Boîtier métallique de contrôle d’accès

Manuel d’utilisation

V1.0.0

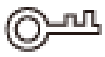
Avant-propos

Généralités

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

Précautions d'emploi

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

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

Historique des révisions

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

Avis de protection de la confidentialité

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

À propos du manuel

- Le manuel est donné uniquement à titre de référence. De légères différences peuvent être constatées entre le manuel et le produit.
- Nous ne sommes pas responsables des pertes encourues en raison d'une exploitation du produit

de manière non conforme au manuel.

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

Précautions et avertissements importants

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

Conditions de transport requises

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

Conditions requises pour le stockage

Stockez le boîtier métallique dans les conditions d'humidité et de température autorisées.

Conditions d'installation requises

 **AVERTISSEMENT**

- Ne connectez pas l'adaptateur d'alimentation au boîtier métallique 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 d'alimentation du boîtier métallique.
- Ne connectez pas le boîtier métallique à deux ou plusieurs sources d'alimentation électrique pour éviter de l'endommager.
- 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 boîtier métallique à un endroit exposé à la lumière du soleil ou proche de sources de chaleur.
- Gardez le boîtier métallique à l'écart de l'humidité, de la poussière et de la suie.
- Installez le boîtier métallique sur une surface stable afin d'éviter toute chute.
- Installez le boîtier métallique 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 boîtier métallique.
- Le boîtier métallique est un équipement électrique de classe I. Assurez-vous que le bloc d'alimentation du boîtier métallique 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 boîtier métallique alors que l'adaptateur est sous tension.
- Utilisez le boîtier métallique dans la plage nominale d'entrée et de sortie d'alimentation.
- Utilisez l'appareil dans les conditions d'humidité et de température autorisées.
- Évitez d'exposer le boîtier métallique aux gouttes ou aux éclaboussures de liquides. Ne placez aucun objet contenant un liquide sur le boîtier métallique afin d'éviter que ce liquide n'y pénètre.
- Ne démontez pas le boîtier métallique sans instructions d'un professionnel.

Table des matières

1 Introduction au produit

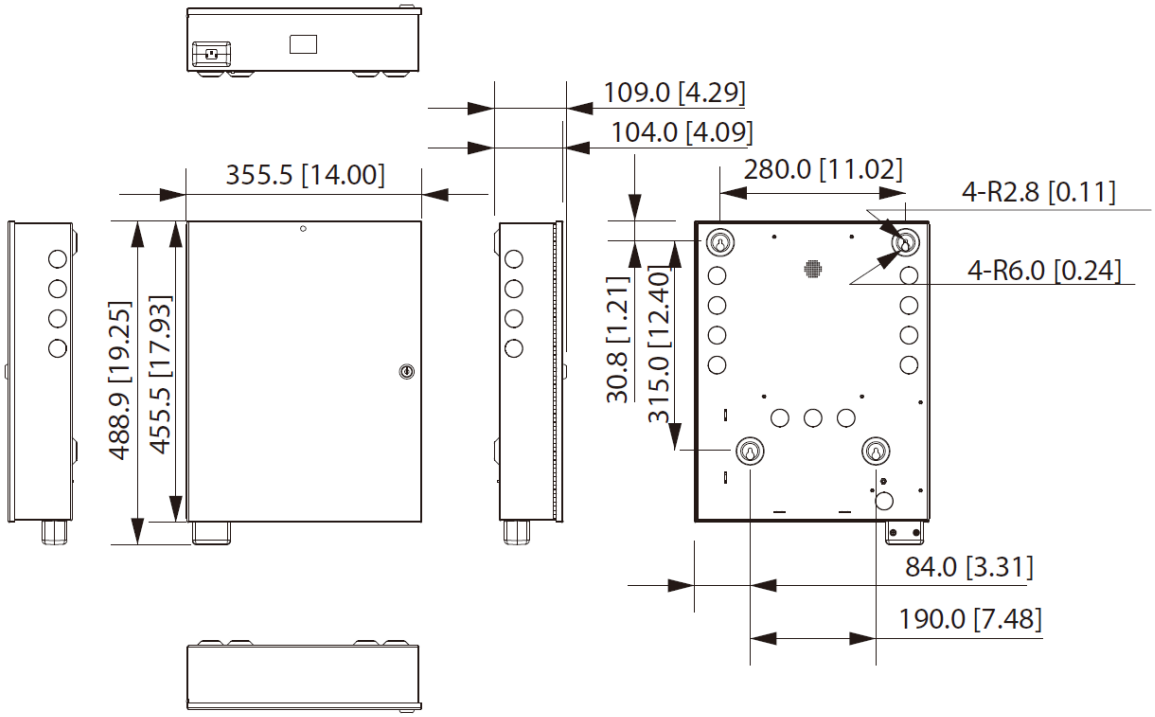
Le boîtier métallique est conçu pour abriter le contrôleur d'accès dans une enceinte élégante et protectrice, idéale pour les parcs commerciaux, les communautés, etc.

