Controller de acces (C)

Manualul utilizatorului

V1.0.2

cuvânt înainte

General

Acest manual prezintă structura, funcțiile și operațiunile controlorului de acces (denumit în continuare „controlerul”).

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 daune materiale, pierderi de date, reduceri de performanță sau rezultate imprevizibile.
SFATURI	Oferă metode care vă ajută să rezolvați o problemă sau să economisiți timp.
NOTĂ	Oferă informații suplimentare ca supliment la text.

Istoricul revizuirilor

Versiune	Conținutul revizuirii	Timpul de eliberare
V1.0.2	Imaginea cablajului actualizată.	iunie 2022
V1.0.1	S-a adăugat un proces de inițializare.	decembrie 2021
V1.0.0	Prima aparitie.	martie 2021

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 Controllerului.
- 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 Controlorului, prevenirea pericolelor, și prevenirea daunelor materiale. Citiți cu atenție înainte de a utiliza controlerul, respectați prevederile ghiduri atunci când îl utilizați și păstrați manualul în siguranță pentru referințe ulterioare.

Cerința de transport

Transportați controlerul în condiții de umiditate și temperatură permise.

Cerință de stocare

Păstrați controlerul în condiții de umiditate și temperatură permise.

Cerințe de instalare

- Nu conectați adaptorul de alimentare la controler 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 Controlerului.
- Nu conectați controlerul la două sau mai multe tipuri de surse de alimentare, pentru a evita deteriorarea Controlor.
- 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 controlerul într-un loc expus la lumina soarelui sau în apropierea surselor de căldură.
- Țineți controlerul departe de umiditate, praf și funingine.
- Instalați controlerul pe o suprafață stabilă pentru a preveni căderea acestuia.
- Instalați controlerul 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 Controlerului.
- Controlerul este un aparat electric de clasa I. Asigurați-vă că sursa de alimentare a controlerului este conectat la o priză cu împământare de protecție.

- Controlerul trebuie să fie împământat atunci când este conectat la rețeaua electrică de 220 V.

Cuprins

Cuvânt înainte..... I Măsuri de protecție și avertismente importante..... III 1 Prezentare de ansamblu..... 1

