Cititor proximitate Dahua ASR2201A-D

Manualul utilizatorului

V1.0.3

cuvânt înainte

General

Acest manual prezintă funcțiile și operațiunile Access Reader (denumit în continuare cititor de carduri). Citiți cu atenție înainte de a utiliza dispozitivul și păstrați manualul în siguranță pentru referințe ulterioare.

Instructiuni de siguranta

Următoarele cuvinte de semnalizare pot apărea în manual.

Cuvinte semnal	Sens
DANGER	Indică un pericol potențial ridicat care, dacă nu este evitat, va duce la moarte sau vătămări grave.
WARNING	Indică un pericol potențial mediu sau scăzut care, dacă nu este evitat, ar putea duce la răniri ușoare sau moderate.
CAUTION	Indică un risc potențial care, dacă nu este evitat, ar putea duce la daune materiale, pierderi de date, reduceri de performanță sau rezultate imprevizibile.
TIPS	Oferă metode care vă ajută să rezolvați o problemă sau să economisiți timp.
NOTE	Oferă informații suplimentare ca supliment la text.

Istoricul revizuirilor

Versiune	Conținutul revizuirii	Timpul de eliberare
V1.0.3	S-a actualizat metoda de deblocare.	martie 2023
V1.0.2	S-au adăugat metode de deblocare și actualizare a sistemului.	decembrie 2022
V1.0.1	Modele de dispozitive actualizate.	decembrie 2021
V1.0.0	Prima aparitie.	octombrie 2020

Notificare privind protecția confidențialității

În calitate de utilizator al dispozitivului sau controlor de date, este posibil să colectați datele personale ale altora, cum ar fi fața lor, amprentele și numărul plăcuței de înmatriculare. Trebuie să respectați legile și reglementările locale privind protecția vieții private pentru a proteja drepturile și interesele legitime ale altor persoane prin implementarea unor măsuri care includ, dar nu sunt limitate: Furnizarea unei identificări clare și vizibile pentru a informa oamenii despre existența zonei de supraveghere și furnizați informațiile de contact necesare.

Despre Manual

- Manualul este doar pentru referință. Pot fi găsite mici diferențe între manual și produs.
- Nu suntem răspunzători pentru pierderile suferite din cauza utilizării produsului în moduri care nu sunt în conformitate cu manualul.
- Manualul va fi actualizat în conformitate cu cele mai recente legi și reglementări ale jurisdicțiilor aferente. Pentru informații detaliate, consultați manualul de utilizare pe hârtie, utilizați CD-ROM-ul nostru, scanați codul QR sau vizitați

site-ul nostru oficial. Manualul este doar pentru referință. S-ar putea găsi mici diferențe între versiunea electronică și versiunea pe hârtie.

- Toate modelele și software-ul pot fi modificate fără notificare prealabilă în scris. Actualizările de produs pot duce la apariția unor diferențe între produsul real și manual. Vă rugăm să contactați serviciul pentru clienți pentru cel mai recent program și documentație suplimentară.
- Pot exista erori în imprimare sau abateri în descrierea funcțiilor, operațiunilor și datelor tehnice. Dacă există vreo îndoială sau dispută, ne rezervăm dreptul la explicații finale.
- Actualizați software-ul de citire sau încercați alt software de citire general dacă manualul (în format PDF) nu poate fi deschis.
- Toate mărcile comerciale, mărcile comerciale înregistrate și numele companiilor din manual sunt proprietăți ale proprietarilor respectivi.
- Vă rugăm să vizitați site-ul nostru web, să contactați furnizorul sau serviciul pentru clienți dacă apar probleme în timpul utilizării dispozitivului.
- Dacă există vreo incertitudine sau controversă, ne rezervăm dreptul la explicații finale.

Măsuri de protecție și avertismente importante

Această secțiune prezintă conținut care acoperă manipularea corectă a cititorului de carduri, prevenirea pericolelor și prevenirea daunelor materiale. Citiți cu atenție înainte de a utiliza cititorul de carduri și respectați instrucțiunile atunci când îl utilizați.

Cerința de transport

Transportați, utilizați și depozitați cititorul de carduri în condiții de umiditate și temperatură permise.

Cerință de stocare

Păstrați cititorul de carduri în condiții de umiditate și temperatură permise.

Cerințe de instalare

 WARNING

- Nu conectați adaptorul de alimentare la cititorul de carduri în timp ce adaptorul este pornit.
- Respectați cu strictețe codul și standardele locale de siguranță electrică. Asigurați-vă că tensiunea ambientală este stabilă și îndeplinește cerințele de alimentare ale controlerului de acces.
- Nu conectați cititorul de carduri la două sau mai multe tipuri de surse de alimentare, pentru a evita deteriorarea cititorului de carduri.
- Utilizarea necorespunzătoare a bateriei poate duce la un incendiu sau o explozie.

- Personalul care lucrează la înălțime trebuie să ia toate măsurile necesare pentru a asigura siguranța personală, inclusiv purtarea căștii și a centurilor de siguranță.
- Nu așezați cititorul de carduri într-un loc expus la lumina soarelui sau în apropierea surselor de căldură.
- Țineți cititorul de carduri departe de umiditate, praf și funingine.
- Instalați cititorul de carduri pe o suprafață stabilă pentru a preveni căderea acestuia.
- Instalați cititorul de carduri într-un loc bine ventilat și nu blocați ventilația acestuia.
- Utilizați un adaptor sau o sursă de alimentare cu dulap furnizată de producător.
- Utilizați cablurile de alimentare recomandate pentru regiune și conform specificațiilor privind puterea nominală.
- Sursa de alimentare trebuie să respecte cerințele ES1 din standardul IEC 62368-1 și să nu fie mai mare decât PS2. Vă rugăm să rețineți că cerințele de alimentare sunt supuse etichetei Card Reader.
- Cititorul de carduri este un aparat electric de clasa I. Asigurați-vă că sursa de alimentare a cititorului de carduri este conectată la o priză cu împământare de protecție.

Cerințe de funcționare

- Verificați dacă sursa de alimentare este corectă înainte de utilizare.
- Nu deconectați cablul de alimentare de pe partea laterală a cititorului de carduri în timp ce adaptorul este pornit.
- Utilizați cititorul de carduri în intervalul nominal de putere de intrare și de ieșire.
- Utilizați cititorul de carduri în condiții de umiditate și temperatură permise.

- Nu scăpați și nu stropiți cu lichid pe cititorul de carduri și asigurați-vă că nu există niciun obiect plin cu lichid pe cititorul de carduri pentru a preveni curgerea lichidului în acesta.
- Nu dezasamblați cititorul de carduri fără instrucțiuni profesionale.

Cuprins

1. Introducere

1.1 Caracteristici

- Material PC și panou acrilic cu un design subțire și rezistent la apă.
- Suporta citirea cardurilor fara contact.
- Suportă citirea cardului IC (Mifare), citirea cardului de identitate (numai pentru cititorul de carduri cu funcție de citire a cardului de identitate) și citirea codului QR (numai pentru cititorul de carduri cu funcție de citire a codului QR).
- Acceptă comunicarea prin RS–485 și Wiegand (cititorul de carduri de amprente și cititorul de coduri QR acceptă doar RS–485).
- Acceptă actualizarea online.
- Suporta alarma de manipulare.
- Buzer și indicator luminos încorporat.
- Watchdog încorporat pentru a asigura stabilitatea cititorului de carduri.
- Sigur și stabil cu protecție la supracurent și supratensiune.

