Contrôleur d’accès

Manuel d’utilisation

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.5

Avant-propos

Généralités

Ce manuel présente les fonctions et les opérations du contrôleur d'accès. Lisez attentivement ce contenu avant d'utiliser l'appareil et conservez-le pour une future consultation.

Précautions d'emploi

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

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

Historique des révisions

Version	Description de la révision	Date de publication
V1.0.5	Mise à jour des descriptions de déverrouillage du mot de passe.	Novembre 2023
V1.0.4	Mise à jour de l'ajout d'utilisateurs et de la configuration des autorisations.	Juin 2023
V1.0.3	Mise à jour de la description de l'ajout d'utilisateurs.	Avril 2023
V1.0.2	Mise à jour des méthodes de déverrouillage.	Mars 2023
V1.0.1	Mise à jour du câblage.	Septembre 2022
V1.0.0	Première publication.	Septembre 2022

Avis de protection de la confidentialité

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

À propos du manuel

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

Précautions et avertissements importants

Le contenu de ce paragraphe aborde la bonne manipulation du contrôleur d'accès, la prévention des risques et la prévention des dommages matériels. Lisez attentivement ce contenu avant d'utiliser le contrôleur d'accès et respectez les consignes lorsque vous l'utilisez.

Conditions de transport requises

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

Conditions requises pour le stockage

Stockez le contrôleur d'accès dans les conditions d'humidité et de température autorisées.

Conditions d'installation requises

AVERTISSEMENT

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

- Le personnel travaillant en hauteur doit prendre toutes les mesures nécessaires pour assurer sa propre sécurité, notamment porter un casque et des ceintures de sécurité.
- Ne placez pas le contrôleur d'accès à un endroit exposé à la lumière du soleil ou proche de sources de chaleur.
- Gardez le contrôleur d'accès à l'écart de l'humidité, de la poussière et de la suie.
- Installez le contrôleur d'accès sur une surface stable afin d'éviter toute chute.
- Installez le contrôleur d'accès à un endroit bien ventilé et empêchez toute obstruction des orifices de ventilation.
- Utilisez un adaptateur ou un boîtier d'alimentation fourni par le fabricant.
- Utilisez les cordons d'alimentation recommandés dans votre région et conformez-vous aux spécifications d'alimentation nominales.
- L'alimentation doit être conforme aux dispositions de la catégorie ES1 contenue dans la norme IEC 62368-1 et ne doit pas être supérieure à PS2. Veuillez noter que l'exigence relative à l'alimentation électrique est soumise à l'étiquette du contrôleur d'accès.

- Le contrôleur d'accès est un équipement électrique de classe I. Assurez-vous que le bloc d'alimentation du contrôleur d'accès est connecté à une prise électrique munie d'une mise à la terre de protection.

Conditions de fonctionnement

- Assurez-vous que l'alimentation électrique est correcte avant utilisation.
- Ne débranchez pas le cordon d'alimentation sur le côté du contrôleur d'accès alors que l'adaptateur est sous tension.
- Utilisez le contrôleur d'accès dans la plage nominale d'entrée et de sortie d'alimentation.
- Utilisez le contrôleur d'accès dans les conditions d'humidité et de température autorisées.
- Évitez d'exposer le contrôleur d'accès aux gouttes ou aux éclaboussures de liquides. Ne placez aucun objet contenant un liquide sur le contrôleur d'accès afin d'éviter que ce liquide ne pénètre dedans.
- Ne démontez pas le contrôleur d'accès si vous n'êtes pas qualifié pour le faire.

Table des matières

1 Présentation du produit

1.1 Introduction au produit

Flexible et pratique, le contrôleur d'accès est doté d'un système convivial qui vous permet d'accéder aux contrôleurs sur la page Web via l'adresse IP. Il est livré avec un système de gestion d'accès professionnel et permet une mise en réseau rapide et facile des modes de contrôle principal et secondaire, répondant ainsi aux besoins des petits systèmes et des systèmes avancés.

1.2 Caractéristiques principales

- Fabriqué en matériau PC et ABS ignifuge, il est à la fois robuste et élégant et bénéficie d'un classement IK06.
- Prend en charge la connexion TCP et IP et le PoE standard.
- Accède aux lecteurs de carte via les protocoles Wiegand et RS-485.
- Fournit de l'énergie à la serrure par son alimentation de sortie de 12 V CC, dotée d'un courant de sortie maximum de 1 000 mA.
- Prend en charge 1 000 utilisateurs, 5 000 cartes, 3 000 empreintes digitales et 300 000 enregistrements.
- Plusieurs méthodes de déverrouillage : carte, mot de passe, empreinte digitale, etc. Vous pouvez également combiner ces méthodes pour créer vos propres méthodes de déverrouillage.
- Plusieurs types d'alarmes sont pris en charge, comme la contrainte, la falsification, l'intrusion, le délai de déverrouillage et la carte illégale.
- Prend en charge un large éventail d'utilisateurs, notamment les utilisateurs généraux, les patrouilleurs, les VIP, les invités, les personnes inscrites sur une liste de blocage, etc.
- Synchronisation manuelle et automatique de l'heure.
- Conserve les données stockées même lorsqu'il est hors tension.
- Offre une variété de fonctions et le système peut être configuré. Les appareils peuvent également être mis à jour via la page Web.
- Comprend des modes de contrôle principal et secondaire. Le mode de contrôle principal permet la gestion des utilisateurs, la gestion et la configuration des dispositifs de contrôle d'accès et bien d'autres options. Les appareils en mode de contrôle secondaire peuvent être ajoutés à plusieurs plateformes.
- Un contrôleur principal peut se connecter à 19 sous-contrôleurs et les gérer.
- Le chien de garde protège le système pour permettre à l'appareil d'être stable et de fonctionner efficacement.
- Des sous-contrôleurs peuvent être ajoutés à SmartPSS Lite et DSS Pro.

1.3 Scénarios d'application

Il est largement utilisé dans les parcs, les communautés, les centres d'affaires et les usines, et idéal

pour des lieux tels que les immeubles de bureaux, les bâtiments gouvernementaux, les écoles et les stades.

Le contrôleur d'accès peut être réglé sur le contrôleur d'accès principal (ci-après dénommé « contrôleur principal ») ou sur le contrôleur d'accès secondaire (ci-après dénommé « Sous-contrôleur »). 2 méthodes de mise en réseau différentes sont disponibles pour le contrôleur d'accès. Vous pouvez sélectionner une méthode de mise en réseau en fonction de vos besoins.

Tableau 1-1 Méthodes de mise en réseau du contrôleur d'accès

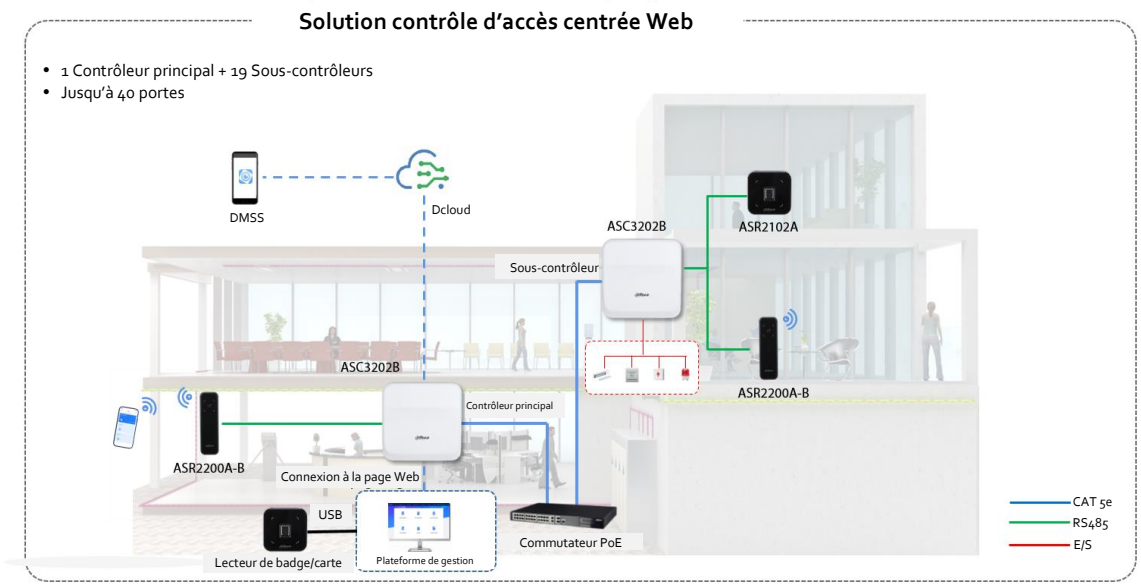
Méthodes de mise en réseau	Description
Contrôleur principal – Sous-contrôleur	Le contrôleur principal est livré avec une plateforme de gestion (ci-après dénommée la « Plateforme »). Les sous-contrôleurs doivent être ajoutés à la plateforme du contrôleur principal. Un contrôleur principal peut gérer jusqu'à 19 sous-contrôleurs. Pour les détails, voir « 2 Contrôleur principal – Sous-contrôleur ». Nous vous déconseillons d'ajouter d'autres plateformes de gestion dans cette méthode de mise en réseau.
SmartPSS Lite – Sous-contrôleur	Les sous-contrôleurs doivent être ajoutés à une plateforme de gestion autonome, telle que SmartPSS Lite. La plateforme peut gérer jusqu'à 64 portes si chaque sous-contrôleur connecte 2 portes. Pour les détails, voir « 3 Sous-contrôleurs Smart PSS Lite ».

2 Contrôleur principal – Sous-contrôleur

2.1 Schéma du réseau

Le contrôleur principal est livré avec une plateforme de gestion (ci-après dénommée la « Plateforme »). Le sous-contrôleur doit être ajouté à la plateforme de gestion du contrôleur principal. Un contrôleur principal peut gérer jusqu'à 19 sous-contrôleurs.

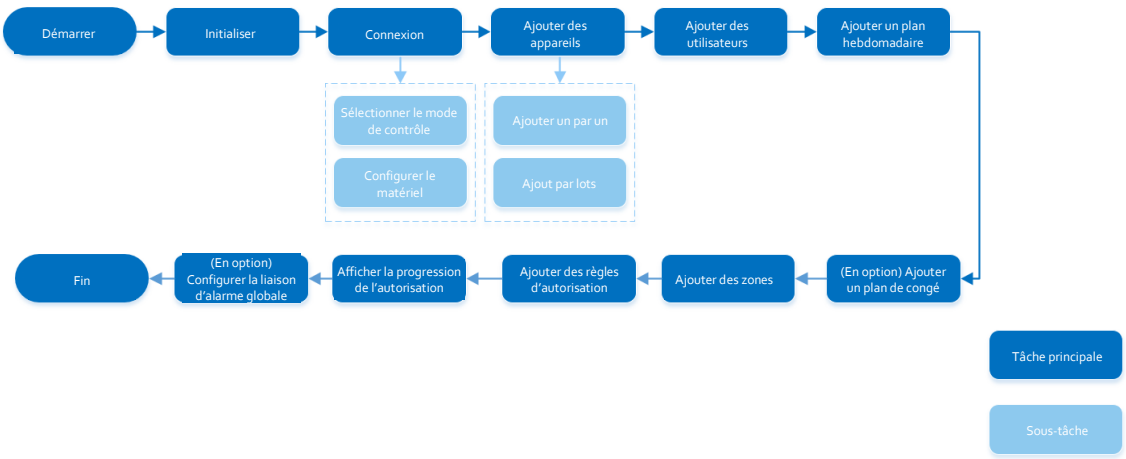
Figure 2-1 Schéma de la mise en réseau



2.2 Configurations du contrôleur principal

2.2.1 Organigramme de configuration

Figure 2-2 Organigramme de configuration



2.2.2 Initialisation

Initialisez le contrôleur principal lorsque vous vous connectez à la page Web pour la première fois ou après avoir rétabli les paramètres d'usine par défaut.

Conditions préalables

Assurez-vous que l'ordinateur utilisé pour se connecter à la page Web se trouve sur le même réseau local que le contrôleur principal.

Procédure

Étape 1 : Ouvrez un navigateur, accédez à l'adresse IP (l'adresse IP est 192.168.1.108 par défaut) du contrôleur principal.

Nous vous recommandons d'utiliser la dernière version de Chrome ou de Firefox.

Étape 2 : Sélectionnez la langue, puis cliquez sur **Suivant** (Next).

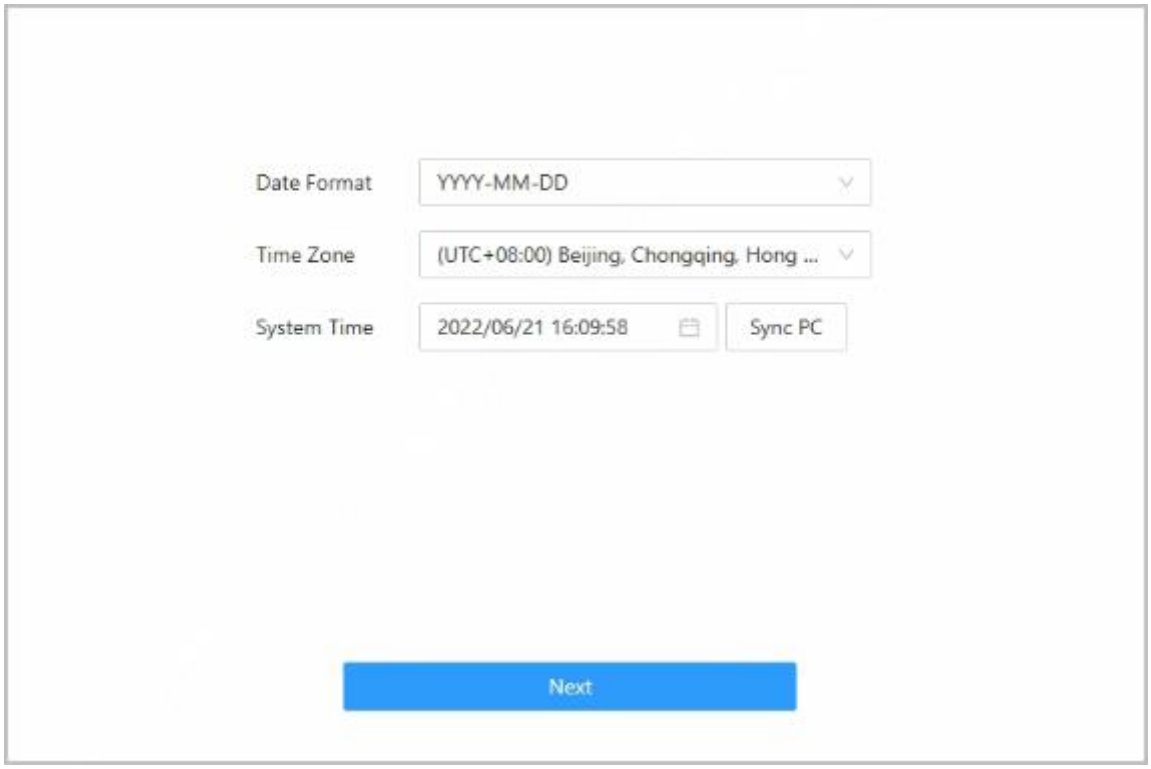
Étape 3 : Lisez attentivement le contrat de licence du logiciel et la politique de confidentialité, sélectionnez **J'ai lu et j'accepte les termes du contrat de licence du logiciel et de la politique de confidentialité.** (I have read and agree to the terms of the Software License Agreement and Privacy Policy.), puis cliquez sur **Suivant** (Next).

Étape 4 : Configurez le mot de passe et l'adresse e-mail.

- Le mot de passe doit être composé de 8 à 32 caractères non blancs et d'au moins deux types de caractères suivants : des majuscules, des minuscules, des chiffres et des caractères spéciaux (sauf ' " ; : &). Définissez un mot de passe de haute sécurité en suivant l'invite relative à la longueur du mot de passe.
- Conservez le mot de passe en lieu sûr après l'initialisation et modifiez-le régulièrement pour améliorer la sécurité.

Étape 5 : Configurez l'heure système, puis cliquez sur **Suivant** (Next).

Figure 2-3 Configuration de l'heure



Étape 6 : (En option) Sélectionnez **Vérification automatique des mises à jour** (Select Auto Check for Updates), puis cliquez sur **Terminé** (Completed).
Le système vérifie automatiquement si une version plus récente est disponible et informe l'utilisateur qu'il doit mettre à jour le système. Le système vérifie automatiquement les nouvelles mises à jour et vous informe lorsqu'une nouvelle mise à jour est disponible.

Étape 7 : Cliquez sur **Terminé** (Completed).
Le système passe automatiquement à la page de connexion une fois l'initialisation réussie.

2.2.3 Connexion

Pour la première connexion pendant l'initialisation, vous devez suivre l'assistant de connexion pour configurer le type de contrôleur principal et son matériel.

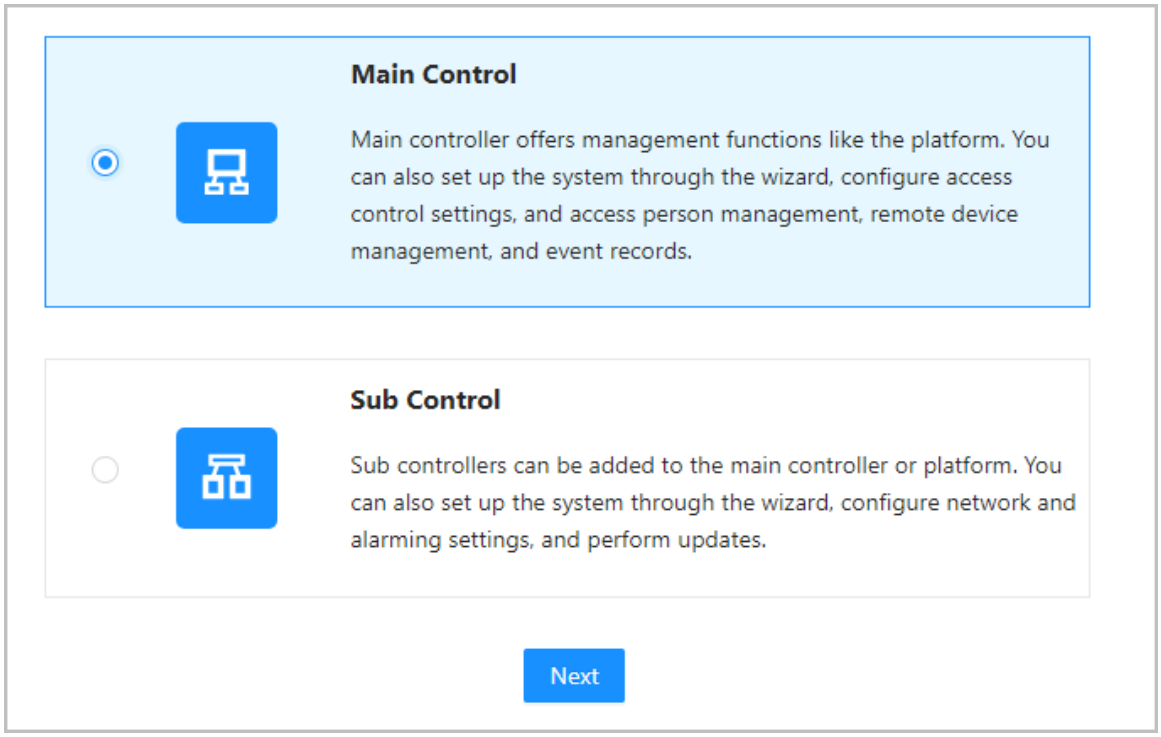
Procédure

Étape 1 : Sur la page de connexion, saisissez le nom d'utilisateur et le mot de passe.

- Le nom d'administrateur par défaut est « admin » et le mot de passe est celui défini au moment de l'initialisation. Nous vous recommandons de modifier régulièrement le mot de passe administrateur afin d'accroître la sécurité de la plateforme.
- Si vous avez oublié le mot de passe administrateur, vous pouvez cliquer sur **Mot de passe oublié ?** (Forgot password?).

Étape 2 : Sélectionnez **Contrôle principal** (Main Control), puis cliquez sur **Suivant** (Next).

Figure 2-4 Type de contrôleur d'accès



- Contrôle principal : Le contrôleur principal est livré avec une plateforme de gestion. Vous pouvez gérer tous les sous-contrôleurs, configurer le contrôle d'accès, accéder à la gestion des personnes sur la plateforme, etc.
- Contrôle secondaire : Les sous-contrôleurs doivent être ajoutés à la plateforme de gestion du contrôleur principal ou à d'autres plateformes de gestion telles que DSS Pro ou SmartPSS Lite. Vous pouvez effectuer les configurations sur la page Web du sous-contrôleur.

Étape 3 : Sélectionnez le nombre de portes, puis saisissez le nom de la porte.

Étape 4 : Configurez les paramètres des portes.

Figure 2-5 Configuration des paramètres de la porte

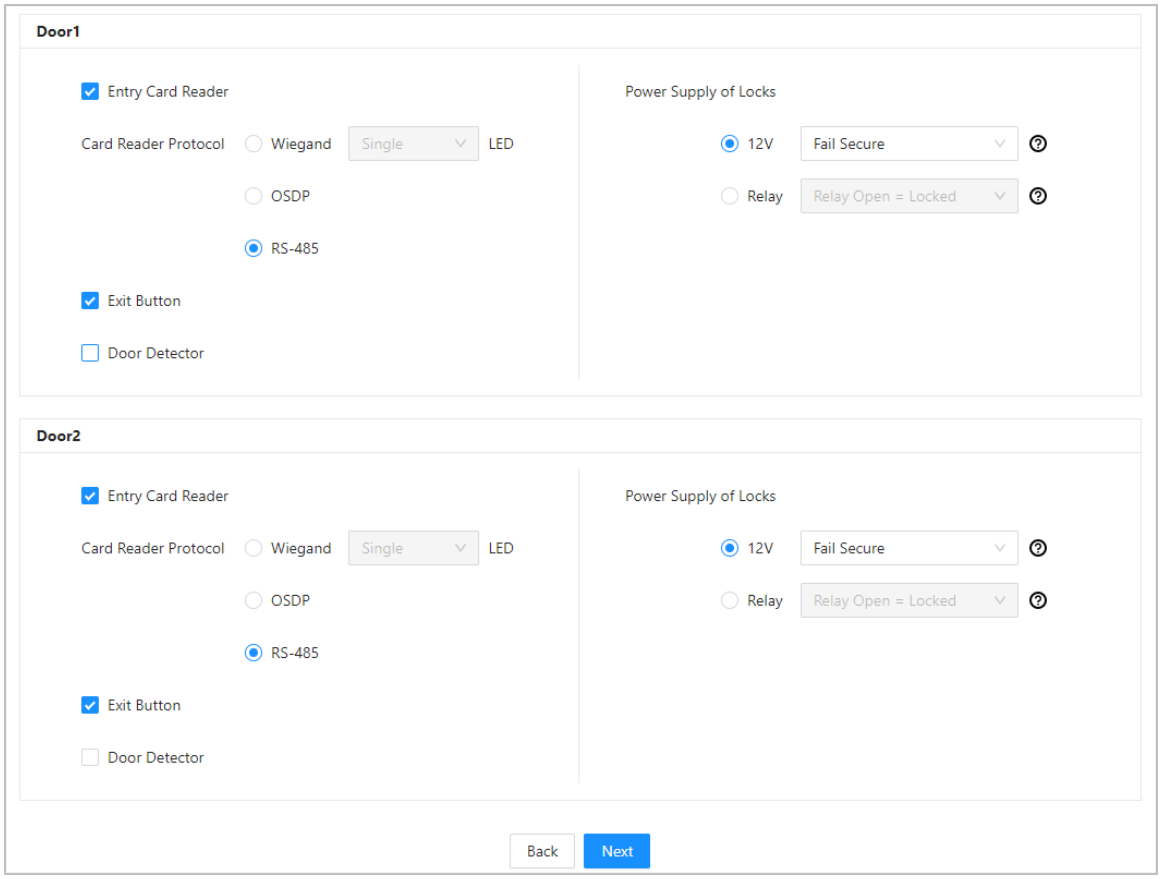


Tableau 2-1 Description des paramètres

Paramètre	Description
Lecteur de carte d'entrée	Sélectionner le protocole du lecteur de carte. ● Wiegand : Se connecte à un lecteur Wiegand. Vous pouvez connecter le fil de la LED au port LED du contrôleur, et le lecteur émettra un signal sonore et clignotera lorsque la porte se déverrouillera. ● OSDP : Se connecte à un lecteur OSDP. ● RS-485 : Se connecte à un lecteur RS-485.
Bouton de Sortie	Se connecte à un bouton de sortie.
Détecteur de porte	Se connecte à un détecteur de porte.

Paramètre	Description
Alimentation des verrouillages	● 12 V : Le contrôleur alimente la serrure. ◇ Sécurité à émission : En cas de coupure de courant ou de panne, la porte reste verrouillée. ◇ Sécurité à rupture : En cas de coupure de courant ou de panne, la porte se déverrouille automatiquement pour permettre aux personnes de sortir. ● Relais : Le relais alimente la serrure. ◇ Relais ouvert = verrouillé : Règle la serrure pour qu'elle reste verrouillée lors de l'ouverture du relais. ◇ Relais ouvert = déverrouillé : Règle la serrure pour qu'elle se déverrouille lors de l'ouverture du relais. La serrure électromagnétique se déverrouille instantanément et se verrouille à nouveau immédiatement lorsque le contrôleur d'accès est en mode de redémarrage progressif.

Étape 5 : Configurez les paramètres de contrôle d'accès.

Étape 6 : Dans **Paramètres de verrouillage** (Unlock Settings), sélectionnez **Ou** (Or) ou **Et** (And) dans **Procédé de combinaison** (Combination Method).

- Ou : Utilisez l'une des méthodes de déverrouillage sélectionnées pour autoriser l'ouverture de la porte.
- Et : Utilisez toutes les méthodes de déverrouillage sélectionnées pour autoriser l'ouverture de la porte.

La carte Bluetooth ne peut pas être sélectionnée lorsque le procédé de combinaison est réglée sur **Et** (And).

Étape 7 : Sélectionnez les méthodes de déverrouillage, puis configurez les autres paramètres.

Figure 2-6 Paramètres de déverrouillage

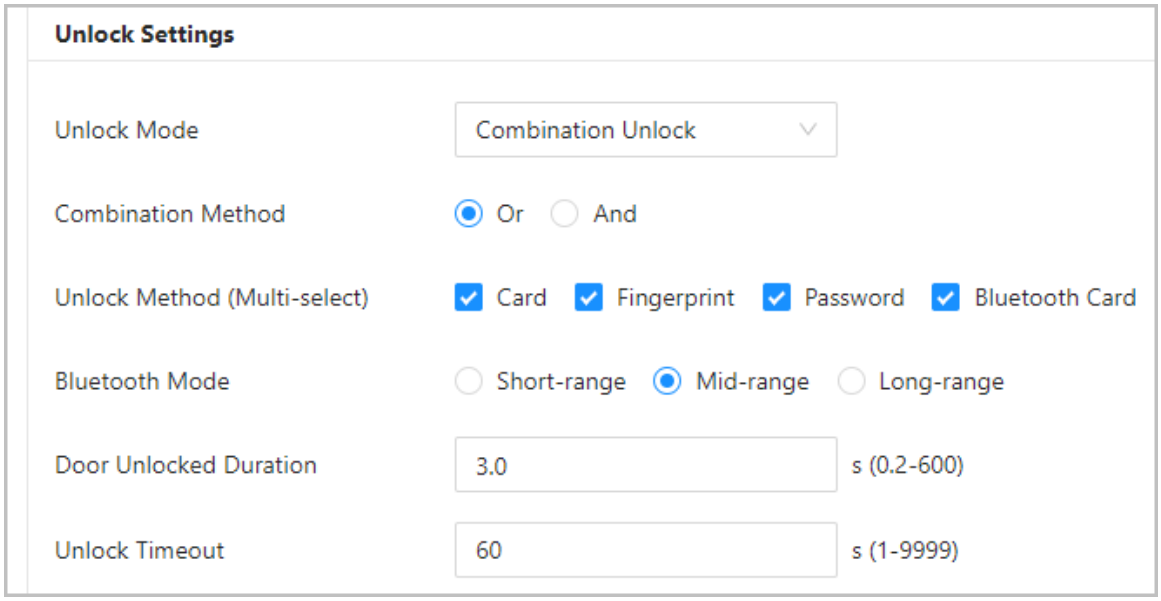


Tableau 2-2 Description des paramètres de déverrouillage

Paramètre	Description
Méthode de déverrouillage (multi-sélection)	Prend en charge le déverrouillage par carte, empreinte digitale, mot de passe ou carte Bluetooth. La fonction de carte Bluetooth est désactivée par défaut.
Mode Bluetooth	La carte Bluetooth doit se trouver à une certaine distance du dispositif de contrôle d'accès pour échanger des données et déverrouiller la porte. Les plages suivantes sont les plus appropriées. ● Courte portée : La portée de déverrouillage Bluetooth est inférieure à 0,2 m. ● Moyenne portée : La portée de déverrouillage Bluetooth est inférieure à 2 m. ● Longue portée : La portée de déverrouillage Bluetooth est inférieure à 10 m. ⚠ La portée de déverrouillage Bluetooth peut varier en fonction des modèles de votre téléphone et de l'environnement.
Durée de déverr. de la porte	Une fois qu'une personne a obtenu l'autorisation d'accès, la porte reste déverrouillée pendant une durée définie pour lui permettre de passer. La valeur de la durée varie de 0,2 à 600 s.
Temporisation de déverrouillage	Une alarme de temporisation se déclenche lorsque la porte reste déverrouillée pendant une durée supérieure à la valeur définie.

Étape 8 : Dans **Paramètres d'alarme** (Alarm Settings), configurez les paramètres de l'alarme.

Figure 2-7 Alarme

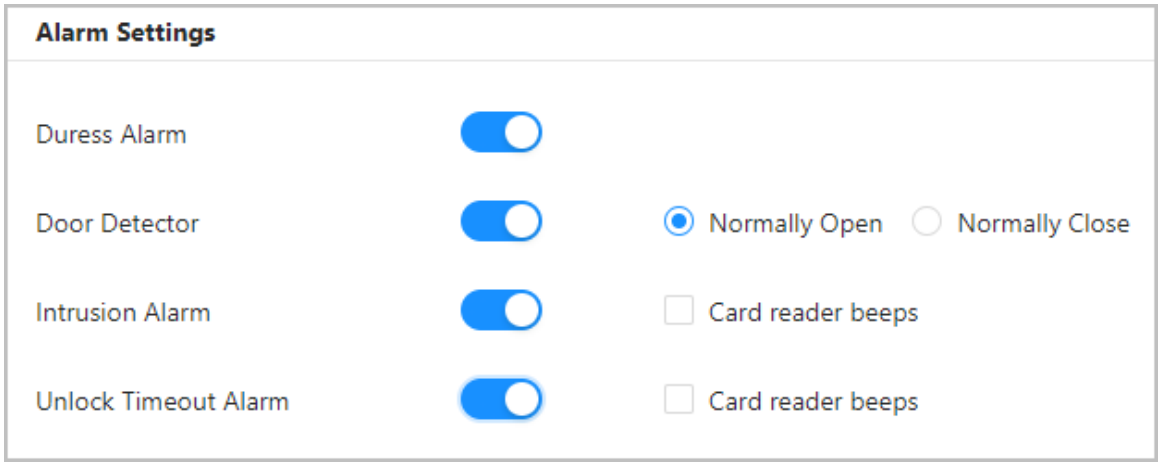


Tableau 2-3 Description des paramètres de l'alarme

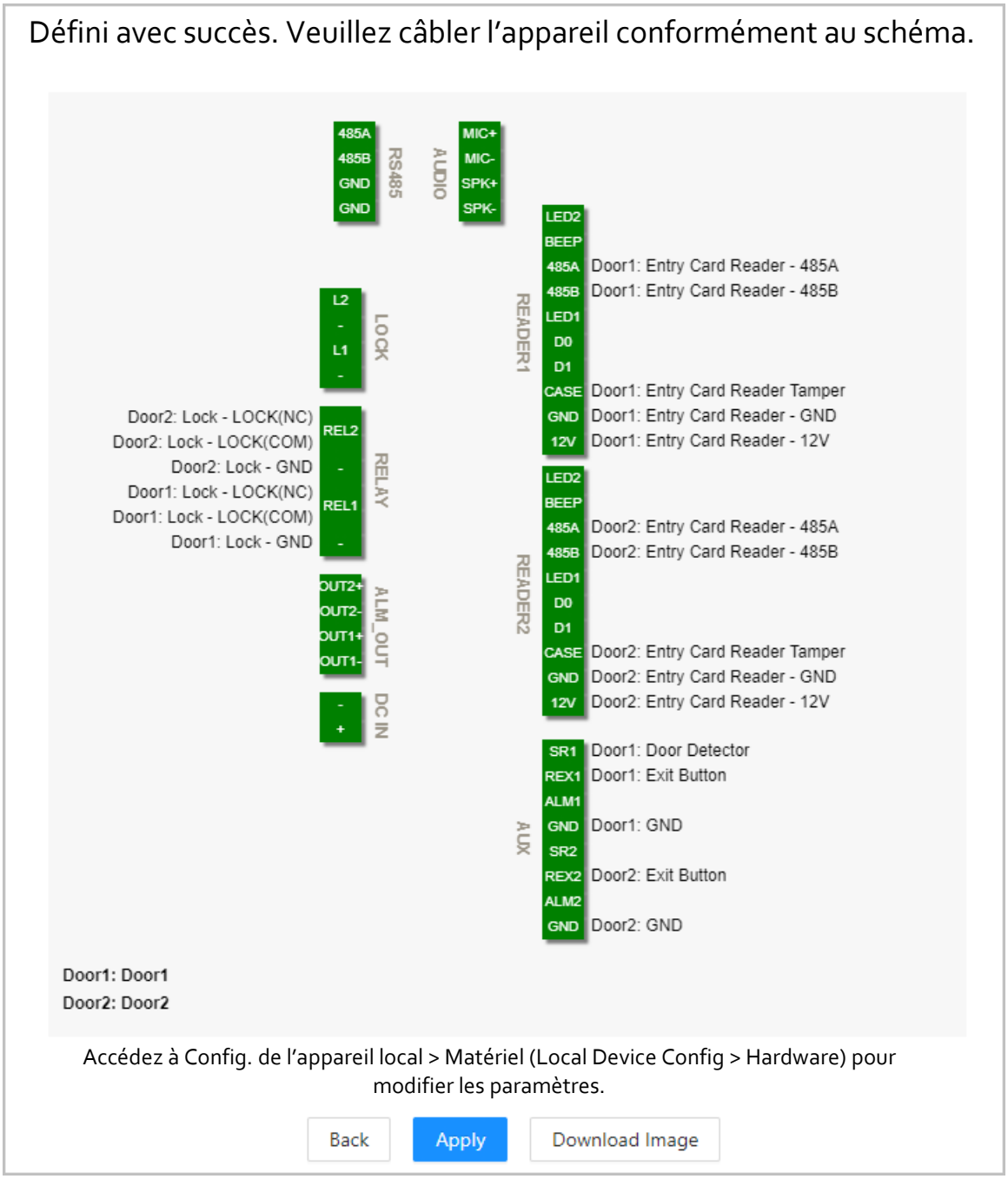
Paramètre	Description
Alarme de contrainte	Une alarme est déclenchée lorsqu'une carte de contrainte, un mot de passe de contrainte ou une empreinte digitale de contrainte est utilisé pour déverrouiller la porte.
Détecteur de porte	Sélectionnez le type de détecteur de porte.
Alarme d'intrusion	• Lorsque le détecteur de porte est activé, une alarme d'intrusion est déclenchée en cas d'ouverture anormale de la porte. • Une alarme de temporisation se déclenche lorsque la porte reste déverrouillée plus longtemps que le temps de déverrouillage défini. • Lorsque l'option **Bips du lecteur de carte** (Card reader beeps) est activée, le lecteur de carte émet un bip lorsque l'alarme d'intrusion ou l'alarme de temporisation est déclenchée.
Alarme de temporisation de déverrouillage	

Étape 9 : Cliquez sur **Suivant** (Next).

Un schéma de câblage est généré en fonction de vos configurations. Vous pouvez câbler l'appareil conformément au schéma.

L'image ci-dessous est donnée uniquement à titre de référence.

Figure 2-8 Schéma de câblage



Étape 10 : Cliquez sur **Appliquer** (Apply).

- Vous pouvez aller dans **Config. de l'appareil local > Matériel** (Local Device Config > Hardware) pour modifier les paramètres après vous être connecté à la plateforme.
- Cliquez sur **Télécharger l'image** (Download Image) pour télécharger le schéma sur votre ordinateur.

Opérations connexes

Si vous souhaitez modifier les paramètres du matériel, accédez à **Config. de l'appareil local > Matériel** (Local Device Config > Hardware).

2.2.4 Tableau de bord

Une fois que vous avez réussi à vous connecter, la page du tableau de bord de la plateforme s'affiche. Le tableau de bord affiche des données visualisées.