1.1 Introducere 1

1.1 Caracteristici 1

1.2 Dimensiuni..... 1

1.3 Aplicație 2

1.3.1 Cu două uși, un singur sens..... 2

1.3.2 Două uși În două sensuri..... 3

1.3.3 Un singur sens cu patru uși..... 3

1.3.4 Cu patru uși, cu două sensuri 4

1.3.5 Un singur sens cu opt uși 4

2 Structura 5

2.1 Cablaje 5

2.1.1 Cu două uși, un singur sens..... 5

2.1.2 Cu două uși, cu două sensuri..... 6

2.1.3 Un singur sens cu patru uși..... 7

2.1.4 În două sensuri cu patru uși 8

2.1.5 Unic cu opt uși 9

2.1.6 Blocare..... 9

2.1.7 Intrare alarmă 10

2.1.8 Ieșire alarmă 10

2.1.9 Cititor de carduri..... 12

2.2 Indicator de putere..... 12

2.3 Comutator DIP 12

2.4 Alimentare electrică..... 13

2.4.1 Portul de alimentare pentru blocarea ușii..... .13

2.4.2 Portul de alimentare al cititorului de carduri..... 13

3 Configurare SmartPSS AC..... 14

3.1 Log in 14

3.2 Inițializare..... 14

3.3 Adăugarea de dispozitive..... 15

3.3.1 Căutare automată..... 15

3.3.2 Adăugarea manuală..... 16

3.4 Managementul utilizatorilor 18

3.4.1 Setarea tipului cardului..... 18

3.4.2 Adăugarea unui utilizator 19

3.5 Configurarea permisiunii 22

3.5.1 Adăugarea unui grup de permisiuni 22

3.5.2 Atribuirea permisiunii de acces..... 23

3.6 Configurația controlerului de acces..... 24

3.6.1 Configurarea funcțiilor avansate 24

3.6.2 Configurarea controlerului de acces 30

3.6.3 Vizualizarea evenimentului istoric..... 33

3.7 Gestionarea accesului 34
3.7.1 Deschiderea și închiderea de la distanță a ușii 34
3.7.2 Setarea stării ușii 35
3.7.3 Configurarea legăturii alarmei 36
4 Configurare ConfigTool 39
4.1 Inițializare 39
4.2 Adăugarea de dispozitive 39
4.2.1 Adăugarea individuală a dispozitivului 40
4.2.2 Adăugarea de dispozitive în loturi 40
4.3 Configurarea controlerului de acces 42
4.4 Schimbarea parolei dispozitivului 43
Appendix 1 Recomandări de securitate cibernetică 45

1.1 Introducere

Controlerul 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.

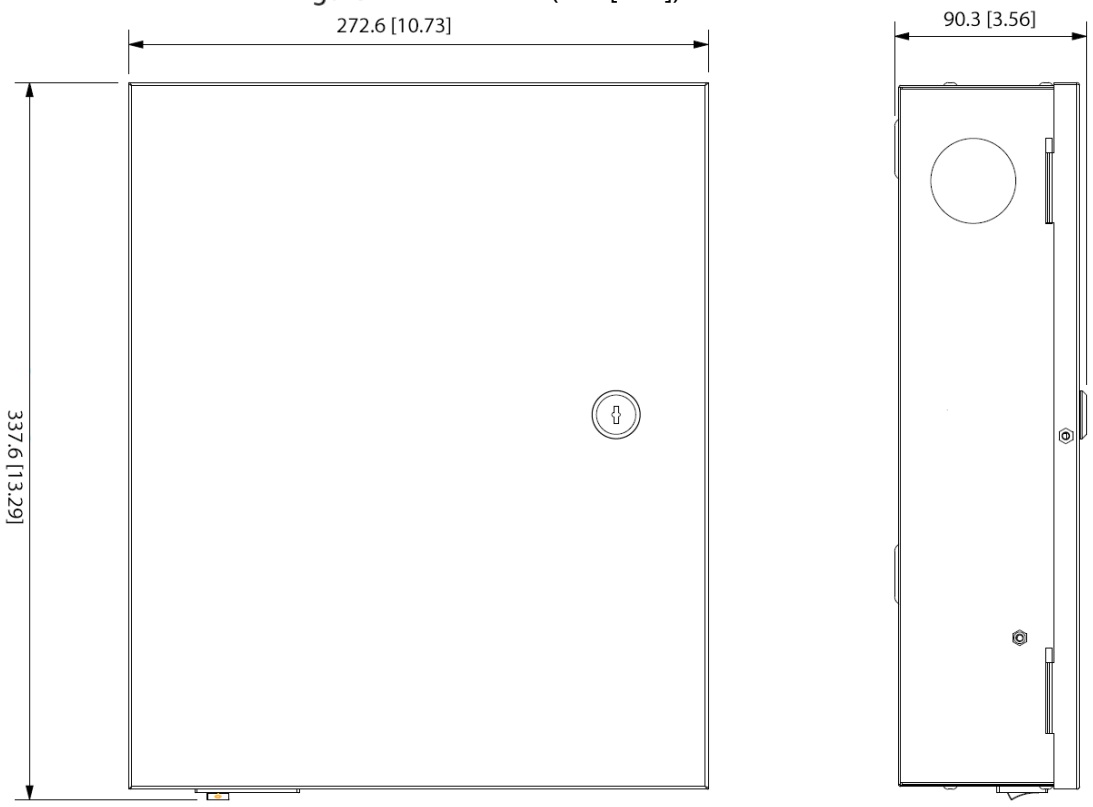
1.1 Caracteristici

- Adoptă placa de oțel SEEC pentru a oferi un aspect high-end.
- Suportă comunicații de rețea TCP/IP. Datele de comunicare sunt criptate pentru securitate. Înregistrare
- automată.
- Suporta protocolul OSDP.
- 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 invalid, 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, funcțiile de stocare și încărcare a înregistrărilor evenimentelor și completarea automată a rețelei (ANR).
- Suportă 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 cărți și perioade de deblocare.
- Sprijină mecanismul de protecție pentru câine de pază pentru a asigura stabilitatea funcționării.