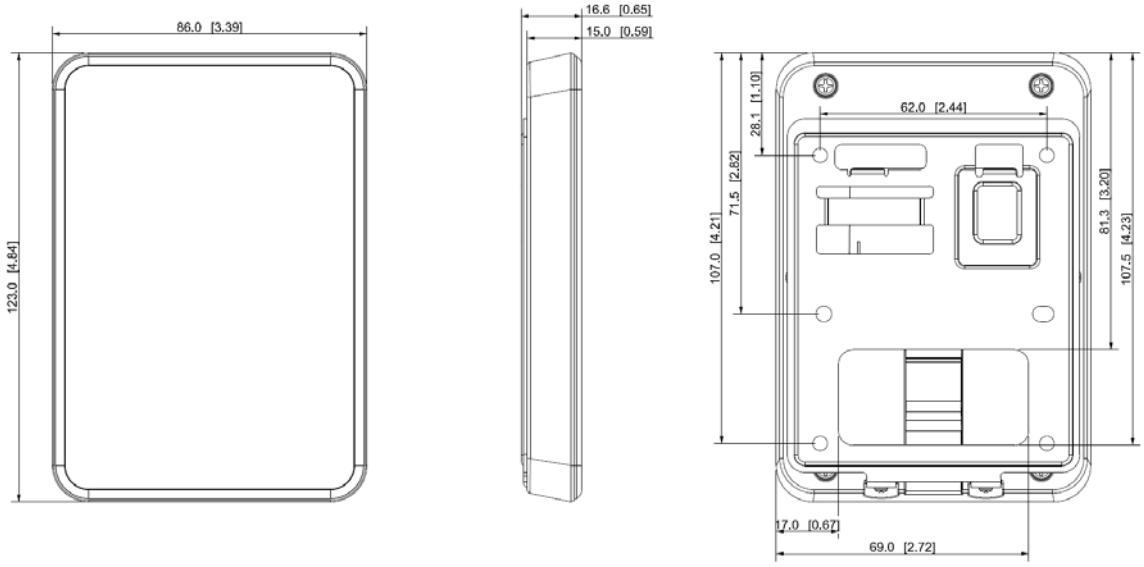
Funcțiile pot varia în funcție de diferite modele.

1.2 Aspectul

Cititorul de carduri poate fi împărțit în model cu 86 de cutii, model subțire și modul de amprentă, în funcție de aspectul lor.

1.2.1 86 Box Model

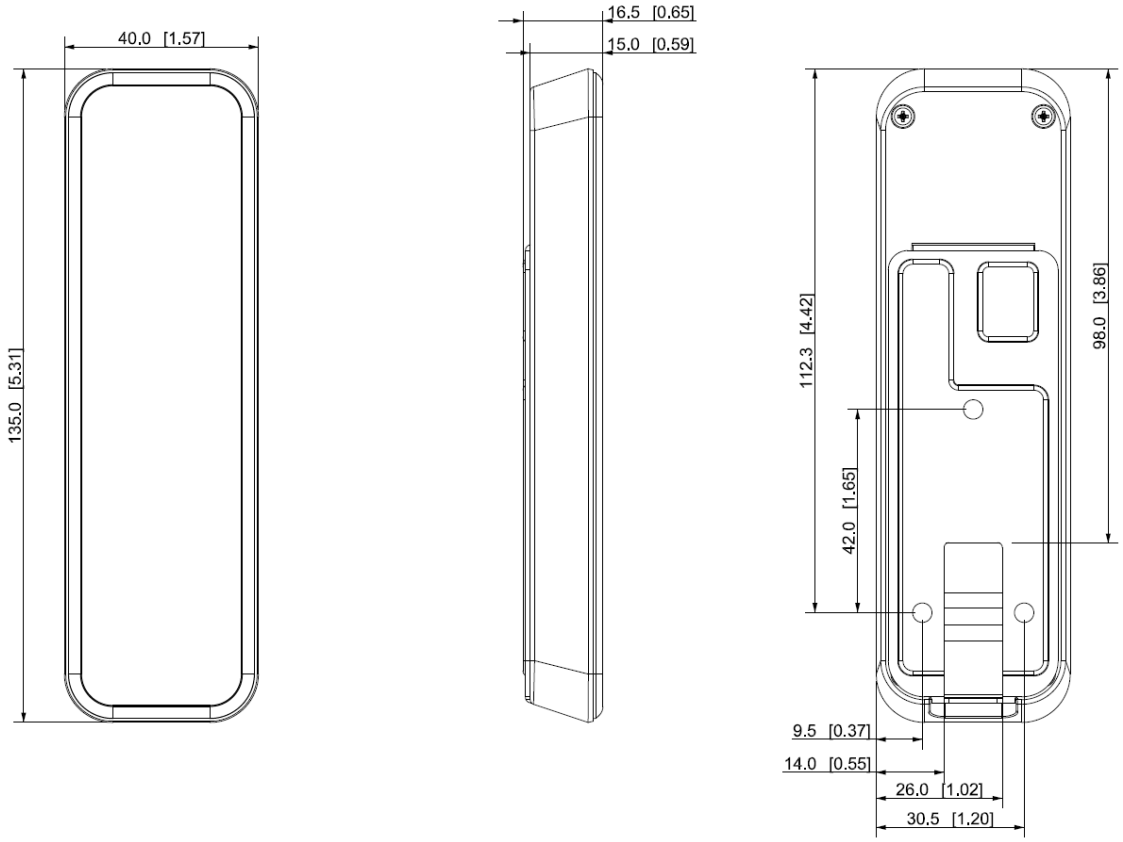
Figura 1-1 Dimensiunile modelului de cutie 86 (mm [inch])



Modelul cu 86 de casete poate fi împărțit în continuare în cititor de carduri cu coduri QR și cititor de carduri general conform funcţiilor lor.

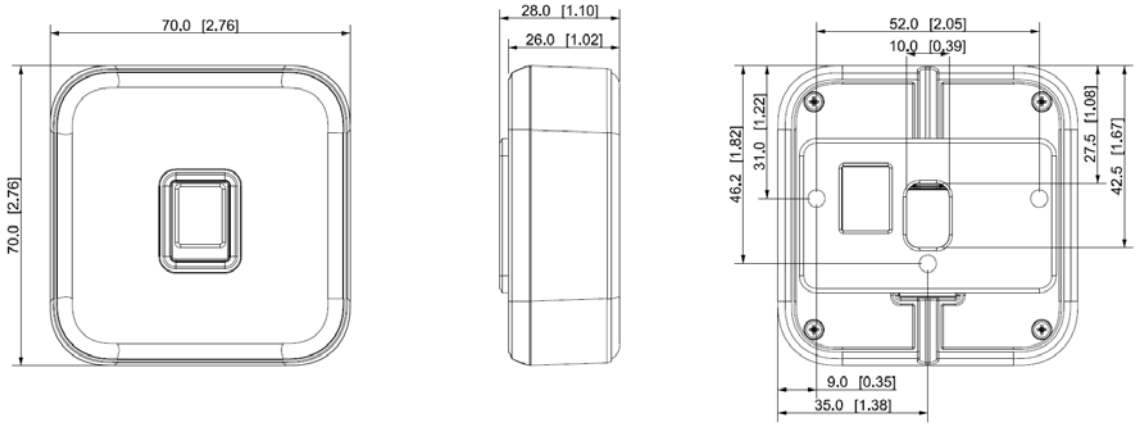
1.2.2 Model Slim

Figura 1-2 Dimensiunile modelului subțire (mm [inch])



1.2.3 Modelul de amprentă

Figura 1-3 Dimensiunile modelului de amprentă (mm [inch])



Prezentare generală a 2 porturi

Utilizați RS–485 sau Wiegand pentru a conecta cititorul de carduri. Numai modelul de amprentă digitală și modelul de cod QR suport RS–485.