Figure 2-9 Tableau de bord

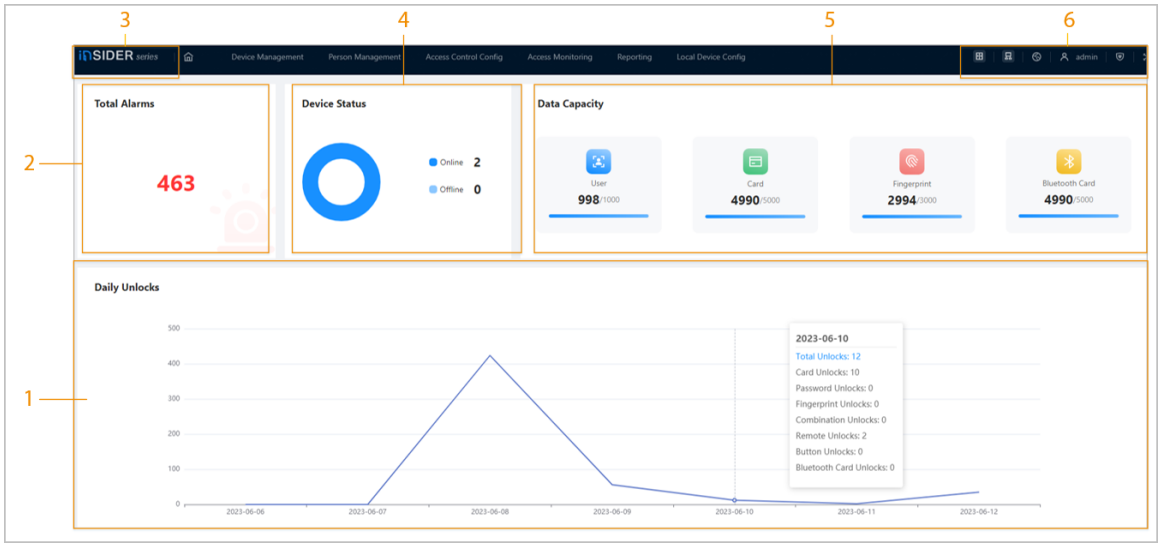


Tableau 2-4 Description de la page d'accueil

N°	Description
1	Affiche les méthodes de déverrouillage utilisées pour la journée. Survolez un jour pour voir le type de déverrouillage utilisé ce jour-là.
2	Affiche le nombre total d'alarmes.
3	● Cliquez pour accéder à la page du tableau de bord. ● Cliquez sur iSIDER series pour accéder à la page du tableau de bord. ● Cliquez sur pour accéder à la page d'accueil de la plateforme.
4	Affiche l'état des appareils, y compris les appareils hors ligne et les appareils en ligne.
5	Affiche la capacité de données des cartes, des empreintes digitales et des cartes Bluetooth.
6	● Nombre de portes du contrôleur. ◇ : Double porte ◇ : Porte unique ● Type de contrôleur. ◇ : Contrôleur principal. ◇ : Sous-contrôleur. ● : Sélectionner la langue de la plateforme. ● : Accéder directement à la page **Sécurité** (Security). ● : Redémarrer ou se déconnecter de la plateforme. ● : Afficher la page Web en plein écran.

2.2.5 Page d'accueil

Une fois que vous avez réussi à vous connecter, la page d'accueil du contrôleur principal s'affiche.

Figure 2-10 Page d'accueil

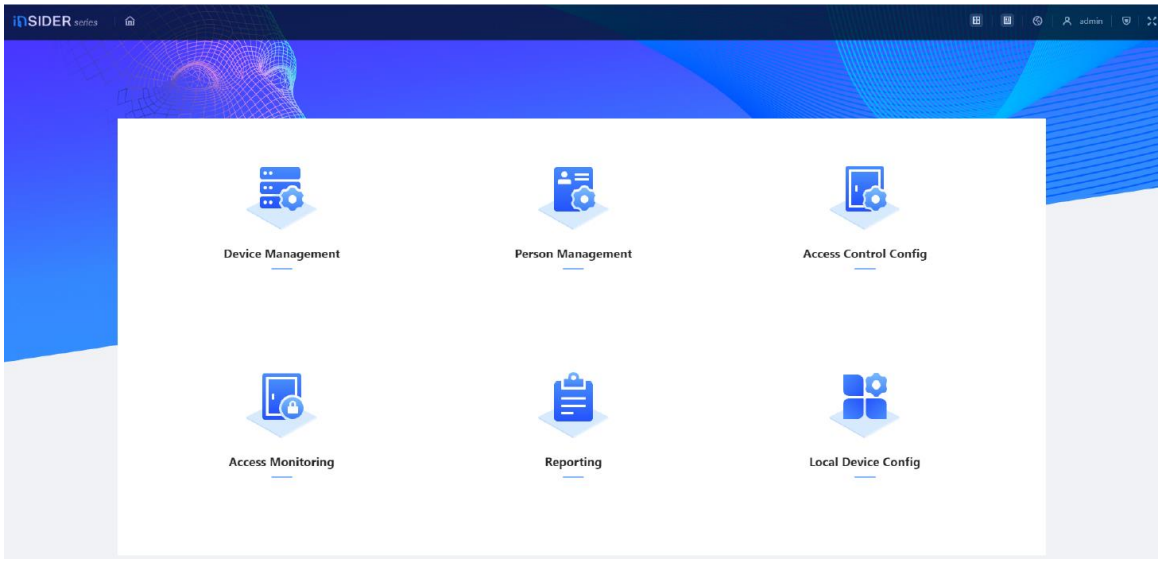


Tableau 2-5 Description de la page d'accueil

Menu	Description
Gestion des Appareils	Ajouter des appareils à la plateforme du contrôleur principal.
Gestion des personnes	Ajouter du personnel et lui attribuer des autorisations de zone.
Configuration du contrôle d'accès	Ajouter des modèles horaires, créer et attribuer des autorisations de zone, configurer des paramètres de porte et des liaisons d'alarme globale, et afficher la progression de l'autorisation.
Surveillance de l'accès	Contrôler les portes à distance et consulter les journaux d'événements.
Rapport	Afficher et exporter les enregistrements d'alarme et de déverrouillage.
Configuration de l'appareil local	Configurer les paramètres de l'appareil local, tels que le réseau et la liaison d'alarme locale.

2.2.6 Ajout des appareils

Vous pouvez ajouter des appareils à la plateforme de gestion du contrôleur principal par lots ou un par un. Si le contrôleur a été défini comme contrôleur principal pendant que vous suiviez l'assistant de connexion, vous pouvez ajouter et gérer des sous-contrôleurs via la plateforme.

Le contrôleur principal n'est livré qu'avec une plateforme de gestion.

2.2.6.1 Ajout d'appareils un par un

Vous pouvez ajouter des sous-contrôleurs au contrôleur principal un par un.

Procédure

Étape 1 : Sur la page d'accueil, cliquez sur **Gestion des appareils** (Device Management), puis sur **Ajouter** (Add).

Étape 2 : Saisissez les informations de l'appareil.

Figure 2-11 Informations de l'appareil

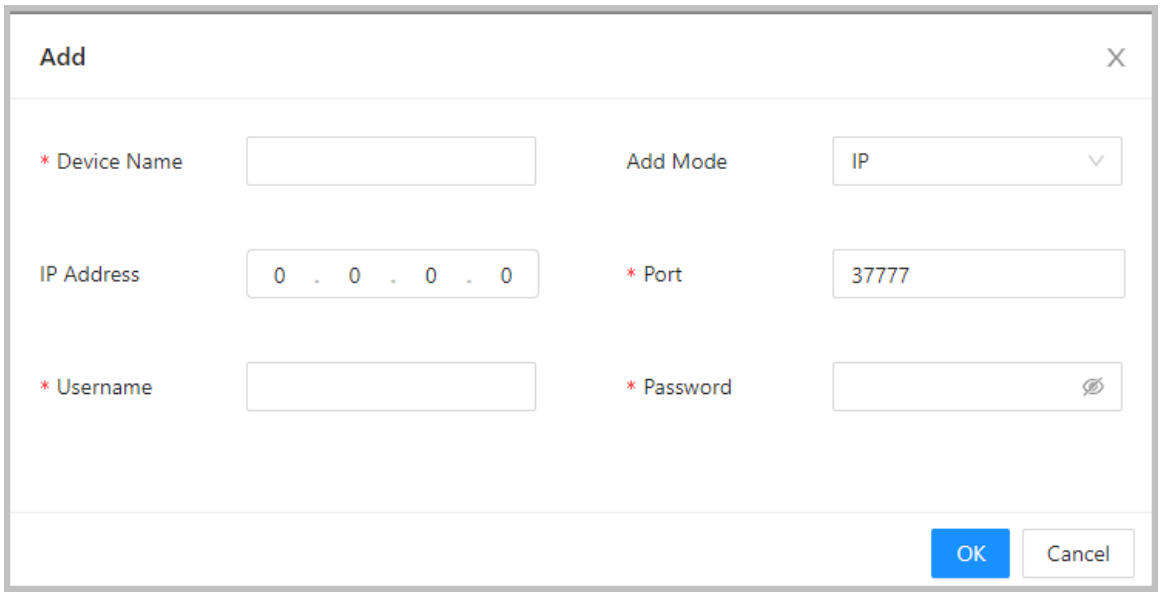


Tableau 2-6 Description des paramètres de l'appareil

Paramètre	Description
Nom de l'appareil	Saisissez le nom du contrôleur. Nous vous recommandons de le nommer d'après sa zone d'installation.
Ajouter mode	Sélectionnez **IP** pour ajouter le contrôleur d'accès en saisissant son adresse IP.
Adresse IP	Saisissez l'adresse IP du contrôleur.
Port	Le numéro de port par défaut est 37777.
Nom d'utilisateur/mot de passe	Saisissez le nom d'utilisateur et le mot de passe du contrôleur.

Étape 3 : Cliquez sur **OK**.

Les contrôleurs ajoutés s'affichent sur la page **Gestion des appareils** (Device Management).

Figure 2-12 Appareils ajoutés avec succès

Si le contrôleur a été défini comme contrôleur principal pendant l'assistant de connexion, il sera automatiquement ajouté à la plateforme de gestion et fonctionnera à la fois comme contrôleur principal et comme sous-contrôleur.

Opérations connexes

- : Modifier les informations sur l'appareil.

  Seuls les sous-contrôleurs prennent en charge les opérations ci-dessous.

- : Accéder à la page Web du sous-contrôleur.
- : Se déconnecter de l'appareil.
- : Supprimer l'appareil.

2.2.6.2 Ajout d'appareils par lots

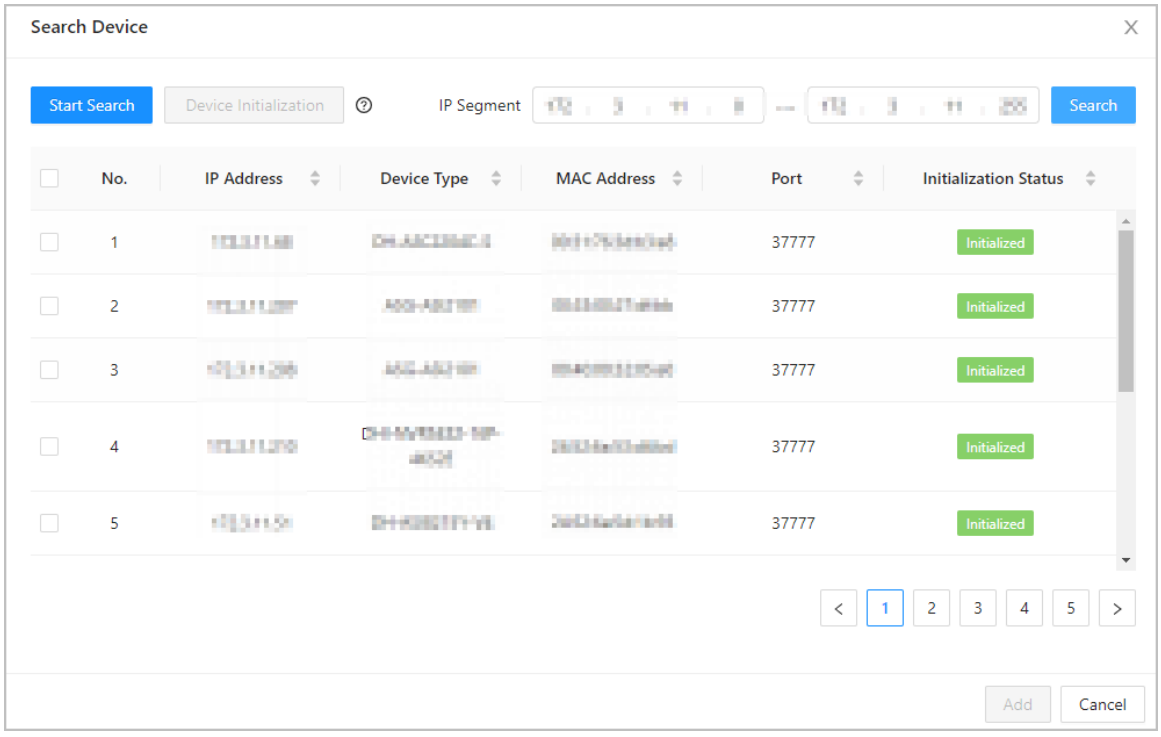
Nous vous recommandons d'utiliser la fonction de recherche automatique lorsque vous ajoutez des sous-contrôleurs par lots. Assurez-vous que les sous-contrôleurs que vous souhaitez ajouter se trouvent sur le même segment réseau.

Procédure

Étape 1 : Sur la page d'accueil, cliquez sur **Gestion des appareils** (Device Management), puis sur **Rechercher l'appareil** (Search Device).

- Cliquez sur **Démarrer la recherche** (Start Search) pour rechercher des appareils sur le même réseau local.
- Saisissez une plage pour le segment réseau, puis cliquez sur **Rechercher** (Search).

Figure 2-13 Recherche automatique



Tous les appareils recherchés s'affichent.

Vous pouvez sélectionner des appareils dans la liste et cliquer sur **Initialisation des appareils** (Device Initialization) pour les initialiser par lots.

Pour garantir la sécurité des appareils, l'initialisation n'est pas prise en charge pour les appareils situés sur des segments différents.

Étape 2 : Sélectionnez les contrôleurs que vous souhaitez ajouter à la plateforme, puis cliquez sur **Ajouter** (Add).

Étape 3 : Saisissez le nom d'utilisateur et le mot de passe du sous-contrôleur, puis cliquez sur **OK**. Les sous-contrôleurs ajoutés s'affichent sur la page **Gestion des appareils** (Device Management).

Opérations connexes

- Modifier l'adresse IP : Sélectionnez les appareils ajoutés, puis cliquez sur **Modifier l'IP** (Modify IP) pour modifier les adresses IP.
- Synchronisation de l'heure : Sélectionnez les appareils ajoutés, puis cliquez sur **Synchro de l'heure** (Sync Time) pour synchroniser l'heure des appareils avec le serveur NTP.
- Supprimer : Sélectionnez les appareils, puis cliquez sur **Supprimer** (Delete) pour les supprimer.

2.2.7 Ajout d'utilisateurs

Ajoutez des utilisateurs aux départements. Saisissez les informations de base des utilisateurs et définissez les méthodes de vérification de leur identité.

Opérations connexes

- Exportation de tous les utilisateurs vers Excel : Sur la page **Gestion des personnes** (Person Management), cliquez sur **Exporter** (Export) pour exporter tous les utilisateurs. Vous pouvez également importer les informations exportées sur les utilisateurs vers d'autres contrôleurs.

  Pour éviter toute perte de données causée par des dommages de force majeure à l'équipement, il est recommandé d'exporter régulièrement les données des utilisateurs à des fins de sauvegarde.
- Importation des utilisateurs : Sur la page **Gestion des personnest** (Person Management), cliquez sur **Télécharger le modèle** (Download Template), saisissez les informations relatives à l'utilisateur dans le modèle, puis cliquez sur **Importer** (Import) pour importer tous les utilisateurs.
- Extraction de tous les utilisateurs : Sur la page **Gestion des personnes** (Person Management), cliquez sur **Plus > Extraire les infos sur les personnes** (More > Extract Person Info), puis sélectionnez un appareil pour extraire tous les utilisateurs du sous-contrôleur et leur envoyer la plateforme du contrôleur principal.

2.2.7.1 Ajout de départements

Procédure

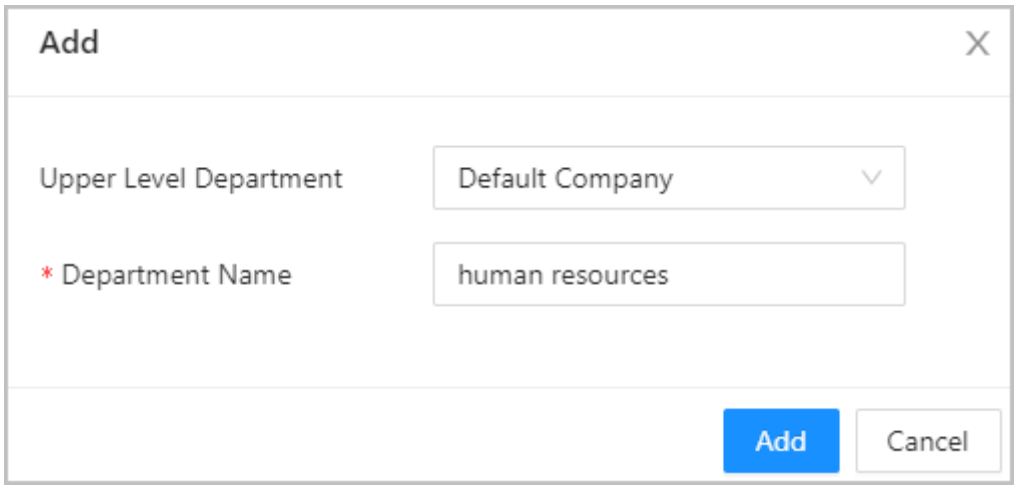
Étape 1 : Sur la page d'accueil, sélectionnez **Gestion des personnes** (Person Management).

Étape 2 : Créez un département.

1. Cliquez sur + .
2. Saisissez le nom du département, puis cliquez sur **Ajouter** (Add).

Le département par défaut ne peut pas être supprimé.

Figure 2-14 Ajout de département



Étape 3 : Cliquez sur **OK**.

2.2.7.2 Ajout de rôles

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Gestion des personnes** (Person Management).

Étape 2 : Créez des rôles.

- Les rôles suivants existent déjà et ne peuvent être ni modifiés ni supprimés : Défaut, Gestionnaire, Administrateur, Visiteur et Employé.
- Le seul type d'utilisateur général ayant le rôle de gestionnaire dispose de l'autorité la plus élevée et n'est pas limité par les règles d'accès avancées, telles que le déverrouillage par la première carte, le déverrouillage multi-personnes, l'antiretour, la porte toujours fermée et les méthodes de déverrouillage.

1. Cliquez sur + .
2. Saisissez le nom du rôle, puis cliquez sur **Ajouter** (Add).

2.2.7.3 Configuration des informations de base sur l'utilisateur

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Gestion des personnes** (Person Management).

Étape 2 : Ajoutez des utilisateurs.

- Ajoutez des utilisateurs une par une.
  1. Cliquez sur **Ajouter** (Add), puis saisissez les informations de base de l'utilisateur.

Figure 2-15 Informations de base sur l'utilisateur

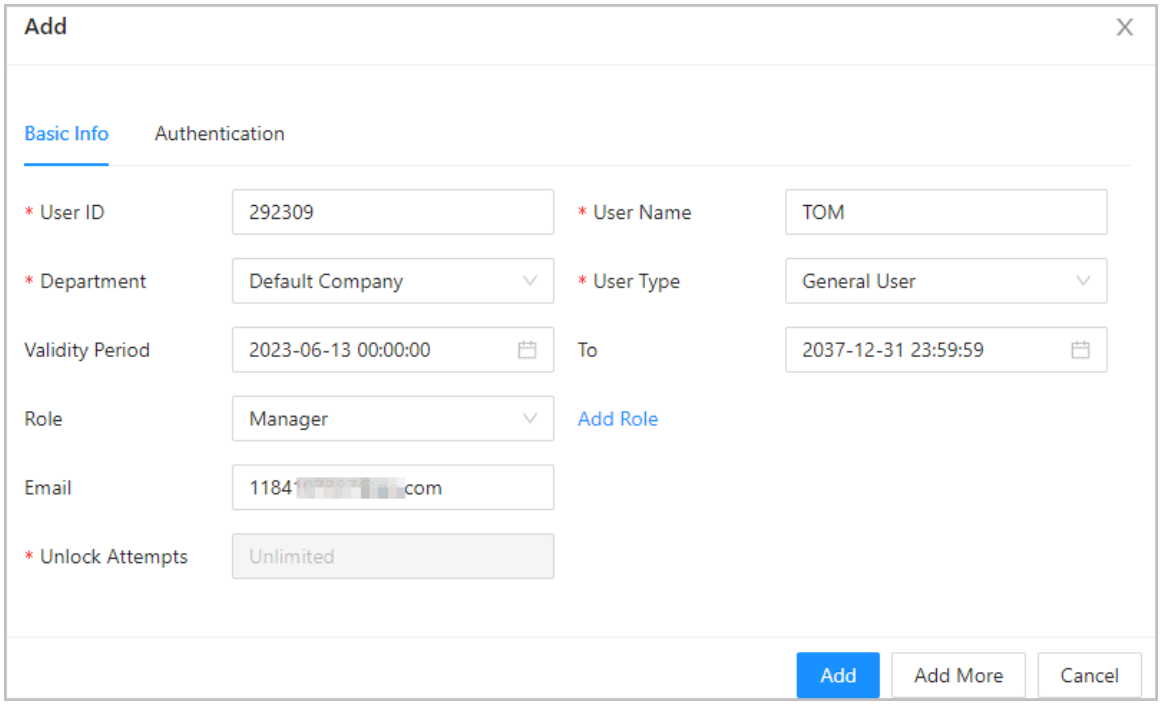


Tableau 2-7 Description des paramètres

Paramètre	Description
ID utilisateur	ID de l'utilisateur.
Service	Département auquel l'utilisateur appartient. Pour plus de détails sur la création de départements, reportez-vous à la section « 2.2.7.1 Ajout de départements ».
Période de validité	Définissez une date à laquelle les autorisations d'accès de la personne seront effectives.
Rôle	Attribuez un rôle existant à l'utilisateur. Vous pouvez également cliquer sur **Ajouter un rôle** (Add Role) pour créer un nouveau rôle.
E-mail	L'adresse e-mail doit être la même que celle utilisée pour s'inscrire au DMSS.
À	Définissez une date à laquelle les autorisations d'accès de la personne expireront.
Nom d'utilisateur	Nom de l'utilisateur.

Paramètre	Description
Type utilisateur	Type d'utilisateur. ● **Utilisateur général :** Les utilisateurs généraux peuvent déverrouiller la porte. ● **Utilisateur VIP :** Lorsque le VIP déverrouille la porte, le personnel de service reçoit une notification. ● **Utilisateur invité :** Les invités peuvent déverrouiller la porte au cours d'une période définie ou pour un nombre de fois déterminé. Une fois que la période définie a expiré ou que le nombre de fois pour le déverrouillage a expisré, ils ne peuvent plus déverrouiller la porte. ● **Utilisateur patrouilleur :** Les utilisateurs patrouilleurs verront leurs présences suivies, mais ils ne sont pas autorisés à déverrouiller la porte. ● **Utilisateur de la liste de blocage :** Lorsque des utilisateurs figurant sur la liste de blocage déverrouillent la porte, le personnel de service reçoit une notification. ● **Autres utilisateurs :** Lorsqu'ils déverrouillent la porte, celle-ci reste déverrouillée pendant 5 secondes supplémentaires.
Tentatives de déverrouillage	Le nombre de fois qu'un utilisateur invité peut déverrouiller la porte.

2. Cliquez sur **Ajouter** (Add).

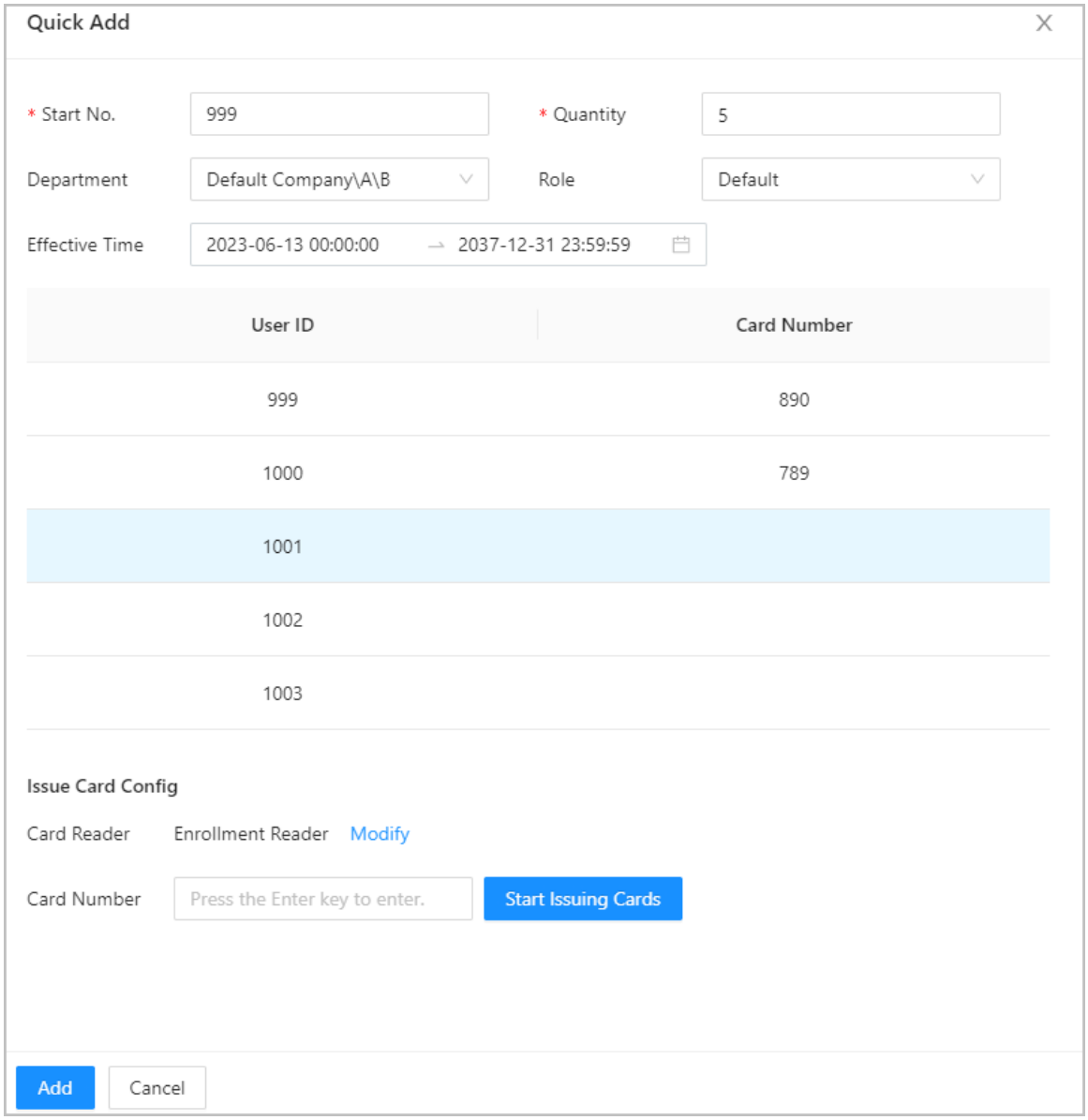
   Vous pouvez cliquer sur **Ajouter plus** (Add More) pour ajouter d'autres utilisateurs.

- Ajoutez des utilisateurs en important le modèle.
  1. Cliquez sur **Importer > Télécharger le modèle** (Import > Download Template) pour télécharger le modèle d'utilisateur.
  2. Saisissez les informations de l'utilisateur dans le modèle, puis enregistrez-le.
  3. Cliquez sur **Importer** (Import) et téléchargez le modèle sur la plateforme.

     Les utilisateurs sont automatiquement ajoutés à la plateforme.
- Utilisez **Ajout rapide** (Quick Add) pour ajouter facilement des utilisateurs.
  1. Cliquez sur **Ajout rapide** (Quick Add).
  2. Saisissez le numéro de départ de l'ID utilisateur et la quantité.

     La plateforme génère une séquence de numéros à partir du numéro de départ défini. Par exemple, si le numéro de départ est 999 et la quantité 5, le système génère une séquence de numéros allant de 999 à 1003.

Figure 2-16 Ajout rapide



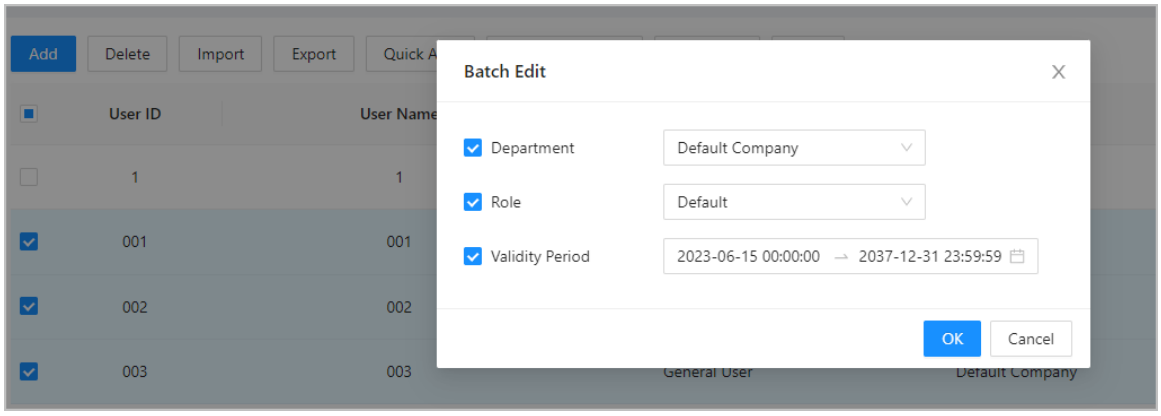
3. Sélectionnez le département, le rôle et l'heure d'entrée en vigueur.
4. Émettez les cartes aux utilisateurs par lots.

   Vous pouvez saisir manuellement le numéro de carte ou utiliser le lecteur de badge ou le lecteur de carte pour lire le numéro de la carte. Pour les détails, voir « 2.2.7.4.2 Ajout de cartes ».

Opérations connexes

Modification par lots : Modifier les informations personnelles par lots.

Figure 2-17 Modification par lots



2.2.7.4 Ajout de méthodes d'authentification

Ajoutez des mots de passe, des cartes, des empreintes digitales ou des cartes Bluetooth aux utilisateurs, afin qu'ils puissent déverrouiller la porte par authentification. Chaque utilisateur peut avoir jusqu'à 1 mot de passe, 5 cartes à puce/d'identité, 3 empreintes digitales et 5 cartes Bluetooth.

2.2.7.4.1 Ajout de mots de passe

Ajoutez des mots de passe aux utilisateurs pour qu'ils puissent accéder à la porte en saisissant leur mot de passe.

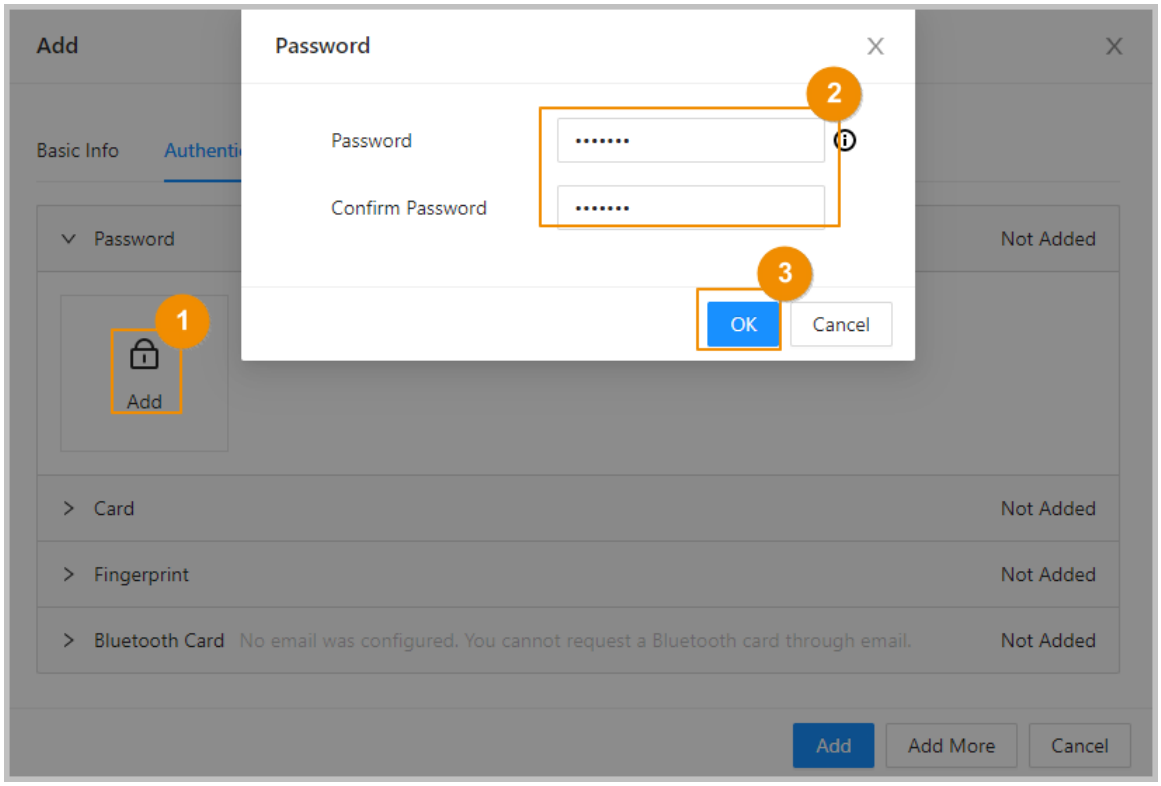
Procédure

Étape 1 : Dans l'onglet **Authentification** (Authentication), cliquez sur **Ajouter** (Add)

Étape 2 : Entrez et confirmez le mot de passe.

Étape 3 : Cliquez sur **OK**.

Figure 2-18 Ajout du mot de passe



- Si l'authentification par code PIN n'est pas activée, vous pouvez déverrouiller la porte en saisissant le mot de passe de déverrouillage au format **ID utilisateur#mot de passe#** (user ID#password#). Par exemple, si l'ID utilisateur est 123 et que le mot de passe défini est 12345, vous devez saisir **123#12345#** pour déverrouiller la porte.
- Si l'authentification par code PIN est activée, vous pouvez déverrouiller la porte en saisissant le mot de passe de déverrouillage au format **mot de passe#** (password#). Par exemple, si l'ID utilisateur est 123 et que le mot de passe défini est 12345, vous devez saisir **12345#** pour déverrouiller la porte.

2.2.7.4.2 Ajout de cartes

Ajoutez des cartes à puce ou des cartes d'identité aux utilisateurs pour qu'ils puissent accéder au système en glissant leur carte

Procédure

Étape 1 : (En option) Avant d'attribuer des cartes aux utilisateurs, définissez le type de carte et le type de numéro de carte.

1. Sur la page **Gestion des personnes** (Person Management), sélectionnez **Plus > Type de carte**(More > Card Type).
2. Si vous prévoyez d'émettre des cartes à l'aide d'un lecteur de badge, sélectionnez un type de carte, puis cliquez sur **OK**.

Assurez-vous que le type de carte est identique à celui qui sera émis lorsque vous prévoyez d'émettre des cartes à l'aide d'un lecteur de badge. Pour les détails, voir #d121e127a1310.

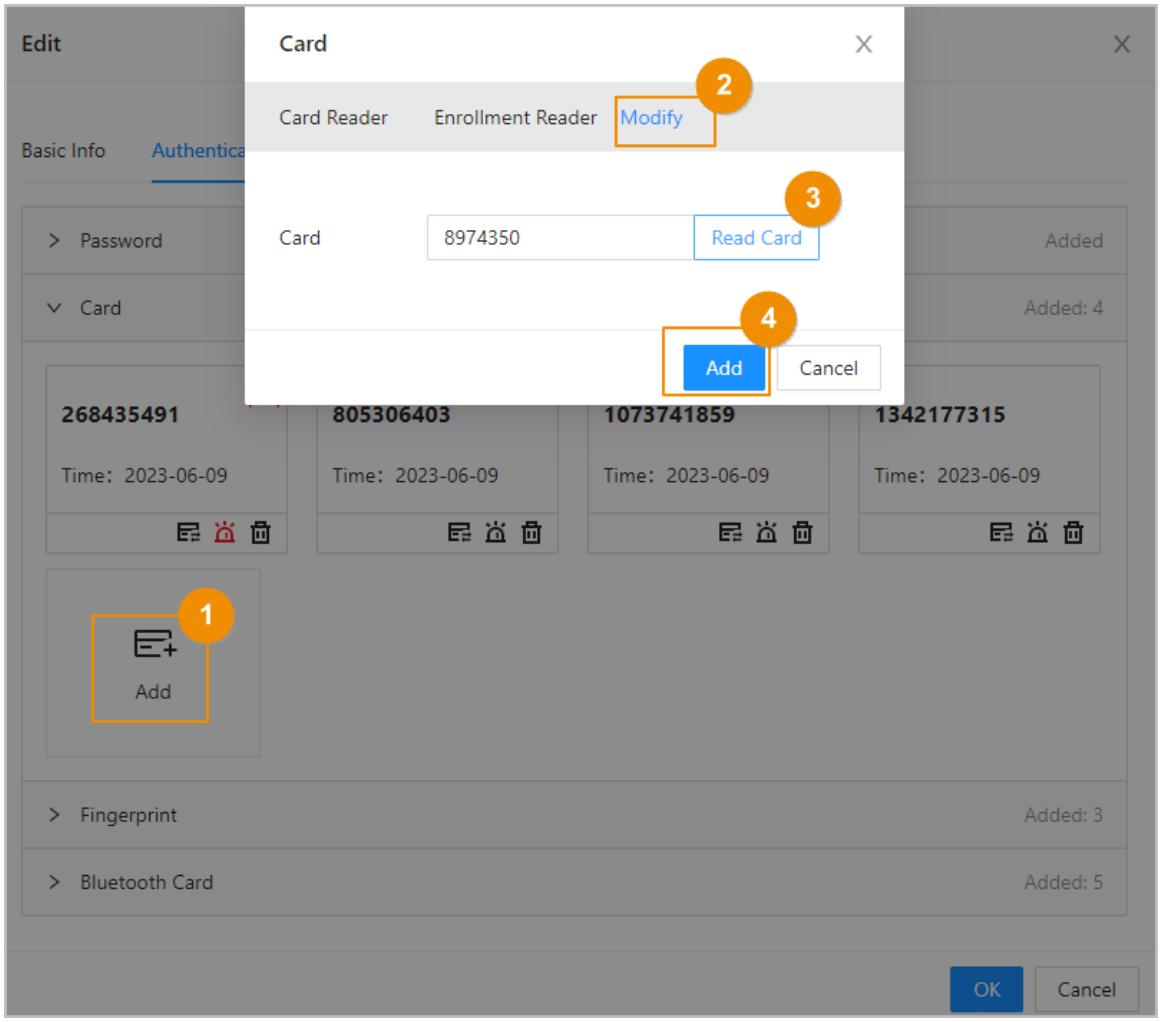
3. Sélectionnez **Plus > Système du n° de carte** (More > Card No. System).
4. Sélectionnez le format décimal ou hexadécimal pour le numéro de carte.

