Controler de acces

Manualul utilizatorului

V1.0.1

cuvânt înainte

General

Acest manual prezintă instalarea și operațiunile detaliate ale Controllerului de acces (denumit în continuare „Dispozitivul”).

Instructiuni de siguranta

Următoarele cuvinte semnalizatoare clasificate cu semnificație definită pot apărea în manual.

Cuvinte semnal	Sens
 **PERICOL**	Indică un pericol potențial ridicat care, dacă nu este evitat, va duce la moarte sau vătămări grave.
 **AVERTIZARE**	Indică un pericol potențial mediu sau scăzut care, dacă nu este evitat, ar putea duce la răniri ușoare sau moderate.
 **PRUDENȚĂ**	Indică un risc potențial care, dacă nu este evitat, ar putea duce la deteriorarea proprietății, pierderea datelor, performanță scăzută sau rezultat imprevizibil.
 SFATURI	Oferă metode care vă ajută să rezolvați o problemă sau să vă economisiți timp.
 **NOTĂ**	Oferă informații suplimentare ca subliniere și completare a textului.

Istoricul revizuirilor

Versiune	Conținutul revizuirii	Timpul de eliberare
V1.0.1	S-a adăugat un proces de inițializare.	decembrie 2021
V1.0.0	Prima aparitie.	septembrie 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

respectarea manualului.

- 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 Dispozitivului, prevenirea pericolelor și prevenirea daunelor materiale. Citiți cu atenție înainte de a utiliza Dispozitivul, respectați instrucțiunile atunci când îl utilizați și păstrați manualul în siguranță pentru referințe ulterioare.

Cerința de transport

Transportați dispozitivul în condiții de umiditate și temperatură permise.

Cerință de stocare

Păstrați dispozitivul în condiții de umiditate și temperatură permise.

Cerințe de instalare

 **WARNING**

- Nu conectați adaptorul de alimentare la Dispozitiv în timp ce adaptorul este pornit.
- Respectați cu strictețe codul și standardele locale de siguranță electrică. Asigurați-vă că tensiunea ambientală este stabil și îndeplinește cerințele de alimentare ale Dispozitivului.
- Nu conectați Dispozitivul la două sau mai multe tipuri de surse de alimentare, pentru a evita deteriorarea Dispozitivului.
- 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 purtând cască și centuri de siguranță.
- Nu așezați dispozitivul într-un loc expus la lumina soarelui sau în apropierea surselor de căldură.
- Păstrați dispozitivul departe de umiditate, praf și funingine.
- Instalați dispozitivul pe o suprafață stabilă pentru a preveni căderea acestuia.
- Instalați dispozitivul 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 puterii nominale specificații.
- Sursa de alimentare trebuie să respecte cerințele ES1 din standardul IEC 62368-1 și să fie nr mai mare decât PS2. Vă rugăm să rețineți că cerințele de alimentare sunt supuse etichetei Dispozitiv.
- Aparatul este un aparat electric de clasa I. Asigurați-vă că sursa de alimentare a dispozitivului este conectat 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 Dispozitivului în timp ce adaptorul este pornit.
- Operați dispozitivul în intervalul nominal de putere de intrare și de ieșire.
- Utilizați dispozitivul în condiții de umiditate și temperatură permise.
- Nu scăpați și nu stropiți cu lichid pe Dispozitiv și asigurați-vă că nu există niciun obiect plin cu lichid pe dispozitiv pentru a preveni curgerea lichidului în el.
- Nu dezasamblați dispozitivul fără instrucțiuni profesionale.

Cuprins

1.1 Introducere

Dispozitivul este un panou de control al accesului care compensează supravegherea video și interfonul vizual. Are un design îngrijit și modern, cu funcționalitate puternică, potrivit pentru clădiri comerciale de ultimă generație, proprietăți de grup și comunități inteligente.

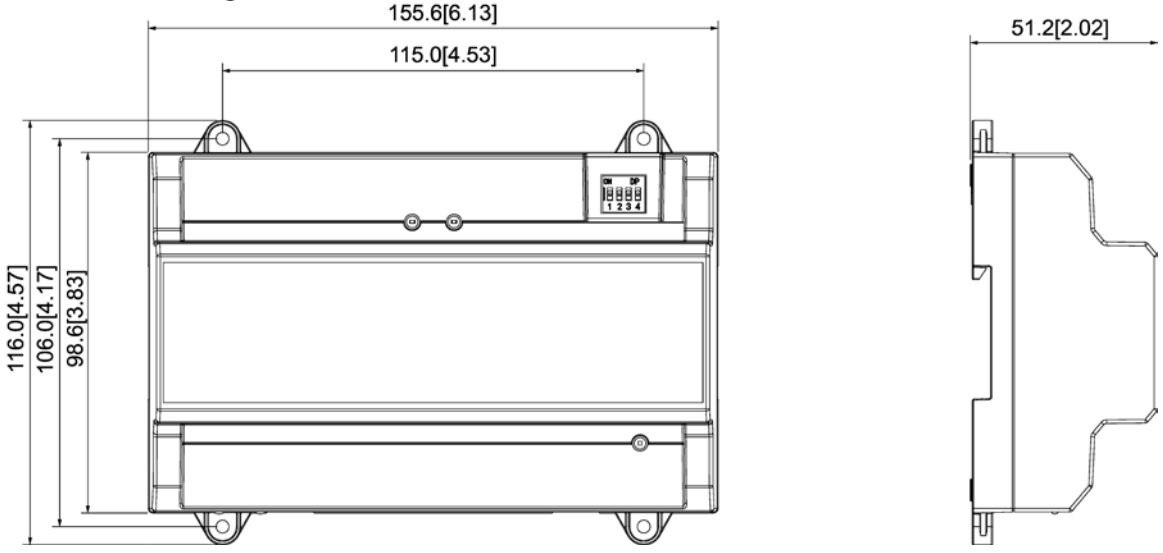
1.2 Caracteristici

- Folosind PC+ABS ca material, aspectul este high-end și îngrijit.
- Suportă comunicații în rețea TCP/IP, datele de comunicare sunt criptate pentru securitate.
- Suporta protocolul OSDP.
- Suporta functia PoE.
- Suportă deblocarea cardului, a parolei și a amprentei.
- Suportă 100.000 de utilizatori, 100.000 de carduri, 3.000 de amprente și 500.000 de înregistrări.
- Acceptă interblocare, anti-passback, deblocare multi-utilizator, deblocare a primului card, deblocare cu parolă de administrator, deblocare de la distanță și multe altele.
- Suportă alarmă de manipulare, alarmă de intruziune, alarmă de expirare a senzorului de ușă, alarmă de constrângere, alarmă de blocare, alarmă de depășire a pragului de card ilegal, alarmă de parolă incorectă și alarmă externă.
- Acceptă tipuri de utilizatori, cum ar fi utilizatorii generali, utilizatorii VIP, utilizatorii invitați, utilizatorii listei blocate, utilizatorii de patrulare și alți utilizatori.
- Suportă RTC încorporat, calibrarea timpului NTP, calibrarea manuală a timpului și funcțiile de calibrare automată a timpului.
- Acceptă funcționarea offline, stocarea înregistrărilor evenimentelor și funcțiile de încărcare, datele pot fi stocate local după deconectarea rețelei și încărcarea continuă după ce rețeaua este restaurată. Acceptă 128 de perioade, 128 de planuri de
- vacanță, 128 de perioade de vacanță, perioade în mod normal deschise, perioade în mod normal închise, perioade de deblocare la distanță, perioade de deblocare a primei carduri și suportă deblocarea în perioade. Sprijină mecanismul de protecție pentru
- câine de pază pentru a asigura stabilitatea funcționării.

1.3 Dimensiuni

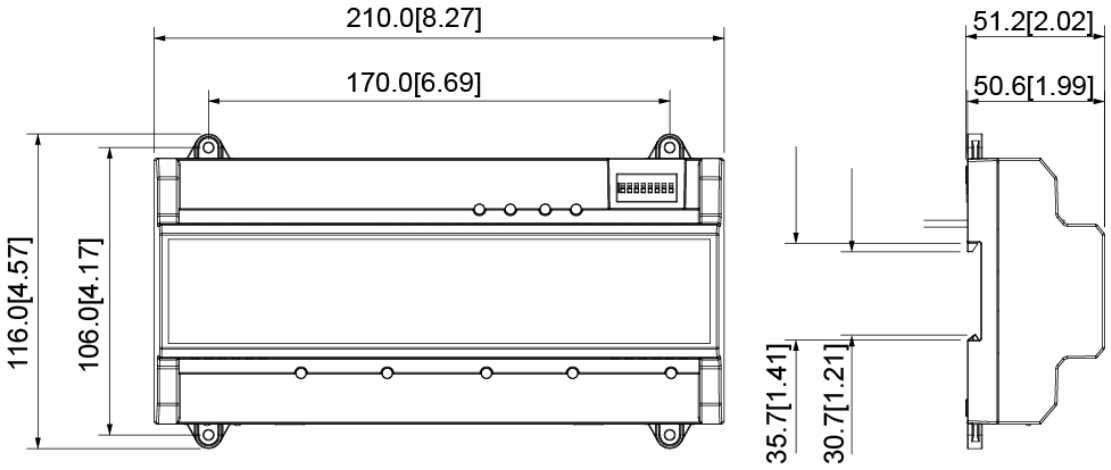
Controller de acces unidirecțional cu două uși

Figure 1-1 Dimensiuni (cu două uși unisens) (mm [inch])



Controller de acces unidirecțional cu două uși, cu două căi/patru uși

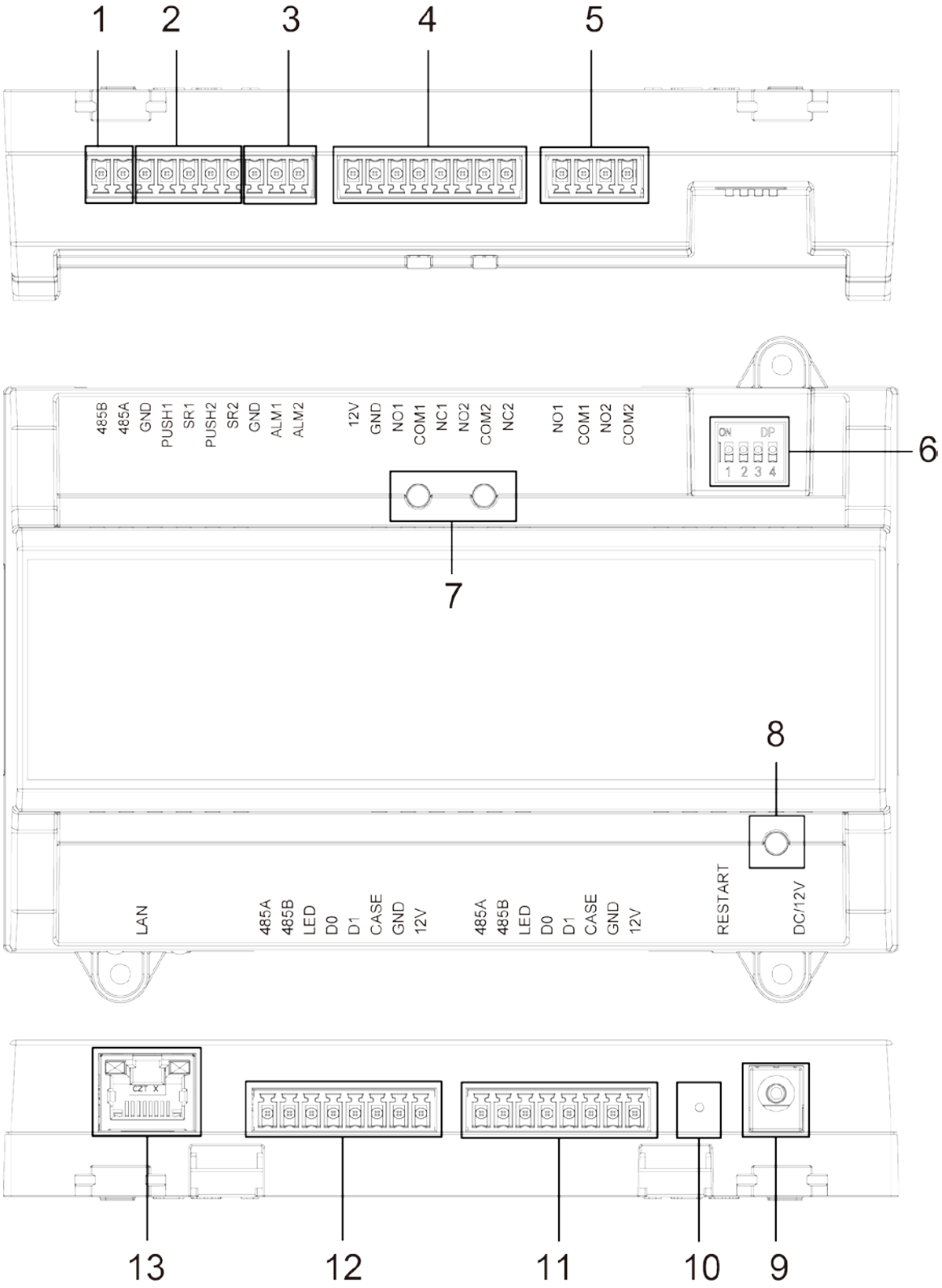
Figure 1-2 Dimensiuni (cu două uși cu două sensuri/cu patru uși cu un singur sens) (mm [inch])



1.4 Componente

Controller de acces unidirecțional cu două uși

Figure 1-3 Componente (cu două uși unisens)



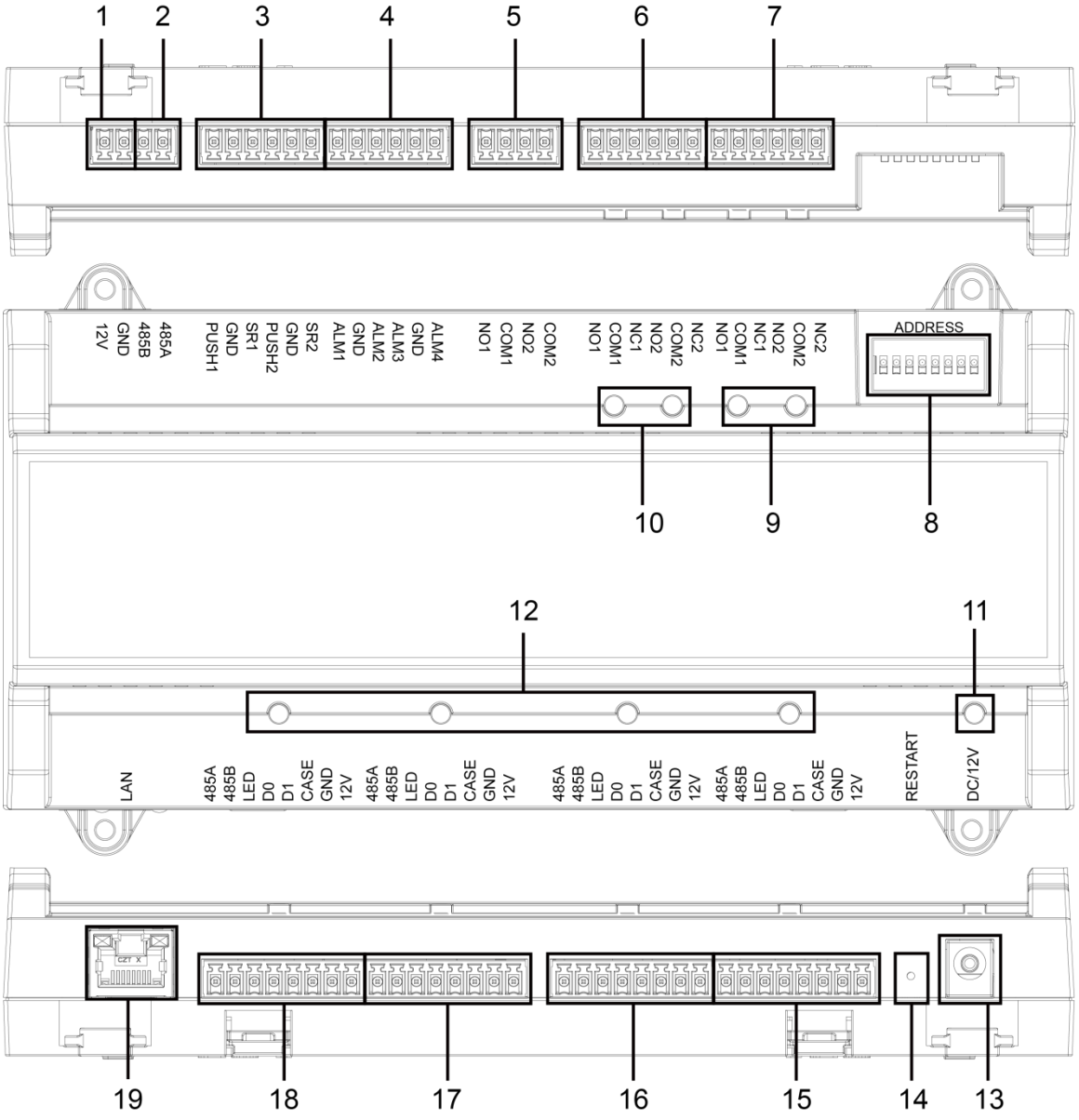
Tabelul 1-1 Descrierea componentelor (cu două uși unisens)

Nu.	Nume	Nu.	Nume
1	Port RS-485	8	Indicator luminos de alimentare
2	Buton de ieșire/port de contact ușă	9	Port de alimentare

Nu.	Nume	Nu.	Nume
3	Port de alarmă IN	10	Butonul de repornire
4	Port OUT pentru blocarea ușii	11	Port cititor card de intrare al ușii nr.2
5	Port alarmă OUT	12	Port cititor card de intrare al ușii nr.1
6	Comutator DIP	13	Port de rețea
7	Indicator luminos al blocării ușii	14	—

Controller de acces bidirecțional cu două uși

Figure 1-4 Componente (cu două uși cu două sensuri)



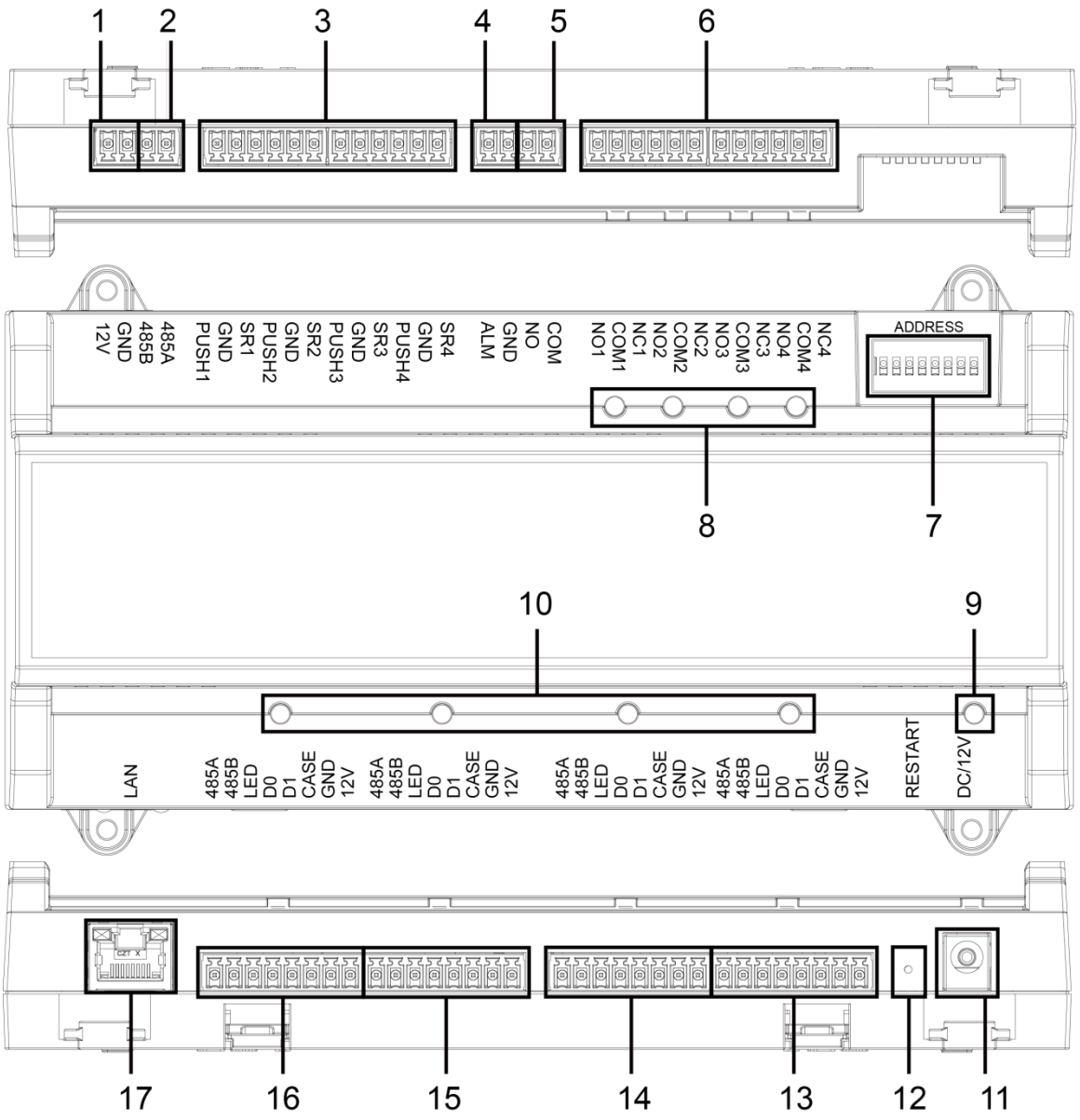
Tabelul 1-2 Descrierea componentelor (cu două uși în două sensuri)

Nu.	Nume	Nu.	Nume
1	Port de alimentare pentru blocarea ușii	11	Indicator luminos de alimentare
2	Port RS-485	12	Indicator luminos al cititorului de carduri
3	Buton de ieșire/port de contact ușă	13	Port de alimentare
4	Port IN al alarmei externe	14	Butonul de repornire
5	Port alarmă externă OUT	15	Ieșiți portul cititorului de carduri din ușa nr. 2

Nu.	Nume	Nu.	Nume
6	Port OUT pentru controlul blocării ușii	16	Port cititor card de intrare al ușii nr.2
7	Alarma internă OUT	17	Ieșiți portul cititorului de carduri de pe ușa nr.1
8	Comutator DIP	18	Port cititor card de intrare al ușii nr.1
9	Indicator luminos de alarmă	19	Port de rețea
10	Indicator luminos de blocare a ușii	—	—

Controler de acces unidirecțional cu patru uși

Figure 1-5 Componente (cu patru uși unisens)



Tabelul 1-3 Descrierea componentelor (cu patru uși unisens)

Nu.	Nume	Nu.	Nume
1	Port de alimentare pentru blocarea ușii	10	Indicator luminos al cititorului de carduri
2	Port RS-485	11	Port de alimentare
3	Buton de ieșire/port de contact ușă	12	Butonul de repornire
4	Port de alarmă IN	13	Port cititor card de intrare al ușii nr.4

Nu.	Nume	Nu.	Nume
5	Port alarmă OUT	14	Port cititor card de intrare al ușii nr.3
6	Port OUT pentru controlul blocării ușii	15	Port cititor card de intrare al ușii nr.2
7	Comutator DIP	16	Port cititor card de intrare al ușii nr.1
8	Indicator luminos de blocare a ușii	17	Port de rețea
9	Indicator luminos de alimentare	—	—

Port

Port auto-adaptabil de 10/100 Mbps și acceptă sursa de alimentare PoE.