Cabluri cu 8 fire pentru modelele 86 Box și Slim

Tabel 2-1 Descrierea conexiunii cablului (1)

Culoare	Port	Descriere
roșu	RD+	PWR (12 VDC)
Negru	RD–	GND
Albastru	CAZ	Semnal de alarmă de manipulare
alb	D1	Semnal de transmisie Wiegand (eficient numai atunci când se utilizează protocolul Wiegand)
Verde	D0	
Maro	LED	Semnal de răspuns Wiegand (eficient numai când se utilizează protocolul Wiegand)
Galben	RS–485_B	
Violet	RS–485_A	

Cabluri cu 5 fire pentru modelul de amprentă digitală

Tabel 2-2 Descrierea conexiunii cablului (2)

Culoare	Port	Descriere
roșu	RD+	PWR (12 VDC)
Negru	RD–	GND
Albastru	CAZ	Semnal de alarmă de manipulare
Galben	RS–485_B	
Violet	RS–485_A	

Tabelul 2-3 Specificațiile și lungimea cablului

cititor de carduri Tip	Metoda de conectare	Lungime
Cititor de carduri RS485	Fiecare fir trebuie să fie în limita a 10 Ω.	100 m (328,08 ft)
Cititor de carduri Wiegand	Fiecare fir trebuie să fie în limita a 2 Ω.	80 m (262,47 ft)

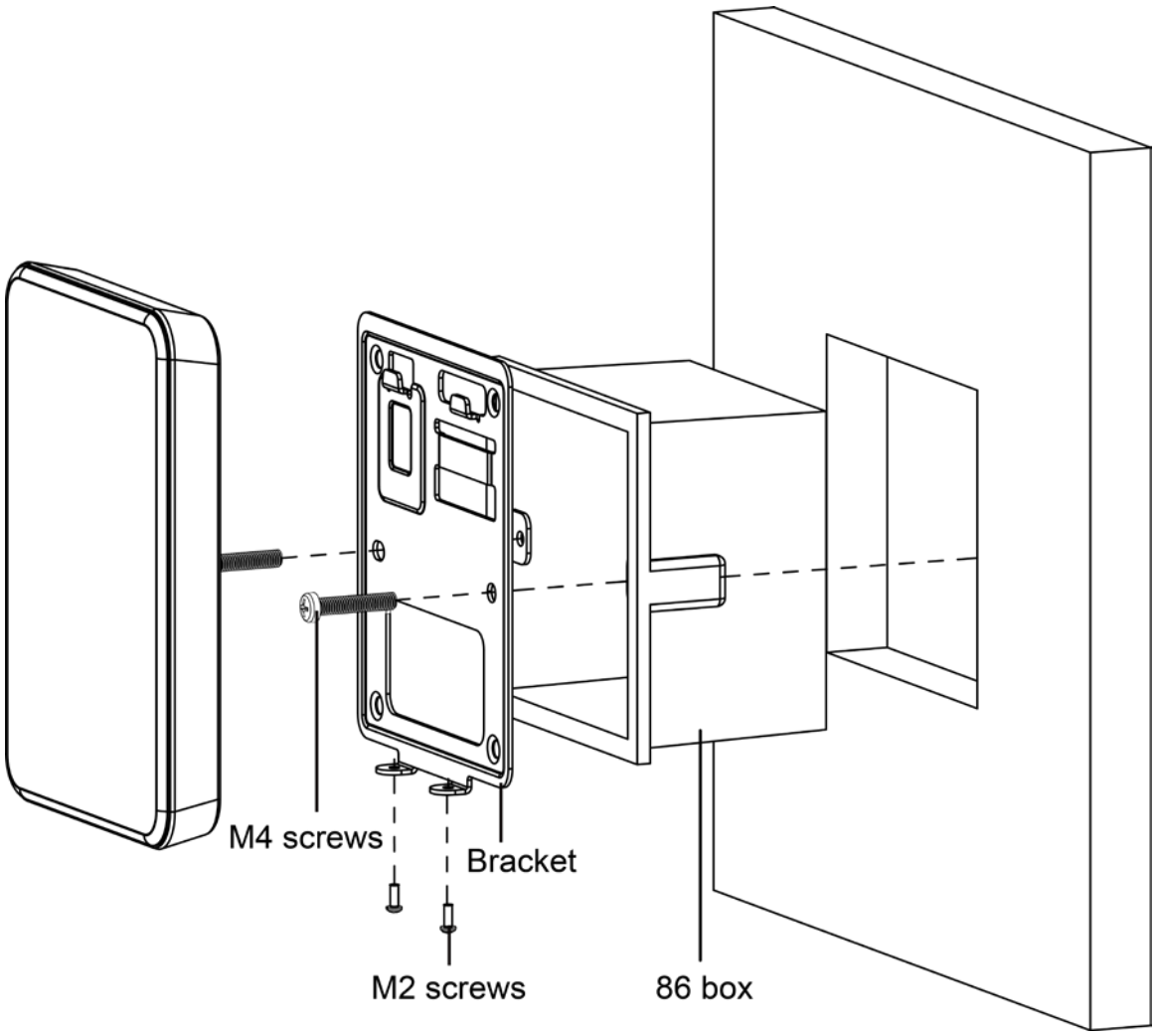
3 Instalare

3.1 Instalarea modelului 86 Box

Suport cutie

1. Montați cutia 86 pe perete.
2. Conectați cititorul de carduri și puneți firele în interiorul cutiei 86.
3. Folosiți două șuruburi M4 pentru a atașa suportul la cutia 86.
4. Atașați cititorul de carduri la suport de sus în jos.
5. Înșurubați cele 2 șuruburi pe partea de jos a cititorului de carduri.