- Fabriqué en tôle d'acier galvanisé, il est élégant et durable.
- Il peut être alimenté par le réseau électrique et par sa batterie de stockage.
- Le disjoncteur à air intégré limite le courant et protège l'appareil contre les fuites d'électricité et les courts-circuits.
- Illuminateur intégré.
- Prend en charge la mise à jour du micrologiciel lorsqu'il est utilisé avec le contrôleur d'accès. Cette fonction est uniquement disponible sur certains modèles de contrôleur d'accès.
- Signale plusieurs types d'événements, tels que les pannes de courant, le rétablissement du courant et les manipulations, lorsqu'il est utilisé avec le contrôleur d'accès. Cette fonction est uniquement disponible sur certains modèles de contrôleur d'accès.
- Émet des alarmes anti-sabotage lorsqu'il est utilisé avec le contrôleur d'accès. Cette fonction est uniquement disponible sur certains modèles de contrôleur d'accès.

2 Dimensions

La figure ci-dessous indique les dimensions à respecter lors de la planification de l'installation du boîtier métallique.

Figure 2-1 Dimensions (mm[pouces])



3 Apparence

Figure 3-1 Présentation

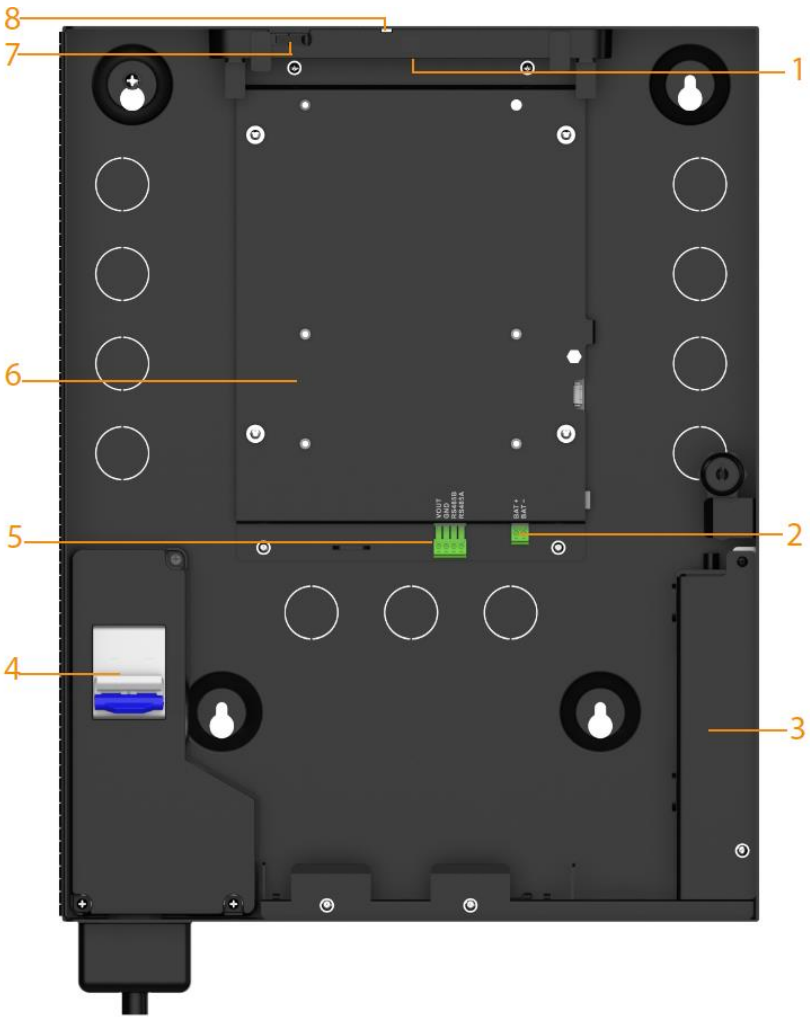


Tableau 3-1 Description des paramètres

N°	Fonction du module	
1	Éclairage	La lumière de l'illuminateur s'allume lorsque le boîtier de montage mural est ouvert et s'éteint lorsque le boîtier est fermé.
2	Batteries de Stockage	• BAT+ : Entrée d'alimentation (12 V, 7 AH) • BAT- : Mise à la terre
3	Adaptateur d'alimentation	Convertit le courant alternatif (CA) entrant de votre prise de courant en une sortie de 15 V CC et le courant maximum est de 4 A. Alimente la carte de transfert de puissance.
4	Disjoncteur	Un disjoncteur est un commutateur électrique conçu pour protéger les systèmes électriques contre les dommages causés par les fuites de courant, les courts-circuits et les surcharges.

