée comme le statut de présence modifié.

**Exemple**
Si l'on fixe l'**heure de sortie** au lundi 11:00 et l'heure **d'entrée au** lundi 12:00, l'authentification de l'utilisateur valide entre le lundi 11:00 et le lundi 12:00 sera marquée comme une interruption.

## 7.10 Maintenance du système

Vous pouvez afficher les informations et la capacité du système de l'appareil. Vous pouvez également restaurer les paramètres d'usine ou les paramètres par défaut du système, dissocier le compte APP et redémarrer le système.

Tapez longuement sur la page initiale pendant 3 secondes et connectez-vous à la page d'accueil. Appuyez sur **Maint.**


**Figure 7-17 Page de maintenance**

**Informations sur le système**

Vous pouvez consulter les informations relatives à l'appareil, notamment le numéro de série, la version du micrologiciel, la version du MCU, l'adresse MAC, les données de production, le code QR de l'appareil et la licence du code source ouvert.

**Note**

La page peut varier en fonction des différents modèles d'appareils. Se référer à la page actuelle pour plus de détails.

**Capacité**

Vous pouvez afficher le numéro de l'administrateur, de l'utilisateur, de la photo de face, de la carte et de l'événement.

**Note**

Certains modèles d'appareils prennent en charge l'affichage du numéro d'empreinte digitale. Pour plus de détails, se référer à la page en question.

**Mise à niveau**

Branchez la clé USB dans l'interface USB de l'appareil. Tapez sur **Upgrade→ OK** , et lappareil lira le fichier *digicap.dav* dans le lecteur flash USB pour commencer la mise à niveau.

**Débrancher le compte APP**

Déconnecter le compte Hik-Connect de la plateforme.

**Rétablissement de l'état d'origine**

Tous les paramètres seront rétablis aux réglages d'usine. Le système doit redémarrer pour prendre effet.

**Rétablir la valeur par défaut**

Tous les paramètres, à l'exception des paramètres de communication et des informations sur l'utilisateur importées à distance, seront rétablis à leur valeur par défaut. Le système redémarre pour prendre effet.

**Reboot**

L'appareil redémarre après la confirmation.

Appuyez longuement sur et entrez le mot de passe administrateur pour afficher les informations sur la version de l'appareil.

# Chapitre 8 Configuration de l'appareil via le navigateur mobile

## 8.1 Connexion

Vous pouvez vous connecter via un navigateur mobile.

**Note**

- Certaines parties du modèle prennent en charge les paramètres Wi-Fi.
- Assurez-vous que le dispositif est activé.

Obtenez l'adresse IP de l'appareil après l'activation du Wi-Fi. Assurez-vous que le segment IP de 'appareil et celui de l'ordinateur sont . Pour plus d'informations, reportez-vous à la section ***Définir les paramètres Wi-Fi*** .

Saisissez l'adresse IP de l'appareil dans la barre d'adresse du navigateur mobile et appuyez sur **Entrée** pour accéder à la page de connexion.

Saisissez le nom d'utilisateur et le mot de passe de l'appareil. Cliquez sur **Connexion**.

## 8.2 Recherche d'un événement

Cliquez sur **Recherche** pour accéder à la page de recherche.

Saisissez les conditions de recherche, notamment l'ID de l'employé, le nom, le numéro de carte, l'heure de début et l'heure de fin, puis cliquez sur **Rechercher**.

**Note**

Prise en charge de la recherche de noms comportant moins de 32 chiffres.

Les résultats s'affichent dans la liste.

## 8.3 Gestion des utilisateurs

Vous pouvez ajouter, modifier, supprimer et rechercher des utilisateurs via un navigateur Web mobile.

**Étapes**

1. Appuyez sur **Utilisateur** pour accéder à la page des paramètres.
2. Ajouter un utilisateur.
   1) Tapez sur .**+**

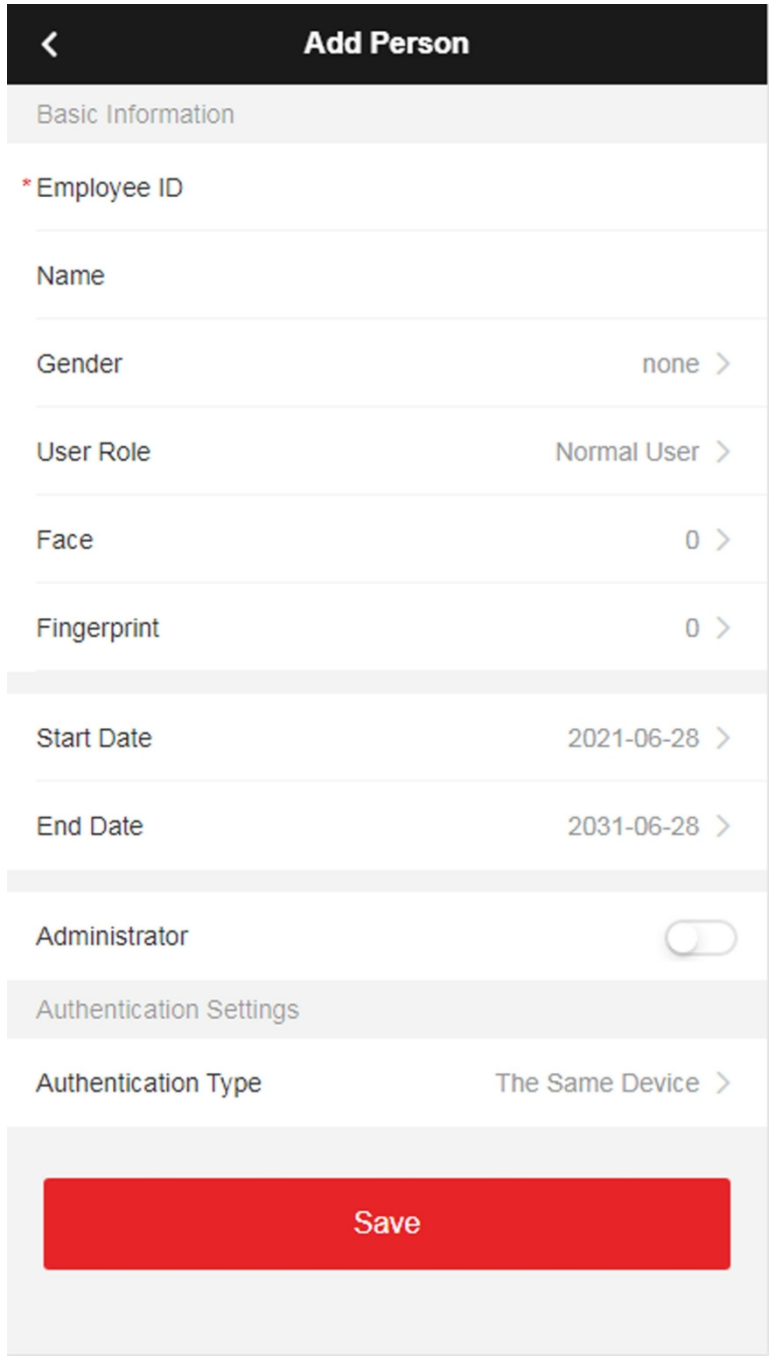



**Figure 8-1 Ajouter un utilisateur**

2) Définissez les paramètres suivants.

**ID de l'employé**

Saisissez l'ID de l'employé. L'ID de l'employé ne peut pas être 0 ou dépasser 32 caractères. Il peut s'agir d'combinaison de lettres majuscules et minuscules et de chiffres.

**Nom**

Saisissez votre nom. Le nom peut contenir des chiffres, des majuscules, des minuscules et des caractères. Il est recommandé de ne pas dépasser 32 caractères.

**Rôle de l'utilisateur**

Sélectionnez votre rôle d'utilisateur.

**N° d'étage / N° de pièce**

Entrez le numéro d'étage/de chambre.

**Visage**

Ajoutez une photo de visage. Appuyez sur **Visage**, puis **surImporter** et sélectionnez le mode d'importation du visage.

**Empreinte digitale**

Ajouter une empreinte digitale. Appuyez sur **Empreinte digitale**, puis sur**+** , et ajoutez une empreinte digitale via le module d'empreintes digitales.

**Date de début/Date de fin**

Définir **la date de début** et la **date de fin de** l'autorisation de l'utilisateur.

**Administrateur**

Si l'utilisateur doit être défini comme administrateur, vous pouvez activer l'option **Administrateur**.

**Type d'authentification**

Définir le type d'authentification.

3) Appuyez sur **Enregistrer**.

**3.** Appuyez sur l'utilisateur qui doit être modifié dans la liste des utilisateurs pour modifier les informations.

**4.** Appuyez sur l'utilisateur à supprimer dans la liste des utilisateurs et appuyez sur pour supprimer l'utilisateur.

**5.** Vous pouvez rechercher l'utilisateur en saisissant l'ID ou le nom de l'employé dans la barre de recherche.

## 8.4 Configuration

### 8.4.1 Afficher les informations sur l'appareil

Affichez le nom de l'appareil, la langue, le modèle, le numéro de série, le code QR, la version, etc.

Appuyez sur **Configuration→ Système→ Paramètres du système→ Informations de base** pour accéder à la page de configuration.

Vous pouvez afficher le nom de l'appareil, la langue, le modèle, le numéro de série, le code QR, la version, etc.

### 8.4.2 Réglages de l'heure

Permet de régler le fuseau horaire, le mode de synchronisation de l'heure et l'heure affichée.

Appuyez sur **Configuration→ Système→ Paramètres du système→ Paramètres de l'heure** pour accéder à la page des paramètres.

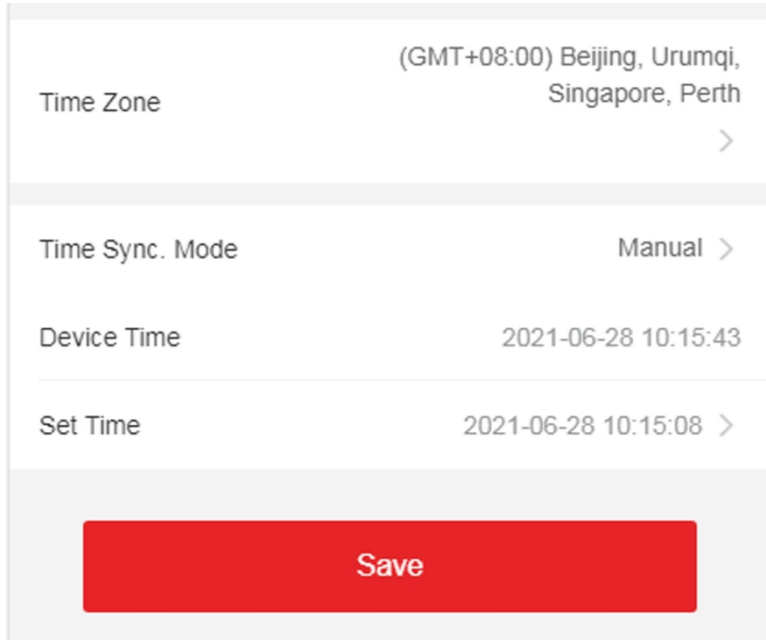



**Figure 8-2 Paramètres de temps**

Appuyez sur **Enregistrer** pour sauvegarder les paramètres.

**Fuseau horaire**

Sélectionnez le fuseau horaire où se trouve l'appareil dans la liste déroulante.

**Synchronisation du temps**

**Mode manuel**

Par défaut, l'heure de l'appareil doit être synchronisée manuellement. Vous pouvez régler l'heure de l'appareil manuellement.

**NTP**

Définissez l'adresse IP, le numéro de port et l'intervalle du serveur NTP.

### 8.4.3 Voir la licence du logiciel libre

Appuyez sur **Configuration→ Système→ Paramètres du système→ À propos**, et appuyez sur **Afficher les licences** pour afficher licence de l'appareil.

### 8.4.4 Paramètres du réseau

Vous pouvez définir les paramètres du port et du Wi-Fi.

## Paramètres du port

Vous pouvez définir les paramètres HTTP, RTSP, HTTPS et Serveur en fonction des besoins réels lors de l'accès à l'appareil via le réseau.

Appuyez sur **Configuration→ Réseau→ Paramètres de base→ Port** , pour accéder à la page des paramètres.

**HTTP**

Il s'agit du port par lequel le navigateur accède à l'appareil. Par exemple, lorsque le port HTTP est modifié en 81, vous devez saisir ***http://192.0.0.65:81*** dans le navigateur pour vous connecter.

**RTSP**

Il s'agit du port du protocole de diffusion en temps réel.

**HTTPS**

Définissez le protocole HTTPS pour l'accès au navigateur. Un certificat est requis lors de l'accès.

**Serveur**

Il s'agit du port par lequel le client ajoute l'appareil.

## Définir les paramètres Wi-Fi

Définissez les paramètres Wi-Fi pour la connexion sans fil de l'appareil.

**Étapes**

**Note**

La fonction doit être prise en charge par l'appareil.

1. Appuyez sur **Configuration→ Réseau→ Paramètres de base→ Wi-Fi** pour accéder à la page des paramètres.
2. Cochez **Activer le Wi-Fi**.

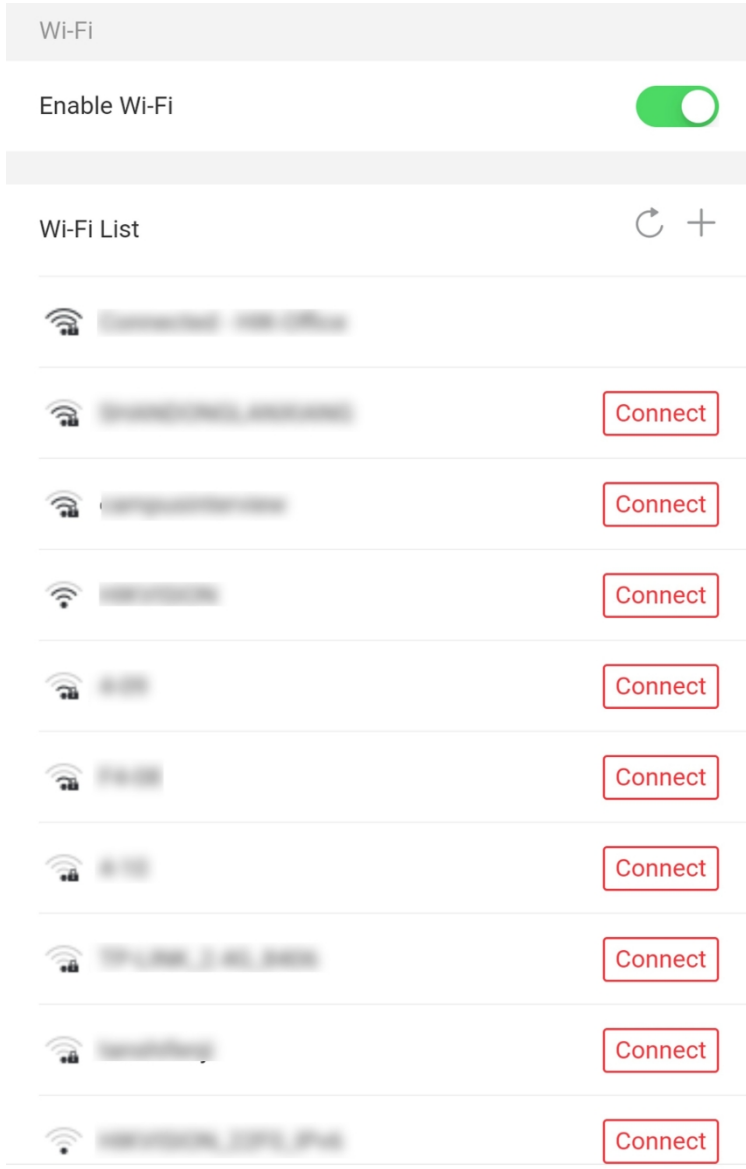



**Figure 8-3 Wi-Fi**

**3.** Ajouter le Wi-Fi.

1) Tapez sur .**+**

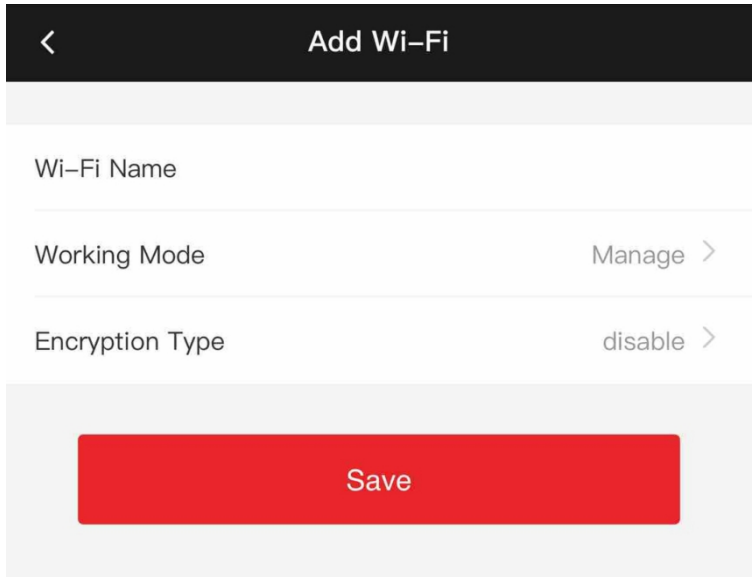



**Figure 8-4 Ajouter un Wi-Fi**

2) Saisissez le **nom** et le **mot de passe Wi-Fi**, puis sélectionnez le **mode de travail** et le **type de cryptage**.
3) Appuyez sur **Enregistrer**.

**4.** Sélectionnez le nom Wi-Fi, puis appuyez sur **Connecter**.

**5.** Saisissez le mot de passe et appuyez sur **Enregistrer**.

**6.** Définir les paramètres WLAN.
1) Définissez l'adresse IP, le masque de sous-réseau et la passerelle. Ou activez DHCP et le système attribuera automatiquement l'adresse IP, le masque de sous-réseau et la passerelle.
2) Appuyez sur **Enregistrer**.

### 8.4.5 Paramètres généraux

#### Paramètres d'authentification

Définir les paramètres d'authentification.

**Étapes**

**1.** Appuyez sur **Configuration → Paramètres généraux→ Paramètres d'authentification** .

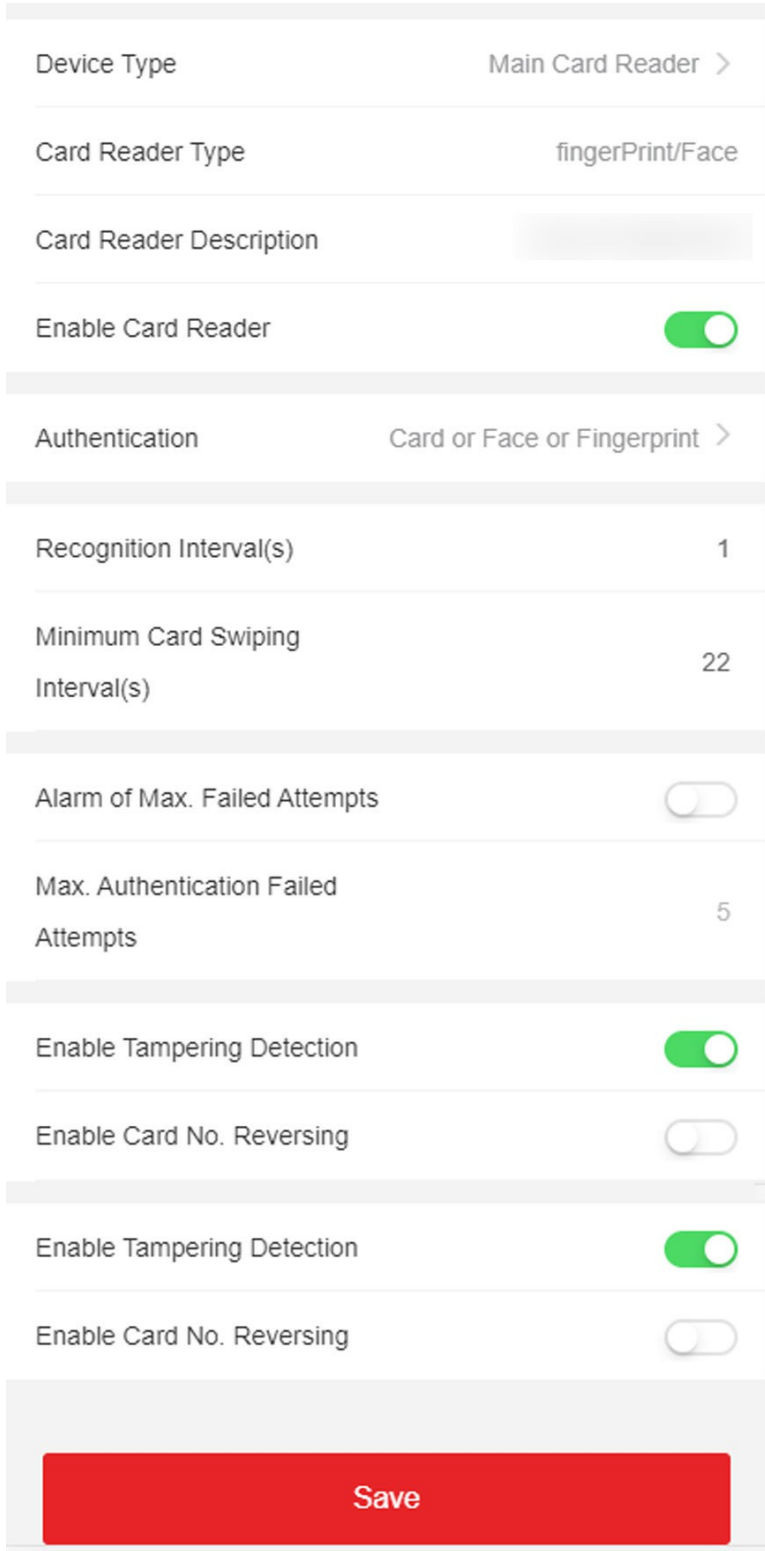



**Figure 8-5 Paramètres d'authentification**

**2.** Appuyez sur **Enregistrer**.

**Type d'appareil**

**Lecteur de carte principal**

Vous pouvez configurer les paramètres du lecteur de cartes de l'appareil. Si vous sélectionnez le lecteur de cartes principal, vous devez configurer les paramètres suivants : **Type de lecteur de cartes**, **Description du lecteur de cartes**, **Activation du lecteur de cartes**, **Authentification**, **Intervalle de reconnaissance (s)**, **Intervalle minimum de glissement de la carte (s)**, Alarme des tentatives d'échec d'**authentification max. Alarme de tentatives d'authentification échouées/Alarme de tentatives d'authentification échouées max. tentatives d'authentification échouées**, **activation de la détection de sabotage** et **activation de l'inversion du numéro de carte**.

**Lecteur de sous-cartes**

Vous pouvez configurer les paramètres du lecteur de cartes périphérique connecté. Si vous sélectionnez un sous lecteur de carte, vous devez configurer les paramètres suivants : **Type de lecteur de cartes**, **Description du lecteur de cartes**, **Activation du lecteur de cartes**, **Authentification**, **Intervalle de reconnaissance (s)**, Alarme des tentatives d'échec d'**authentification max. Alarme tentatives d'authentification échouées/Alarme tentatives d'authentification échouées max. Activer la détection de sabotage**, **Communication avec le contrôleur Tous les (s)** et **Intervalle max. de saisie du mot de passe (s) Intervalle lors de la saisie du mot de passe (s)**.

**Type de lecteur de carte**

Obtenir le type de lecteur de carte.

**Description du lecteur de cartes**

Obtenir la description du lecteur de cartes. Elle est en lecture seule.

**Activer le lecteur de cartes**

Activer la fonction du lecteur de cartes.

**Authentification**

Sélectionnez un mode d'authentification en fonction de vos besoins réels dans la liste déroulante.

**Intervalle de reconnaissance**

Si l'intervalle entre les présentations d'une même carte est inférieur à la valeur configurée, présentation de la carte n'est pas valide. La plage de temps de l'intervalle est comprise entre 0 et 255 secondes (lorsque la valeur est fixée à 0, cela signifie que l'intervalle de reconnaissance n'est pas activé et que la même authentification peut être utilisée pour un nombre illimité de fois).

**Intervalle d'authentification**

Vous pouvez définir l'intervalle d'authentification d'une même personne. La même personne ne peut s'authentifier qu'une seule fois dans l'intervalle configuré. Une deuxième authentification échouera.

**Alarme des tentatives d'échec d'authentification max. Alarme de tentatives d'authentification échouées/Alarme de tentatives d'authentification échouées max. Tentatives échouées**

Permet de déclencher une alarme lorsque les tentatives de lecture de la carte atteignent la valeur définie.

**Activer la détection de sabotage**

Activer la détection anti-sabotage pour le lecteur de cartes.

**Activer l'inversion du numéro de carte**

Le numéro de la carte lue sera dans l'ordre inverse après l'activation de la fonction.

**Communication avec le contrôleur Chaque (s)**

Lorsque le dispositif de contrôle d'accès ne peut pas se connecter au lecteur de cartes pendant une période plus longue que celle définie, le lecteur de cartes se déconnecte automatiquement.

**Intervalle max. Intervalle de saisie du mot de passe (s)**

Lorsque vous saisissez le mot de passe sur le lecteur de cartes, si l'intervalle entre la pression de deux chiffres est supérieur à la valeur définie, les chiffres que vous avez appuyés auparavant seront automatiquement effacés.

## Paramètres de confidentialité

Définissez le type de stockage des événements, les paramètres de téléchargement et de stockage des images, ainsi que les paramètres d'effacement des images.

Appuyez sur **Configuration→ Paramètres généraux→ Confidentialité** .

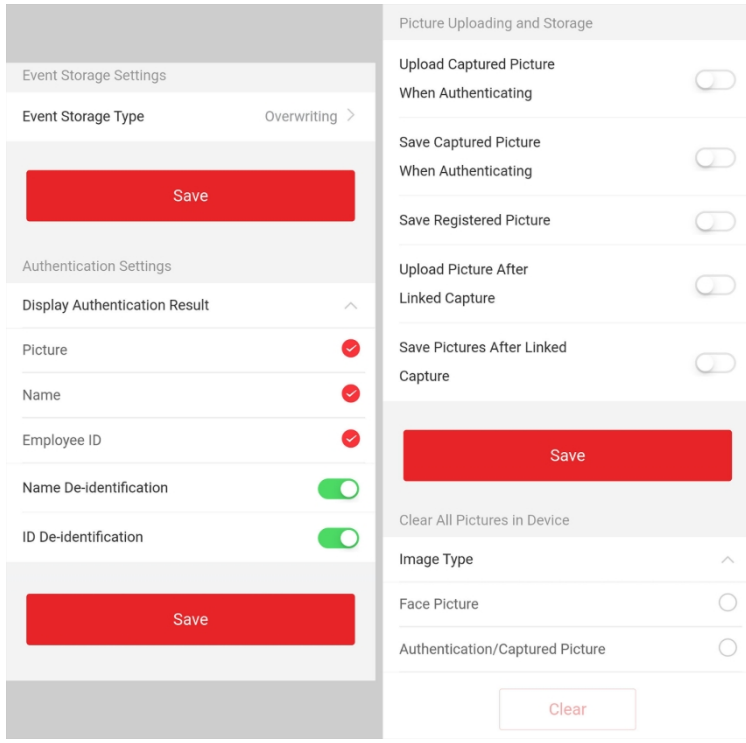



**Figure 8-6 Paramètres de confidentialité**

## Paramètres de stockage des événements

Sélectionnez une méthode pour supprimer l'événement. Vous pouvez choisir entre **Supprimer les anciens événements périodiquement**, **Supprimer les anciens événements par période spécifiée** ou **Écraser**.