Étape 2 : Dans l'onglet **Authentification** (Authentication), cliquez sur **Carte** (Card) pour ajouter des cartes.

4 méthodes sont disponibles pour l'ajout de cartes.

- Saisissez le numéro de carte manuellement.
  1. Cliquez sur **Ajouter** (Add).
  2. Saisissez le numéro de carte, puis cliquez sur **Ajouter** (Add).
- Utilisez le lecteur de badge pour lire le numéro de carte.

Figure 2-19 Utilisation du lecteur de badge pour lire le numéro de carte



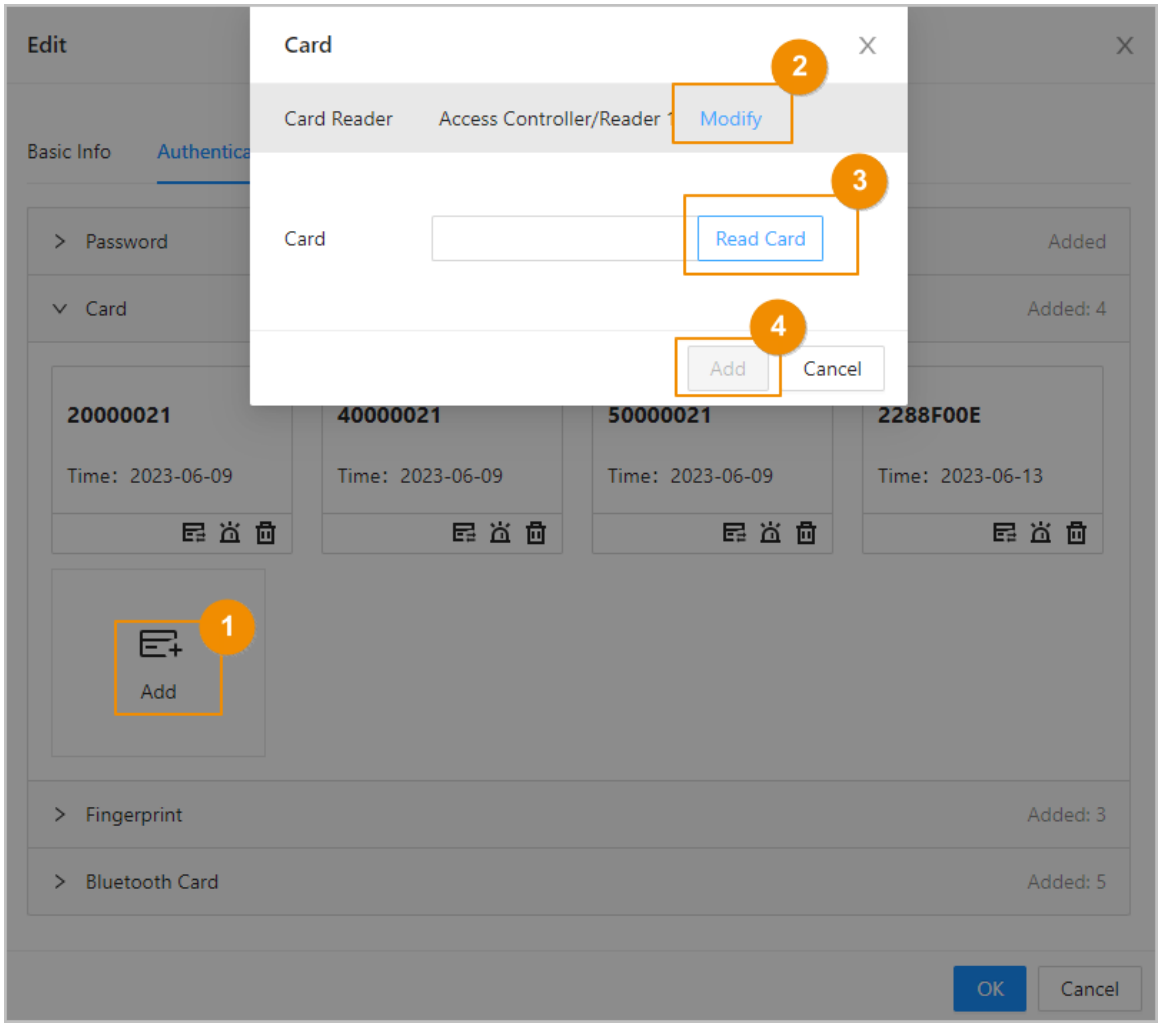
1. Cliquez sur **Ajouter** (Add).
2. Cliquez sur **Modifier** (Modify), puis sélectionnez un **Lecteur de badge/carte** (Enrollment Reader).

   Assurez-vous que le lecteur de badge/carte est connecté à votre ordinateur.
3. Suivez les instructions à l'écran pour télécharger et installer le plug-in.

4. Cliquez sur **Lire la carte** (Read Card), puis glissez les cartes dans le lecteur de badge/carte.
   Un compte à rebours de 60 secondes s'affiche pour vous rappeler de glisser la carte, et le système lit automatiquement le numéro de carte. Si le compte à rebours de 60 secondes expire, cliquez à nouveau sur **Lire la carte** (Read Card) pour lancer un nouveau compte à rebours.
5. Cliquez sur **Ajouter** (Add).

- Utilisez le lecteur de carte pour lire le numéro de carte.

Figure 2-20 Utilisation du lecteur de carte pour lire le numéro de carte



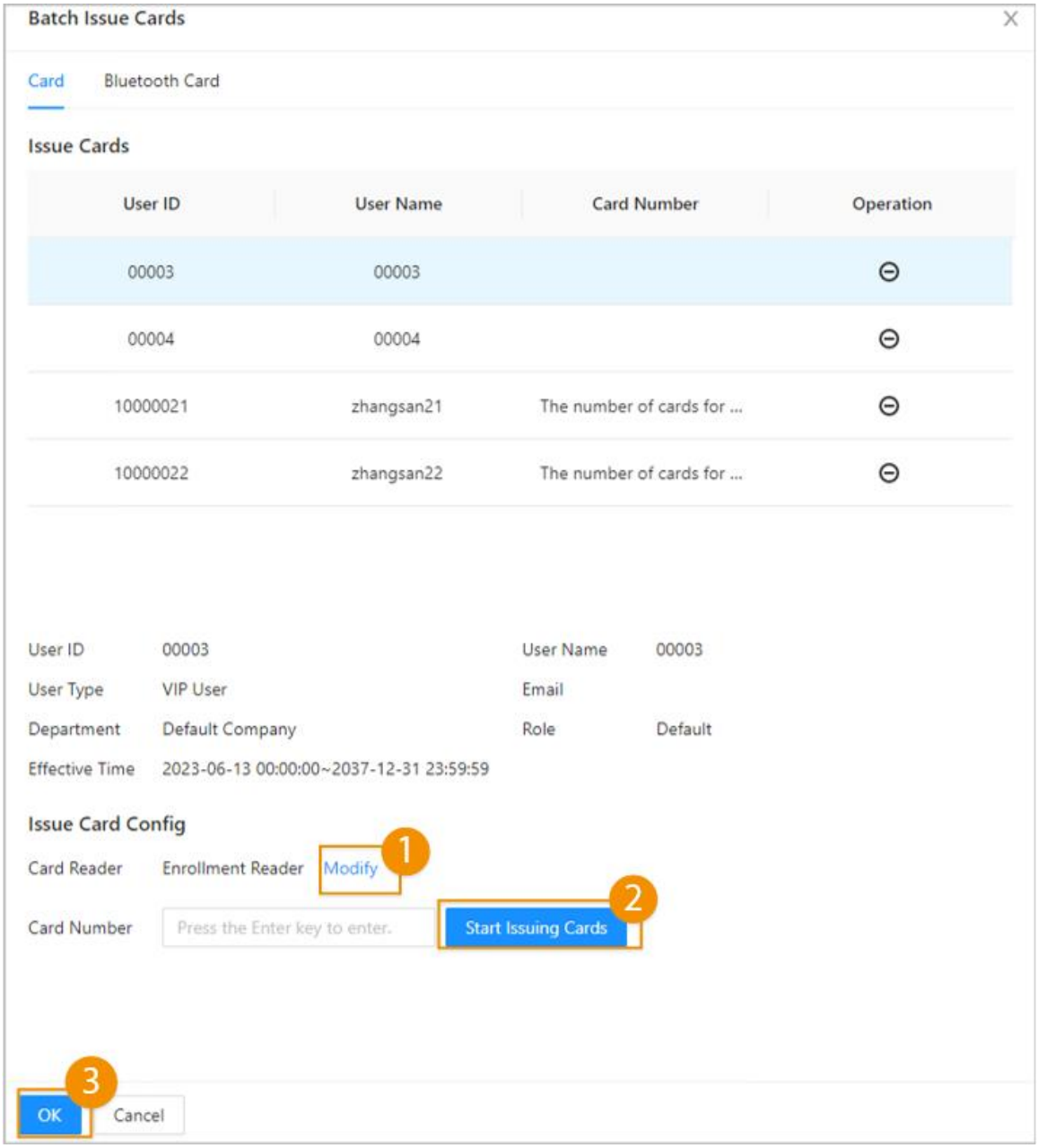
1. Cliquez sur **Modifier** (Modify), puis sélectionnez un Lecteur de carte.
   Assurez-vous que le lecteur de carte est connecté au contrôleur d'accès.
2. Cliquez sur **Lire la carte** (Read Card), puis glissez les cartes dans le lecteur de carte.
   Un compte à rebours de 60 secondes s'affiche pour vous rappeler de glisser la carte, et le système lit automatiquement le numéro de carte. Si le compte à rebours de 60 secondes expire, cliquez à nouveau sur **Lire la carte** (Read Card) pour lancer un nouveau compte à rebours.
3. Cliquez sur **Ajouter** (Add).

- Ajoutez des cartes par lots : Émettez les cartes aux utilisateurs par lots.
  1. Cliquez sur **Émission des cartes par lots** (Issue Cards to All Users), puis sélectionnez

Émission des cartes aux utilisateurs sélectionnés (Issue Cards to Selected Users) ou **Émission des cartes à tous les utilisateurs** (Issue Cards to All Users).

2. Vous pouvez saisir manuellement le numéro de la carte ou cliquer sur **Modifier** (Modify) pour émettre des cartes via le lecteur de badge ou le lecteur de carte.

Figure 2-21 Émission des cartes via le lecteur de badge ou le lecteur de carte



Opérations connexes

- : Modifier le numéro de la carte.
- : Définir la carte comme carte sous contrainte.
  Une alarme est déclenchée lorsque des personnes utilisent la carte sous contrainte pour déverrouiller la porte.
- : Supprimer la carte.

2.2.7.4.3 Ajout des empreintes digitales

Ajoutez des empreintes digitales aux utilisateurs pour qu'ils puissent utiliser leurs empreintes digitales pour déverrouiller les portes.

Procédure

Étape 1 : Dans l'onglet **Authentification** (Authentication), cliquez sur **Empreinte digitale** (Fingerprint).

Étape 2 : Connectez un scanner d'empreintes digitales à l'ordinateur et suivez les instructions à l'écran pour enregistrer l'empreinte digitale.

Étape 3 : Cliquez sur **Ajouter** (Add).

2.2.7.4.4 Ajout des cartes Bluetooth

Ajoutez des cartes Bluetooth aux utilisateurs pour qu'ils puissent accéder aux portes à l'aide de cartes Bluetooth.

Conditions préalables

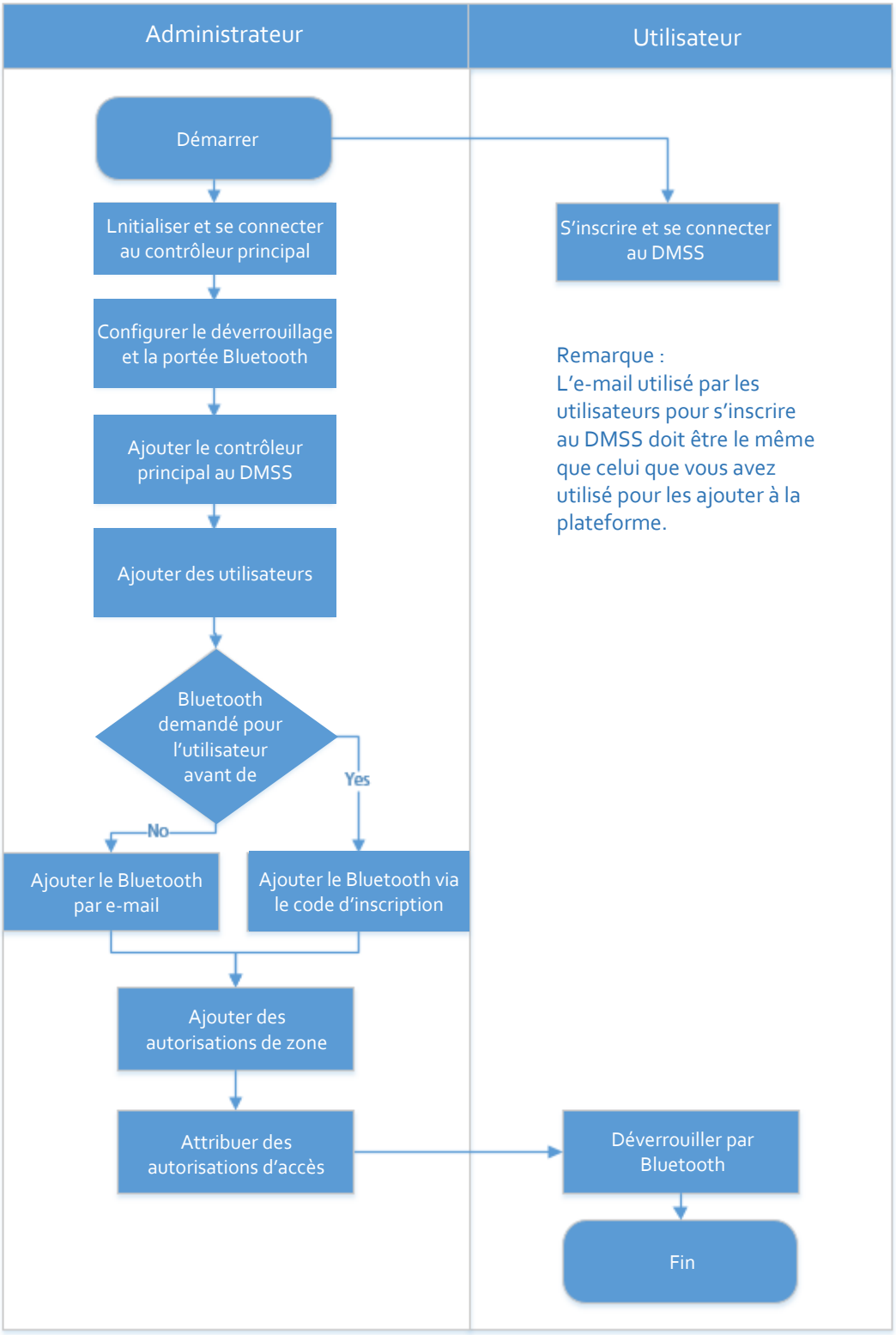
- La fonction de déverrouillage Bluetooth a été activée.
- Le contrôleur principal a été ajouté au DMSS. Pour les détails, voir « 2.2.21.4.3 Configuration du service cloud ».
- Des utilisateurs ont été ajoutés à la plateforme du contrôleur d'accès. Pour les détails, voir « 2.2.7.3 Configuration des informations de base sur l'utilisateur ».
- Les utilisateurs généraux, comme les employés d'une entreprise, ont installé le DMSS et s'y sont inscrits avec leur e-mail.

L'e-mail utilisé par les utilisateurs pour s'inscrire au DMSS doit être le même que celui que vous avez utilisé pour les ajouter au contrôleur d'accès.

Préambule

Reportez-vous à l'organigramme de la configuration du déverrouillage Bluetooth. L'administrateur et les utilisateurs généraux doivent effectuer des opérations différentes pour terminer le processus. Les utilisateurs généraux, comme les employés de l'entreprise, ne doivent que s'inscrire et se connecter au DMSS via leur e-mail pour déverrouiller les portes à l'aide des cartes Bluetooth qui leur ont été délivrées.

Figure 2-22 Organigramme de la configuration du déverrouillage Bluetooth



Procédure

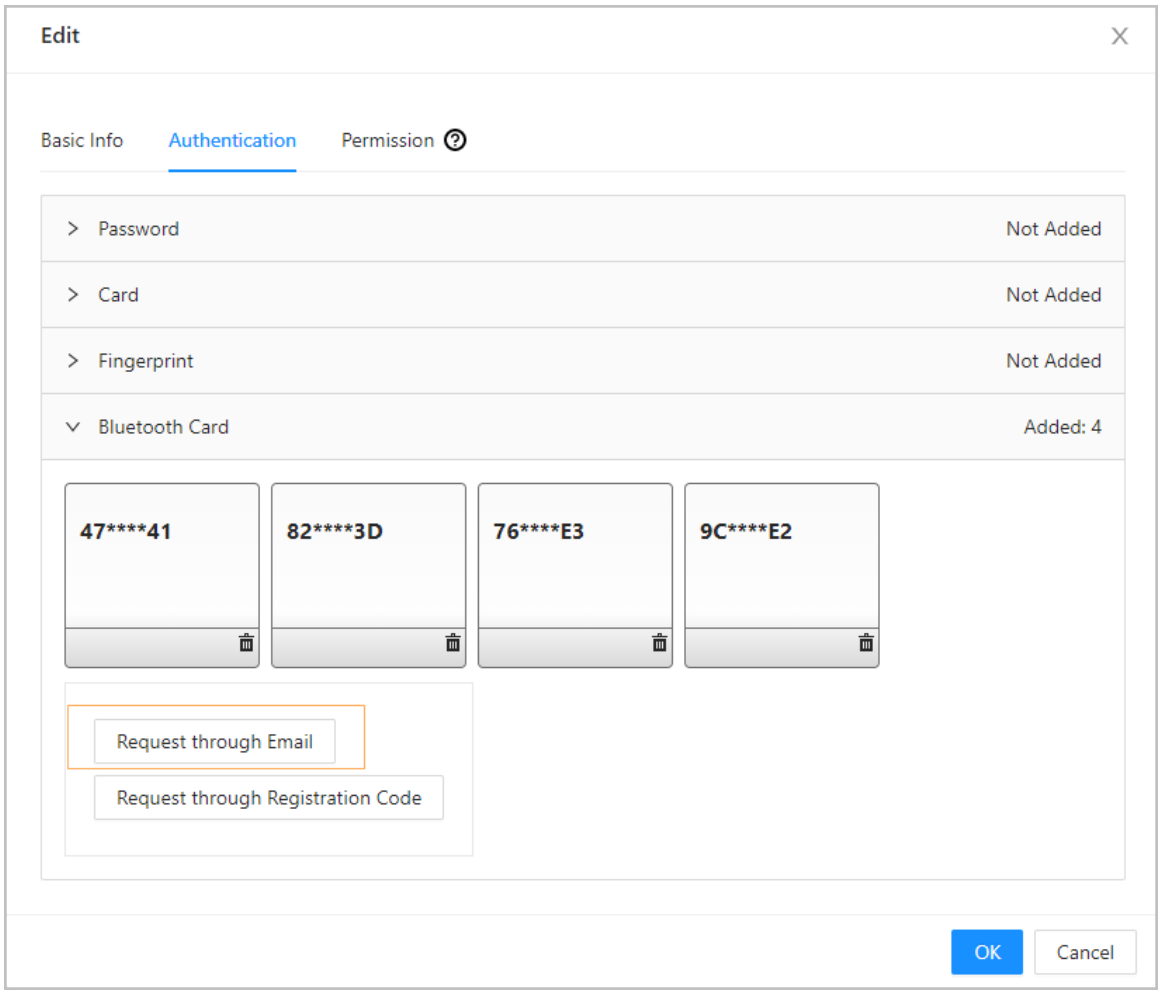
Étape 1 : Dans l'onglet, cliquez sur **Carte Bluetooth** (Bluetooth Card).

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

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

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

Figure 2-23 Demande par e-mail

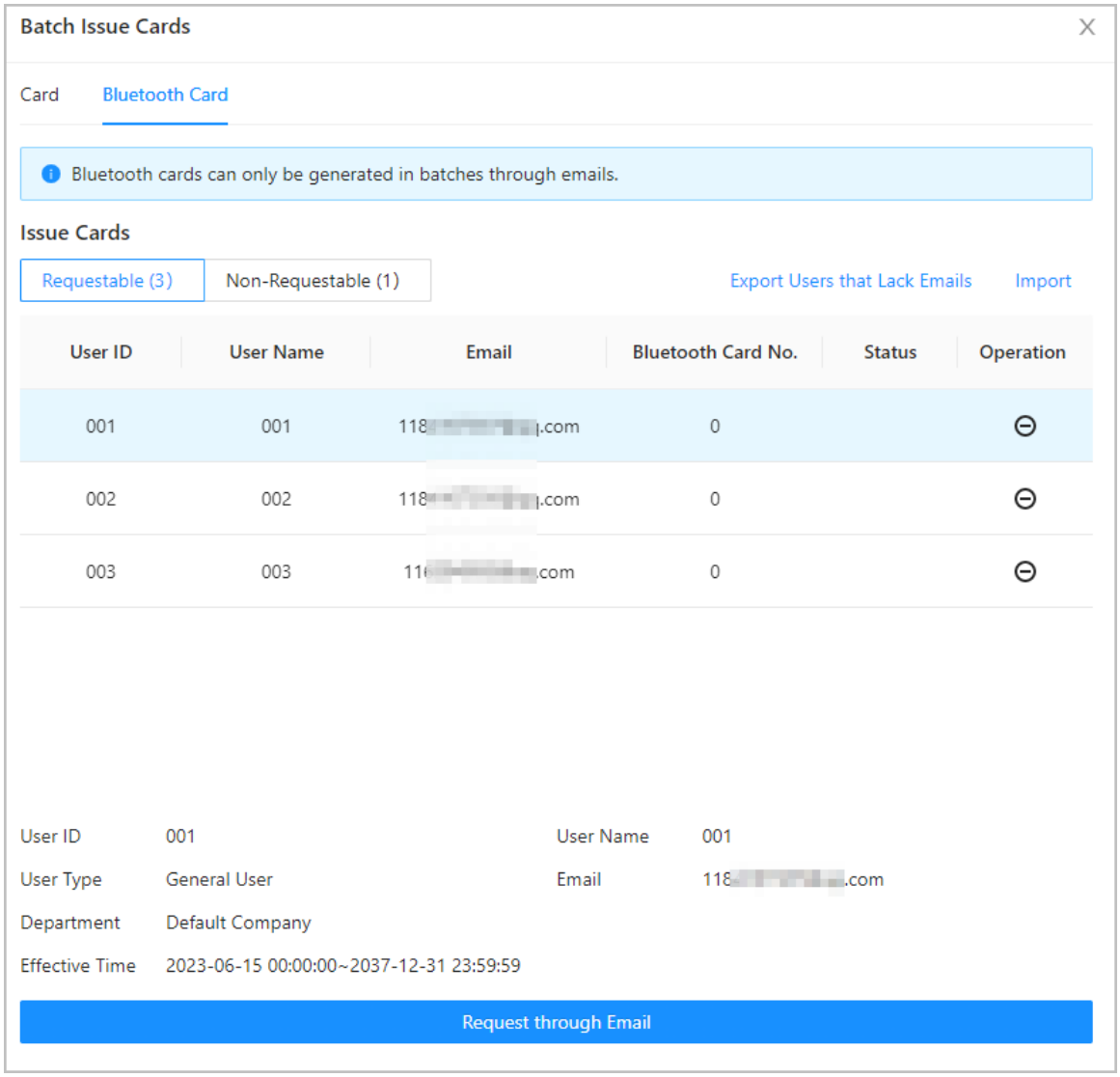


- Demande via e-mail par lots.
  1. Dans la page **Gestion des personnes** (Person Management), cliquez sur **Émission des cartes par lots** (Batch Issue Cards).

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

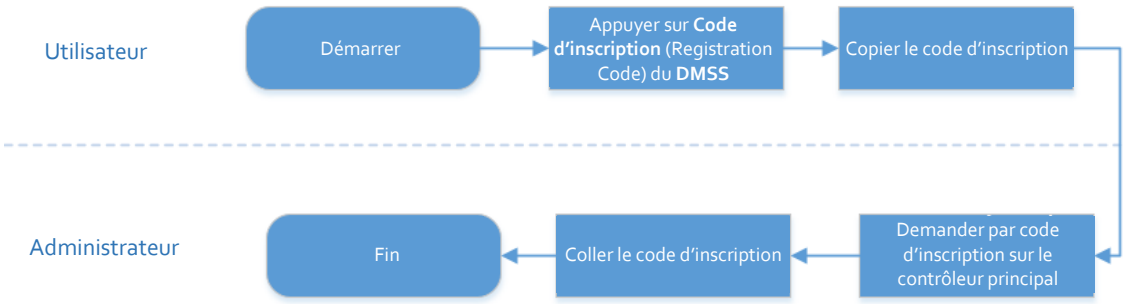
- Les utilisateurs qui ne disposent pas d'e-mail ou qui possèdent déjà 5 cartes Bluetooth seront affichés dans la liste des utilisateurs ne pouvant pas faire de demande.
- Exporter les utilisateurs n'ayant pas d'e-mail : Cliquez sur **Exporter** (Export), entrez les e-mails dans le format correct, puis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

Figure 2-24 Émission des cartes par lots



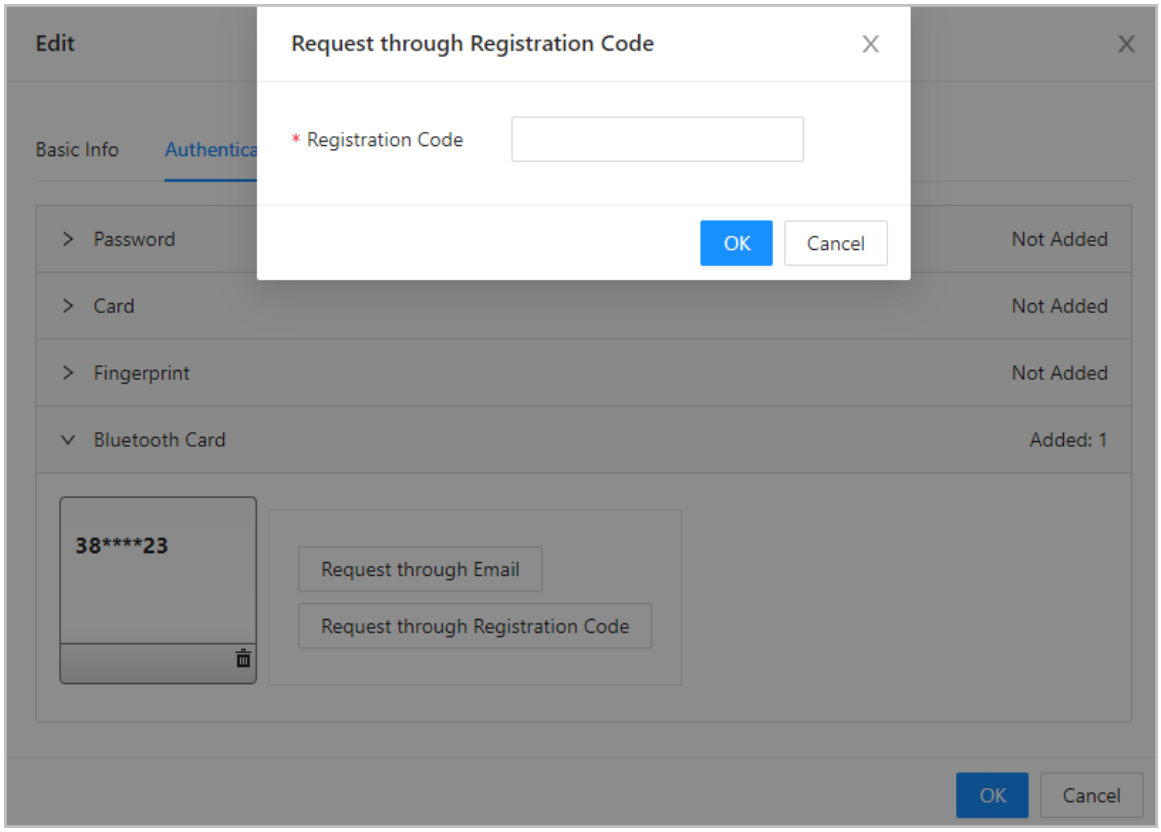
- Si vous avez déjà demandé des cartes Bluetooth pour l'utilisateur, vous pouvez ajouter les cartes Bluetooth à l'aide d'un code d'inscription en utilisant des codes d'inscription.

Figure 2-25 Organigramme de la demande par code d'inscription



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

Figure 2-26 Demande par code d'inscription



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

Étape 2 : Cliquez sur **OK**.

Résultat

Une fois que les utilisateurs se sont inscrits et connectés à DMSS avec leur adresse e-mail, ils peuvent ouvrir DMSS pour déverrouiller la porte à l'aide des cartes Bluetooth. Pour plus de détails, consultez le

manuel d'utilisation du DMSS.

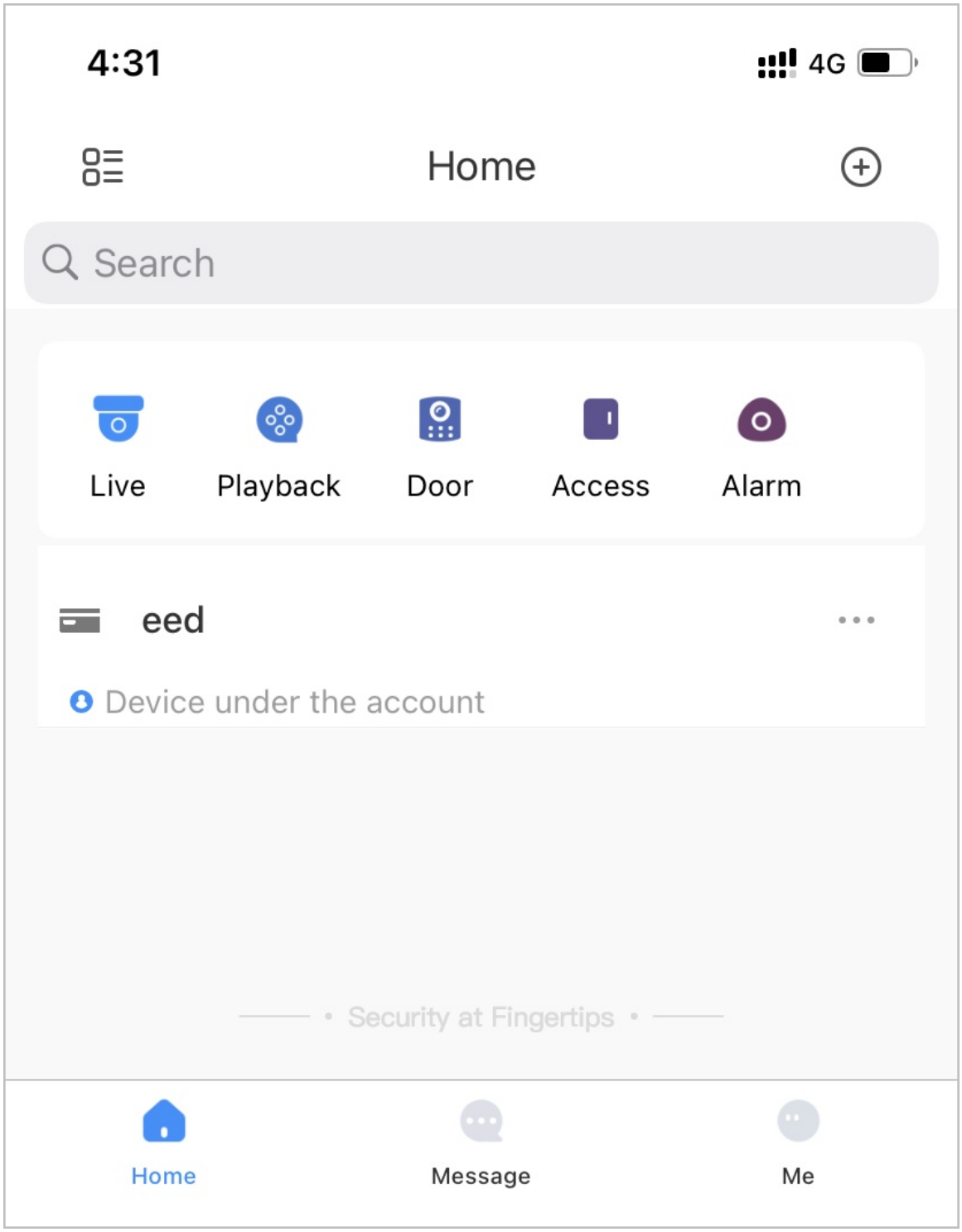
- Déverrouillage automatique : La porte se déverrouille automatiquement lorsque vous vous trouvez dans la zone Bluetooth définie, ce qui permet à la carte Bluetooth de transmettre des signaux au lecteur de carte.

  En mode de déverrouillage automatique, la carte Bluetooth peut déverrouiller continuellement la porte lorsque vous êtes dans la portée Bluetooth pendant une longue période jusqu'à ce qu'une défaillance se produise. Veuillez désactiver le Bluetooth sur le téléphone et le réactiver.

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

Figure 2-27 Déverrouillage de la porte à l'aide des cartes Bluetooth



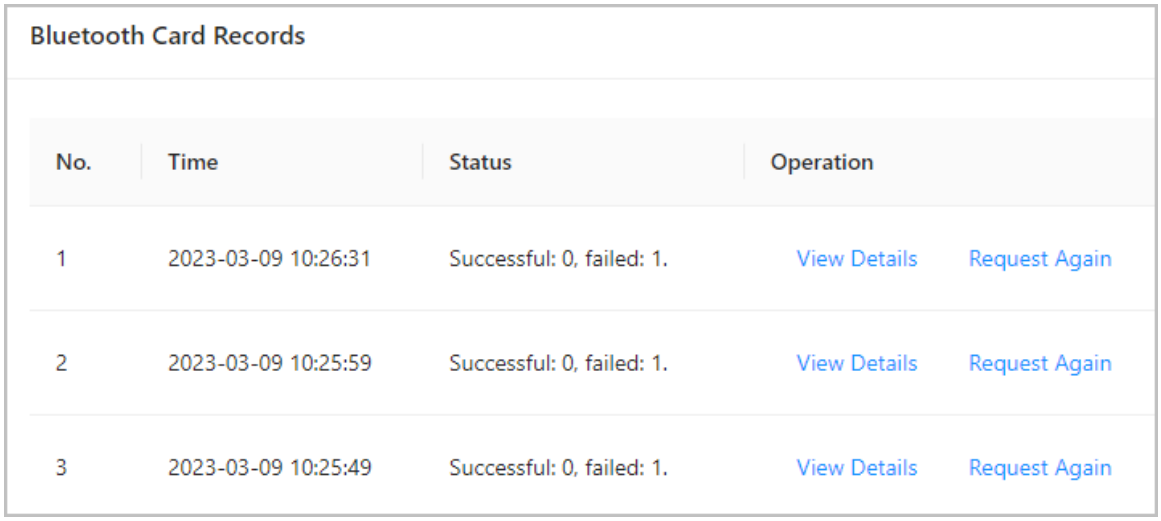
Opérations connexes

- Les utilisateurs peuvent gérer les cartes Bluetooth sur le DMSS.
  - Déplacer vers le haut : Si plusieurs cartes Bluetooth ont été ajoutées, vous pouvez déplacer vers le haut les cartes en cours d'utilisation.
  - Renommer : Renommez la carte Bluetooth.
  - Supprimer : Supprimez la carte Bluetooth.
- Exporter les utilisateurs n'ayant pas d'e-mail : Cliquez sur **Exporter** (Export), entrez les e-mails dans le format correct, puis cliquez sur Importer (Import). Ils seront déplacés vers la liste des

utilisateurs pouvant faire de demande.