N°	Fonction du module	
5	RS-485	● RS-485AB : Communique avec le contrôleur d'accès ● VOUT : Alimente le contrôleur d'accès. ● GND : Mise à la terre
6	Carte de l'adaptateur secteur	Alimente le contrôleur d'accès et communique avec lui.
7	Anti-antisabotage	Une alarme anti-sabotage est déclenchée en cas de sabotage.
8	Voyant d'alimentation	L'indicateur est rouge lorsque le boîtier métallique est sous tension.

4 Câblage

Figure 4-1 Schéma du contrôleur d'accès basé sur le Web

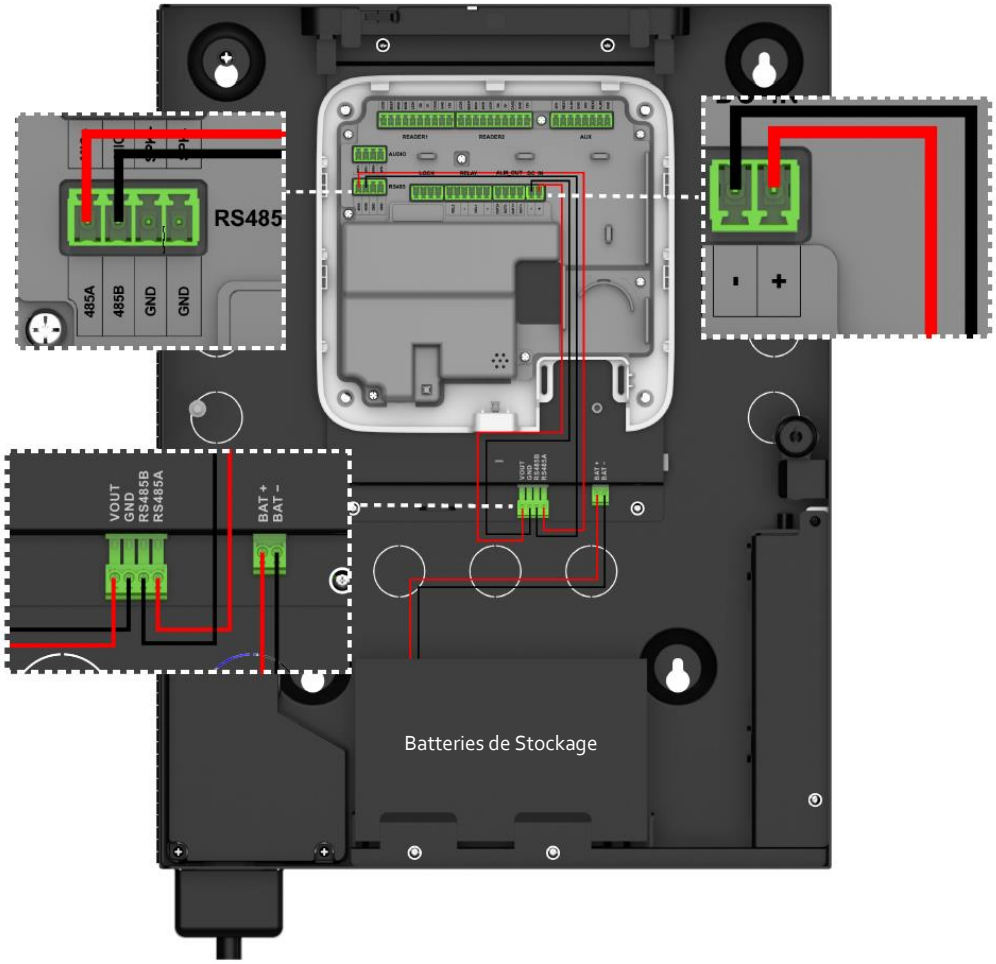


Figure 4-2 Essai du contrôleur d'accès (B) (modèle long)