Indicator luminos

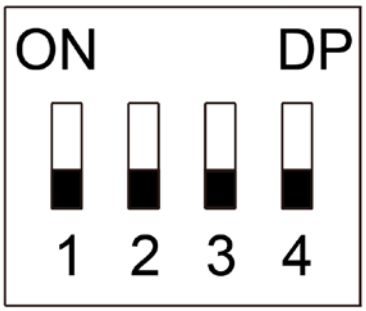
- Indicator luminos de alimentare
  - ◇ Verde: Funcționează normal.
  - ◇ Roșu: anomalie de putere.
  - ◇ Albastru: Upgrade.
- Indicator luminos de alarmă
  - ◇ Pornit: alarma este declanșată. Oprit:
  - ◇ Alarma nu este declanșată. Indicator
- luminos de blocare a ușii
  - ◇ Pornit: Încuietoarea ușii este conectată.
  - ◇ Oprit: Încuietoarea ușii nu este conectată.
- Indicator luminos cititor de carduri
  - ◇ Pornit: Cititorul de carduri este conectat. Oprit:
  - ◇ Cititorul de carduri nu este conectat.

Comutator DIP

Efectuați operația corespunzătoare prin comutatorul DIP.

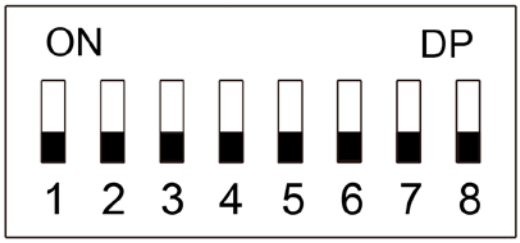
 Înseamnă 1;  înseamnă 0.

Figure 1-6 Comutator DIP (controller de acces unidirecțional cu două uși)



- 1–4 sunt toate 0, dispozitivul pornește normal după pornire. 1–4 sunt
- toate 1, dispozitivul intră în modul de pornire după pornire.
- 1 și 3 sunt 1, 2 și 4 sunt 0, Dispozitivul revine la valorile implicite din fabrică după repornire.
- 2 și 4 sunt 1, 1 și 3 sunt 0, Dispozitivul revine la valorile implicite din fabrică după repornire. Dar informațiile despre utilizator vor fi păstrate.

Figure 1-7 Comutator DIP (controller de acces cu două uși, două căi/patru uși, unidirecțional)



- 1–8 sunt toate 0, dispozitivul pornește normal după pornire. 1–8 sunt
- toate 1, dispozitivul intră în modul de pornire după pornire.
- 1, 3, 5 și 7 sunt 1, 2, 4, 6 și 8 sunt 0, Dispozitivul revine la valorile implicite din fabrică după repornire.
- 1, 2, 4, 6 și 8 sunt 1, 1, 3, 5 și 7 sunt 0, Dispozitivul revine la valorile implicite din fabrică după repornire. Dar informațiile despre utilizator vor fi păstrate.

Repornire

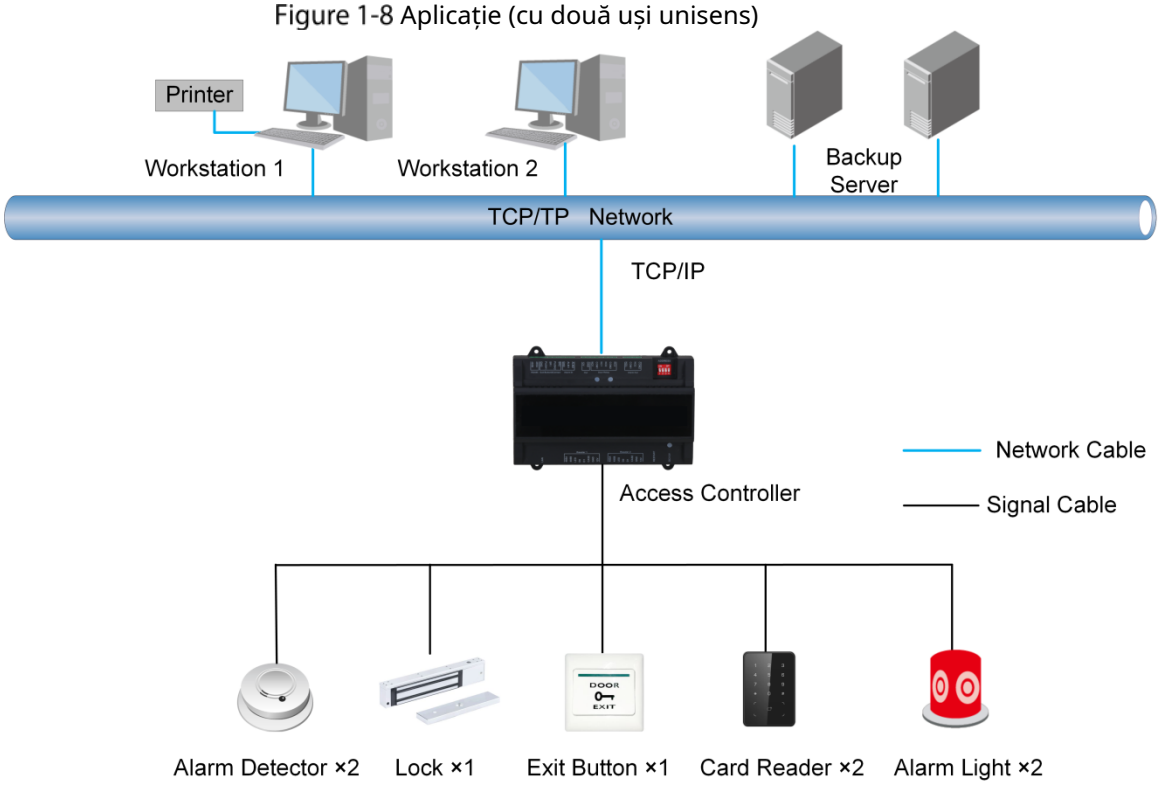
Introduceți un ac în orificiul RESTART și apăsați-l pentru a reporni dispozitivul.

Butonul de repornire este pentru a reporni dispozitivul, mai degrabă decât pentru a modifica configurația.

1.5 Aplicație

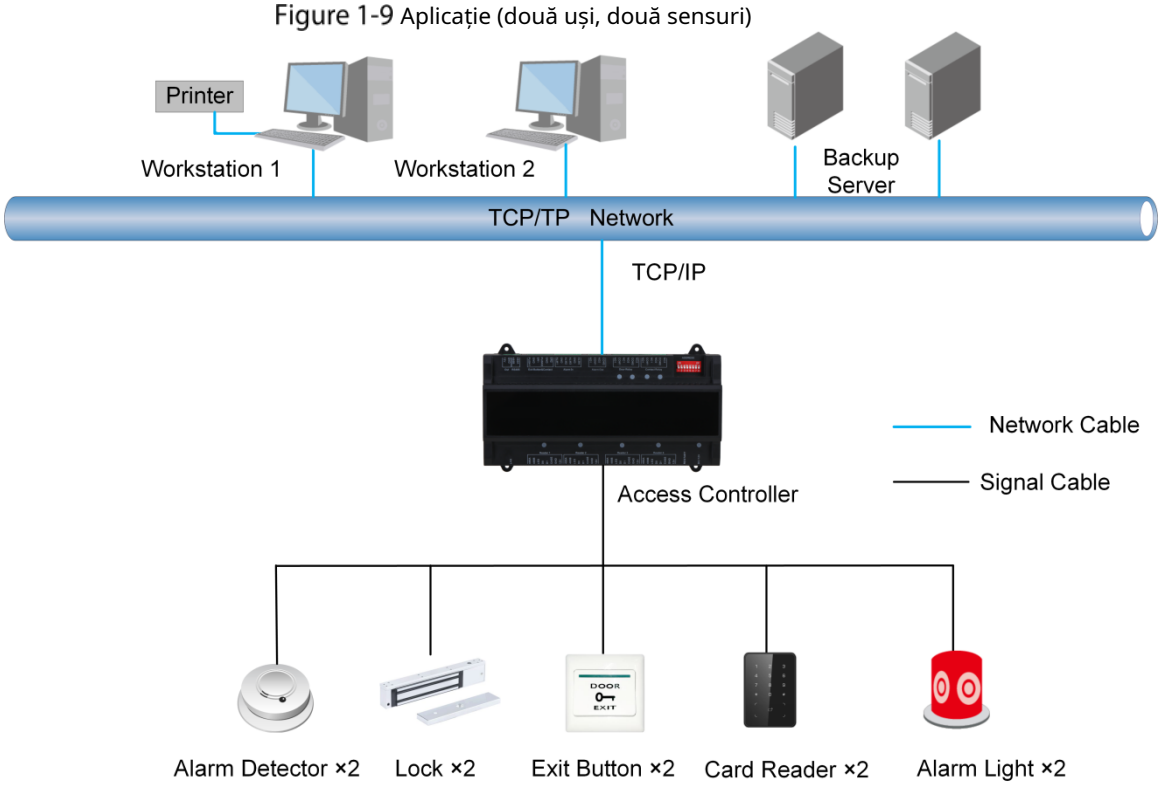
Controller de acces unidirecțional cu două uși

Figure 1-8 Aplicație (cu două uși unisens)



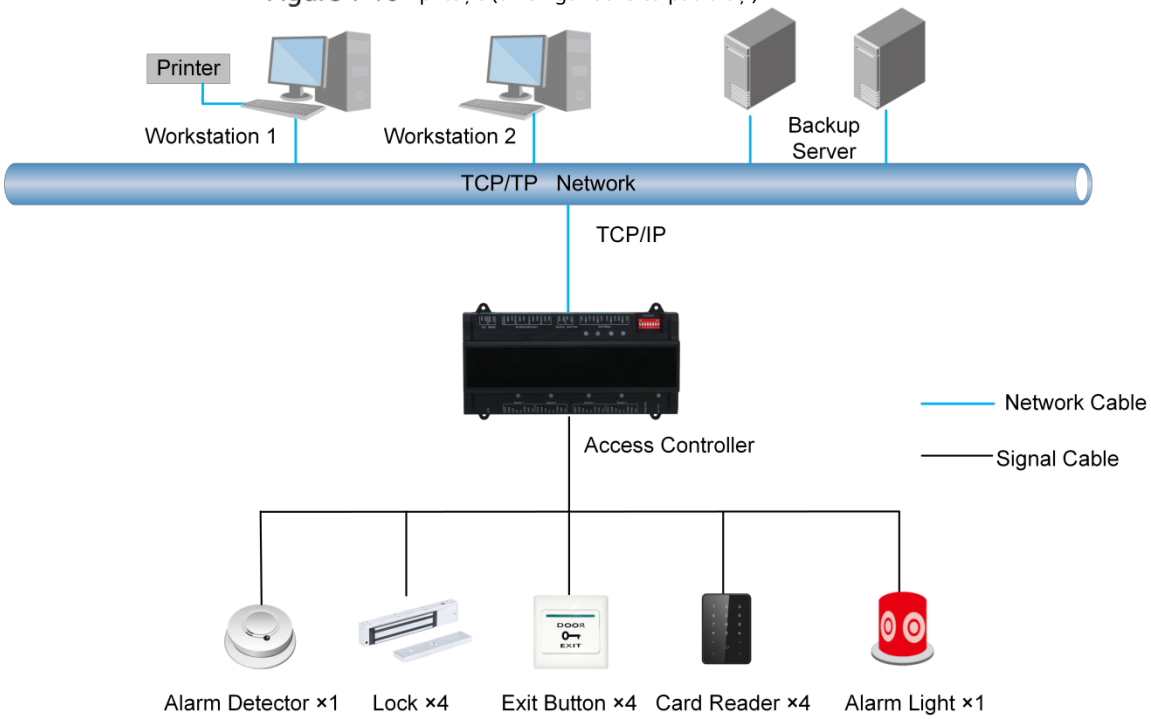
Controller de acces bidirecțional cu două uși

Figure 1-9 Aplicație (două uși, două sensuri)



Controler de acces unidirecțional cu patru uși

Figure 1-10 Aplicație (un singur sens cu patru uși)

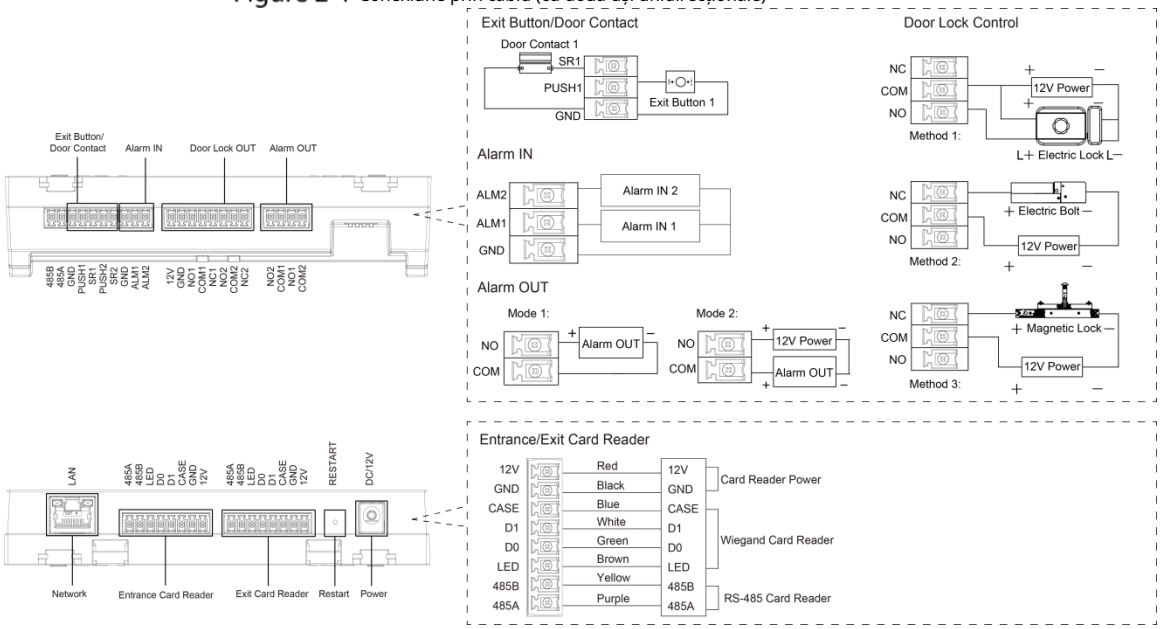


2 Instalare

2.1 Conexiune prin cablu

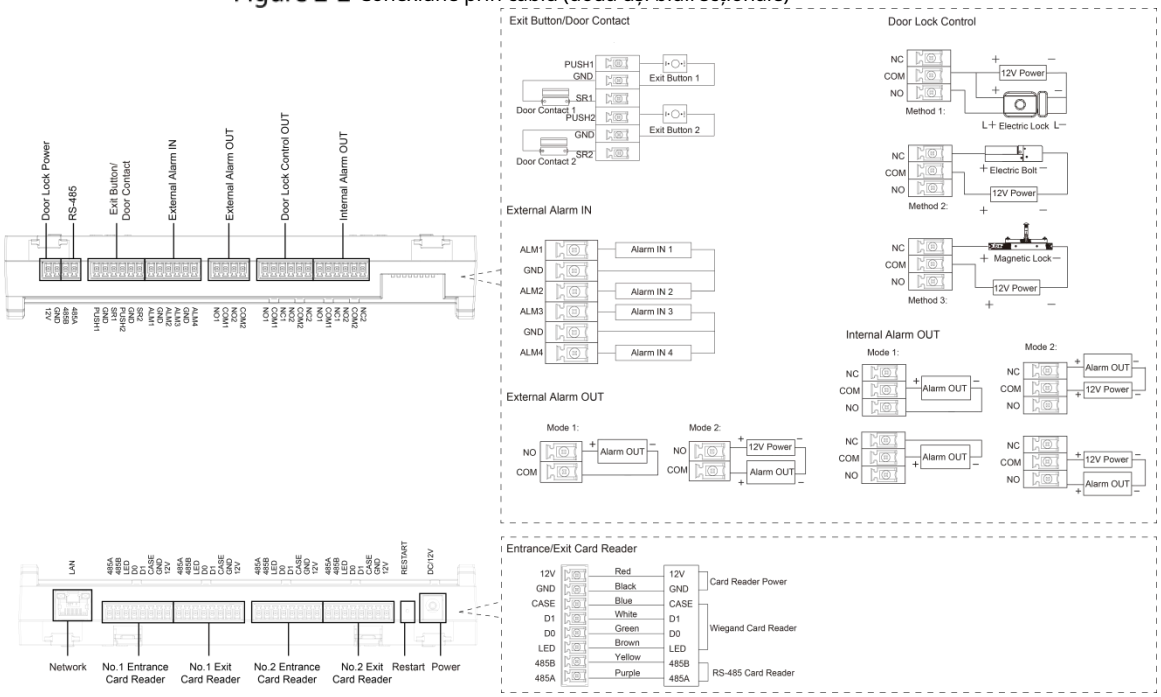
Controller de acces unidirecțional cu două uși

Figure 2-1 Conexiune prin cablu (cu două uși unidirecționale)



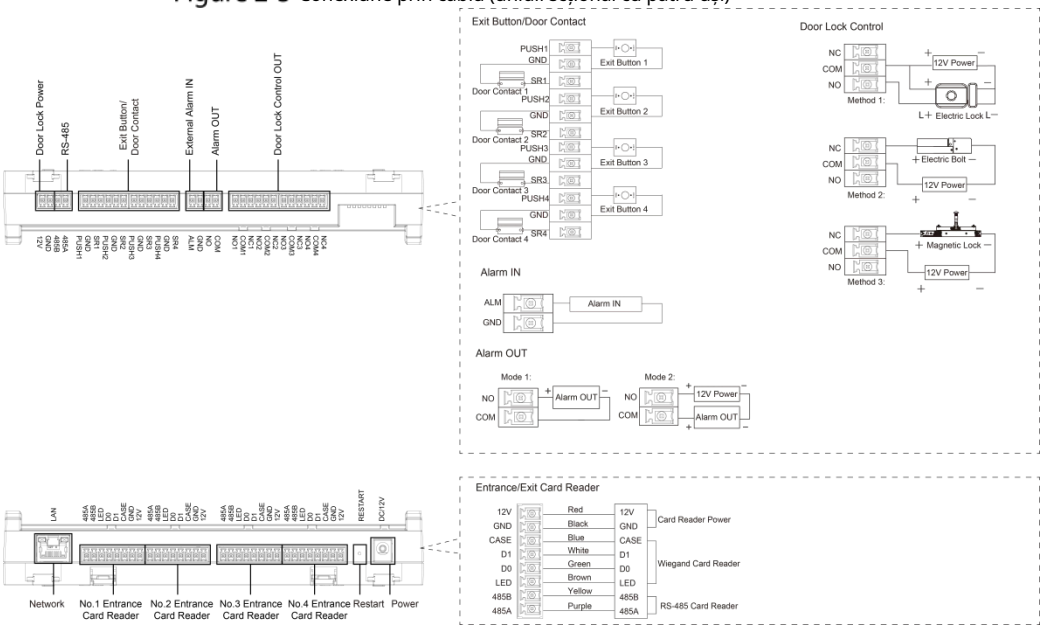
Controller de acces bidirecțional cu două uși

Figure 2-2 Conexiune prin cablu (două uși bidirecționale)



Controler de acces unidirecțional cu patru uși

Figure 2-3 Conexiune prin cablu (unidirecțional cu patru uși)



2.1.1 Conectarea prin cablu a intrării de alarmă

Portul extern de intrare pentru alarmă poate fi conectat la detectoare de fum, detectoare cu infraroșu și multe altele.