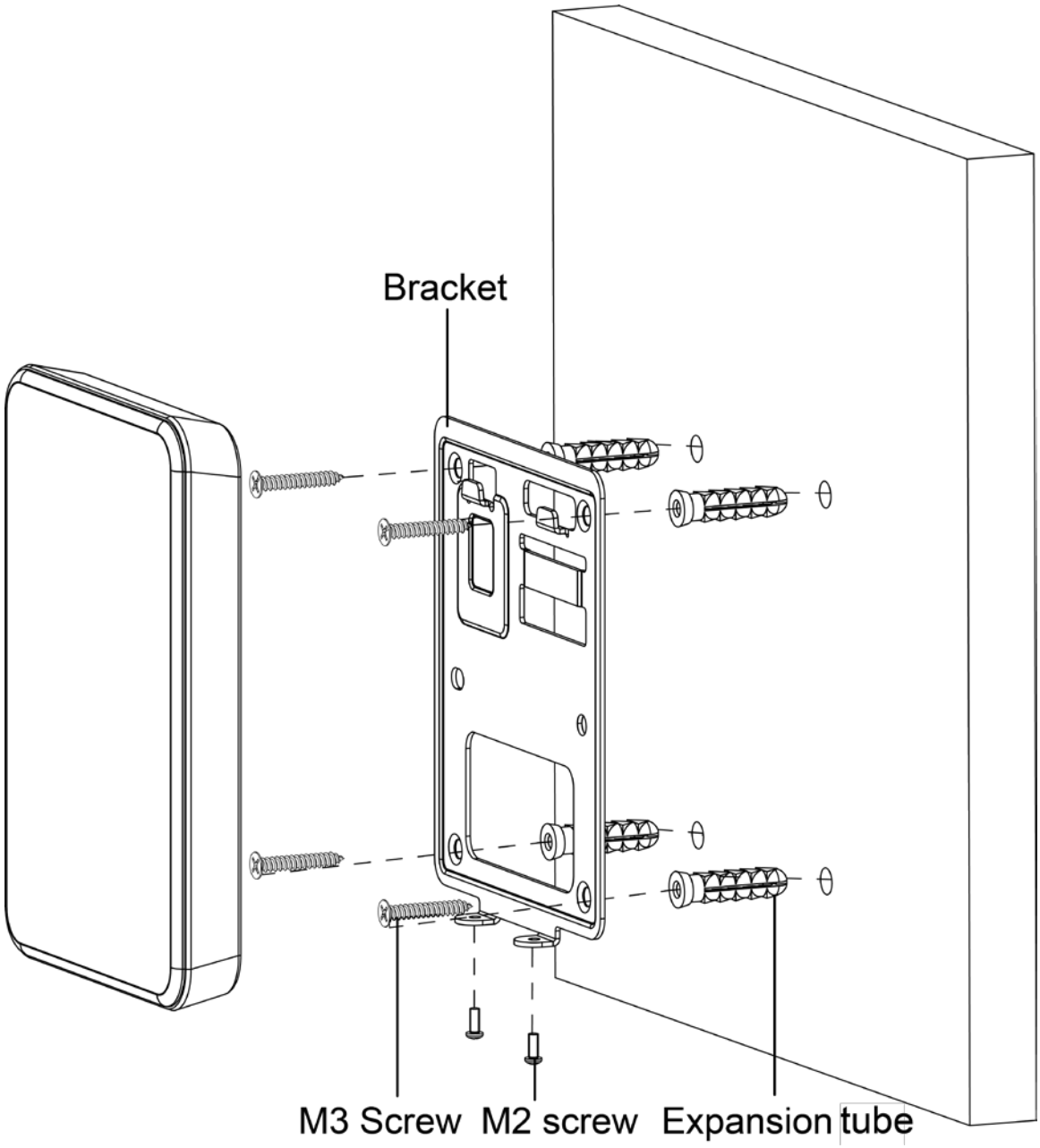
Figura 3-1 Montare pe perete



montare pe perete

1. Faceți găuri pe perete.
2. Puneți 4 șuruburi de expansiune în găuri.
3. Conectați cititorul de carduri prin fanta suportului.
4. Folosiți două șuruburi M3 pentru a monta suportul pe perete.
5. Atașați cititorul de carduri la suport de sus în jos.
6. Înșurubați cele 2 șuruburi pe partea de jos a cititorului de carduri.

Figura 3-2 Montare pe perete



3.2 Instalarea modelului Slim

Procedură

Pasul 1 Faceți 4 găuri și o ieșire de cablu pe perete.

Pentru cablarea montată pe suprafață, nu este necesară ieșirea cablului.

Pasul 2 Puneți 3 șuruburi de expansiune în găuri.

Pasul 3 Firele cititorului de carduri și treceți firele prin fanta suportului. Utilizați trei

Pasul 4 șuruburi M3 pentru a monta suportul pe perete.

Pasul 5 Atașați cititorul de carduri la suport de sus în jos. Înșurubați

Pasul 6 un șurub M2 pe partea de jos a cititorului de carduri.