- Afficher les enregistrements des demandes : Sur la page **Gestion des personnes** (Person Management), cliquez sur **Plus > Enregistrements de carte Bluetooth** (More > Bluetooth Card Records) pour afficher l'état de la demande.

Figure 2-28 État de la demande



  - ◇ Afficher les détails : Affichez les détails de la demande, y compris les informations sur l'utilisateur, les raisons pour lesquelles les demandes ont échoué, etc. Vous pouvez également effectuer une nouvelle demande pour les utilisateurs dont la demande a échoué.
  - ◇ Demander à nouveau : Effectuez à nouveau la demande pour les utilisateurs ayant échoué.

2.2.8 Ajout des plans hebdomadaires

Le plan hebdomadaire permet de définir le calendrier de déverrouillage de la semaine. La plateforme propose un modèle par défaut avec un horaire de jour complet. Vous pouvez également créer vos propres modèles.

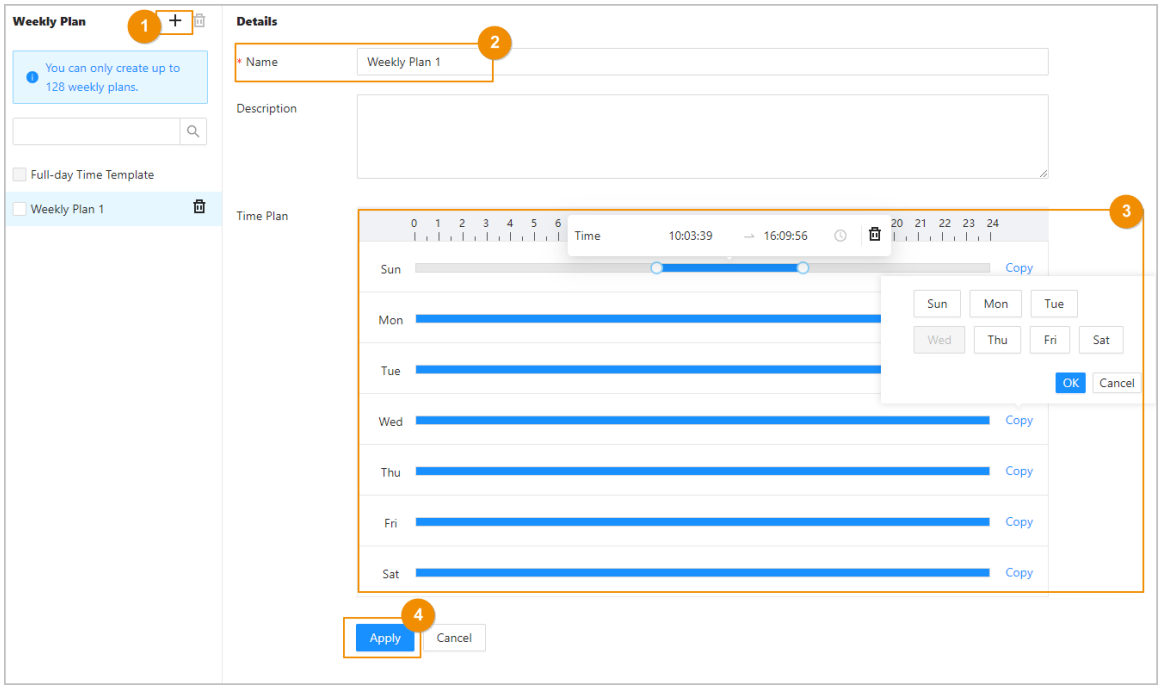
Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. du contrôle d'accès > Plan hebdomadaire** (Access Control Config > Weekly Plan), puis cliquez sur + .

- Le modèle horaire de journée complète par défaut ne peut pas être modifié.
- Vous pouvez créer jusqu'à 128 plans hebdomadaires.

Étape 2 : Saisissez le nom du modèle horaire.

Figure 2-29 Création du plan hebdomadaire



Étape 3 : Faites glisser le curseur pour ajuster la période de temps pour chaque jour.

Vous pouvez également cliquer sur **Copier** (Copy) pour appliquer la période configurée à d'autres jours.

Vous pouvez configurer jusqu'à 4 tranches horaires par jour.

Étape 4 : Cliquez sur **Appliquer** (Apply).

2.2.9 Ajout de plans de congé (en option)

Le plan de congé permet de définir le calendrier de déverrouillage des congés.

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. du contrôle d'accès > Plan de congé** (Access Control Config > Holiday Plan), puis cliquez sur +.

Vous pouvez créer jusqu'à 128 plans de congé.

Étape 2 : Saisissez le nom du plan de congé.

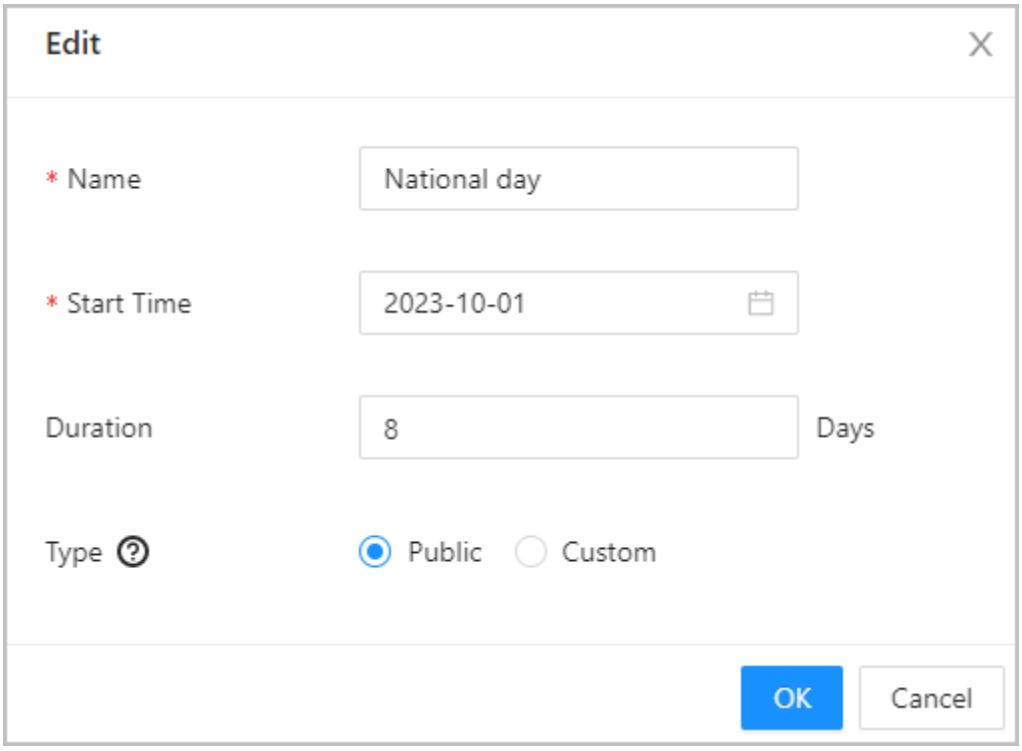
Étape 3 : Faites glisser le curseur pour ajuster la période de temps pour chaque jour.

Vous pouvez configurer jusqu'à 4 tranches horaires par jour.

Étape 4 : Cliquez sur **Ajouter** (Add) pour ajouter des jours fériés au plan de vacances, puis cliquez sur **OK**.

- Public : Le jour férié sera partagé avec tous vos plans de vacances.
- Personnalisé : Le congé n'est utilisé que pour le plan de congé en cours.

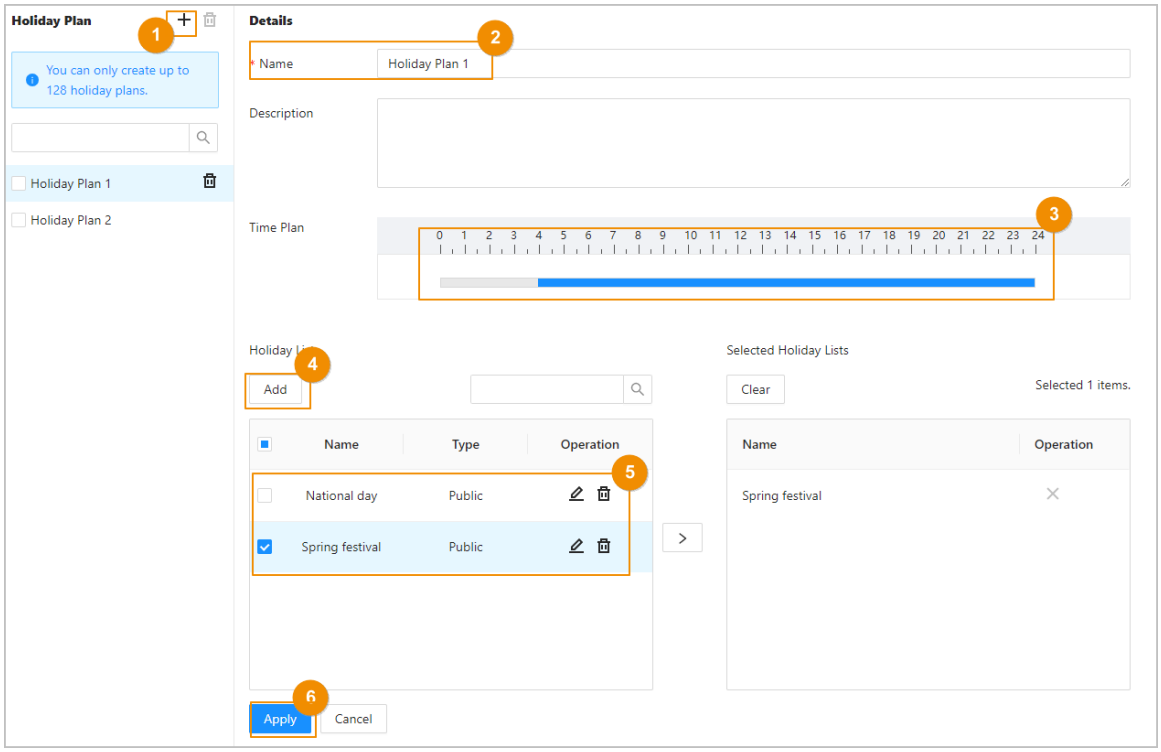
Figure 2-30 Ajout de congés



Étape 5 : Sélectionnez des congés.

Étape 6 : Cliquez sur **Appliquer** (Apply).

Figure 2-31 Créer un plan de congé



2.2.10 Ajout de zones

Un zone est un ensemble d'autorisations d'accès aux portes. Créez une zone, puis reliez les utilisateurs à cette zone afin qu'ils puissent obtenir les autorisations d'accès définies pour cette zone.

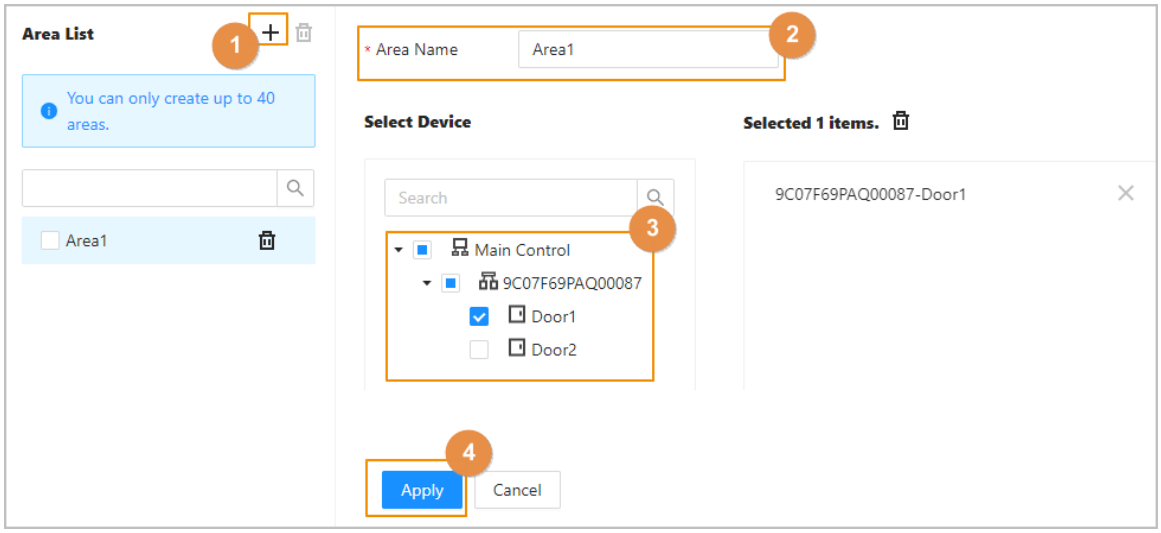
Procédure

Étape 1 : Cliquez sur **Config. du contrôle d'accès > Paramètres de zone** (Access Control Config > Area Settings).

Étape 2 : Cliquez sur + pour ajouter des zones.

Vous pouvez ajouter jusqu'à 40 autorisations de zone.

Figure 2-32 Ajout de zones



Étape 3 : Saisissez le nom de la zone.

Étape 4 : Sélectionnez les portes.

Étape 5 : Cliquez sur **Appliquer** (Apply).

2.2.11 Ajout des règles d'autorisation

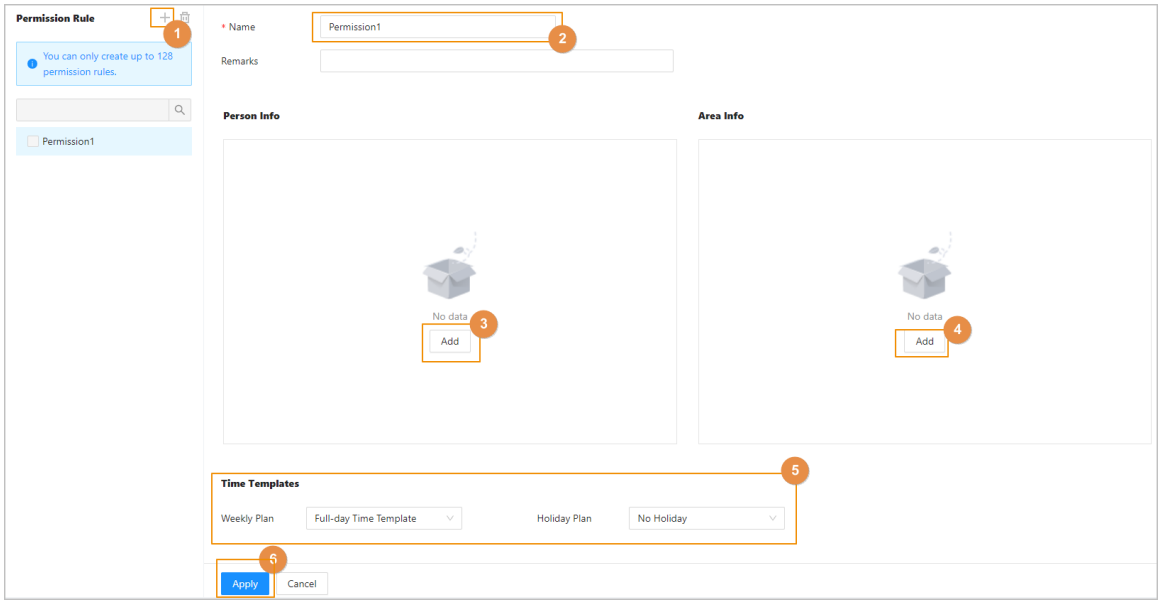
En créant des règles d'autorisation, vous pouvez attribuer des autorisations d'accès aux utilisateurs en les reliant aux zones. Cela permettra au personnel autorisé à des zones sécurisées.

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. du contrôle d'accès > Paramètres d'autorisation** (Access Control Config > Permission Settings).

Étape 2 : Cliquez sur + pour ajouter une règle d'autorisation.

Figure 2-33 Attribution d'autorisations par lots



Étape 3 : Saisissez le nom de la règle d'autorisation.

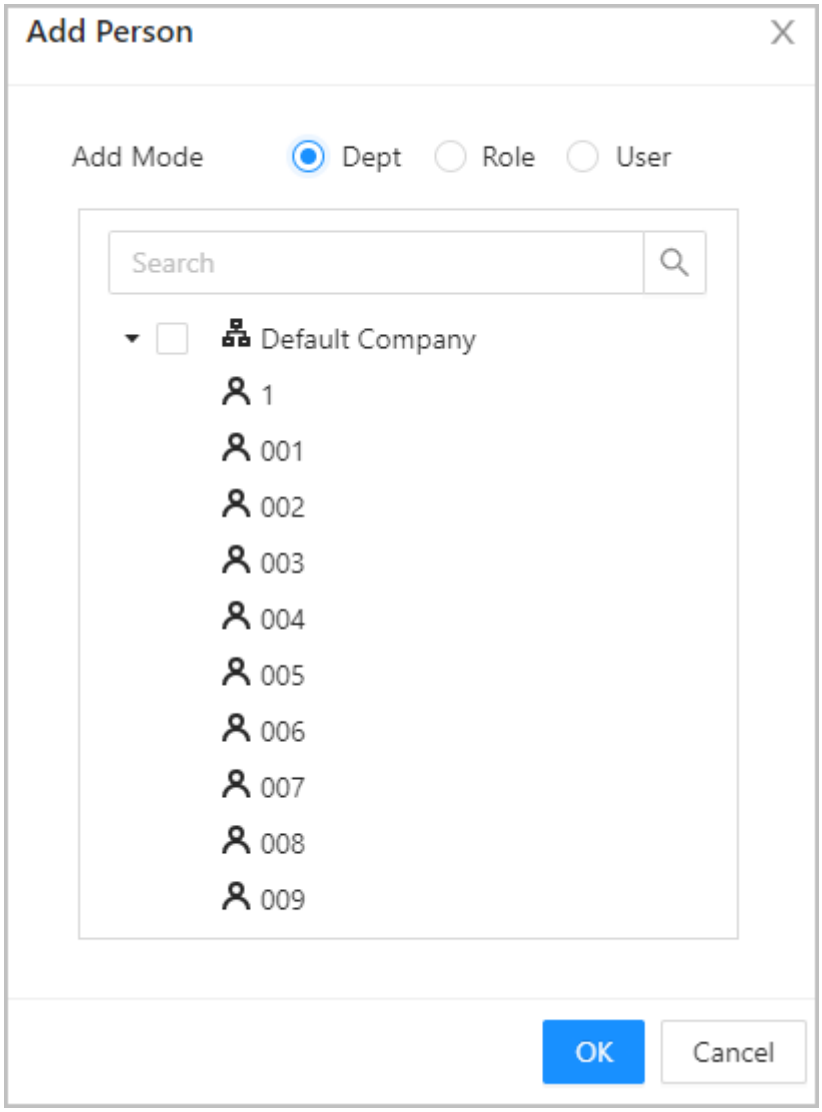
Étape 4 : Dans la zone **Infos personnelles** (Person Info), cliquez sur **Ajouter** (Add) pour sélectionner le personnel, puis cliquez sur **OK**.

Vous pouvez sélectionner le personnel dans le département, le rôle ou les utilisateurs individuels.

- Dépt. : Tous les membres du personnel du service se verront attribuer des autorisations d'accès.
- Rôle : Tous les membres du personnel ayant ces rôles se verront attribuer des autorisations d'accès.
- Utilisateur (User) : Seuls les utilisateurs sélectionnés se verront attribuer des autorisations d'accès.

Lorsque vous souhaitez attribuer une autorisation à une nouvelle personne ou modifier les autorisations d'accès d'une personne existante, vous pouvez simplement ajouter l'utilisateur dans un département existant ou le lier à un rôle existant, il se verra automatiquement attribuer les autorisations d'accès définies pour le département ou le rôle.

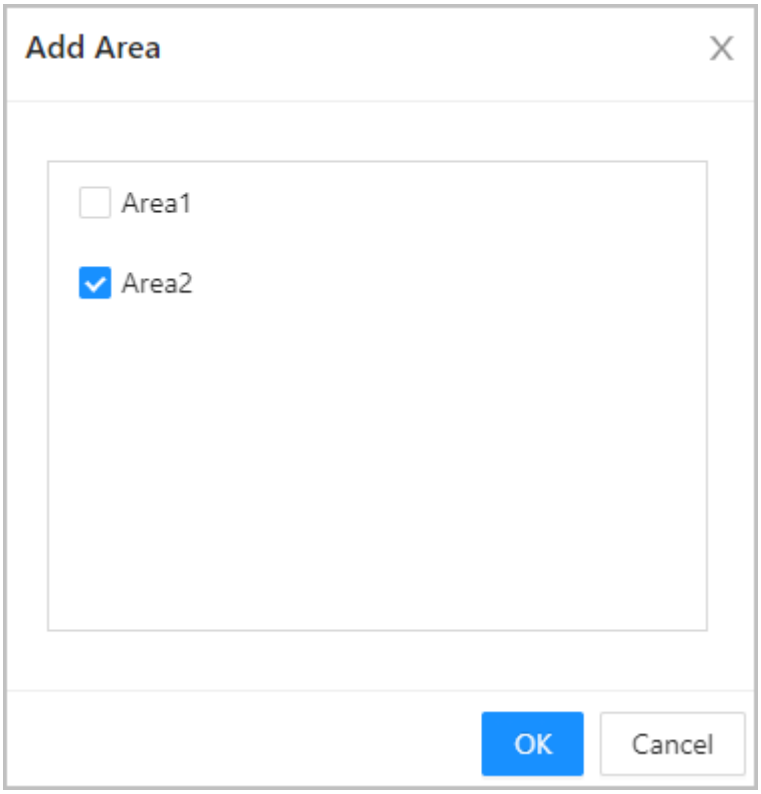
Figure 2-34 Ajout de membres du personnel



Vous pouvez cliquer sur + pour créer de nouveaux groupes d'autorisations. Pour plus de détails sur la création de groupes d'autorisation, reportez-vous à « 2.2.10 Ajout de zones ».

Étape 5 : Dans **Infos sur la zone** (Area Info), cliquez sur **Ajouter** (Add) pour sélectionner une zone, puis cliquez sur **OK**.

Figure 2-35 Ajout de zone



Étape 6 : Dans la zone **Modèles horaires** (Time Templates), sélectionnez le plan hebdomadaire et le plan de congé.

Étape 7 : Cliquez sur **Appliquer** (Apply).

Opérations connexes

2.2.12 Affichage de la progression des autorisations

Après avoir attribué des autorisations d'accès aux utilisateurs, vous pouvez afficher le processus d'autorisation.

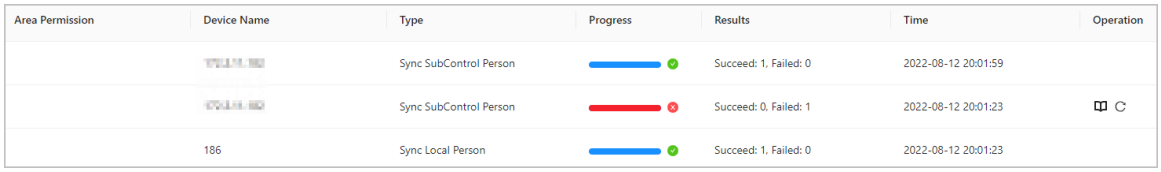
Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. du contrôle d'accès > Progression de l'autorisation** (Access Control Config > Authorization Progress).

Étape 2 : Affichez la progression de l'autorisation.

- Synchro. le personnel du contrôleur principal : Synchronisez le personnel du contrôleur principal avec celui du sous-contrôleur.
- Synchro. le personnel local : Synchronisez le personnel de la plateforme de gestion du contrôleur principal avec son serveur.
- Synchro. l'heure locale : Synchronisez les modèles horaires des autorisations de zone avec le sous-contrôleur.

Figure 2-36 Progression de l'autorisation



Étape 3 : (En option) Si l'autorisation a échoué, cliquez sur pour réessayer.
Vous pouvez cliquer sur pour afficher les détails de la tâche d'autorisation qui a échoué.

2.2.13 Configuration du contrôle d'accès (en option)

2.2.13.1 Configuration des paramètres de base

Procédure

Étape 1 : Sélectionnez **Config. du contrôle d'accès > Paramètres de porte** (Access Control Config > Door Parameters).

Étape 2 : Dans **Paramètres de base** (Basic Settings), configurez les paramètres de base du contrôle d'accès.

Figure 2-37 Paramètres de base

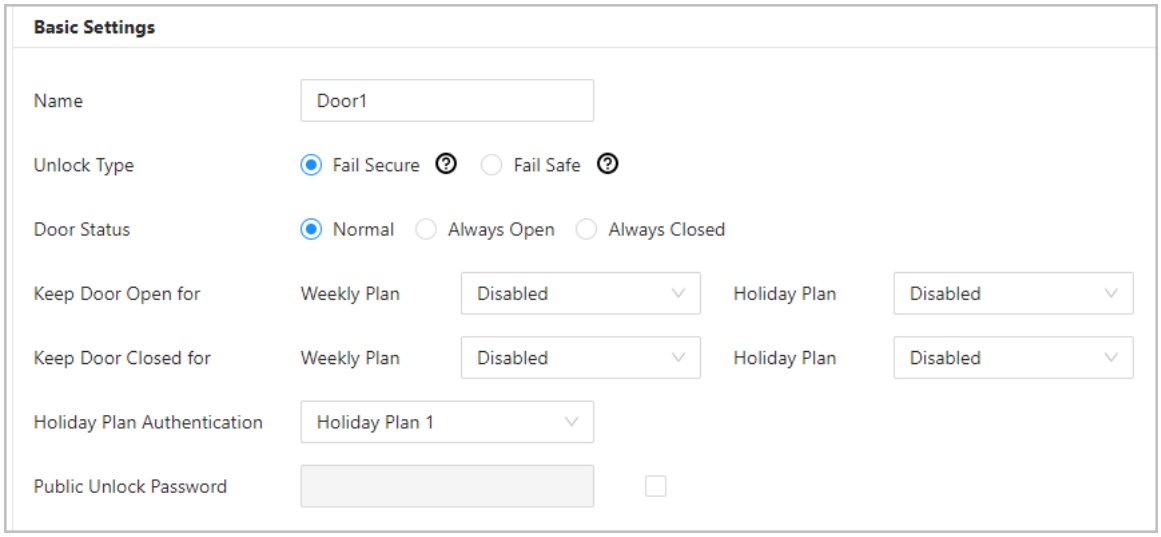


Tableau 2-8 Description des paramètres de base

Paramètre	Description
Nom	Nom de l'appareil.

Paramètre	Description
Type de déverr.	● Si vous avez sélectionné **12 V** pour alimenter la serrure via le contrôleur au cours de l'assistant de connexion, vous pouvez définir Sécurité à émission ou Sécurité à rupture. ◇ Sécurité à émission : En cas de coupure de courant ou de panne, la porte reste verrouillée. ◇ Sécurité à rupture : En cas de coupure de courant ou de panne, la porte se déverrouille automatiquement pour permettre aux personnes de sortir. ● Si vous avez sélectionné **Relai** (Relay) pour alimenter la serrure via le relai au cours de l'assistant de connexion, vous pouvez définir Relais ouvert ou Relais fermé. ◇ Relais ouvert = verrouillé : Règle la serrure pour qu'elle reste verrouillée lors de l'ouverture du relais. ◇ Relais ouvert = déverrouillé : Règle la serrure pour qu'elle se déverrouille lors de l'ouverture du relais.
Statut de porte	Définissez l'état de la porte. ● **Normal :** La porte sera déverrouillée et verrouillée en fonction de vos paramètres. ● **Toujours ouvert :** La porte reste déverrouillée en permanence. ● **Toujours fermé :** La porte reste verrouillée en permanence.
Garder la porte ouverte pour	La porte reste ouverte pendant le plan hebdomadaire ou le plan de congé défini.
Garder la porte fermée pour	La porte reste fermée pendant le plan hebdomadaire ou le plan de congé défini.
Authentification du plan de congé	Un accès autorisé est permis pour la porte toujours fermée dans le plan de congé défini.
Période de fermeture normale	Lorsque vous sélectionnez **Normal**, vous pouvez sélectionner un modèle horaire dans la liste déroulante. La porte reste ouverte ou fermée pendant la période définie.
Mot de passe de déverrouillage public	Activez cette fonction, puis entrez un mot de passe. Vous pouvez alors déverrouiller la porte en entrant uniquement le mot de passe public.

2.2.13.2 Configuration des méthodes de déverrouillage

Vous pouvez utiliser plusieurs méthodes de déverrouillage pour déverrouiller la porte, telles que la carte Bluetooth, l'empreinte digitale, la carte et le mot de passe. Vous pouvez également les combiner pour créer votre propre méthode de déverrouillage.

Procédure

Étape 1 : Sélectionnez **Config. du contrôle d'accès > Paramètres de porte** (Access Control Config > Door Parameters).

Étape 2 : Dans **Paramètres de déverrouillage** (Unlock Settings), sélectionnez un mode de

déverrouillage.

- Déverrouillage par combinaison
  1. Sélectionnez **Déverrouillage par combinaison** (Combination Unlock) dans la liste **Mode de déverrouillage** (Unlock Mode).
  2. Sélectionnez **Ou** (Or) ou **Et** (And).
     - Ou : Utilisez l'une des méthodes de déverrouillage sélectionnées pour ouvrir la porte.
     - Et : Utilisez toutes les méthodes de déverrouillage sélectionnées pour ouvrir la porte.

     La carte Bluetooth ne peut pas être sélectionnée lorsque le procédé de combinaison est réglée sur **Et** (And).
  3. Sélectionnez les méthodes de déverrouillage, puis configurez les autres paramètres.

Figure 2-38 Paramètres de déverrouillage

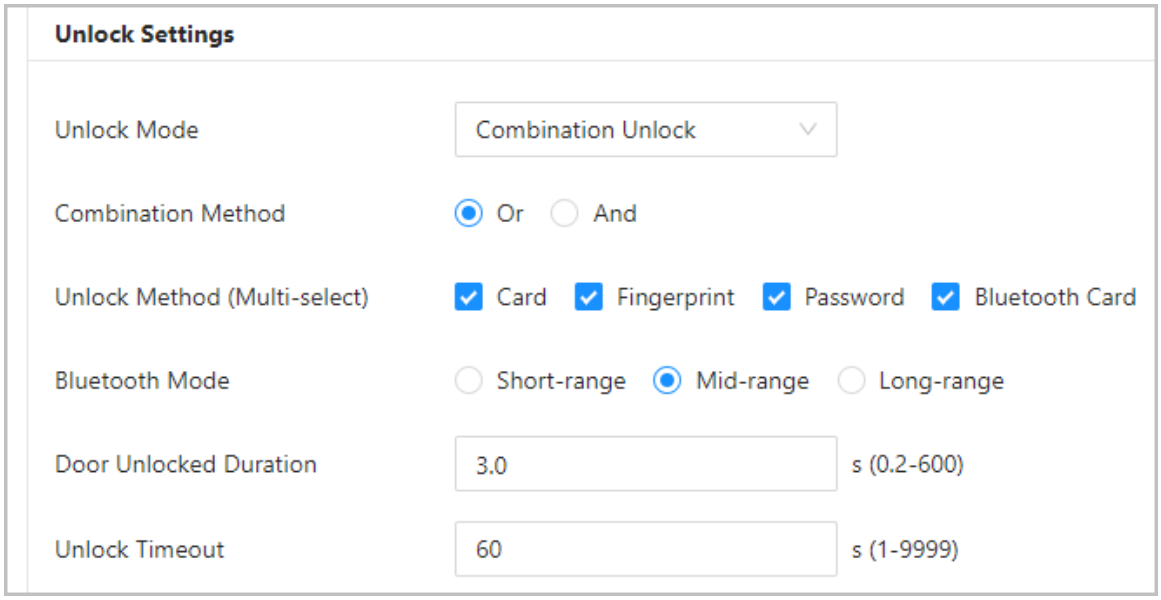


Tableau 2-9 Description des paramètres de déverrouillage

Paramètre	Description
Méthode de déverrouillage (multi-sélection)	Prend en charge le déverrouillage par carte, empreinte digitale, mot de passe ou carte Bluetooth. La fonction de carte Bluetooth est désactivée par défaut.

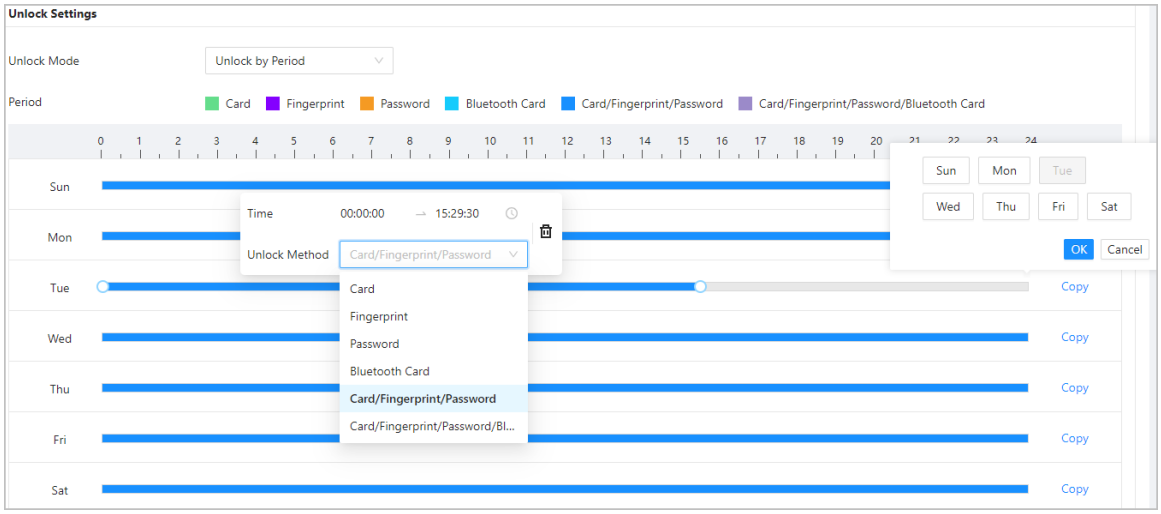
Paramètre	Description
Mode Bluetooth	La carte Bluetooth doit se trouver à une certaine distance du dispositif de contrôle d'accès pour échanger des données et déverrouiller la porte. Les plages suivantes sont les plus appropriées. ● Courte portée : La portée de déverrouillage Bluetooth est inférieure à 0,2 m. ● Moyenne portée : La portée de déverrouillage Bluetooth est inférieure à 2 m. ● Longue portée : La portée de déverrouillage Bluetooth est inférieure à 10 m. ⚠ La portée de déverrouillage Bluetooth peut varier en fonction des modèles de votre téléphone et de l'environnement.
Durée de déverr. de la porte	Une fois qu'une personne a obtenu l'autorisation d'accès, la porte reste déverrouillée pendant une durée définie pour lui permettre de passer. La valeur de la durée varie de 0,2 à 600 secondes.
Temporisation de déverrouillage	Une alarme de temporisation se déclenche lorsque la porte reste déverrouillée pendant une durée supérieure à la valeur définie.

- Débloquer par période
  1. Dans la liste **Mode de déverrouillage** (Unlock Mode), sélectionnez **Débloquer par période** (Unlock by Period).
  2. Faites glisser le curseur pour ajuster la période de temps pour chaque jour.

     Vous pouvez également cliquer sur **Copier** (Copy) pour appliquer la période configurée à d'autres jours.
  3. Sélectionnez une méthode de déverrouillage pour la période, puis configurez d'autres paramètres.

Vous pouvez configurer jusqu'à 4 tranches horaires par jour.

Figure 2-39 Déverrouillage par période



Étape 3 : Cliquez sur **Appliquer** (Apply).

2.2.13.3 Configuration des alarmes

Une alarme est déclenchée en cas d'accès anormal.

Procédure

Étape 1 : Sélectionnez **Config. du contrôle d'accès > Paramètres de porte > Paramètres d'alarme** (Access Control Config > Door Parameters > Alarm Settings).

Étape 2 : Configurez les paramètres d'alarme.

Figure 2-40 Alarme

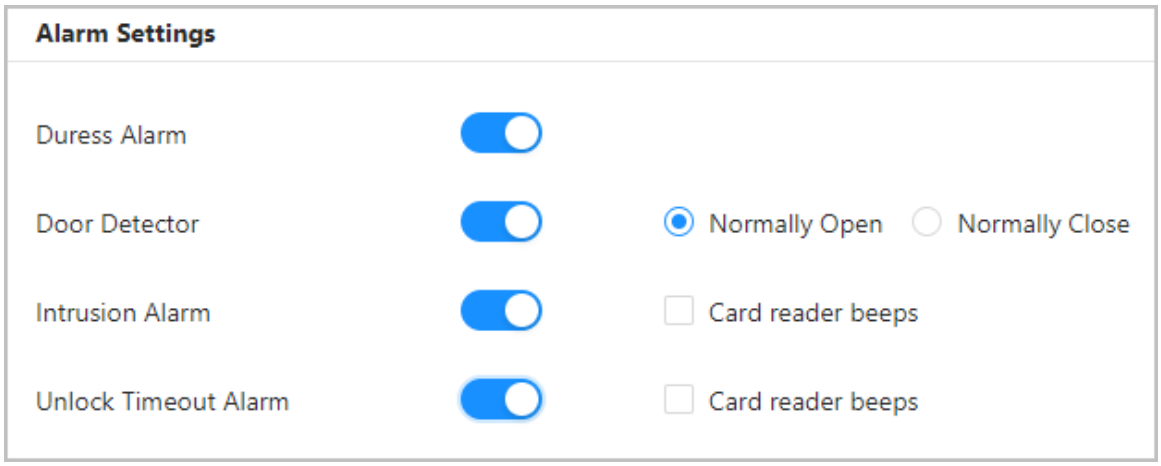


Tableau 2-10 Description des paramètres d'arlame

Paramètre	Description
Alarme de contrainte	Une alarme est déclenchée lorsqu'une carte de contrainte, un mot de passe de contrainte ou une empreinte digitale de contrainte est utilisé pour déverrouiller la porte.