Tabel 2-1 Conectarea prin cablu a intrării de alarmă

Model	Canal de intrare de alarmă	Descriere
Cu două uși Sens unic	Intrare alarma cu 2 canale.	Alarma externă poate fi legată de starea de blocare/ deblocare a ușii. Alarma externă ALM1 leagă toate ușile pentru a fi deschise în mod normal. Alarma externă ALM2 leagă toate ușile pentru a fi închise în mod normal.
Cu două uși în două sensuri	Intrare alarma cu 4 canale.	Alarma externă poate fi legată de starea de blocare/ deblocare a ușii. Alarma externă ALM1–ALM2 leagă toate ușile pentru a fi deschise în mod normal. Alarma externă ALM3–ALM4 leagă toate ușile pentru a fi închise în mod normal.
Cu patru uși Sens unic	Intrare alarmă cu 1 canal.	Când alarma externă este declanșată, toate ușile sunt în mod normal deschise.

2.1.2 Conectarea prin cablu a ieșirii de alarmă

Intrarea de alarmă internă sau externă declanșează o alarmă, iar dispozitivul de ieșire de alarmă dă o alarmă timp de 15 s.

Există două moduri de conectare a ieșirii alarmei. Selectați modul de conectare în funcție de dispozitivul de alarmă. De exemplu, IPC poate folosi modul 1, iar dispozitivul de sunet și lumină poate folosi modul 2.

Când controlerele de acces în două căi cu două uși sunt conectate la dispozitivul de ieșire de alarmă intern, selectați NC/NO în funcție de starea normal deschis sau normal închis.

Tabel 2-2 Conectarea prin cablu a ieșirii alarmei

Model	Canal de ieșire de alarmă	Port	Descriere
	Ieșire alarmă cu 2 canale.	NUMARUL 1	ALM1 declanșează ieșirea de alarmă.

Model	Canal de ieșire de alarmă	Port	Descriere
Cu două uși Sens unic		COM1	Alarmă de timeout contact ușă și alarmă de intruziune. Ieșire alarmă de manipulare a cititorului de carduri de intrare pentru ușă nr. 1.
		NO2	ALM2 declanșează ieșirea de alarmă.
		COM2	Ieșire alarmă de manipulare a cititorului de carduri de intrare pentru ușă nr. 2.
Cu două uși în două sensuri	2 canale extern ieșire de alarmă.	NUMARUL 1	ALM1/ALM2 declanșează ieșirea de alarmă.
		COM1	
		NO2	ALM3/ALM4 declanșează ieșirea alarmă.
		COM2	
	2 canale intern ieșire de alarmă.	NC1	Ieșire alarmă de manipulare a cititoarelor de carduri de intrare și ieșire ale ușii nr. 1.
		COM1	
		NUMARUL 1	Alarmă de expirare a contactului ușii și alarma de intruziune a ușii nr.1.
		NC2	Ieșire alarmă de manipulare a cititoarelor de carduri de intrare și ieșire ale ușii nr. 2.
		COM2	
		NO2	Alarma de expirare a contactului ușii și alarma de intruziune a ușii nr.2.
Cu patru uși Sens unic	Ieșire alarmă cu 1 canal.	NU	ALM declanșează ieșirea de alarmă.
		COM	Alarmă de timeout contact ușă și alarmă de intruziune. Ieșire alarmă de manipulare a cititorului de carduri.

2.1.3 Conectarea prin cablu a cititorului de carduri

O singură ușă acceptă un singur tip de cititor de carduri: RS-485 sau Wiegand.

Tabelul 2-3 Specificațiile cablului și lungimea cititorului de carduri

Tip cititor de carduri	Modul de conectare	Lungime
Cititor de carduri RS-485	Cablu de rețea CAT5e, conexiune RS-485	100 m
Cititor de carduri Wiegand	Cablu de rețea CAT5e, conexiune Wiegand	30 m

2.2 Instalarea dispozitivului

Există două metode de instalare.

- Fixați dispozitivul pe perete cu șuruburi.
- Instalați șina de ghidare în formă de U (nu este furnizată) pe perete și apoi agățați dispozitivul de șina de ghidare.

Figure 2-4 Instalare (1)

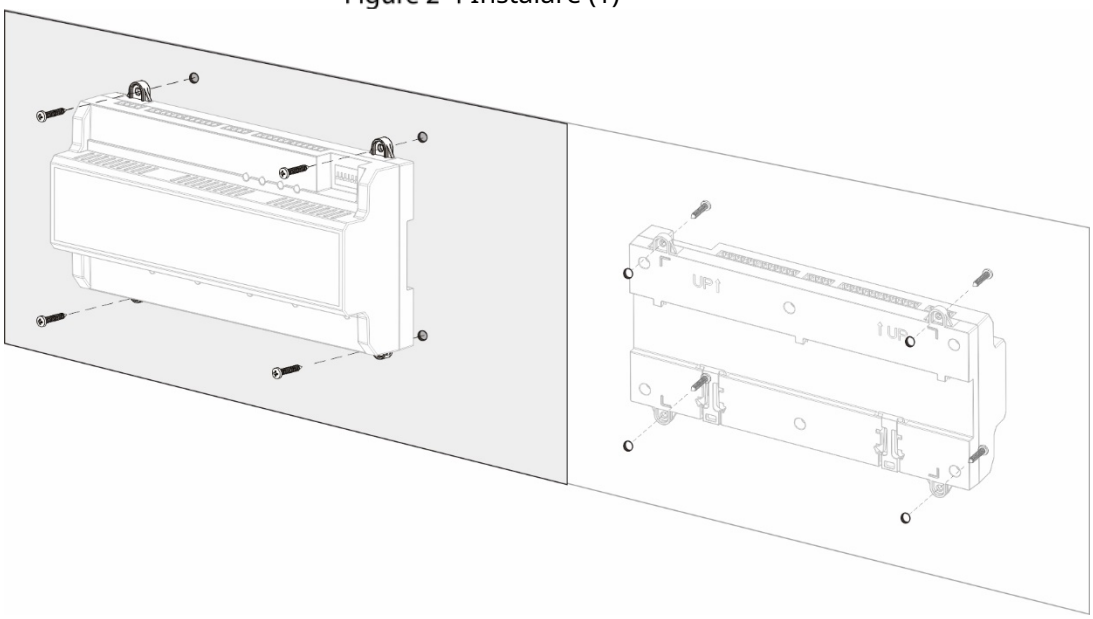
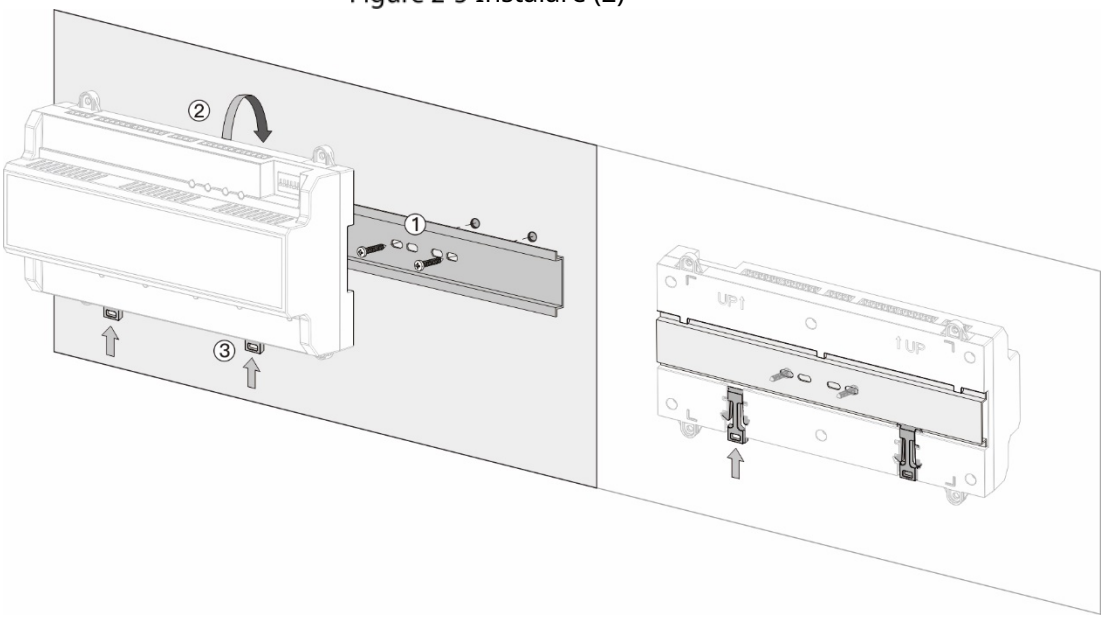


Figure 2-5 Instalare (2)



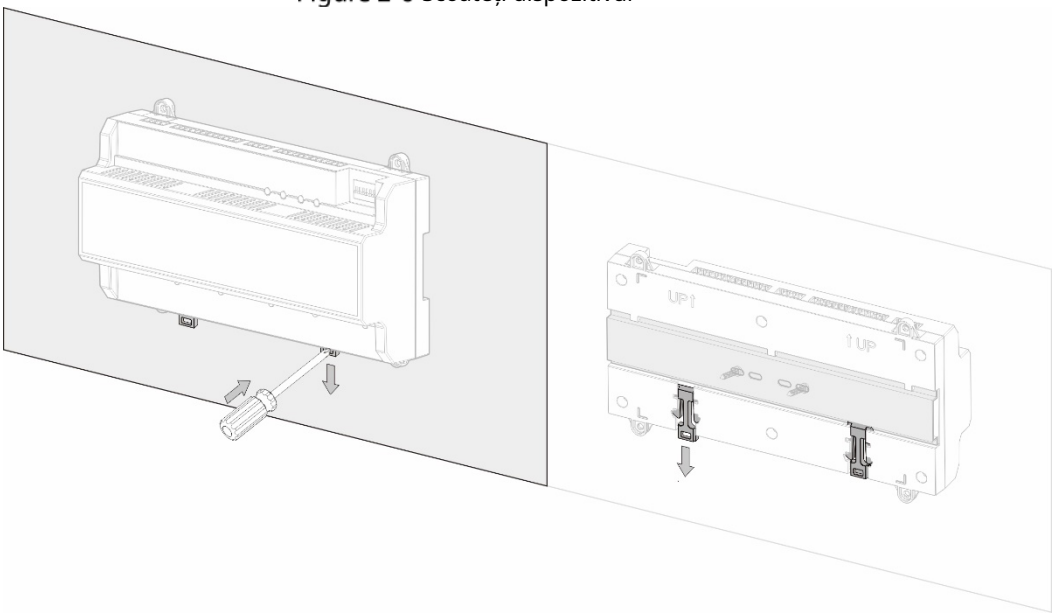
Step 1 Fixați șina de ghidare în formă de U pe perete cu șuruburi.
Step 2 Închideți partea superioară din spate a dispozitivului în șina de ghidare în formă de U.
Step 3 Împingeți catarama din partea inferioară a dispozitivului până când auziți un clic.

2.3 Scoaterea dispozitivului

Dacă Dispozitivul este instalat cu a doua metodă de instalare, vă rugăm să consultați Figura 2-6 când doriți să eliminați Dispozitivul.

Folosiți o șurubelniță pentru a apăsa ferm catarama, apoi aruncați catarama pentru a scoate dispozitivul.

Figure 2-6 Scoateți dispozitivul



3 Configurare SmartPSS AC

Puteți gestiona dispozitivul prin SmartPSS AC. Această secțiune prezintă în principal configurarea rapidă a dispozitivelor. Pentru detalii, consultați manualul utilizatorului SmartPSS AC.

Capturile de ecran ale clientului Smart PSS AC din acest manual sunt doar pentru referință și pot diferi de produsul real.

3.1 Log in

Step 1 Instalați SmartPSS AC.

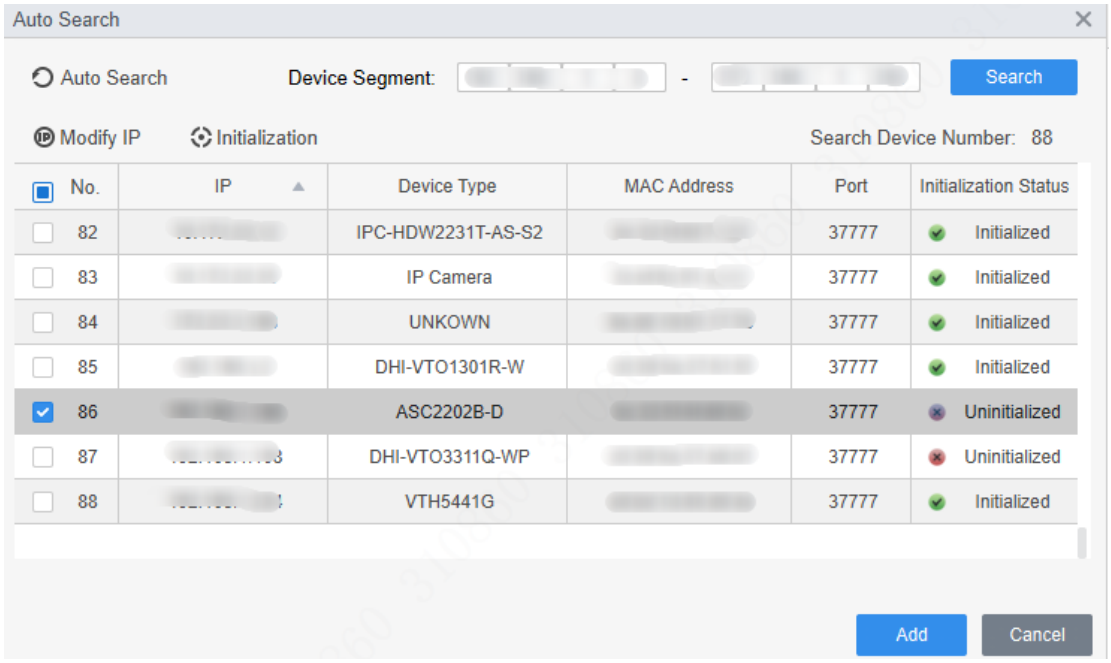
Step 2 Dublu click , apoi urmați instrucțiunile pentru a finaliza inițializarea și a vă conecta.

3.2 Inițializare

Înainte de inițializare, asigurați-vă că dispozitivul și computerul sunt în aceeași rețea.

Step 1 Pe pagina de pornire, selectați**Manager de dispozitiv**, apoi faceți clic**Căutare automată**.

Figure 3-1 Căutare automată



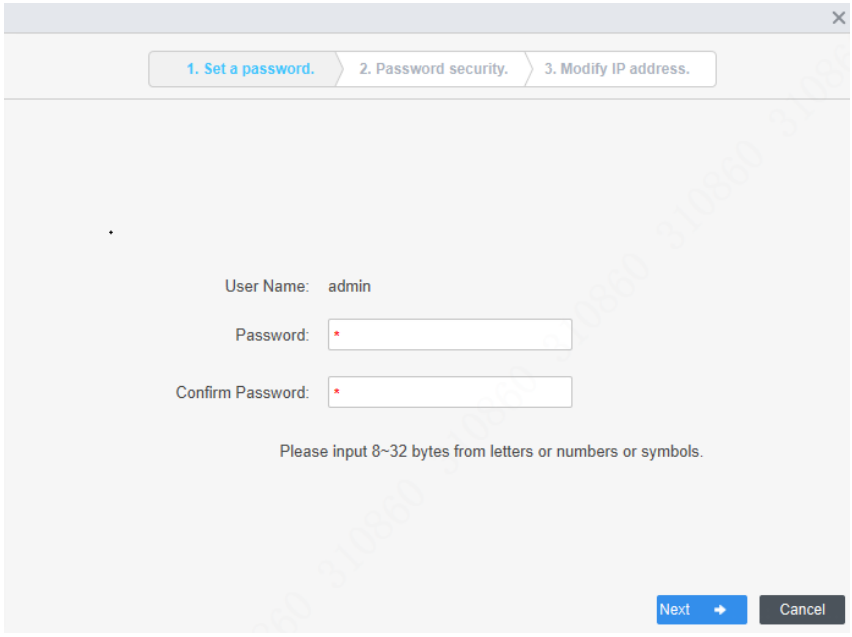
Step 2 Introduceți un interval de segment de rețea, apoi faceți clic**Căutare**.

Step 3 Selectați dispozitivul și apoi faceți clic**Inițializare**. Setați parola de

Step 4 administrator, apoi faceți clic**Următorul**.

Dacă uitați parola, utilizați comutatorul DIP pentru a restabili setările implicite din fabrică. Pentru detalii, vezi „1.4 Componente".

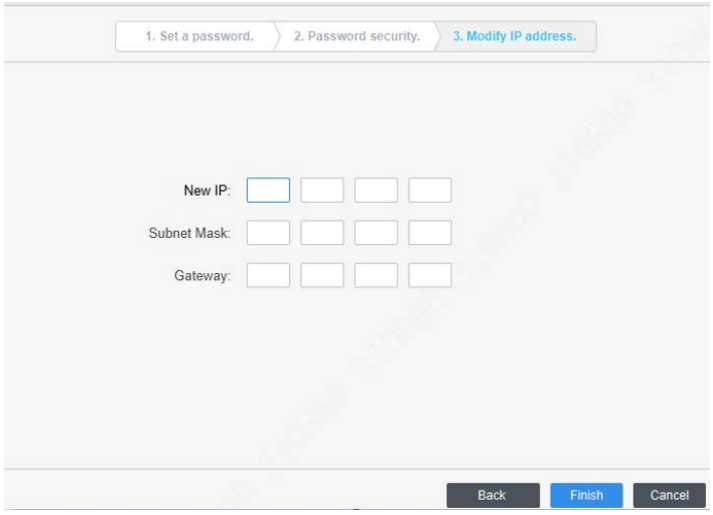
Figure 3-2 Seteaza parola



Step 5 Asociați numărul de telefon, apoi faceți clic**Următorul**.

Step 6 Introduceți noua IP, mască de subrețea și gateway.

Figure 3-3 Modificați adresa IP



Step 7 Clic**finalizarea**.

3.3 Adăugarea de dispozitive

Trebuie să adăugați dispozitivul la SmartPSS AC. Puteți adăuga dispozitive în loturi prin căutare automată sau puteți adăuga dispozitive individual.

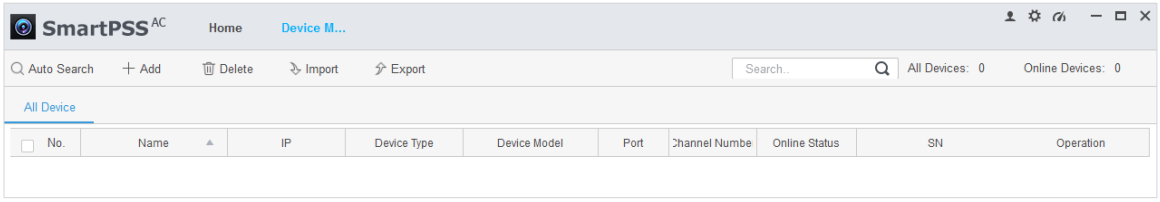
3.3.1 Căutare automată

Vă recomandăm să adăugați dispozitive prin căutare automată atunci când trebuie să adăugați dispozitive în loturi pe același segment de rețea sau când cunoașteți intervalul segmentului de rețea în loc de adresa IP exactă.

Step 1 Conectați-vă la SmartPSS AC.