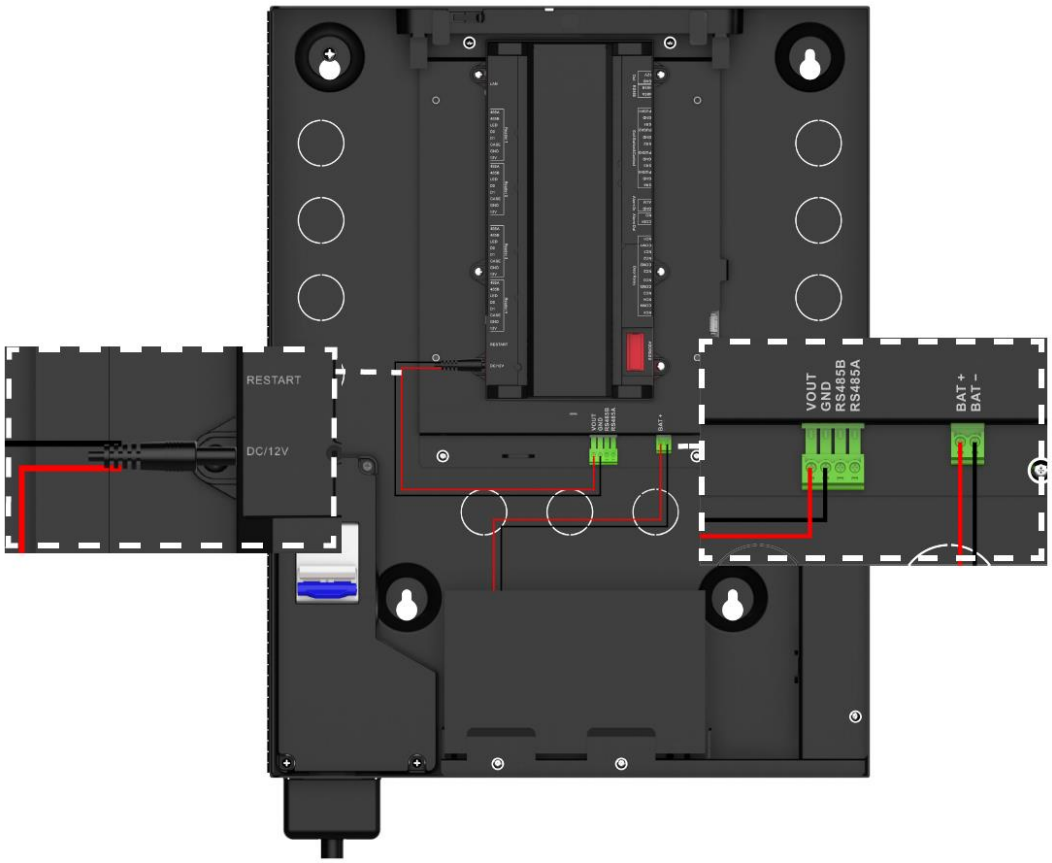
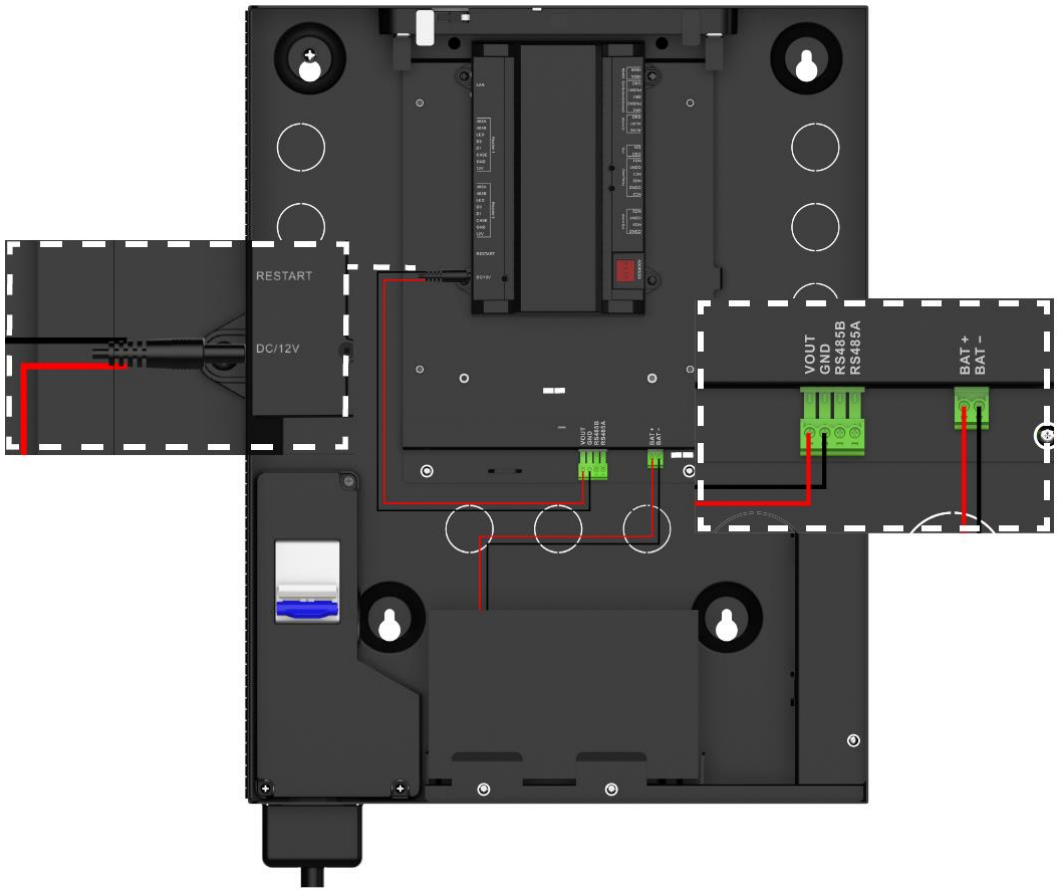