1.2 Dimensiuni

Există cinci tipuri de controlere de acces, inclusiv cu două uși unidirecționale, cu două uși cu două sensuri, cu patru uși unidirecționale, cu patru uși cu două sensuri și cu opt uși unidirecționale. Dimensiunile lor sunt aceleași.

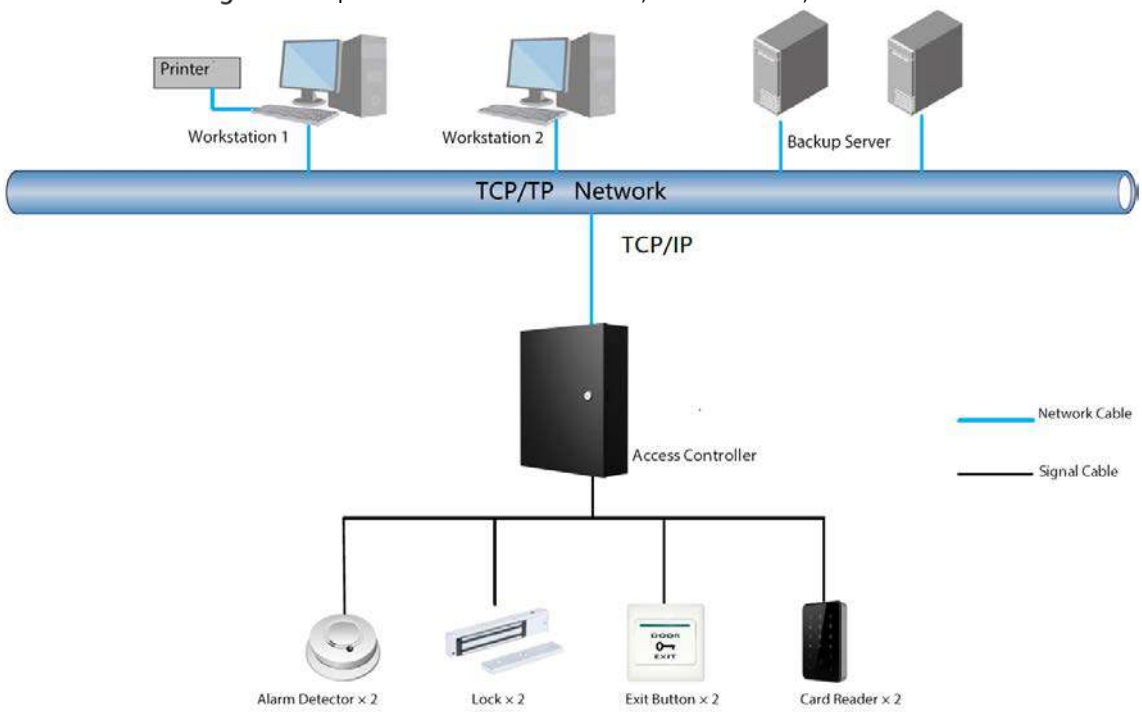
Figure 1-1 Dimensiuni (mm [inch])