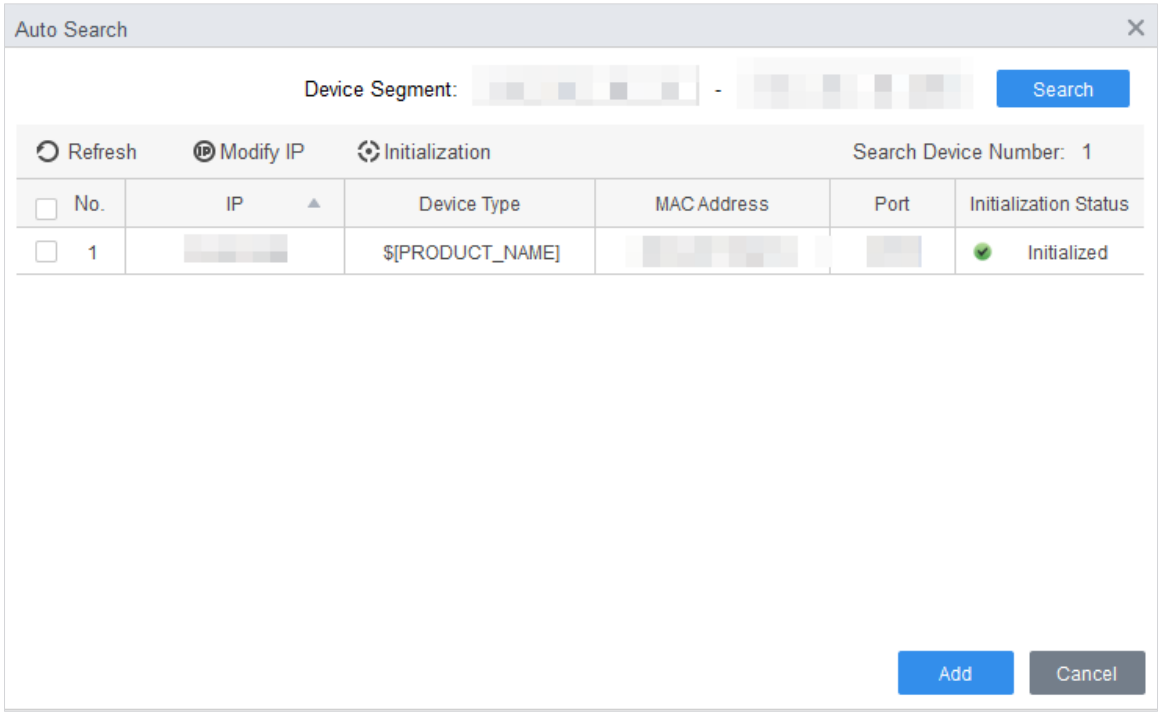
Step 2 Clic**Manager de dispozitiv**în colțul din stânga jos.

Figure 3-4 Dispozitive



Step 3 Clic**Căutare automată**.

Figure 3-5 Căutare automată



Step 4 Introduceți segmentul de rețea, apoi faceți clic**Căutare**.

- Clic**Reîmprospăta**pentru a actualiza informațiile despre dispozitiv.
- Selectați un dispozitiv, faceți clic**Modificați IP-ul**pentru a-și modifica adresa IP.

Step 5 Selectați dispozitivele pe care doriți să le adăugați la SmartPSS AC, apoi faceți clic**Adăuga**. Introduceți

Step 6 numele de utilizator și parola de conectare pentru a vă autentifica.

- Numele de utilizator este admin și parola este admin123 în mod implicit. Vă recomandăm modificați parola după autentificare.
- După conectarea cu succes, se afișează starea dispozitivului**Pe net**. În caz contrar, se afișează**Deconectat**.

3.3.2 Adăugarea manuală

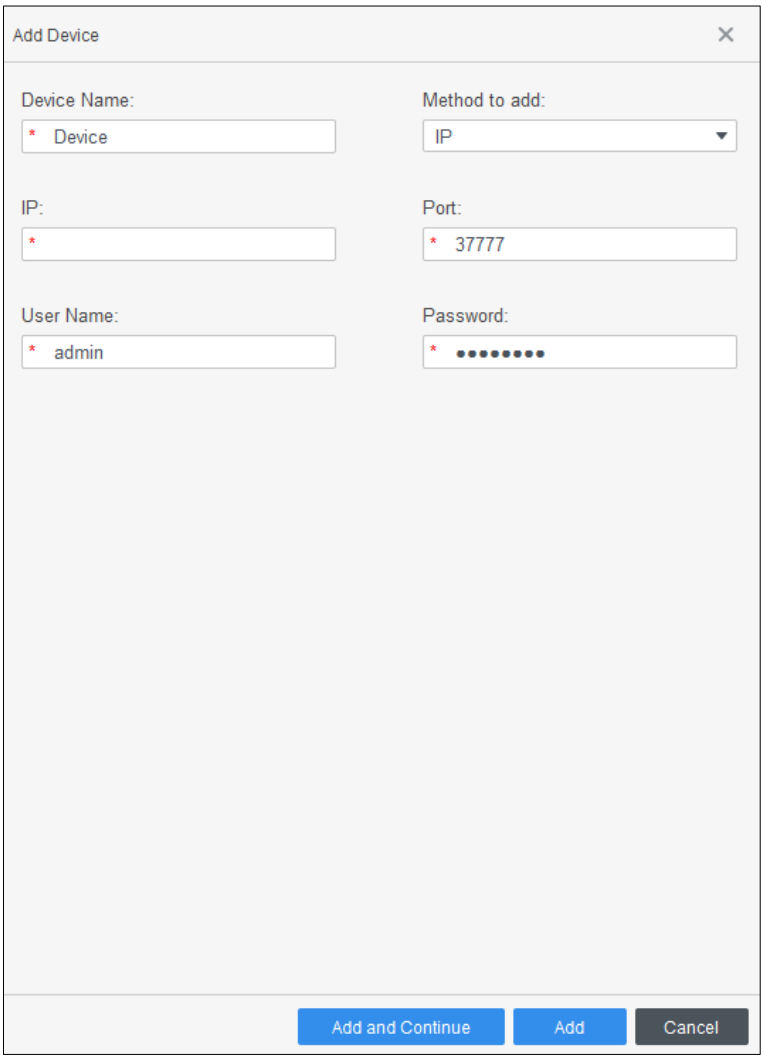
Puteți adăuga dispozitive manual. Trebuie să știți adresele IP și numele de domenii ale controlerului de acces pe care doriți să-l adăugați.

Step 1 Conectați-vă la SmartPSS AC.

Step 2 Clic**Manager de dispozitiv**în colțul din stânga jos. Clic

Step 3 **Adăuga**pe**Manager de dispozitiv**pagină.

Figure 3-6 Adăugarea manuală



Step 4 Introduceți informațiile despre dispozitiv.

Tabelul 3-1 Parametri

Parametru	Descriere
Nume dispozitiv	Introduceți un nume pentru dispozitiv. Vă recomandăm să denumiți dispozitivul după locația de instalare pentru o identificare ușoară.
Metoda de adaugat	Selectați**IP**pentru a adăuga Dispozitivul prin adresa sa IP.
IP	Introdu adresa IP a dispozitivului. Este implicit 192.168.1.108.
Port	Introduceți numărul portului dispozitivului. Numărul de port implicit este 37777.
Nume de utilizator, Parola	Introduceți numele de utilizator și parola dispozitivului. Numele de utilizator este admin și parola este admin123 în mod implicit. Se recomandă modificarea parolei după autentificare.

Step 5 Clic**Adăuga**, iar apoi puteți vedea Dispozitivul pe**Dispozitive**pagină.

După adăugare, SmartPSS AC se conectează automat la Dispozitiv. După conectarea cu succes, afișează stare**Pe net**. În caz contrar, se afișează**Deconectat**.

3.4 Managementul utilizatorilor

3.4.1 Setare tip card

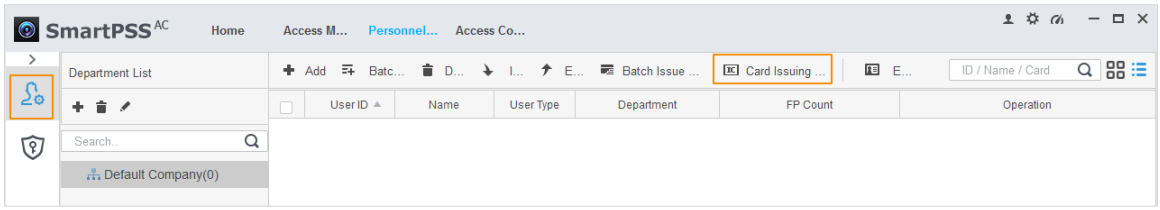
Înainte de a atribui cardul, setați mai întâi tipul cardului. De exemplu, dacă cardul alocat este carte de identitate, selectați tipul ca carte de identitate.

Tipul de card selectat trebuie să fie același cu tipul de card alocat real; altfel numere de card nu poate fi citit.

Step 1 Conectați-vă la SmartPSS AC.

Step 2 Clic**Manager de personal**.

Figure 3-7 Manager de personal

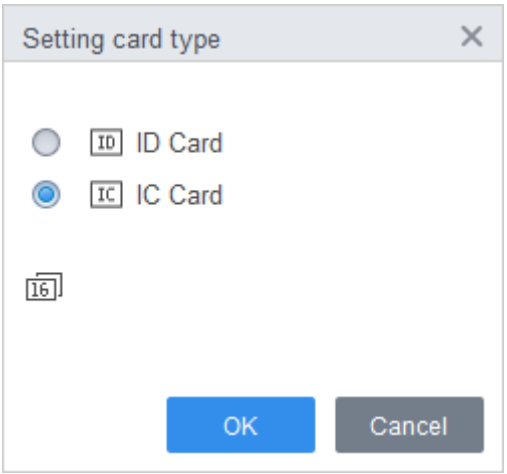


Step 3 Pe**Manager de personal**pagina, faceți clic  , apoi faceți clic  .

Step 4 Pe**Setarea tipului cardului**pagina, selectați un tip de card.

Step 5 Clic  pentru a selecta metoda de afișare a numărului cardului în zecimală sau în hexadecimal.

Figure 3-8 Setarea tipului cardului



Step 6 Clic**Bine**.

3.4.2 Adăugarea utilizatorului

3.4.2.1 Adăugarea manuală

Puteți adăuga utilizatori indivmanual sau manual.

Step 1 Conectați-vă la SmartPSS AC.

Step 2 Clic**Manager de personal**>**Utilizator**>**Adăuga**.

Step 3 Adăugați informații de bază ale utilizatorului.

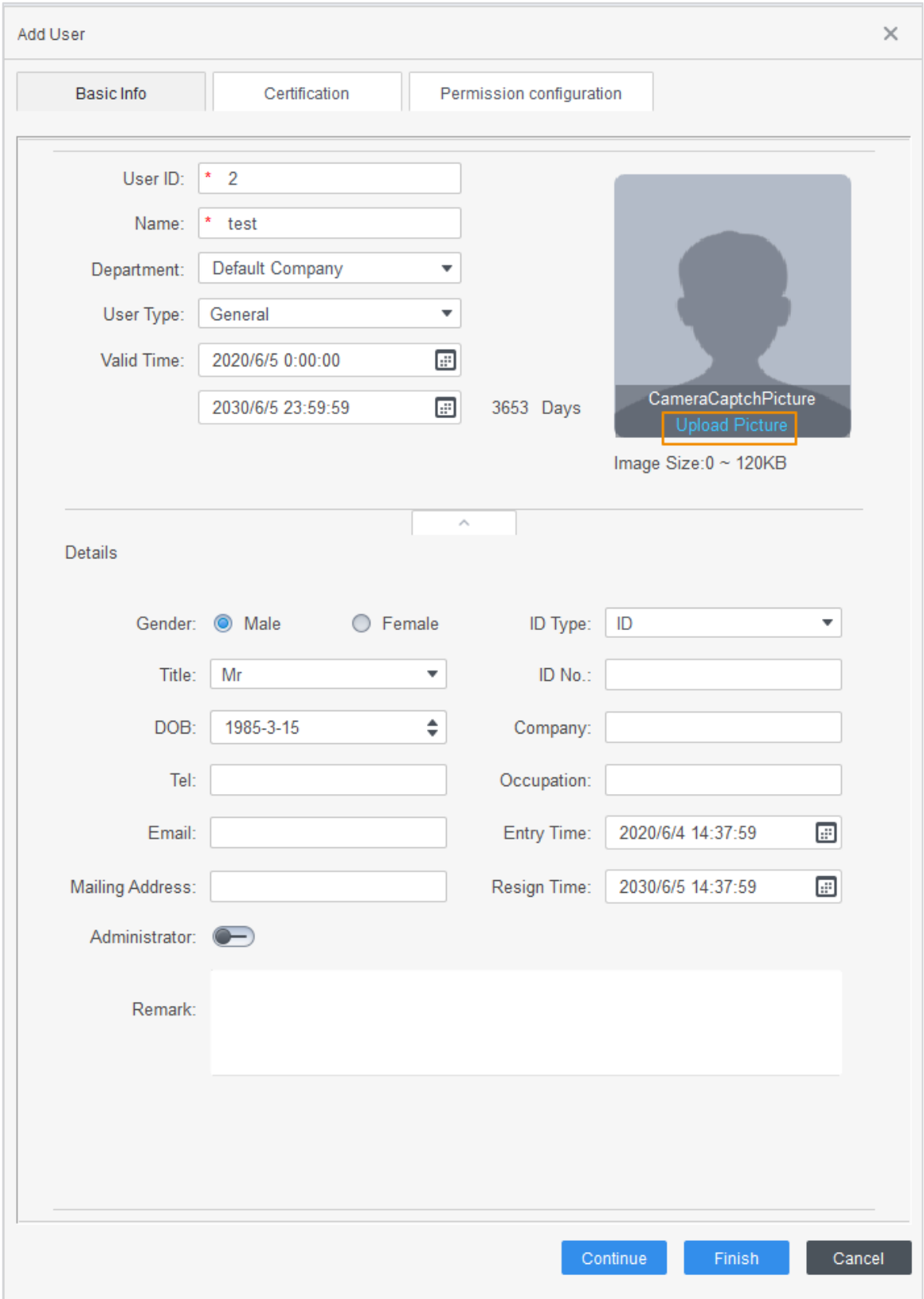
1) Faceți clic pe**Informatii de baza**fila de pe**Adăugați utilizator**pagina și apoi adăugați informații de bază despre utilizator.

2) Faceți clic pe imagine, apoi faceți clic**Încarcă imagine**pentru a adăuga o imagine a feței.

Imaginea feței încărcate se va afișa pe cadrul de captură.

Asigurați-vă că pixelii imaginii sunt mai mari de 500 × 500; dimensiunea imaginii este mai mică de 120 KB.

Figure 3-9 Adăugați informații de bază



Step 4 Apasă pe**Certificare**pentru a adăuga informații de certificare ale utilizatorului.

- Configurați parola.

  Seteaza parola. Pentru controlerele de acces din a doua generație, setați parola de personal; pentru alte dispozitive, setați parola cardului. Noua parolă trebuie să fie formată din 6 cifre. Configurați
- cardul.

Numărul cardului poate fi citit automat sau completat manual. Pentru citire automată, selectați un cititor de carduri, apoi așezați cardul pe cititorul de carduri. Se citește numărul cardului automat după aceea.

1) Faceți clic  a selecta**Dispozitiv**sau**Emitentul cardului**ca cititor de carduri.

2) Adăugați card. Numărul cardului trebuie adăugat dacă este utilizat controlerul de acces care nu este de a doua generație.

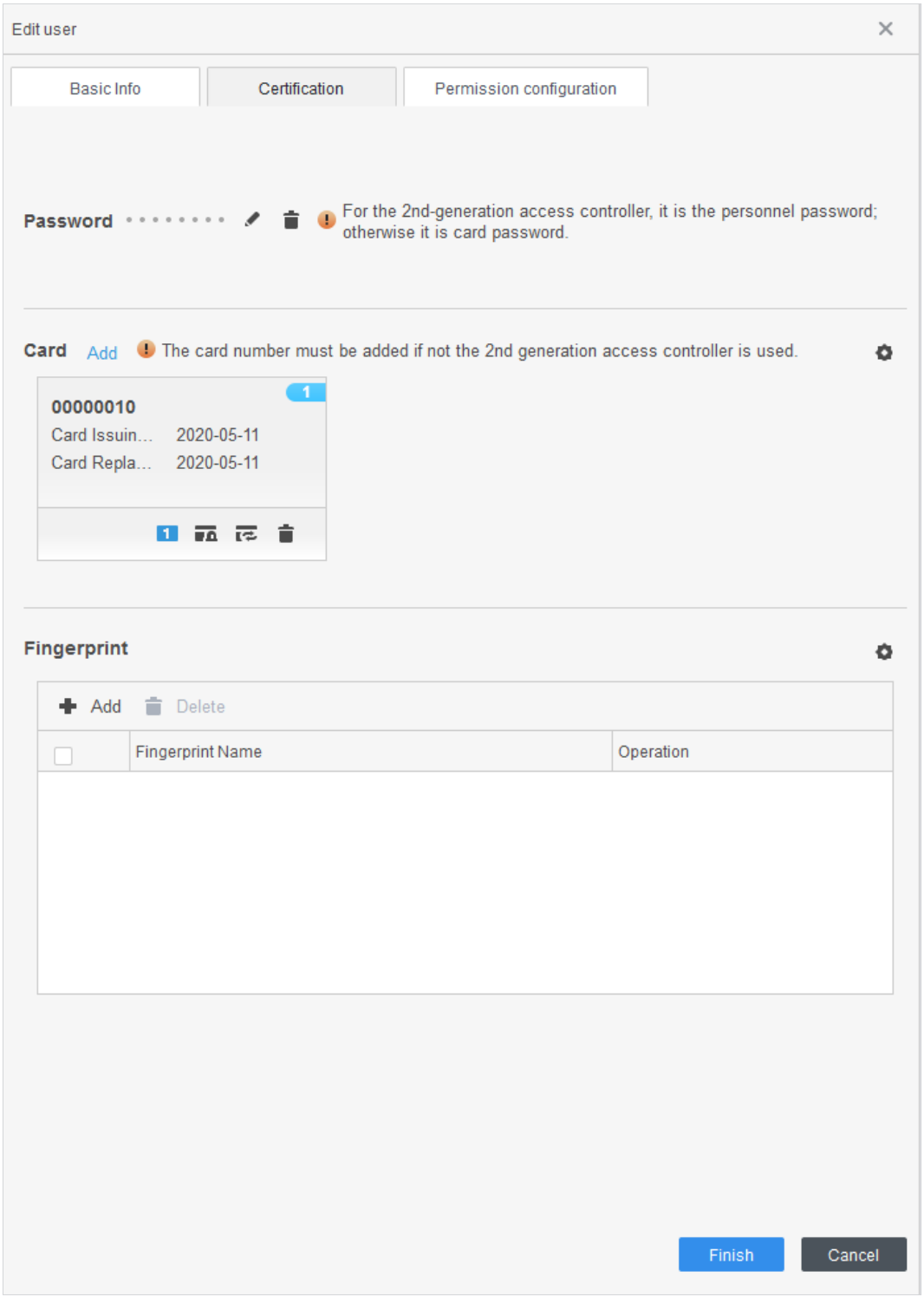
3) După adăugare, puteți selecta cardul ca card principal sau card de constrângere sau puteți înlocui cardul cu unul nou sau ștergeți cardul.

- Configurați amprenta digitală.

1) Faceți clic  a selecta**Dispozitiv**sau**Scaner de amprente**ca colector de amprente.

2) Adăugați amprenta. Clic**Adăugați amprenta**și apăsați degetul pe scaner de trei ori continuu.

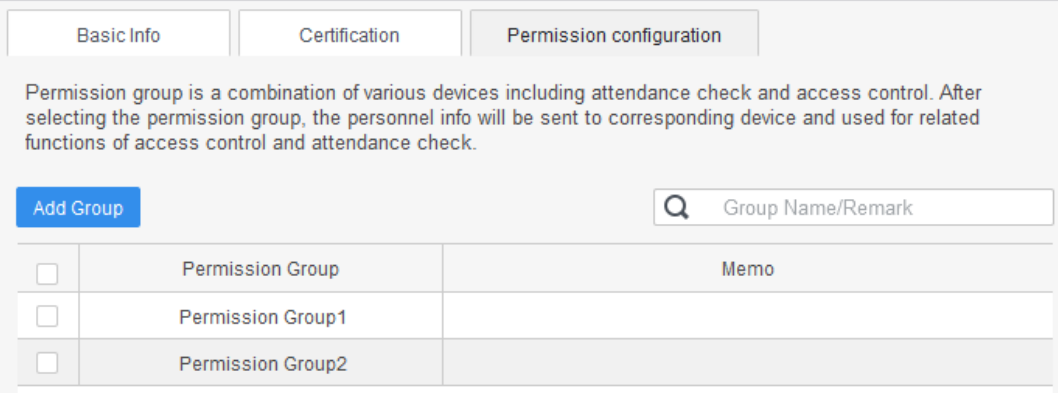
Figure 3-10 Configurați certificarea



Step 5 Configurați permisiunea pentru utilizator.