Figure 4-3 Essai du contrôleur d'accès (B) (modèle court)



5 Procédure d’installation

L’installation prend en charge le câblage encastré et le câblage en saillie. Cette section se base sur le câblage encastré ci-dessus comme exemple.

Procédure

Étape 1 : Connectez le cordon d’alimentation au port d’alimentation du boîtier métallique, puis vissez 2 vis pour fixer le protecteur du cordon d’alimentation au boîtier métallique.

Étape 2 : Mettez à niveau et marquez les quatre trous de montage sur la surface de montage. Reportez-vous aux dimensions approximatives indiquées dans « 2 Dimensions » pour une planification et une installation correctes.

Étape 3 : Percez les 4 trous de montage marqués sur la surface de montage, puis insérez-y 4 tubes d’expansion.

Figure 5-1 Trous de perçage (câblage encastré)

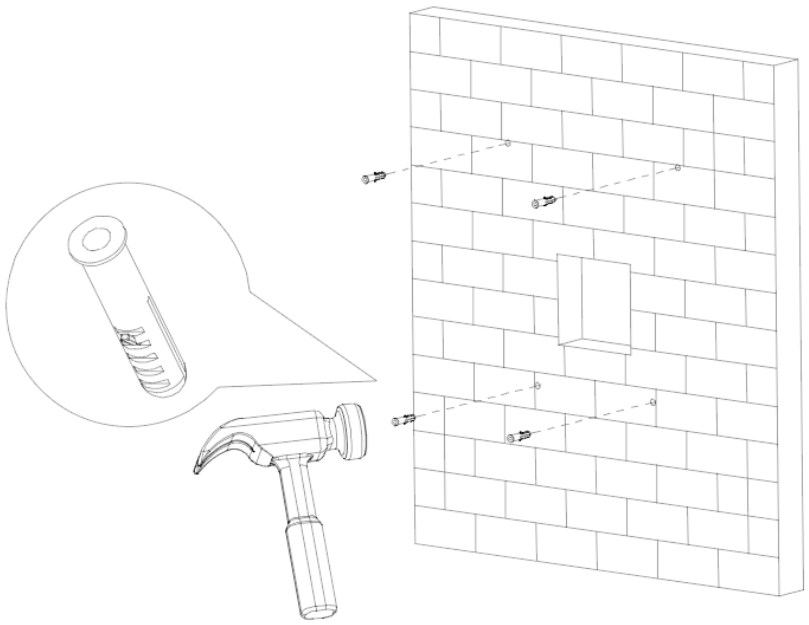
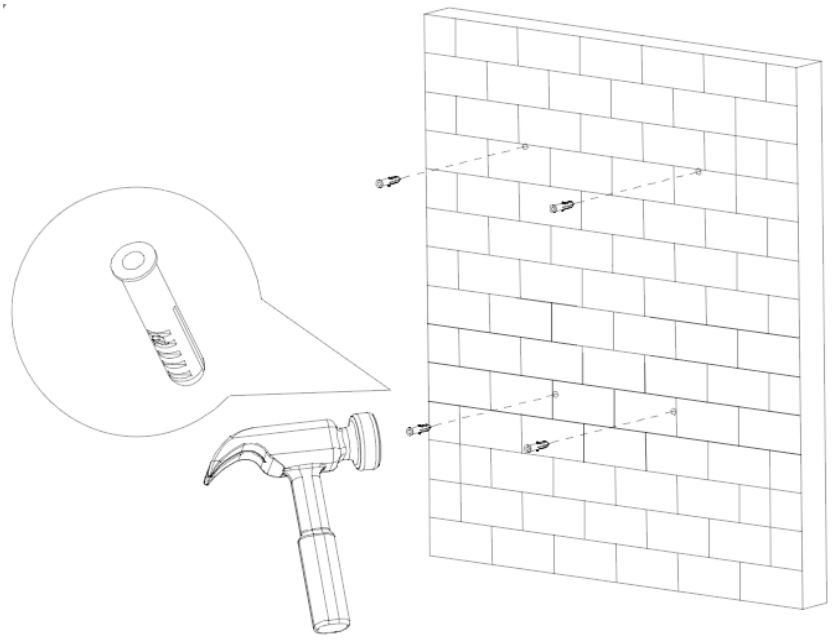
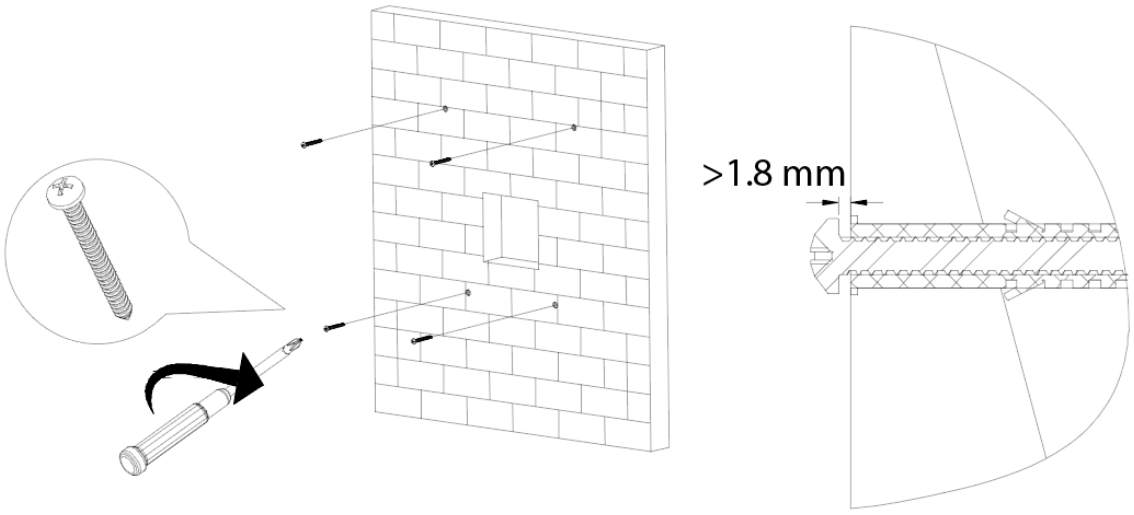


Figure 5-2 Trous de perçage (câblage en saillie)



Étape 4 : Vissez 4 vis à expansion dans les tubes d'expansion, en laissant suffisamment d'espace pour suspendre le boîtier métallique.

Figure 5-3 Vissage de 4 vis à expansion



Étape 5 : Appuyez sur le bord d'un tournevis sur le bord estampé de la débouchure le plus à l'intérieur pour écarter doucement la débouchure du boîtier métallique.

Une « débouchure » (knock out) ou « KO » est une ouverture partiellement estampée dans le boîtier métallique pour faire passer des fils ou des câbles. Il est probable qu'il y ait plusieurs débouchures de tailles différentes dans le boîtier métallique. Choisissez celui qui sera le plus facile pour connecter les fils ou les câbles.

Étape 6 : Faites passer les fils à travers les débouchures et dans l'ouverture du mur.

Figure 5-4 Retrait des débouchures et câblage du boîtier métallique (câblage encastré)