Paramètre	Description
Détecteur de porte	Sélectionnez le type de détecteur de porte.
Alarme d'intrusion	• Lorsque le détecteur de porte est activé, une alarme d'intrusion est déclenchée en cas d'ouverture anormale de la porte. • Une alarme de temporisation se déclenche lorsque la porte reste déverrouillée plus longtemps que le temps de déverrouillage défini. • Lorsque l'option **Bips du lecteur de carte** (Card reader beeps) est activée, le lecteur de carte émet un bip lorsque l'alarme d'intrusion ou l'alarme de temporisation est déclenchée.
Alarme de temporisation de déverrouillage	

Étape 3 : Cliquez sur **Appliquer** (Apply).

2.2.14 Configuration du déverrouillage par mot de passe

Lorsque l'authentification par code PIN est activée, les personnes peuvent déverrouiller la porte en entrant simplement le mot de passe.

Préambule

- Si l'authentification par code PIN n'est pas activée, vous pouvez déverrouiller la porte en saisissant le mot de passe de déverrouillage au format **ID utilisateur#mot de passe#** (user ID#password#). Par exemple, si l'ID utilisateur est 123 et que le mot de passe défini est 12345, vous devez saisir **123#12345#** pour déverrouiller la porte.
- Si l'authentification par code PIN est activée, vous pouvez déverrouiller la porte en saisissant le mot de passe de déverrouillage au format **mot de passe#** (password#). Par exemple, si l'ID utilisateur est 123 et que le mot de passe défini est 12345, vous devez saisir **12345#** pour déverrouiller la porte.

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. du contrôle d'accès > Config. de la méthode de déverrouillage** (Access Control Config > Unlock Method Config).

Étape 2 : Activez **Authentification par code PIN** (PIN Code Authentication), puis cliquez sur **Appliquer** (Apply).

L'activation de l'authentification par code PIN présente certains risques pour la sécurité. Lorsqu'elle est activée, les types d'utilisateurs et les rôles deviennent inefficaces et les situations suivantes se produisent.

- Les détenteurs de la première carte et les utilisateurs des groupes de déverrouillage multi-personnes doivent vérifier leur identité à l'aide des méthodes de déverrouillage définies, à l'exception du mot de passe. S'ils vérifient leur identité à l'aide d'un mot de passe, la fonction de déverrouillage par la première carte ou de déverrouillage multi-personnes devient inefficace.
- Les utilisateurs doivent vérifier leur identité au moyen des méthodes de déverrouillage définies, à l'exception du mot de passe. S'ils obtiennent l'accès par mot de passe, la fonction antiretour devient inefficace.
- Les utilisateurs patrouilleurs et les utilisateurs inscrits sur une liste de blocage peuvent simplement saisir leur mot de passe pour déverrouiller la porte.
- Les comptes gelés et expirés peuvent toujours déverrouiller les portes en entrant simplement leur mot de passe.
- Lorsque la méthode de déverrouillage par mot de passe est désactivée simultanément, tous les types d'utilisateurs ne peuvent pas déverrouiller la porte à l'aide de leur mot de passe.

2.2.15 Configuration des liaisons d'alarme globales (en option)

Vous pouvez configurer des liaisons d'alarme globales entre différents contrôleurs d'accès.

Procédure

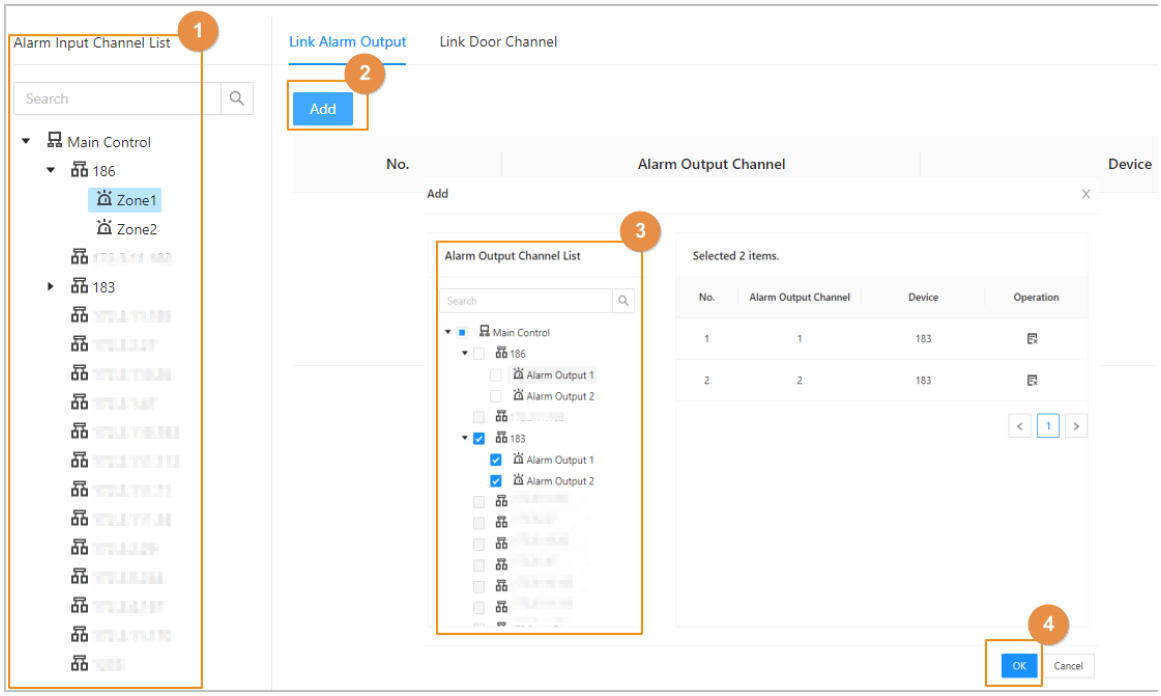
Étape 1 : Sélectionnez **Config. du contrôle d'accès > Liaison d'alarme globale** (Access Control Config > Global Alarm Linkage).

- Lorsque vous avez configuré des liaisons d'alarme globales et des liaisons d'alarme locales, et si les liaisons d'alarme globales entrent en conflit avec les liaisons d'alarme locales, les dernières liaisons d'alarme que vous avez configurées prendront effet.
- Lorsque vous avez configuré des liaisons d'alarme pour les sous-contrôleurs via le contrôleur principal, si le contrôleur principal a été restauré aux valeurs par défaut d'usine, nous vous recommandons de restaurer les valeurs par défaut d'usine des sous-contrôleurs en même temps.

Étape 2 : Configurez la sortie d'alarme.

1. Sélectionnez une entrée d'alarme dans la liste des canaux d'entrée d'alarme, puis cliquez sur **Sortie d'alarme de liaison** (Link Alarm Output).
2. Cliquez sur **Ajouter** (Add), sélectionnez un canal de sortie d'alarme, puis cliquez sur **OK**.

Figure 2-41 Sortie d'alarme

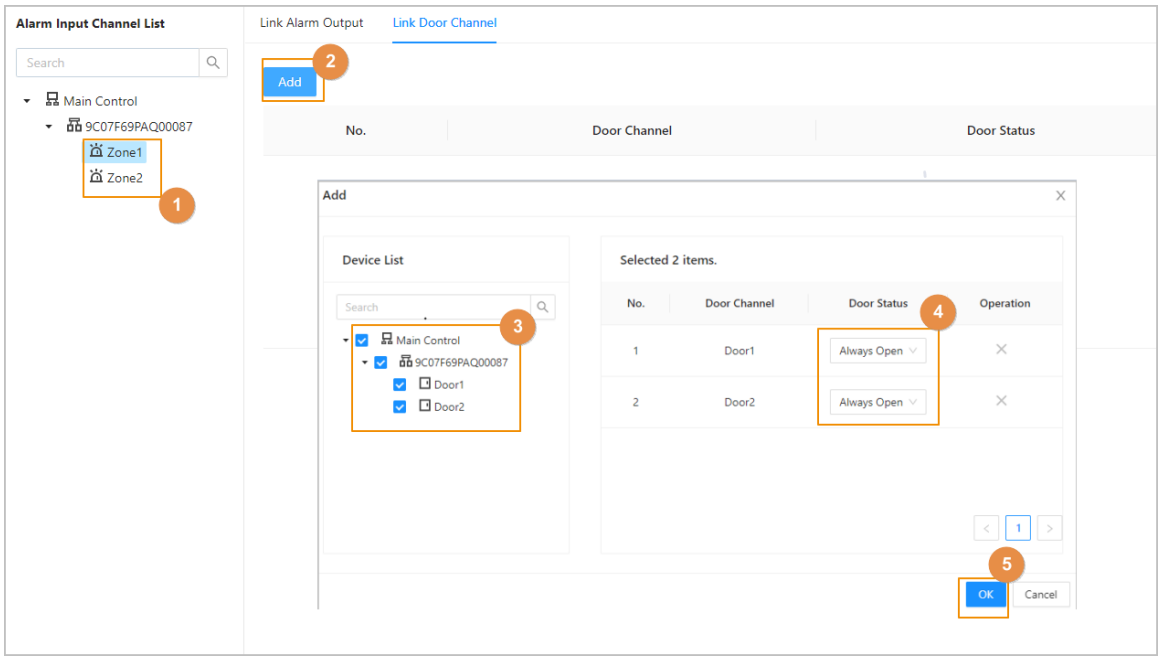


3. Activez la fonction de sortie d'alarme et entrez la durée de l'alarme.
4. Cliquez sur **Appliquer** (Apply).

Étape 3 : Configurez la liaison de porte.

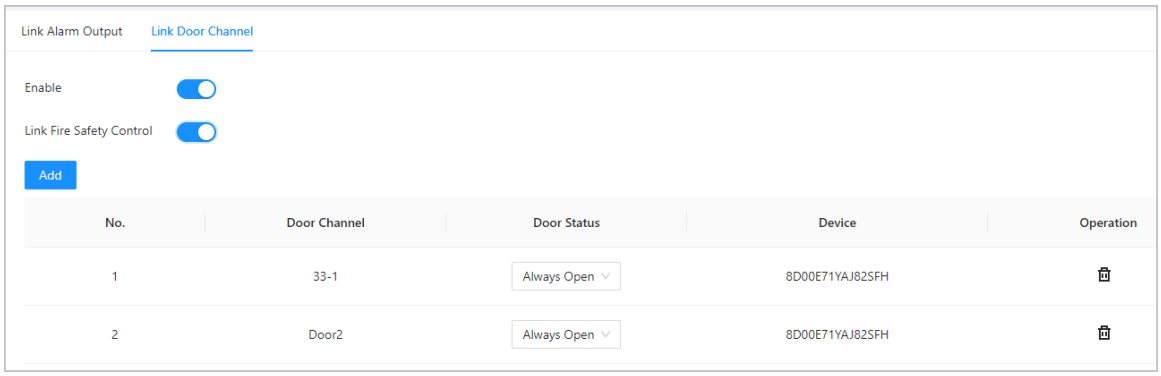
1. Sélectionnez une entrée d'alarme dans la liste de canaux, puis cliquez sur **Ajouter** (Add).
2. Sélectionnez la porte de liaison, puis sélectionnez l'état de la porte et cliquez sur **OK**.
   - Toujours fermé : La porte se verrouille automatiquement lorsqu'une alarme est déclenchée.
   - Toujours ouvert : La porte se déverrouille automatiquement lorsqu'une alarme est déclenchée.

Figure 2-42 Liaison de porte



3. Cliquez sur **Activer** (Enable) pour activer la fonction de liaison de porte.

Figure 2-43 Liaison de porte



Si vous activez la liaison de contrôle de sécurité incendie, toutes les liaisons de porte passeront automatiquement à l'état **Toujours ouvert** et toutes les portes s'ouvriront lorsque l'alarme incendie sera déclenchée.

4. Cliquez sur **Appliquer** (Apply).
   Vous pouvez cliquer sur **Copier vers** (Copy to) pour appliquer les liaisons d'alarme préconfigurées à d'autres canaux d'entrée d'alarme.

2.2.16 Configuration du déverrouillage par la première carte

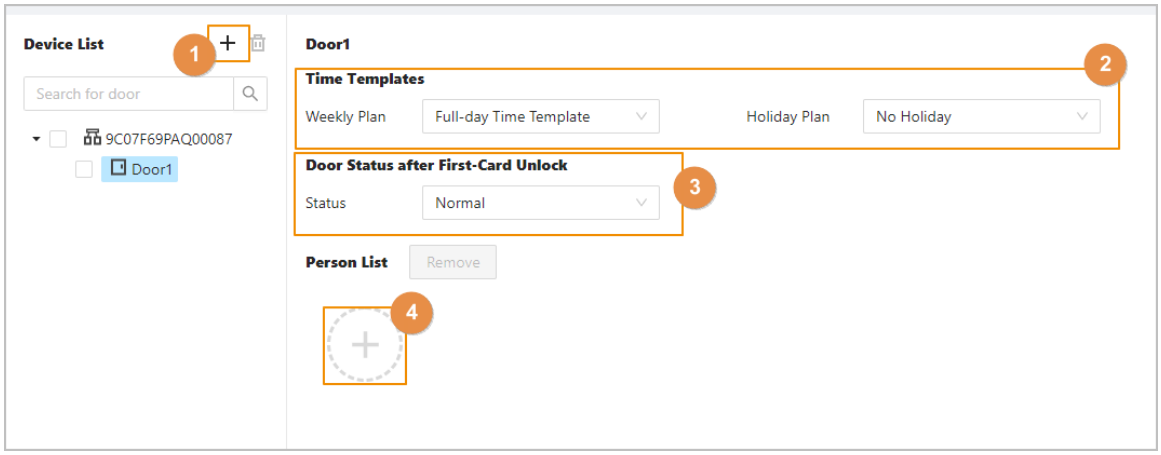
Définissez certaines personnes comme détenteur de la première carte, les autres utilisateurs peuvent vérifier leur identité pour déverrouiller la porte uniquement après que les détenteurs de la première carte ont vérifié leur identité.

Procédure

Étape 1 : Sélectionnez **Config. du contrôle d'accès > Déverrouillage par la première carte** (Access Control Config > First-card Unlock).

Étape 2 : Dans la liste des appareils, cliquez sur ＋, puis sélectionnez la porte.

Figure 2-44 Attribution d'une autorisation par la première carte aux utilisateurs



Étape 3 : Sélectionnez le plan hebdomadaire et le plan de congé.
La première carte n'est valable que pendant la période définie.

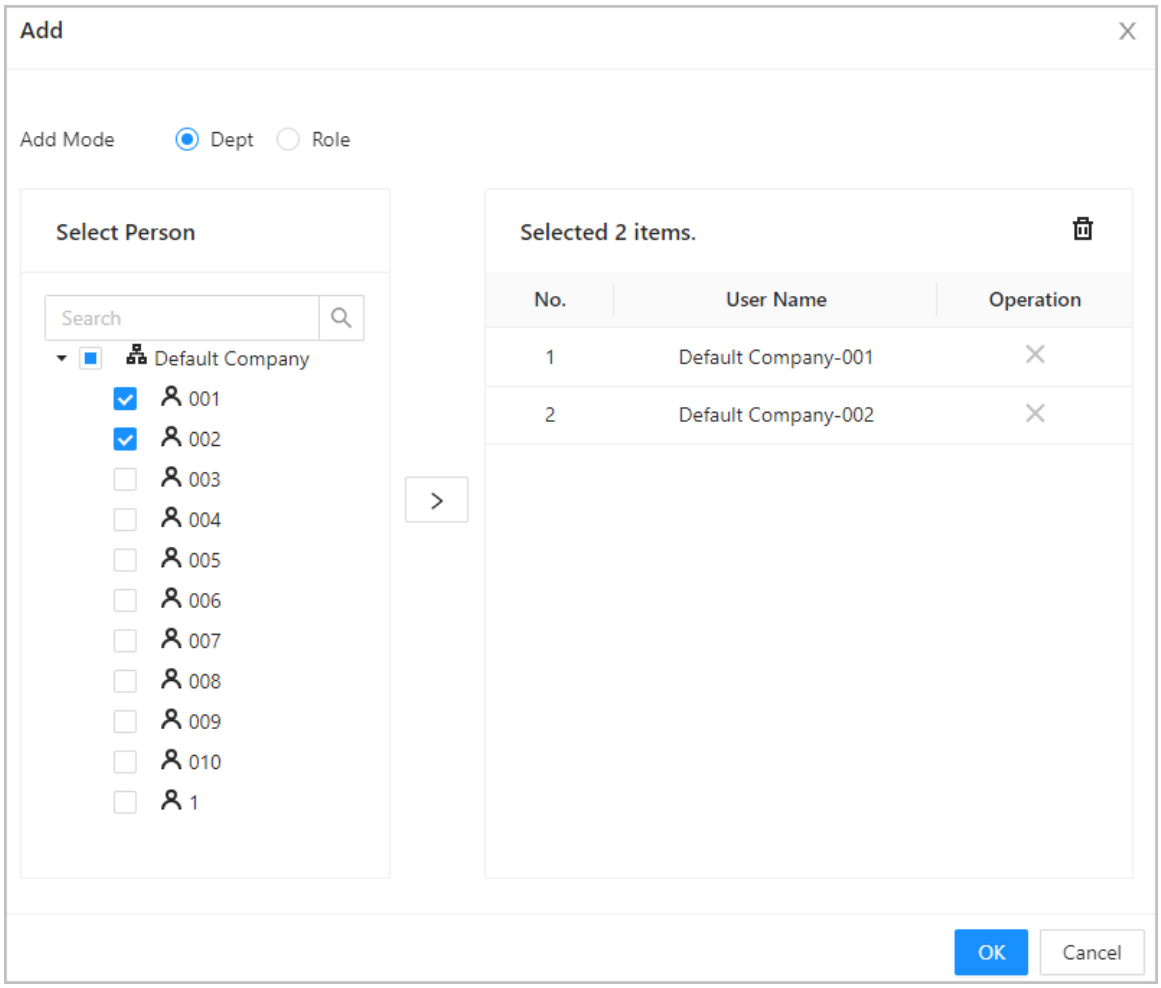
Étape 4 : Sélectionnez l'état de la porte.

- Normal : Les utilisateurs ne disposant pas d'une première carte doivent vérifier leur identité pour déverrouiller la porte après que les utilisateurs disposant d'une première carte ont accordé l'accès sur le contrôleur d'accès.
- Toujours ouvert : La porte reste ouverte après que les utilisateurs disposant d'une première carte ont accordé l'accès au contrôleur d'accès.

Étape 5 : Cliquez sur ⊕ pour ajouter des utilisateurs disposant d'une première carte, puis cliquez sur **OK**.

Vous pouvez sélectionner des utilisateurs à partir d'un département ou d'un rôle.

Figure 2-45 Ajout d'utilisateurs disposant d'une première carte



2.2.17 Configuration du déverrouillage multi-personnes

Les utilisateurs doivent vérifier leur identité sur le contrôleur d'accès dans un ordre établi avant que la porte ne se déverrouille.

Préambule

Nous vous déconseillons d'ajouter des utilisateurs disposant d'un première carte dans les groupes de déverrouillage multi-personnes.

Procédure

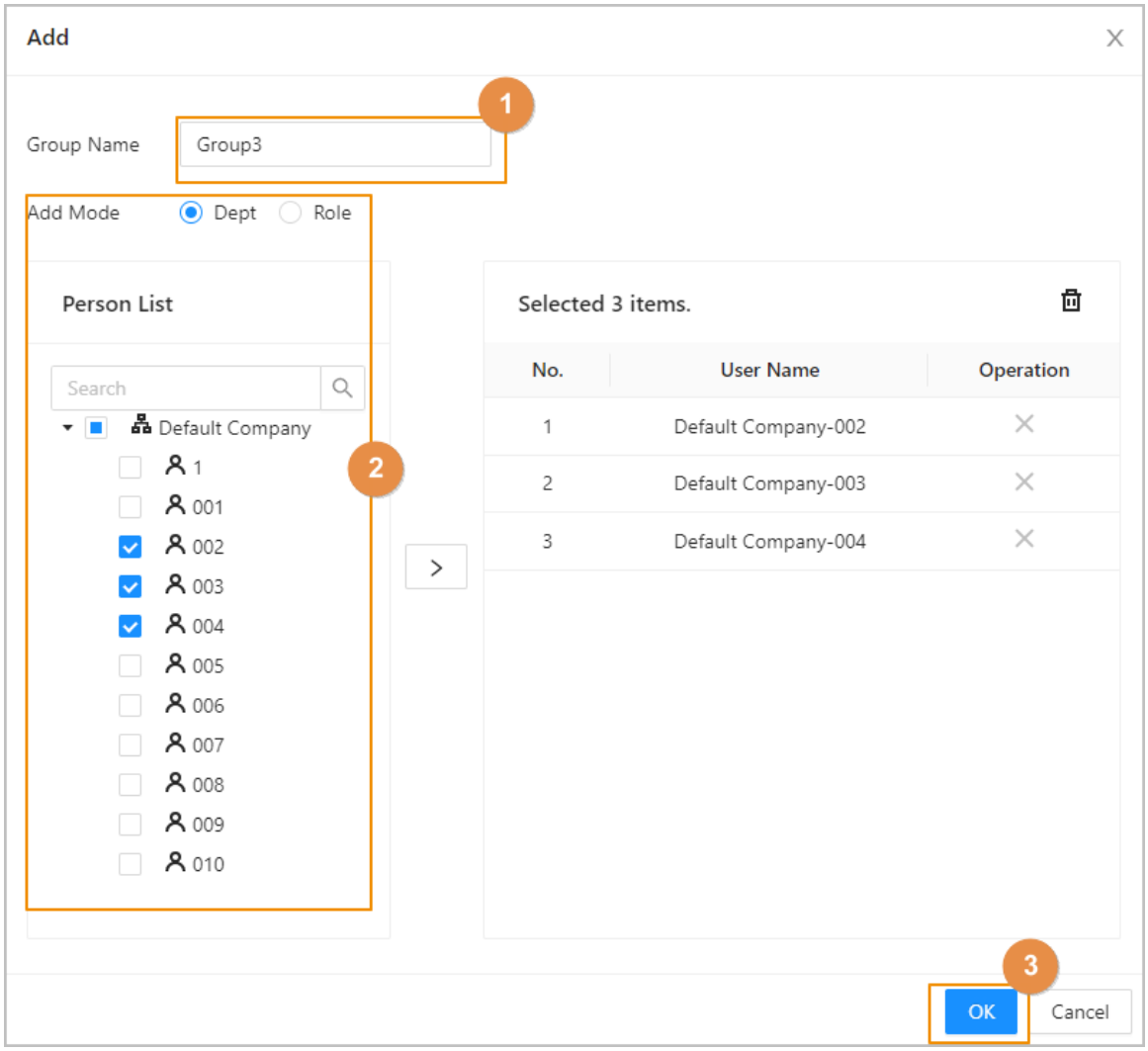
Étape 1 : Sélectionnez **Config. du contrôle d'accès > Déverrouillage multi-personnes** (Access Control Config > Multi-person Unlock).

Étape 2 : Cliquez sur + pour ajouter des portes à la liste des appareils.

Étape 3 : Cliquez sur **Person Group Management** (Person Group Management), puis sur **Ajouter** (Add) pour ajouter des groupes de déverrouillage multi-personnes.

1. Créez un nom de groupe.
2. Sélectionnez les utilisateurs à partir des départements ou des rôles.
3. Cliquez sur **OK**.

Figure 2-46 Ajout des groupes



Étape 4 : Sélectionnez une porte, puis cliquez sur **Ajouter des groupes de personnes** (Add Person Groups).

Étape 5 : Sélectionnez les groupes, puis cliquez sur **OK**.

Vous pouvez ajouter jusqu'à 4 groupes pour chaque porte. Chaque groupe peut contenir jusqu'à 50 utilisateurs.

Étape 6 : Configurez les paramètres du déverrouillage multi-personnes.

1. Entrez le numéro valide.

   Le numéro valide indique le nombre de personnes dans chaque groupe qui doivent vérifier leur identité sur le contrôleur d'accès avant que la porte ne se déverrouille. Par exemple, si le numéro valide est défini sur 2 pour un groupe, deux personnes du groupe doivent vérifier leur identité pour déverrouiller la porte.

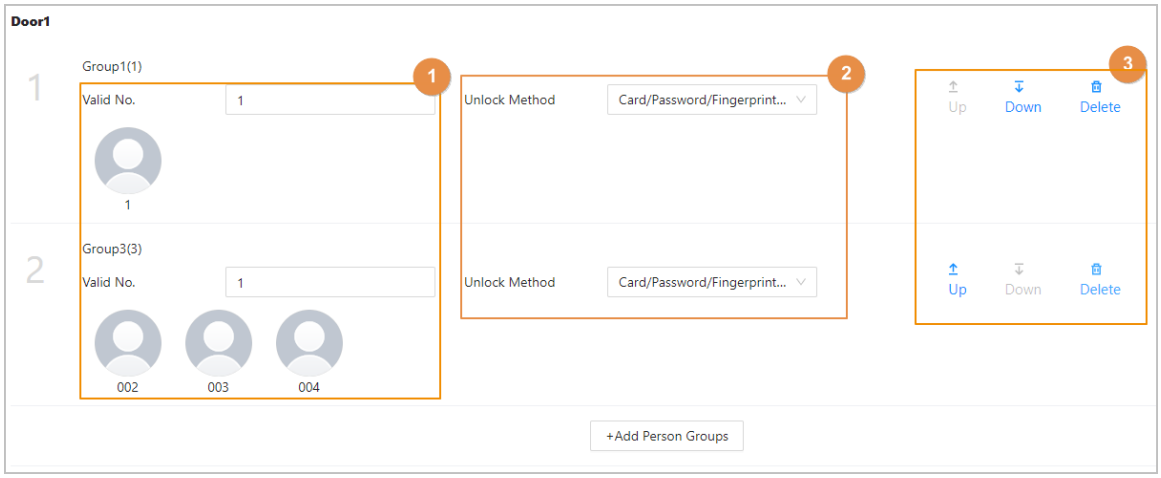
   Le nombre valide est compris entre 1 et 5 pour chaque groupe.

2. Sélectionnez la méthode de déverrouillage.

   Les utilisateurs du groupe doivent vérifier leur identité à l'aide des méthodes de déverrouillage définies.

3. (En option) Cliquez sur **Haut** (Up) ou **Bas** (Down) pour modifier l'ordre des groupes.
Si plusieurs groupes sont ajoutés, les utilisateurs doivent vérifier leur identité en fonction de l'ordre défini pour les groupes.

Figure 2-47 Configuration du déverrouillage multi-personnes



Étape 7 : Cliquez sur **Appliquer** (Apply).

2.2.18 Configuration de l'antiretour

Les utilisateurs doivent vérifier leur identité à l'entrée et à la sortie, sinon une alarme antiretour sera déclenchée. Elle empêche un détenteur de carte de repasser sa carte d'accès à une autre personne pour qu'elle puisse entrer. Lorsque l'alarme antiretour est activée, le détenteur de la carte doit quitter la zone sécurisée avant que le système ne lui accorde une autre entrée.

Préambule

- Si une personne entre après avoir été autorisée et ressort sans avoir été autorisée, une alarme se déclenche lorsqu'elle tente d'entrer à nouveau et que l'accès lui est refusé en même temps.
- Si une personne entre après avoir été autorisée et ressort après avoir été autorisée, une alarme se déclenche lorsqu'elle tente d'entrer à nouveau et l'accès lui est refusé en même temps.

- Lorsque vous avez configuré l'antiretour pour les sous-contrôleurs via le contrôleur principal et que vous prévoyez de restaurer les valeurs par défaut d'usine du contrôleur principal, nous vous recommandons de restaurer également les valeurs par défaut d'usine du sous-contrôleur en même temps.
- Si la règle antiretour est utilisée lorsque le réseau n'est pas stable, la porte peut s'ouvrir après vérification de l'identité, mais une alarme de temporisation peut être déclenchée sur le lecteur de carte. Veuillez vous assurer que votre réseau est stable.

Procédure

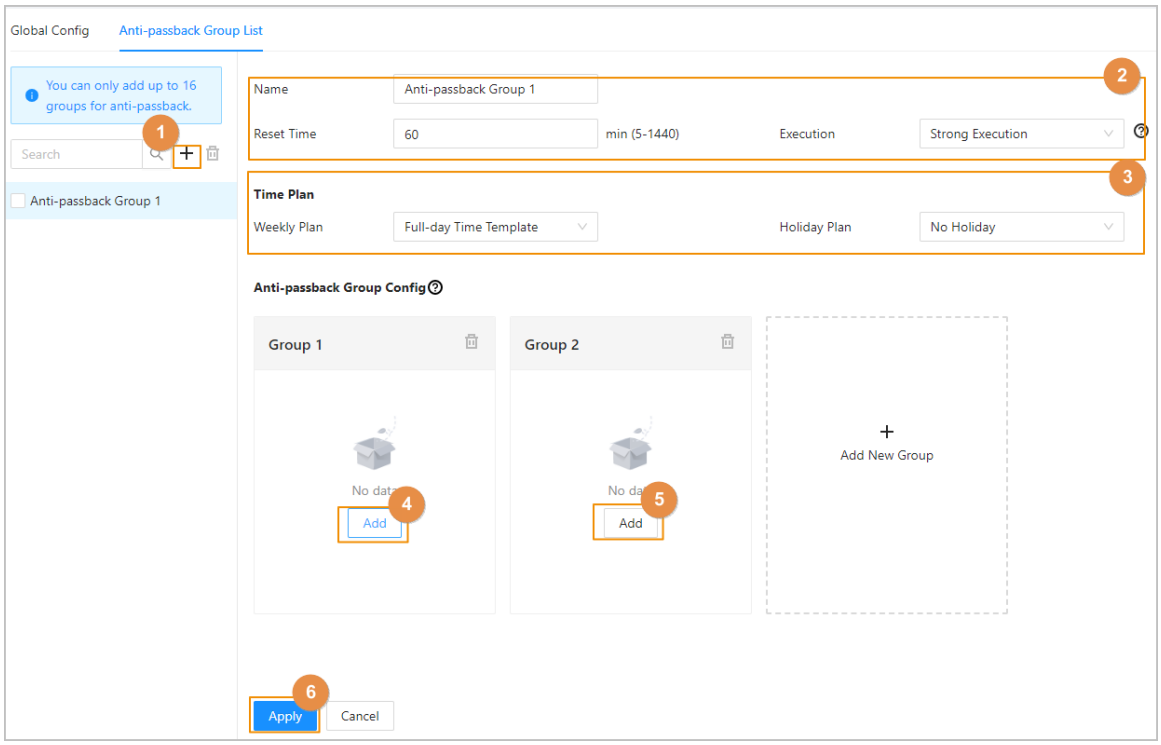
Étape 1 : Sélectionnez **Config. du contrôle d'accès > Antiretour global** (Access Control Config > Global Anti-passback).

Étape 2 : Activez la fonction **Réinitialiser l'antiretour** (Reset Anti-Passback), puis sélectionnez une heure de réinitialisation.

Spécifiez l'heure à laquelle le statut antiretour de l'ensemble du personnel sera réinitialisé.

Étape 3 : Cliquez sur **Liste des groupes d'antiretour** (Anti-passback Group List), puis sur + pour ajouter un groupe d'antiretour.

Figure 2-48 Configuration de l'antiretour



Étape 4 : Créez un nom pour le groupe d'antiretour, saisissez une heure de réinitialisation, puis sélectionnez le mode d'exécution.

Définissez une période de temps pendant laquelle l'alarme antiretour sera déclenchée. Par exemple, si l'heure de réinitialisation est fixée à 30 minutes, lorsqu'une personne entre après avoir été autorisée et sort sans avoir été autorisée, si elle tente d'entrer à nouveau dans les 30 minutes, une alarme antiretour se déclenche.

- Exécution solide : Le sous-contrôleur et le contrôleur principal exécutent la fonction antiretour même s'ils sont hors ligne.
- Faible exécution : Le sous-contrôleur et le contrôleur principal n'exécutent pas la fonction antiretour lorsqu'ils sont hors ligne.

Étape 5 : Sélectionnez le plan hebdomadaire et le plan de congé.

L'antiretour est efficace pendant la période définie.

Étape 6 : Dans le groupe 1, cliquez sur **Ajouter** (Add), puis sélectionnez les lecteurs de carte.

Étape 7 : Dans le groupe 2, cliquez sur **Ajouter** (Add), puis sélectionnez les lecteurs de carte.

Au moins 2 groupes doivent être ajoutés.

Étape 8 : (En option) vous pouvez cliquer sur **Ajouter nouveau groupe** (Add New Group) pour ajouter d'autres groupes.

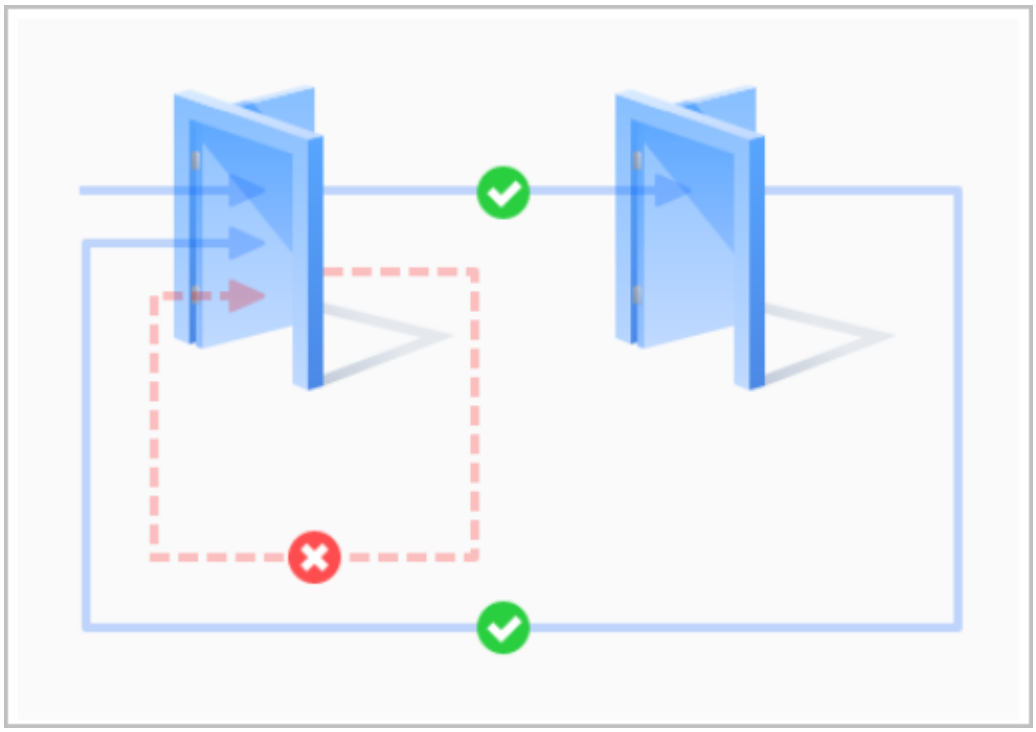
Vous pouvez ajouter plusieurs lecteurs dans un groupe, et les utilisateurs peuvent passer sur n'importe lequel des lecteurs pour obtenir l'accès.

Étape 9 : Cliquez sur **Appliquer** (Apply).

Résultat

Le numéro de groupe indique la séquence d'insertion des cartes. La carte doit être utilisée selon la séquence spécifique des groupes. Par exemple, vous devez passer la carte sur un lecteur du groupe 1, puis sur un lecteur du groupe 2, puis sur un lecteur du groupe 3, etc. Tant que vous passez la carte dans l'ordre établi, le système fonctionne correctement.

Figure 2-49 Fonction antiretour



2.2.19 Configuration du verrouillage multiporte

Le verrouillage multiporte contrôle le verrouillage de deux portes ou plus. Si une porte est déverrouillée, l'accès est interdit aux autres portes.

Préambule

- Lorsque vous avez configuré le verrouillage multiporte pour les sous-contrôleurs via le contrôleur principal et que vous prévoyez de restaurer les valeurs par défaut d'usine du contrôleur principal, nous vous recommandons de restaurer également les valeurs par défaut d'usine du sous-contrôleur en même temps.
- Si la règle de verrouillage multiporte est utilisée lorsque le réseau n'est pas stable, la porte peut s'ouvrir après vérification de l'identité, mais une alarme de temporisation peut être déclenchée sur le lecteur de carte. Veuillez vous assurer que votre réseau est stable.

2.2.19.1 Configuration du verrouillage au sein d'un groupe

Si une porte d'un groupe est ouverte, les autres portes du groupe ne peuvent pas être déverrouillées.

Procédure

Étape 1 : Sélectionnez **Config. du contrôle d'accès > Verrouillage multiporte global** (Access Control Config > Global Multi-door Interlock), puis cliquez sur **Verrouillage au sein d'un groupe** (Interlock within Group).

Étape 2 : Cliquez sur + , puis ajoutez un groupe de verrouillage.