Pentru detalii, consultați „3.5 Configurarea permisiunii”.

Figure 3-11 Configurarea permisiunii



Step 6 Clic**finalizarea**.

3.4.2.2 Adăugarea în loturi

Puteți adăuga utilizatori în loturi.

Step 1 Conectați-vă la SmartPSS AC.

Step 2 Clic**Manager de personal**>**Utilizator**>**Adăugare lot**. Selectați

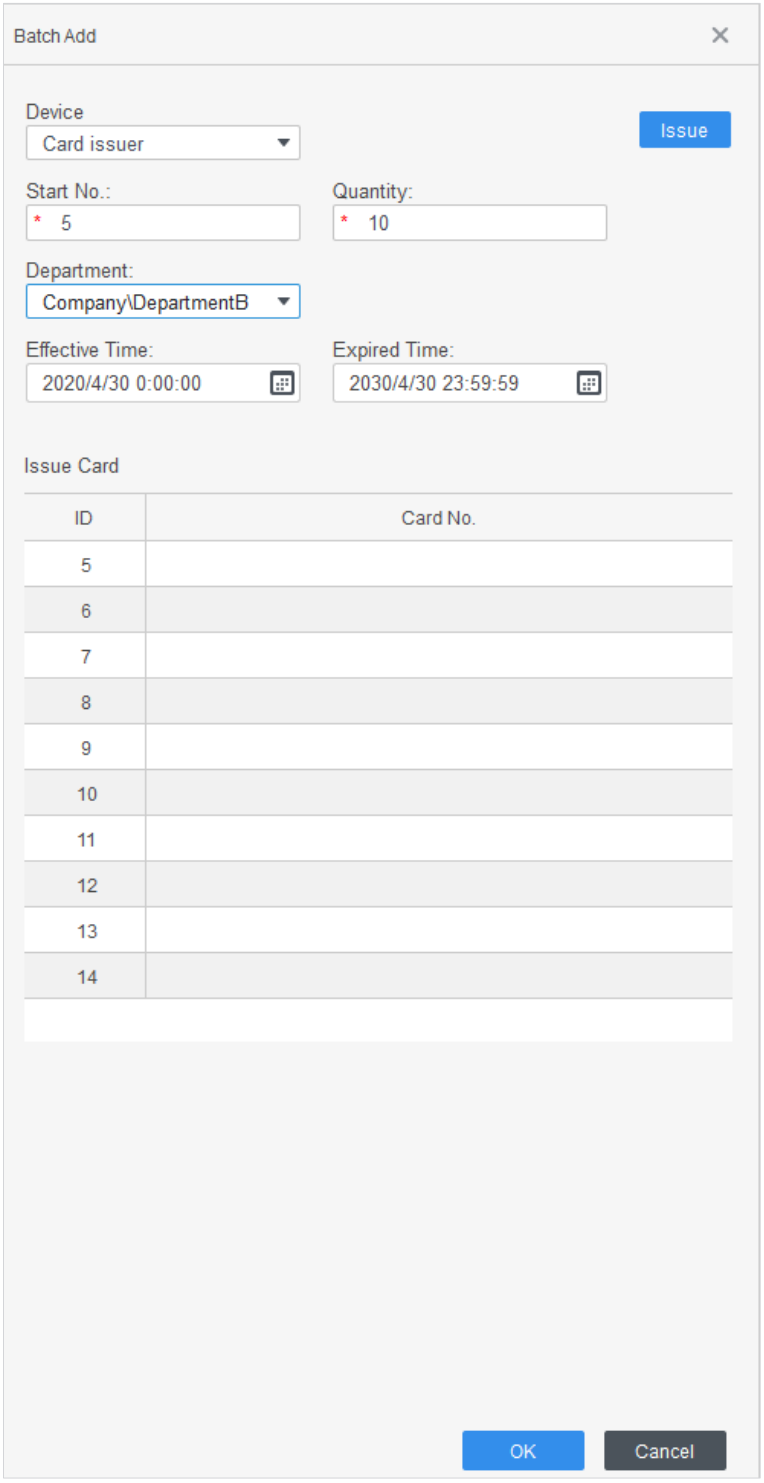
Step 3 cititorul de carduri și departamentul de utilizator.

Step 4 Setați numărul de început, cantitatea cardului, timpul efectiv și timpul expirat al

Step 5 cardului. Clic**Emisiune**pentru a atribui carduri de acces utilizatorilor. Numărul cardului va fi citit automat. Clic**Stop**după atribuirea cardului, apoi faceți clic**Bine**.

Step 6

Figure 3-12 Adăugați utilizator în loturi



Step 7 În lista de utilizatori, faceți clic pentru a modifica informații sau pentru a adăuga detalii despre utilizatori.

3.5 Configurarea permisiunii

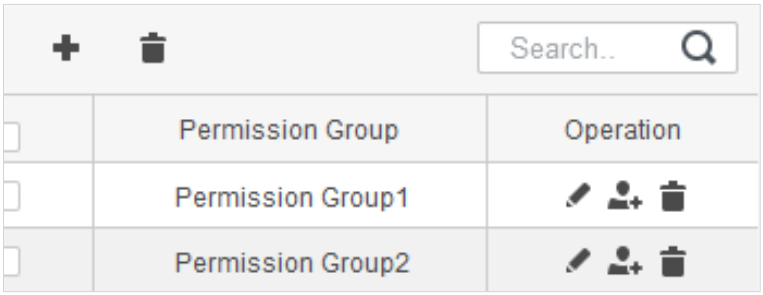
3.5.1 Adăugarea unui grup de permisiuni

Creați un grup de permisiuni care este o colecție de permisiuni de acces la uși.

Step 1 Conectați-vă la SmartPSS AC.

Step 2 Clic**Manager de personal**>**Configurarea permisiunii**.

Figure 3-13 Lista grupurilor de permisiuni



Step 3 Clic pentru a adăuga un grup de permisiuni.

Step 4 Setați parametrii de permisiune.

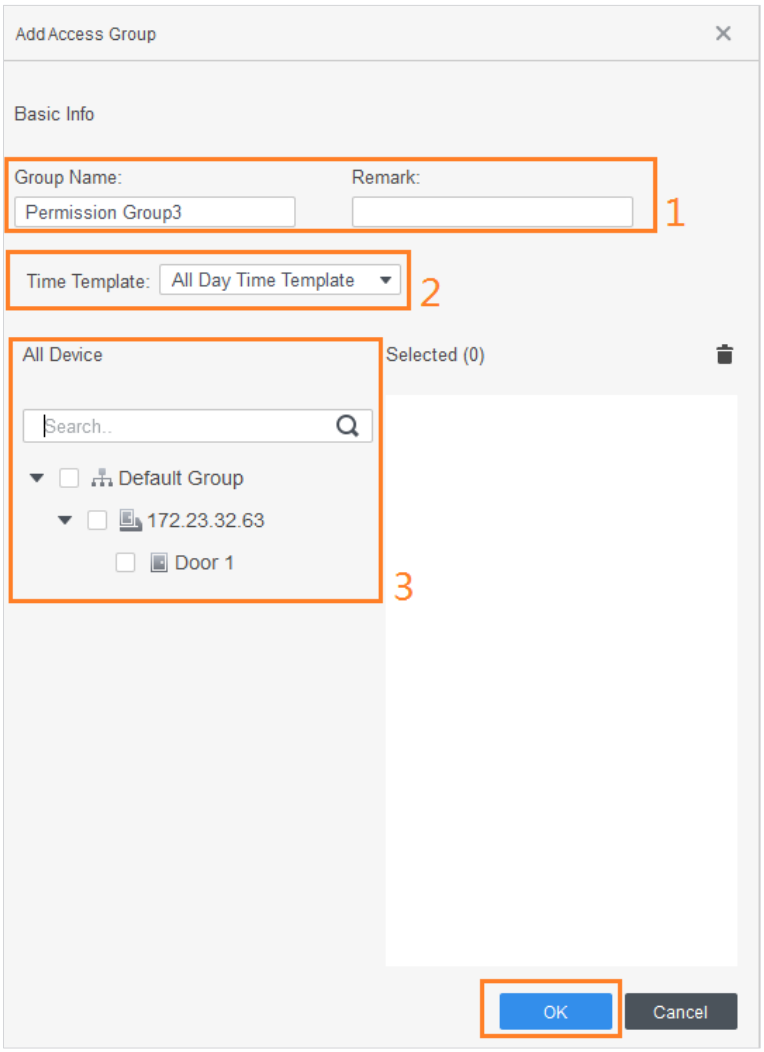
1) Introduceți numele grupului și observația.

2) Selectați un șablon de timp.

Pentru detalii, consultați manualul de utilizare SmartPSS AC.

3) Selectați dispozitivul corespunzător, cum ar fi ușa 1.

Figure 3-14 Adăugați un grup de permisiuni



Step 5 Clic**Bine**.

Pe**Lista grupurilor de permisiuni**pagină:

- Clic pentru a șterge grupul.
- Clic pentru a modifica informațiile de grup.
- Faceți dublu clic pe numele grupului de permisiuni pentru a vedea informațiile grupului.

3.5.2 Atribuirea permisiunilor de acces

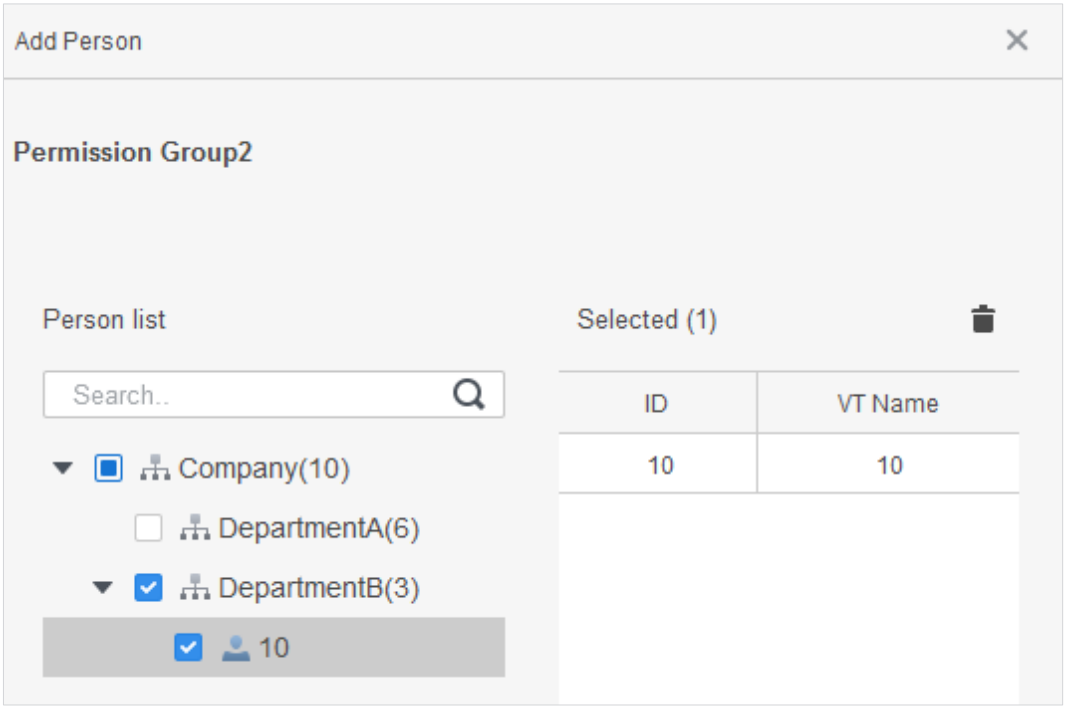
Asociați utilizatorii cu grupurile de permisiuni dorite, iar apoi utilizatorilor li se vor atribui permisiuni de acces la ușile definite.

Step 1 Conectați-vă la SmartPSS AC.

Step 2 Clic**Manager de personal**>**Configurarea permisiunii**.

Step 3 Selectați un grup de permisiuni, apoi faceți clic .

Figure 3-15 Configurați permisiunea



Step 4 Selectați utilizatori pentru a-i asocia cu grupul selectat.

Step 5 Clic**Bine**.

3.6 Configurația controlerului de acces

3.6.1 Configurare funcții avansate

3.6.1.1 Deblocarea primului card

Alți utilizatori pot glisa pentru a debloca ușa numai după ce primul deținător de card specificat trece cardul. Puteți seta mai multe prime cărți. Alți utilizatori fără primul card pot debloca ușa numai după ce unul dintre deținătorii primului card glisează primul card.

- Persoana care i se acordă permisiunea pentru primul card ar trebui să fie**General**tip de utilizator și au acces la anumite uși. Pentru detalii, consultați „3.4.2 Adăugarea unui utilizator”.
- Pentru detalii despre atribuirea permisiunilor, consultați „3.5 Configurarea permisiunii”.

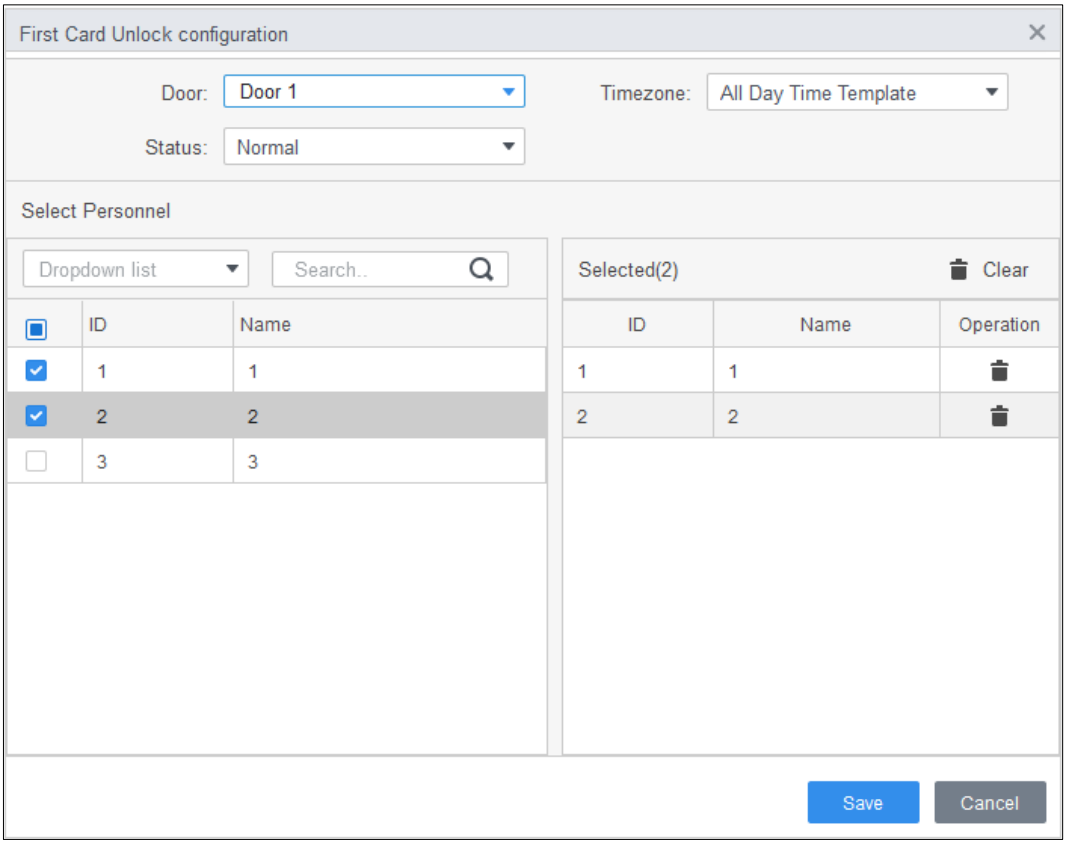
Step 1 Selectați**Configurare acces**>**Configurare avansată**. Apasă pe

Step 2 **Prima deblocare a cardului**fila. Clic**Adăuga**.

Step 3

Step 4 Configurați**Prima deblocare a cardului**parametrii și faceți clic**Salvați**.

Figure 3-16 Prima configurație de deblocare a cardului



Tabelul 3-2 Parametrii deblocării primei carduri

Parametru	Descriere
Uşă	Selectați ușa pentru permisiunea primului card.

Parametru	Descriere
Fus orar	Permisiunea primului card este valabilă numai în timpul șablonului de timp selectat.
stare	După ce prima deblocare a cardului este activată, selectați starea ușii:**Mod normal**sau **Modul Întotdeauna Deschis**.
Utilizator	Puteți selecta unul sau mai mulți deținători ai primului card.

Step 5 (Opțional) Faceți clic . Pictograma se schimbă în indica**Prima deblocare a cardului**este activat.

Cel nou adăugat**Prima deblocare a cardului**este activat implicit.

3.6.1.2 Deblocare cu mai multe carduri

Utilizatorii pot debloca ușa numai după ce utilizatorii sau grupurile de utilizatori definiți acordă acces în secvență.

- Un grup poate avea până la 50 de utilizatori, iar o persoană poate aparține mai multor grupuri.
- Puteți adăuga până la patru grupuri de utilizatori cu permisiunea de deblocare cu mai multe carduri pentru o ușă, cu până la 200 de utilizatori în total și până la 5 utilizatori validi.

- Deblocarea primului card are prioritate față de deblocarea cu mai multe carduri, ceea ce înseamnă că cele două reguli sunt ambele activată, prima deblocare a cardului este pe primul loc. Vă recomandăm să nu atribuiți deblocarea cu mai multe carduri permisiunea primilor deținători de card.
- Nu setați tipul VIP sau Patrol pentru persoanele din grupul de utilizatori. Pentru detalii, consultați „3.4.2 Adăugarea unui utilizator”.
- Pentru detalii despre atribuirea permisiunilor, consultați „3.5 Configurarea permisiunii”.

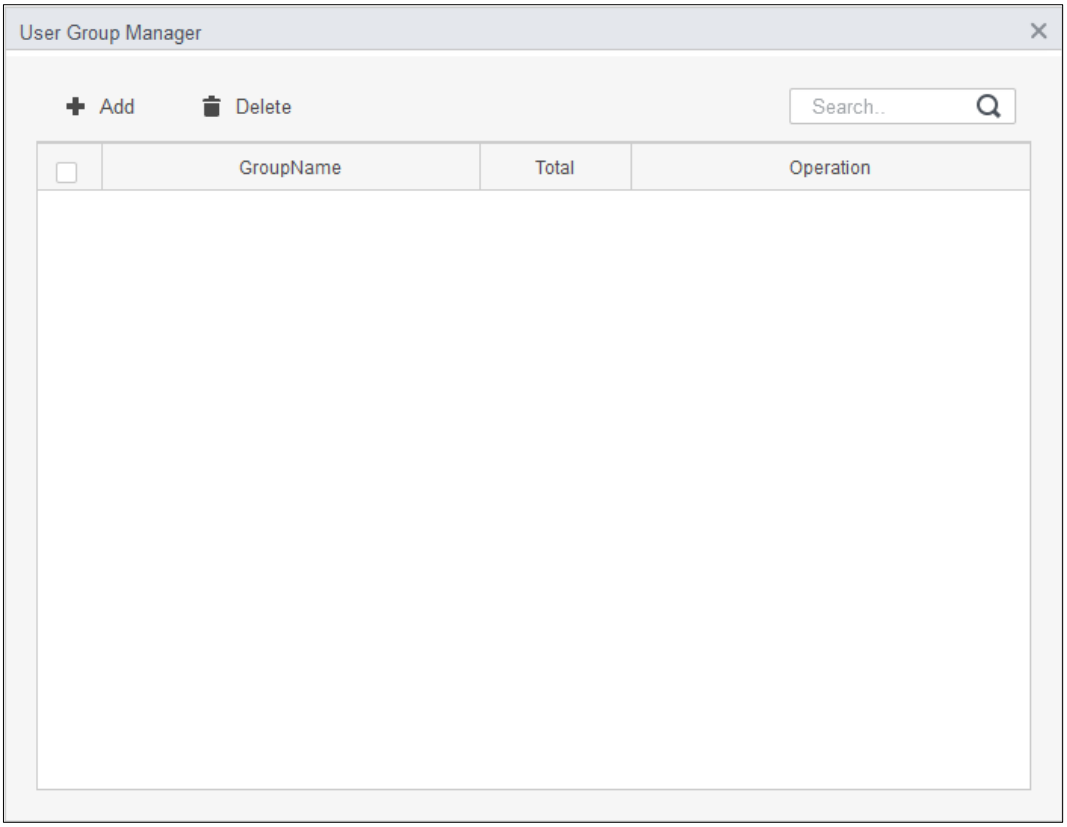
Step 1 Selectați**Configurare acces**>**Configurare avansată**. Apasă pe

Step 2 **Deblocare cu mai multe carduri**fila. Adăugați un grup de utilizatori.