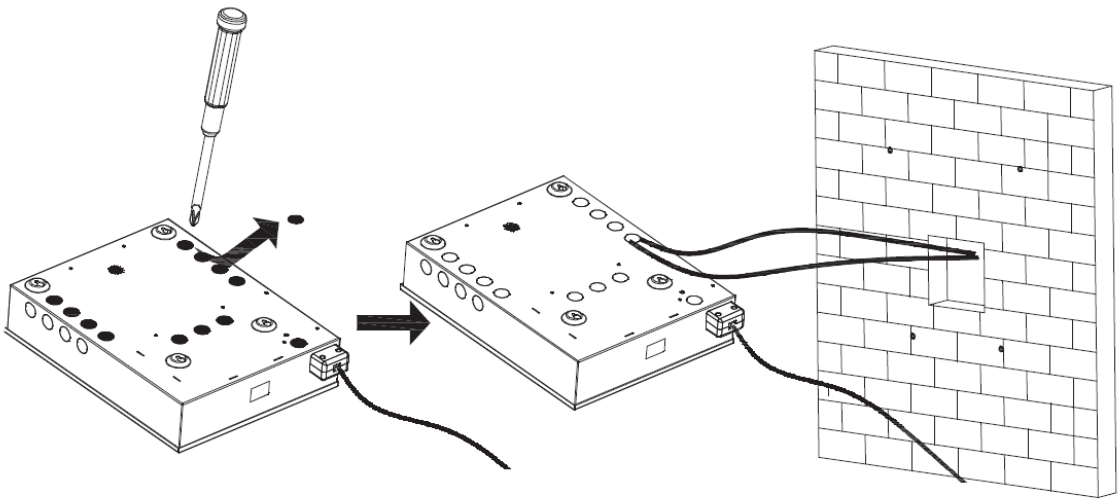
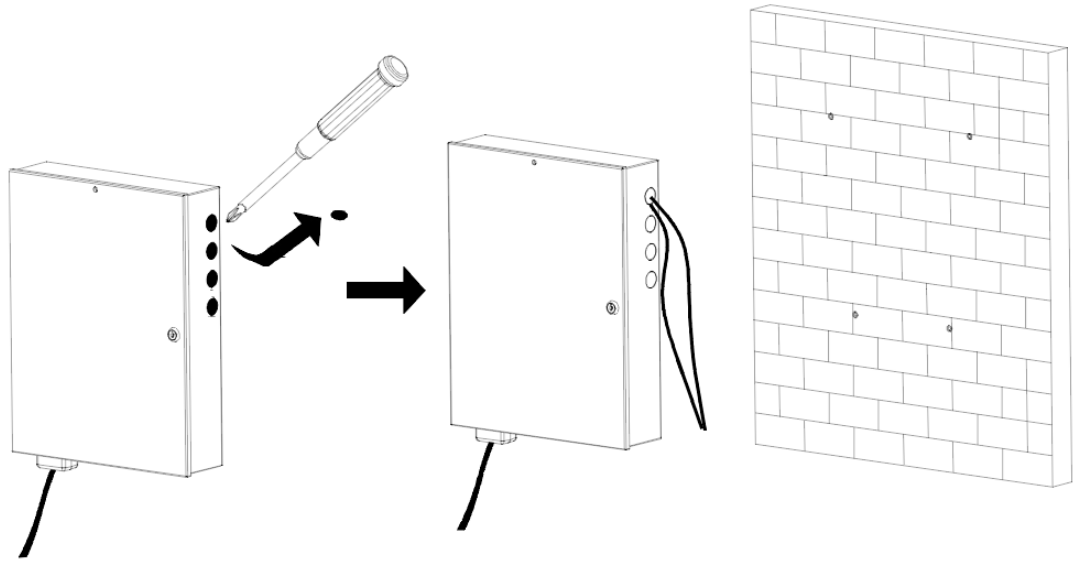