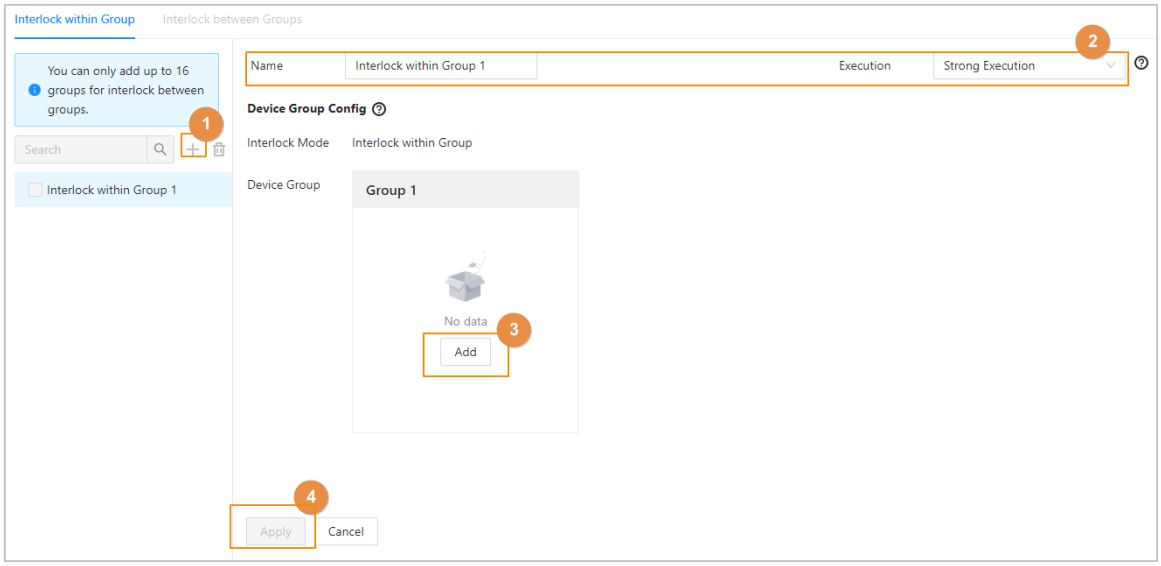
Étape 3 : Créez un nom pour le groupe de verrouillage, puis sélectionnez le mode d'exécution.

- Exécution solide : Le sous-contrôleur et le contrôleur principal exécutent la fonction de déverrouillage même s'ils sont hors ligne.
- Faible exécution : Le sous-contrôleur et le contrôleur principal n'exécutent pas la fonction de déverrouillage lorsqu'ils sont hors ligne.

Étape 4 : Cliquez sur **Ajouter** (Add) pour ajouter des portes à un groupe d'appareils.

Au moins 2 portes doivent être ajoutées à un groupe.

Figure 2-50 Verrouillage au sein d'un groupe



Étape 5 : Cliquez sur **Appliquer** (Apply).

Résultat

Une fois que l'identité d'une personne a été vérifiée et qu'elle a ouvert la porte, elle doit d'abord fermer la porte derrière elle avant de pouvoir ouvrir la porte suivante.

2.2.19.2 Configuration du verrouillage entre groupes

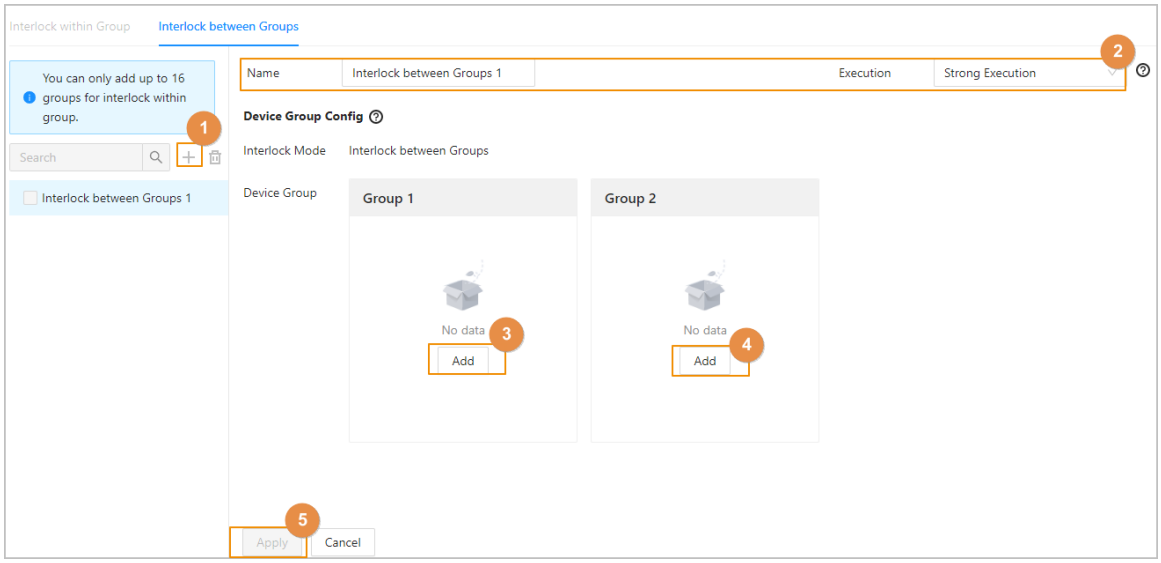
Si l'une des portes d'un groupe est déverrouillée, les portes des autres groupes ne peuvent pas s'ouvrir.

Procédure

Étape 1 : Sélectionnez **Config. du contrôle d'accès > Verrouillage multiporte global** (Access Control Config > Global Multi-door Interlock), puis cliquez sur **Verrouillage entre groupes** (Interlock between Groups).

Étape 2 : Cliquez sur ＋, puis ajoutez un groupe de verrouillage.

Figure 2-51 Verrouillage entre groupes



Étape 3 : Créez un nom pour le groupe de verrouillage, puis sélectionnez le mode d'exécution.

- Exécution solide : Le sous-contrôleur et le contrôleur principal exécutent la fonction de déverrouillage même s'ils sont hors ligne.
- Faible exécution : Le sous-contrôleur et le contrôleur principal n'exécutent pas la fonction de déverrouillage lorsqu'ils sont hors ligne.

Étape 4 : Dans le groupe 1, cliquez sur **Ajouter** (Add) pour ajouter des portes au groupe.

Étape 5 : Dans le groupe 2, cliquez sur **Ajouter** (Add) pour ajouter des portes au groupe.

Étape 6 : Cliquez sur **Appliquer** (Apply).

Résultat

Si l'une des portes d'un groupe est déverrouillée, les portes des autres groupes ne peuvent pas s'ouvrir.

2.2.20 Surveillance de l'accès (en option)

2.2.20.1 Ouverture et fermeture des portes à distance

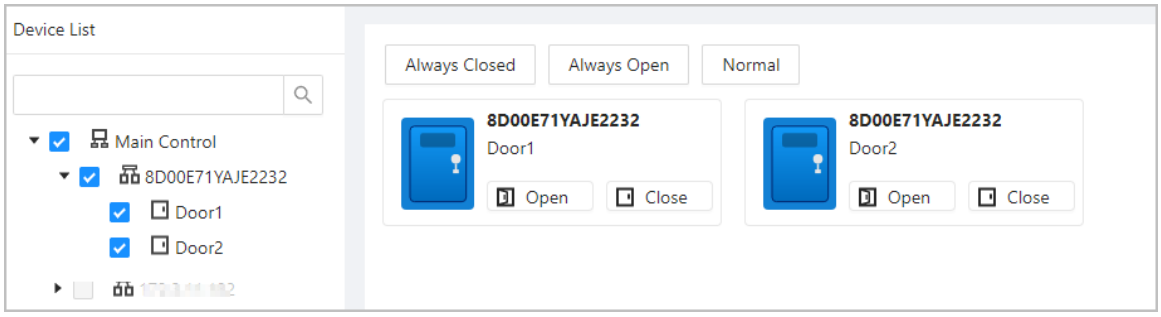
Vous pouvez surveiller et contrôler la porte à distance via la plateforme. Par exemple, vous pouvez ouvrir ou fermer la porte à distance.

Procédure

Étape 1 : Cliquez sur **Surveillance de l'accès** (Access Monitoring) sur la page d'accueil.

Étape 2 : Sélectionnez la porte, puis cliquez sur **Ouvrir** (Open) ou **Fermer** (Close) pour contrôler la porte à distance.

Figure 2-52 Contrôle à distance de la porte



Opérations connexes

- Filtrage d'événements : Sélectionnez le type d'événement dans **Info événement** (Event Info), et la liste des événements affiche les types d'événements sélectionnés, tels que les événements d'alarme et les événements anormaux.
- Suppression d'événement : Cliquez sur pour effacer tous les événements de la liste.

2.2.20.2 Réglage des options Toujours ouverte et Toujours fermée

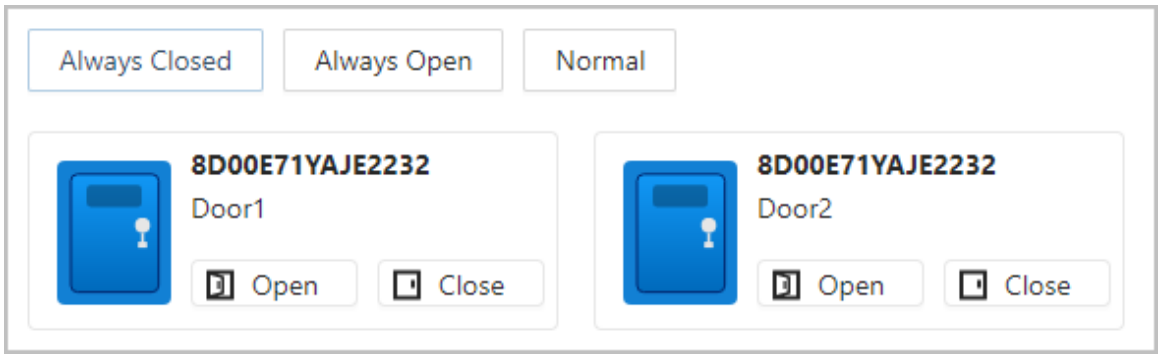
Après avoir défini l'option Toujours ouverte ou Toujours fermée, la porte reste ouverte ou fermée en permanence.

Procédure

Étape 1 : Cliquez sur **Surveillance de l'accès** (Access Monitoring) sur la page d'accueil.

Étape 2 : Cliquez sur **Toujours ouverte** (Always Open) ou **Toujours fermée** (Always Closed) pour ouvrir ou fermer la porte.

Figure 2-53 Toujours ouverte ou fermée



La porte reste ouverte ou fermée en permanence. Vous pouvez cliquer sur **Normal** pour rétablir l'état normal du contrôle d'accès, et la porte sera ouverte ou fermée en fonction des méthodes de vérification configurées.

2.2.21 Configurations des appareils locaux (en option)

Les configurations des appareils locaux ne peuvent être appliquées qu'aux contrôleurs d'accès locaux.

2.2.21.1 Configuration des liaisons d'alarme locales

Vous ne pouvez configurer les liaisons d'alarme locales que sur le même contrôleur d'accès. Chaque

contrôleur possède 2 entrées et 2 sorties d'alarme.

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. de l'appareil local > Liaison d'alarme locale** (Local Device Config > Local Alarm Linkage).

Étape 2 : Cliquez sur pour configurer la liaison d'alarme locale.

Figure 2-54 Liaison d'alarme locale

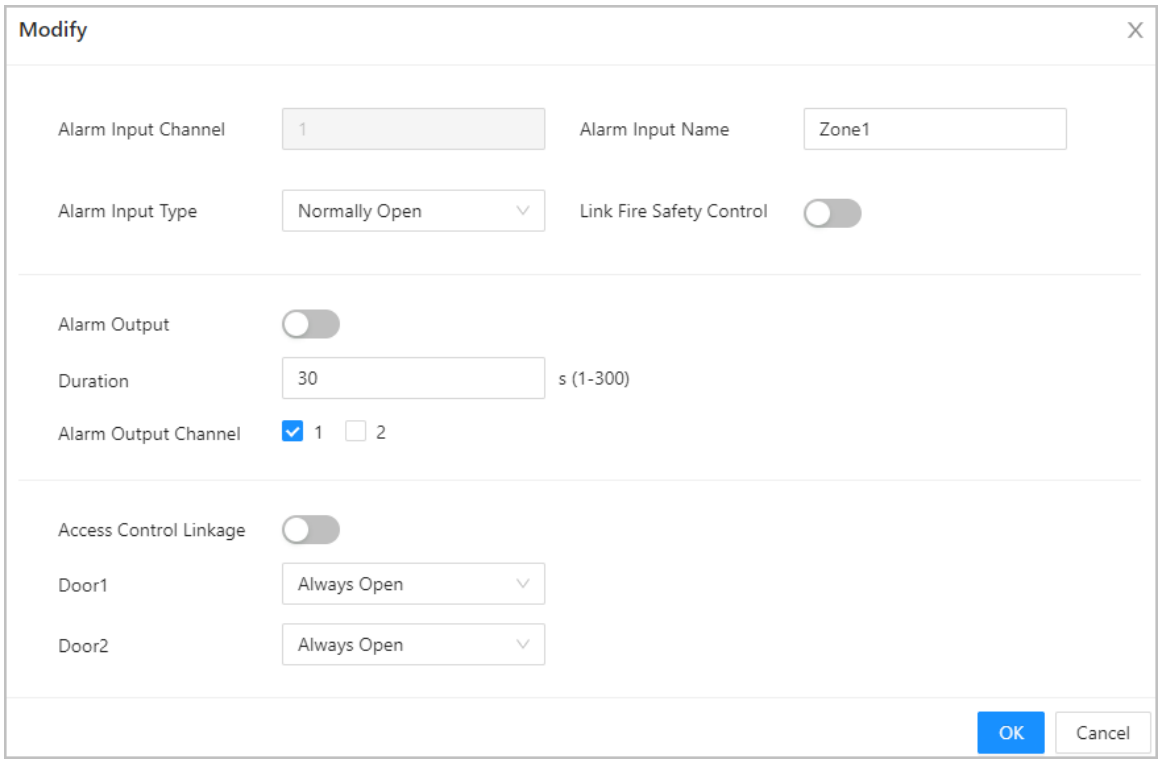


Tableau 2-11 Liaison d'alarme locale

Paramètre	Description
Canal d'entrée d'alarme	Numéro du canal d'entrée d'alarme. Chaque contrôleur possède 2 entrées et 2 sorties d'alarme.
Nom de l'entrée d'alarme	Nom de l'entrée d'alarme.
Type alarme entrée	Type d'entrée d'alarme. ● Normalement ouvert ● Normalement fermé
Liaison de contrôle de sécurité incendie	Si vous activez la liaison de contrôle de sécurité incendie, toutes les portes s'ouvriront lorsque l'alarme incendie sera déclenchée.
Sortie d'alarme	Vous pouvez activer la fonction de sortie d'alarme.
Durée	Lorsqu'une alarme est déclenchée, elle reste activée pendant une durée définie.
Canal de sortie alarme	Sélectionnez le canal de sortie. Chaque contrôleur possède 2 entrées et 2 sorties d'alarme.

Paramètre	Description
Associer le contrôle d'accès	Activez cette fonction pour configurer la liaison de porte.
Porte 1/Porte 2	Réglez la porte sur l'état toujours ouverte ou toujours fermée. Lorsqu'une alarme est déclenchée, la porte s'ouvre ou se ferme automatiquement.

Étape 3 : Cliquez sur **OK**.

2.2.21.2 Configuration des règles sur les cartes

La plateforme prend en charge 5 types de formats Wiegand par défaut. Vous pouvez également ajouter des formats Wiegand personnalisés.

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. de l'appareil local > Config. des règles sur la carte d'accès** (Local Device Config > Access Card Rule Config).

Étape 2 : Cliquez sur **Ajouter** (Add), puis configurez de nouveaux formats Wiegand.
Vous pouvez également cliquer sur **Ajouter un protocole** (Add Protocol) pour importer un fichier Wiegand sur la plateforme.

Figure 2-55 Ajout de nouveaux formats Wiegand

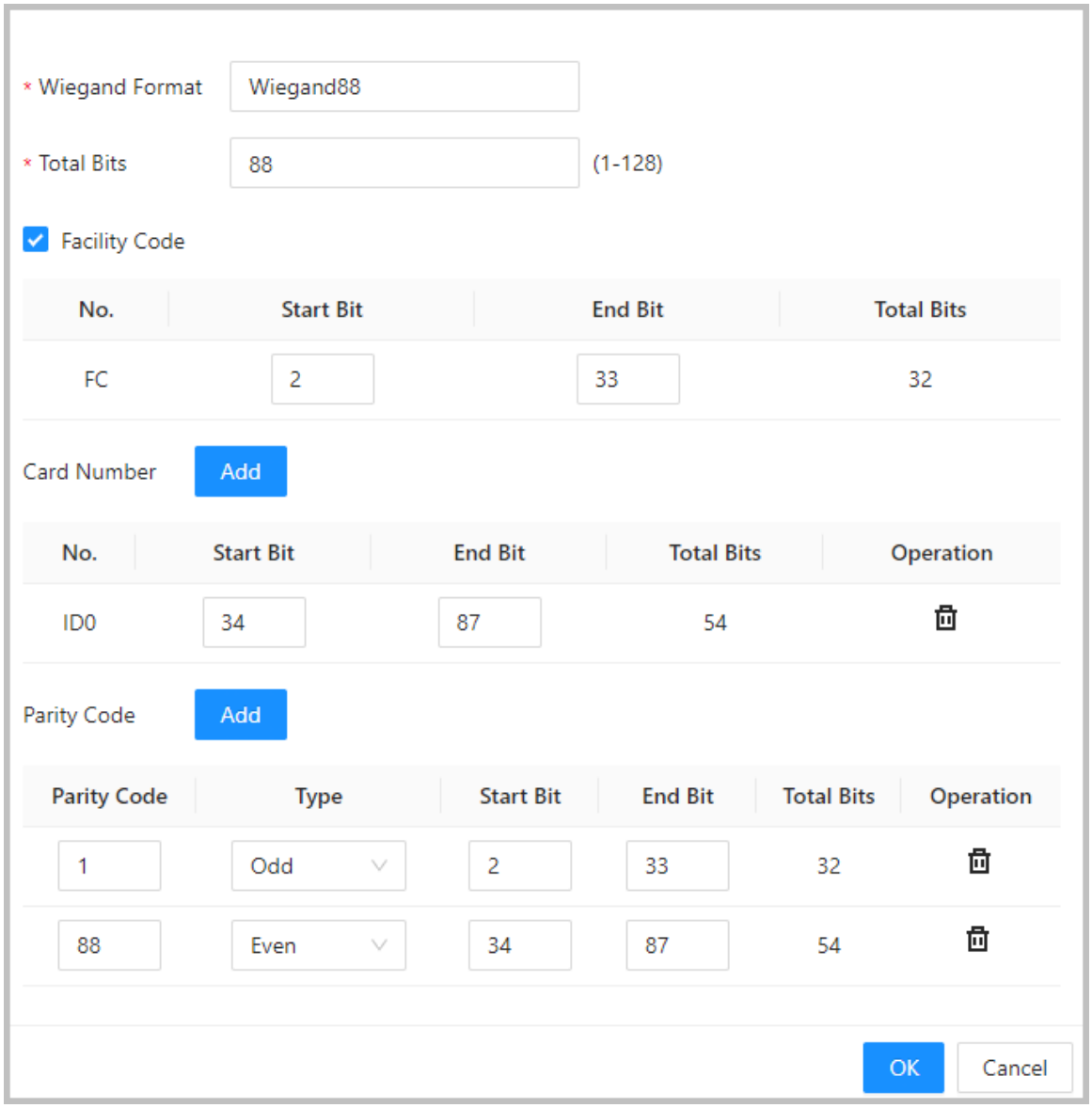


Tableau 2-12 Configuration du format Wiegand

Paramètre	Description
Format Wiegand	Nom du format Wiegand.
Nombre total de bits	Entrez le nombre total de bits.
Code de facilité	Entrez le bit de départ et le bit de fin pour le code de facilité.
Numéro de carte	Entrez le bit de départ et le bit de fin pour le numéro de carte.
Code de parité	1. Entrez le bit de départ de parité paire et le bit de fin de parité paire. 2. Entrez le bit de départ de parité impaire et le bit de fin de parité impaire.

Étape 3 : Cliquez sur **OK**.

Opérations connexes

- Code de facilité : Si cette fonction est activée et que vous réglez **Système de n° de carte** (Card No. System) au format décimal sur la page **Gestion des personnes** (Person Management), le

code de facilité et le numéro de carte sont convertis en format décimal séparément, puis combinés ensemble.

- HID26 : Si cette fonction est activée :
  - Seul Wiegand 26 est pris en charge.
  - La plateforme ne prend en charge que l'affichage des cartes au format décimal.
  - Le numéro de la carte doit comporter 5 caractères et le code de facilité doit comporter 3 caractères au maximum. Lors de la saisie manuelle de la carte, le système ajoutera automatiquement un zéro à la longueur du numéro fixe. Par exemple, si le numéro de carte que vous saisissez est inférieur à 5 caractères, comme 56, le zéro initial est ajouté pour fixer la longueur du numéro à 5 caractères, comme 00056, et un autre 0 est ajouté pour servir de code de facilité. Le numéro de carte final sera par conséquent 000056.

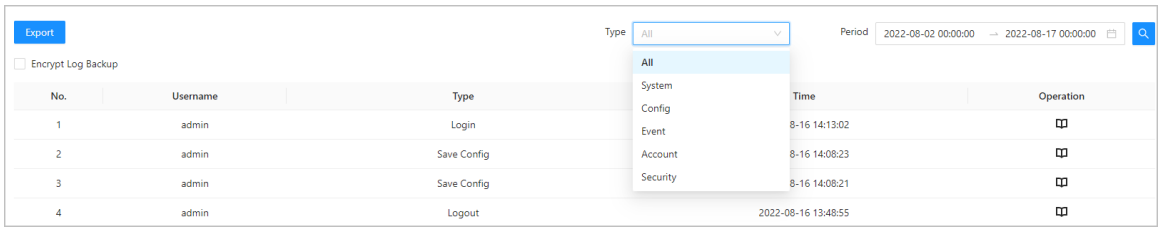
2.2.21.3 Sauvegarde des journaux système

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. de l'appareil local > Journaux système** (Local Device Config > System Logs).

Étape 2 : Sélectionnez le type de journal, puis la plage horaire.

Figure 2-56 Sauvegarde de journaux



Étape 3 : Cliquez sur **Sauvegarde de journaux cryptés** (Encrypt Log Backup), puis saisissez le mot de passe pour sauvegarder les journaux cryptés.

Étape 4 : (En option) vous pouvez également cliquer sur **Exporter** (Export) pour exporter les journaux.

2.2.21.4 Configuration du réseau

2.2.21.4.1 Configuration de TCP/IP

Vous devez configurer l'adresse IP du contrôleur d'accès pour vous assurer qu'il peut communiquer avec d'autres appareils.

Procédure

Étape 1 : Sélectionnez **Config. de l'appareil local > Paramètres réseau > TCP/IP** (Local Device Config > Network Setting > TCP/IP).

Étape 2 : Configurez les paramètres.

Figure 2-57 TCP/IP

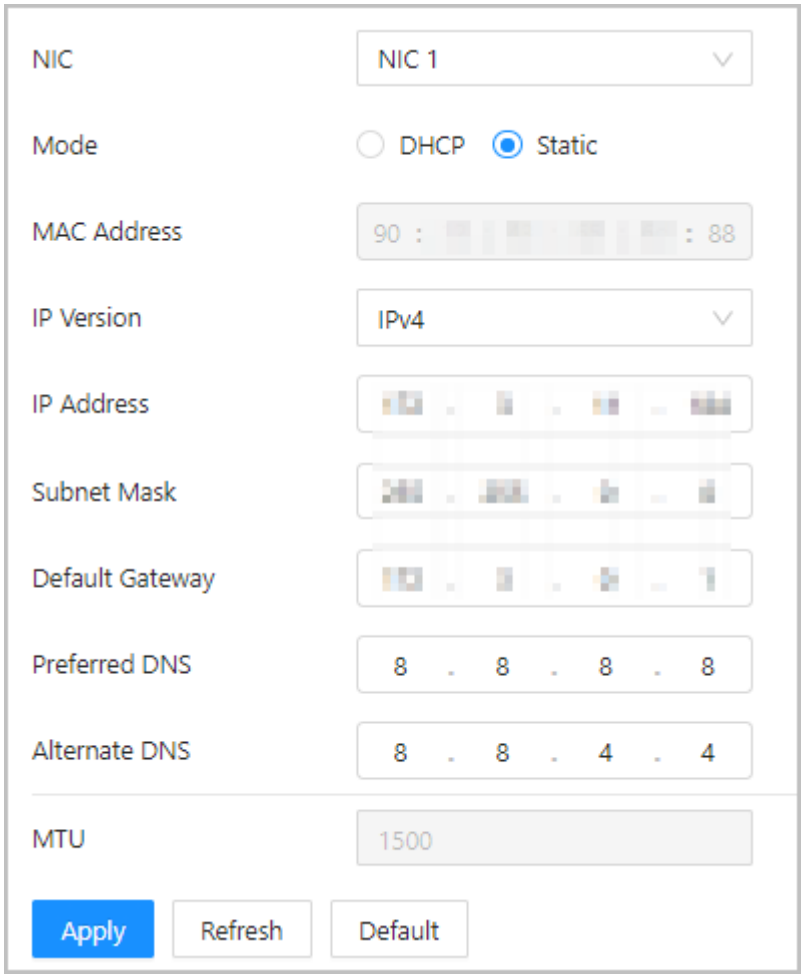


Tableau 2-13 Description de TCP/IP

Paramètre	Description
Version IP	IPv4.
Adresse MAC	Adresse MAC du contrôleur d'accès.
Mode	• **Statique** : Entrez manuellement l'adresse IP, le masque de sous-réseau et la passerelle. • **DHCP** : Protocole de configuration d'hôte dynamique. Lorsque le DHCP est activé, l'adresse IP, le masque de sous-réseau et la passerelle sont automatiquement attribués au contrôleur d'accès.
Adresse IP	Si vous sélectionnez le mode statique, configurez l'adresse IP, le masque de sous-réseau et la passerelle. L'adresse IP et la passerelle doivent être sur le même segment réseau.
Masque sous-réseau	
Passerelle défaut	
DNS préféré	Définissez l'adresse IP du serveur DNS préféré.
DNS alternatif	Définissez l'adresse IP du serveur DNS auxiliaire.

Étape 3 : Cliquez sur **OK**.

2.2.21.4.2 Configuration des ports

Vous pouvez limiter l'accès au contrôleur d'accès simultanément via le Web, le client de bureau et le téléphone.

Procédure

Étape 1 : Sélectionnez **Config. de l'appareil local > Paramètres réseau > Port** (Local Device Config > Network Setting > Port).

Étape 2 : Configurez les numéros de port.

Vous devez redémarrer le contrôleur pour que les configurations soient effectives pour tous les paramètres, à l'exception de **Connexion max.** (Max Connection) et **Port RTSP** (RTSP Port).

Figure 2-58 Configuration des ports

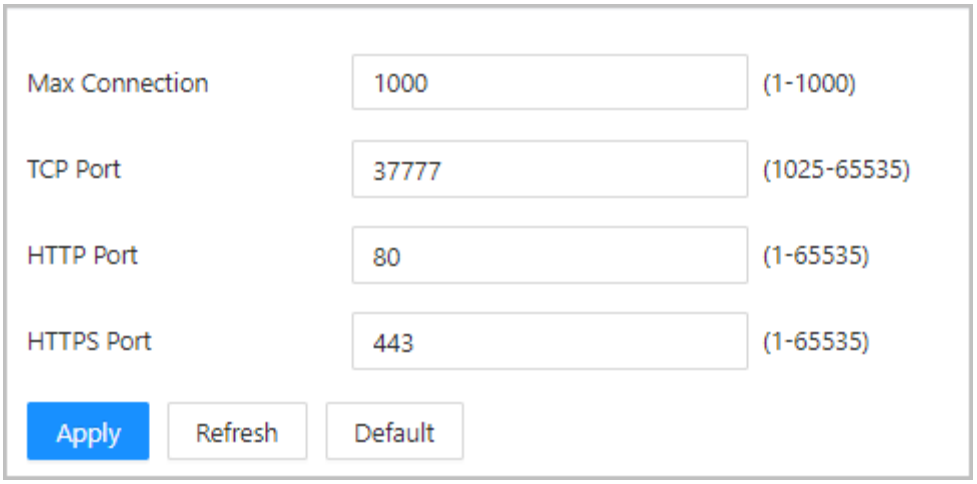


Tableau 2-14 Description des ports

Paramètre	Description
Connexion max	Vous pouvez définir le nombre maximum de clients qui peuvent accéder au contrôleur d'accès en même temps, tels que le client Web, le client de bureau et le téléphone.
Port TCP	C'est le 37777 par défaut.
Port HTTP	La valeur par défaut est 80. Si vous souhaitez modifier le numéro de port, ajoutez le nouveau numéro de port après l'adresse IP lorsque vous vous connectez à la page Web.
Port HTTPS	Il est de 443 par défaut.

Étape 3 : Cliquez sur **OK**.

2.2.21.4.3 Configuration du service cloud

Ajoutez le contrôleur principal au DMSS avant de demander des cartes Bluetooth pour les utilisateurs. Pour plus de détails sur l'utilisation du DMSS, consultez le manuel d'utilisation du DMSS.

Préambule

Si vous avez modifié le mot de passe du contrôleur principal ou restauré les paramètres d'usine, vous devez supprimer le contrôleur du DMSS et l'ajouter à nouveau au DMSS.

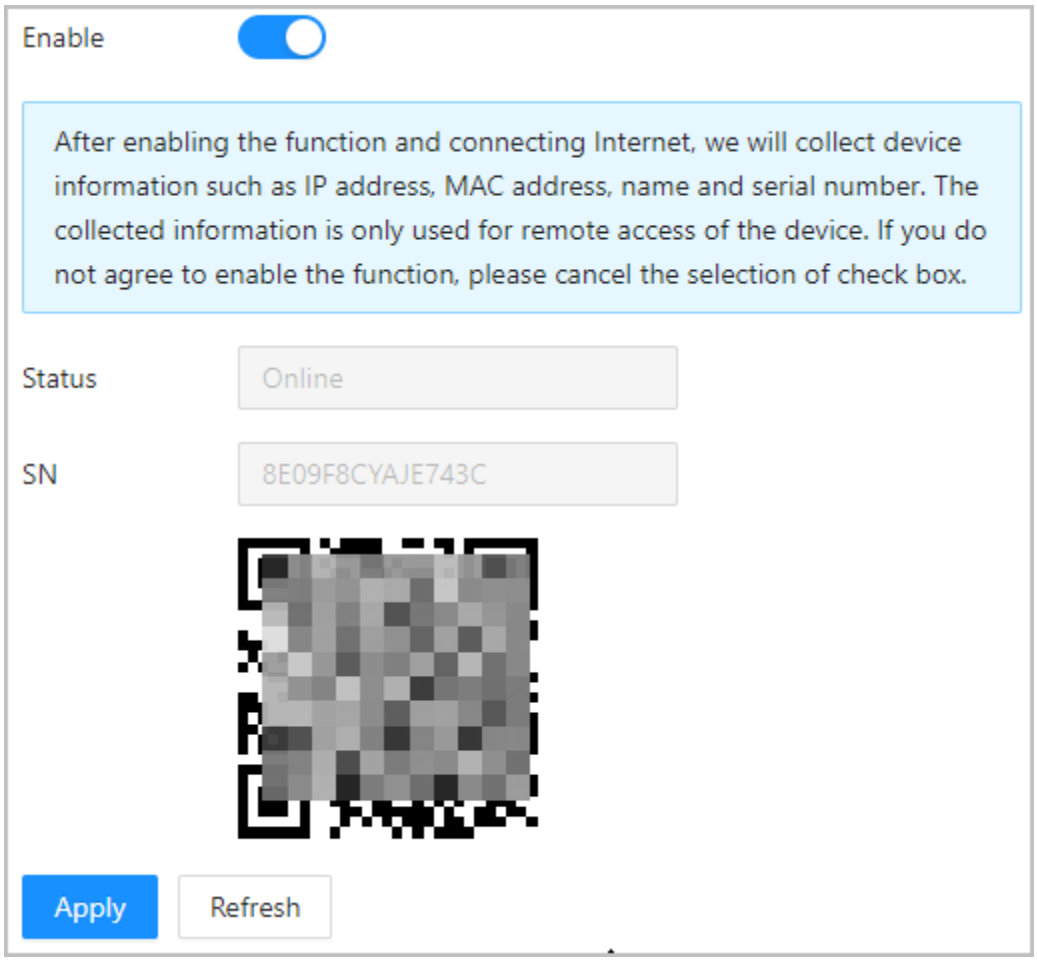
Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. de l'appareil local > Paramètres réseau > Service cloud** (Local Device Config > Network Setting > Cloud Service).

Étape 2 : Activez la fonction de service cloud.

La fonction de service cloud est activée par défaut.

Figure 2-59 Service cloud



Étape 3 : Cliquez sur **Appliquer** (Apply).

Étape 4 : Téléchargez DMSS et inscrivez-vous avec un e-mail, puis scannez le code QR avec le DMSS pour ajouter le contrôleur d'accès.

2.2.21.4.4 Configuration de l'enregistrement automatique

Le contrôleur d'accès communique son adresse au serveur désigné afin que vous puissiez accéder au

contrôleur d'accès via la plateforme de gestion.

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Paramètres réseau > Inscription** (Network Setting > Register).

Étape 2 : Activez la fonction d'enregistrement automatique, puis configurez les paramètres.

Figure 2-60 Inscription

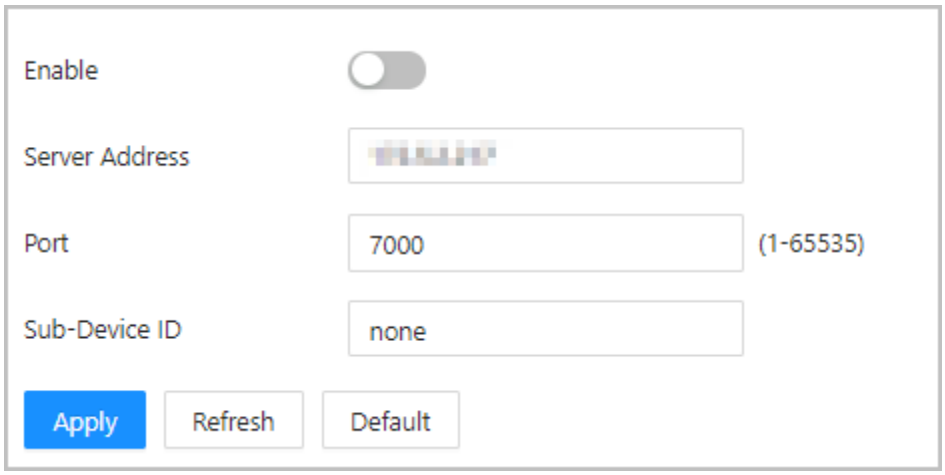


Tableau 2-15 Description de l'enregistrement automatique

Paramètre	Description
Adresse serveur	L'adresse IP du serveur.
Port	Le port du serveur utilisé pour l'enregistrement automatique.
ID du sous-appareil	Entrez l'ID du sous-appareil (défini par l'utilisateur). Lorsque vous ajoutez le contrôleur d'accès à la plateforme de gestion, l'ID du sous-appareil sur la plateforme de gestion doit être conforme à l'ID du sous-appareil défini sur le contrôleur d'accès.

Étape 3 : Cliquez sur **Appliquer** (Apply).

2.2.21.4.5 Configuration du service de base

Lorsque vous souhaitez connecter le contrôleur d'accès à une plateforme tierce, activez les fonctions CGI et ONVIF.

Procédure

Étape 1 : Sélectionnez **Paramètres réseau > Service de base** (Network Settings > Basic Service).

Étape 2 : Configurez le service de base.

Figure 2-61 Service de base

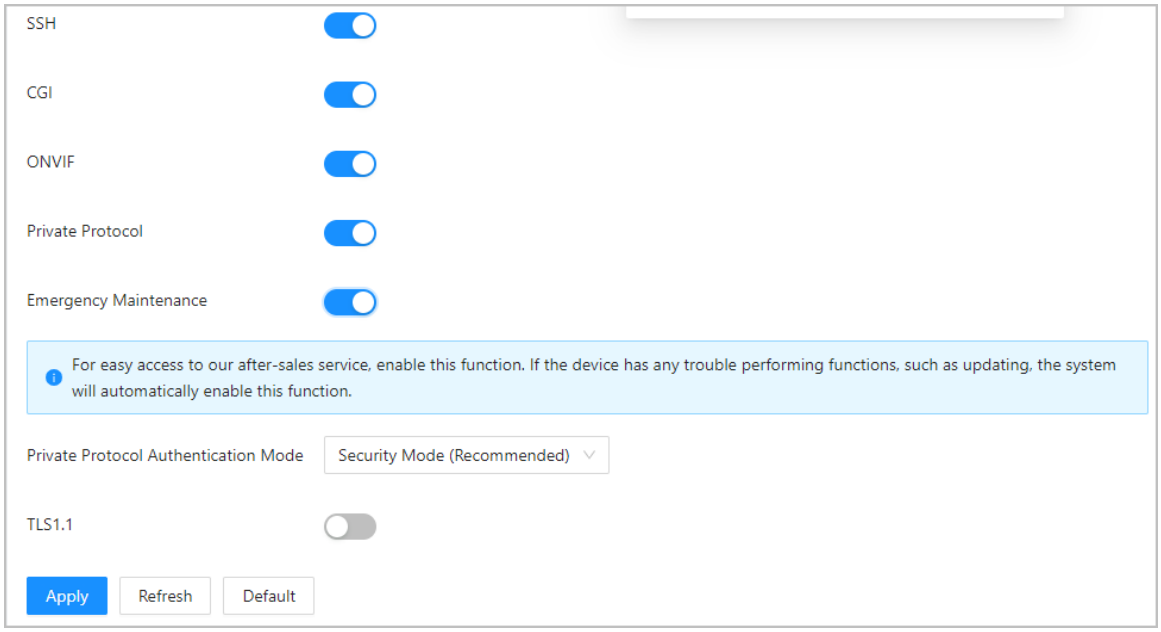


Tableau 2-16 Description des paramètres du service de base

Paramètre	Description
SSH	SSH, ou Secure Shell Protocol, est un protocole d'administration à distance qui permet aux utilisateurs d'accéder, de contrôler et de modifier leurs serveurs distants via Internet.
CGI	L'interface CGI (Common Gateway Interface) est une intersection entre les serveurs Web qui permet l'échange de données normalisées entre les applications et les serveurs externes.
ONVIF	ONVIF est l'acronyme de Open Network Video Interface Forum. Il a pour but de fournir une norme pour l'interface entre différents appareils de sécurité basés sur IP. Ces spécifications ONVIF normalisées sont comme un langage commun que tous les appareils peuvent utiliser pour communiquer.
Protocole privé	La plateforme ajoute des appareils via le protocole TLSv1.1. Des risques de sécurité peuvent survenir lorsque le protocole TLSv1.1 est activé. Agissez avec prudence.
Maintenance d'urgence	Il est désactivé par défaut.