**Supprimer périodiquement les anciens événements**

Entrez un nombre pour définir la période de suppression des événements. Tous les événements seront supprimés en fonction de durée configurée.

**Suppression d'anciens événements à la date spécifiée**

Définissez une heure et tous les événements seront supprimés à l'heure configurée.

**Surécriture**

Les 5 % d'événements les plus anciens sont supprimés lorsque le système détecte que les événements stockés ont dépassé 95 % de l'espace disponible.

## Paramètres d'authentification

**Afficher le résultat de l'authentification**

Vérifier la photo du visage, le nom ou l'identité de l'employé. Une fois l'authentification terminée le système affiche le contenu sélectionné dans le résultat.

**Nom Désidentification**

Les informations sur le nom sont désensibilisées par un astérisque.

**ID Désidentification**

Les informations d'identification sont désensibilisées par un astérisque.

## Téléchargement et stockage d'images

Vous pouvez télécharger et stocker des photos.

**Téléchargement d'une image capturée lors de l'authentification**

Télécharger automatiquement les photos prises lors de l'authentification sur la plateforme.

**Sauvegarde de l'image capturée lors de l'authentification**

Si vous activez cette fonction, vous pouvez enregistrer l'image lors de l'authentification à l'appareil.

**Enregistrer l'image enregistrée**

L'image du visage enregistrée sera sauvegardée dans le système si vous activez la fonction.

**Téléchargement d'une image après la capture d'un lien**

Téléchargez automatiquement sur la plateforme les images capturées par l'appareil photo relié.

**Sauvegarde des images après la capture liée**

Si vous activez cette fonction, vous pouvez enregistrer l'image capturée par l'appareil photo lié sur l'appareil.

## Effacer toutes les images de l'appareil

Vous pouvez effacer les photos de visage enregistrées et les photos prises dans l'appareil.

**Clear Registered Face Pictures (photos de la face enregistrée)**

Sélectionnez **Image de face**, puis appuyez sur **Effacer**. Toutes les photos enregistrées dans l'appareil seront supprimées.

**Authentification claire/image capturée**

Sélectionnez **Authentification/photo capturée** et appuyez sur **Effacer**. Toutes les photos d'authentification/capture présentes dans l'appareil seront supprimées.

### Définir la sécurité de la carte

Appuyez sur **Configuration→ General Settings→ Card Security** pour accéder à la page des paramètres.

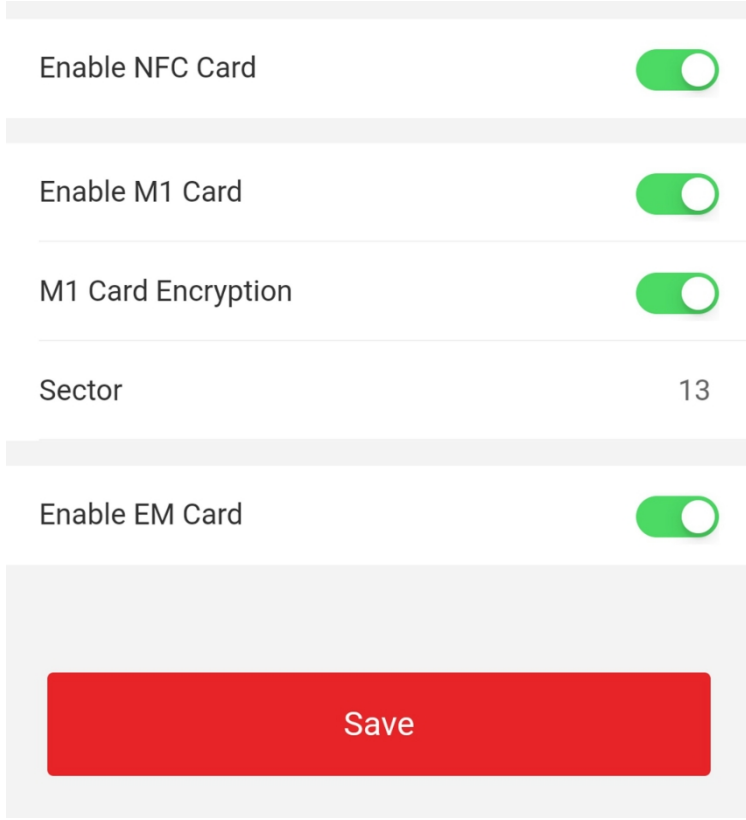



**Figure 8-7 Sécurité de la carte**

Définissez les paramètres et cliquez sur
**Enregistrer**. **Activer la carte NFC**

Afin d'empêcher le téléphone portable d'obtenir les données du contrôle d'accès, vous pouvez activer la carte NFC pour augmenter le niveau de sécurité des données.

**Activer la carte M1**

L'activation de la carte M1 et l'authentification par présentation de la carte M1 sont disponibles.

**Chiffrement de la carte M1**

Le cryptage de la carte M1 peut améliorer le niveau de sécurité de l'authentification.

**Secteur**

Activez la fonction et définissez le secteur de cryptage. Par défaut, le secteur 13 est crypté. Il est recommandé de crypter le secteur 13.

**Activer la carte EM**

L'activation de la carte EM et l'authentification par présentation de la carte EM sont disponibles.

**Note**

Si le lecteur de carte périphérique prend en charge la présentation de la carte EM, la fonction d'activation/désactivation de la fonction de carte EM est également prise en charge.

**Activer la carte CPU**

L'appareil peut lire les données de la carte CPU lorsque la fonction de carte CPU est activée.

**Carte CPU Contenu en lecture**

Après avoir activé la fonction de lecture du contenu de la carte CPU, l'appareil peut lire le contenu de la carte CPU.

**Activer la carte d'identité**

L'activation de la carte d'identité et l'authentification par la présentation de la carte d'identité sont disponibles.

### Définir les paramètres d'authentification de la carte

Définissez le contenu de la lecture de la carte lors de l'authentification par carte sur l'appareil. Tapez sur **Configuration→ General Settings→ Card Authentication Settings** .

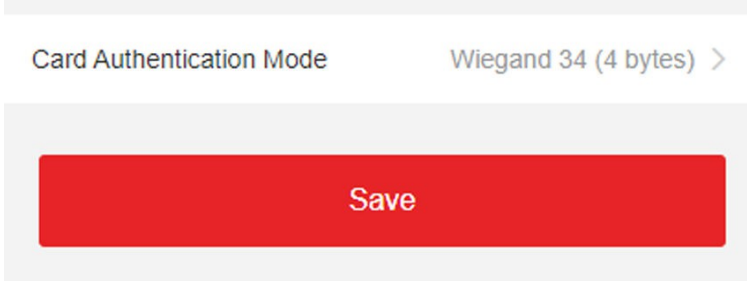



**Figure 8-8 Page d'authentification de la carte**

Sélectionnez un mode d'authentification de la carte et appuyez sur **Enregistrer**. **N° de carte complet**

Tous les numéros de carte seront lus.

**Wiegand 26 (3 octets)**

L'appareil lira la carte via le protocole Wiegand 26 (lecture de 3 octets).

**Wiegand 34 (4 octets)**

L'appareil lira la carte via le protocole Wiegand 34 (lecture de 4 octets).

## 8.4.6 Paramètres du visage

Régler les paramètres du visage.

## Paramètres du visage

Tapez sur **Configuration→ Smart→ Intelligent Parameter** .

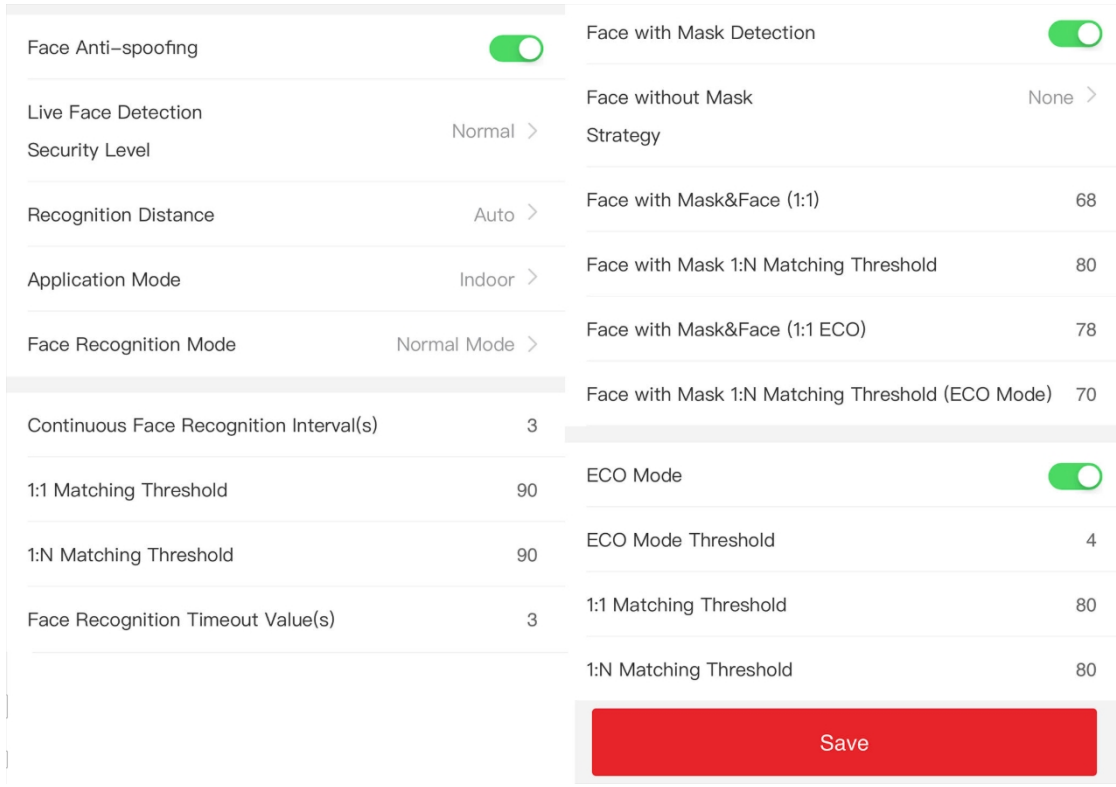



**Figure 8-9 Paramètres de la face**

**Note**

Les fonctions varient selon les modèles. Pour plus de détails, se référer à l'appareil lui-même.

Régler les paramètres de la face.

**Anti-usurpation de visage**

Active ou désactive la fonction de détection des visages vivants. Si cette fonction est activée, l'appareil peut reconnaître si la personne est vivante ou non.

**Détection des visages en direct Niveau de sécurité**

Après avoir activé la fonction anti-falsification des visages, vous pouvez définir le niveau de sécurité correspondant lors de l'authentification des visages en direct.

**Distance de reconnaissance**

Sélectionnez la distance entre l'utilisateur qui s'authentifie et la caméra de l'appareil.

**Mode d'application**

Sélectionnez **Intérieur** ou **Autres** en fonction de l'environnement réel. Dans une scène extérieure, une scène intérieure près d'une fenêtre ou un mauvais environnement, vous pouvez choisir **Autres.**

**Note**

Si l'appareil n'est pas activé par d'autres outils, il utilise par défaut l'intérieur comme mode d'environnement.

**Mode reconnaissance des visages Mode normal**

L'appareil utilise une caméra pour effectuer la reconnaissance faciale.

**Mode profond**

Il s'applique à des environnements plus complexes et l'éventail des personnes reconnues est plus large.

**Note**

- Les deux modes ne sont pas compatibles l'un avec l'autre. Ne changez pas de mode une fois qu'il est sélectionné. Si vous changez de mode, toutes les photos de visage du mode précédent seront effacées.
- En mode approfondi, vous pouvez ajouter des photos de visage uniquement via la fonction d'ajout d'utilisateur de 'appareil ou de la station d'inscription. Il n'est pas possible d'ajouter des photos de visage via l'importation d'images.

L'appareil utilise une caméra pour effectuer la reconnaissance faciale.

**Intervalle de reconnaissance continue des visages (s)**

Définir l'intervalle de temps entre deux reconnaissances continues du visage lors de l'authentification.

**Note**

Plage de valeurs : 1 à 10.

**Seuil de correspondance 1:1**

Définit le seuil de correspondance lors de l'authentification en mode de correspondance 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est important.

**Seuil de correspondance 1:N**

Définir le seuil de correspondance lors de l'authentification en mode de correspondance 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est important. La valeur maximale est de 100.

**Valeur du délai de reconnaissance des visages (s)**

Configurez le délai d'attente pour la reconnaissance des visages. Si le temps de reconnaissance des visages dépasse la valeur configurée, l'appareil demande un délai d'attente pour la reconnaissance des visages.

**Détection de visage avec masque**

Après avoir activé la détection de visage avec masque, le système reconnaîtra le visage capturé avec l'image du masque. Vous pouvez définir le seuil de correspondance visage avec masque1:N, le mode ECO et la stratégie.

**Aucun**

Si la personne ne porte pas de masque facial lors de l'authentification, l'appareil n' pas de notification.

**Rappel du port**

Si la personne ne porte pas de masque facial lors de l'authentification, l'appareil émet une notification et la porte s'ouvre.

**Must Wear**

Si la personne ne porte pas de masque facial lors de l'authentification, le dispositif émet une notification et la porte reste fermée.

**Visage avec masque et visage (1:1)**

Définir la valeur de correspondance lors de l'authentification par masque facial en mode de correspondance 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.

**Visage avec masque Seuil de correspondance 1:N**

Définir le seuil de correspondance lors de l'authentification par masque facial en mode de correspondance 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est important.

**Face avec Mask & Face (1:1 ECO)**

Définir la valeur de correspondance lors de l'authentification avec un masque facial en mode ECO 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.

**Visage avec masque Seuil de correspondance 1:N (mode ECO)**

Définir le seuil de correspondance lors de l'authentification avec un masque facial via le mode ECO 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.

**Mode ECO**

Après avoir activé le mode ECO, l'appareil utilisera la caméra IR pour authentifier les visages dans un environnement sombre ou faiblement éclairé. Vous pouvez définir le seuil du mode ECO, le mode ECO (seuil de correspondance 1:1) et le mode ECO (seuil de correspondance 1:N).

**Seuil du mode ECO**

Définir le seuil de correspondance lors de l'authentification via le mode ECO 1:1 et le mode ECO 1:N.

**Seuil de correspondance 1:1**

Définir le seuil de correspondance lors de l'authentification en mode ECO 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.

**Seuil de correspondance 1:N**

Définir le seuil de correspondance lors de l'authentification en mode ECO 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé. La valeur maximale est de 100.

### Définir la zone de reconnaissance

Tapez sur **Configuration→ Smart→ Area Configuration** pour accéder à la page.
Faites glisser le cadre bleu dans la vidéo en direct pour ajuster la zone de reconnaissance. Seul le visage situé dans cette zone peut être reconnu par le système.
Faites glisser le curseur pour configurer la zone efficace de la reconnaissance faciale. Appuyez sur **Enregistrer** pour sauvegarder les paramètres.

## 8.4.7 Paramètres de l'interphone vidéo

### Définir l'ID de l'appareil

L'appareil peut être utilisé comme poste de porte, poste de porte extérieur ou dispositif de contrôle d'accès. Vous devez définir l'ID de l'appareil avant de l'utiliser.

### Paramètres de l'identifiant de l'appareil

Appuyez sur **Configuration→ Intercom→ Device ID Settings** .
Si vous définissez le type d'appareil comme **Poste de Porte** ou **Dispositif de Contrôle d'Accès**, vous pouvez définir le N° d'étage et le N° de poste de porte.
Appuyez sur **Enregistrer** pour sauvegarder les paramètres après la configuration.

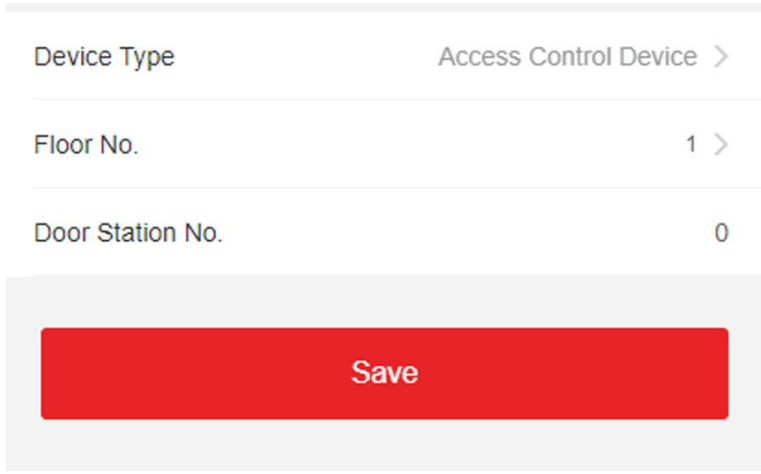



**Figure 8-10 Paramètres d'identification de l'appareil (poste de porte)**

**Type d'appareil**

Le dispositif peut être utilisé comme poste de porte, poste de porte extérieur ou dispositif de contrôle d'accès. Sélectionnez un type de dispositif dans la liste déroulante.

**Note**

Si vous modifiez le type d'appareil, vous devez redémarrer l'appareil.

**N° d'étage**

Définir le numéro d'étage du dispositif installé.

**Numéro de la station de porte**

Définir le numéro d'étage du dispositif installé.

**Note**

Si vous modifiez le numéro, vous devez redémarrer l'appareil.

Si vous définissez le type d'appareil comme **Poste de Porte Extérieur**, vous pouvez définir le N° de poste de porte extérieur.

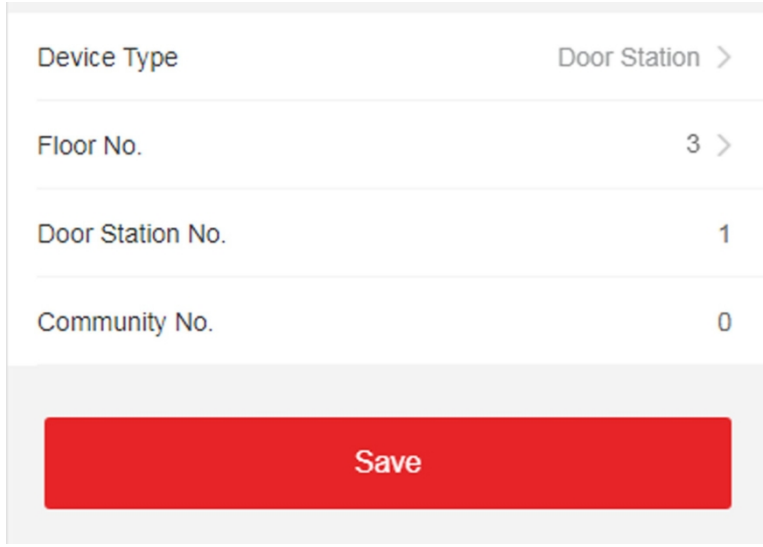



**Figure 8-11 Paramètres d'identification du dispositif (poste de porte extérieur)**

**Porte extérieure Poste n°.**

Si vous sélectionnez la station de porte extérieure comme type d'appareil, vous devez saisir un numéro entre **1** et **99**.

**Note**

Si vous modifiez le numéro, vous devez redémarrer l'appareil.

## Configuration des paramètres SIP

Définissez l'adresse IP du dispositif et l'adresse IP du serveur SIP. Après avoir défini les paramètres, vous pouvez communiquer entre le dispositif de contrôle d'accès, le poste de porte, le poste intérieur, le poste principal et la plate-forme.

**Note**

Seul le dispositif de contrôle d'accès et d'autres dispositifs ou systèmes (tels que le poste de porte, le poste intérieur, le poste principal, la plate-forme) se trouvent dans le même segment IP, et l'audio bidirectionnelle peut être réalisée.

Appuyez sur **Configuration→ Intercom→ Paramètres du réseau lié** .

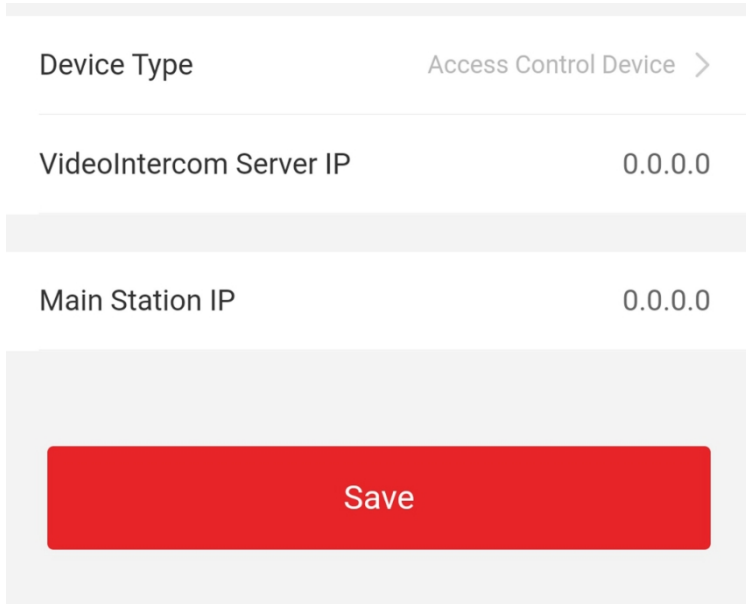



**Figure 8-12 Paramètres du réseau lié**

Définissez l'IP du serveur d'interphone vidéo et l'IP de la station principale. Appuyez sur **Enregistrer**.

### Appuyer sur le bouton pour appeler

**Étapes**

1. Appuyez sur **Configuration→ Intercom→ Appuyez sur le bouton pour appeler** pour accéder à la page des paramètres.
2. Définissez le bouton à appeler.
   - Cochez **Appeler poste intérieur** et définissez le poste intérieur Non pour définir le bouton d'appel du poste intérieur.
   - Cochez **Centre de gestion des** appels pour définir le bouton sur le centre de gestion des appels.

## 8.4.8 Paramètres de contrôle d'accès

### Paramètres de la porte

**Configuration du** robinet→ **Contrôle d'accès→ Paramètres de la porte** .

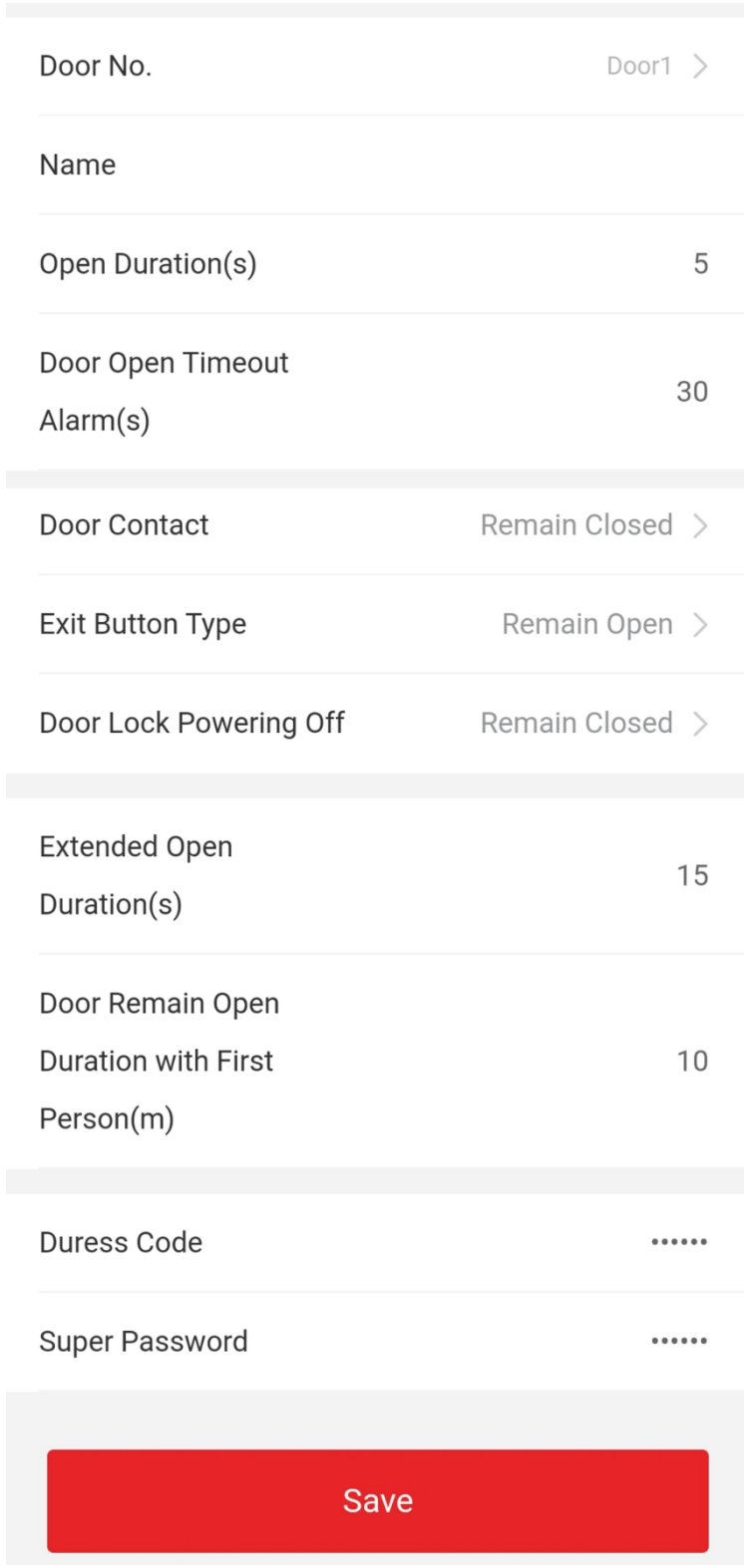



**Figure 8-13 Page de configuration des paramètres de la porte**

Cliquez sur **Enregistrer** pour sauvegarder les paramètres après la configuration.

**N° de porte**

Sélectionnez l'appareil correspondant à la porte No.

**Nom**

Vous pouvez créer un nom pour la porte.

**Ouvert Durée**

Régler la durée de déverrouillage de la porte. Si la porte n'est pas ouverte pendant la durée programmée, elle est verrouillée.

**Alarme de délai d'ouverture de la porte**

Une alarme est déclenchée si la porte n'a pas été fermée pendant la durée configurée.

**Contact de porte**

Vous pouvez définir le contact de porte comme **restant ouvert** ou **restant fermé** en fonction de vos besoins réels. Par défaut, le contact **reste fermé**.

**Type de bouton de sortie**

Vous pouvez définir le bouton de sortie comme **restant ouvert** ou **restant fermé** en fonction de vos besoins réels. Par défaut, il **reste ouvert**.

**État de la mise hors tension de la serrure de porte**

Vous pouvez définir l'état de la serrure de porte lorsque celle-ci est hors tension. Par défaut, l'état **reste fermé**.