Figura 3-3 Cablări în perete

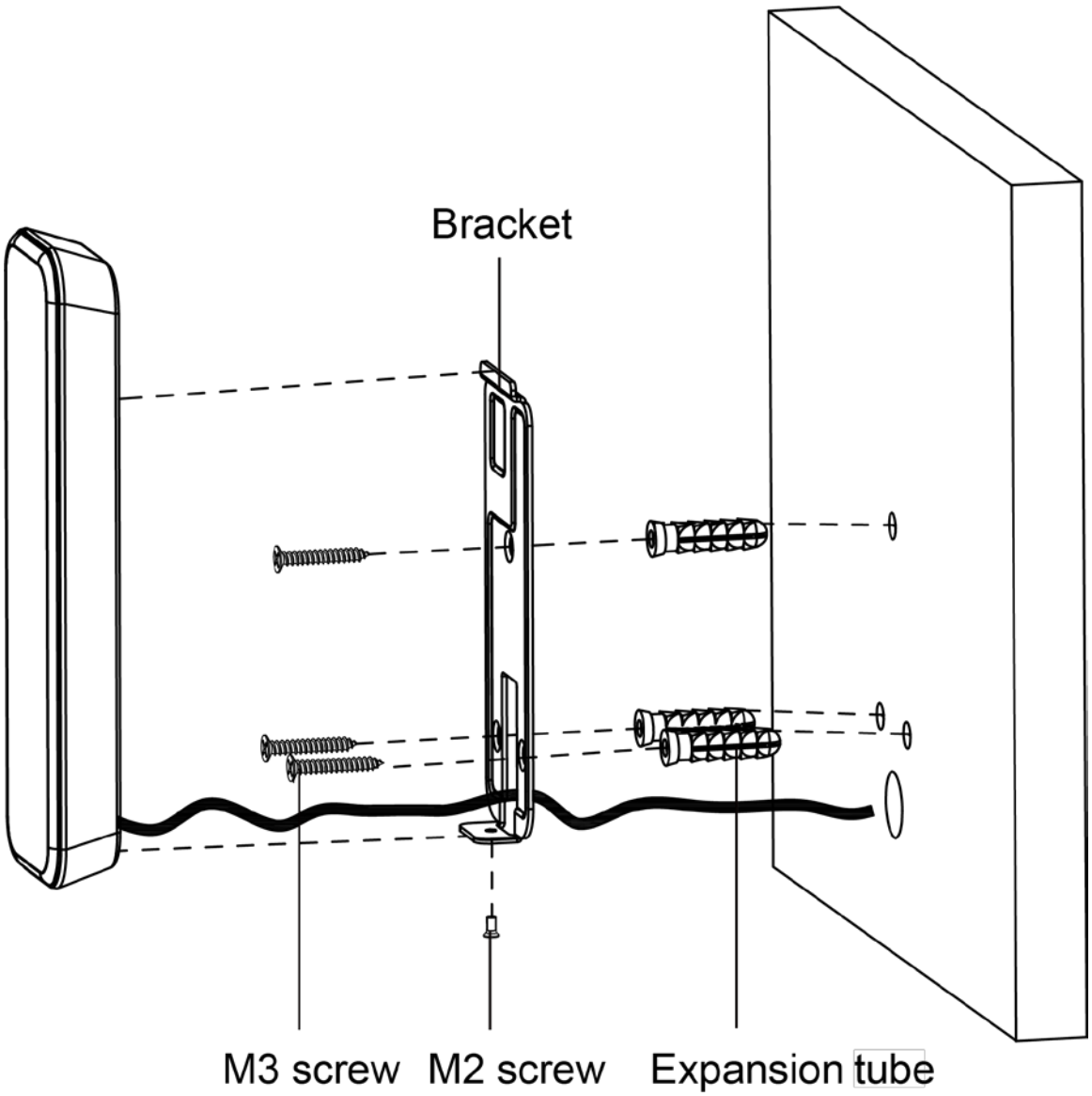
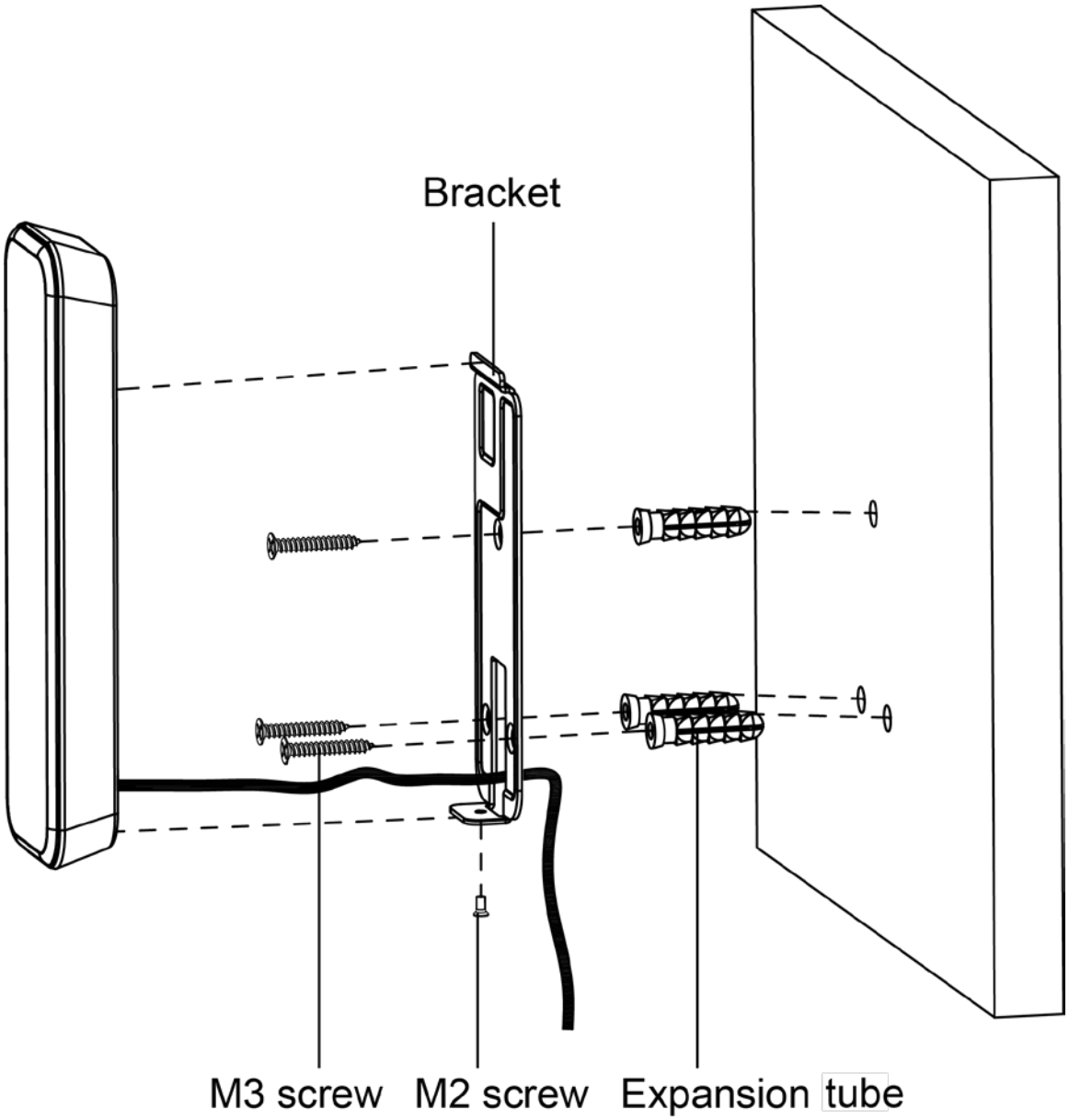


Figura 3-4 Cablaj montat la suprafață



3.3 Instalarea modelului de amprentă

Procedură

Pasul 1 Faceți 4 găuri și o ieșire de cablu pe perete.

Pentru cablarea montată pe suprafață, nu este necesară ieșirea cablului.

Pasul 2 Puneți 3 șuruburi de expansiune în găuri.

Pasul 3 Utilizați trei șuruburi M3 pentru a monta suportul pe perete.

Pasul 4 Cablajul cititorului de carduri.

Pasul 5 Atașați cititorul de carduri la suport de sus în jos.