Step 3

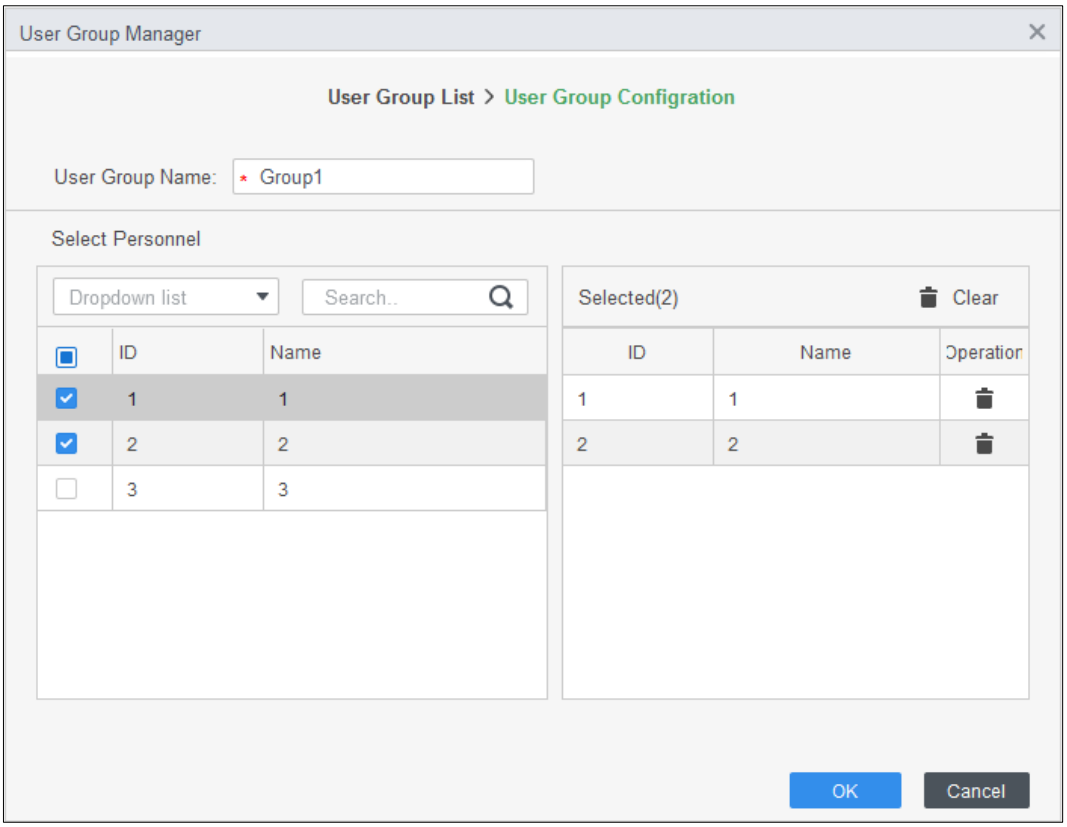
1) Faceți clic**Grup de utilizatori**.

Figure 3-17 Manager de grup de utilizatori



2) Faceți clic**Adăuga**.

Figure 3-18 Configurarea grupului de utilizatori



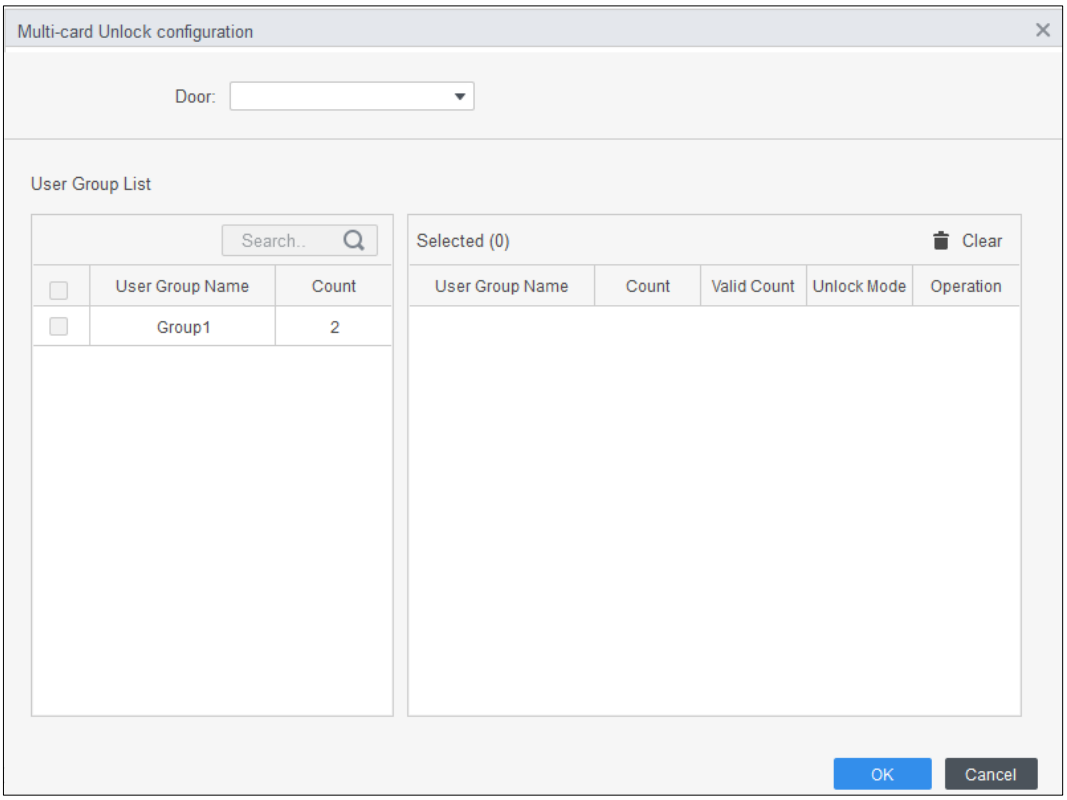
3) Introduceți numele grupului de utilizatori. Selectați utilizatori din lista de utilizatori și faceți clic**Bine**. Puteți selecta până la 50 de utilizatori într-un grup.

4) Faceți clic pe .

Step 4 Configurați parametrul de deblocare a mai multor carduri.

1) Faceți clic**Adăuga**.

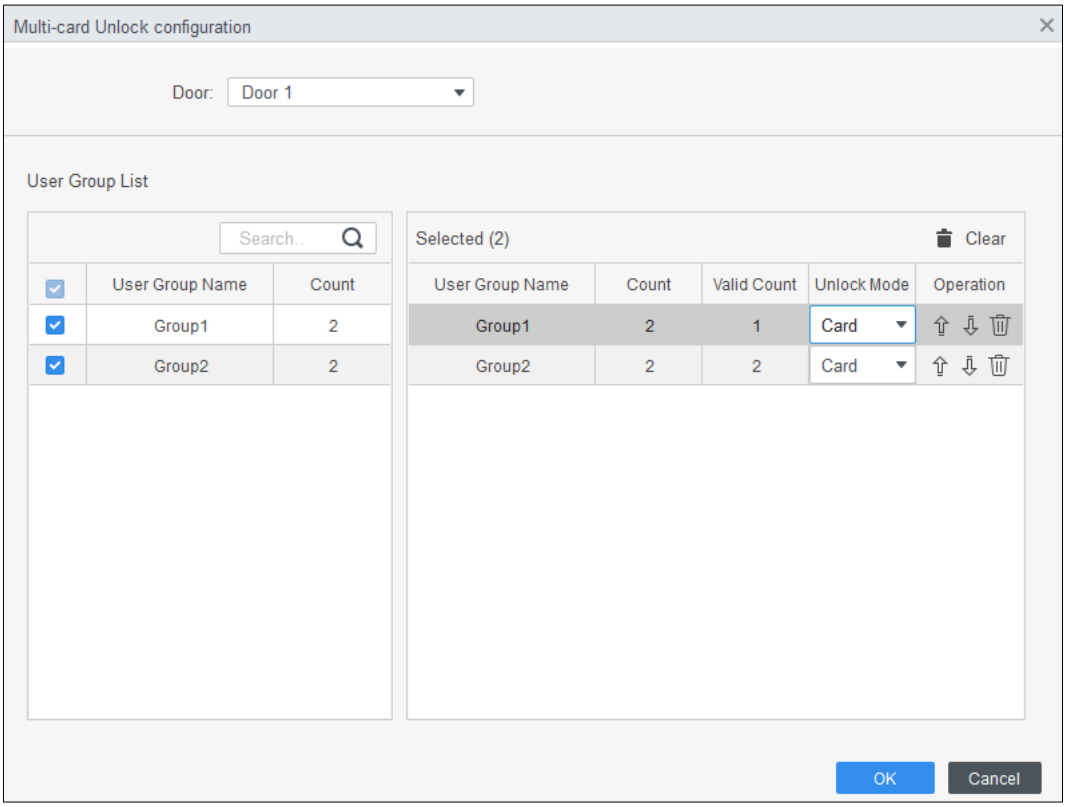
Figure 3-19 Configurație de deblocare cu mai multe carduri (1)



2) Selectați ușa.

3) Selectați grupul de utilizatori. Puteți selecta până la patru grupuri.

Figure 3-20 Configurație de deblocare cu mai multe carduri (2)



4) Introduceți**Număr valid**în fiecare grupă. Faceți clic pe sau pentru a ajusta secvența grupului

verifica identitatea.

- Numărul valid se referă la numărul de utilizatori din fiecare grup la care trebuie să fie prezenți să-și verifice identitatea pentru a debloca ușa. Luați ca exemplu Figura 3-20. Usa poate fi deblocat numai după ce un utilizator din grupul 1 trece mai întâi cardul și doi utilizatori în grup glisați cardurile.
- Sunt permise până la cinci utilizatori validi în total.

5) Faceți clic**Bine**.

Step 5 (Opțional) Faceți clic . Pictograma se schimbă în indica**Deblocare cu mai multe carduri**este activat.

The**Deblocare cu mai multe carduri**este activat implicit.

3.6.1.3 Anti-passback

Utilizatorii trebuie să își verifice identitățile atât la intrare, cât și la ieșire; în caz contrar, va fi declanșată o alarmă.

Dacă o persoană intră cu verificare validă a identității și iese fără verificare, o alarmă va fi declanșată atunci când încearcă să intre din nou și accesul este interzis în același timp.

Dacă o persoană intră fără verificarea identității și iese cu verificare, ieșirea este refuzată atunci când încearcă să iasă.

Step 1 Selectați**Configurare acces**>**Configurare avansată**. Clic

Step 2 **Adăuga**.

Step 3 Configurați parametrii.

1) Selectați dispozitivul și introduceți numele dispozitivului.

2) Selectați șablonul de timp.

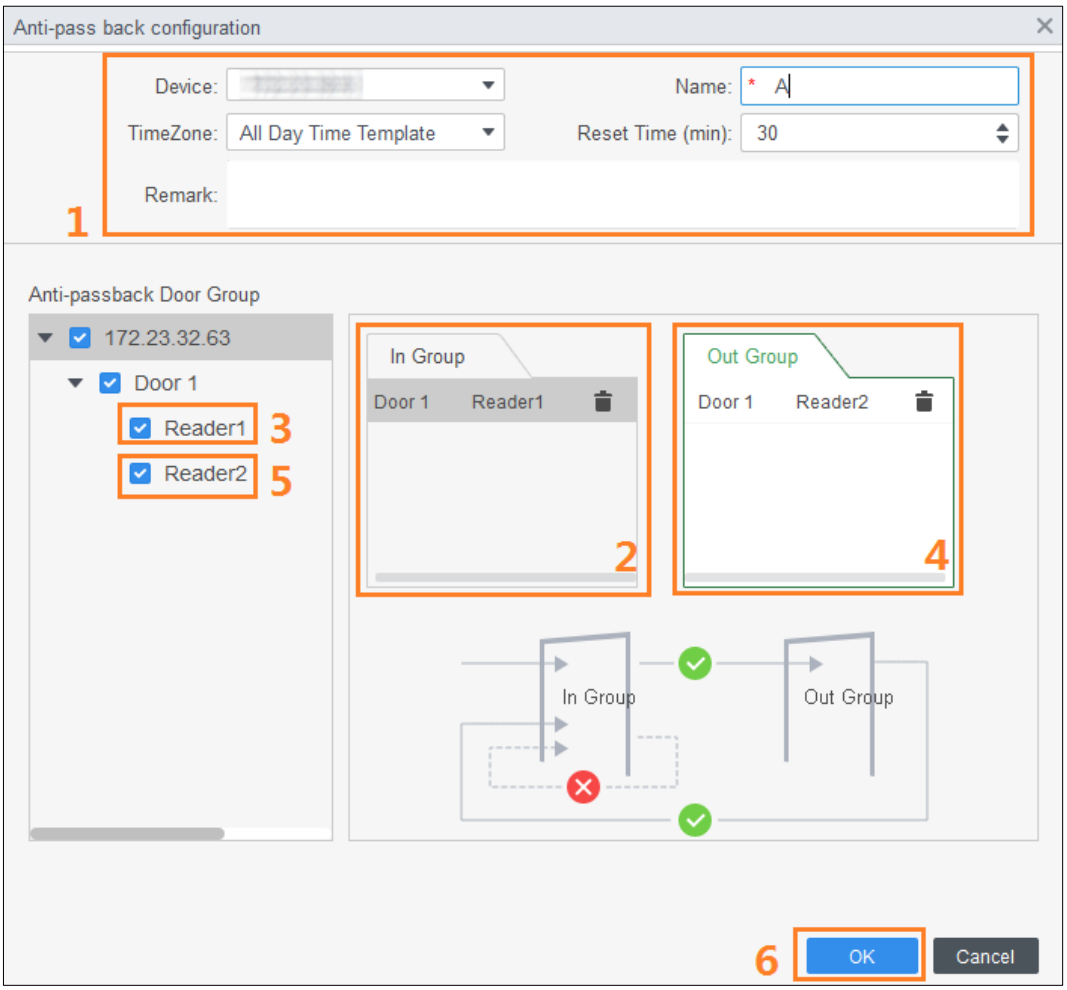
3) Setați timpul de odihnă.

De exemplu, setați timpul de resetare la 30 de minute. Dacă o persoană trece înăuntru, dar nu iese afară, alarma anti-pass back va fi declanșată atunci când persoana încearcă să treacă din nou înăuntru în decurs de 30 de minute. Ei pot intra în zona controlată până la trecerea perioadei de timp definite.

4) Faceți clic**In grup**și selectați cititorul de intrare, apoi faceți clic**Out Group**și selectați cititorul de ieșire.

5) Faceți clic**Bine**.

Figure 3-21 Configurație anti-pass back



Step 4 (Opțional) Faceți clic . Pictograma se schimbă în indica**Anti-passback**este activat.

The**Anti-passback**este activat implicit.

3.6.1.4 Blocare uși

Accesul prin una sau mai multe uși depinde de starea altei uși (sau uși). De exemplu, când două uși sunt interblocate, puteți accesa printr-o ușă numai când cealaltă ușă este închisă. Un dispozitiv acceptă două grupuri de uși cu până la 4 uși în fiecare grup.

Step 1 Selectați**Configurare acces**>**Configurare avansată**.

Step 2 Apasă pe**Inter-Lock**fila. Clic**Adăuga**.

Step 3

Step 4 Configurați parametrii și faceți clic**Bine**.

1) Selectați un dispozitiv și introduceți numele dispozitivului.

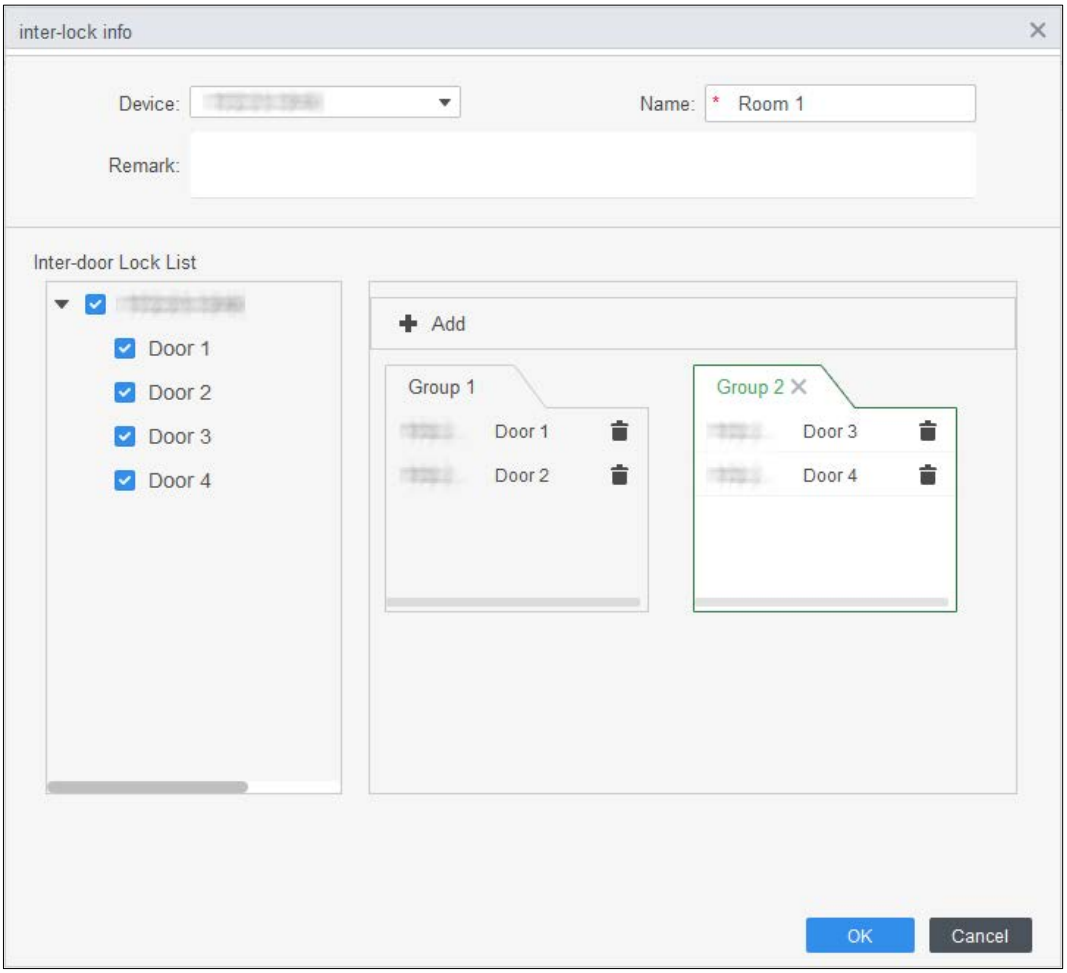
2) Introduceți observația.

3) Faceți clic**Adăuga**de două ori pentru a adăuga două grupuri de uși.

4) Adăugați uși la grupurile de uși.

5) Faceți clic**Bine**.

Figure 3-22 Configurație încuietoare inter-uși



Step 5 (Opțional) Faceți clic . Pictograma se schimbă în indica**Încuietoare inter-uși**este activat.

The**Încuietoare inter-uși**este activat implicit.

3.6.2 Configurarea controlerului de acces

Puteți configura ușa de acces, cum ar fi cititorul de intrare și cititorul de ieșire și starea ușii.

Step 1 Selectați**Configurare acces**>**Accesați Config**.

Step 2 Faceți clic pe ușă.

Step 3 Configurați parametrii.