**Durée d'ouverture prolongée**

Le contact de porte peut être activé avec un délai approprié après que la personne ayant des besoins d'accès étendus a glissé sa carte.

**Durée de la porte restée ouverte avec la première personne**

Définir la durée d'ouverture de la porte lorsque la première personne entre. Une fois que la première personne est autorisée, plusieurs personnes peuvent accéder à la porte ou à d'autres actions d'authentification.

**Code de contrainte**

En cas de contrainte, la porte peut s'ouvrir en entrant le code de contrainte. En même temps, le client peut signaler l'événement de contrainte.

**Super mot de passe**

La personne concernée peut ouvrir la porte en saisissant le super mot de passe.

**Note**

Le code de contrainte et le super code doivent être différents. Les chiffres vont de 4 à 8.

## Réglage des paramètres RS-485

Vous pouvez définir les paramètres RS-485, notamment le périphérique, l'adresse, le débit en bauds, etc.

**Configuration du** robinet→ **Contrôle d'accès→ RS-485** .

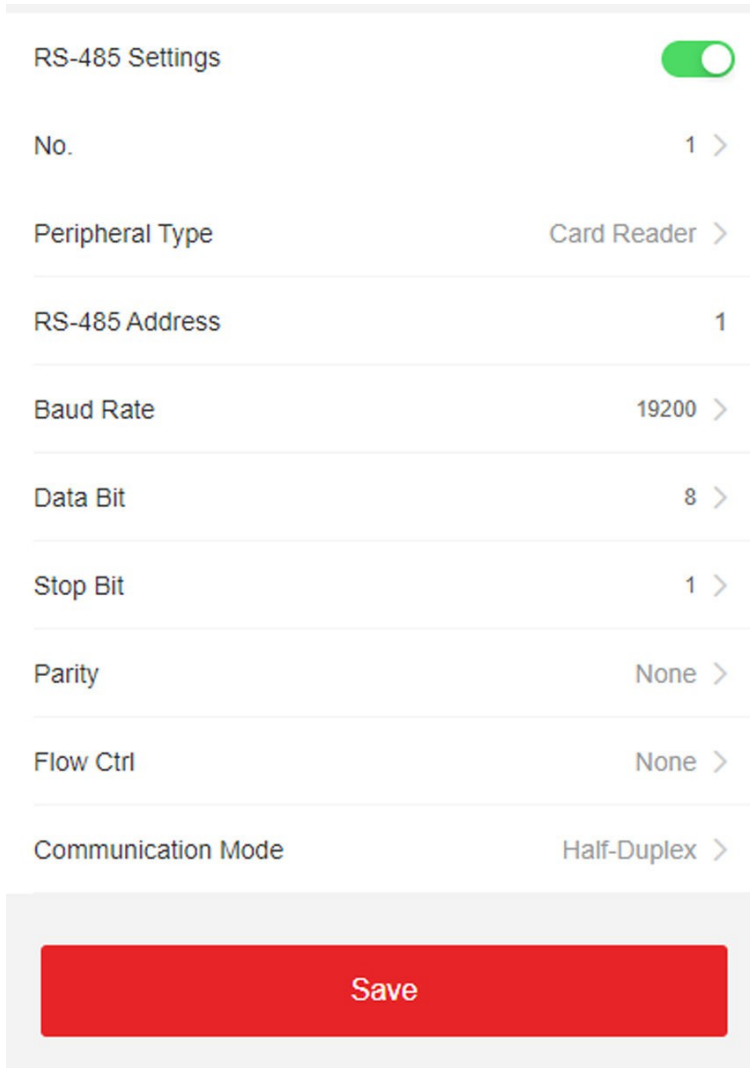



**Figure 8-14 Page RS-485**

Appuyez sur **Enregistrer** pour sauvegarder les paramètres après la configuration.

**Type de périphérique**

Sélectionnez un périphérique dans la liste déroulante en fonction de la réelle. Vous pouvez choisir entre Lecteur **de cartes**, **module d'extension** ou **contrôleur d'accès.**

**Note**

Une fois le périphérique modifié et enregistré, l'appareil redémarre automatiquement.

**Adresse RS-485**

Réglez l'adresse RS-485 en fonction de vos besoins réels.

**Note**

Si vous sélectionnez **Contrôleur d'accès** : Si vous connectez l'appareil à un terminal via l'interface RS-485, réglez l'adresse RS-485 sur 2. Si vous connectez l'appareil à un contrôleur, réglez l'adresse RS-485 en fonction du numéro de porte.

**Débit en bauds**

La vitesse de transmission lorsque les appareils communiquent via le protocole RS-485.

**Bit de données**

Le bit de données lorsque les appareils communiquent via le protocole RS-485.

**Bit d'arrêt**

Le bit d'arrêt lorsque les appareils communiquent via le protocole RS-485.

**Parité/Contrôle de flux/Mode de communication**

Activé par défaut.

## Paramètres Wiegand

Vous pouvez définir la direction de la transmission Wiegand.

**Étapes**

1. Appuyez sur **Configuration→ Contrôle d'accès→ Paramètres Wiegand** .

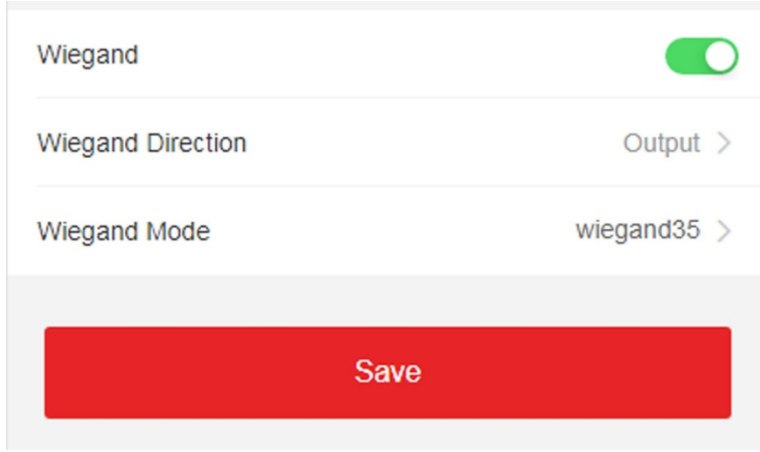



**Figure 8-15 Page Wiegand**

2. Activer **Wiegand** pour activer la fonction Wiegand.
3. Définir un sens de transmission.

   **Sortie**

   Il est possible de connecter un contrôleur d'accès externe. Les deux appareils transmettront le numéro de carte via Wiegand 26 ou 34.
4. Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

**Note**

Si vous changez de périphérique, et après avoir sauvegardé les paramètres de l'appareil, ce dernier redémarre automatiquement.

# Chapitre 9 Fonctionnement via le navigateur Web

## 9.1 Connexion

Vous pouvez vous connecter via le navigateur web ou la configuration à distance du logiciel client.

**Note**

Assurez-vous que l'appareil est activé. Pour plus d'informations sur l'activation, voir ***Activation***.

### Connexion via le navigateur Web

Saisissez l'adresse IP de l'appareil dans la barre d'adresse du navigateur web et appuyez sur **Entrée** pour accéder à page de connexion.

**Note**

Assurez-vous que l'adresse IP commence par "Https :".

Saisissez le nom d'utilisateur et le mot de passe de l'appareil. Cliquez sur **Connexion**.

### Connexion via la configuration à distance du logiciel client

Téléchargez et ouvrez le logiciel client. Après avoir ajouté l'appareil, cliquez sur pour accéder à la page de configuration.

## 9.2 Vue en direct

Vous pouvez visualiser la vidéo en direct de l'appareil.

Après avoir ouvert une , vous accédez à la page d'affichage en direct. Vous pouvez effectuer l'affichage en direct, la capture, l'enregistrement vidéo et d'autres opérations.

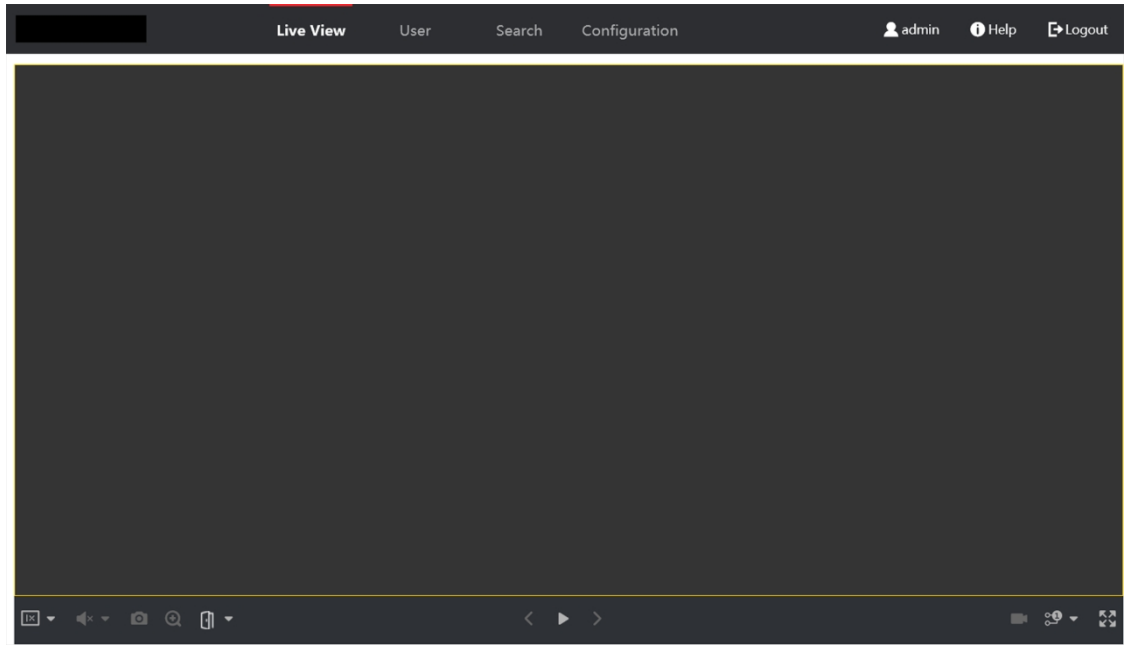



**Figure 9-1 Page Live View**

Description des fonctions :

Sélectionner la taille de l'image au début de la visualisation en direct. Régler le volume au début de la visualisation en direct.

**Note**

Si vous réglez le volume lors du démarrage de l'audio bidirectionnel, il se peut que vous entendiez des sons répétés.

Vous pouvez capturer une image lors du démarrage de la vue en direct. Fonction réservée. Vous pouvez zoomer sur l'image en direct. Démarrer ou arrêter la visualisation en direct.

Démarrer ou arrêter l'enregistrement vidéo.

Sélectionnez le type de diffusion lors du démarrage de l'affichage en direct. Vous pouvez choisir entre le flux principal et flux secondaire.

Vue plein écran.

## 9.3 Gestion des personnes

Cliquez et ajoutez les informations de la personne, y compris les informations de base, la carte, le mode d'authentification et la photo.

Cliquez sur **OK** pour enregistrer la personne.

### Ajouter des informations de base

Cliquez sur **User→ Add** pour accéder à la page Add Person.
Ajoutez les informations de base de la personne, y compris l'ID de l'employé, le nom de la personne, le niveau de l'utilisateur, le numéro de l'étage et le numéro de la chambre.

Cliquez sur **OK** pour enregistrer les paramètres.

### Ajouter une carte

Cliquez sur **User→ Add** pour accéder à la page Add Person. Cliquez sur **Ajouter une carte** et saisissez un numéro de carte.

Cliquez sur **OK** pour enregistrer les paramètres.

### Ajouter une photo de face

Cliquez sur **User→ Add** pour accéder à la page Add Person.

Cliquez sur**+** à droite pour télécharger une photo de votre visage à partir de votre PC local.

**Note**

Le format de l'image doit être JPG, JPEG ou PNG. La taille doit être inférieure à 200K.

Cliquez sur **OK** pour enregistrer les paramètres.

### Définir le délai d'autorisation

Cliquez sur **User→ Add** pour accéder à la page Add Person. Définissez l'**heure de début** et l'**heure de fin**.

Cliquez sur **OK** pour enregistrer les paramètres.

### Définir le contrôle d'accès

Cliquez sur **User→ Add** pour accéder à la page Add Person.
Après avoir coché la case **Administrateur** dans **Contrôle d'accès**, la personne ajoutée peut se connecter en 'authentifiant. Vous pouvez cliquer sur **Ajouter** pour saisir le **numéro d'étage** et le **numéro de salle** du contrôle d'accès, et cliquer sur pour supprimer. Cliquez sur **OK** pour enregistrer les paramètres.

### Ajouter un mode d'authentification

Cliquez sur **User→ Add** pour accéder à la page Add Person. Définissez le type d'authentification.

Cliquez sur **OK** pour enregistrer les paramètres.

## 9.4 Recherche d'un événement

Cliquez sur **Recherche** pour accéder à la page de recherche.

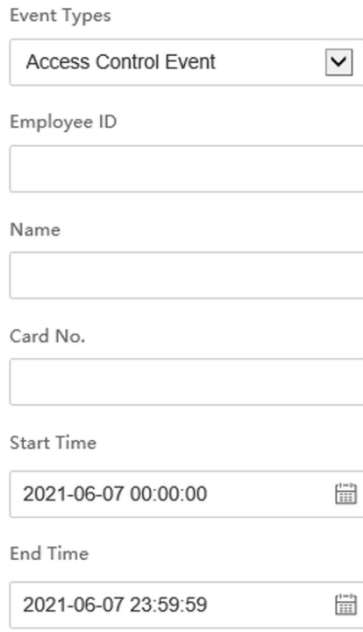



**Figure 9-2 Page de recherche**

Saisissez les conditions de recherche, notamment l'ID de l'employé, le nom, le numéro de carte, l'heure de début et l'heure de fin, puis cliquez sur **Rechercher**.

Les résultats s'affichent dans le panneau de droite.

## 9.5 Configuration

### 9.5.1 Paramètres locaux

Réglez les paramètres de l'affichage en direct, le chemin d'enregistrement du fichier d'enregistrement et le chemin d'enregistrement des images capturées.

#### Régler les paramètres de Live View

Cliquez sur **Configuration→ Local** pour accéder à la page Local. Configurez le type de flux, la performance de lecture, le démarrage automatique de l'affichage en direct et le format d'image, puis cliquez sur **Enregistrer**.

### Définir le chemin d'enregistrement du fichier d'enregistrement

Cliquez sur **Configuration→ Local** pour accéder à la page Local. Sélectionnez une taille de fichier d'enregistrement et un chemin d'enregistrement à partir de votre ordinateur local, puis cliquez sur **Enregistrer**.

Vous pouvez également cliquer sur **Ouvrir** pour ouvrir le dossier du fichier afin d'en visualiser les détails.

### Définir le chemin d'enregistrement des images capturées

Cliquez sur **Configuration→ Local** pour accéder à la page Local. Sélectionnez un chemin d'enregistrement à partir de votre ordinateur local et cliquez sur **Enregistrer**.

Vous pouvez également cliquer sur **Ouvrir** pour ouvrir le dossier du fichier afin d'en visualiser les détails.

## 9.5.2 Afficher les informations sur l'appareil

Affichez le nom de l'appareil, la langue, le modèle, le numéro de série, le code QR, la version, le nombre de canaux, l'entrée d'alarme, la sortie d'alarme, le verrouillage et le RS-485, la capacité de l'appareil, etc.

Cliquez sur **Configuration→ System→ System Settings→ Basic Information** pour accéder à la page de configuration.

Vous pouvez visualiser le nom de l'appareil, la langue, le modèle, le numéro de série, le code QR, la version, le nombre de canaux, l'entrée d'alarme, la sortie d'alarme, le verrouillage et le RS-485, la capacité de l'appareil, etc.

## 9.5.3 Temps de réglage

Définissez le fuseau horaire de l'appareil, le mode de synchronisation et l'heure de l'appareil. Cliquez sur **Configuration → Système → Paramètres du système → Paramètres de l'heure** .

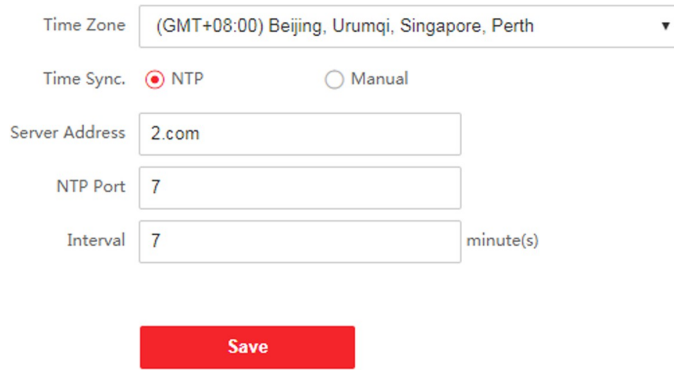



**Figure 9-3 Réglages de l'heure**

Cliquez sur **Enregistrer** pour sauvegarder les paramètres après la configuration.

**Fuseau horaire**

Sélectionnez le fuseau horaire de l'appareil dans la liste déroulante.

**Synchronisation du temps.**

**NTP**

Vous devez définir l'adresse IP, le numéro de port et l'intervalle du serveur NTP.

**Manuel**

Par défaut, l'heure de l'appareil doit être synchronisée manuellement. Vous pouvez régler l'heure de l'appareil manuellement ou cocher la case **Sync. avec l'heure de l'ordinateur** pour synchroniser l'heure de l'appareil avec celle de l'ordinateur.

### 9.5.4 Régler l'heure d'été

**Étapes**

1. Cliquez sur **Configuration→ System→ System Settings→ DST** .

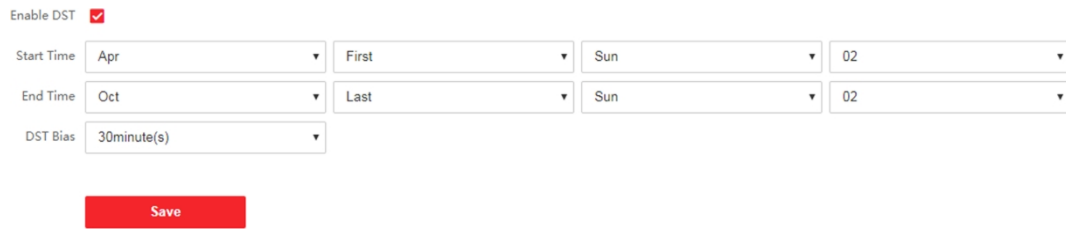



**Figure 9-4 Page DST**

2. Cochez **Activer DST**.
3. Réglez l'heure de début, l'heure de fin et l'heure de polarisation de l'heure d'été.
4. Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

### 9.5.5 Voir la licence du logiciel libre

Allez sur **Configuration→ System→ System Settings→ About** , et cliquez sur **View Licenses** pour afficher la licence de l'appareil.

### 9.5.6 Mise à niveau et maintenance

Redémarrer l'appareil, restaurer les paramètres de l'appareil et mettre à jour la version de l'appareil.

#### Redémarrer l'appareil

Cliquez sur **Configuration→ Système→ Maintenance→ Mise à niveau et maintenance** .

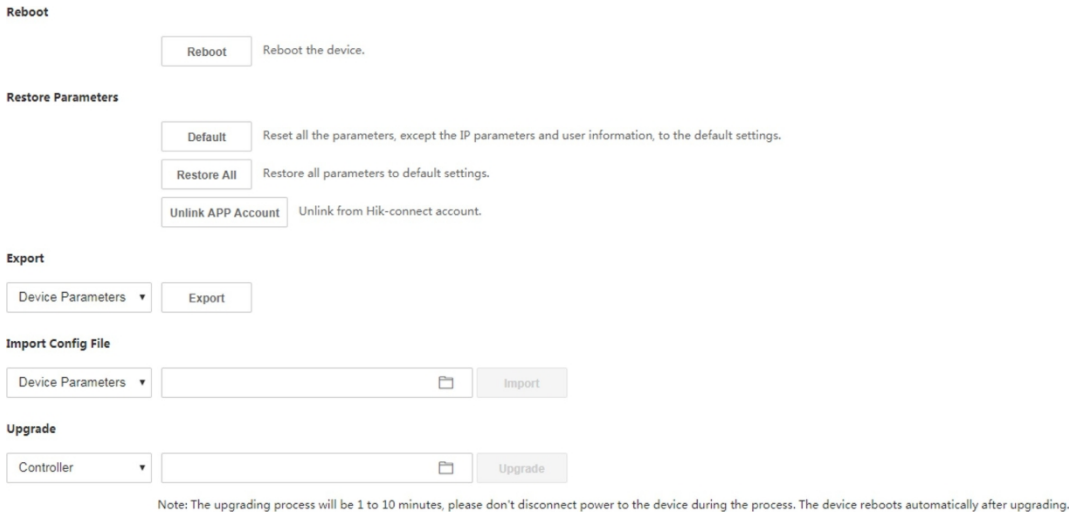



**Figure 9-5 Page de mise à niveau et de maintenance**

Cliquez sur **Redémarrer** pour lancer le redémarrage de l'appareil.

## Restaurer les paramètres

Cliquez sur **Configuration→ Système→ Maintenance→ Mise à niveau et maintenance** .

**Restaurer tout**

Tous les paramètres seront rétablis aux réglages d'usine. Vous devez activer l'appareil avant de l'utiliser.

**Défaut**

L'appareil rétablit les paramètres par défaut, à l'exception de l'adresse IP de l'appareil et des informations sur l'utilisateur.

**Débrancher le compte APP**

Déconnecter le compte Hik-Connect de la plateforme.

## Paramètres d'importation et d'exportation

Cliquez sur **Configuration→ Système→ Maintenance→ Mise à niveau et maintenance** .

**Exportation**

Cliquez sur **Exporter** pour exporter les journaux ou les paramètres de l'appareil.

**Note**

Vous pouvez importer les paramètres exportés vers un autre appareil.

**Importation**

Cliquez sur et sélectionnez le fichier à importer. Cliquez sur **Importer** pour lancer l'importation du fichier de configuration.

### Mise à niveau

Cliquez sur **Configuration→ Système→ Maintenance→ Mise à niveau et maintenance** .
Sélectionnez un type de mise à niveau dans la liste déroulante. Cliquez sur et sélectionnez le fichier de mise à niveau sur votre PC local. Cliquez sur **Mise à niveau** pour démarrer la mise à niveau.

**Note**
Ne pas éteindre l'appareil pendant la mise à jour.

## 9.5.7 Requête de journal

Vous pouvez rechercher et consulter les journaux de l'appareil.

Allez dans **Configuration→ System→ Maintenance→ Log Query** .

Définissez le type majeur et le type mineur du type de journal. Définissez l'heure de début et l'heure de fin de la recherche, puis cliquez sur **Rechercher**.

Les résultats s'affichent ci-dessous, y compris le numéro, l'heure, le type majeur, le type mineur, le numéro de canal, les informations sur l'utilisateur local/éloigné, l'IP de l'hôte éloigné, etc.

## 9.5.8 Paramètres du mode de sécurité

Définir le mode de sécurité pour la connexion au logiciel client.

Sur la page Device for Management, cliquez sur **Configuration→ System→ Security→ Security Service** .

Sélectionnez un mode de sécurité dans la liste déroulante et cliquez sur

**Enregistrer**. **Mode de sécurité**

Niveau de sécurité élevé pour la vérification des informations de l'utilisateur lors de la connexion au logiciel client.

**Mode compatible**

La vérification des informations de l'utilisateur est compatible avec l'ancienne version du logiciel client lors de la connexion.

**Activer SSH**

Pour améliorer la sécurité du réseau, désactivez le service SSH. La configuration ne sert qu'à déboguer l'appareil pour les professionnels.

**Activer HTTPS**

Afin d'augmenter le niveau de sécurité du réseau lors de la visite de sites web, vous pouvez activer HTTPS pour obtenir un environnement de communication réseau plus sûr et plus crypté. La communication doit être authentifiée par l'identité et le mot de passe de cryptage après l'activation de HTTPS, qui est sauvegardé.

### 9.5.9 Gestion des certificats

Il permet de gérer les certificats du serveur/client et le certificat de l'autorité de certification.

**Note**

Cette fonction n'est prise en charge que par certains modèles d'appareils.

#### Créer et installer un certificat auto-signé

**Étapes**

1. Allez à **Configuration→ Système→ Sécurité→ Gestion des certificats** .
2. Dans la zone **Fichiers de certificat**, sélectionnez un **type de certificat** dans la liste déroulante.
3. Cliquez sur **Créer**.
4. Saisir les informations relatives au certificat.
5. Cliquez sur **OK** pour enregistrer et installer le certificat.
   Le certificat créé est affiché dans la zone **Détails du certificat**. Le certificat sera sauvegardé automatiquement.
6. Téléchargez le certificat et enregistrez-le dans un fichier de demande sur l'ordinateur local.
7. Envoyer le fichier de demande à une autorité de certification pour signature.
8. Importer le certificat signé.
   1) Sélectionnez un type de certificat dans la zone **Importer des mots de passe**, puis sélectionnez un certificat dans le répertoire local et cliquez sur **Installer**.
   2) Sélectionnez un type de certificat dans la zone **Importer un certificat de communication**, puis sélectionnez un certificat dans le répertoire local et cliquez sur **Installer**.

#### Installer un autre certificat autorisé

Si vous disposez déjà d'un certificat autorisé (non créé par l'appareil), vous pouvez l'importer directement dans lappareil.

**Étapes**

1. Allez à **Configuration→ Système→ Sécurité→ Gestion des certificats** .
2. Dans les zones **Importer des mots de passe** et **Importer un certificat de communication**, sélectionnez le type de certificat et téléchargez le certificat.
3. Cliquez sur **Installer**.

#### Installer le certificat de l'autorité de certification

**Avant de commencer**

Préparez un certificat CA à l'avance.

**Étapes**

1. Allez à **Configuration→ Système→ Sécurité→ Gestion des certificats** .
2. Créez un identifiant dans la zone **Certificat CA Inport.**

**Note**

L'ID du certificat d'entrée ne peut pas être le même que celui certificats existants.

3. Télécharger un fichier de certificat à partir du site local.
4. Cliquez sur **Installer**.

### 9.5.10 Modifier le mot de passe de l'administrateur

**Étapes**

1. Cliquez sur **Configuration→ Gestion des utilisateurs** .
2. Cliquez sur .
3. Saisissez l'ancien mot de passe et créez un nouveau mot de passe.
4. Confirmez le nouveau mot de passe.
5. Cliquez sur **OK**.

**Attention**

La force du mot de passe de l'appareil peut être automatiquement vérifiée. Nous vous recommandons vivement de modifier le mot de passe de votre choix (en utilisant un minimum de 8 caractères, dont au moins trois des catégories suivantes : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) afin d'accroître la sécurité de votre produit. Nous vous recommandons également de modifier votre mot de passe régulièrement, en particulier dans le cas d'un système de haute sécurité, un changement de mot de passe mensuel ou hebdomadaire permet de mieux protéger votre produit.
La configuration correcte de tous les mots de passe et autres paramètres de sécurité relève de la responsabilité de 'installateur et/ou de l'utilisateur final.

### 9.5.11 Visualiser les informations d'armement/désarmement du dispositif

Afficher le type d'armement de l'appareil et l'adresse IP d'armement.

Allez à **Configuration→ Arming/Disarming Information (Informations sur l'armement et le désarmement)** .