Figura 3-5 Cablaj în perete

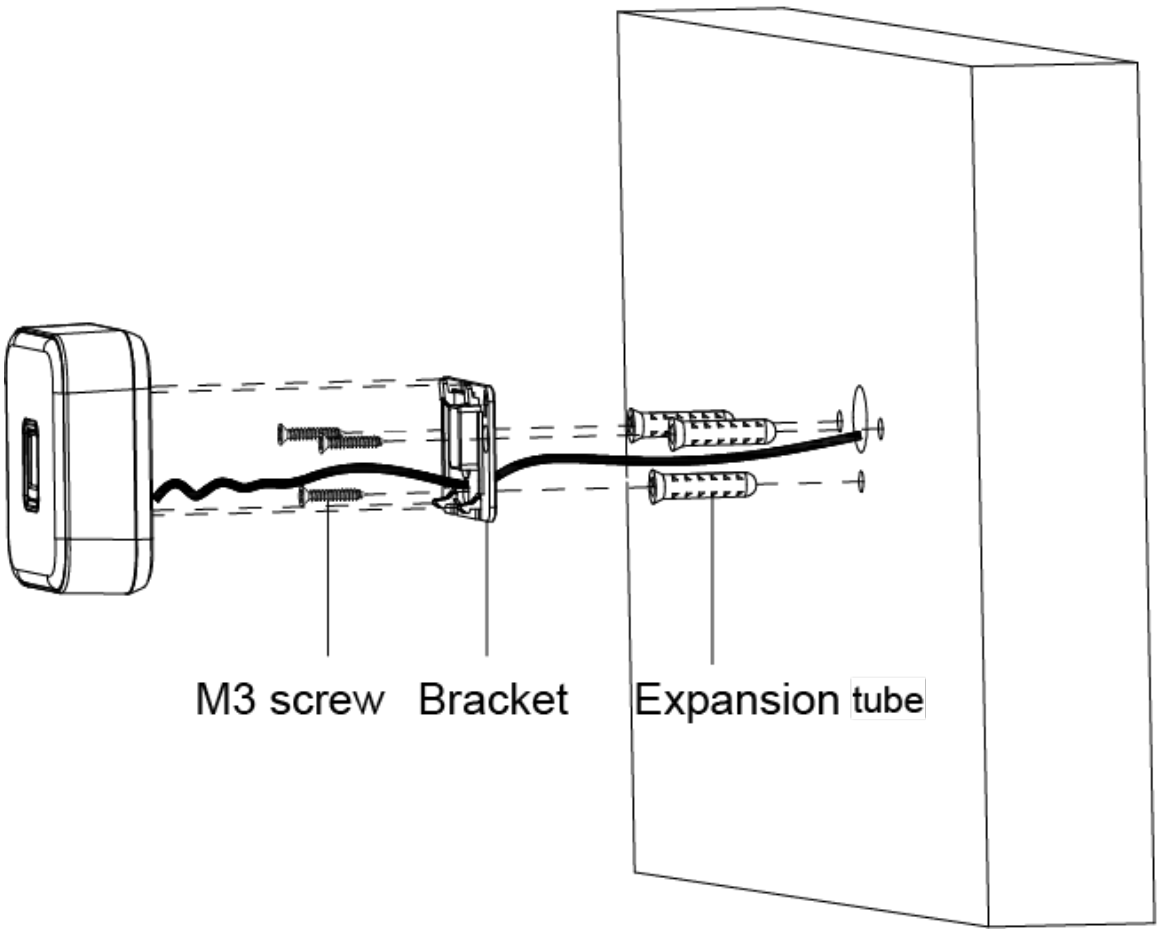
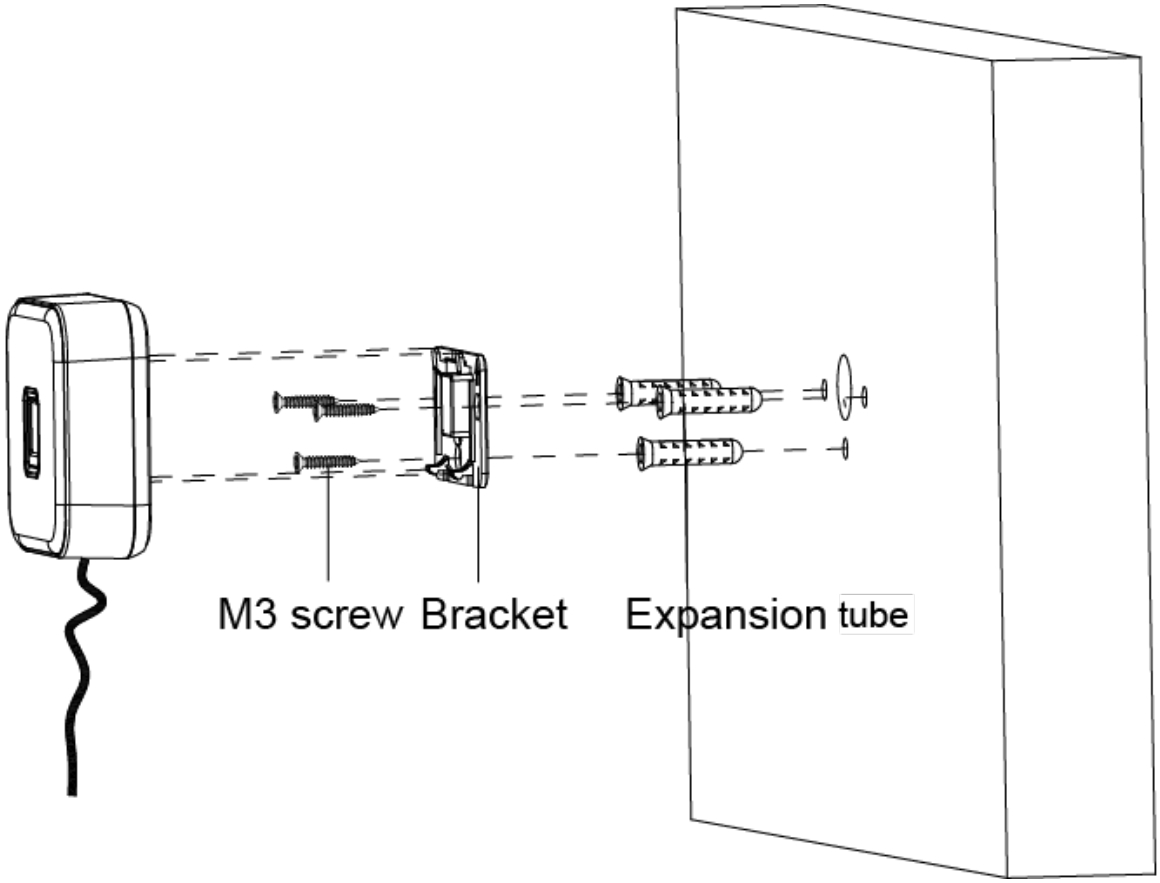
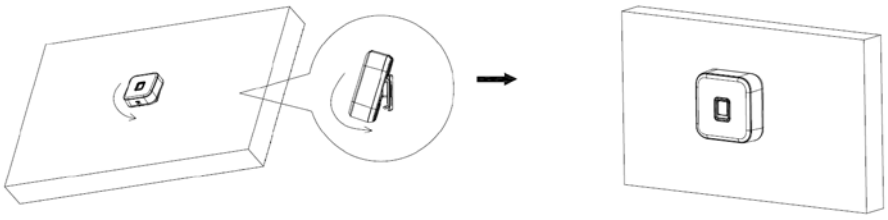


Figura 3-6 Cablaj montat la suprafață



Pasul 6 Apăsați cititorul de carduri spre până când auziți un sunet de „clic” și instalarea se termină.