Paramètre	Description
Mode d'authentification de protocole privé	Définissez le mode d'authentification, y compris le mode sécurité et le mode de compatibilité. Il est recommandé de choisir **Mode sécurité** (Security Mode). ● Mode Sécurité (recommandé) : Ne prend pas en charge l'accès à l'appareil via les méthodes d'authentification Digest, DES et Texte en clair, ce qui améliore la sécurité de l'appareil. ● Mode compatible : Prend en charge l'accès à l'appareil via les méthodes d'authentification Digest, DES et Texte en clair, avec une sécurité réduite.

Étape 3 : Cliquez sur **Appliquer** (Apply).

2.2.21.5 Configuration de l'heure

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. de l'appareil local > Heure** (Local Device Config > Time).

Étape 2 : Configurez l'heure de la plateforme.

Figure 2-62 Réglages de la date

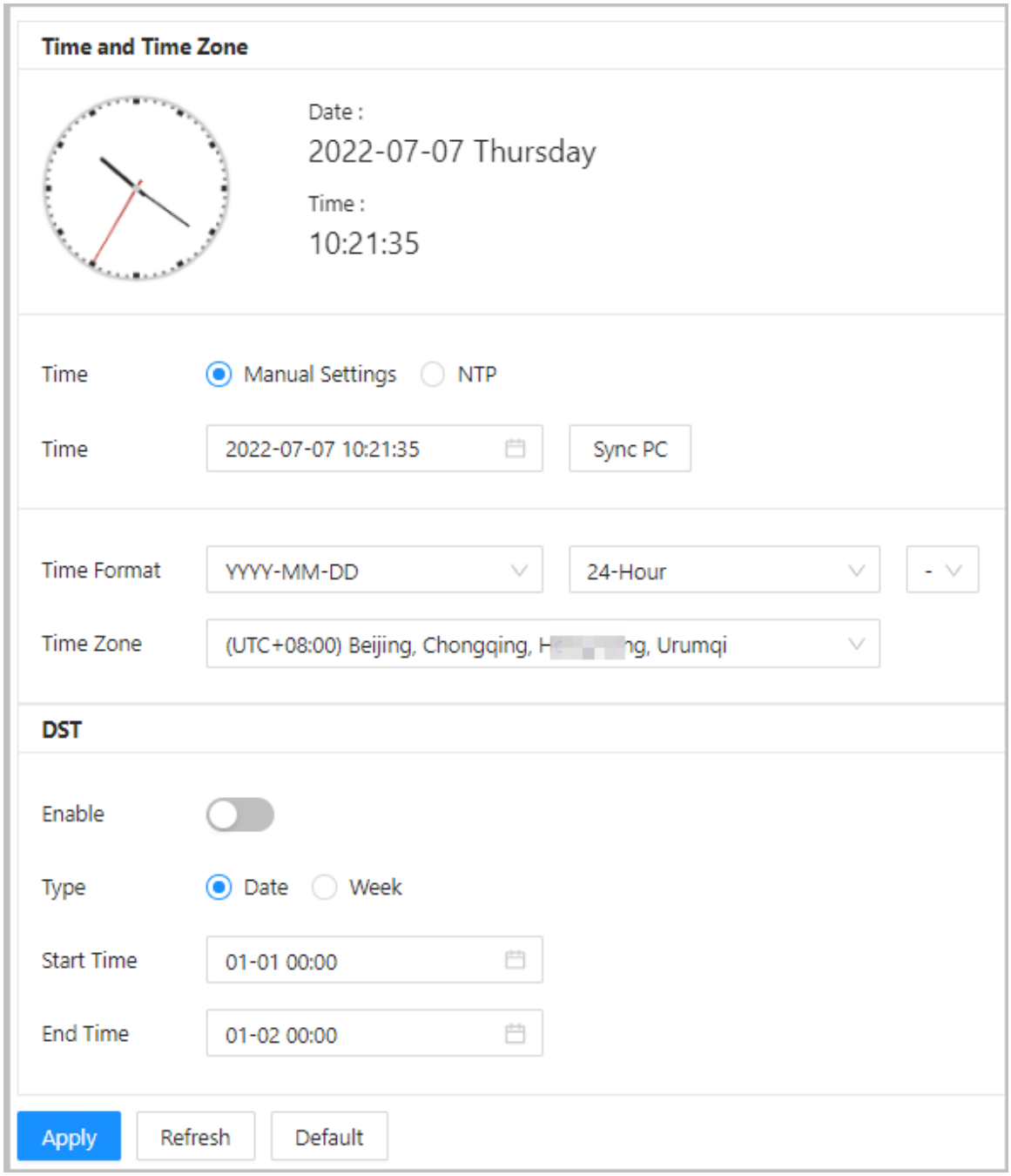


Tableau 2-17 Description des réglages de l'heure

Paramètre	Description
Heure	● Réglages manuels : Entrez manuellement l'heure ou cliquez sur **Synchroniser PC** (Sync PC) pour synchroniser l'heure avec l'ordinateur. ● NTP : Le contrôleur d'accès synchronisera automatiquement l'heure avec le serveur NTP. ◇ **Serveur** : Entrez le domaine du serveur NTP. ◇ **Port** : Entrez le port du serveur NTP. ◇ **Intervalle** : Entrez son heure et l'intervalle de synchronisation.

Paramètre	Description
Format d'heure	Sélectionnez le format de l'heure de la plateforme.
Fuseau horaire	Entrez le fuseau horaire du contrôleur d'accès.
Heure légale (DST)	1. (En option) Activez l'heure d'été (DST). 2. Sélectionnez **Date** ou **Semaine** (Week) dans le champ **Type**. 3. Configurez l'heure de début et l'heure de fin.

Étape 3 : Cliquez sur **Appliquer** (Apply).

2.2.21.6 Gestion de compte

Vous pouvez ajouter ou supprimer des utilisateurs, modifier le mot de passe de l'utilisateur et saisir une adresse e-mail pour réinitialiser votre mot de passe en cas d'oubli.

2.2.21.6.1 Ajout de comptes administrateurs

Ajoutez des administrateurs sur le contrôleur d'accès.

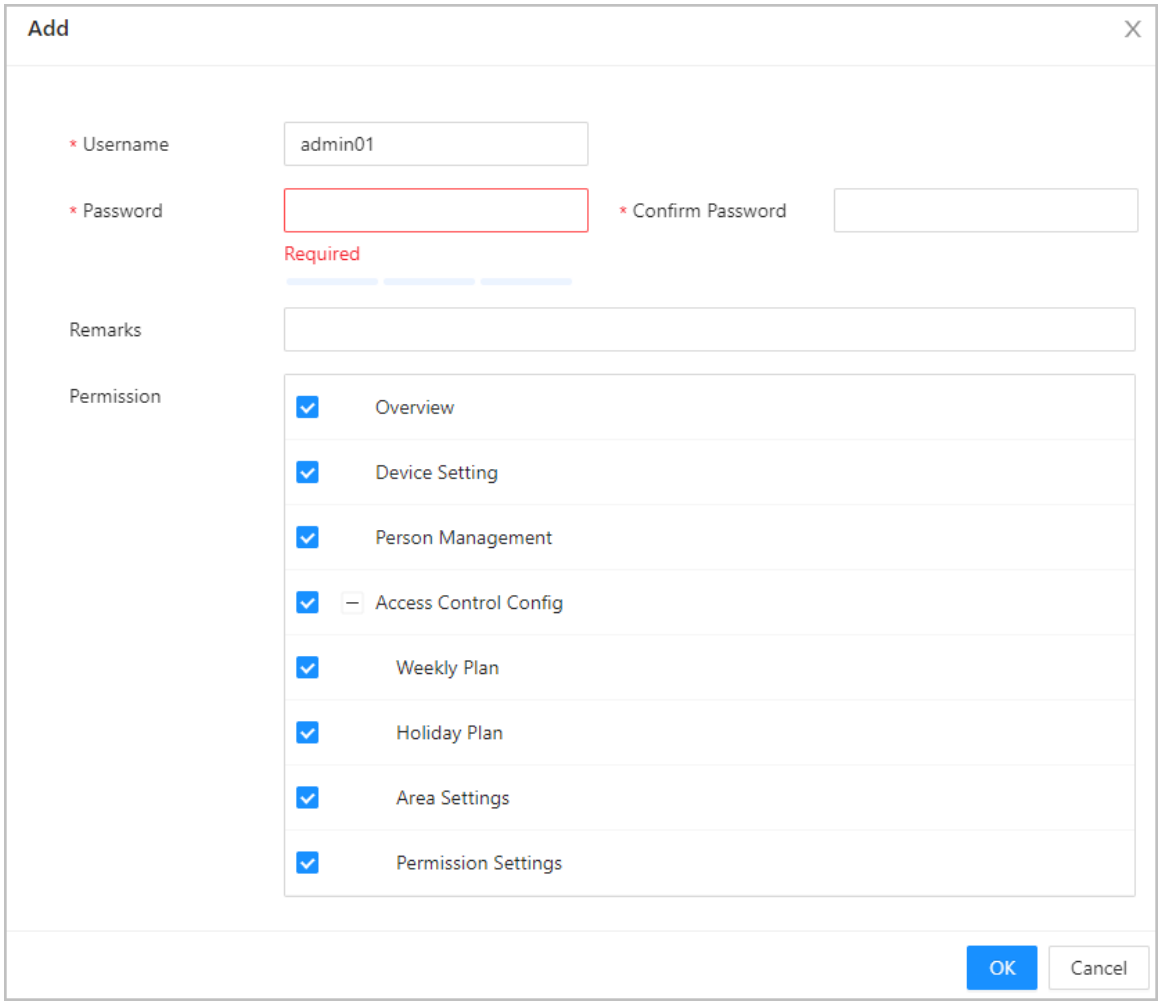
Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. de l'appareil local > Gestion de compte > Compte** (Local Device Config > Account Management > Account).

Étape 2 : Cliquez sur **Ajouter** (Add), puis saisissez les informations sur l'utilisateur.

- Le nom d'utilisateur ne peut pas être identique à celui du compte existant. Le nom d'utilisateur peut contenir jusqu'à 31 caractères et prend en charge les chiffres, les lettres, les soulignements, les points et les @.
- Le mot de passe doit être composé de 8 à 32 caractères non blancs et d'au moins 2 types de caractères parmi des majuscules, des minuscules, des chiffres et des caractères spéciaux (sauf ' " ; : &). Définissez un mot de passe de haute sécurité en suivant l'invite relative à la longueur du mot de passe.

Figure 2-63 Ajout de comptes administrateurs



Étape 3 : Cliquez sur **OK**.

Seul le compte administrateur peut modifier le mot de passe et le compte administrateur ne peut pas être supprimé.

2.2.21.6.2 Réinitialisation du mot de passe

Réinitialisez le mot de passe via l'e-mail lié lorsque vous oubliez votre mot de passe.

Procédure

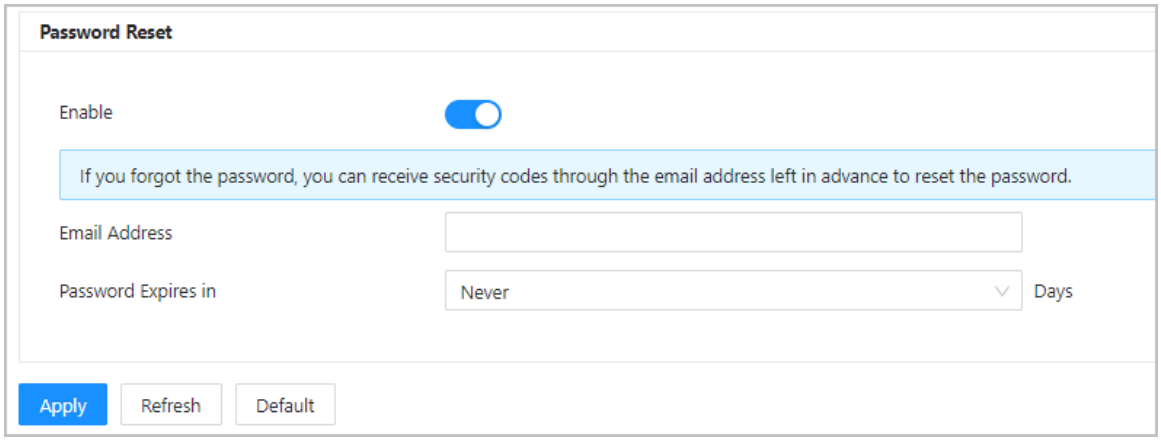
Étape 1 : Sélectionnez **Config. de l'appareil local > Gestion de compte > Compte** (Local Device

Config > Account Management > Account).

Étape 2 : Saisissez l'adresse e-mail et définissez l'heure d'expiration du mot de passe.

Étape 3 : Activez la fonction de réinitialisation du mot de passe.

Figure 2-64 Réinitialisation du mot de passe



Si vous avez oublié le mot de passe, vous pouvez recevoir des codes de sécurité via l'adresse e-mail liée pour réinitialiser le mot de passe.

Étape 4 : Cliquez sur **Appliquer** (Apply).

2.2.21.6.3 Ajout des utilisateurs ONVIF

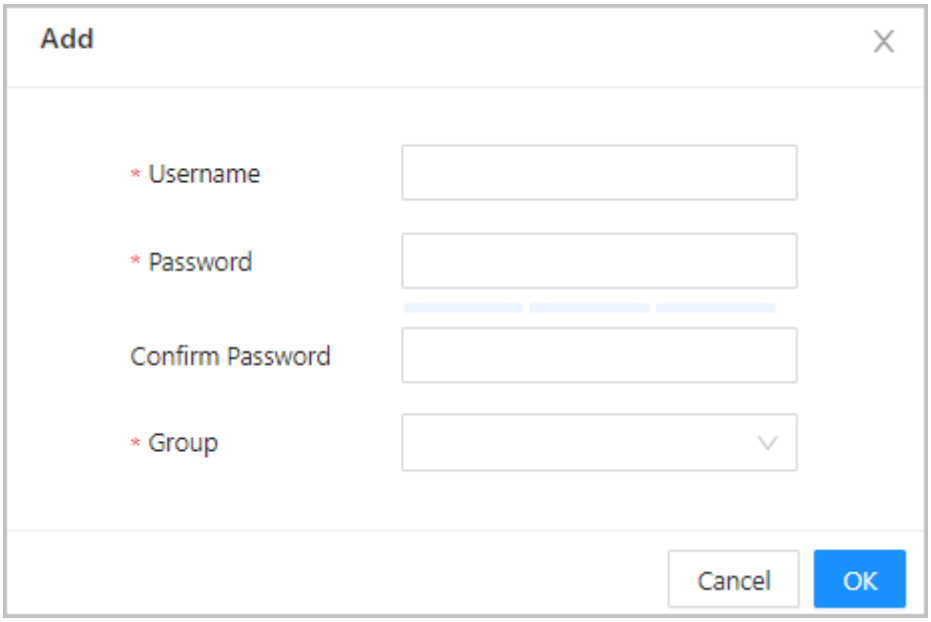
Open Network Video Interface Forum (ONVIF), un forum industriel mondial et ouvert qui a été créé pour développer une norme ouverte mondiale pour l'interface des produits de sécurité physique basés sur IP, ce qui permet la compatibilité entre les différents fabricants. L'identité des utilisateurs ONVIF est vérifiée via le protocole ONVIF. L'utilisateur ONVIF par défaut est admin.

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. de l'appareil local > Gestion de compte > Compte ONVIF** (Local Device Config > Account Management > ONVIF Account).

Étape 2 : Cliquez sur **Ajouter** (Add), puis configurez les paramètres.

Figure 2-65 Ajout d'utilisateur ONVIF



Étape 3 : Cliquez sur **OK**.

2.2.21.7 Maintenance

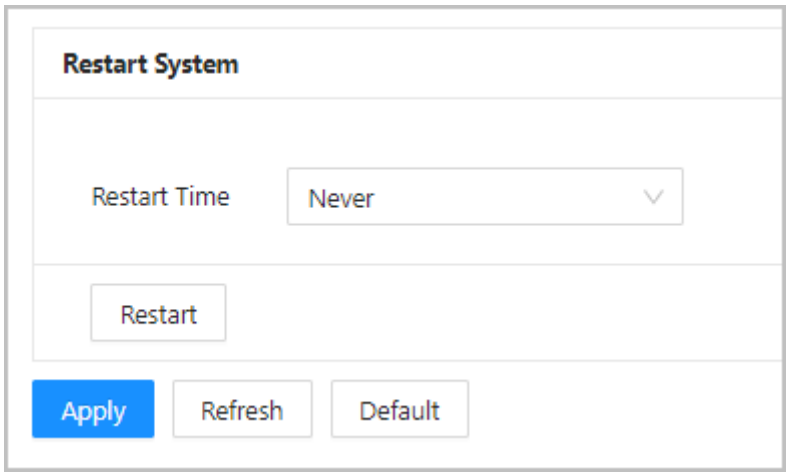
Vous pouvez redémarrer régulièrement le contrôleur d'accès pendant sa période d'inactivité afin d'améliorer ses performances. Par défaut, il est défini sur **Jamais** (Never) par défaut, nous vous recommandons de le modifier pour qu'il soit effectué un jour par semaine.

Procédure

Étape 1 : Connectez-vous à la page Web.

Étape 2 : Sélectionnez **Config. de l'appareil local > Maintenance** (Local Device Config > Maintenance).

Figure 2-66 Maintenance



Étape 3 : Définissez l'heure de redémarrage, puis cliquez sur **OK**.

Étape 4 : (En option) Cliquez sur **Redémarrer** (Restart) pour que le contrôleur d'accès redémarre immédiatement.

2.2.21.8 Gestion avancée

Lorsque plusieurs contrôleurs d'accès nécessitent les mêmes configurations, vous pouvez les configurer rapidement en important ou en exportant des fichiers de configuration.

2.2.21.8.1 Exportation et importation de fichiers de configuration

Vous pouvez importer et exporter le fichier de configuration du contrôleur d'accès. Lorsque vous souhaitez appliquer les mêmes configurations à plusieurs appareils, vous pouvez y importer le fichier de configuration.

Préambule

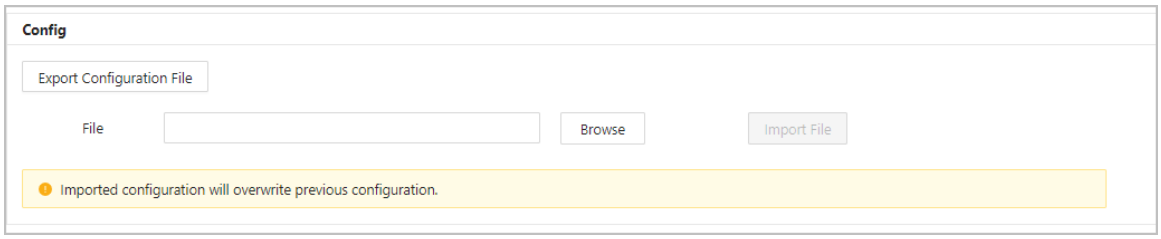
Les configurations relatives à la gestion des appareils, au contrôle d'accès avancé, aux horaires et au matériel ne peuvent pas être exportées.

Procédure

Étape 1 : Connectez-vous à la page Web.

Étape 2 : Sélectionnez **Config. de l'appareil local > Paramètres avancés** (Local Device Config > Advanced Settings).

Figure 2-67 Gestion des configurations



Étape 3 : Exportez ou importez des fichiers de configuration.

- Exportez le fichier de configuration.

  Cliquez sur **Exporter le fichier de configuration** (Export Configuration file) pour télécharger le fichier sur l'ordinateur local.

  L'IP ne sera pas exporté.

- Importez le fichier de configuration.
  1. Cliquez sur **Parcourir** (Browse) pour sélectionner le fichier de configuration.
  2. Cliquez sur **Importer la configuration** (Import Configuration).

     Les fichiers de configuration ne peuvent être importés que vers des appareils ayant le même modèle.

2.2.21.8.2 Configuration du lecteur de carte

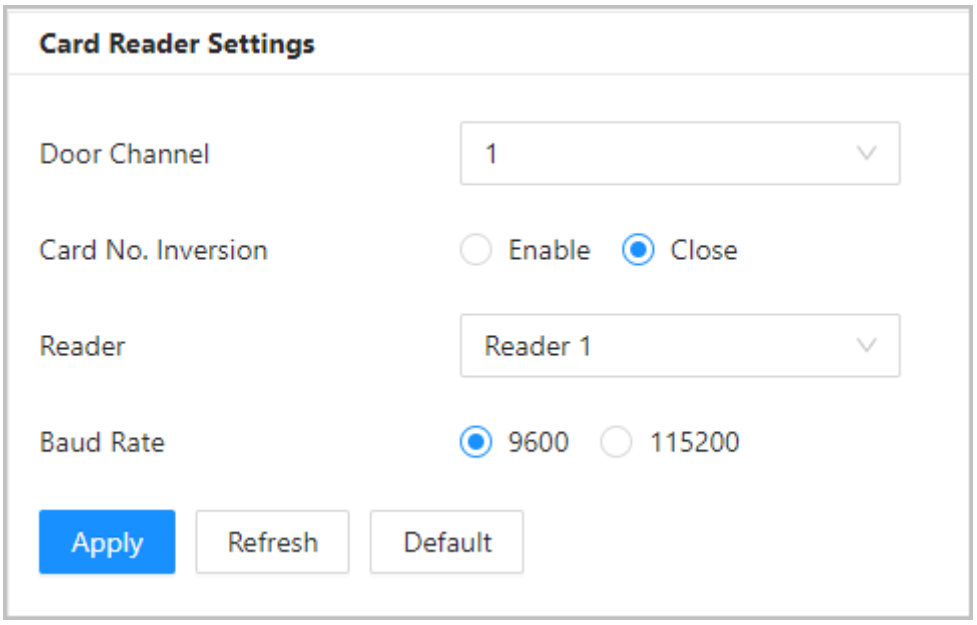
Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Config. de l'appareil local > Paramètres avancés** (Local

Device Config > Advanced Settings).

Étape 2 : Configurez le lecteur de carte.

Figure 2-68 Configuration du lecteur de carte



2.2.21.8.3 Configuration du niveau d'empreinte digitale

Sur la page d'accueil, sélectionnez **Config. de l'appareil local > Paramètres avancés** (Local Device Config > Advanced Settings), puis entrez le seuil d'empreinte digitale. La valeur est comprise entre 1 et 10, et une valeur plus élevée signifie une plus grande précision de reconnaissance.

Figure 2-69 Niveau d'empreinte digitale

2.2.21.8.4 Configuration de l'extension RS-485

Si le contrôleur d'accès est monté sur le boîtier métallique du contrôleur d'accès, sélectionnez **Config. de l'appareil local > Extension RS-485** (Local Device Config > RS-485 Expansion), puis sélectionnez **Boîtier métallique du contrôleur d'accès** (Access Control Metal Case).

2.2.21.8.5 Restauration des réglages d'usine par défaut

Procédure

Étape 1 : Sélectionnez **Config. de l'appareil local > Paramètres avancés** (Local Device Config > Advanced Settings).

La restauration des configurations par défaut du **Contrôleur d'accès** (Access Controller) entraînera une perte de données. Agissez avec prudence.

Étape 2 : Rétablissez les réglages d'usine par défaut si nécessaire.

- **Réglages d'usine par défaut** : Réinitialise toutes les configurations du contrôleur et supprime toutes les données.
- **Restaurer les param. par défaut (excepté pour les infos utilisateur)** : Réinitialise les configurations du contrôleur d'accès et supprime toutes les données, à l'exception des informations sur l'utilisateur et des informations configurées pendant l'assistant de connexion.

Seul le contrôleur principal prend en charge **Restaurer les param. par défaut (excepté pour les infos utilisateur)** (Restore to Default (Except for User Info)).

2.2.21.9 Mise à jour du système

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

2.2.21.9.1 Mise à jour du fichier

Procédure

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

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

L'extension du fichier de mise à jour doit être « .bin ».

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

Le contrôleur d'accès redémarre une fois la mise à jour terminée.

2.2.21.9.2 Mise à jour en ligne

Procédure

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

Étape 2 : Dans la zone **Mise à jour en ligne** (Online Update), sélectionnez une méthode de mise à jour.

- Sélectionnez **Vérification automatique des mises à jour** (Auto Check for Updates), et

le contrôleur d'accès vérifiera automatiquement la présence de la dernière version mise à jour.

- Sélectionnez **Vérification manuelle** (Manual Check), et vous pouvez immédiatement vérifier si la dernière version est disponible.

Étape 3 : Cliquez sur **Vérification manuelle** (Manual Check) pour mettre à jour le contrôleur d'accès lorsque la dernière version est disponible.

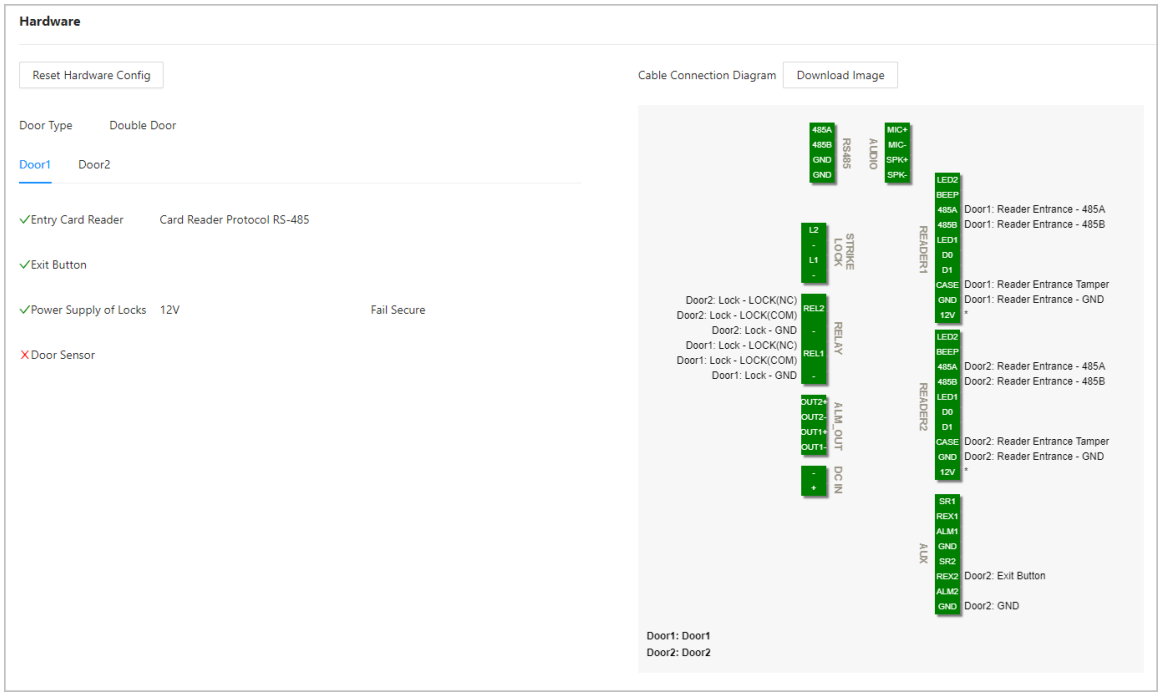
2.2.21.10 Configuration du matériel

Sur la page d'accueil, sélectionnez **Config. de l'appareil local > Matériel** (Local Device Config > Hardware). Vous pouvez voir le matériel que vous avez configuré lorsque vous vous connectez à la plateforme pour la première fois. Vous pouvez également cliquer sur **Réinitialiser la config. matérielle** (Reset Hardware Config) pour reconfigurer le matériel. Pour plus de détails, reportez-vous au Tableau 2-1.

Lorsque vous passez d'une porte simple à une porte double, nous vous recommandons de rétablir les paramètres d'usine du contrôleur principal.

Le schéma de câblage est généré pour votre référence. Vous pouvez le télécharger sur votre ordinateur.

Figure 2-70 Matériel



2.2.21.11 Affichage des informations sur la version

Sur la page d'accueil, sélectionnez **Config. de l'appareil local > Infos version** (Local Device Config > Version Info), et vous pourrez afficher des informations sur la version, telles que le modèle de l'appareil, le numéro de série, la version du matériel, les informations légales, etc.

2.2.21.12 Affichage des informations légales

Sur la page d'accueil, sélectionnez **Config. de l'appareil local > infos légales** (Local Device Config > Legal Info), et vous pourrez afficher le contrat de licence du logiciel, la politique de confidentialité et l'avis sur les logiciels libres.

2.2.22 Affichage des enregistrements

Vous pouvez afficher les journaux d'alarme et les journaux de déverrouillage.

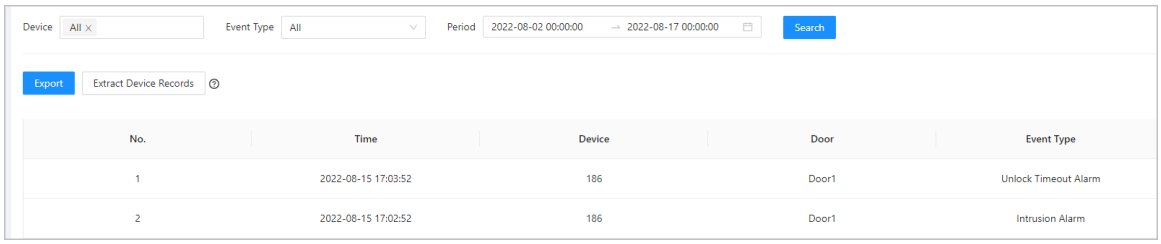
2.2.22.1 Affichage des enregistrements d'alarme

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Rapports > Enregistrements d'alarme** (Reporting > Alarm Records).

Étape 2 : Sélectionnez l'appareil, le service et la plage horaire, puis cliquez sur **Rechercher** (Search).

Figure 2-71 Enregistrements d'alarme



- **Exporter :** Exporte les journaux de déverrouillage du contrôleur principal vers un ordinateur local.
- **Extraire les enregistrements de l'appareil :** Lorsque les journaux du sous-contrôleur sont générés lorsqu'ils sont mis en ligne, vous pouvez extraire les journaux du sous-contrôleur vers le contrôleur principal.

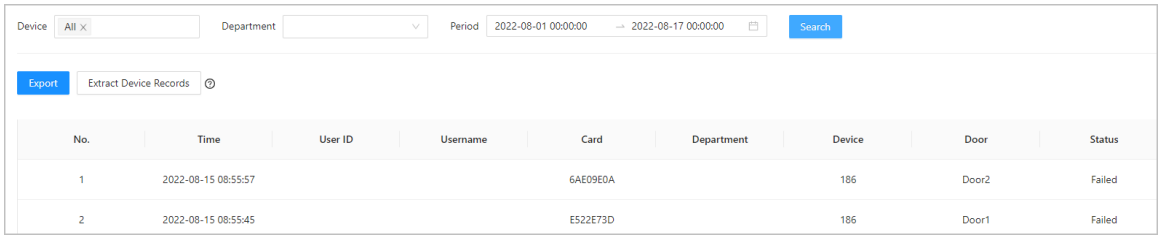
2.2.22.2 Affichage des enregistrements de déverrouillage

Procédure

Étape 1 : Sur la page d'accueil, sélectionnez **Rapports > Enregistrements de déverrouillage** (Reporting > Unlock Records)

Étape 2 : Sélectionnez l'appareil, le service et la plage horaire, puis cliquez sur **Rechercher** (Search).

Figure 2-72 Journaux de déverrouillage



- Exporter : Exporte les journaux de déverrouillage.
- Extraire les enregistrements de l'appareil : Lorsque les journaux du sous-contrôleur sont générés lorsqu'ils sont mis en ligne, vous pouvez extraire les journaux du sous-contrôleur vers le contrôleur principal.

2.2.23 Réglages de sécurité (en option)

2.2.23.1 État de sécurité

Analysez les utilisateurs, le service et les modules de sécurité pour vérifier l'état de sécurité du contrôleur d'accès.

Préambule

- Détection d'utilisateur et de service : Vérifiez si la configuration actuelle est conforme aux recommandations.
- Analyse des modules de sécurité : Analyse l'état de fonctionnement des modules de sécurité, tels que la transmission audio et vidéo, la protection fiable, les avertissements de sécurité et la défense contre les attaques, et ne détecte pas s'ils sont activés.

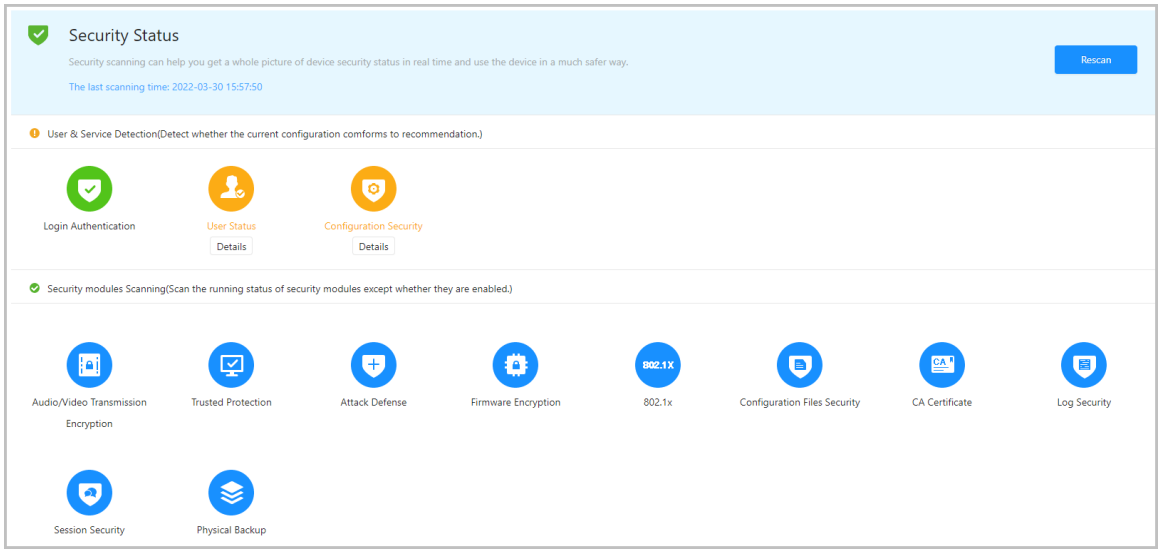
Procédure

Étape 1 : Sélectionnez **Sécurité > État de sécurité** (Security > Security Status).

Étape 2 : Cliquez sur **Nouvelle recherche** (Rescan) pour effectuer une analyse de sécurité du contrôleur d'accès.

Passez le curseur sur les icônes des modules de sécurité pour voir leur état de fonctionnement.

Figure 2-73 État de sécurité



Opérations connexes

Une fois l'analyse effectuée, les résultats s'affichent dans différentes couleurs. Le jaune indique que les modules de sécurité sont anormaux, et le vert indique que les modules de sécurité sont normaux.

- Cliquez sur **Détails** (Details) pour afficher les détails du résultat de l'analyse.
- Cliquez sur **Ignorer** (Ignore) pour ignorer l'anomalie, et elle ne sera pas analysée. L'anomalie qui a été ignorée est surlignée en gris.

  Cliquez sur **Rejoindre la détection** (Rejoin Detection) pour que l'anomalie ignorée soit à nouveau analysée.
- Cliquez sur **Optimiser** (Optimize) pour résoudre l'anomalie.

2.2.23.2 Configuration du protocole HTTPS

Créez un certificat ou téléchargez un certificat authentifié, puis vous pourrez vous connecter à la page Web via HTTPS avec votre ordinateur. HTTPS sécurise la communication sur un réseau informatique.

Procédure

Étape 1 : Sélectionnez **Sécurité > Service système > HTTPS** (Security > System Service > HTTPS).