Vous pouvez consulter les informations relatives à l'armement et au désarmement de l'appareil. Cliquez sur **Rafraîchir** pour actualiser la page.

### 9.5.12 Paramètres du réseau

Définissez les paramètres TCP/IP, le port, les paramètres Wi-Fi, la stratégie de rapport, l'accès à la plateforme et l'écoute HTTP.

**Note**

Certains modèles d'appareils ne prennent pas en charge les paramètres Wi-Fi. Reportez-vous aux produits réels pour la configuration.

## Régler les paramètres de base du réseau

Cliquez sur **Configuration→ Réseau→ Paramètres de base→ TCP/IP** .

Définissez les paramètres et cliquez sur **Enregistrer** pour sauvegarder

les paramètres.

**DHCP**

Si vous décochez la fonction, vous devez définir l'adresse IPv4, le masque de sous-réseau IPv4, la passerelle par défaut IPv4, le MTU et le port de l'appareil.

Si vous cochez cette fonction, le système attribuera automatiquement l'adresse IPv4, le masque de sous-réseau IPv4 et passerelle par défaut IPv4.

**Type de NIC**

Sélectionnez un type de carte réseau dans la liste déroulante. Par défaut, il s'agit de **Auto**.

**Serveur DNS**

Définissez le serveur DNS préféré et le serveur DNS alternatif en fonction de vos besoins réels.

## Paramètres du port

Définissez les paramètres HTTP, RTSP, HTTPS et le port du serveur.

Cliquez sur **Configuration→ Network→ Basic Settings→ Port** .

**HTTP**

Il s'agit du port par lequel le navigateur accède à l'appareil. Par exemple, lorsque le port HTTP est modifié en 81, vous devez saisir ***http://192.0.0.65:81*** dans le navigateur pour vous connecter.

**RTSP**

Il s'agit du port du protocole de diffusion en temps réel.

**HTTPS**

Définissez le protocole HTTPS pour l'accès au navigateur. Un certificat est requis lors de l'accès.

**Serveur**

Il s'agit du port par lequel le client ajoute l'appareil.

## Définir les paramètres Wi-Fi

Définissez les paramètres Wi-Fi pour la connexion sans fil de l'appareil.

**Étapes**

**Note**

La fonction doit être prise en charge par l'appareil.

**1.** Cliquez sur **Configuration→ Réseau→ Paramètres de base→ Wi-Fi** .


**Figure 9-6 Page des paramètres Wi-Fi**

**2.** Vérifier le **Wi-Fi**.

**3.** Sélectionnez un réseau Wi-Fi

- Cliquez sur d'un Wi-Fi dans la liste et entrez le mot de passe du Wi-Fi.
- Cliquez sur **Ajouter**, puis entrez le SSID, le mode de fonctionnement et le type de cryptage. Cliquez sur **Connecter**. Lorsque le Wi-Fi est connecté, cliquez sur **OK**.

**4. En option :** Définissez les paramètres WLAN.

1) Cliquez sur **Paramètres réseau**.
2) Définissez l'adresse IP, le masque de sous-réseau et la passerelle par défaut. Ou cochez **Activer DHCP** et le système attribuera automatiquement l'adresse IP, le masque de sous-réseau et la passerelle par défaut.

**5.** Cliquez sur **OK**.

## Paramètres de la stratégie du rapport

Vous pouvez définir le groupe de centres pour le téléchargement du journal via le

protocole ISUP. Allez dans **Configuration → Réseau → Paramètres de base →**

**Stratégie de rapport** .

Vous pouvez définir le groupe de centres et le système transférera les journaux via le protocole ISUP. Cliquez sur **Enregistrer** pour sauvegarder

les réglages.

**Groupe central**

Sélectionnez un groupe de centres dans la liste déroulante.

**Canal principal**

Le dispositif communiquera avec le centre via le canal principal.

**Note**

N1 fait référence au réseau câblé.

## Accès à la plate-forme

L'accès à la plate-forme vous permet de gérer les appareils via la plate-forme.

**Étapes**

1. Cliquez sur **Configuration→ Network→ Advanced→ Platform Access** pour accéder à la page des paramètres.
2. Sélectionnez le **mode d'accès à la plate-forme**.

**Note**

Hik-Connect est une application pour les appareils mobiles. L'application permet de visualiser l'image en direct dispositif, de recevoir des notifications d'alarme, etc.

3. Cochez la case **Activer** pour activer la fonction.
4. **Facultatif :** Cochez la case **Personnalisé** pour définir vous-même l'adresse du serveur.
5. Créez une **clé de chiffrement de flux/chiffrement** pour l'appareil.

**Note**

6 à 12 lettres (a à z, A à Z) ou chiffres (0 à 9), en respectant la casse. Il est recommandé d'utiliser une combinaison d'au moins 8 lettres ou chiffres.

6. Cliquez sur **Enregistrer** pour activer les paramètres.

## Paramètres ISUP

Définir les paramètres ISUP pour accéder à l'appareil via le protocole ISUP.

**Étapes**

**Note**

La fonction doit être prise en charge par l'appareil.

1. Cliquez sur **Configuration→ Network→ Advanced Settings→ Platform** .
2. Sélectionnez **ISUP** dans la liste déroulante du mode d'accès à la plate-forme.
3. Vérifier l'**activation**.
4. Définir la version de l'ISUP et afficher le type de récepteur d'alarme, l'adresse du serveur, le port, l'ID de l'appareil, l'état du registre.

**Note**

Si vous choisissez la version 5.0, vous devez également définir la clé ISUP.

5. Définir les paramètres d'écoute ISUP, y compris l'adresse IP/le nom de domaine du centre d'alarme ISUP, l'URL du centre d'alarme ISUP et le port du centre d'alarme ISUP.
6. Cliquez sur **Enregistrer**.

### Configuration de l'écoute HTTP

L'appareil peut envoyer des informations d'alarme à l'adresse IP ou au nom de domaine de l'alarme d'événement via le protocole HTTP/HTTPS.

**Avant de commencer**
L'adresse IP ou le nom de domaine de l'alarme doit prendre en charge le protocole HTTP/HTTPS pour recevoir les informations d'alarme.

**Note**
La fonction doit être prise en charge par l'appareil.

**Étapes**

1. Cliquez sur **Configuration→ Network→ Advanced→ HTTP Listening** .
2. Modifier l'adresse IP ou le nom de domaine, l'URL, le port et le protocole de l'alarme d'événement.
3. **Facultatif :** Cliquez sur **Défaut** pour réinitialiser l'adresse IP ou le nom de domaine de l'alarme d'événement.
4. Cliquez sur **Enregistrer**.

## 9.5.13 Régler les paramètres vidéo et audio

Réglez la qualité de l'image, la résolution et le volume de l'appareil.

### Paramètres vidéo

Cliquez sur **Configuration→ Vidéo/Audio→ Vidéo** .

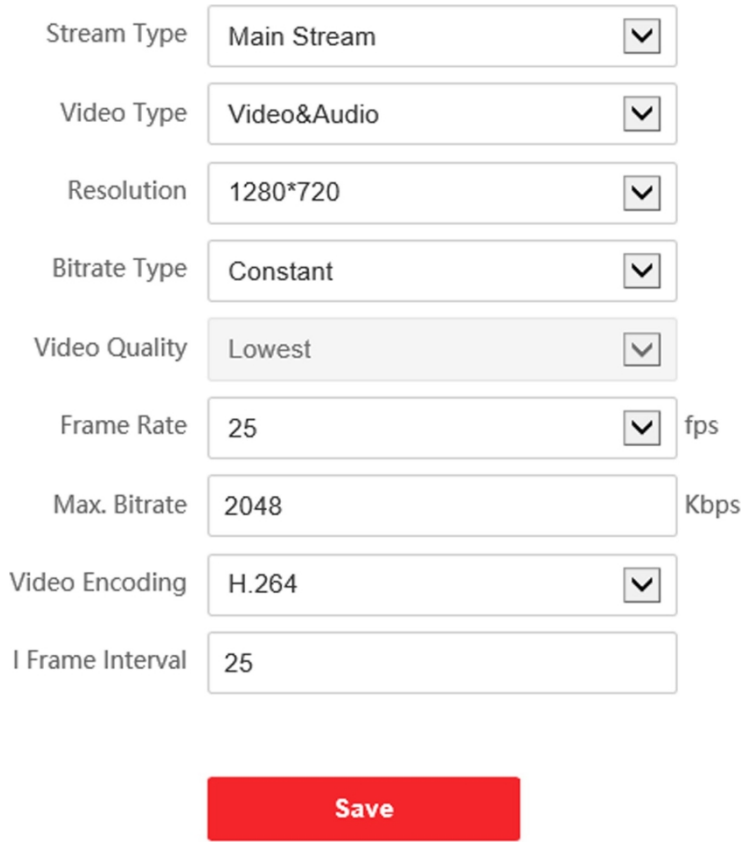



**Figure 9-7 Page des paramètres vidéo**

Réglez le type de flux, le type de vidéo, le type de débit binaire, la fréquence d'images, le débit binaire maximal, l'encodage vidéo et l'intervalle d'images.

Cliquez sur **Enregistrer** pour sauvegarder les paramètres après la configuration.

### Régler les paramètres audio

Cliquez sur **Configuration → Vidéo/Audio → Audio** .

Définissez le type de flux audio et l'encodage audio.

Vous pouvez également faire glisser le bloc pour régler le volume d'entrée et de sortie de l'appareil. Cliquez sur **Enregistrer** pour sauvegarder les paramètres après la configuration.

**Note**

Les fonctions varient selon les modèles. Pour plus de détails, se référer à l'appareil lui-même.

## 9.5.14 Personnaliser le contenu audio

Personnaliser le contenu audio de sortie en cas de succès ou d'échec de l'authentification.

**Étapes**

1. Cliquez sur **Configuration→ Video/Audio→ Prompt** .

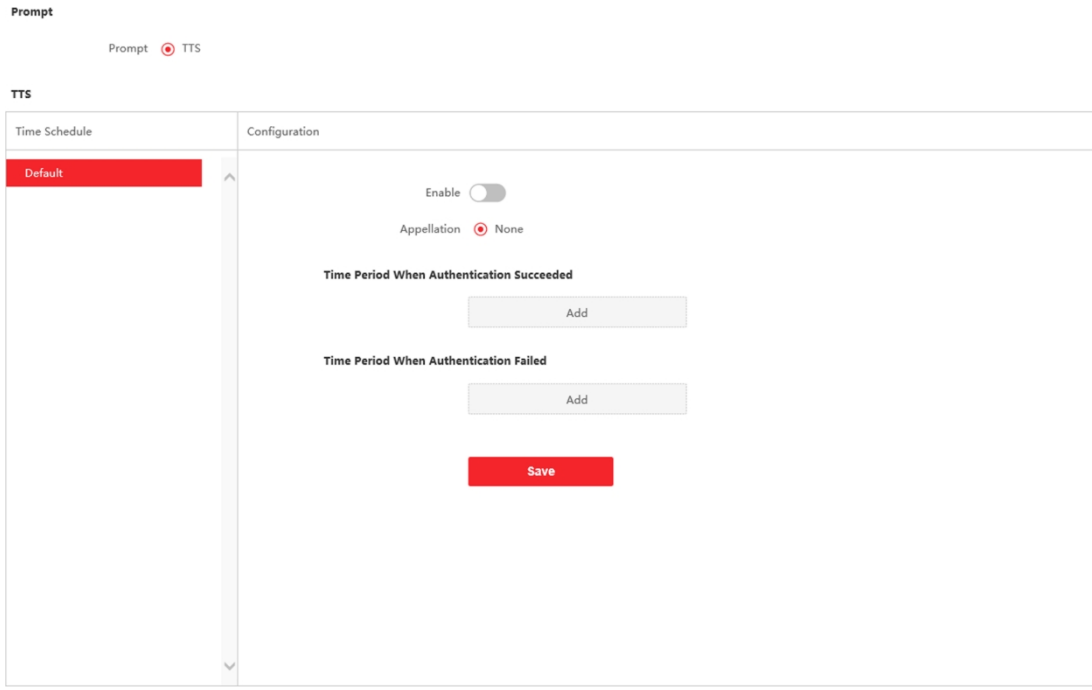



**Figure 9-8 Personnaliser le contenu audio**

2. Sélectionnez **Prompt as TTS** (Text to Speech) pour transformer le texte en contenu audio.
3. Sélectionner l'horaire.
4. Activer la fonction.
5. Définir l'appellation.
6. Définir la période de temps pendant laquelle l'authentification a réussi.
   1) Cliquez sur **Ajouter**.
   2) Régler la durée et la langue.

      **Note**

      Si l'authentification est réussie dans le configuré, l'appareil diffusera le contenu configuré.

   3) Entrez le contenu audio.
   4) **Optionnel :** Répéter les sous-étapes 1 à 3.
   5) **En option, cliquez sur pour supprimer la durée configurée :** Cliquez sur pour supprimer la durée configurée.
7. Définir la durée de l'échec de l'authentification.
   1) Cliquez sur **Ajouter**.
   2) Régler la durée et la langue.

**Note**

Si l'authentification échoue pendant la durée configurée, l'appareil diffuse le contenu configuré.

3) Entrez le contenu audio.
4) **Optionnel :** Répéter les sous-étapes 1 à 3.
5) **En option, cliquez sur pour supprimer la durée configurée :** Cliquez sur pour supprimer la durée configurée.

**8. Optionnel :** Ajouter le calendrier des vacances.
1) Cliquez sur **Ajouter** pour ajouter un programme de vacances.
2) Répéter les étapes 3 à 6.

**9.** Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

## 9.5.15 Paramètres de l'image

Réglez la norme vidéo, WDR, la luminosité, le contraste, la saturation et la netteté.

**Étapes**

**1.** Cliquez sur **Configuration→ Ajustement de l'image** .

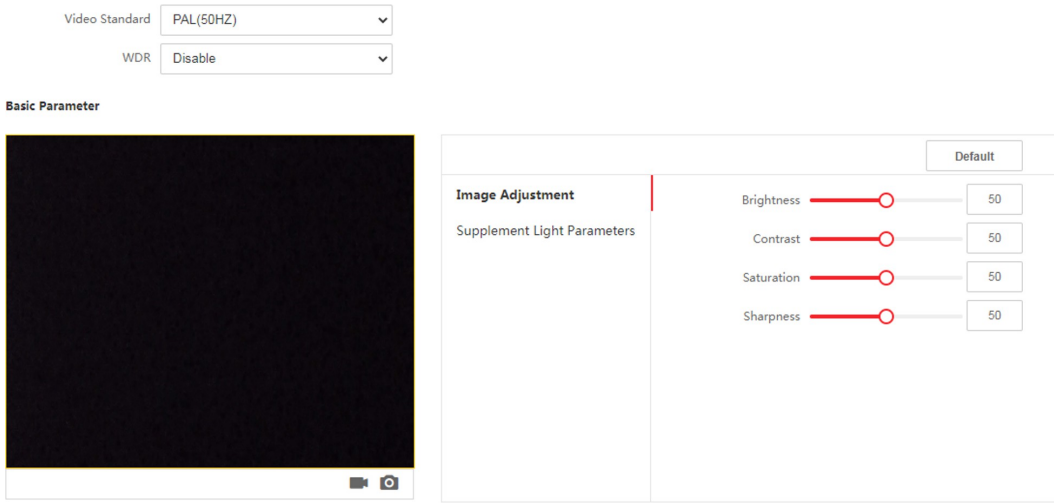



**Figure 9-9 Page des paramètres de l'image**

**2.** Configurer les paramètres pour ajuster l'image.

**Standard vidéo**

Définissez la fréquence d'images vidéo lorsque vous effectuez une visualisation en direct à distance. Après avoir modifié la norme, vous devez redémarrer l'appareil pour qu'elle prenne effet.

**PAL**

25 images par seconde. Convient à la Chine continentale, à Hong Kong (Chine), aux pays du , aux pays d'Europe, etc.

**NTSC**

30 images par seconde. Convient aux États-Unis, au Canada, au Japon, à Taïwan (Chine), à Corée, aux Philippines, etc.

**WDR**

Active ou désactive la fonction WDR.

Lorsqu'il y a simultanément des zones très lumineuses et très sombres dans l'image, la fonction WDR équilibre le niveau de luminosité de l'ensemble de l'image et fournit des images claires avec des détails.

**Luminosité/Contraste/Saturation/Netteté**

Faites glisser le bloc ou saisissez la valeur pour régler la luminosité, le contraste, la saturation et la netteté de la vidéo en direct.

Démarrer/terminer

l'enregistrement vidéo.

Capturer l'image.

**3.** Cliquez sur **Défaut** pour rétablir les paramètres par défaut.

## 9.5.16 Supplément Régler la luminosité de la lumière

Régler la luminosité de l'éclairage supplémentaire de l'appareil.

**Étapes**

**1.** Cliquez sur **Configuration→ Image→ Supplement Light Parameters** .

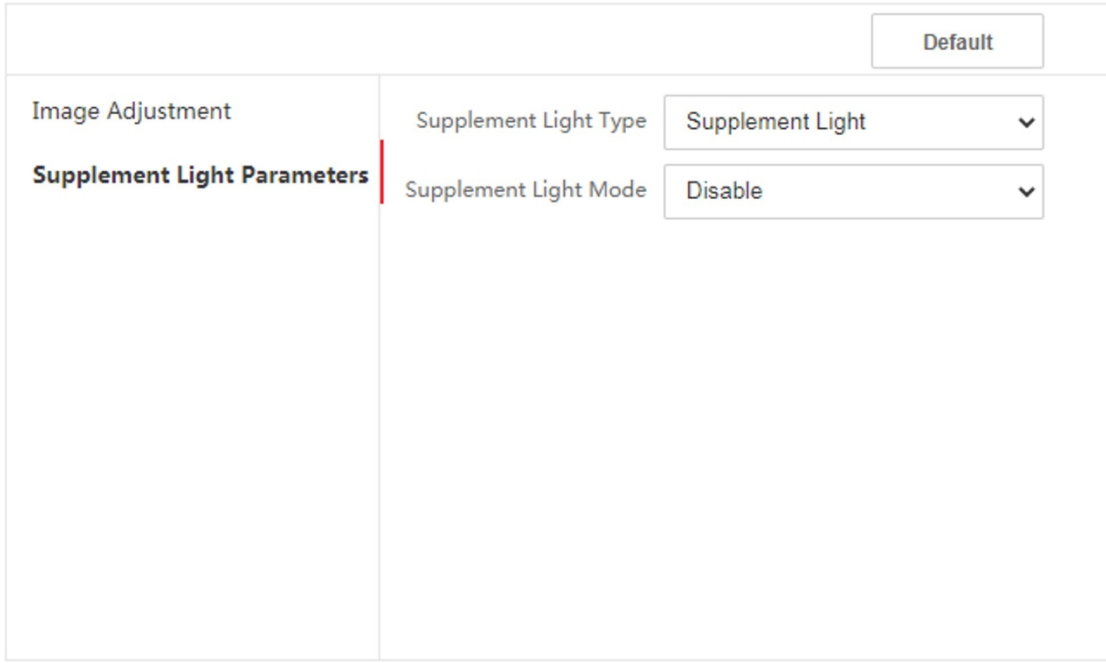



**Figure 9-10 Page des paramètres de l'éclairage d'appoint**

2. Sélectionnez un type d'éclairage supplémentaire et un mode dans la liste déroulante. Si vous sélectionnez le mode **ON**, vous devez régler la luminosité.

## 9.5.17 Paramètres de temps et de présence

Si vous souhaitez suivre et contrôler l'heure à laquelle les personnes commencent/arrêtent le travail et surveiller leurs heures de travail, leurs arrivées tardives, leurs départs anticipés, le temps consacré aux pauses et l'absentéisme, vous pouvez ajouter personne au groupe d'affectations et affecter un plan d'affectation (une règle de présence définissant le mode de répétition du plan, le type d'affectation, les paramètres de pause et la règle de lecture des cartes) au groupe d'affectations afin de définir les paramètres de présence pour les personnes dans le groupe d'affectations.

### Désactiver le mode présence via le Web

Désactivez le mode de présence et le système n'affichera pas l'état de la présence sur la page initiale.

**Étapes**

1. Cliquez sur **Configuration→ Attendance** pour accéder à la page des paramètres.
2. Réglez **le mode de présence** sur **Désactivé**.

**Résultat**

Vous ne verrez ni ne configurerez l'état des présences sur la page initiale. Le système suivra la règle de présence configurée sur la plateforme.

## Réglages de l'heure

**Étapes**

1. Cliquez sur **Configuration→ Time Settings** pour accéder à la page des paramètres.
2. Sélectionnez le **type de statut**.
3. **Facultatif :** Modifier le **nom de l'horaire** en fonction des besoins réels.
4. Faites glisser la souris pour définir l'horaire.

**Note**

Fixer l'horaire du lundi au dimanche en fonction des besoins réels.

5. **Facultatif :** Sélectionnez une ligne de temps et cliquez sur **Supprimer**. Ou cliquez sur **Supprimer tout** pour effacer les paramètres.
6. Cliquez sur **Enregistrer**.

## Régler les présences manuelles via le Web

Définissez le mode de présence comme étant manuel, et vous devrez sélectionner un statut manuellement lorsque vous prendrez des présences.

**Avant de commencer**

Ajoutez au moins un et définissez son mode d'authentification. Pour plus de détails, voir *Gestion des utilisateurs*.

**Étapes**

1. Cliquez sur **Configuration→ Attendance** pour accéder à la page des paramètres.
2. Réglez **le mode de participation** sur **Manuel**.
3. Activez le **statut de présence requise** et définissez la durée du statut de présence.
4. Activer un groupe de statuts de présence.

**Note**

La propriété de l'assiduité ne sera pas modifiée.

5. **Optionnel :** Sélectionnez un statut et modifiez son nom si nécessaire.

**Résultat**

Vous devez sélectionner manuellement un statut de présence après l'authentification.

**Note**

Si vous ne sélectionnez pas de statut, l'authentification échouera et ne sera pas marquée comme une présence valide.

## Régler la présence automatique via le Web

Définissez le mode de présence comme automatique, et vous pouvez définir le statut de présence et son horaire disponible. Le système modifie automatiquement le statut de présence en fonction de l'horaire configuré.

**Avant de commencer**

Ajoutez au moins un et définissez son mode d'authentification. Pour plus de détails, voir *Gestion des utilisateurs*.

**Étapes**

1. Cliquez sur **Configuration→ Attendance** pour accéder à la page des paramètres.
2. Réglez **le mode de participation** sur **Auto**.
3. Activer la fonction **Statut de présence.**
4. Activer un groupe de statuts de présence.

   **Note**

   La propriété de l'assiduité ne sera pas modifiée.
5. **Optionnel :** Sélectionnez un statut et modifiez son nom si nécessaire.
6. Définir le calendrier de l'état. Pour plus de détails, reportez-vous aux ***SeFngs temporels***.

## Régler la présence manuelle et automatique via le Web

Définissez le mode de présence comme **Manuel et Auto**, et le système changera automatiquement statut de présence selon le calendrier configuré. En même temps, vous pouvez modifier manuellement le statut de présence après l'authentification.

**Avant de commencer**

Ajoutez au moins un et définissez son mode d'authentification. Pour plus de détails, voir *Gestion des utilisateurs*.

**Étapes**

1. Cliquez sur **Configuration→ Attendance** pour accéder à la page des paramètres.
2. Réglez **le mode de présence** sur **Manuel et Auto**.
3. Activer la fonction **Statut de présence.**
4. Activer un groupe de statuts de présence.

   **Note**

   La propriété de l'assiduité ne sera pas modifiée.
5. **Optionnel :** Sélectionnez un statut et modifiez son nom si nécessaire.
6. Définir le calendrier de l'état. Pour plus de détails, reportez-vous aux ***SeFngs temporels***.

**Résultat**

Sur la page initiale et s'authentifier. L'authentification sera marquée comme l'état de présence configuré selon le calendrier. Si vous appuyez sur l'icône de modification dans l'onglet des résultats, vous pouvez sélectionner un statut pour prendre des présences manuellement, l'authentification sera marquée comme le statut de présence modifié.

**Exemple**
Si l'on fixe l'**heure de sortie** au lundi 11:00 et l'heure **d'entrée au** lundi 12:00, l'authentification de l'utilisateur valide entre le lundi 11:00 et le lundi 12:00 sera marquée comme une interruption.

## 9.5.18 Paramètres généraux

### Paramètres d'authentification

Cliquez sur **Configuration→ General→ Authentication Settings** .

**Note**
Les fonctions varient selon les modèles. Pour plus de détails, se référer à l'appareil lui-même.

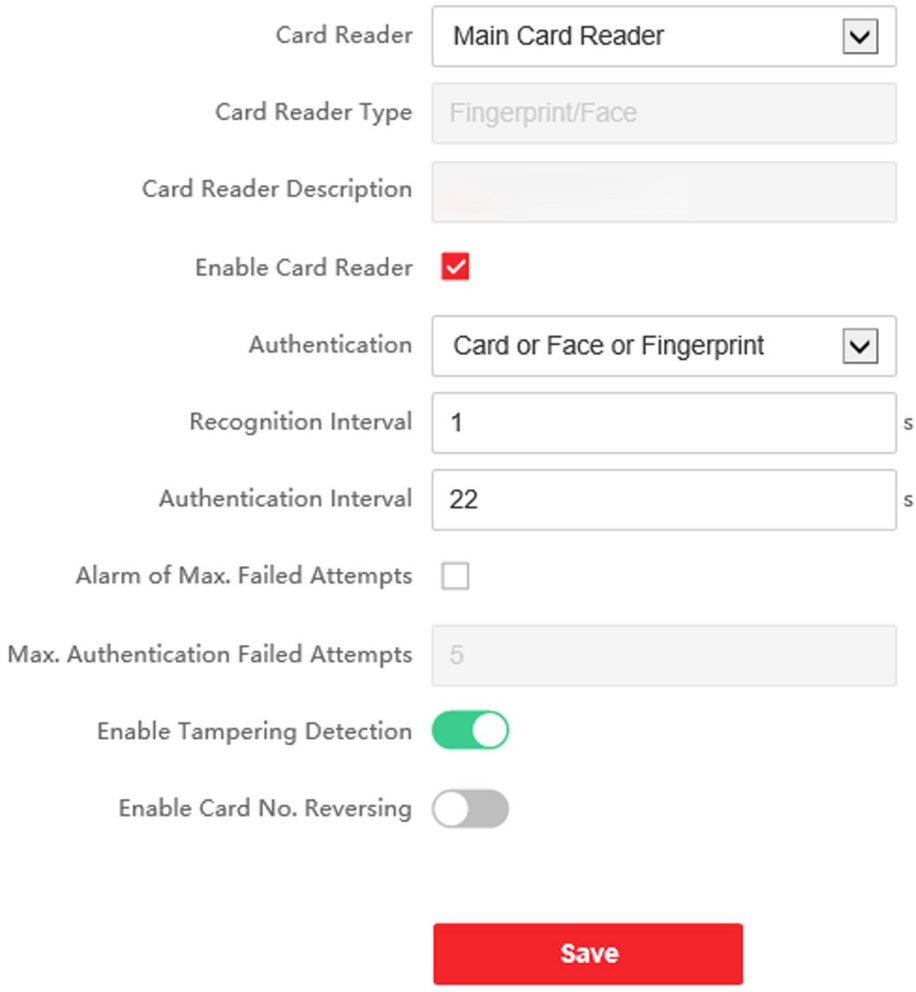



**Figure 9-11 Paramètres d'authentification**

Cliquez sur **Enregistrer** pour sauvegarder les paramètres après la configuration.