1.3 Aplicație

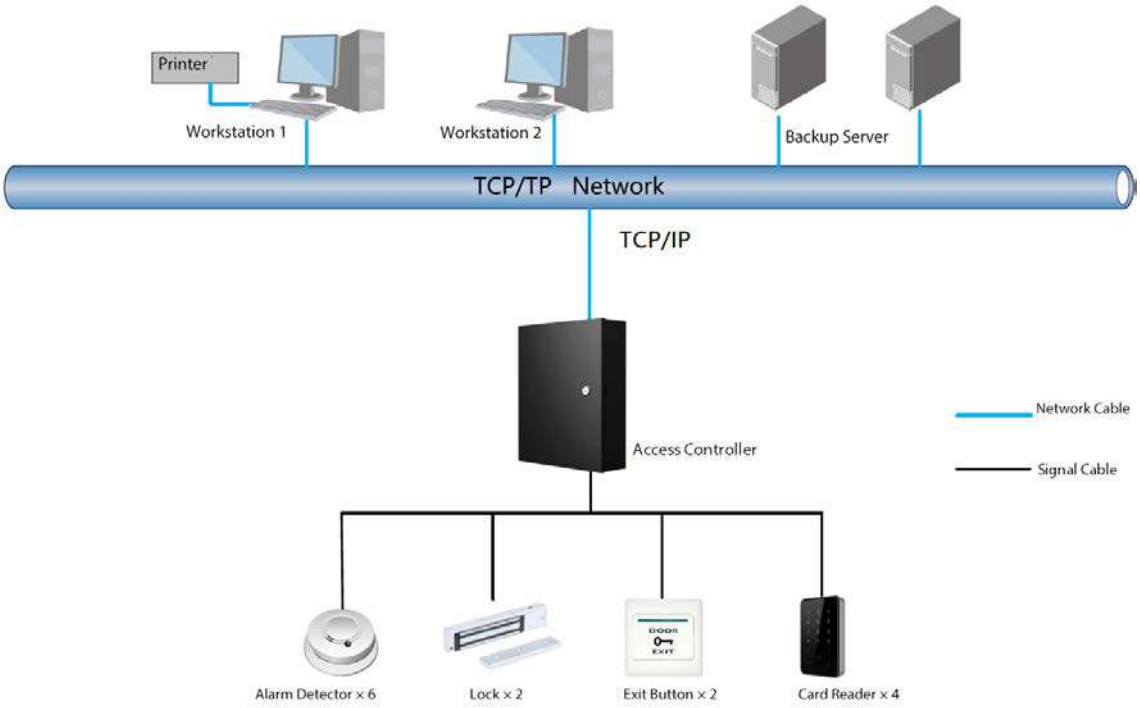
1.3.1 Două uși Unic

Figure 1-2 Aplicarea controlerului unidirecțional cu două uși



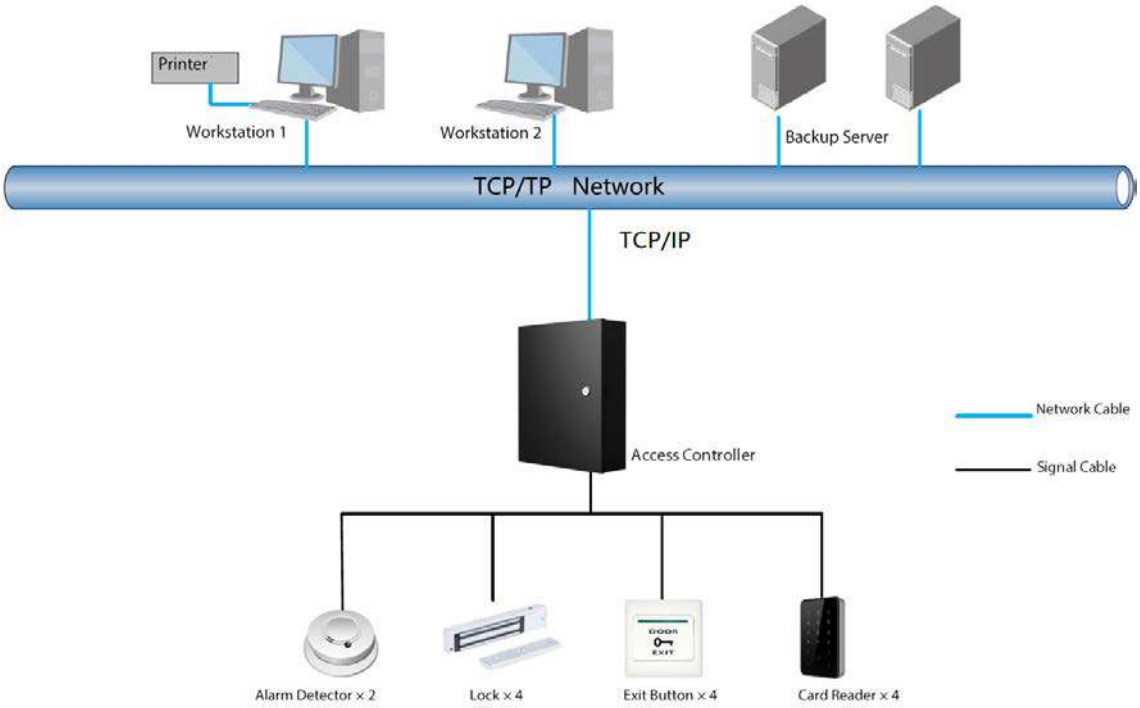
1.3.2 Două uși În două sensuri

Figure 1-3 Aplicarea controlerului bidirecțional cu două uși