Figure 3-23 Configurați ușa de acces

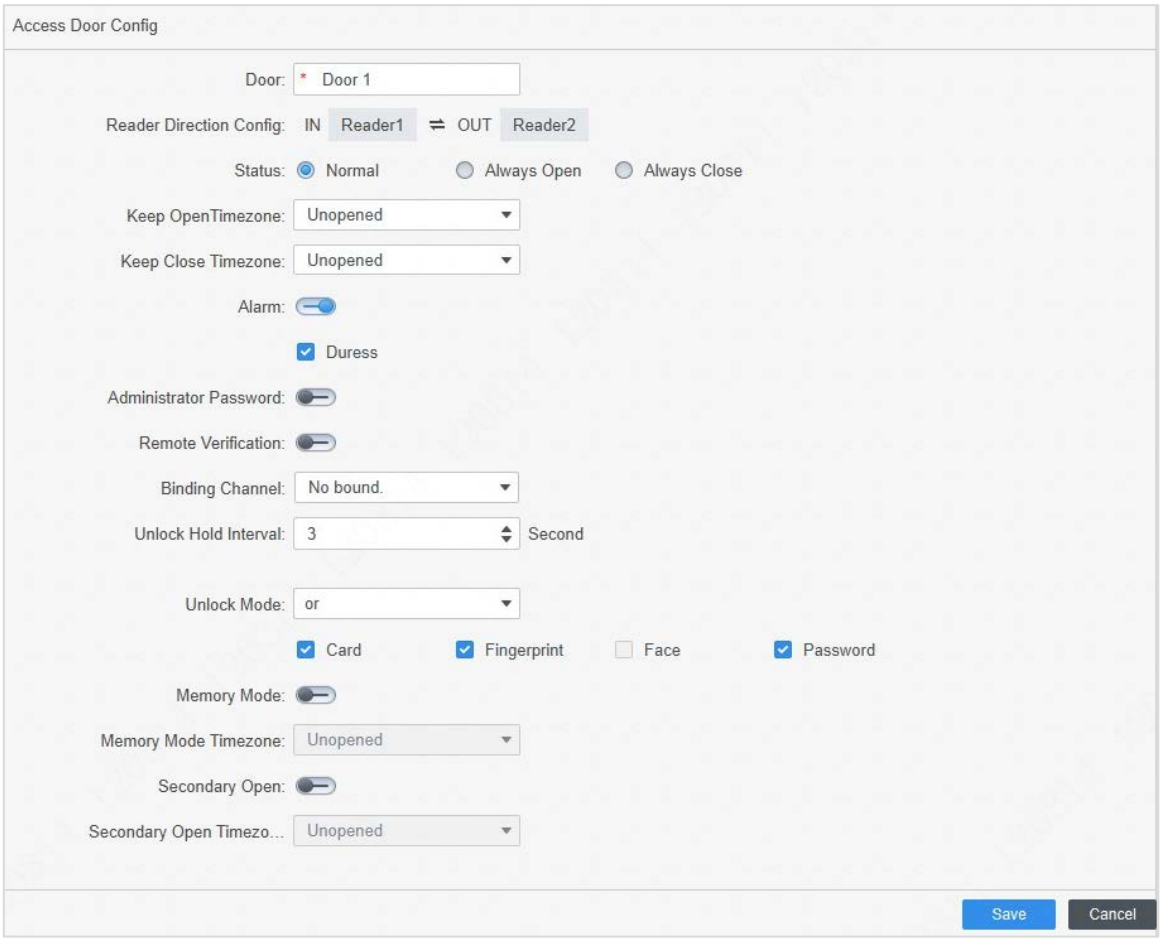
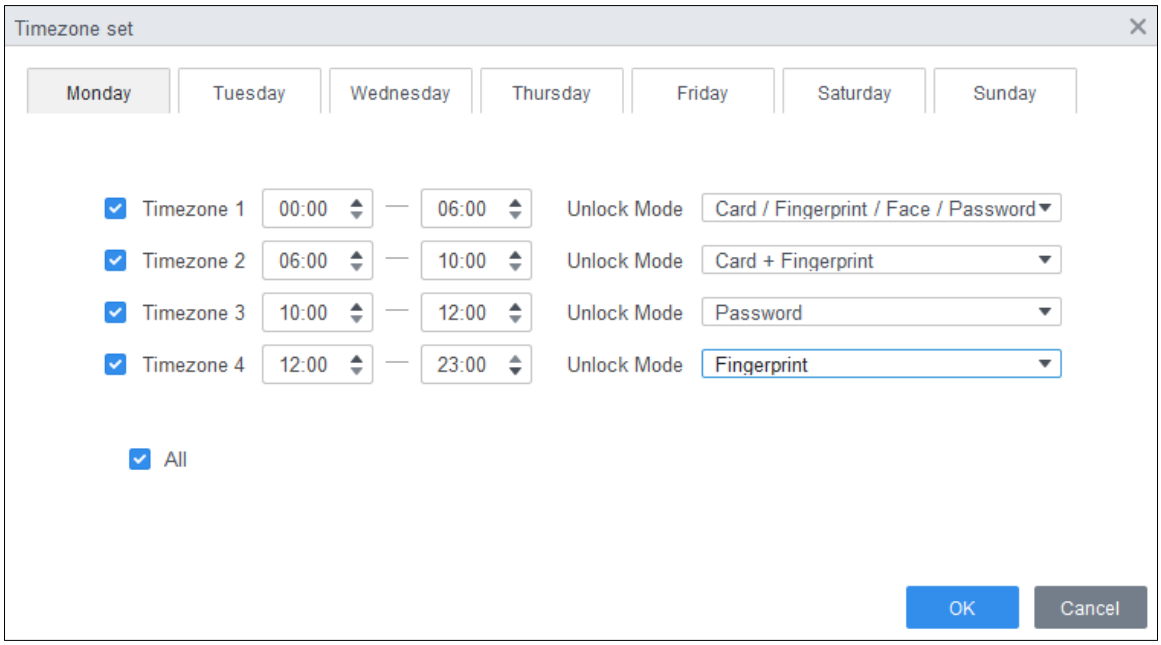


Figure 3-24 Deblocați după perioadă de timp



Tabelul 3-3 Parametrii ușii de acces

Parametru	Descriere
Uşă	Introduceți numele ușii.
Direcția cititorului	Clic ⇌ pentru a seta cititorul de intrare și ieșire.
stare	Setați starea ușii, inclusivNormal,Mereu deschisșiÎntotdeauna aproape. Nu este starea reală a ușii, deoarece SmartPSS-AC poate trimite doar comenzi către dispozitiv. Dacă doriți să aflați starea reală a ușii, activați senzorul ușii.
Păstrați fusul orar deschis	Selectați șablonul de timp și ușa va rămâne deschisă în perioada definită.
Păstrați în apropiere fusul orar	Selectați șablonul de timp și ușa va rămâne închisă în perioada definită.
Alarma	Activați funcția de alarmă și setați tipul de alarmă, inclusiv intruziune, ore suplimentare și constrângere. Când funcția de alarmă este activată, SmartPSS-AC va primi mesaje de alarmă atunci când alarma este declanșată.
Senzor de ușă	Activați senzorul ușii, astfel încât să puteți cunoaște starea reală a ușii. Vă recomandăm să activați funcția.
Parola de administrator	Activați și setați parola de administrator. Puteți accesa introducând parola.
Verificare de la distanță	Activați funcția și setați șablonul de timp. Accesul trebuie să fie acordat de la SmartPSS-AC atunci când un utilizator încearcă să deblocheze ușa după verificarea validă a identității.

Parametru	Descriere
Canal de la distanță	Conectați canalul video cu canalul de acces. Puteți vizualiza videoclipul în timp real al canalului de acces.
Deblocați intervalul de așteptare	Timpul în care ușa rămâne deschisă după deblocarea ușii. Ușa se va închide automat când se termină timpul predefinit.
Închideți Timeout	O alarmă este declanșată atunci când ușa rămâne deschisă dincolo de perioada definită. De exemplu, setați durata de închidere la 60 de secunde. Dacă ușa rămâne deschisă mai mult de 60 de secunde, alarma este declanșată.
Modul de deblocare	Selectați modul de deblocare. **Și:**Verificați toate metodele de deblocare selectate pentru a deschide ușa. **Sau**: Verificați una dintre metodele de deblocare selectate pentru a deschide ușa. **Deblocați după perioadă de timp**: Utilizatorii pot debloca ușa doar prin metode de deblocare predefinite și pe baza orarului.
Modul de memorie	După ce glisați cardul o dată, mai mult de o persoană poate trece turnichetul. Există două moduri: Oprit (implicit) și Pornit. Dacă mai multor persoane li se permite accesul prin turnichet, iar una dintre ele nu a început să treacă de turnichet în 5 secunde, sau una dintre ele nu a trecut de turnichet într-o perioadă definită și rămâne peste timp între turnichete, barierele de leagăn vor fi blocate. . În acest moment, trebuie să glisați cardurile de mai multe ori pentru a permite mai multor persoane să treacă continuu turnichetul. În modul memorie, dacă intervalul de trecere a cardului depășește durata de trecere a unei singure persoane, funcția de memorie nu va fi declanșată. Intervalul dintre două verificări de identitate trebuie să fie mai mare decât durata de deblocare a controlerului de acces sau controlerului de acces pentru recunoașterea feței; în caz contrar, va fi luată în considerare o singură verificare de identitate. Intervalul recomandat de verificare a identității este de 2 s până la 5 s. În modul de memorie, cel mult 255 de persoane pot trece continuu de turnichet.
A doua deblocare	După ce oamenii au intrat în turnichet și au declanșat alarmele, nu trebuie să facă un pas înapoi și pot obține identitățile verificate. Numai turnichetele acceptă modul de memorie și funcțiile de deblocare secunde.

Step 4 Clic**Salvați**.

3.6.3 Vizualizarea evenimentului istoric

Evenimentele istorice ale ușii includ evenimente atât pe SmartPSS-AC, cât și pe dispozitive. Extrageți istoricul evenimentelor de pe dispozitive pentru a vă asigura că toate jurnalele de evenimente sunt disponibile pentru a fi căutate.

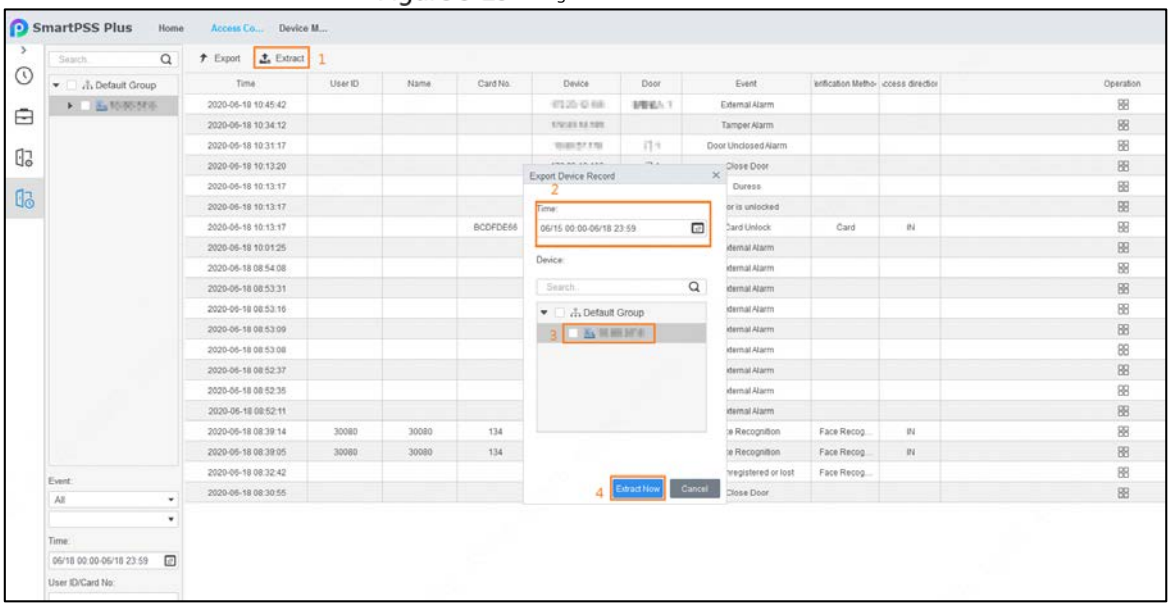
Step 1 Clic**Configurare acces**>**Eveniment istoric**pe pagina de start. Clic

Step 2 **Manager de acces**.

Step 3 Extrageți evenimentele de la dispozitivul de ușă în local. Clic**Extrage**, setați ora, selectați dispozitivul, apoi faceți clic**Extrage acum**.

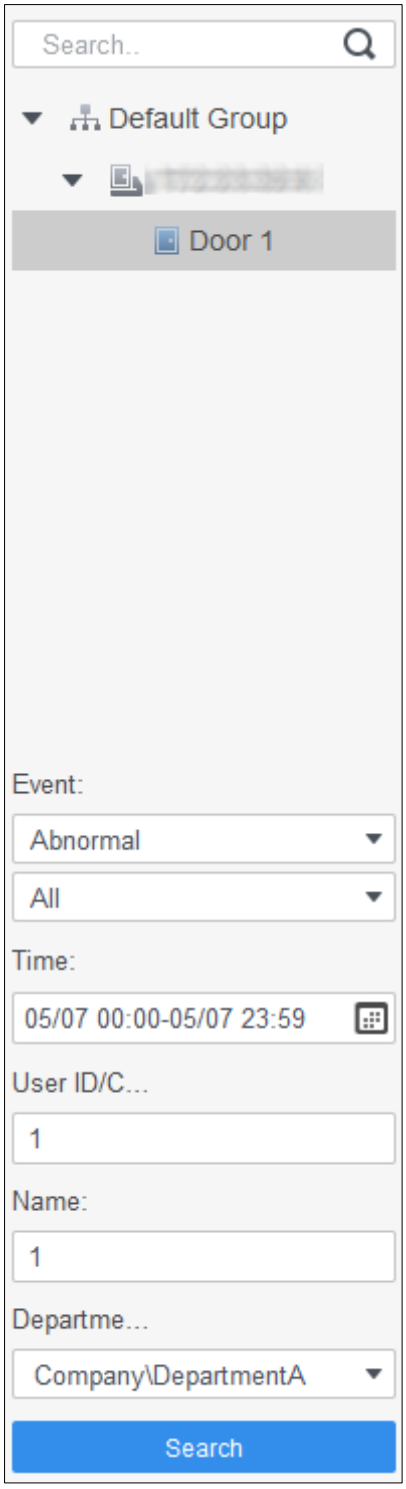
Puteți selecta mai multe dispozitive în același timp.

Figure 3-25 Extrage evenimente



Step 4 Setați condițiile de filtrare, apoi faceți clic**Căutare**.

Figure 3-26 Căutați evenimente prin filtrarea condițiilor



3.7 Managementul accesului

3.7.1 Accesul la ușă controlat de la distanță

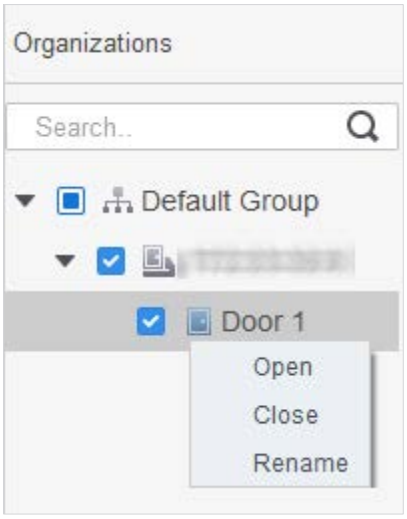
Puteți controla ușa de la distanță prin SmartPSS AC.

Step 1 Clic**Manager de acces**pe pagina de pornire sau faceți clic**Ghid de acces >** .

Step 2 Controlați de la distanță accesul ușii. Există două metode.

- Metoda 1: Selectați ușa, faceți clic dreapta și selectați**Deschis**.

Figure 3-27 Control de la distanță (metoda 1)



- Metoda 2: Faceți clic sau pentru a deschide sau a închide ușa. Control de la distanță (metoda 2)

Figure 3-28

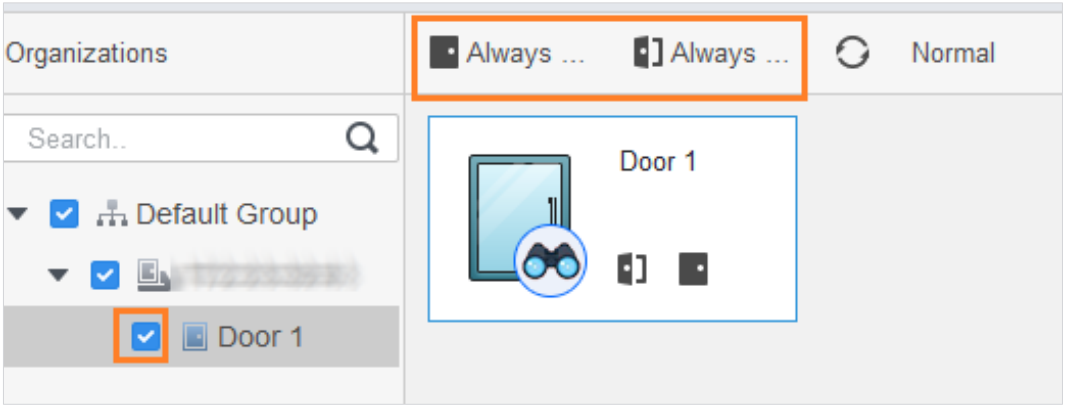
3.7.2 Setarea stării ușii

După setarea stării mereu deschis sau întotdeauna închis, ușa rămâne deschisă sau închisă tot timpul. Puteți da clic**Normal**pentru a restabili starea ușii la normal, astfel încât utilizatorii să poată debloca ușa după verificarea identității.

Step 1 Clic**Manager de acces**pe pagina de start. (Sau faceți clic**Ghid de acces >**).

Step 2 Selectați ușa, apoi faceți clic**Mereu deschis**sau**Întotdeauna aproape**.

Figure 3-29 Setați întotdeauna deschis sau întotdeauna închis



3.8 Configurarea legăturii alarmei

După ce configurați conectarea alarmelor, alarmele vor fi declanșate. Pentru detalii, consultați manualul de utilizare al SmartPss AC. Această secțiune folosește alarma de intruziune ca exemplu.

- Configurați conexiuni de alarmă externe conectate la controlerul de acces, cum ar fi alarma de fum. Configurați
- legături ale evenimentelor controlerului de acces.
  - ◇ Eveniment de alarmă
  - ◇ Eveniment anormal
  - ◇ Eveniment normal

Step 1 Clic**Configurare eveniment**pe pagina de start.

Step 2 Selectați ușa și selectați**Eveniment de alarmă > Eveniment de intruziune**. Porniți

Step 3 **Eveniment de intruziune**. Configurați conexiunea alarmei de intruziune.

Step 4

- Activați alarma sonoră.

  Apasă pe**Notifică**fila și porniți**Sunet de alarmă**. Când apar evenimente de intruziune, sunt declanșate alarme sonore.

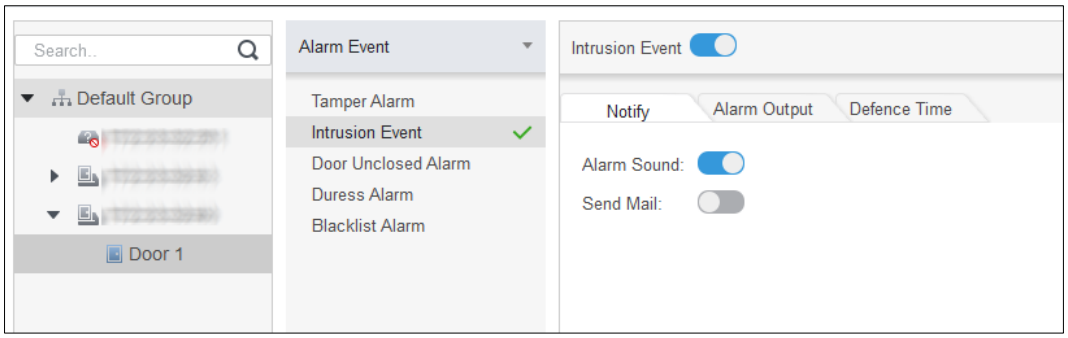
- Trimite e-mail.

1) Porniți**Trimite e-mail**și confirmați pentru a seta SMTP.

2) Configurați SMTP, cum ar fi adresa serverului, numărul portului și modul de criptare.

Când apar evenimente de intruziune, sistemul trimite notificări de alarmă prin e-mail la receptorul specificat.

Figure 3-30 Configurați alarma de intruziune



- Configurați ieșirea alarmei.

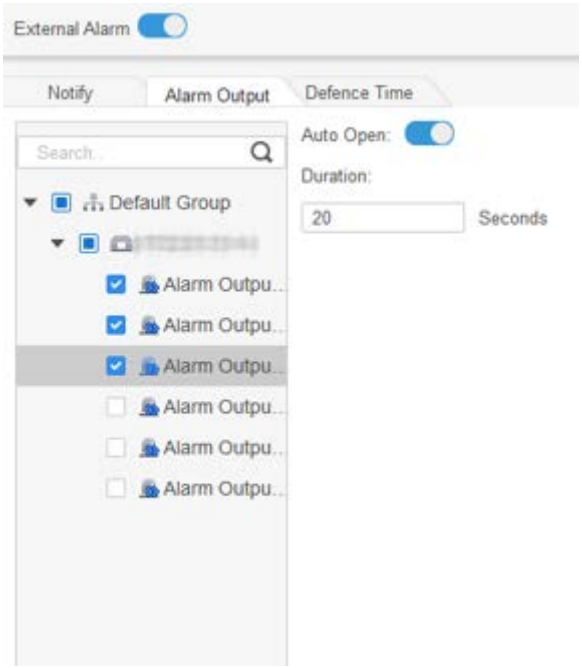
1) Faceți clic**Ieșire de alarmă**fila.

2) Selectați dispozitivul care acceptă ieșirea alarmei, apoi selectați portul de ieșire alarmă.

3) Porniți**Deschidere automată**pentru conectarea alarmei.