**Type d'appareil**

Sélectionnez **Main Card Reader** ou **Sub Card Reader** dans la liste déroulante.

**Lecteur de carte principal**

Vous pouvez configurer les paramètres du lecteur de cartes.

**Lecteur de sous-cartes**

Vous pouvez configurer les paramètres du lecteur de carte périphérique connecté.

Si vous sélectionnez **Lecteur de carte principal** :

**Type de lecteur de cartes/Description du lecteur de cartes**

Obtenir le type et la description du lecteur de cartes. Ils sont en lecture seule.

**Activer le lecteur de cartes**

Activer la fonction du lecteur de cartes.

**Authentification**

Sélectionnez un mode d'authentification en fonction de vos besoins réels dans la liste déroulante.

**Intervalle de reconnaissance**

Vous pouvez définir l'intervalle entre deux reconnaissances continues d'une même personne au cours de l'authentification. Dans l'intervalle configuré, la personne A ne peut être reconnue qu'une seule fois. Si une autre personne (personne B) a été reconnue pendant l'intervalle, la personne A peut être reconnue à nouveau.

**Intervalle d'authentification**

Vous pouvez définir l'intervalle d'authentification d'une même personne. La même personne ne peut s'authentifier qu'une seule fois dans l'intervalle configuré. Une deuxième authentification échouera.

**Alarme de tentatives max. Tentatives échouées**

Permet de déclencher une alarme lorsque les tentatives de lecture de la carte atteignent la valeur définie.

**Max. Tentatives d'authentification échouées**

Permet de déclencher une alarme lorsque les tentatives de lecture de la carte atteignent la valeur définie.

**Activer la détection de sabotage**

Activer la détection anti-sabotage pour le lecteur de cartes.

**Activer l'inversion du numéro de carte**

Le numéro de la carte lue sera dans l'ordre inverse après l'activation de la fonction.

Si vous sélectionnez **Lecteur de sous-cartes** :

**Type de lecteur de carte/Description du lecteur de carte**

Obtenir le type et la description du lecteur de cartes. Ils sont en lecture seule.

**Activer le lecteur de cartes**

Activer la fonction du lecteur de cartes.

**Authentification**

Sélectionnez un mode d'authentification en fonction de vos besoins réels dans la liste déroulante.

**Intervalle de reconnaissance**

Si l'intervalle entre les présentations d'une même carte est inférieur à la valeur configurée, présentation de la carte n'est pas valide.

**Intervalle d'authentification**

Vous pouvez définir l'intervalle d'authentification d'une même personne. La même personne ne peut s'authentifier qu'une seule fois dans l'intervalle configuré. Une deuxième authentification échouera.

**Alarme de tentatives max. Tentatives échouées**

Permet de déclencher une alarme lorsque les tentatives de lecture de la carte atteignent la valeur définie.

**Max. Tentatives d'authentification échouées**

Permet de déclencher une alarme lorsque les tentatives de lecture de la carte atteignent la valeur définie.

**Communication avec le contrôleur Chaque**

Lorsque le dispositif de contrôle d'accès ne peut pas se connecter au lecteur de cartes pendant une période plus longue que celle définie, le lecteur de cartes se déconnecte automatiquement.

**Max. Intervalle lors de la saisie du mot de passe**

Lorsque vous saisissez le mot de passe sur le lecteur de cartes, si l'intervalle entre la pression de deux chiffres est supérieur à la valeur définie, les chiffres que vous avez appuyés auparavant seront automatiquement effacés.

**Polarité de la LED OK/Polarité de la LED Erreur**

Régler la polarité de la LED OK/la polarité de la LED d'erreur du dispositif de contrôle d'accès en fonction des paramètres du lecteur de cartes. En général, les paramètres par défaut sont adoptés.

**Activer la détection de sabotage**

Activer la détection anti-sabotage pour le lecteur de cartes.

## Paramètres de confidentialité

Définissez le type de stockage des événements, les paramètres de téléchargement et de stockage des images, ainsi que les paramètres d'effacement des images.

Allez dans **Configuration→ General→ Privacy** .

## Paramètres de stockage des événements

Sélectionnez une méthode pour supprimer l'événement. Vous pouvez choisir entre **Supprimer les anciens événements périodiquement**, **Supprimer les anciens événements par période spécifiée** ou **Écraser**.

**Supprimer périodiquement les anciens événements**

Faites glisser le bloc ou entrez un chiffre pour définir la période de suppression des événements. Tous les événements seront supprimés en fonction de la durée configurée.

**Suppression d'anciens événements à la date spécifiée**

Définissez une heure et tous les événements seront supprimés à l'heure configurée.

**Surécriture**

Les 5 % d'événements les plus anciens sont supprimés lorsque le système détecte que les événements stockés ont dépassé 95 % de l'espace disponible.

## Paramètres d'authentification

**Afficher le résultat de l'authentification**

Vous pouvez vérifier la **photo du visage**, le **nom**, l'**ID de l'employé** et la **température** pour afficher le résultat de l'authentification.

**Nom Désidentification**

Vous pouvez cocher la case **Désidentification du nom**, et le nom entier ne sera pas affiché.

## Téléchargement et stockage d'images

**Téléchargement d'une image capturée lors de l'authentification**

Télécharger automatiquement les photos prises lors de l'authentification sur la plateforme.

**Sauvegarde de l'image capturée lors de l'authentification**

Si vous activez cette fonction, vous pouvez enregistrer l'image lors de l'authentification à l'appareil.

**Enregistrer l'image enregistrée**

L'image du visage enregistrée sera sauvegardée dans le système si vous activez la fonction.

**Téléchargement d'une image après la capture d'un lien**

Téléchargez automatiquement sur la plateforme les images capturées par l'appareil photo relié.

**Sauvegarde des images après la capture liée**

Si vous activez cette fonction, vous pouvez enregistrer l'image capturée par l'appareil photo lié sur l'appareil.

## Effacer toutes les images de l'appareil

**Note**

Toutes les photos ne peuvent pas être restaurées une fois qu'elles ont été supprimées.

**Photos d'un visage enregistré clair**

Toutes les photos enregistrées dans l'appareil seront supprimées.

**Effacer les images capturées**

Toutes les photos prises dans l'appareil seront supprimées.

## Paramètres de reconnaissance des visages

Vous pouvez définir les paramètres de reconnaissance des visages pour l'accès.

Cliquez sur **Configuration→ Contrôle d'accès→ Paramètres de reconnaissance faciale** .

Vous pouvez définir le **mode de travail** comme **mode de contrôle d'accès**. Le mode de contrôle d'accès est le mode normal de l'appareil. Vous devez authentifier vos données d'identification pour accéder à l'appareil.

## Définir la sécurité de la carte

Cliquez sur **Configuration→ General→ Card Security** pour accéder à la page de configuration. Définissez les paramètres et cliquez sur **Enregistrer**.

**Activer la carte NFC**

Afin d'empêcher le téléphone portable d'obtenir les données du contrôle d'accès, vous pouvez activer la carte NFC pour augmenter le niveau de sécurité des données.

**Activer la carte M1**

L'activation de la carte M1 et l'authentification par présentation de la carte M1 sont disponibles.

**Chiffrement de la carte M1**

Le cryptage de la carte M1 peut améliorer le niveau de sécurité de l'authentification.

**Secteur**

Activez la fonction et définissez le secteur de cryptage. Par défaut, le secteur 13 est crypté. Il est recommandé de crypter le secteur 13.

**Activer la carte EM**

L'activation de la carte EM et l'authentification par présentation de la carte EM sont disponibles.

**Note**

Si le lecteur de carte périphérique prend en charge la présentation de la carte EM, la fonction d'activation/désactivation de la fonction de carte EM est également prise en charge.

**Activer la carte DESFire**

L'appareil peut lire les données de la carte DESFire lorsque la fonction de la carte DESFire est activée.

**Carte DESFire Lire le contenu**

Après avoir activé la fonction de lecture du contenu de la carte DESFire, l'appareil peut lire le contenu de la carte DESFire.

## Définir les paramètres d'authentification de la carte

Définir le contenu de la lecture de la carte lors de l'authentification par carte sur l'appareil.

Allez sur **Configuration→ Contrôle d'accès→ Paramètres d'authentification de la carte**

. Sélectionnez un mode d'authentification de carte et cliquez sur **Enregistrer**.

**Numéro de la carte complète**

Tous les numéros de carte seront lus.

**Wiegand 26 (3 octets)**

L'appareil lira la carte via le protocole Wiegand 26 (lecture de 3 octets).

**Wiegand 34 (4 octets)**

L'appareil lira la carte via le protocole Wiegand 34 (lecture de 4 octets).

## 9.5.19 Paramètres de l'interphone vidéo

### Réglage des paramètres de l'interphone vidéo

L'appareil peut être utilisé comme poste de porte, poste de porte extérieur ou dispositif de contrôle d'accès. Vous devez définir le numéro de l'appareil avant de l'utiliser.

Cliquez sur **Configuration→ Video Intercom→ Device No.**

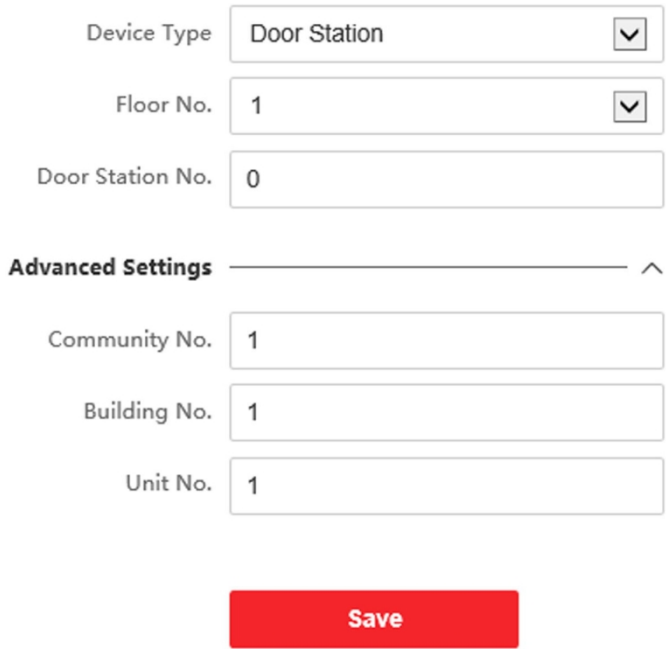



**Figure 9-12 Définition des paramètres de l'interphone vidéo**

Si le type de dispositif est défini comme **poste de porte** et **dispositif de contrôle d'accès**, vous pouvez définir le numéro d'étage, le numéro de poste de porte et cliquer sur **Paramètres avancés** pour définir le numéro de communauté, le numéro de bâtiment et le numéro d'unité.

Cliquez sur **Enregistrer** pour sauvegarder les paramètres après la configuration.

**Type d'appareil**

Le dispositif peut être utilisé comme poste de porte, poste de porte extérieur ou dispositif de contrôle d'accès. Sélectionnez un type de dispositif dans la liste déroulante.

**Note**
Si vous modifiez le type d'appareil, vous devez redémarrer l'appareil.

**N° d'étage**

Définir le numéro d'étage du dispositif installé.

**Numéro de la station de porte**

Définir le numéro d'étage du dispositif installé.

**Note**

Si vous modifiez le numéro, vous devez redémarrer l'appareil.

**No. de la communauté**

Définir le numéro de communauté du dispositif installé.

**Bâtiment n°.**

Définir le numéro de bâtiment installé sur l'appareil.

**N° d'unité**

Définir le numéro de l'unité installée sur l'appareil.

Si le type de dispositif est défini comme **Poste de Porte Extérieur**, vous pouvez définir le numéro du poste de porte extérieur, puis cliquer sur
**Paramètres avancés** pour définir le numéro de communauté.

**Porte extérieure Poste n°.**

Si vous sélectionnez la station de porte extérieure comme type d'appareil, vous devez saisir un numéro entre **1** et
**99**.

**Note**

Si vous modifiez le numéro, vous devez redémarrer l'appareil.

**No. de la communauté**

Définir le numéro de communauté du dispositif installé.

## Configuration des paramètres SIP

Définissez l'adresse IP du dispositif et l'adresse IP du serveur SIP. Après avoir défini les paramètres, vous pouvez communiquer entre le dispositif de contrôle d'accès, le poste de porte, le poste intérieur, le poste principal et la plate-forme.

**Note**

Seul le dispositif de contrôle d'accès et d'autres dispositifs ou systèmes (tels que le poste de porte, le poste intérieur, le poste principal, la plate-forme) se trouvent dans le même segment IP, et l'audio bidirectionnelle peut être réalisée.

Allez sur **Configuration→ Video Intercom→ Linked Network Settings** .

Définissez l'adresse IP du poste principal et l'adresse IP du serveur SIP.

Cliquez sur **Enregistrer**.

### Appuyer sur le bouton pour appeler

**Étapes**

1. Cliquez sur **Intercom→ Press Button to Call** pour accéder à la page de configuration.
2. Régler les paramètres.
   - Modifier le numéro d'appel pour chaque bouton.
   - Cochez **Centre de gestion des appels** pour définir le centre d'appel des boutons.

**Note**

Si vous cochez la case **Centre de gestion des appels** et que vous définissez le numéro d'appel, le centre de gestion des appels dispose d'un privilège plus élevé que le numéro d'appel.

## 9.5.20 Paramètres de contrôle d'accès

### Paramètres de la porte

Cliquez sur **Configuration→ Contrôle d'accès→ Paramètres de la porte** .

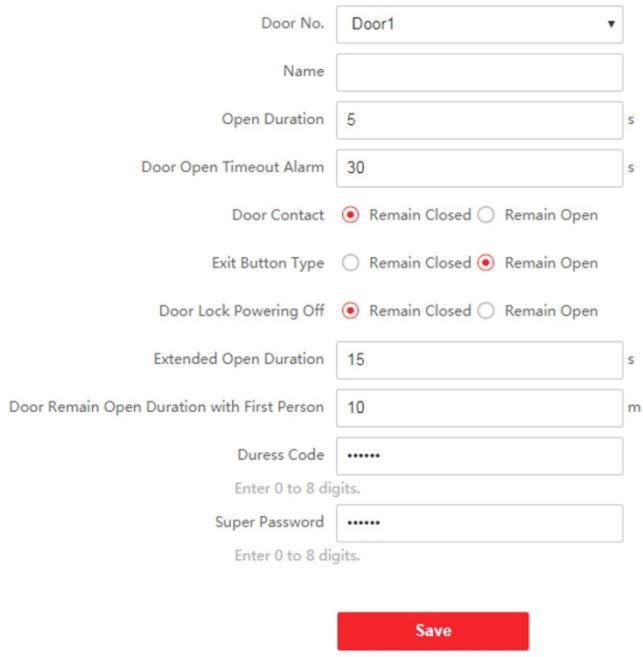



**Figure 9-13 Page de configuration des paramètres de la porte**

Cliquez sur **Enregistrer** pour sauvegarder les paramètres après la configuration.

**N° de porte**

Sélectionnez l'appareil correspondant à la porte No.

**Nom**

Vous pouvez créer un nom pour la porte.

**Ouvert Durée**

Régler la durée de déverrouillage de la porte. Si la porte n'est pas ouverte pendant la durée programmée, elle est verrouillée.

**Alarme de délai d'ouverture de la porte**

Une alarme est déclenchée si la porte n'a pas été fermée pendant la durée configurée.

**Contact de porte**

Vous pouvez définir le contact de porte comme **restant ouvert** ou **restant fermé** en fonction de vos besoins réels. Par défaut, le contact **reste fermé**.

**Type de bouton de sortie**

Vous pouvez définir le bouton de sortie comme **restant ouvert** ou **restant fermé** en fonction de vos besoins réels. Par défaut, il **reste ouvert**.

**État de la mise hors tension de la serrure de porte**

Vous pouvez définir l'état de la serrure de porte lorsque celle-ci est hors tension. Par défaut, l'état **reste fermé**.

**Durée d'ouverture prolongée**

Le contact de porte peut être activé avec un délai approprié après que la personne ayant des besoins d'accès étendus a glissé sa carte.

**Durée de la porte restée ouverte avec la première personne**

Définir la durée d'ouverture de la porte lorsque la première personne entre. Une fois que la première personne est autorisée, plusieurs personnes peuvent accéder à la porte ou à d'autres actions d'authentification.

**Code de contrainte**

En cas de contrainte, la porte peut s'ouvrir en entrant le code de contrainte. En même temps, le client peut signaler l'événement de contrainte.

**Super mot de passe**

La personne concernée peut ouvrir la porte en saisissant le super mot de passe.

**Note**

Le code de contrainte et le super code doivent être différents.

## Réglage des paramètres RS-485

Vous pouvez définir les paramètres RS-485, notamment le périphérique, l'adresse, le débit en bauds, etc. Cliquez sur **Configuration → Contrôle d'accès → Paramètres RS-485** .

Cochez **Enable RS-485 (Activer RS-485**) et définissez les paramètres.

Cliquez sur **Enregistrer** pour sauvegarder les paramètres après la configuration.

**Non.**

Réglez le numéro RS-485.

**Type de périphérique**

Sélectionnez un périphérique dans la liste déroulante en fonction de la réelle. Vous pouvez choisir entre Lecteur **de carte**, **module d'extension**, **contrôleur d'accès** ou **désactivé**.

**Note**

Une fois le périphérique modifié et enregistré, l'appareil redémarre automatiquement.

**Adresse RS-485**

Réglez l'adresse RS-485 en fonction de vos besoins réels.

**Note**

Si vous sélectionnez **Contrôleur d'accès** : Si vous connectez l'appareil à un terminal via l'interface RS-485, réglez l'adresse RS-485 sur 2. Si vous connectez l'appareil à un contrôleur, réglez l'adresse RS-485 en fonction du numéro de porte.

**Débit en bauds**

La vitesse de transmission lorsque les appareils communiquent via le protocole RS-485.

## Paramètres Wiegand

Vous pouvez définir la direction de la transmission Wiegand.

**Étapes**

**Note**

Certains modèles d'appareils ne prennent pas en charge cette fonction. Se référer aux produits réels lors de la configuration.

1. Cliquez sur **Configuration→ Access Control→ Wiegand Settings** .

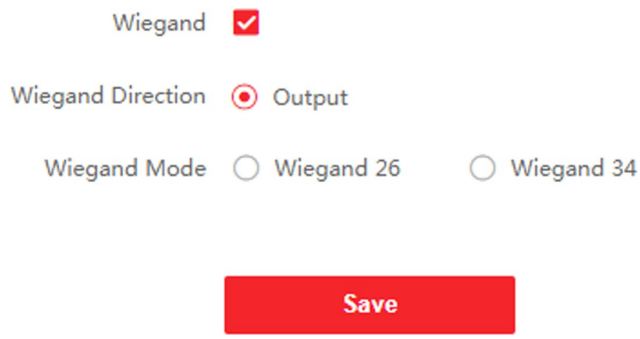



**Figure 9-14 Page Wiegand**

2. Cochez **Wiegand** pour activer la fonction Wiegand.
3. Définir un sens de transmission.

   **Sortie**

   Il est possible de connecter un contrôleur d'accès externe. Les deux appareils transmettront le numéro de carte via Wiegand 26 ou 34.
4. Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

**Note**

Si vous changez de périphérique, et après avoir sauvegardé les paramètres de l'appareil, ce dernier redémarre automatiquement.

### 9.5.21 Régler les paramètres biométriques Régler les paramètres de base

Cliquez sur **Configuration→ Smart→ Smart** .


**Figure 9-15 Paramètres de la face**

**Note**

Les fonctions varient selon les modèles. Pour plus de détails, se référer à l'appareil lui-même.

Cliquez sur **Enregistrer** pour sauvegarder les paramètres après la configuration.

**Anti-usurpation de visage**

Active ou désactive la fonction de détection des visages vivants. Si cette fonction est activée, l'appareil peut reconnaître si la personne est vivante ou non.

**Note**

Les produits de reconnaissance biométrique ne sont pas totalement adaptés aux environnements de lutte contre l'usurpation d'identité. Si vous avez besoin d'un niveau de sécurité plus élevé, utilisez plusieurs modes d'authentification.

**Détection des visages en direct Niveau de sécurité**

Après avoir activé la fonction anti-falsification des visages, vous pouvez définir le niveau de sécurité correspondant lors de l'authentification des visages en direct.

**Distance de reconnaissance**

Sélectionnez la distance entre l'utilisateur qui s'authentifie et la caméra de l'appareil.

**Mode d'application**

Sélectionnez "autres" ou "intérieur" en fonction de l'environnement réel.

**Mode de reconnaissance**

**des visages Mode**

**normal**

Reconnaître un visage via l'appareil photo normalement.

**Mode profond**

En mode approfondi, vous pouvez ajouter des photos de visage uniquement via la fonction d'ajout d'utilisateur de 'appareil ou de la station d'inscription. Il n'est pas possible d'ajouter des photos de visage via l'importation d'images.

**Note**

En mode approfondi, vous pouvez ajouter des photos de visage uniquement via l'appareil ou la station d'enrôlement. Il n'est pas possible d'ajouter des photos de visage via l'importation de photos.

**Intervalle de reconnaissance continue des visages**

Définir l'intervalle de temps entre deux reconnaissances continues du visage lors de l'authentification.

**Angle d'inclinaison**

L'angle d'inclinaison maximal lors du démarrage de l'authentification de la face.

**Angle de lacet**

Angle de lacet maximal lors du démarrage de l'authentification de la face.

**Classement des visages**

Réglez le calibrage du visage en fonction de vos besoins.

**Seuil de correspondance 1:1**

Définit le seuil de correspondance lors de l'authentification en mode de correspondance 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est important.

**Seuil de correspondance 1:N**

Définit le seuil de correspondance lors de l'authentification en mode de correspondance 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est important.

**Valeur du délai de reconnaissance des visages**

Définir la valeur du délai d'attente lors de la reconnaissance des visages. Si le délai de reconnaissance des visages est supérieur à la valeur configurée, le système affiche une invite.

**Détection de visage avec masque**

Après avoir activé la détection de visage avec masque, le système reconnaîtra le visage capturé avec l'image du masque. Vous pouvez définir le seuil de correspondance visage avec masque1:N, le mode ECO et la stratégie.

**Aucun**

Si la personne ne porte pas de masque facial lors de l'authentification, l'appareil n' pas de notification.

**Rappel du port**

Si la personne ne porte pas de masque facial lors de l'authentification, l'appareil émet une notification et la porte s'ouvre.

**Must Wear**

Si la personne ne porte pas de masque facial lors de l'authentification, le dispositif émet une notification et la porte reste fermée.

**Visage avec masque et visage (1:1)**

Définir la valeur de correspondance lors de l'authentification par masque facial en mode de correspondance 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.

**Visage avec masque Seuil de correspondance 1:N**

Définir le seuil de correspondance lors de l'authentification par masque facial en mode de correspondance 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est important.

**Mode ECO**

Après avoir activé le mode ECO, l'appareil utilisera la caméra IR pour authentifier les visages dans un environnement sombre ou faiblement éclairé. Vous pouvez définir le seuil du mode ECO, le mode ECO (1:N) et le mode ECO (1:1).

**Seuil du mode ECO**

Définir le seuil du mode ECO. Plus la valeur est élevée, plus l'appareil passe facilement en mode ECO.

**Mode ECO (1:1)**

Définir le seuil de correspondance lors de l'authentification en mode ECO 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.

**Mode ECO (1:N)**

Définir le seuil de correspondance lors de l'authentification en mode ECO 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.

**Face avec Mask & Face (1:1 ECO)**

Définir la valeur de correspondance lors de l'authentification avec un masque facial en mode ECO 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.

**Visage avec masque Seuil de correspondance 1:N (mode ECO)**

Définir le seuil de correspondance lors de l'authentification avec un masque facial via le mode ECO 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé.

**Niveau de sécurité des empreintes digitales**

Sélectionnez le niveau de sécurité des empreintes digitales.

Plus le niveau de sécurité est élevé, plus le taux de fausses acceptations (FAR) est faible.

### Définir la zone de reconnaissance

Cliquez sur **Configuration→ Smart→ Area Configuration** .
Faites glisser le cadre jaune dans la vidéo en direct pour ajuster la zone de reconnaissance. Seul le visage situé dans cette zone peut être reconnu par le système.
Réglez **la configuration de la zone**, la **marge (gauche)**, la **marge (droite)**, la **marge (supérieure)** et la **marge (inférieure)** comme vous le souhaitez.
Cliquez sur **Enregistrer** pour sauvegarder les paramètres.
Cliquez sur  ou  pour enregistrer des vidéos ou prendre des photos.

## 9.5.22 Fixer la publication de l'avis

Vous pouvez définir le thème de l'appareil.

Cliquez sur **Configuration→ Theme→ Media Database** , cliquez sur**+ Add**, et cliquez sur **Upload** pour télécharger matériel dans la médiathèque.

Cliquez sur **Configuration→ Theme→ Theme** .

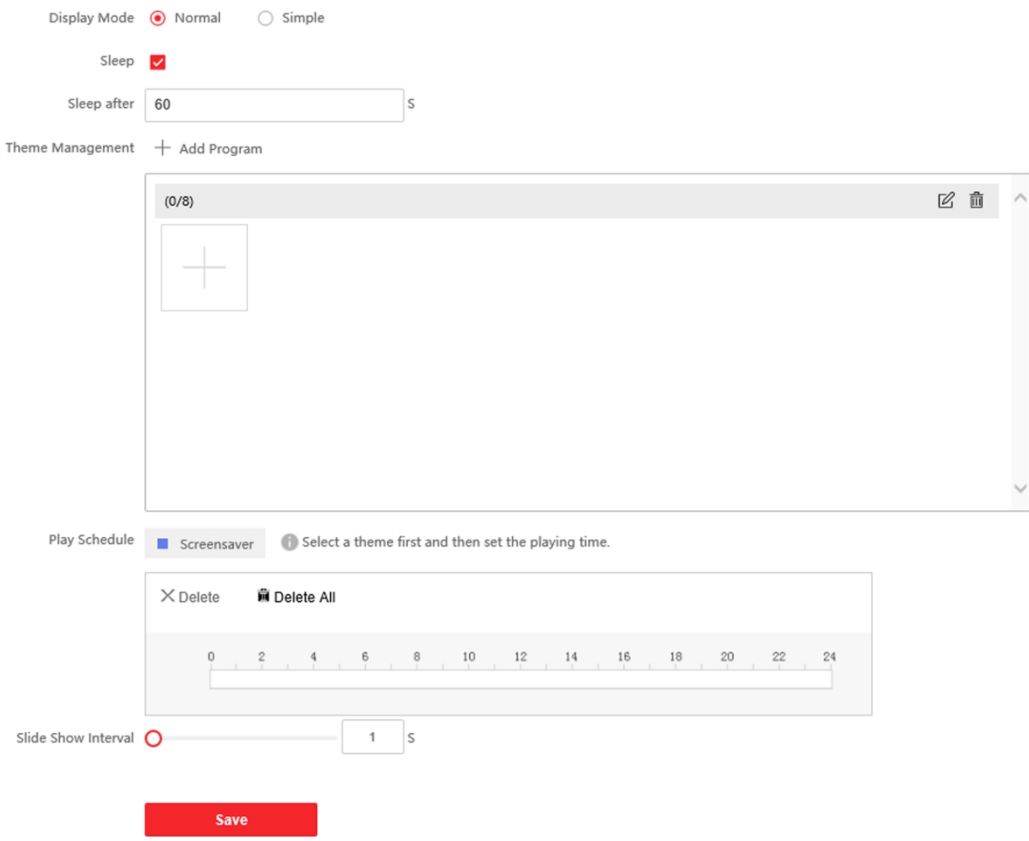



**Figure 9-16 Page Thème**

**Mode d'affichage**

Vous pouvez sélectionner le thème d'affichage pour l'authentification de l'appareil. Vous pouvez sélectionner le **mode d'affichage Simple** ou **Normal**. Lorsque vous sélectionnez **Simple**, les informations relatives au nom, à l'identifiant et à la photo du visage ne s'affichent pas.