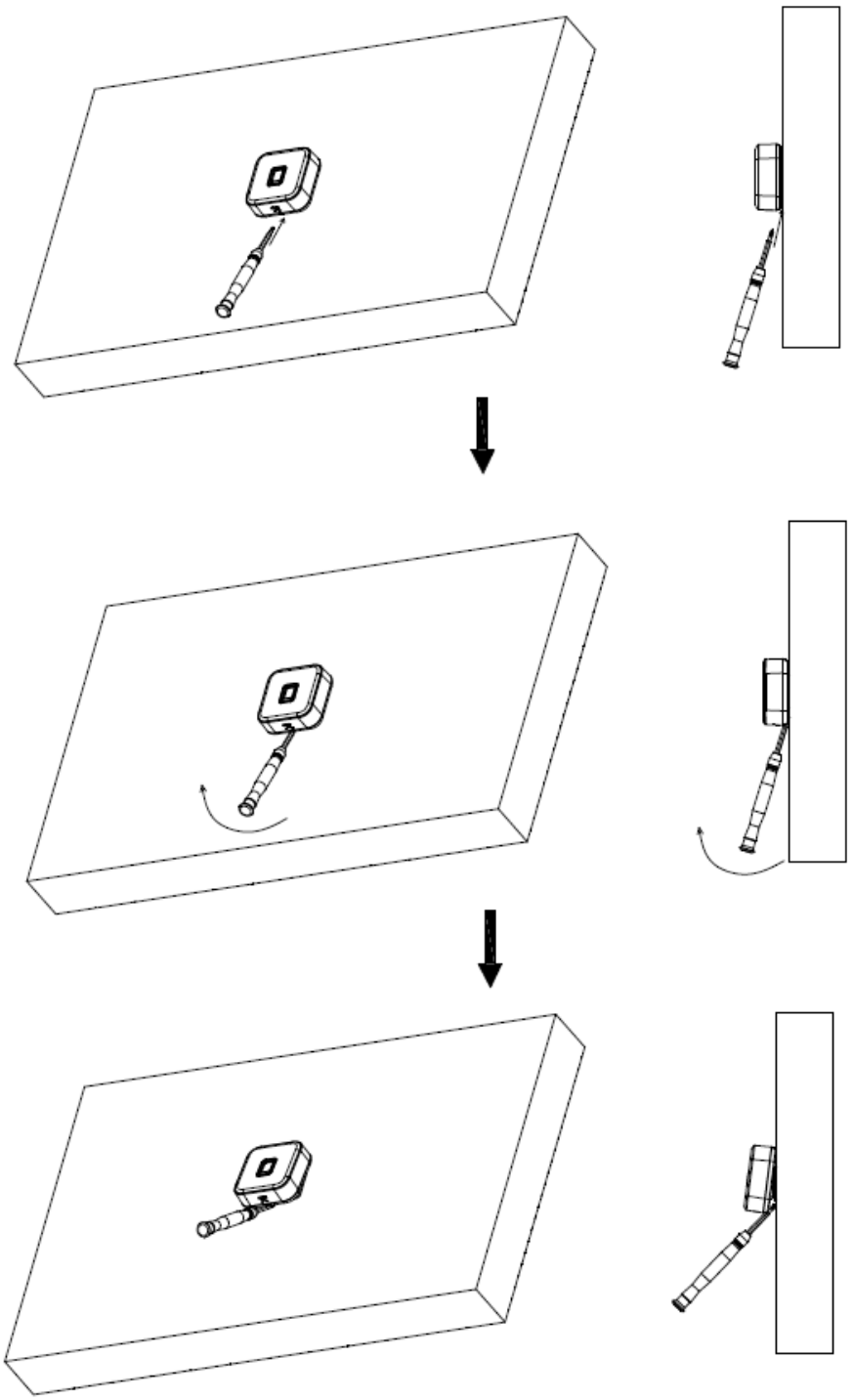
Figura 3-7 Asigurați cititorul de carduri



Operațiuni conexe

Pentru a scoate cititorul de carduri de pe perete, folosiți șurubelnița, deschideți cititorul de carduri de jos până auziți un sunet de „clic”.

Figura 3-8 Scoateți cititorul de carduri



4 Solicitare sunet și lumină

4.1 86 Modele Box și Slim

Tabelul 4-1 Descriere promptă a sunetului și luminii

Situatie	Solicitare de sunet și lumină
Aprinde.	Buzz o dată. Indicatorul este albastru continuu.
Scoaterea cititorului de carduri.	Bâzâit lung timp de 15 secunde.
Apăsarea butoanelor.	Buzz scurt o dată.
Alarma declanșată de controler.	Bâzâit lung timp de 15 secunde.
Comunicare RS–485 și trecerea unui card autorizat.	Buzz o dată. Indicatorul clipește verde o dată, apoi devine albastru continuu ca mod de așteptare.
Comunicare RS–485 și trecerea unui card neautorizat.	Buzz de patru ori. Indicatorul clipește roșu o dată, apoi devine albastru continuu ca mod de așteptare.
Comunicare 485 anormală și trecerea unui card autorizat/neautorizat.	Buzz de trei ori. Indicatorul clipește roșu o dată, apoi devine albastru continuu ca mod de așteptare.
Comunicare Wiegand și trecerea unui card autorizat.	Buzz o dată. Indicatorul clipește verde o dată, apoi devine albastru continuu ca mod de așteptare.
Comunicare Wiegand și trecerea unui card neautorizat.	Buzz de trei ori. Indicatorul clipește roșu o dată, apoi devine albastru continuu ca mod de așteptare.
Actualizarea software-ului sau așteptarea actualizării în BOOT.	Indicatorul clipește albastru până la finalizarea actualizării.

4.2 Model de amprentă

Tabelul 4-2 Descrierea promptă a sunetului și luminii

Situatie	Solicitare de sunet și lumină
cititorul de carduri este pornit.	Buzz o dată. Indicatorul este albastru continuu.
Scoaterea cititorului de carduri.	Bâzâit lung timp de 15 secunde.
Legătura de alarmă declanșată de controler.	
485 și trecerea unui card autorizat.	Buzz o dată. Indicatorul clipește verde o dată, apoi devine albastru continuu ca mod de așteptare.
485 și trecerea unui card neautorizat.	Buzz de patru ori. Indicatorul clipește roșu o dată, apoi devine albastru continuu ca mod de așteptare.

Situatie	Solicitare de sunet și lumină
Comunicare 485 anormală și trecerea unui card/amprentă autorizată sau neautorizată.	Buzz de trei ori. Indicatorul clipește roșu o dată, apoi devine albastru continuu ca mod de așteptare.
Comunicarea 485 și o amprentă este recunoscută.	Buzz o dată.
485 comunicare și trecerea unei amprente autorizate.	Bâzâie de două ori cu un interval de 1 secundă. Indicatorul clipește verde o dată, apoi devine albastru continuu ca mod de așteptare.
485 comunicare și glisarea unei amprente digitale neautorizate.	Bâzâie o dată, apoi de patru ori. Indicatorul clipește roșu o dată, apoi devine albastru continuu ca mod de așteptare.
Operațiuni cu amprenta, inclusiv adăugarea, ștergerea și sincronizarea.	Indicatorul clipește în verde.
Ieșire din operațiunile de amprentă, inclusiv adăugarea, ștergerea și sincronizarea.	Indicatorul este albastru continuu.
Actualizarea software-ului sau așteptarea actualizării în BOOT.	Indicatorul clipește albastru până la finalizarea actualizării.

5 Deblocarea ușii

Glisați cardul pe cititorul de carduri pentru a deschide ușa. Pentru cititorul de carduri cu tastatură, puteți debloca ușa introducând ID-ul de utilizator și parola.

- Deblocați ușa prin parola publică: introduceți parola publică, apoi atingeți**#**.
- Deblocați ușa prin parola utilizatorului: introduceți ID-ul utilizatorului și atingeți**#**, apoi introduceți parola utilizatorului și atingeți**#**.
- Deblocați ușa prin card + parolă: glisați cardul, introduceți parola și apoi atingeți**#**. Dacă parola este corectă, indicatorul este verde și soneria sună o dată. Dacă parola este incorectă, indicatorul este roșu și soneria se aude de 4 ori (comunicație RS-485) sau de 3 ori (comunicație Wiegand sau nu este conectată nicio linie de semnal).

6 Actualizarea sistemului

6.1 Actualizare prin SmartPSS Lite

Cerințe preliminare

- Cititorul de carduri a fost adăugat la controlerul de acces prin fire RS-485.
- Controlerul de acces și cititorul de carduri sunt pornite.

Procedură

Pasul 1 Instalați și conectați-vă la SmartPSS Lite, apoi selectați**Manager de dispozitiv**. Faceți

Pasul 2 clic pe .