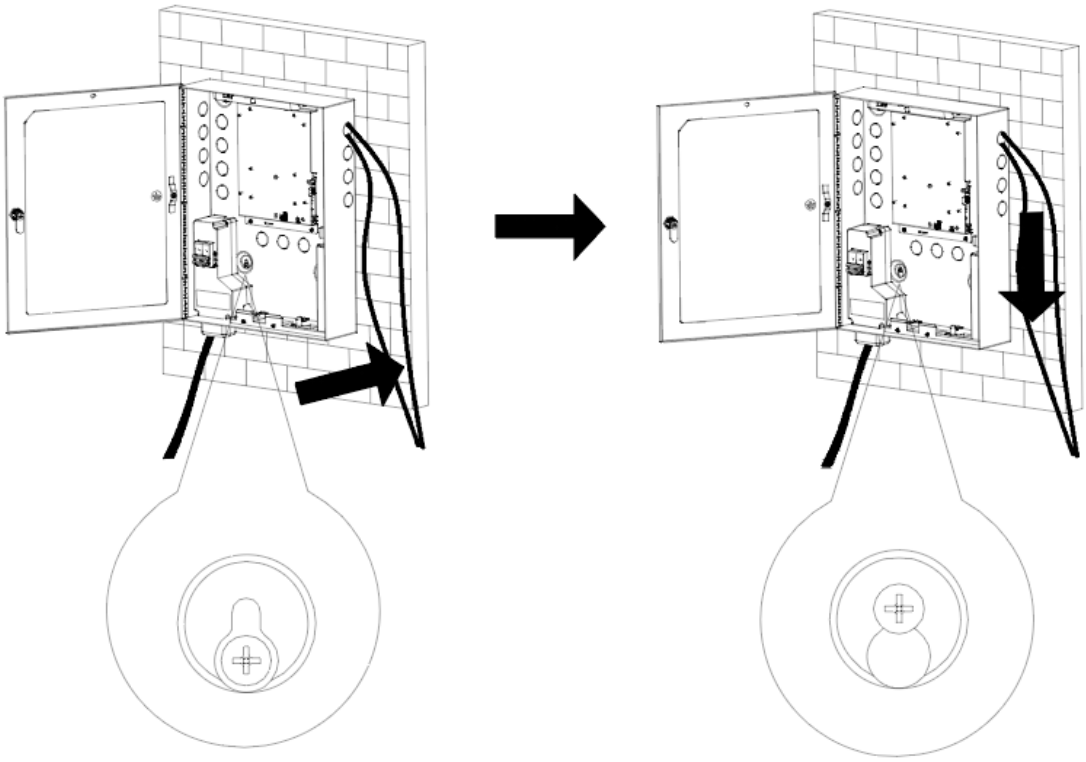
Figure 5-5 Retrait des débouchures et câblage du boîtier métallique (câblage en saillie)



Étape 7 : Alignez les 4 encoches du boîtier métallique sur les 4 vis installées, puis fixez le boîtier métallique aux vis.

Étape 8 : Faites glisser doucement le boîtier métallique vers le bas jusqu'à ce que les 4 vis soient en haut de chaque encoche.

Figure 5-6 Glissement du boîtier vers le bas



Étape 9 : Serrez les 4 vis et verrouillez le boîtier métallique à l'aide de la clé.

6 Configuration sur la page Web

Lorsque le boîtier métallique fonctionne avec le contrôleur d'accès, il peut se connecter au contrôleur d'accès par RS-485, ce qui permet d'envoyer les événements du boîtier métallique à la page Web du contrôleur d'accès, tels que les événements anti-sabotage, les pannes d'électricité principale et les événements de rétablissement de l'électricité principale. Vous pouvez également mettre à jour le système du boîtier métallique à travers le contrôleur d'accès.

Préambule

Cette fonction est uniquement disponible sur certains modèles de contrôleur d'accès.

Procédure

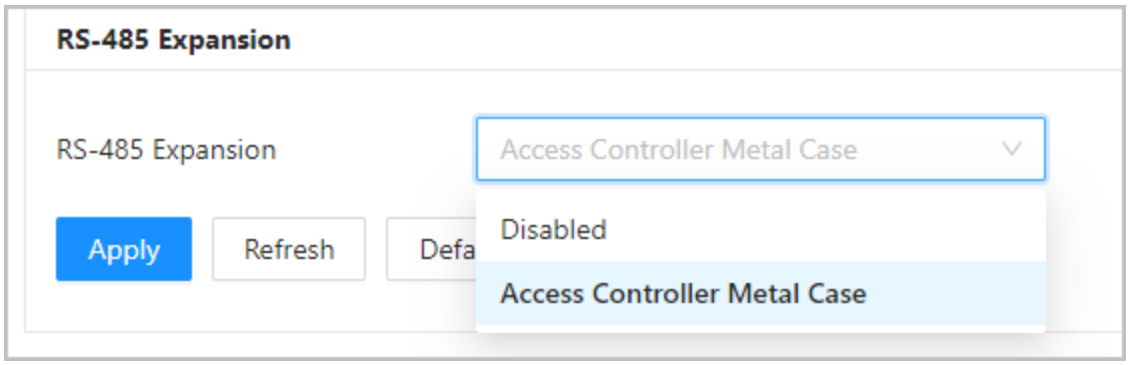
Étape 1 : Connectez-vous à la page Web du contrôleur d'accès.

Étape 2 : Accédez à **Config. de l'appareil local > Paramètres avancés > Expansion RS-485** (Local Device Config > Advanced Settings > RS-485 Expansion).

Étape 3 : Sélectionnez **Boîtier métallique du contrôleur d'accès** (Access Controller Metal Case).

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

Figure 6-1 Configuration du boîtier métallique sur la page Web



Annexe 1 – Recommandations en matière de cybersécurité

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.