**Sommeil**

Activez le mode veille et l'appareil passera en mode veille si aucune opération n'est effectuée pendant le délai de veille configuré.

**Gestion des thèmes**

Vous pouvez cliquer sur**+ Add Program** dans le cadre et télécharger les images de l'écran de veille à partir du PC local.

**Note**

Pour l', il n'y a qu'un seul thème qui peut être ajouté.

**Programme de jeu**

Après avoir créé un thème, vous pouvez le sélectionner et dessiner un calendrier sur la ligne temporelle pour définir le calendrier de jeu du thème.

Sélectionnez l'horaire dessiné et vous pouvez modifier l'heure exacte de début et de fin.

Sélectionnez la programmation dessinée et cliquez sur **Supprimer** ou **Supprimer tout** pour supprimer la programmation.

**Intervalle du diaporama**

Faites glisser le bloc ou entrez le nombre pour définir l'intervalle du diaporama. L'image est modifiée en fonction de l'intervalle.

# Chapitre 10 Configuration du logiciel client

## 10.1 Flux de configuration du logiciel client

Suivez l'organigramme ci-dessous pour configurer le logiciel client.

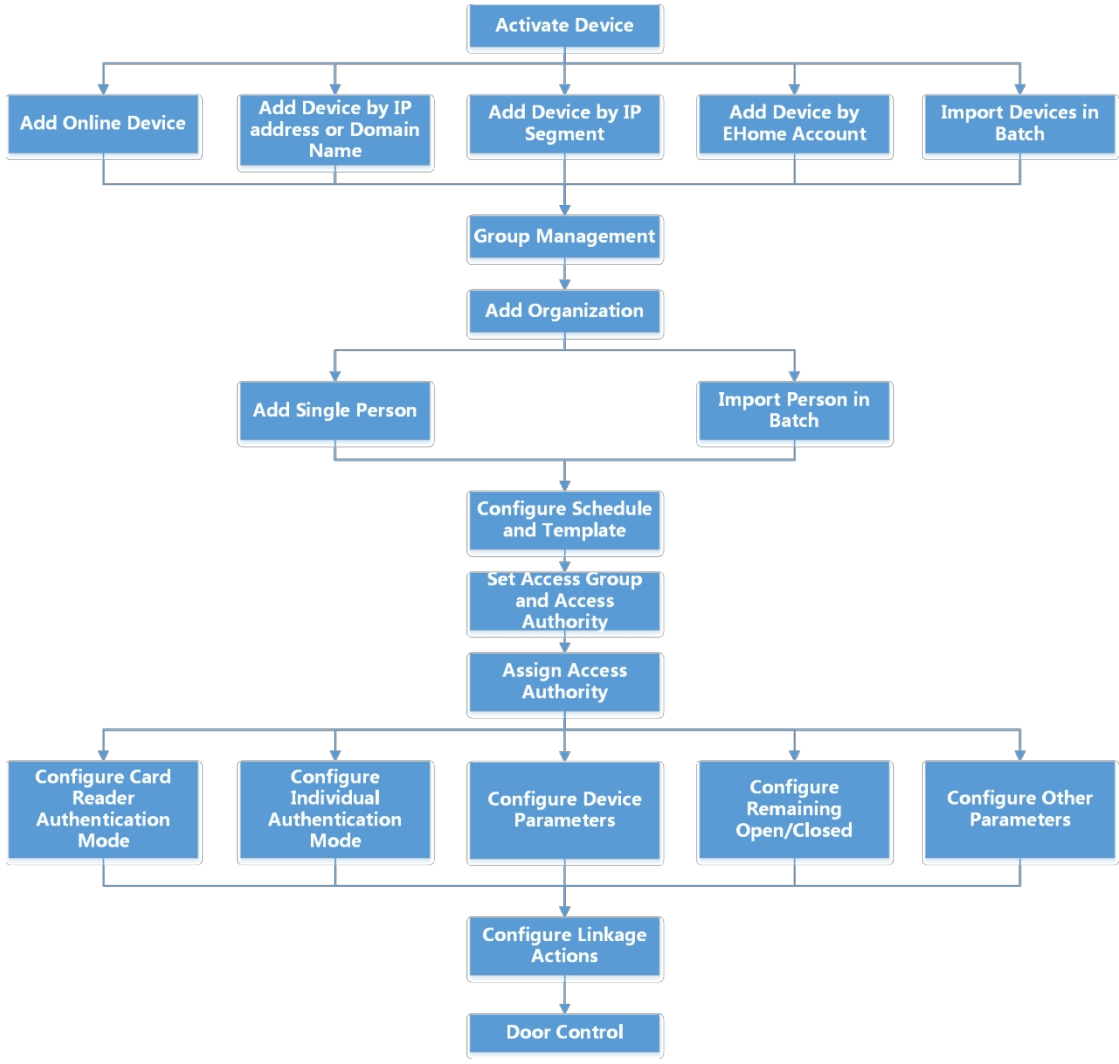



**Figure 10-1 Diagramme de flux de la configuration sur le logiciel client**

## 10.2 Gestion des appareils

Le client permet de gérer les dispositifs de contrôle d'accès et les interphones vidéo.

**Exemple**
Vous pouvez contrôler les entrées et les sorties et gérer les présences après avoir ajouté des dispositifs de contrôle d'accès client ; vous pouvez réaliser un interphone vidéo avec les postes intérieurs et les postes de porte.

### 10.2.1 Ajouter un dispositif

Le client propose trois modes d'ajout d'appareils : par IP/domaine, par segment IP et par protocole EHome. Le client prend également en charge l'importation de plusieurs appareils par lot lorsqu'il y a un grand nombre d'appareils à ajouter.

#### Ajouter un appareil par adresse IP ou nom de domaine

Si vous connaissez l'adresse IP ou le nom de domaine de l'appareil à ajouter, vous pouvez ajouter des appareils au client en spécifiant l'adresse IP (ou le nom de domaine), le nom d'utilisateur, le mot de passe, etc.

**Étapes**

1. Entrer dans le module de gestion des appareils.
2. Cliquez sur l'onglet **Device** en haut du panneau de droite.

   Les appareils ajoutés sont affichés dans le panneau de droite.
3. Cliquez sur **Ajouter** pour ouvrir la fenêtre Ajouter, puis sélectionnez **IP/Domaine** comme mode d'ajout.
4. Saisissez les informations requises.

   **Nom**

   Créez un nom descriptif pour l'appareil. Par exemple, vous pouvez utiliser un surnom qui indique l'emplacement ou les caractéristiques de l'appareil.

   **Adresse**

   L'adresse IP ou le nom de domaine de l'appareil.

   **Port**

   Les appareils à ajouter partagent le même numéro de port. La valeur par défaut est ***8000***.

   **Nom de l'utilisateur**

   Saisissez le nom d'utilisateur de l'appareil. Par défaut, le nom d'utilisateur est ***admin***.

   **Mot de passe**

   Saisissez le mot de passe de l'appareil.

   **Attention**

   La force du mot de passe de l'appareil peut être automatiquement vérifiée. Nous vous recommandons vivement de modifier le mot de passe de votre choix (en utilisant un minimum de 8 caractères, dont au moins trois des catégories suivantes : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) afin d'accroître la sécurité de votre produit. Nous vous recommandons également

vous changez  mot de passe régulièrement, en particulier dans le système de haute sécurité, le changement du mot de passe tous les mois ou toutes les semaines peut mieux protéger votre produit. La configuration correcte de tous les mots de passe et autres paramètres de sécurité relève de la responsabilité de 'installateur et/ou de l'utilisateur final.

5. **Facultatif :** Cochez **Transmission Encryption (TLS**) pour activer le cryptage de la transmission à l'aide du protocole TLS (Transport Layer Security) à des fins de sécurité.

**Note**

- Cette fonction doit être prise en charge par l'appareil.
- Si vous avez activé la vérification des certificats, vous devez cliquer sur **Ouvrir le répertoire des certificats** pour ouvrir le dossier par défaut et copier le fichier de certificat exporté depuis l'appareil dans ce répertoire par défaut afin de renforcer la sécurité. Voir pour plus de détails sur l'activation de la vérification des certificats.
- Vous pouvez vous connecter à l'appareil pour obtenir le fichier de certificat à l'aide d'un navigateur web.

6. Cochez la case **Synchroniser l'**heure pour synchroniser l'heure de l'appareil avec celle du PC exécutant le client après avoir ajouté l'appareil au client.
7. **Facultatif :** Cochez la case **Importer dans le groupe** pour créer un groupe à partir du nom de l'appareil et importer tous canaux de l'appareil dans ce groupe.

**Exemple**

Pour un dispositif de contrôle d'accès, ses points d'accès, ses entrées/sorties d'alarme et ses canaux d'encodage (s'ils existent) seront importés dans ce groupe.

8. Terminer l'ajout du dispositif.
   - Cliquez sur **Ajouter** pour ajouter le périphérique et revenir à la page de la liste des périphériques.
   - Cliquez sur **Ajouter et Nouveau** pour enregistrer les paramètres et continuer à ajouter d'autres appareils.

## Importer des dispositifs par lots

Vous pouvez ajouter plusieurs appareils au client par lot en saisissant les paramètres de l'appareil dans un fichier CSV prédéfini.

**Étapes**

1. Entrez dans le module de gestion des appareils.
2. Cliquez sur l'onglet **Device** en haut du panneau de droite.
3. Cliquez sur **Ajouter** pour ouvrir la fenêtre Ajouter, puis sélectionnez **Importation par lots** comme mode d'ajout.
4. Cliquez sur **Exporter le** modèle et enregistrez le modèle prédéfini (fichier CSV) sur votre PC.
5. Ouvrez le fichier modèle exporté et saisissez les informations requises sur les appareils à ajouter dans la colonne correspondante.

**Note**

Pour une description détaillée des champs obligatoires, reportez-vous aux introductions du modèle.

**Mode d'ajout**

Saisir ***0*** ou ***1*** ou ***2***.

**Adresse**

Modifier l'adresse de l'appareil.

**Port**

Saisissez le numéro de port de l'appareil. Le numéro de port par défaut est ***8000***.

**Nom de l'utilisateur**

Saisissez le nom d'utilisateur de l'appareil. Par défaut, le nom d'utilisateur est ***admin***.

**Mot de passe**

Saisissez le mot de passe de l'appareil.

**Attention**

La force du mot de passe de l'appareil peut être automatiquement vérifiée. Nous vous recommandons vivement de modifier le mot de passe de votre choix (en utilisant un minimum de 8 caractères, dont au moins trois des catégories suivantes : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) afin d'accroître la sécurité de votre produit. Nous vous recommandons également de modifier votre mot de passe régulièrement, en particulier dans le cas d'un système de haute sécurité, un changement de mot de passe mensuel ou hebdomadaire permet de mieux protéger votre produit.
La configuration correcte de tous les mots de passe et autres paramètres de sécurité relève de la responsabilité de 'installateur et/ou de l'utilisateur final.

**Importer dans un groupe**

Entrez ***1*** pour créer un groupe par le nom de l'appareil. Tous les canaux de l'appareil seront importés par défaut dans le groupe correspondant. Entrez ***0*** pour désactiver cette fonction.

6. Cliquez sur ··· et sélectionnez le fichier modèle.
7. Cliquez sur **Ajouter** pour importer les appareils.

### 10.2.2 Réinitialiser le mot de passe de l'appareil

Si vous avez oublié le mot de passe des appareils en ligne détectés, vous pouvez réinitialiser le mot de passe de l'appareil via le client.

**Étapes**

1. Entrer dans la page de gestion des appareils.
2. Cliquez sur **Appareil en ligne** pour afficher la zone de l'appareil en ligne.

   Tous les appareils en ligne partageant le même sous-réseau seront affichés dans la liste.
3. Sélectionnez l'appareil dans la liste et cliquez sur dans la colonne Opération.
4. Réinitialiser le mot de passe de l'appareil.
   - Cliquez sur **Générer** pour faire apparaître la fenêtre du code QR et cliquez sur **Télécharger** pour enregistrer le code QR sur votre PC. Vous pouvez également prendre une photo du code QR pour l'enregistrer sur votre téléphone. Envoyez la photo à notre service d'assistance technique.

**Note**

Pour les opérations suivantes de réinitialisation du mot de passe, contactez notre support technique.

**Attention**

La force du mot de passe de l'appareil peut être automatiquement vérifiée. Nous vous recommandons vivement de modifier le mot de passe de votre choix (en utilisant un minimum de 8 caractères, dont au moins trois des catégories suivantes : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) afin d'accroître la sécurité de votre produit. Nous vous recommandons également de modifier votre mot de passe régulièrement, en particulier dans le cas d'un système de haute sécurité, un changement de mot de passe mensuel ou hebdomadaire permet de mieux protéger votre produit.
La configuration correcte de tous les mots de passe et autres paramètres de sécurité relève de la responsabilité de 'installateur et/ou de l'utilisateur final.

### 10.2.3 Gérer les appareils ajoutés

Après avoir ajouté des appareils à la liste des appareils, vous pouvez gérer les appareils ajoutés, y compris la modification des paramètres de l'appareil, la configuration à distance, la visualisation de l'état de l'appareil, etc.

**Tableau 10-1 Gérer les dispositifs ajoutés**

| | |
|---|---|
| Modifier le dispositif | Cliquez sur pour modifier les informations relatives à l'appareil, notamment son nom, son adresse, son nom d'utilisateur, son mot de passe, etc. |
| Supprimer le dispositif | Cochez un ou plusieurs appareils, puis cliquez sur **Supprimer** pour supprimer les appareils sélectionnés. |
| Configuration à distance | Cliquez sur pour définir la configuration à distance de l'appareil correspondant. Pour plus de détails, reportez-vous au manuel d'utilisation de l'appareil. |
| Visualiser l'état de l'appareil | Cliquez sur pour afficher l'état de l'appareil, y compris le numéro de porte, l'état de la porte, etc.<br>**Note**<br>Les informations relatives à l'état des appareils varient en fonction de l'appareil. |
| Voir l'utilisateur en ligne | Cliquez sur pour afficher les détails de l'utilisateur en ligne qui accède à l'appareil, y compris le nom d'utilisateur, le type d'utilisateur, l'adresse IP et l'heure de connexion. |
| Rafraîchir les informations sur l'appareil | Cliquez sur pour actualiser et obtenir les dernières informations sur l'appareil. |

## 10.3 Gestion du groupe

Le client fournit des groupes pour gérer les ressources ajoutées dans différents groupes. Vous pouvez regrouper les ressources dans différents groupes en fonction de leur emplacement.

**Exemple**
Par exemple, au 1er étage, il y a 16 portes, 64 entrées d'alarme et 16 sorties d'alarme. Vous pouvez organiser ces ressources en un seul groupe (appelé 1er étage) pour une gestion plus pratique. Vous pouvez contrôler l'état des portes et effectuer d'autres opérations sur les dispositifs après avoir géré les ressources par groupes.

### 10.3.1 Ajouter un groupe

Vous pouvez ajouter des groupes pour organiser les appareils ajoutés afin d'en faciliter la gestion.

**Étapes**
1. Entrez dans le module de gestion des appareils.
2. Cliquez sur **Device Management (Gestion des appareils→Group (Groupe)** pour accéder à la page de gestion des groupes.
3. Créer un groupe.
   - Cliquez sur **Ajouter un groupe** et saisissez le nom du groupe que vous souhaitez.
   - Cliquez sur **Créer un groupe par nom de périphérique** et sélectionnez un périphérique ajouté pour créer un nouveau groupe portant le nom du périphérique sélectionné.

   **Note**
   Les ressources (telles que les entrées/sorties d'alarme, les points d'accès, etc.) de cet appareil seront importées dans le groupe par défaut.

### 10.3.2 Importer des ressources dans un groupe

Vous pouvez importer les ressources des dispositifs (telles que les entrées/sorties d'alarme, les points d'accès, etc.) dans groupe ajouté par lots.

**Avant de commencer**
Ajoutez un groupe pour gérer les appareils. Voir ***Ajouter un groupe*** .

**Étapes**
1. Entrez dans le module de gestion des appareils.
2. Cliquez sur **Device Management (Gestion des appareils→Group (Groupe)** pour accéder à la page de gestion des groupes.
3. Sélectionnez un groupe dans la liste des groupes et sélectionnez le type de ressource comme **Point d'accès**, **Entrée d'alarme**, **Sortie d'alarme**, etc.
4. Cliquez sur **Importer**.
5. Sélectionnez les vignettes/noms des ressources dans la vue vignettes/liste.

**Note**

Vous pouvez cliquer sur ou sur pour passer du mode d'affichage des ressources à l'affichage sous forme de vignettes ou de listes.

**6.** Cliquez sur **Importer** pour importer les ressources sélectionnées dans le groupe.

## 10.4 Gestion des personnes

Vous pouvez ajouter des informations sur les personnes au système pour d'autres opérations telles que le contrôle d'accès, l'interphone vidéo, la gestion du temps et des présences, etc. Vous pouvez gérer les personnes ajoutées, par exemple en leur délivrant des cartes par lots, en important et en exportant des informations sur les personnes par lots, etc.

### 10.4.1 Ajouter une organisation

Vous pouvez ajouter une organisation et importer des informations sur les personnes dans l'organisation pour une gestion efficace des personnes. Vous pouvez également ajouter une organisation secondaire à l'ajoutée.

**Étapes**

**1.** Entrer dans le module **Personne.**

**2.** Sélectionnez une organisation mère dans la colonne de gauche et cliquez sur **Ajouter** dans le coin supérieur gauche pour ajouter une organisation.

**3.** Créez un nom pour l'organisation ajoutée.

**Note**

Il est possible d'ajouter jusqu'à 10 niveaux d'organisations.

**4. En option :** Effectuez la ou les opérations suivantes.

**Modifier une organisation** Passez la souris sur une organisation ajoutée et cliquez sur pour modifier son nom.

**Supprimer l'organisation** Passez la souris sur une organisation ajoutée et cliquez sur pour la supprimer.

**Note**

- Les organisations de niveau inférieur seront également supprimées si vous supprimez une organisation.
- Assurez-vous qu'aucune personne n'a été ajoutée sous l'organisation, sinon l'organisation ne peut pas être supprimée.

**Afficher les personnes dans la sous-organisation** Cochez la case **Afficher les personnes dans les sous-organisations** et sélectionnez une organisation pour afficher les personnes dans ses sous-organisations.

### 10.4.2 Importation et exportation d'informations d'identification des personnes

Vous pouvez importer par lots les informations et les photos de plusieurs personnes dans le logiciel client. Parallèlement, vous pouvez également exporter les informations et les photos des personnes et les enregistrer sur votre PC.

## Importer des informations sur les personnes

Vous pouvez saisir les informations de plusieurs personnes dans un modèle prédéfini (fichier CSV/Excel) pour les importer par lots dans le client.

**Étapes**

1. Entrez dans le module Personne.
2. Sélectionnez une organisation ajoutée dans la liste ou cliquez sur **Ajouter** dans le coin supérieur gauche pour ajouter une organisation et la sélectionner.
3. Cliquez sur **Importer** pour ouvrir le panneau d'importation.
4. Sélectionnez **Information sur** la **personne** comme mode d'importation.
5. Cliquez sur **Télécharger le modèle d'importation de la personne** pour télécharger le modèle.
6. Saisissez les informations relatives à la personne dans le modèle téléchargé.

**Note**

- Si la personne possède plusieurs cartes, séparez le numéro de la carte par un point-virgule.
- Les éléments marqués d'un astérisque sont obligatoires.
- Par défaut, la date d'embauche est la date du jour.

7. Cliquez sur pour sélectionner le fichier CSV/Excel contenant les informations sur les personnes à partir du PC local.
8. Cliquez sur **Importer** pour commencer l'importation.

**Note**

- Si un numéro de personne existe déjà dans la base de données du client, supprimez les informations existantes avant l'importation.
- Vous pouvez importer des informations sur un maximum de 2 000 personnes.

## Importer des photos de personnes

Après avoir importé les photos de visage des personnes ajoutées au client, les personnes figurant sur les photos peuvent identifiées par un terminal de reconnaissance faciale supplémentaire. Vous pouvez importer les photos d'une personne une par une ou importer plusieurs photos à la fois, selon vos besoins.

**Avant de commencer**

Veillez à ce que les informations sur la personne importée soient communiquées au client à l'avance.

**Étapes**

1. Entrez dans le module Personne.
2. Sélectionnez une organisation ajoutée dans la liste ou cliquez sur **Ajouter** dans le coin supérieur gauche pour ajouter une organisation et la sélectionner.
3. Cliquez sur **Importer** pour ouvrir le panneau d'importation et vérifiez la **face**.
4. **Facultatif :** Activez l'option **Vérifier par le** dispositif pour vérifier si le dispositif de reconnaissance faciale géré par client peut reconnaître le visage sur la photo.
5. Cliquez sur pour sélectionner un fichier d'image de visage.

**Note**

- Le (dossier ) photos de face doit être au format ZIP.
- Chaque fichier image doit être au format JPG et ne doit pas dépasser 200 KB.
- Chaque fichier image doit être nommé "ID_Nom de la personne". L'identifiant de la personne doit être le même que celui des informations importées.

6. Cliquez sur **Importer** pour commencer l'importation.
   La progression et le résultat de l'importation s'affichent.

## Informations sur la personne à exporter

Vous pouvez exporter les informations relatives aux personnes ajoutées vers un PC local sous la forme d'un fichier CSV/Excel.

**Avant de commencer**

Assurez-vous d'avoir ajouté des personnes à une organisation.

**Étapes**

1. Entrez dans le module Personne.
2. **Optionnel :** Sélectionnez une organisation dans la liste.

   **Note**

   Toutes les informations relatives aux personnes seront exportées si vous ne sélectionnez aucune organisation.
3. Cliquez sur **Exporter** pour ouvrir le panneau Exporter.
4. Cochez **Information sur** la **personne** comme contenu à exporter.
5. Cochez les éléments à exporter.
6. Cliquez sur **Exporter** pour enregistrer le fichier exporté dans un fichier CSV/Excel sur votre PC.

## Exporter des images de personnes

Vous pouvez exporter les photos des personnes ajoutées et les enregistrer sur votre PC.

**Avant de commencer**

Assurez-vous d'avoir ajouté des personnes et leurs photos à une organisation.

**Étapes**

1. Entrez dans le module Personne.
2. **Optionnel :** Sélectionnez une organisation dans la liste.

   **Note**

   Toutes les photos de visage des personnes seront exportées si vous ne sélectionnez aucune organisation.
3. Cliquez sur **Exporter** pour ouvrir le panneau Exporter et cochez **Face** comme contenu à exporter.
4. Cliquez sur **Exporter** pour lancer l'exportation.

**Note**

- Le fichier exporté est au format ZIP.
- L'image de visage exportée est nommée "Person ID_Name_0" ("0" pour un visage de face).

### 10.4.3 Obtenir des informations sur les personnes à partir d'un dispositif de contrôle d'accès

Si le dispositif de contrôle d'accès ajouté a été configuré avec des informations sur les personnes (y compris les coordonnées de la personne, l'empreinte digitale et les informations de la carte émise), vous pouvez obtenir les informations sur les personnes à partir du dispositif et les importer dans le client pour d'autres opérations.

**Étapes**

**Note**

- Si le nom de la personne stocké dans l'appareil est vide, le nom de la personne sera complété par le numéro de la carte émise après l'importation vers le client.
- Si le numéro de carte ou l'ID de personne (ID d'employé) enregistré sur le dispositif existe déjà dans la base de données du client, la personne portant ce numéro de carte ou cet ID de personne ne sera pas importée dans le client.

1. Entrer dans le module **Personne.**
2. Sélectionnez une organisation pour importer les personnes.
3. Cliquez sur **Obtenir de l'appareil**.
4. Sélectionnez un dispositif de contrôle d'accès ajouté ou la station d'enrôlement dans la liste déroulante.

   **Note**

   Si vous sélectionnez la station d'inscription, vous devez cliquer sur **Connexion** et définir l'adresse IP, le numéro de port, le nom d'utilisateur et le mot de passe de l'appareil.
5. Cliquez sur **Importer** pour commencer à importer les informations relatives à la personne dans le client.

   **Note**

   Il est possible d'importer jusqu'à 2 000 personnes et 5 000 cartes.

   Les informations relatives à la personne, y compris ses coordonnées, ses empreintes digitales (si elles sont configurées) et les cartes liées (si elles sont configurées), seront importées dans l'organisation sélectionnée.

### 10.4.4 Délivrer des cartes à des personnes par lot

Le client offre un moyen pratique de délivrer des cartes à plusieurs personnes en un seul lot.

**Étapes**

1. Entrer dans le module **Personne.**
2. Cliquez sur **Émission de cartes par lots**.

   Toutes les personnes ajoutées sans carte délivrée seront affichées dans le panneau de droite.

3. **Facultatif :** Saisissez des mots clés (nom ou ID de la personne) dans le champ de saisie pour filtrer les personnes qui ont besoin de cartes de délivrance.
4. **En option, cliquez sur Paramètres pour définir les paramètres d'émission des cartes :** Cliquez sur **Paramètres** pour définir les paramètres d'émission des cartes. Pour plus d'informations, reportez-vous à la section *Émission d'une carte en mode local*.
5. Cliquez sur **Initialiser** pour initialiser la station d'enrôlement des cartes ou le lecteur de cartes afin qu'ils soient prêts à émettre des cartes.
6. Cliquez sur la colonne **N° de carte** et saisissez le numéro de la carte.
   - Placez la carte sur la station d'enrôlement des cartes.
   - Passez la carte sur le lecteur de cartes.
   - Introduisez manuellement le numéro de la carte et appuyez sur

   la touche **Entrée.** La ou les personne(s) figurant dans la liste

   recevront une ou plusieurs carte(s).

### 10.4.5 Perte du bulletin de notes

Si la personne a perdu sa carte, vous pouvez signaler la perte de la carte afin que l'autorisation d'accès à la carte soit désactivée.

**Étapes**

1. Entrer dans le module **Personne.**
2. Sélectionnez la personne pour laquelle vous souhaitez signaler une perte de carte et cliquez sur **Modifier** pour ouvrir la fenêtre Modifier la personne.
3. Dans le panneau **Credential→ Card**, cliquez sur sur la carte ajoutée pour définir cette carte comme carte perdue.