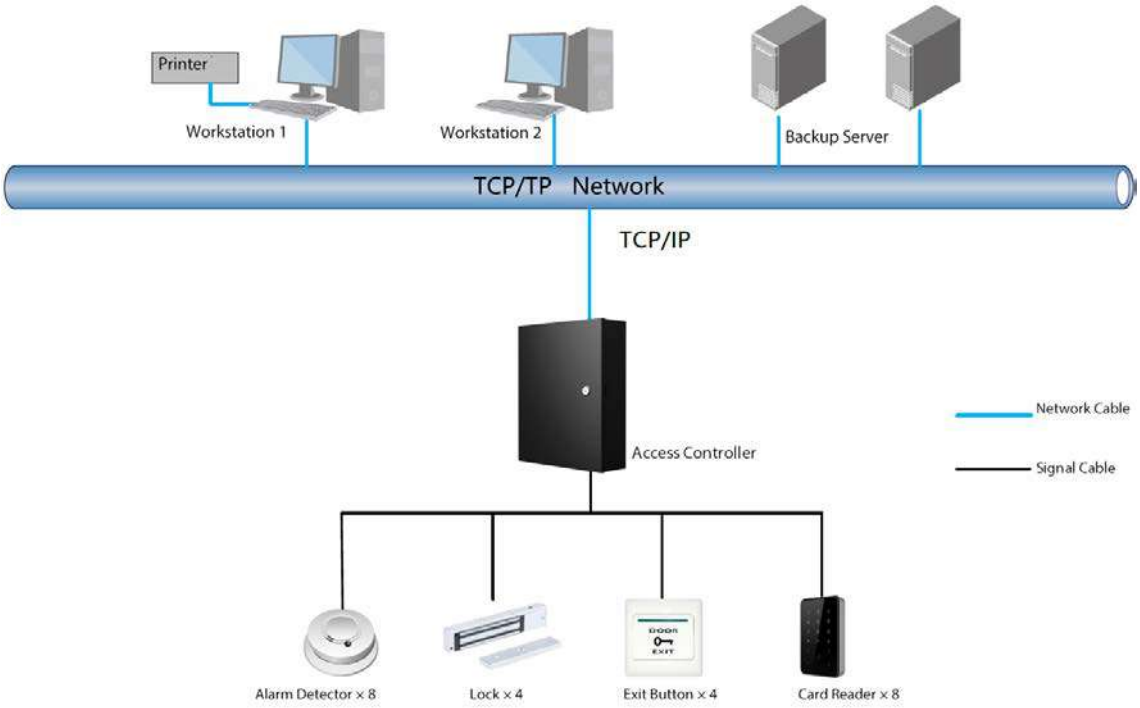
1.3.3 Un singur sens cu patru uși

Figure 1-4 Aplicarea controlerului unidirecțional cu patru uși



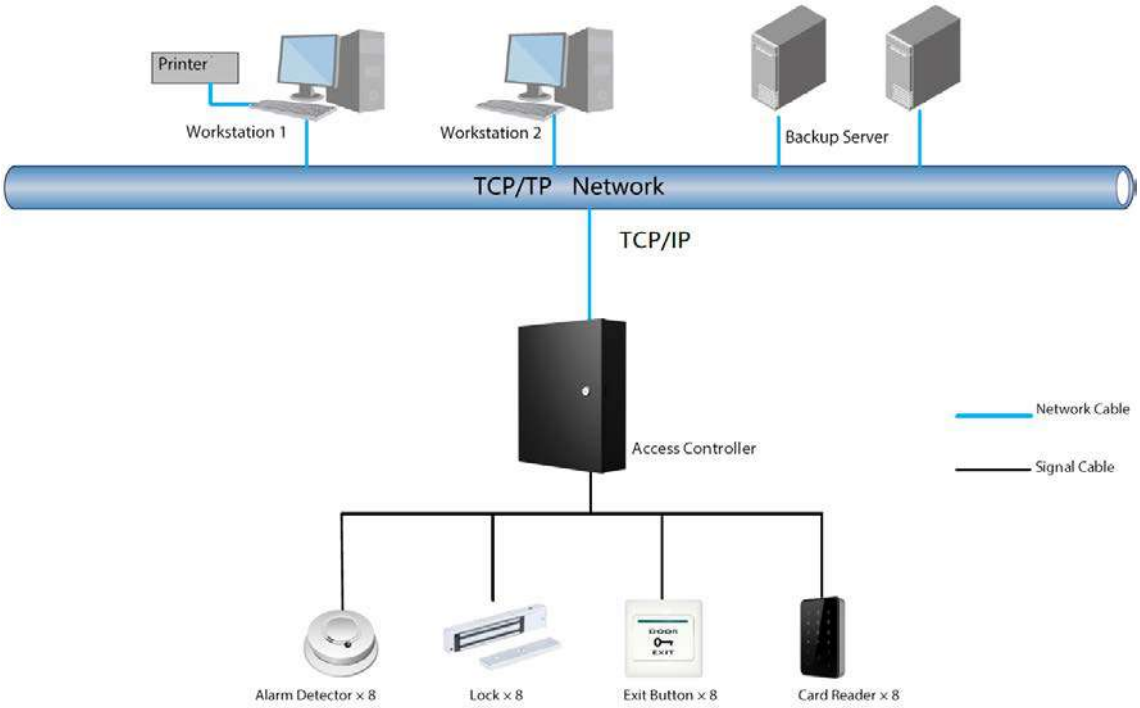
1.3.4 În două sensuri cu patru uși