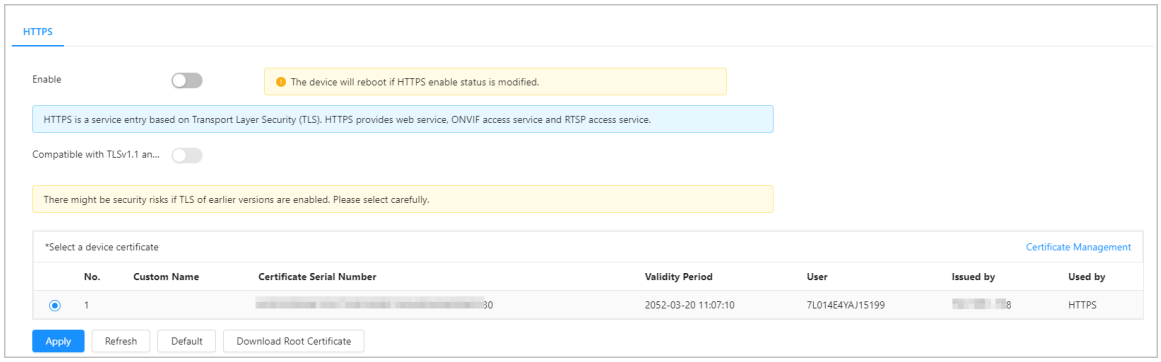
Étape 2 : Activez le service HTTPS.

Si vous activez le service compatible avec TLS v1.1 et les versions antérieures, des risques de sécurité peuvent survenir. Agissez avec prudence.

Étape 3 : Sélectionnez le certificat.

Si la liste ne contient aucun certificat, cliquez sur **Gestion des certificats** (Certificate Management) pour télécharger un certificat. Pour les détails, voir « 2.2.23.4 Installation d'un certificat d'appareil ».

Figure 2-74 HTTPS



Étape 4 : Cliquez sur **Appliquer** (Apply).

Saisissez « https://*IP address*: *httpsport* » dans un navigateur Web. Si le certificat est installé, vous pouvez vous connecter à la page Web avec succès. Dans le cas contraire, la page Web affichera le certificat comme étant erroné ou non fiable.

2.2.23.3 Protection contre les attaques

2.2.23.3.1 Configuration du pare-feu

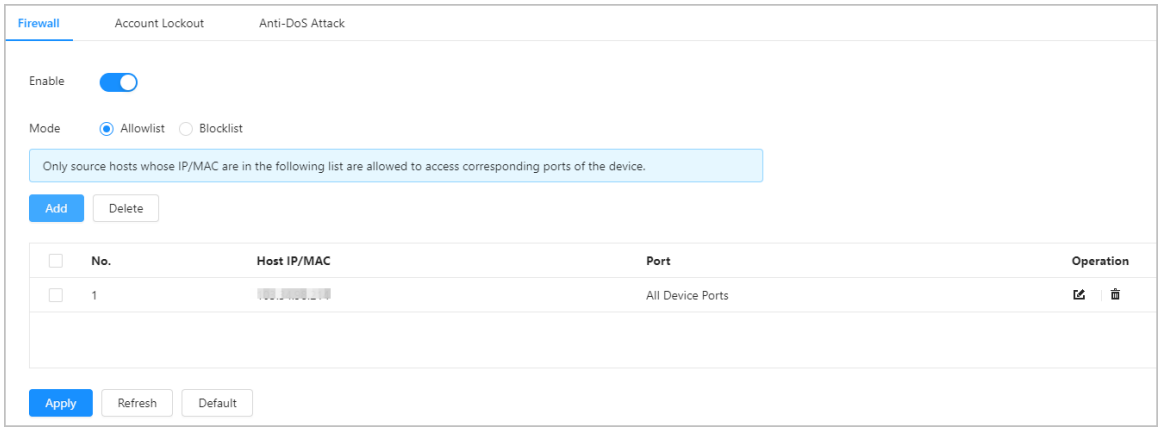
Configurez le pare-feu pour limiter l'accès au contrôleur d'accès.

Procédure

Étape 1 : Sélectionnez **Sécurité > Protection contre les attaques > Pare-feu** (Security > Attack Defense > Firewall).

Étape 2 : Cliquez sur pour activer la fonction de pare-feu.

Figure 2-75 Pare-feu



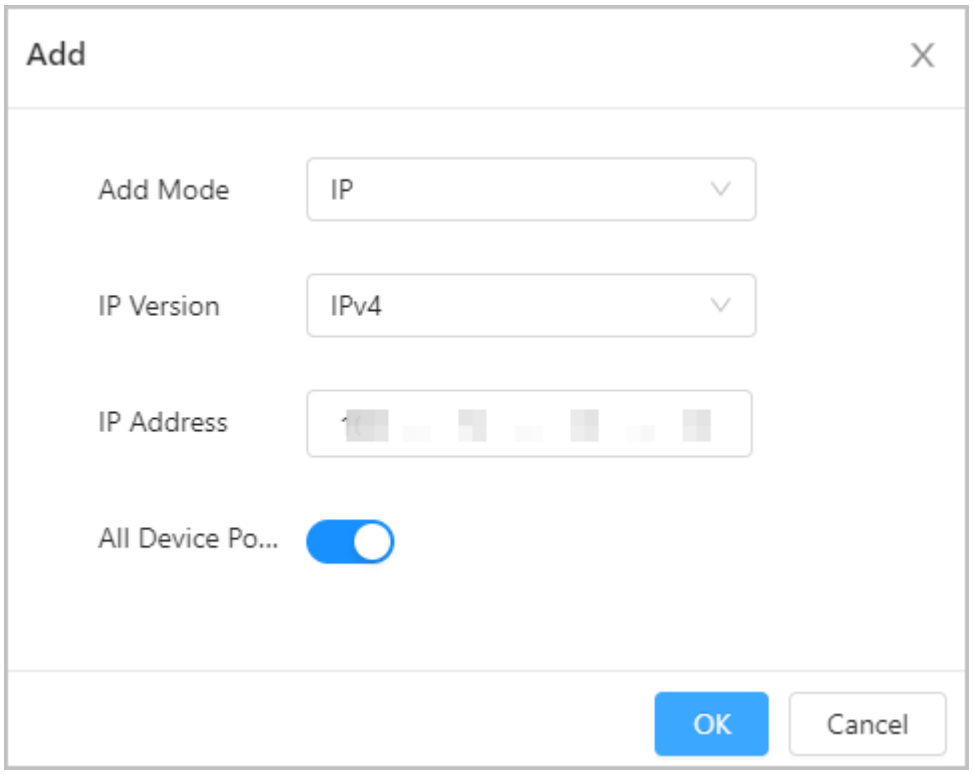
Étape 3 : Sélectionnez un mode : **Liste d'autorisation** (Allowlist) et **Liste de blocage** (Blocklist).

- **Liste d'autorisation :** Seules les adresses IP/MAC figurant sur la liste d'autorisation peuvent accéder au contrôleur d'accès.
- **Liste de blocage :** Les adresses IP/MAC figurant sur la liste de blocage ne peuvent

accéder au contrôleur d'accès.

Étape 4 : Cliquez sur **Ajouter** (Add) pour saisir les informations IP.

Figure 2-76 Ajout des Informations IP



Étape 5 : Cliquez sur **OK**.

Opérations connexes

- Cliquez sur pour modifier les informations IP.
- Cliquez sur pour supprimer l'adresse IP.

2.2.23.3.2 Configuration du verrouillage de compte

Si un mot de passe incorrect est saisi un certain nombre de fois, le compte est verrouillé.

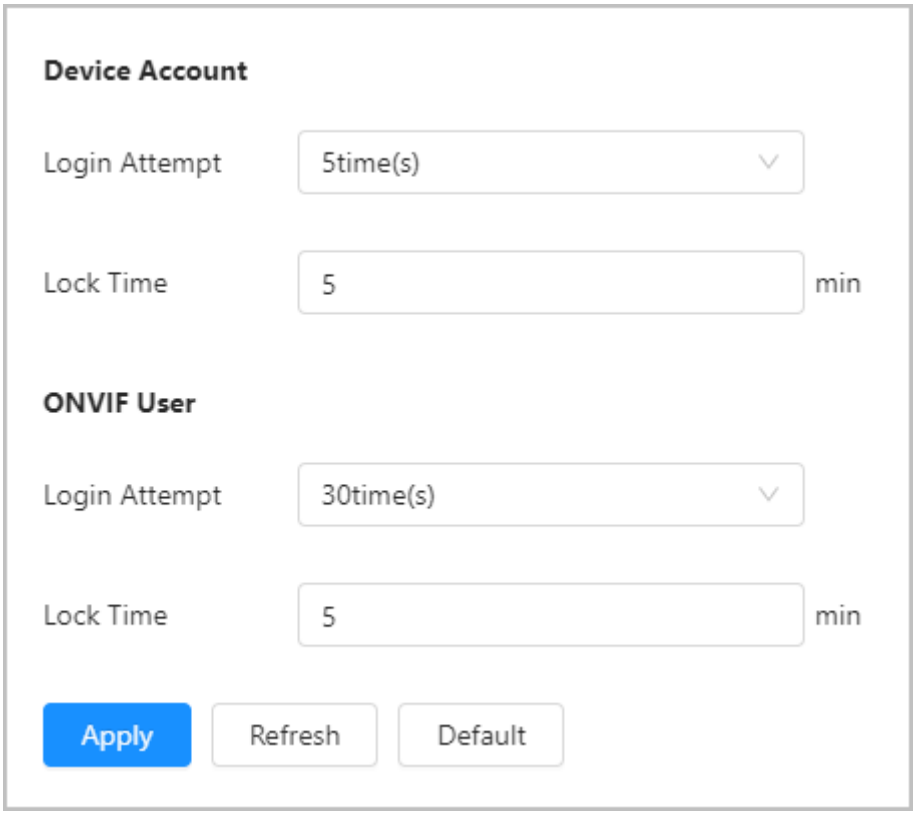
Procédure

Étape 1 : Sélectionnez **Sécurité > Protection contre les attaques > Verrouillage du compte** (Security > Attack Defense > Account Lockout).

Étape 2 : Saisissez le nombre de tentatives de connexion et la durée pendant laquelle le compte administrateur et l'utilisateur ONVIF seront verrouillés.

- Tentatives de connexion : La limite des tentatives de connexion. Si un mot de passe incorrect est saisi un certain nombre de fois, le compte est verrouillé.
- Délai de verrouillage : La durée pendant laquelle vous ne pouvez pas vous connecter après le verrouillage du compte.

Figure 2-77 Verrouillage du compte



Étape 3 : Cliquez sur **Appliquer** (Apply).

2.2.23.3.3 Configuration de l'attaque par déni de service

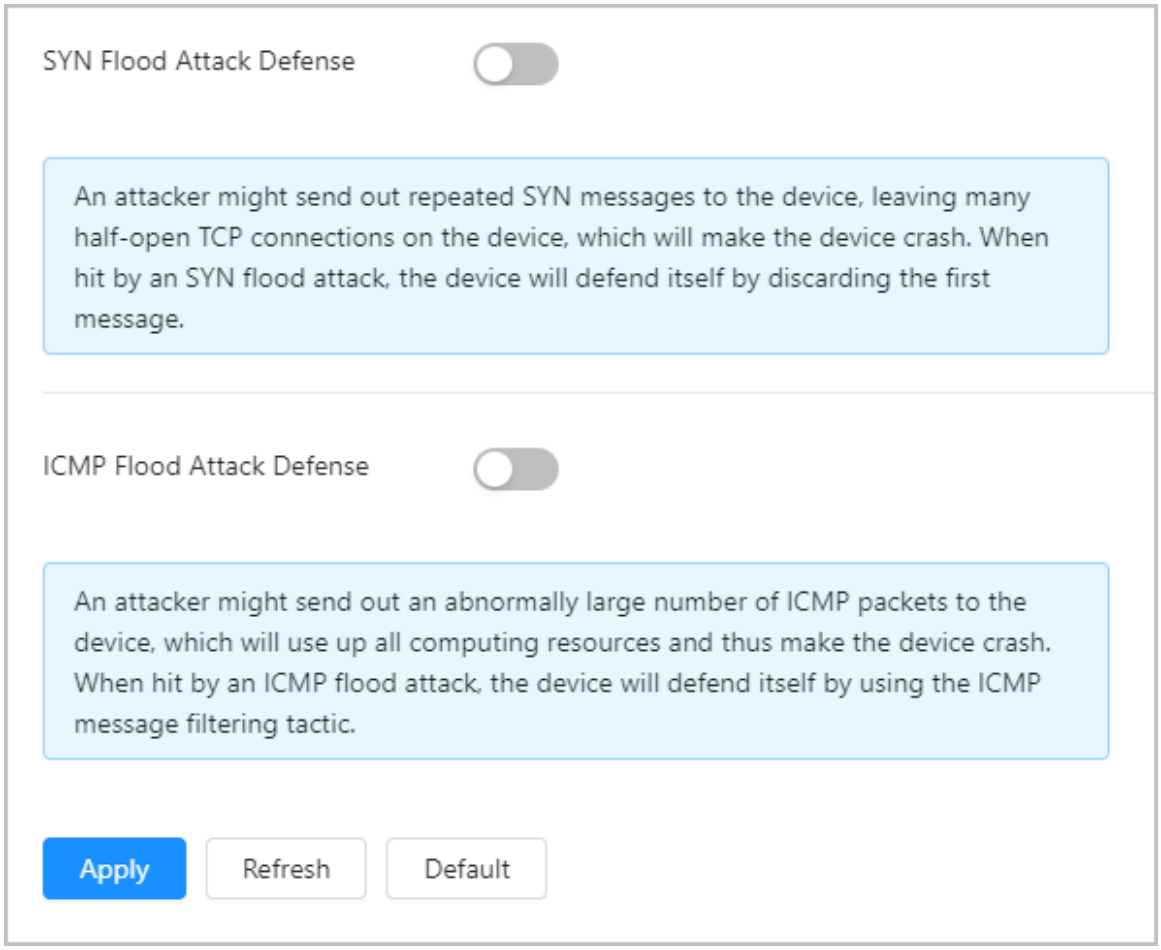
Vous pouvez activer la **Protection contre les attaques par flood SYN** (SYN Flood Attack Defense) et la **Protection contre les attaques par flood ICMP** (ICMP Flood Attack Defense) pour protéger le contrôleur d'accès contre les attaques Dos.

Procédure

Étape 1 : Sélectionnez **Sécurité > Protection contre les attaques > Protection contre les attaques par déni de service** (Security > Attack Defense > Anti-DoS Attack).

Étape 2 : Activez **Protection contre les attaques par flood SYN** (SYN Flood Attack Defense) et **Protection contre les attaques par flood ICMP** (ICMP Flood Attack Defense) pour protéger le contrôleur d'accès contre les attaques par déni de service.

Figure 2-78 Protection contre les attaques par déni de service



Étape 3 : Cliquez sur **Appliquer** (Apply).

2.2.23.4 Installation d'un certificat d'appareil

Créez un certificat ou téléchargez un certificat authentifié, puis vous pourrez vous connecter via HTTPS avec votre ordinateur.

2.2.23.4.1 Création d'un certificat

Créez un certificat pour le contrôleur d'accès.

Procédure

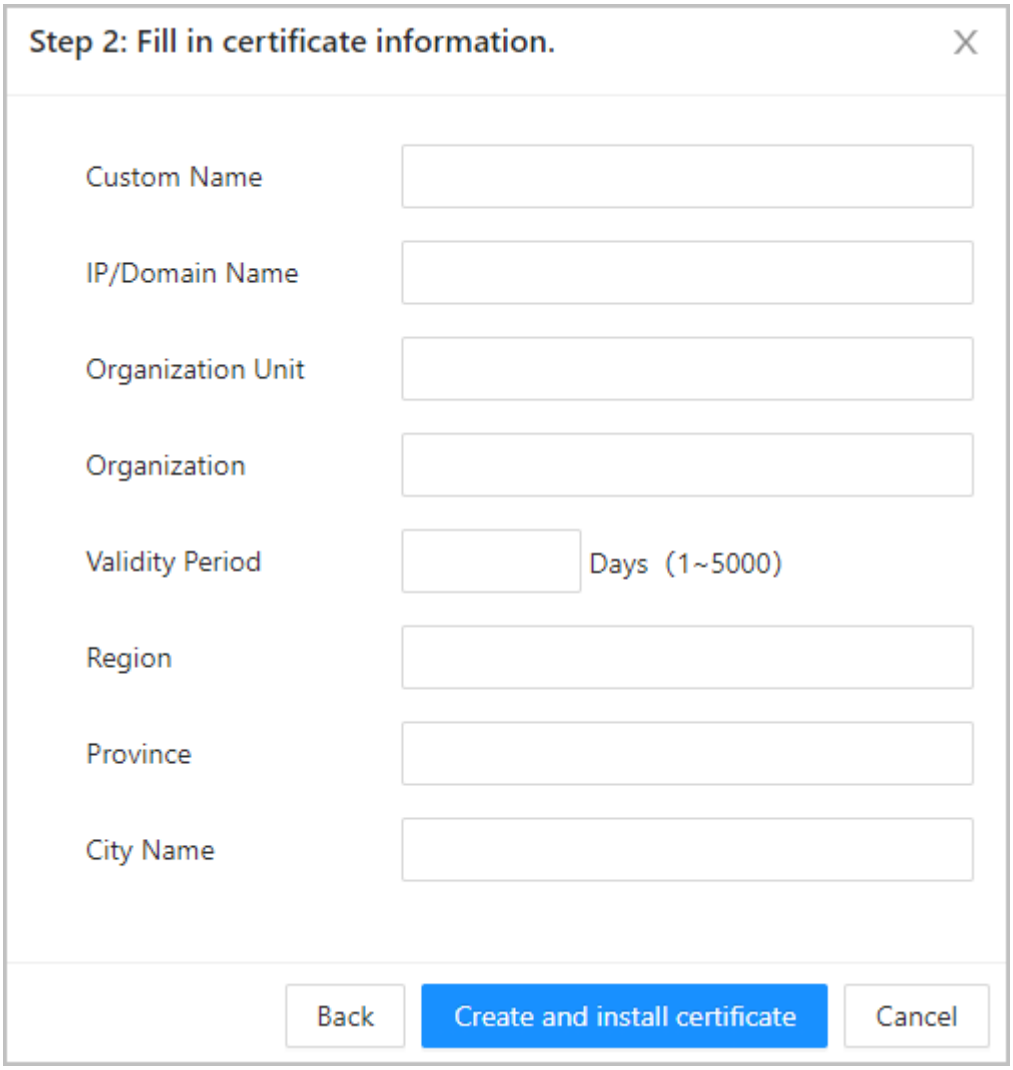
Étape 1 : Sélectionnez **Sécurité > Certificat CA > Certificat d'appareil** (Security > CA Certificate > Device Certificate).

Étape 2 : Sélectionnez **Installation d'un certificat d'appareil** (Installing Device Certificate).

Étape 3 : Sélectionnez **Créer un certificat** (Create Certificate), puis cliquez sur **Suivant** (Next).

Étape 4 : Saisissez les informations du certificat.

Figure 2-79 Informations sur le certificat



Le nom de la région ne doit pas dépasser 2 caractères. Il est recommandé de saisir l'abréviation du nom de la région.

Étape 5 : Cliquez sur **Créer et installer le certificat** (Create and install certificate).

Le nouveau certificat installé est affiché sur la page **Certificat de l'appareil** (Device Certificate) une fois que le certificat a été installé avec succès.

Opérations connexes

- Cliquez sur **Entrer en mode édition** (Enter Edit Mode) sur la page **Certificat de l'appareil** (Device Certificate) pour modifier le nom du certificat.
- Cliquez sur pour télécharger le certificat.
- Cliquez sur pour supprimer le certificat.

2.2.23.4.2 Demande et importation de certificat CA

Importez le certificat CA tiers sur le contrôleur d'accès.

Procédure

Étape 1 : Sélectionnez **Sécurité > Certificat CA > Certificat d'appareil** (Security > CA Certificate >

Device Certificate).

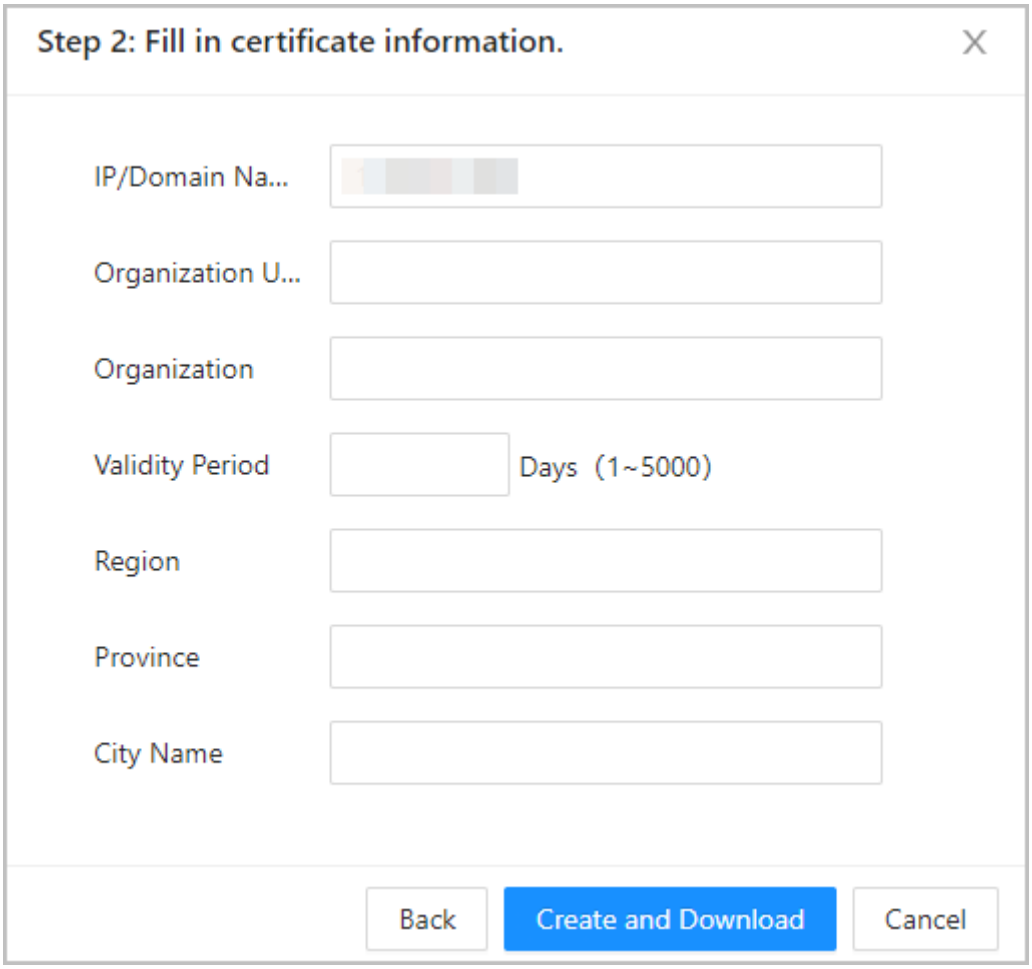
Étape 2 : Cliquez sur **Installation d'un certificat d'appareil** (Installing Device Certificate).

Étape 3 : Sélectionnez **Demander et importer un certificat CA (recommandé)** (Apply for CA Certificate and Import (Recommended)), puis cliquez sur **Suivant** (Next).

Étape 4 : Saisissez les informations du certificat.

- IP/Nom de domaine : l'adresse IP ou le nom de domaine du contrôleur d'accès.
- Région : Le nom de la région ne doit pas dépasser 3 caractères. Nous vous recommandons de saisir l'abréviation du nom de la région.

Figure 2-80 Informations du certificat (2)



Étape 5 : Cliquez sur **Créer et télécharger** (Create and Download).

Sauvegardez le fichier de demande sur votre ordinateur.

Étape 6 : Demandez le certificat à une autorité CA tierce à l'aide du fichier de demande.

Étape 7 : Importez le certificat CA signé.

1) Sauvegardez le certificat CA sur votre ordinateur.
2) Cliquez sur **Installation d'un certificat d'appareil** (Installing Device Certificate).
3) Cliquez sur **Parcourir** (Browse) pour sélectionner le certificat CA.
4) Cliquez sur **Importer et installer** (Import and Install).

   Le nouveau certificat installé est affiché sur la page **Certificat de l'appareil** (Device Certificate) une fois que le certificat a été installé avec succès.

   - Cliquez sur **Recréer** (Recreate) pour créer le fichier de requête à nouveau.
   - Cliquez sur **Importer plus tard** (Import Later) pour importer le certificat à un autre

moment.

Opérations connexes

- Cliquez sur **Entrer en mode édition** (Enter Edit Mode) sur la page **Certificat de l'appareil** (Device Certificate) pour modifier le nom du certificat.
- Cliquez sur pour télécharger le certificat.
- Cliquez sur pour supprimer le certificat.

2.2.23.4.3 Installation d'un certificat existant

Si vous disposez déjà d'un certificat et d'un fichier de clé privée, importez le certificat et le fichier de clé privée.

Procédure

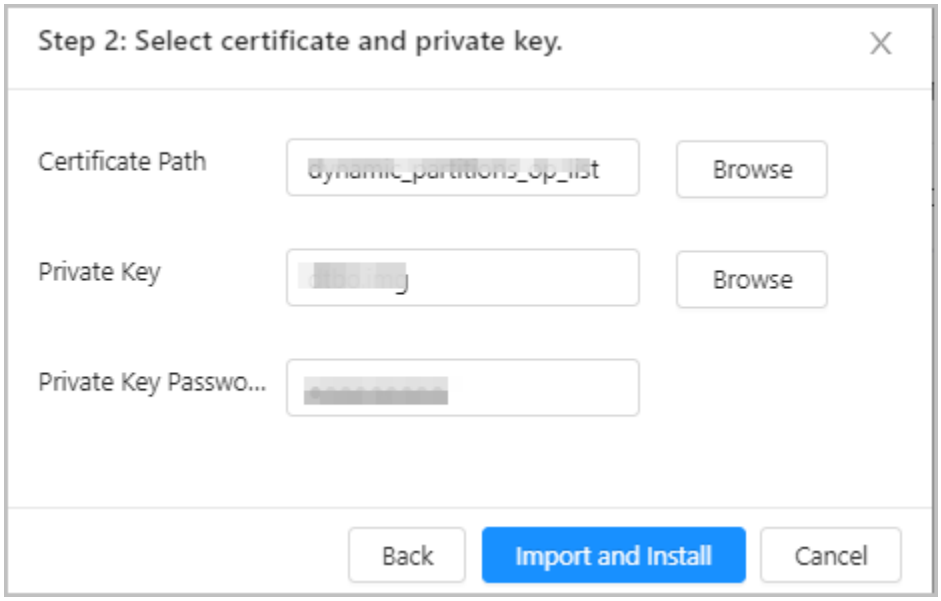
Étape 1 : Sélectionnez **Sécurité > Certificat CA > Certificat d'appareil** (Security > CA Certificate > Device Certificate).

Étape 2 : Cliquez sur **Installation d'un certificat d'appareil** (Installing Device Certificate).

Étape 3 : Sélectionnez **Installer un certificat existant** (Install Existing Certificate), puis cliquez sur **Suivant** (Next).

Étape 4 : Cliquez sur **Parcourir** (Browse) pour sélectionner le certificat et le fichier de clé privée, puis saisissez le mot de passe de la clé privée.

Figure 2-81 Certificat et clé privée



Étape 5 : Cliquez sur **Importer et installer** (Import and Install).
Le nouveau certificat installé est affiché sur la page **Certificat de l'appareil** (Device Certificate) une fois que le certificat a été installé avec succès.

Opérations connexes

- Cliquez sur **Entrer en mode édition** (Enter Edit Mode) sur la page **Certificat de l'appareil** (Device Certificate) pour modifier le nom du certificat.
- Cliquez sur pour télécharger le certificat.
- Cliquez sur pour supprimer le certificat.

2.2.23.5 Installation d'un certificat CA de confiance

Un certificat CA de confiance est un certificat numérique utilisé pour valider l'identité des sites Web et des serveurs. Par exemple, lorsque le protocole 802.1x est utilisé, le certificat CA des commutateurs est nécessaire pour authentifier leur identité.

Préambule

802.1X est un protocole d'authentification réseau qui ouvre les ports pour l'accès au réseau lorsqu'une organisation authentifie l'identité d'un utilisateur et l'autorise à accéder au réseau.

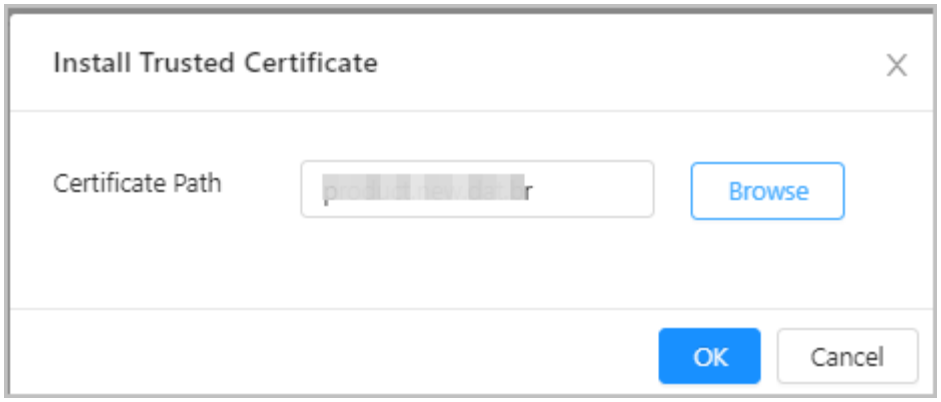
Procédure

Étape 1 : Sélectionnez **Sécurité > Certificat CA > Certificats CA de confiance** (Security > CA Certificate > Trusted CA Certificates).

Étape 2 : Sélectionnez **Installer un certificat de confiance** (Install Trusted Certificate).

Étape 3 : Cliquez sur **Parcourir** (Browse) pour sélectionner le certificat de confiance.

Figure 2-82 Installation du certificat de confiance



Étape 4 : Cliquez sur **OK**.

Le nouveau certificat installé est affiché sur la page **Certificats CA de confiance** (Trusted CA Certificates) une fois que le certificat a été installé avec succès.

Opérations connexes

- Cliquez sur **Entrer en mode édition** (Enter Edit Mode) sur la page **Certificat de l'appareil** (Device Certificate) pour modifier le nom du certificat.
- Cliquez sur pour télécharger le certificat.
- Cliquez sur pour supprimer le certificat.

2.2.23.6 Avertissement de sécurité

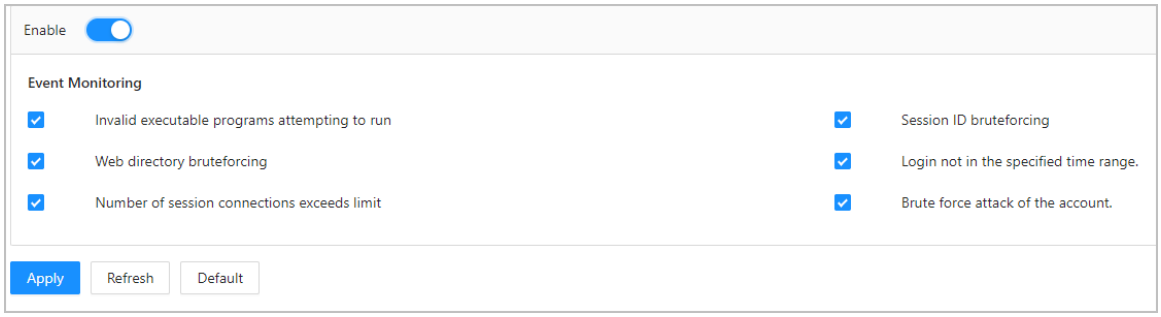
Procédure

Étape 1 : Sélectionnez **Sécurité > Certificat CA > Avertissement de sécurité** (Security > CA Certificate > Security Warning).

Étape 2 : Activez la fonction d'avertissement de sécurité.

Étape 3 : Sélectionnez les éléments de surveillance.

Figure 2-83 Avertissement de sécurité



Étape 4 : Cliquez sur **Appliquer** (Apply).

2.3 Configurations du sous-contrôleur

Vous pouvez vous connecter à la page Web du sous-contrôleur pour le configurer localement.

2.3.1 Initialisation

Initialisez le sous-contrôleur lorsque vous vous connectez à la page Web pour la première fois ou après avoir rétabli les paramètres d'usine par défaut du sous-contrôleur. Pour plus de détails sur l'initialisation du sous-contrôleur, reportez-vous à la section « 2.2.2 Initialisation ».

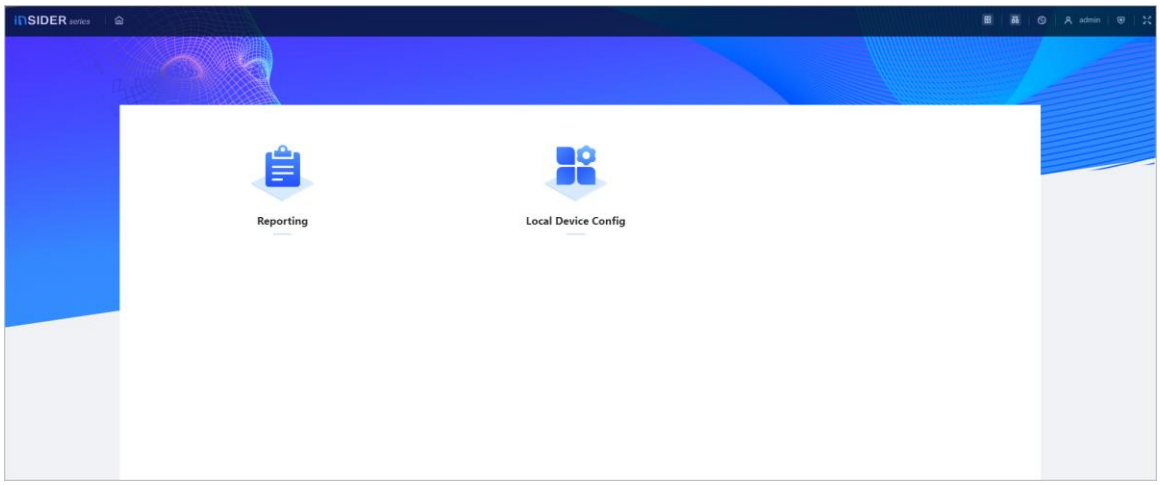
2.3.2 Connexion

Réglez le contrôle d'accès au sous-contrôleur lors de l'exécution de l'assistant de connexion. Pour les détails, voir « 2.2.3 Connexion ».

2.3.3 Page d'accueil

La page Web du sous-contrôleur ne comprend que les menus **Config. de l'appareil local** (Local Device Config) et **Rapports** (Reporting). Pour plus de détails, reportez-vous à « 2.2.21 Configurations des appareils locaux (en option) » et « 2.2.22 Affichage des enregistrements ».

Figure 2-84 Page d'accueil

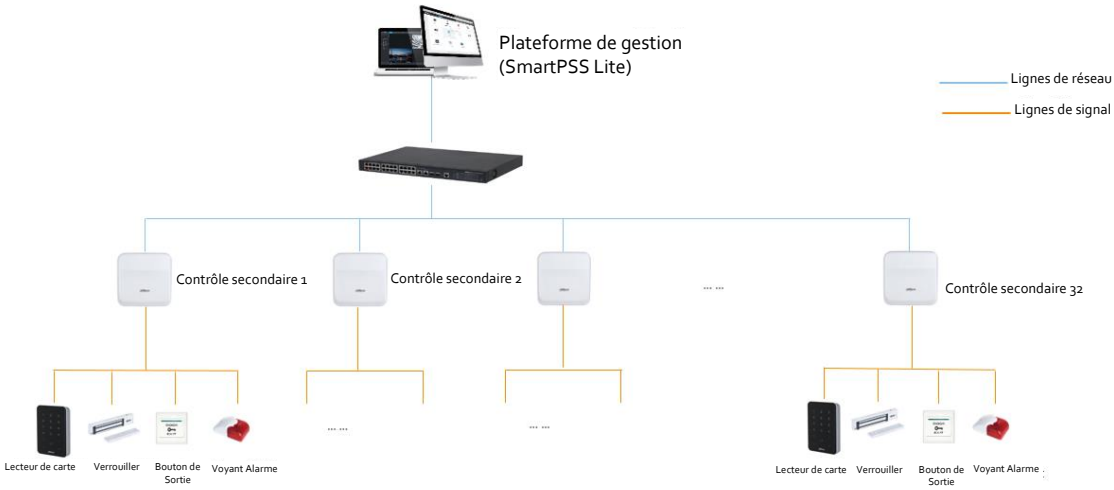


3 Sous-contrôleurs Smart PSS Lite

3.1 Schéma du réseau

Les sous-contrôleurs sont ajoutés à une plateforme de gestion autonome, telle que SmartPSS Lite. Vous pouvez gérer tous les sous-contrôleurs via SmartPSS Lite.

Figure 3-1 Schéma de la mise en réseau



3.2 Configurations sur SmartPSS Lite

Ajoutez des sous-contrôleurs à SmartPSS Lite et configurez-les sur la plateforme. Pour plus de détails, consultez le manuel d'utilisation de SmartPSS Lite.

3.3 Configurations du sous-contrôleur

Pour les détails, voir « 2.3 Configurations du sous-contrôleur ».

Annexe 1 – Recommandations en matière de cybersécurité

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

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

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

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

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

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

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

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

1. **Protection matérielle**

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

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

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

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

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

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

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

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

13. **Construire un environnement réseau sécurisé**

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

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

En savoir plus

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

POUR UNE SOCIÉTÉ PLUS SÛRE ET UNE VIE PLUS INTELLIGENTE

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Adresse : No. 1399, Binxing Road, Binjiang District, Hangzhou, R.P. Chine | Site Web : www.dahuasecurity.com | Code postal : 310053
Adresse e-mail : dhoverseas@dhvisiontech.com | Tél. : +86-571-87688888 28933188