   Après avoir signalé la perte de la carte, l'autorisation d'accès de cette carte sera invalide et inactive. Une autre personne qui reçoit cette carte ne peut pas accéder aux portes en passant cette carte perdue.
4. **Facultatif :** si la carte perdue est retrouvée, vous pouvez cliquer sur pour annuler la perte.

   Après l'annulation de la perte de la carte, l'autorisation d'accès de la personne sera valide et active.
5. Si la carte perdue est ajoutée à un groupe d'accès et que le groupe d'accès est déjà appliqué à l'appareil, après avoir signalé la perte de la carte ou annulé la perte de la carte, une fenêtre s'ouvrira pour vous demander d'appliquer les changements à l'appareil. Après l'application au dispositif, ces changements peuvent prendre effet sur le dispositif.

### 10.4.6 Définir les paramètres d'émission des cartes

Le client propose deux modes de lecture du numéro d'une carte : via la station d'enrôlement des cartes ou via le lecteur de cartes du dispositif de contrôle d'accès. Si une station d'enrôlement des cartes est disponible, connectez-la au PC exécutant le client par l'interface USB ou COM, et placez la carte sur la station d'enrôlement des cartes pour lire le numéro de la carte. , vous pouvez également glisser la carte sur le lecteur de cartes du dispositif de contrôle d'accès ajouté pour obtenir le numéro de la carte. Par conséquent, avant de délivrer une carte à une personne, vous devez définir paramètres d'émission de la carte, y compris le mode d'émission et les paramètres connexes.

Lorsque vous ajoutez une carte à une personne, cliquez sur **Paramètres** pour ouvrir la fenêtre Paramètres d'émission des cartes.

### Mode local : Émission de la carte par la station d'enrôlement de la carte

Connectez une station d'enrôlement des cartes au PC qui exécute le client. Vous pouvez placer la carte sur la station d'enrôlement pour obtenir le numéro de la carte.

**Station d'enrôlement des cartes**

Sélectionner le modèle de la station d'enrôlement de cartes connectée

**Note**

Actuellement, les modèles de stations d'enrôlement de cartes pris en charge sont les suivants : DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E et DS-K1F180-D8E.

**Type de carte**

Ce champ n'est disponible que lorsque le modèle est DS-K1F100-D8E ou DS-K1F180-D8E.

Sélectionnez le type de carte (carte EM ou carte IC) en fonction du type de carte actuel.

**Port série**

Elle n'est disponible que lorsque le modèle est DS-K1F100-M.

Sélectionnez la COM à laquelle la station d'enrôlement des cartes

se connecte.

**Buzzing**

Active ou désactive le signal sonore lorsque le numéro de la carte est lu avec succès.

**N° de carte Type**

Sélectionnez le type de numéro de carte en fonction de vos besoins.

**Chiffrement de la carte M1**

Ce champ n'est disponible que lorsque le modèle est DS-K1F100-D8, DS-K1F100-D8E ou DS-K1F180-D8E.

Si la carte est une carte M1 et si vous devez activer la fonction de cryptage de la carte M1, vous devez activer cette fonction et sélectionner le secteur de la carte à crypter.

### Mode à distance : Émission de cartes par lecteur de cartes

Sélectionnez un dispositif de contrôle d'accès ajouté dans le client et passez la carte sur son lecteur pour lire le numéro de la carte.

## 10.5 Configuration du calendrier et du modèle

Vous pouvez configurer le modèle en y incluant les vacances et le calendrier hebdomadaire. Après avoir défini le modèle, vous pouvez adopter le modèle configuré pour les groupes d'accès lors de la définition des groupes d'accès, de sorte que le groupe d'accès prenne effet pendant les durées du modèle.

**Note**

Pour les paramètres des groupes d'accès, voir ***Définir un groupe d'accès pour attribuer une autorisation d'accès à des personnes***.

### 10.5.1 Ajouter des vacances

Vous pouvez créer des jours fériés et définir les jours de ces jours, y compris la date de début, la date de fin et la durée du jour férié en un seul jour.

**Étapes**

**Note**

Vous pouvez ajouter jusqu'à 64 jours fériés dans le système logiciel.

1. Cliquez sur **Access Control→ Schedule→ Holiday** pour accéder à la page Holiday.
2. Cliquez sur **Ajouter** dans le panneau de gauche.
3. Créez un nom pour la fête.
4. **Facultatif :** Saisissez les descriptions ou certaines notifications relatives à ce jour férié dans la case Remarques.
5. Ajoutez une période de vacances à la liste des vacances et configurez la durée des vacances.

   **Note**

   Il est possible d'ajouter jusqu'à 16 périodes de vacances à un même séjour.

   1) Cliquez sur **Ajouter** dans le champ Liste de vacances.
   2) Faites glisser le curseur pour dessiner la durée, ce qui signifie que le groupe d'accès configuré est activé pendant cette durée.

      **Note**

      Il est possible de définir jusqu'à 8 durées pour une période de vacances.

   3) **En option, vous pouvez effectuer les opérations suivantes pour modifier les durées de temps :** Effectuez les opérations suivantes pour modifier les durées.
      - Déplacez le curseur sur la durée et faites glisser la durée sur la barre temporelle jusqu'à position souhaitée lorsque le curseur devient .
      - Cliquez sur la durée et modifiez directement l'heure de début et de fin dans la boîte de dialogue qui s'affiche.
      - Déplacez le curseur sur le début ou la fin de la durée et faites-le glisser pour allonger ou raccourcir la durée lorsque le curseur devient .
   4) **Facultatif :** Sélectionnez la ou les périodes à supprimer, puis cliquez sur dans colonne Opération pour supprimer la ou les périodes sélectionnées.
   5) **En option :** Cliquez sur dans la colonne Opération pour effacer toutes les durées dans la barre de temps.
   6) **En option :** Cliquez sur dans la colonne Opération pour supprimer la période de vacances ajoutée de liste des vacances.
6. Cliquez sur **Enregistrer**.

### 10.5.2 Ajouter un modèle

Le modèle comprend un calendrier hebdomadaire et des vacances. Vous pouvez définir un calendrier hebdomadaire et attribuer la durée de l'autorisation d'accès à différentes personnes ou à différents groupes. Vous pouvez également sélectionner le(s) jour(s) férié(s) ajouté(s) au modèle.

**Étapes**

**Note**

Vous pouvez ajouter jusqu'à 255 modèles dans le logiciel.

1. Cliquez sur **Access Control→ Schedule→ Template** pour accéder à la page Template.

   **Note**

   Il existe deux modèles par défaut : Autorisé toute la journée et Refusé toute la journée, qui ne peuvent être ni modifiés ni supprimés.

   **Autorisé toute la journée**

   L'autorisation d'accès est valable chaque jour de la semaine et n'a pas de vacances.

   **Toute la journée refusée**

   L'autorisation d'accès est invalide chaque jour de la semaine et il n'y a pas de jour férié.

2. Cliquez sur **Ajouter** dans le panneau de gauche pour créer un nouveau modèle.
3. Créez un nom pour le modèle.
4. Saisissez la description ou une notification de ce modèle dans la case Remarque.
5. Modifiez l'horaire hebdomadaire pour l'appliquer au modèle.
   1) Cliquez sur l'onglet **Calendrier hebdomadaire** dans le panneau inférieur.
   2) Sélectionnez un jour de la semaine et dessinez la durée sur la barre temporelle.

      **Note**

      Il est possible de définir jusqu'à 8 durées pour chaque jour de la semaine.

   3) **En option, vous pouvez effectuer les opérations suivantes pour modifier les durées de temps :** Effectuez les opérations suivantes pour modifier les durées.
      - Déplacez le curseur sur la durée et faites glisser la durée sur la barre temporelle jusqu'à position souhaitée lorsque le curseur devient .
      - Cliquez sur la durée et modifiez directement l'heure de début et de fin dans la boîte de dialogue qui s'affiche.
      - Déplacez le curseur sur le début ou la fin de la durée et faites-le glisser pour allonger ou raccourcir la durée lorsque le curseur devient .
   4) Répétez les deux étapes ci-dessus pour dessiner d'autres durées pour les autres jours de la semaine.
6. Ajouter un jour férié pour l'appliquer au modèle.

   **Note**

   Jusqu'à 4 jours fériés peuvent être ajoutés à un modèle.

   1) Cliquez sur l'onglet **Vacances**.
   2) Sélectionnez un jour férié dans la liste de gauche et il sera ajouté à la liste sélectionnée dans le panneau de droite.
   3) **Facultatif :** Cliquez sur **Ajouter** pour ajouter un nouveau jour férié.

      **Note**

      Pour plus d'informations sur l'ajout d'un jour férié, voir ***Ajouter un jour férié***.

4) **Facultatif :** Sélectionnez un jour férié dans la liste de droite et cliquez sur pour supprimer le jour férié sélectionné, ou cliquez sur Effacer pour effacer tous les jours fériés sélectionnés dans la liste de droite.

**7.** Cliquez sur **Enregistrer** pour sauvegarder les paramètres et terminer l'ajout du modèle.

## 10.6 Définir un groupe d'accès pour attribuer des autorisations d'accès à des personnes

Après avoir ajouté la et configuré ses informations d'identification, vous pouvez créer les groupes d'accès pour définir quelle(s) personne(s) peut(vent) accéder à quelle(s) porte(s), puis appliquer le groupe d'accès au dispositif de contrôle d'accès pour qu'il prenne effet.

**Avant de commencer**

- Ajouter une personne au client.
- Ajouter un dispositif de contrôle d'accès au client et grouper les points d'accès. Pour plus d'informations, reportez-vous à la section ***Gestion des groupes*** .
- Ajouter un modèle.

**Étapes**

Lorsque les paramètres des groupes d'accès sont modifiés, vous devez à nouveau appliquer les groupes d'accès aux dispositifs pour qu'ils prennent effet. Les modifications des groupes d'accès comprennent les modifications du modèle, des paramètres du groupe d'accès, des paramètres du groupe d'accès de la personne et des détails relatifs à la personne (y compris le numéro de la carte, l'empreinte digitale, la photo du visage, le lien entre le numéro de la carte et l'empreinte digitale, le lien entre le numéro de la carte et l'empreinte digitale, le mot de passe de la carte, la période d'effet de la carte, etc.)

**1.** Cliquez sur **Access Control→ Authorization→ Access Group** pour accéder à l'interface Access Group.

**2.** Cliquez sur **Ajouter** pour ouvrir la fenêtre Ajouter.

**3.** Dans le champ de texte **Nom**, créez un nom pour le groupe d'accès comme vous le souhaitez.

**4.** Sélectionnez un modèle pour le groupe d'accès.

**Note**

Vous devez configurer le modèle avant les paramètres du groupe d'accès. Pour plus d'informations, reportez-vous à la section ***Configuration de la programmation et du modèle.***

**5.** Dans la liste de gauche du champ Select Person, sélectionnez la ou les personne(s) à qui attribuer une autorité d'accès.

**6.** Dans la liste de gauche du champ Sélectionner un point d'accès, sélectionnez la ou les portes, la ou les platines de rue ou le ou les étages auxquels les personnes sélectionnées doivent accéder.

**7.** Cliquez sur **Enregistrer**.

Vous pouvez voir la ou les personnes sélectionnées et le ou les points d'accès sélectionnés sur le côté droit de l'interface.

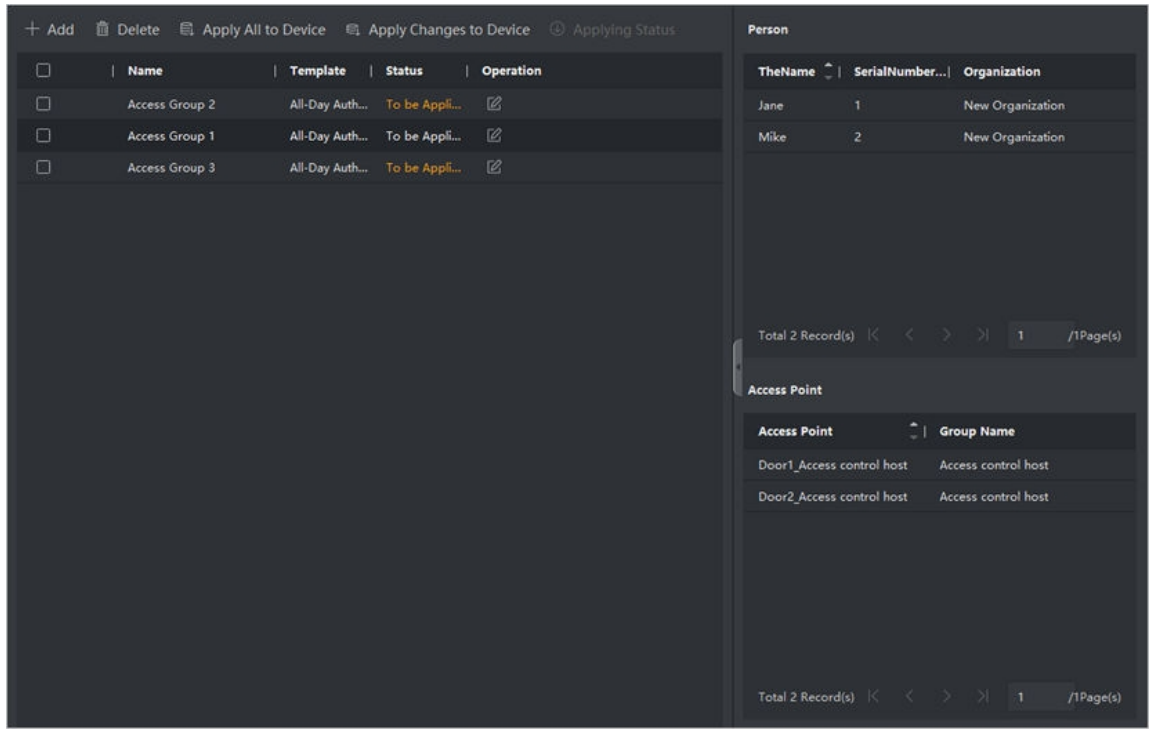



**Figure 10-2 Afficher les personnes et les points d'accès sélectionnés**

**8.** Après avoir ajouté les groupes d'accès, vous devez les appliquer au dispositif de contrôle d'accès pour qu'ils prennent effet.

1) Sélectionnez le(s) groupe(s) d'accès à appliquer au dispositif de contrôle d'accès.
2) Cliquez sur **Appliquer tout aux appareils pour** commencer à appliquer tous les groupes d'accès sélectionnés au dispositif de contrôle d'accès ou au poste de porte.
3) Cliquez sur **Appliquer tout aux dispositifs** ou **sur Appliquer les modifications aux dispositifs**. **Appliquer tout aux dispositifs**

   Cette opération efface tous les groupes d'accès existants des appareils sélectionnés et applique ensuite le nouveau groupe d'accès à l'appareil.

   **Appliquer les modifications aux dispositifs**

   Cette opération n'efface pas les groupes d'accès existants des appareils sélectionnés et n'applique que la partie modifiée du ou des groupes d'accès sélectionnés à l'appareil ou aux appareils.
4) Affichez le statut de l'application dans la colonne Statut ou cliquez sur **Statut de l'application** pour afficher tous les groupes d'accès appliqués.

**Note**

Vous pouvez cocher la case **Afficher uniquement les échecs** pour filtrer les résultats de l'application.

Les personnes sélectionnées dans les groupes d'accès appliqués auront l'autorisation d'entrer/sortir des portes/postes de porte sélectionnés à l'aide de leur(s) carte(s) ou empreinte(s) digitale(s) liée(s).

**9. Facultatif :** Cliquez sur pour modifier le groupe d'accès si nécessaire.

**Note**

Si vous modifiez les informations d'accès des personnes ou d'autres informations connexes, vous verrez apparaître le message **Groupe d'**accès **à appliquer** dans le coin droit du client.
Vous pouvez cliquer sur l'invite pour appliquer les données modifiées au périphérique. Vous pouvez sélectionner **Appliquer maintenant** ou **Appliquer plus tard**.

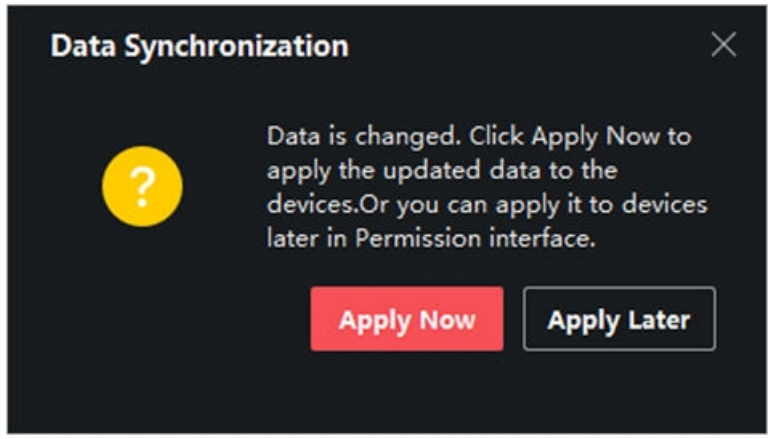



**Figure 10-3 Synchronisation des données**

## 10.7 Configuration des fonctions avancées

Vous pouvez configurer les fonctions avancées du contrôle d'accès pour répondre à certaines exigences particulières dans différents contextes.

**Note**

- Pour les fonctions liées aux cartes (le type de carte de contrôle d'accès), seules les cartes auxquelles un groupe d'accès a été appliqué seront répertoriées lors de l'ajout de cartes.
- Les fonctions avancées doivent être prises en charge par l'appareil.
- Placez le curseur sur la fonction avancée, puis cliquez sur pour personnaliser la ou les fonctions avancées à afficher.

### 10.7.1 Configuration des paramètres de l'appareil

Après avoir ajouté le dispositif de contrôle d'accès, vous pouvez configurer les paramètres du dispositif de contrôle d'accès, les points de contrôle d'accès.

## Configuration des paramètres du dispositif de contrôle d'accès

Après avoir ajouté le dispositif de contrôle d'accès, vous pouvez configurer ses paramètres, y compris la superposition des informations de l'utilisateur sur l'image, le téléchargement des images après la capture, l'enregistrement des images capturées, etc.

**Étapes**

1. Cliquez sur **Contrôle d'accès→ Fonction avancée→ Paramètre de l'appareil** .

**Note**

Si vous trouvez le paramètre de l'appareil dans la liste des fonctions avancées, placez le curseur sur fonction avancée, puis cliquez sur pour sélectionner le paramètre de l'appareil à afficher.

2. Sélectionnez un dispositif d'accès pour afficher ses paramètres sur la page de droite.
3. Placez l'interrupteur sur ON pour activer les fonctions correspondantes.

**Note**

- Les paramètres affichés peuvent varier selon les dispositifs de contrôle d'accès.
- Certains des paramètres suivants ne sont pas répertoriés dans la page Informations de base, cliquez sur **Plus** pour modifier les paramètres.

**Invite vocale**

Si vous activez cette fonction, l'invite vocale est activée dans l'appareil. Vous pouvez entendre l'invite vocale lorsque vous utilisez l'appareil.

**Télécharger la photo. Après la capture liée**

Télécharger automatiquement sur le système les images capturées par l'appareil photo associé.

**Sauvegarder la photo. Après la capture liée**

Si vous activez cette fonction, vous pouvez enregistrer l'image capturée par l'appareil photo lié sur l'appareil.

**Mode reconnaissance des**

**visages Mode normal**

Reconnaître un visage via l'appareil photo normalement.

**Mode profond**

L'appareil peut reconnaître une gamme de personnes beaucoup plus large que le mode normal. Ce mode s'applique à un environnement plus complexe.

**Activer la carte NFC**

Si la fonction est activée, l'appareil peut reconnaître la carte NFC. Vous pouvez présenter la carte NFC à l'appareil.

**Activer la carte M1**

Si la fonction est activée, l'appareil peut reconnaître la carte M1. Vous pouvez présenter la carte M1 sur l'appareil.

**Activer la carte EM**

Si la fonction est activée, l'appareil peut reconnaître la carte EM. Vous pouvez présenter la carte EM à l'appareil.

**Note**

Si le lecteur de carte périphérique prend en charge la présentation de la carte EM, la fonction d'activation/désactivation de la fonction de carte EM est également prise en charge.

4. Cliquez sur **OK**.
5. **Optionnel :** Cliquez sur **Copier vers**, puis sélectionnez le(s) dispositif(s) de contrôle d'accès pour copier les paramètres de la page vers le(s) dispositif(s) sélectionné(s).

## Configuration des paramètres pour la porte/l'ascenseur

Après avoir ajouté le dispositif de contrôle d'accès, vous pouvez configurer les paramètres de son point d'accès (porte ou étage).

**Avant de commencer**

Ajouter un dispositif de contrôle d'accès au client.

**Étapes**

1. Cliquez sur **Contrôle d'accès→ Fonction avancée→ Paramètre de l'appareil** .
2. Sélectionnez un dispositif de contrôle d'accès dans le panneau de gauche, puis cliquez sur pour afficher les portes ou les étages du dispositif sélectionné.
3. Sélectionnez une porte ou un étage pour afficher ses paramètres sur la page de droite.
4. Modifier les paramètres de la porte ou du sol.

**Note**

- Les paramètres affichés peuvent varier selon les dispositifs de contrôle d'accès.
- Certains des paramètres suivants ne sont pas répertoriés dans la page Informations de base, cliquez sur **Plus** pour modifier les paramètres.

**Nom**

Modifiez le nom du lecteur de cartes comme vous le souhaitez.

**Contact de porte**

Vous pouvez définir le capteur de porte comme restant fermé ou restant ouvert. En règle générale, le capteur reste fermé.

**Type de bouton de sortie**

Vous pouvez définir le bouton de sortie comme restant fermé ou restant ouvert. En général, il reste ouvert.

**Temps de verrouillage de la porte**

Après le passage de la carte normale et l'action du relais, la minuterie de verrouillage de la porte commence à fonctionner.

**Durée d'ouverture prolongée**

Le contact de la porte peut être activé avec un délai approprié après que la personne ayant des besoins d'accès étendus a glissé sa carte.

**Alarme de délai d'ouverture de la porte**

L'alarme peut être déclenchée si la porte n'a pas été fermée pendant une période de temps configurée. S'il est réglé sur 0, aucune alarme ne sera déclenchée.

**Verrouiller la porte lorsqu'elle est fermée**

La porte peut être verrouillée une fois qu'elle est fermée, même si le **temps de verrouillage de la porte** n'est pas atteint.

**Code de contrainte**

En cas de contrainte, la porte peut s'ouvrir en entrant le code de contrainte. En même temps, le client peut signaler l'événement de contrainte.

**Super mot de passe**

La personne concernée peut ouvrir la porte en saisissant le super mot de passe.

**Annuler le code**

Créez un code d'annulation qui peut être utilisé pour arrêter le buzzer du lecteur de cartes (en entrant le code d'annulation sur le clavier).

**Note**

- Le code de contrainte, le super code et le code de licenciement doivent être différents.
- code de contrainte, le super mot de passe et le code de renvoi doivent être différents du mot de passe d'authentification.
- La longueur du code de contrainte, du super mot de passe et du code de renvoi dépend de l'appareil, mais doit généralement comporter de 4 à 8 chiffres.

5. Cliquez sur **OK**.
6. **Optionnel :** Cliquez sur **Copier vers** , puis sélectionnez la ou les portes/étages pour copier les paramètres de la page sur les portes/étages sélectionnés.

**Note**

Les paramètres de durée de l'état de la porte ou de l'étage seront également copiés sur la (les) porte(s) ou l'étage sélectionné(s).

## Configuration des paramètres du lecteur de cartes

Après avoir ajouté le dispositif de contrôle d'accès, vous pouvez configurer les paramètres de son lecteur de cartes.

**Avant de commencer**

Ajouter un dispositif de contrôle d'accès au client.

**Étapes**

1. Cliquez sur **Contrôle d'accès→ Fonction avancée→ Paramètre de l'appareil** .
2. Dans la liste des appareils à gauche, cliquez sur pour développer la porte, sélectionnez un lecteur de cartes et vous pouvez modifier les paramètres du lecteur de cartes à droite.
3. Modifiez les paramètres de base du lecteur de cartes dans la page Informations de base.

**Note**

- Les paramètres affichés peuvent varier selon les dispositifs de contrôle d'accès. Une partie paramètres est répertoriée comme suit. Pour plus de détails, reportez-vous au manuel d'utilisation de l'appareil.
- Certains des paramètres suivants ne sont pas répertoriés dans la page Informations de base, cliquez sur **Plus** pour modifier les paramètres.

**Nom**

Modifiez le nom du lecteur de cartes comme vous le souhaitez.

**Polarité de la LED OK/Polarité de la LED d'erreur/Polarité du buzzer**

Réglez la polarité de la LED OK/Polarité de la LED Erreur/Polarité de la LED Buzzer de la carte principale en fonction des paramètres du lecteur de cartes. En général, les paramètres par défaut sont adoptés.

**Intervalle minimum de passage de la carte**

Si l'intervalle entre deux passages de la même carte est inférieur à la valeur définie, le passage de la carte n'est pas valide. La valeur peut être comprise entre 0 et 255.

**Intervalle max. Intervalle lors de la saisie du PWD**

Lorsque vous saisissez le mot de passe sur le lecteur de cartes, si l'intervalle entre la pression de deux chiffres est supérieur à la valeur définie, les chiffres que vous avez appuyés auparavant seront automatiquement effacés.

**Alarme de tentatives max. Tentatives échouées**

Permet de déclencher une alarme lorsque les tentatives de lecture de la carte atteignent la valeur définie.

**Max. Temps de défaillance de la carte**

Définir le nombre maximum de tentatives d'échec de la lecture de la carte.

**Détection de sabotage**

Activer la détection anti-sabotage pour le lecteur de cartes.

**Communiquer avec le contrôleur Chaque**

Lorsque le dispositif de contrôle d'accès ne peut pas se connecter au lecteur de cartes pendant la durée programmée, le lecteur de cartes se déconnecte automatiquement.

**L'heure du buzzing**

Régler le temps de sonnerie du lecteur de cartes. Le temps disponible est compris entre 0 et 5 999 secondes. 0 représente un bourdonnement continu.

**Type de lecteur de cartes/Description du lecteur de cartes**

Obtenir le type et la description du lecteur de cartes. Ils sont en lecture seule.

**Niveau de reconnaissance des empreintes digitales**

Sélectionnez le niveau de reconnaissance des empreintes digitales dans la liste déroulante.

**Mode d'authentification par défaut du lecteur de cartes**

Afficher le mode d'authentification par défaut du lecteur de cartes.

**Capacité d'empreintes digitales**

Afficher le nombre maximum d'empreintes digitales disponibles.

**Numéro d'empreinte digitale existant**

Afficher le nombre d'empreintes digitales existantes dans l'appareil.

**Score**

L'appareil évalue l'image capturée en fonction de l'angle de lacet, de l'angle de tangage et de l'écart pupillaire. Si le score est inférieur à la valeur configurée, la reconnaissance des visages échoue.

**Valeur du délai de reconnaissance des visages**

Si le temps de reconnaissance est supérieur au temps configuré, l'appareil vous le rappelle.

**Intervalle de reconnaissance des visages**

Intervalle de temps entre deux reconnaissances continues du visage lors de l'authentification. Par défaut, il est de 2 secondes.