Figure 1-5 Aplicarea controlerului bidirecțional cu patru uși



1.3.5 Un singur sens cu opt uși

Figure 1-6 Aplicarea controlerului unidirecțional cu opt uși



2 Structura

2.1 Cablaj

⚠

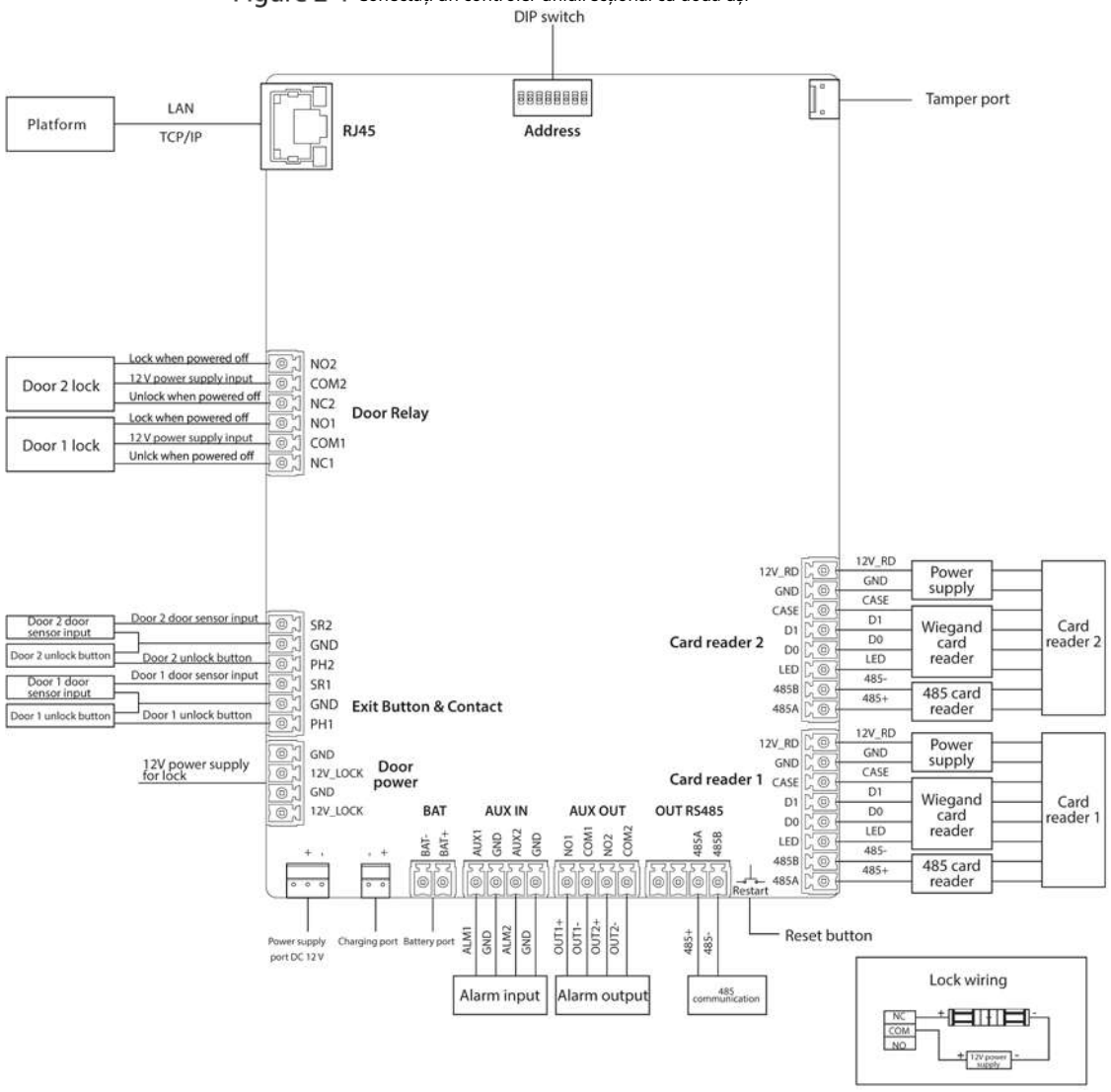
- Conectați firele numai când sunt oprite.
- Asigurați-vă că ștecherul sursei de alimentare este împământat. 12 V:
- curentul maxim pentru un modul de extensie este de 100 mA. 12 V_RD:
- curentul maxim pentru un cititor de carduri este de 2,5 A.
- 12 V_LOCK: curentul maxim pentru o lacăt este de 2 A.