Figura 6-1 Selectați controlerul de acces

Pasul 3 Clic și pentru a selecta fișierul de actualizare.

Pasul 4 Clic**Actualizare.**

Indicatorul cititorului de carduri clipește în albastru până la finalizarea actualizării, apoi cititorul de carduri repornește automat.

6.2 Actualizarea prin Config Tool

Cerințe preliminare

- Cititorul de carduri a fost adăugat la controlerul de acces prin fire RS-485.
- Controlerul de acces și cititorul de carduri sunt pornite.

Procedură

Pasul 1 Instalați și deschideți Configtool, apoi selectați**Upgrade de dispozitiv**.

Pasul 2 Faceți clic pe un controler de acces, apoi faceți clic pe .

Pasul 3 Clic**Actualizare**.

Indicatorul cititorului de carduri clipește în albastru până la finalizarea actualizării, apoi cititorul de carduri repornește automat.

Anexa 1 Recomandări de securitate cibernetică

Acțiuni obligatorii care trebuie întreprinse pentru securitatea rețelei echipamentelor de bază:

1.**Utilizați parole puternice**

Consultați următoarele sugestii pentru a seta parole:

- Lungimea nu trebuie să fie mai mică de 8 caractere.
- Includeți cel puțin două tipuri de personaje; tipurile de caractere includ litere mari și mici, numere și simboluri.
- Nu conține numele contului sau numele contului în ordine inversă.
- Nu utilizați caractere continue, cum ar fi 123, abc etc.
- Nu utilizați caractere suprapuse, cum ar fi 111, aaa etc.

2.**Actualizați firmware-ul și software-ul client la timp**

- Conform procedurii standard din industria tehnologiei, vă recomandăm să vă păstrați firmware-ul echipamentului (cum ar fi NVR, DVR, cameră IP etc.) actualizat pentru a vă asigura că sistemul este echipat cu cele mai recente corecții și corecții de securitate. Când echipamentul este conectat la rețeaua publică, se recomandă activarea funcției „verificare automată pentru actualizări" pentru a obține informații în timp util despre actualizările de firmware lansate de producător.
- Vă sugerăm să descărcați și să utilizați cea mai recentă versiune a software-ului client.

Recomandări „Îmi place" pentru a îmbunătăți securitatea rețelei echipamentelor dvs.:

1.**Protecție fizică**

Vă sugerăm să efectuați protecție fizică a echipamentelor, în special a dispozitivelor de stocare. De exemplu, plasați echipamentul într-o sală de calculatoare și un cabinet special și implementați permisiunea de control al accesului și gestionarea cheilor pentru a împiedica personalul neautorizat să efectueze contacte fizice, cum ar fi deteriorarea hardware-ului, conexiunea neautorizată a echipamentelor amovibile (cum ar fi un disc flash USB, un serial). port), etc.

2.**Schimbați parolele în mod regulat**

Vă sugerăm să schimbați parolele în mod regulat pentru a reduce riscul de a fi ghicit sau spart.

3.**Setați și actualizați parolele Resetați informațiile în timp util**

Dispozitivul acceptă funcția de resetare a parolei. Vă rugăm să configurați informațiile aferente pentru resetarea parolei la timp, inclusiv cutia poștală a utilizatorului final și întrebările privind protecția prin parolă. Dacă informațiile se modifică, vă rugăm să le modificați din timp. Când setați întrebări privind protecția cu parolă, se recomandă să nu le folosiți pe cele care pot fi ușor de ghicit.

4.**Activați Blocarea contului**

Funcția de blocare a contului este activată în mod implicit și vă recomandăm să o păstrați activată pentru a garanta securitatea contului. Dacă un atacator încearcă să se conecteze cu parola greșită de mai multe ori, contul corespunzător și adresa IP sursă vor fi blocate.

5.**Schimbați HTTP implicit și alte porturi de servicii**

Vă sugerăm să schimbați HTTP implicit și alte porturi de serviciu în orice set de numere între 1024–65535, reducând riscul ca persoanele din afară să poată ghici ce porturi utilizați.

6.**Activați HTTPS**

Vă sugerăm să activați HTTPS, astfel încât să vizitați serviciul Web printr-un canal de comunicare securizat.

7.**Legarea adresei MAC**

Vă recomandăm să legați adresa IP și MAC a gateway-ului la echipament, reducând astfel riscul de falsificare ARP.

8.**Alocați conturi și privilegii în mod rezonabil**

În funcție de cerințele de afaceri și de management, adăugați în mod rezonabil utilizatori și atribuiți a

set minim de permisiuni pentru ei.

9.**Dezactivați serviciile inutile și alegeți moduri sigure**

Dacă nu este necesar, se recomandă dezactivarea unor servicii precum SNMP, SMTP, UPnP etc., pentru a reduce riscurile.

Dacă este necesar, este foarte recomandat să utilizați moduri sigure, inclusiv, dar fără a se limita la următoarele servicii:

- SNMP: Alegeți SNMP v3 și configurați parole puternice de criptare și parole de autentificare.
- SMTP: Alegeți TLS pentru a accesa serverul de cutie poștală.
- FTP: alegeți SFTP și configurați parole puternice.
- Hotspot AP: alegeți modul de criptare WPA2-PSK și configurați parole puternice.

10.**Transmisie criptată audio și video**

Dacă conținutul datelor dvs. audio și video este foarte important sau sensibil, vă recomandăm să utilizați funcția de transmisie criptată, pentru a reduce riscul ca datele audio și video să fie furate în timpul transmisiei.

Memento: transmisia criptată va cauza o oarecare pierdere a eficienței transmisiei.

11.**Audit securizat**

- Verificați utilizatorii online: vă sugerăm să verificați în mod regulat utilizatorii online pentru a vedea dacă dispozitivul este conectat fără autorizație.
- Verificați jurnalul echipamentului: prin vizualizarea jurnalelor, puteți cunoaște adresele IP care au fost utilizate pentru a vă conecta la dispozitivele dvs. și operațiunile cheie ale acestora.

12.**Jurnal de rețea**

Datorită capacității limitate de stocare a echipamentului, jurnalul stocat este limitat. Dacă trebuie să salvați jurnalul pentru o perioadă lungă de timp, se recomandă să activați funcția de jurnal de rețea pentru a vă asigura că jurnalele critice sunt sincronizate cu serverul de jurnal de rețea pentru urmărire.

13.**Construiți un mediu de rețea sigur**

Pentru a asigura mai bine siguranța echipamentelor și pentru a reduce potențialele riscuri cibernetice, vă recomandăm:

- Dezactivați funcția de mapare porturi a routerului pentru a evita accesul direct la dispozitivele intranet din rețeaua externă.
- Rețeaua ar trebui să fie partiționată și izolată în funcție de nevoile reale ale rețelei. Dacă nu există cerințe de comunicare între două subrețele, se recomandă utilizarea VLAN, network GAP și alte tehnologii pentru a partiționa rețeaua, astfel încât să obțineți efectul de izolare a rețelei.
- Stabiliți sistemul de autentificare a accesului 802.1x pentru a reduce riscul accesului neautorizat la rețelele private.
- Activați funcția de filtrare a adreselor IP/MAC pentru a limita intervalul de gazde permise să acceseze dispozitivul.