**Seuil de concordance des visages 1:1**

Définir le seuil de correspondance lors de l'authentification en mode 1:1. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé lors de l'authentification.

**1:N Niveau de sécurité**

Définit le niveau de sécurité de la correspondance lors de l'authentification via le mode de correspondance 1:N. Plus la valeur est élevée, plus le taux de fausses acceptations est faible et plus le taux de faux rejets est élevé lors de l'authentification.

**Détection des visages en direct**

Active ou désactive la fonction de détection des visages vivants. Si cette fonction est activée, l'appareil peut reconnaître si la personne est vivante ou non.

**Détection des visages en direct Niveau de sécurité**

Après avoir activé la fonction de détection des visages en direct, vous pouvez définir le niveau de sécurité correspondant lors de l'authentification des visages en direct.

**Max. Tentatives d'échec pour l'authentification des visages.**

Définir le nombre maximum de tentatives d'échec de la détection des visages en direct. Le système verrouille le visage de l'utilisateur pendant 5 minutes si la détection du visage en direct échoue au-delà du nombre de tentatives configuré. Le même utilisateur ne peut pas s'authentifier via le faux visage dans les 5 minutes. Pendant ces 5 minutes, l'utilisateur peut s'authentifier deux fois en continu avec son vrai visage pour se déverrouiller.

**Échec de l'authentification de la serrure Face**

Après avoir activé la fonction de détection des visages en direct, le système verrouille le visage de l'utilisateur pendant 5 minutes si la détection des visages en direct échoue après plus de tentatives que le nombre configuré. Le même utilisateur ne peut pas s'authentifier via le faux visage dans les 5 minutes. Pendant ces 5 minutes, l'utilisateur peut s'authentifier deux fois en continu avec son vrai visage pour se déverrouiller.

**Mode d'application**

Vous pouvez sélectionner les modes d'application intérieur ou extérieur en fonction de l'environnement réel.

**4.** Cliquez sur **OK**.

5. **Facultatif :** Cliquez sur **Copier vers**, puis sélectionnez le(s) lecteur(s) de cartes pour copier les paramètres de la page vers le(s) lecteur(s) de cartes sélectionné(s).

### Configuration des paramètres de la sortie d'alarme

Après avoir ajouté le dispositif de contrôle d'accès, si le dispositif est lié à des sorties d'alarme, vous pouvez configurer les paramètres.

**Avant de commencer**

Ajouter un dispositif de contrôle d'accès au client et s'assurer que le dispositif prend en charge la sortie d'alarme.

**Étapes**

1. Cliquez sur **Access Control→ Advanced Function→ Device Parameter** pour accéder à la page de configuration des paramètres de contrôle d'accès.
2. Dans la liste des appareils à gauche, cliquez sur pour développer la porte, sélectionnez une entrée d'alarme et vous pouvez modifier les paramètres de l'entrée d'alarme à droite.
3. Définir les paramètres de la sortie d'alarme.

   **Nom**

   Modifiez le nom du lecteur de cartes comme vous le souhaitez.

   **Temps d'activation de la sortie d'alarme**

   Durée de la sortie de l'alarme après son déclenchement.
4. Cliquez sur **OK**.
5. **En option :** Placez l'interrupteur situé dans le coin supérieur droit sur **ON** pour déclencher la sortie d'alarme.

## 10.7.2 Configuration des paramètres de l'appareil

Après avoir ajouté le dispositif de contrôle d'accès, vous pouvez définir ses paramètres, tels que les paramètres réseau.

### Paramètres du terminal de reconnaissance faciale

Pour le terminal de reconnaissance faciale, vous pouvez définir ses paramètres, notamment la base de données des photos de visage, l'authentification par code QR, etc.

**Étapes**

**Note**

Cette fonction doit être prise en charge par l'appareil.

1. Entrez dans le module de contrôle d'accès.
2. Dans la barre de navigation de gauche, entrez dans **Fonction avancée→ Plus de paramètres** .
3. Sélectionnez un dispositif de contrôle d'accès dans la liste des dispositifs et cliquez sur **Terminal de reconnaissance faciale**.
4. Régler les paramètres.

**Note**

Ces paramètres affichés varient en fonction des différents modèles d'appareils.

**COM**

Sélectionnez un port COM pour la configuration. COM1 correspond à l'interface RS-485 et COM2 à l'interface RS-232.

**Base de données d'images de visages**

sélectionner Deep Learning comme base de données d'images de visages.

**Authentification par code QR**

Si cette fonction est activée, la caméra de l'appareil peut scanner le code QR pour s'authentifier. Par défaut, la fonction est désactivée.

**Authentification par liste de blocage**

Si cette option est activée, l'appareil compare la personne qui souhaite accéder à l'appareil avec les personnes figurant sur la liste de blocage.

En cas de correspondance (la personne figure sur la liste de blocage), l'accès est refusé et l'appareil envoie une alarme au client.

En cas de non-concordance (la personne ne figure pas sur la liste de blocage), l'accès est accordé.

**Sauvegarder l'image du visage d'authentification**

Si cette option est activée, la photo du visage capturée lors de l'authentification sera enregistrée sur l'appareil.

**Version MCU**

Affichez la version du MCU de l'appareil.

5. Cliquez sur **Enregistrer**.

## Réglage des paramètres RS-485

Vous pouvez définir les paramètres RS-485 du dispositif de contrôle d'accès, notamment le débit en bauds, le bit de données, le bit d'arrêt, le type de parité, le type de contrôle de flux, le mode de communication, le mode de travail et le mode de connexion.

**Étapes**

**Note**

Les paramètres RS-485 doivent être pris en charge par l'appareil.

1. Entrez dans le module de contrôle d'accès.
2. Dans la barre de navigation de gauche, entrez dans **Fonction avancée→ Plus de paramètres** .
3. Sélectionnez un dispositif de contrôle d'accès dans la liste des dispositifs et cliquez sur **RS-485** pour accéder à la page RS-485 Settings (Paramètres RS-485).
4. Sélectionnez le numéro du port série dans la liste déroulante pour définir les paramètres RS-485.
5. Définissez le numéro de série, l'appareil externe, le centre d'authentification, le débit en bauds, le bit de données, le bit d'arrêt, le type de parité, le type de contrôle de flux, le mode de communication et le mode de travail dans la liste déroulante.

6. Cliquez sur **Enregistrer**.
   - Les paramètres configurés seront appliqués automatiquement à l'appareil.
   - Lorsque vous changez de mode de travail ou de mode de connexion, l'appareil redémarre automatiquement.

## Paramètres Wiegand

Vous pouvez définir le canal Wiegand du dispositif de contrôle d'accès et le mode de communication.

**Étapes**

**Note**

Cette fonction doit être prise en charge par l'appareil.

1. Entrez dans le module de contrôle d'accès.
2. Dans la barre de navigation de gauche, entrez dans **Fonction avancée→ Plus de paramètres** .
3. Sélectionnez un dispositif de contrôle d'accès dans la liste des dispositifs et cliquez sur **Wiegand** pour accéder à la page Wiegand Settings (Paramètres Wiegand).
4. Placez l'interrupteur sur on pour activer la fonction Wiegand pour l'appareil.
5. Sélectionnez le numéro de canal Wiegand et le mode de communication dans la liste déroulante.

   **Note**

   Si vous définissez **la direction de la communication** comme étant l'**envoi**, vous devez définir le **mode Wiegand** comme étant

   **Wiegand 26** ou **Wiegand 34**.
6. Cochez **Enable Wiegand** pour activer la fonction Wiegand.
7. Cliquez sur **Enregistrer**.
   - Les paramètres configurés seront appliqués automatiquement à l'appareil.
   - Après avoir modifié la direction de la communication, l'appareil redémarre automatiquement.

## Activer le cryptage de la carte M1

Le cryptage de la carte M1 peut améliorer le niveau de sécurité de l'authentification.

**Étapes**

**Note**

La fonction doit être prise en charge par le dispositif de contrôle d'accès et le lecteur de cartes.

1. Entrez dans le module de contrôle d'accès.
2. Dans la barre de navigation de gauche, entrez dans **Fonction avancée→ Plus de paramètres** .
3. Sélectionnez un dispositif de contrôle d'accès dans la liste des dispositifs et cliquez sur **Vérification du cryptage de la carte M1** pour accéder à la page Vérification du cryptage de la carte M1.
4. Placez le commutateur sur on pour activer la fonction de cryptage de la carte M1.

**5.** Définir l'ID du secteur.

**Note**

- L'ID du secteur est compris entre 1 et 100.
- Par défaut, le secteur 13 est crypté. Il est recommandé de crypter le secteur 13.

**6.** Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

## 10.8 Contrôle des portes

Dans le module de surveillance, vous pouvez visualiser l'état en temps réel des portes gérées par le dispositif de contrôle d'accès ajouté. Vous pouvez également contrôler les portes, par exemple ouvrir/fermer la porte, ou maintenir la porte ouverte/fermée via le client à distance. Les événements d'accès en temps réel sont affichés dans ce module. Vous pouvez visualiser les détails de l'accès et les détails de la personne.

**Note**

Si l'utilisateur a l'autorisation de contrôler la porte, il peut entrer dans le module de surveillance et contrôler la porte. Sinon, les icônes utilisées pour le contrôle ne s'afficheront pas. Pour définir l'autorisation de l'utilisateur, reportez-vous à la section ***Gestion des personnes*** .

### 10.8.1 État de la porte de contrôle

Vous pouvez contrôler l'état de la ou des portes, notamment déverrouiller la porte, verrouiller la porte, laisser la porte déverrouillée, laisser la porte verrouillée, laisser toutes les portes déverrouillées, etc.

**Avant de commencer**

- Ajoutez une personne et attribuez-lui une autorisation d'accès. Cette personne aura l'autorisation d'accéder aux points d'accès (portes). Pour plus d'informations, voir ***Gestion des personnes*** et ***Définir un groupe d'accès pour attribuer une autorisation d'accès aux personnes***.
- Assurez-vous que l'utilisateur de l'opération a l'autorisation d'accéder aux points d'accès (portes). Pour plus de détails, voir .

**Étapes**

**1.** Cliquez sur **Surveillance** pour accéder à la page de surveillance de l'état.

**2.** Sélectionnez un groupe de points d'accès dans le coin supérieur droit.

**Note**

Pour gérer le groupe de points d'accès, reportez-vous à la section ***Gestion des groupes*** . Les portes du groupe de contrôle d'accès sélectionné s'affichent.

**3.** Cliquez sur une icône de porte pour sélectionner une porte, ou appuyez sur **Ctrl** pour sélectionner plusieurs portes.

**Note**

Pour **Rester tous déverrouillés** et **Rester tous verrouillés**, ignorez cette étape.

**4.** Cliquez sur les boutons suivants pour contrôler la porte.

**Déverrouiller**

Lorsque la porte est verrouillée, il suffit de la déverrouiller pour qu'elle s'ouvre une fois. Après la durée d'ouverture, la porte se referme et se verrouille automatiquement.

**Verrouiller**

Lorsque la porte est déverrouillée, il suffit de la verrouiller pour qu'elle se ferme. La personne qui a l'autorisation d'accès peut accéder à la porte avec des informations d'identification.

**Rester déverrouillé**

La porte sera déverrouillée (qu'elle soit fermée ou ouverte). Toutes les personnes peuvent accéder à la porte sans avoir besoin d'informations d'identification.

**Rester verrouillé**

La porte sera fermée et verrouillée. Personne ne peut accéder à la porte même s'il/elle possède les informations d'identification autorisées, à l'exception des super utilisateurs.

**Rester tous déverrouillés**

Toutes les portes du groupe seront déverrouillées (qu'elles soient fermées ou ouvertes). Toutes les personnes peuvent accéder aux portes sans avoir besoin d'informations d'identification.

**Rester tous verrouillés**

Toutes les portes du groupe seront fermées et verrouillées. Personne ne peut accéder aux portes même s'il/elle possède les informations d'identification autorisées, à l'exception des super utilisateurs.

**Capture**

Prendre une photo manuellement.

**Note**

Le bouton **Capturer** est disponible lorsque l'appareil prend en charge la fonction de capture. L'image est enregistrée sur le PC qui exécute le client. Pour définir le chemin d'*enregistrement*, reportez-vous à la section *Définir le chemin d'enregistrement des fichiers* dans le manuel d'utilisation du logiciel client.

**Résultat**

L'icône des portes changera en temps réel en fonction de l'opération si celle-ci est réussie.

## 10.8.2 Vérifier les enregistrements d'accès en temps réel

Les enregistrements d'accès s'affichent en temps réel, y compris les enregistrements de passage de carte, les enregistrements de reconnaissance faciale, les enregistrements de comparaison d'empreintes digitales, etc. Vous pouvez consulter les informations relatives à la personne et voir la photo prise lors de l'accès.

**Étapes**

1. Cliquez sur **Surveillance** et sélectionnez un groupe dans la liste déroulante située dans le coin supérieur droit.

   Les enregistrements d'accès déclenchés aux portes du groupe sélectionné s'affichent en réel. Vous pouvez consulter les détails des enregistrements, notamment le numéro de carte, le nom de la personne, l'organisation, l'heure de l'événement, etc.
2. **Facultatif :** Cochez le type et l'état de l'événement pour que ces événements s'affichent dans la liste s'ils sont détectés. Les événements dont le type ou l'état n'est pas coché ne seront pas affichés dans la liste.
3. **Facultatif :** Cochez la case **Afficher l'événement le plus** récent pour que le dernier enregistrement d'accès soit sélectionné et affiché en haut de la liste des enregistrements.
4. **Facultatif :** Cliquez sur l'événement pour afficher les détails de la personne accédée, y compris les photos de la personne (photo capturée et profil), le numéro de la personne, le nom de la personne, l'organisation, le téléphone, l'adresse de contact, etc.

   **Note**
   Vous pouvez double-cliquer sur l'image capturée pour l'agrandir et voir les détails.
5. **Facultatif :** Cliquez avec le bouton droit de la souris sur le nom de la colonne du tableau des événements d'accès pour afficher ou masquer la colonne en fonction des besoins.

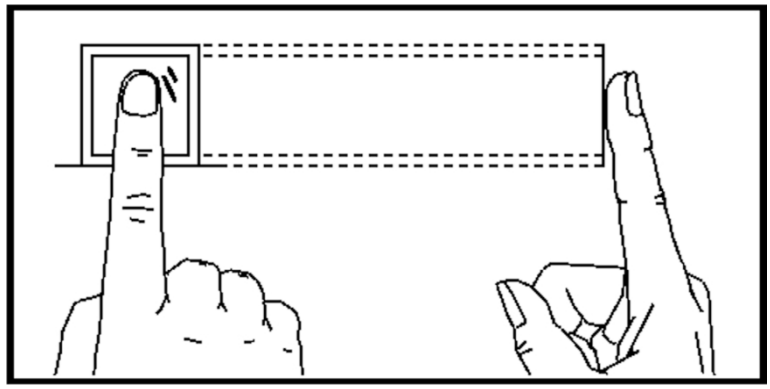
# Annexe A. Conseils pour la numérisation des empreintes digitales

### Doigt recommandé

L'index, le majeur ou le troisième doigt.

### Numérisation correcte

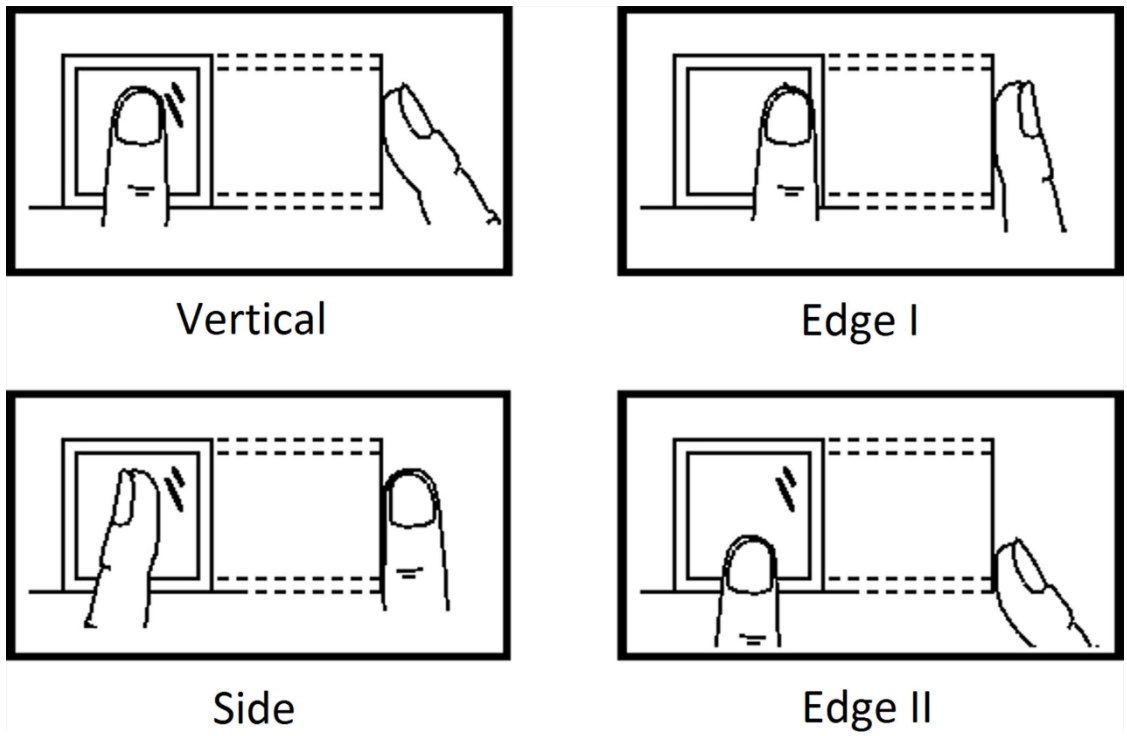
La figure ci-dessous représente la manière correcte de scanner votre doigt :



Vous devez appuyer votre doigt sur le scanner horizontalement. Le centre de votre doigt numérisé doit être aligné avec le centre du scanner.

### Numérisation incorrecte

Les chiffres de la numérisation des empreintes digitales affichés ci-dessous sont incorrects :




### Environnement

Le scanner doit être protégé de la lumière directe du soleil, des températures élevées, de l'humidité et de la pluie. Lorsqu'il est sec, le scanner peut ne pas reconnaître correctement votre empreinte digitale. Vous pouvez souffler votre doigt et scanner à nouveau.

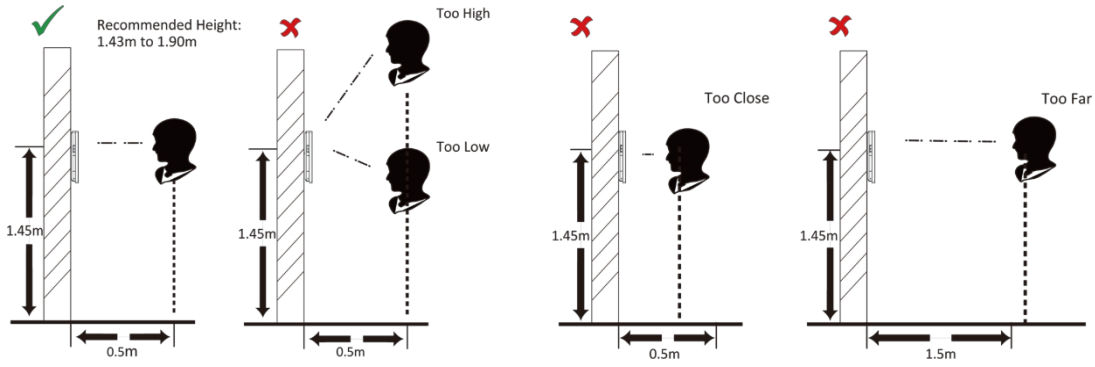
### Autres

Si votre  digitale est peu profonde ou s'il est difficile de la scanner, nous vous recommandons d'utiliser d'autres méthodes d'authentification.
Si vous avez des blessures sur le doigt scanné, il se peut que le scanner ne le reconnaisse pas. Vous pouvez changer doigt et réessayer.

# Annexe B. Conseils pour la collecte et la comparaison d'images de visages

La position lors de la collecte ou de la comparaison d'images de visages est la suivante :

### Positions (distance recommandée : 0,5 m)




### Expression

- Gardez une expression naturelle lorsque vous recueillez ou comparez des images de visages, comme dans l'image ci-dessous.

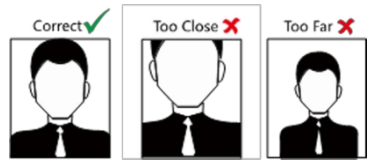
- Ne portez pas de chapeau, de lunettes de soleil ou d'autres accessoires susceptibles d'affecter la fonction de reconnaissance faciale.
- Les cheveux ne doivent pas couvrir les yeux, les oreilles, etc. et le maquillage lourd n'est pas autorisé.

### Posture

Afin d'obtenir une photo de visage précise et de bonne qualité, placez votre visage face à l'appareil photo lorsque vous recueillez ou comparez des photos de visage.

### Taille

Assurez-vous que votre visage se trouve au milieu de la fenêtre de collecte.



# Annexe C. Conseils pour l'environnement d'installation

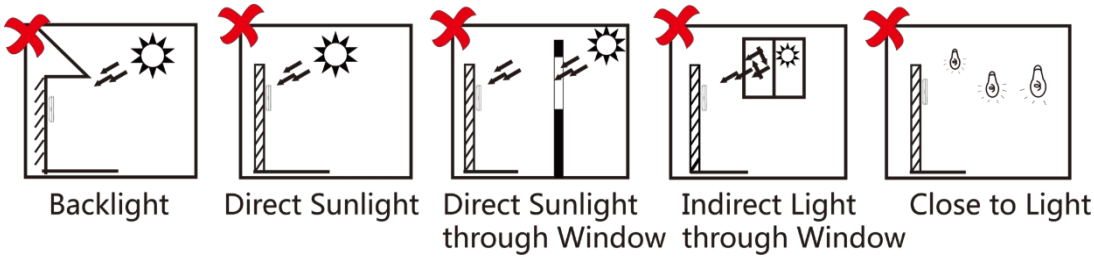
1. Source lumineuse Valeur de référence de l'éclairage

Bougie : 10Lux

Ampoule : 100~850Lux

Lumière du soleil : Plus de 1200Lux

2. Éviter le contre-jour, la lumière directe et indirecte du soleil



# Annexe D. Dimension

Les dimensions de l'appareil avec empreinte digitale sont les suivantes :

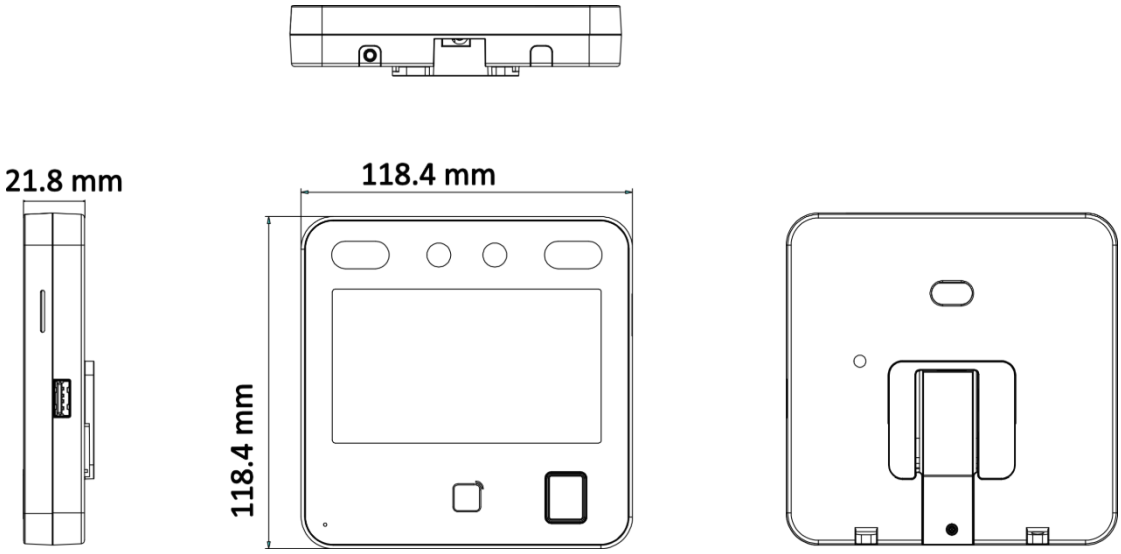



**Figure D-1 Dimension (avec empreinte digitale)**

Les dimensions de l'appareil sans empreinte digitale sont les suivantes :

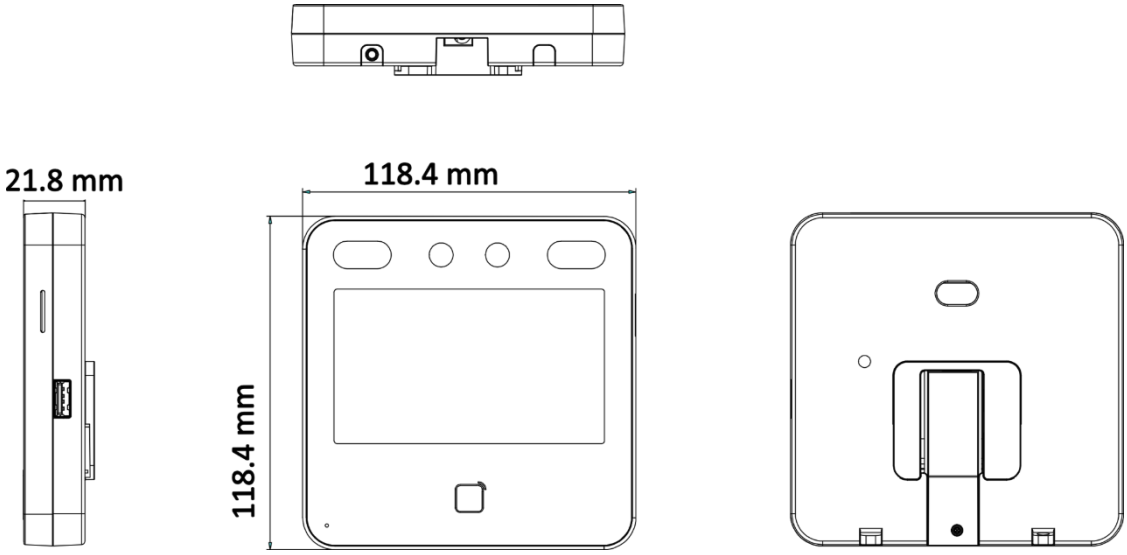



**Figure D-2 Dimension (sans empreinte digitale)**

# Annexe E. Matrice de communication et commande de dispositif

## Matrice de communication

Scannez le code QR suivant pour obtenir la matrice de communication de l'appareil.
Notez que la matrice contient tous les ports de communication des dispositifs de contrôle d'accès et d'interphone vidéo Hikvision.

**Figure E-1 Code QR de la matrice de communication**

## Commande de l'appareil

Scannez le code QR suivant pour obtenir les commandes courantes du port série de l'appareil.
Notez que la liste des commandes contient toutes les commandes de ports série couramment utilisées pour tous les dispositifs de contrôle d'accès et d'interphone vidéo Hikvision.

**Figure E-2 Commande de l'appareil**


See Far, Go Further