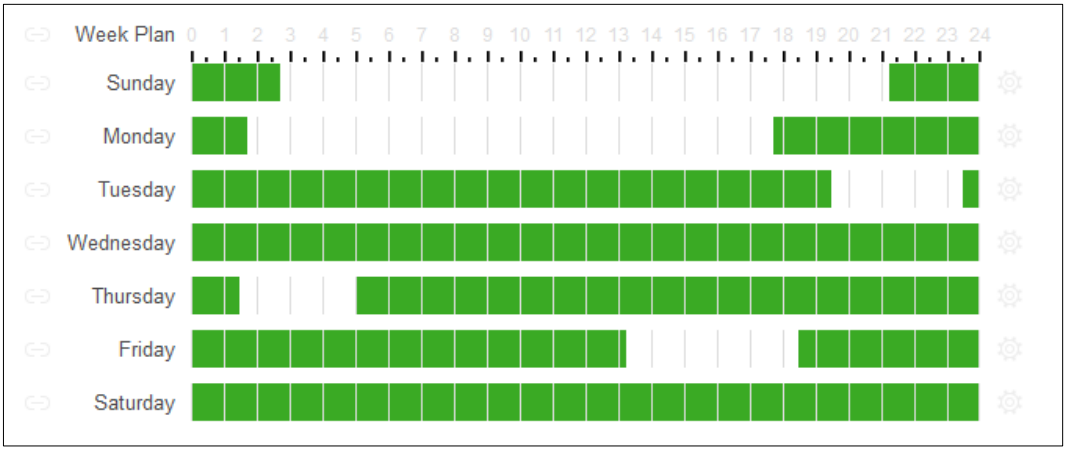
4) Setați durata alarmei.

Figure 3-31 Configurați conexiunea alarmei



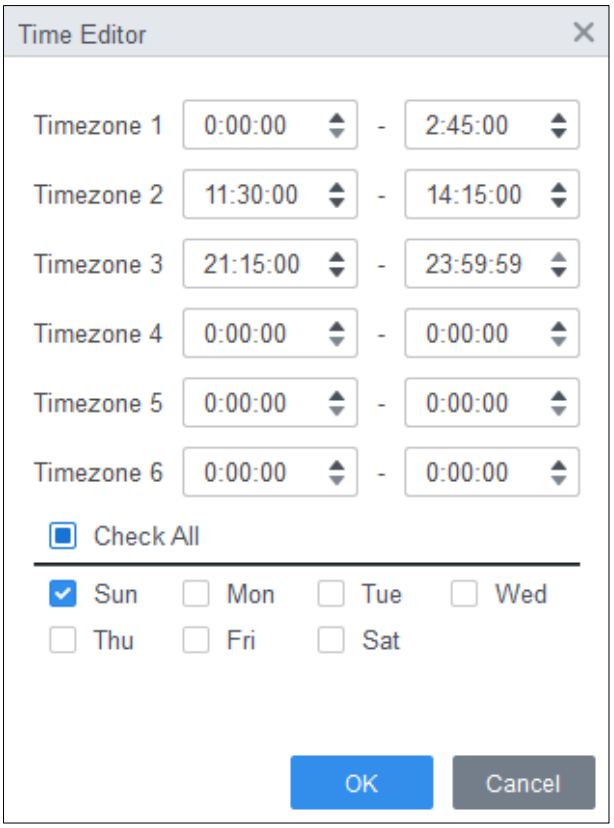
- Setați perioade de armare. Există două metode.
  - Metoda 1: Mutați cursorul pentru a seta perioade. Când cursorul este creion, faceți clic pentru a adăuga puncte; când cursorul este șters, faceți clic pentru a elimina punctele. Zona verde sunt perioadele de armare

Figure 3-32 Set defense timpul (metoda 1)



-Metoda 2: Faceți clic pentru a seta perioadele de armare, apoi faceți clic**Bine**.

Figure 3-33 Setați timpul de armare (metoda 2)



Step 5 (Opțional) Dacă doriți să setați aceleași perioade de armare pentru alt controler de acces, faceți clic**Copiaza in**, selectați controlerul de acces, apoi faceți clic**Bine**. Clic**Salvați**.

Step 6

4 Configurare ConfigTool

ConfigTool este folosit în principal pentru a configura și întreține dispozitivul.

Nu utilizați ConfigTool și SmartPSS AC în același timp, altfel poate provoca rezultate anormale când cauți dispozitive.

4.1 Inițializare

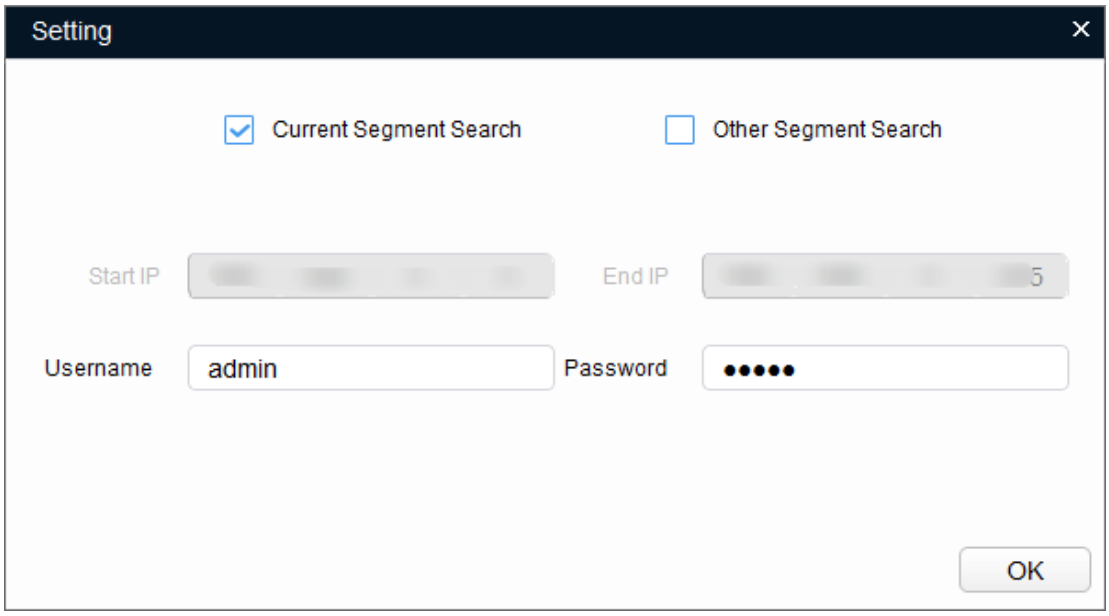
Înainte de inițializare, asigurați-vă că Dispozitivul și computerul sunt în aceeași rețea.

Step 1 Căutați dispozitivul prin ConfigTool. 1) Faceți dublu clic pe ConfigTool pentru a-l deschide.

2) Faceți clic**Setare de căutare**, introduceți intervalul de segmente de rețea, apoi faceți clic**Bine**.

3) Selectați dispozitivul neinițializat, apoi faceți clic**Inițializați**.

Figure 4-1 Căutați dispozitivul



Step 2 Selectați dispozitivele neinițializate, apoi faceți clic**Inițializați.**

Step 3 Clic**Bine**.

Sistemul începe inițializarea. indică succesul inițializării, indica inițializare eșuată.

Step 4 Clic**finalizarea**.

4.2 Adăugarea de dispozitive

Puteți adăuga unul sau mai multe dispozitive.

Asigurați-vă că Dispozitivul și computerul pe care este instalat ConfigTool sunt conectate; în caz contrar, ConfigTool nu poate găsi dispozitivul.

4.2.1 Adăugarea dispozitivului individual

Step 1 Clic .

Step 2 Clic**Adăugare manuală**.

Step 3 Select**t Adresa IP**sau**SN dispozitiv**din**Adăugați tip**listă.

Figure 4-2 Adăugați manual (adresă IP)

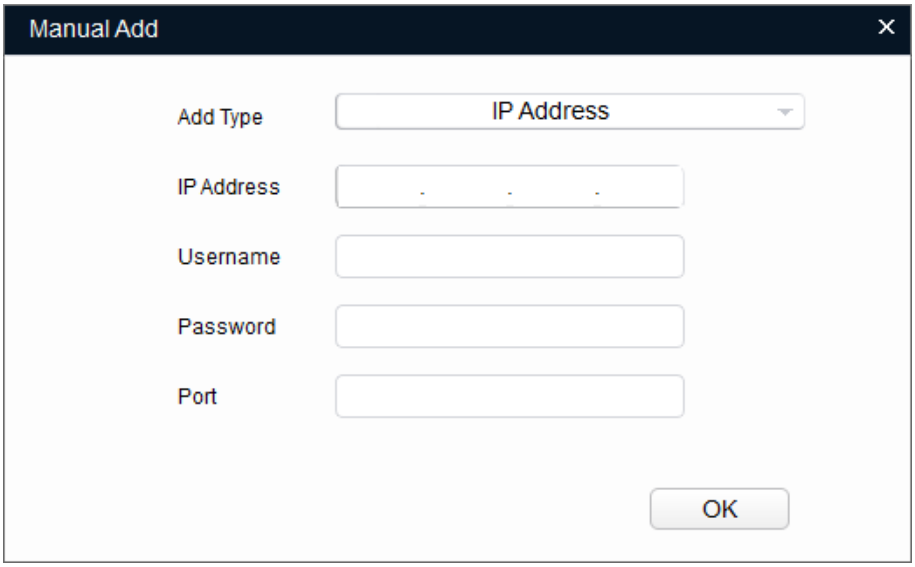


Figure 4-3 Adăugați manual (numărul dispozitivului)

Step 4 Setați parametrii dispozitivului.

Tabelul 4-1 Parametri de adăugare manuală

Adăugați metoda	Parametru	Descriere
Adresa IP	Adresa IP	Adresa IP a dispozitivului. Este implicit 192.168.1.108.

Adăugați metoda	Parametru	Descriere
	Nume de utilizator	Numele de utilizator și parola pentru autentificarea dispozitivului.
	Parola	
	Port	Numărul portului dispozitivului.
Device SN (Dispozitiv acceptă numai P2P)	SN	Numărul de serie al dispozitivului.
	Nume de utilizator	Numele de utilizator și parola pentru autentificarea dispozitivului.
	Parola	

Step 5 Clic**Bine**.

Dispozitivul adăugat se afișează în lista de dispozitive.

4.2.2 Adăugarea dispozitivului în loturi

Puteți adăuga mai multe dispozitive prin căutarea dispozitivelor sau importând șablonul.

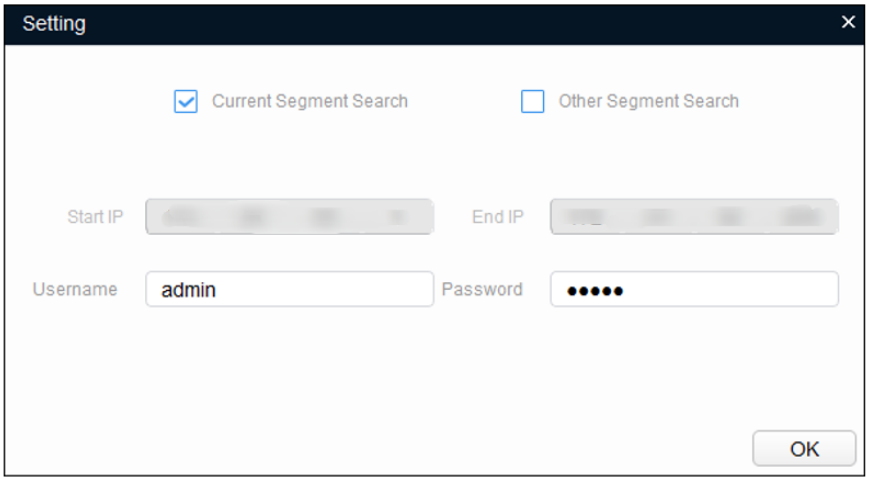
4.2.2.1 Adăugarea prin căutare

Puteți adăuga mai multe dispozitive căutând segmentul de rețea curent sau alt segment de rețea.

Puteți seta condițiile de filtrare pentru a căuta dispozitive.

Step 1 Clic Search setting .

Figure 4-4 Setare



Step 2 Selectați metodele de căutare.

- Căutarea segmentului curent

Selectați**Căutarea segmentului curent**. Introduceți numele de utilizator și parola. Sistemul va căuta dispozitive în consecință.

- Căutare alt segment

Selectați**Căutare alt segment**. Introduceți adresa IP de început și adresa IP de final. Introduceți numele de utilizator și parola. Sistemul va căuta dispozitive în consecință.

- Dacă le selectați pe ambele**Căutarea segmentului curent**și**Căutare alt segment**, sistemul caută dispozitive pe ambele segmente.
- Numele de utilizator și parola sunt cele folosite pentru a vă autentifica atunci când doriți să modificați IP, configurați sistemul, actualizați dispozitivul, reporniți dispozitivul și multe altele.

Step 3 Clic**Bine**pentru a căuta dispozitive.

Dispozitivele căutate se vor afișa în lista de dispozitive.

- Clic  pentru a reîmprospăta lista de dispozitive.
- Sistemul salvează condițiile de căutare atunci când părăsiți software-ul și reutilizați aceleași condiții atunci când software-ul este lansat data viitoare.

4.2.2.2 Adăugarea prin importul șablonului dispozitivului

Puteți adăuga dispozitivele importând un șablon Excel. Puteți importa până la 1000 de dispozitive.

Închideți fișierul șablon înainte de a importa dispozitivele; în caz contrar, importul va eșua.

Step 1 Clic  , selectați un dispozitiv, apoi faceți clic**Export**pentru a exporta un șablon de dispozitiv.

Step 2 Urmați instrucțiunile de pe ecran pentru a salva fișierul șablon local.

Step 3 Deschideți fișierul șablon, modificați informațiile existente despre dispozitiv în informațiile dispozitivelor pe care doriți să le adăugați.

Step 4 Importați șablonul. Clic**Import**, selectați șablonul și faceți clic**Deschis**.

Sistemul începe să importe dispozitivele.

Step 5 Clic**Bine**.

Dispozitivele nou importate se afișează în lista de dispozitive.

4.3 Configurarea controlerului de acces

Capturile de ecran și parametrii pot fi diferiți în funcție de tipurile și modelele de dispozitive.

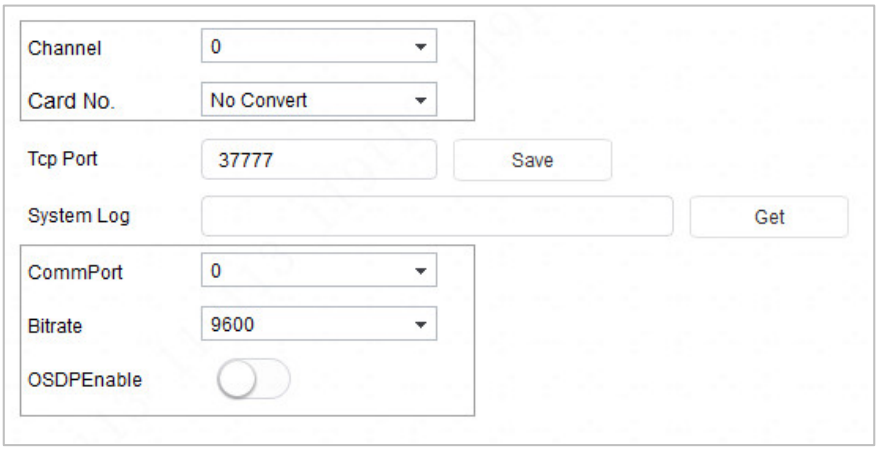
Step 1 Clic  pe meniul principal.

Step 2 Faceți clic pe controlerul de acces pe care doriți să-l configurați în lista de dispozitive, apoi faceți clic**Obțineți informații despre dispozitiv**.

Step 3 (Opțional) Dacă se afișează pagina de conectare, introduceți numele de utilizator și parola, apoi faceți clic**Bine**. Setați

Step 4 parametrii controlerului de acces.

Figure 4-5 Configurați controlerul de acces



Tabelul 4-2 Parametrii controlerului de acces

Parametru	Descriere
Canal	Selectați canalul pentru a seta parametrii.
Card Nr.	Setați regula de procesare a numărului de card pentru controlerul de acces. Este**Fără conversie**în mod implicit. Când rezultatul citirii cardului nu se potrivește cu numărul real al cardului, selectați**Byte invers**sau**HIDpro Convert**. **Byte invers**: Când controlerul de acces funcționează cu cititoare terțe, iar numărul cardului citit de cititorul de carduri este în ordine inversă față de numărul real al cardului. De exemplu, numărul cardului citit de cititorul de carduri este hexazecimal 12345678, în timp ce numărul real al cardului este hexazecimal 78563412 și puteți selecta**Byte invers**. **HIDpro Convert**: Când controlerul de acces funcționează cu cititoare HID Wiegand, iar numărul cardului citit de cititorul de carduri se potrivește cu numărul real al cardului, puteți selecta HIDpro Revert pentru a le potrivi. De exemplu, numărul cardului citit de cititorul de carduri este hexazecimal 1BAB96, în timp ce numărul real al cardului este hexazecimal 78123456,
Port TCP	Modificați numărul portului TCP al dispozitivului.
SysLog	Clic**obține**pentru a selecta o cale de stocare pentru jurnalele de sistem.
CommPort	Selectați cititorul pentru a seta rata de biți și pentru a activa OSDP.
Rata de biți	Dacă citirea cardului este lentă, puteți crește rata de biți. Este 9600 implicit.
Activare OSDP	Când controlerul de acces lucrează cu cititoare terțe prin protocolul ODSP, activați ODSP.

Step 5 (Opțional) Faceți clic**Aplica pentru**, selectați dispozitivele cărora trebuie să aplicați parametrii configurați, apoi faceți clic**Config**.

✓ indică succesul aplicației; ⚠ indică faptul că aplicația a eșuat. Puteți da clic pe ele pentru a le vizualiza Detalii.

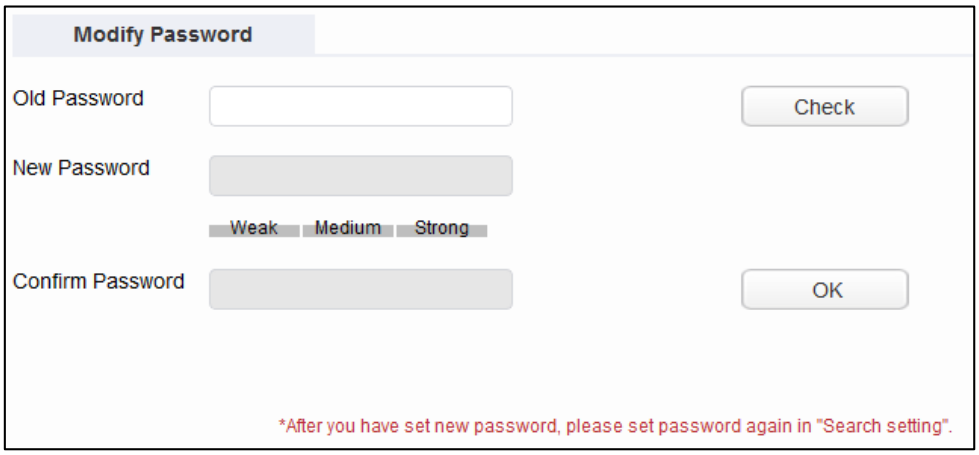
4.4 Modificarea parolei dispozitivului

Puteți modifica parola de conectare a dispozitivului.

Step 1 Clic .

Step 2 Apasă pe**Parola dispozitivului**fila.

Figure 4-6 Parola dispozitivului



Step 3 Clic lângă tipul de dispozitiv, apoi selectați unul sau mai multe dispozitive.

Dacă selectați mai multe dispozitive, parolele de conectare trebuie să fie aceleași.

Step 4 Setați parola.

Urmați indicația privind nivelul de securitate al parolei pentru a seta o nouă parolă.

Tabelul 4-3 Parametrii parolei

Parametru	Descriere
Parola veche	Introduceți parola veche a dispozitivului. Pentru a vă asigura că vechea parolă este introdusă corect, puteți face clic**Verifica**a verifica.
Parolă Nouă	Introduceți noua parolă pentru dispozitiv. Există o indicație pentru puterea parolei. Parola trebuie să fie formată din 8 până la 32 de caractere care nu sunt goale și să conțină cel puțin două tipuri de caractere dintre majuscule, minuscule, număr și caractere speciale (excluzând „ ” ; : &).
Confirmă parola	Confirmați noua parolă.

Step 5 Clic**Bine**pentru a finaliza modificarea.

Appendix 1 Recomandări de securitate cibernetică

Acțiuni obligatorii care trebuie întreprinse pentru securitatea de bază a rețelei dispozitivului: 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 păstrați firmware-ul dispozitivului (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 dispozitivul este conectat la rețeaua publică, se recomandă activarea funcției de „verificare automată a actualizărilor” 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 dispozitivului dvs.: 1. Protecție fizică

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

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 cu 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 de dispozitiv, reducând astfel

riscul de falsificare ARP.

8. Alocați conturi și privilegii în mod rezonabil

În conformitate cu cerințele de afaceri și de management, adăugați în mod rezonabil utilizatori și atribuiți-le un set minim de permisiuni.

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 dispozitivului: 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 dispozitivului, 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 dispozitivului 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.