Tabelul 2-1 Specificațiile cablurilor

Dispozitiv	Cablu
Cititor de carduri	Cat5 8-core ecranat tw
cablu Ethernet	Cat5 8-core ecranat tw
Buton	2-nuclee
Contact la ușă	2-nuclee

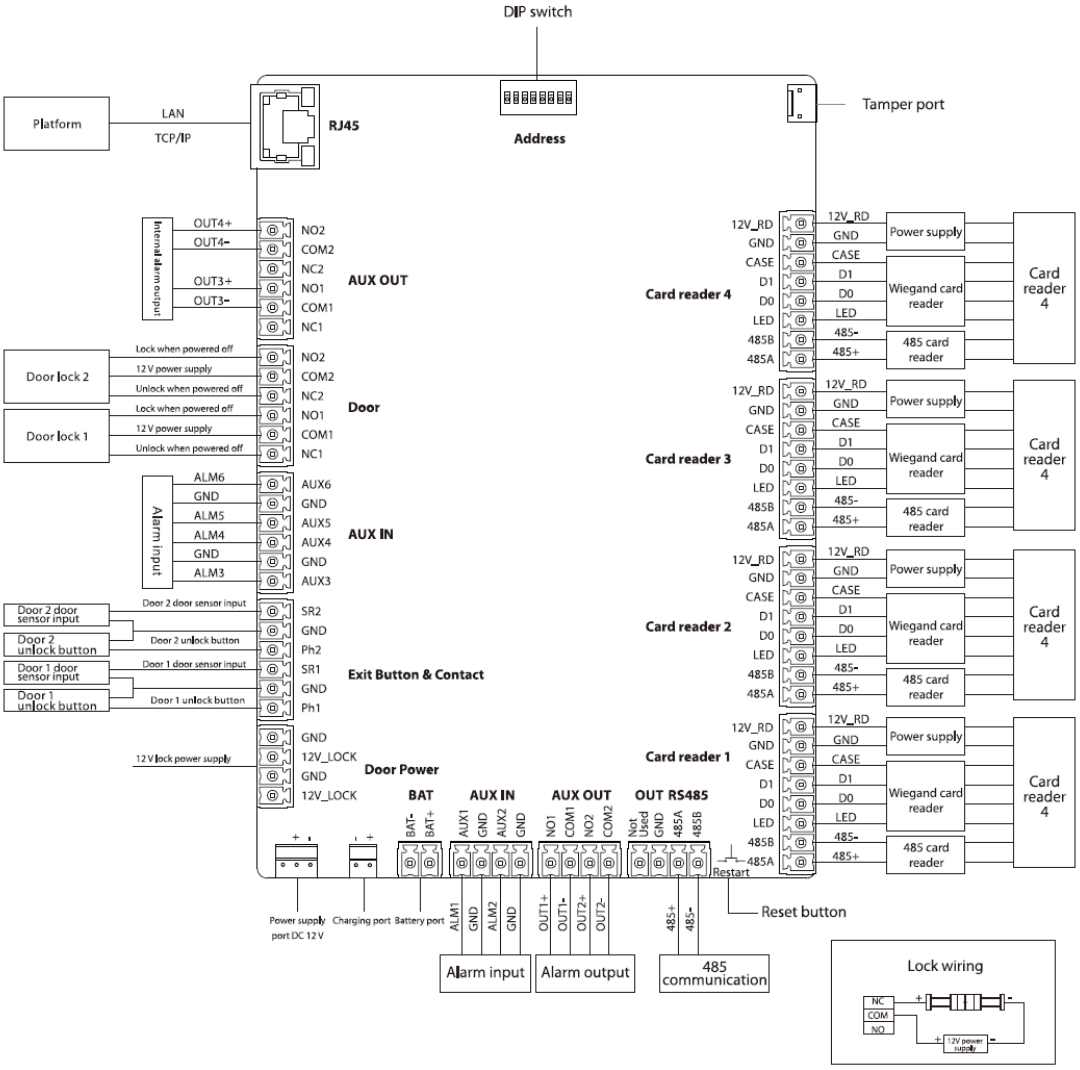
2.1.1 Două uși Unic

Figure 2-1 Conectați un controler unidirecțional cu două uși



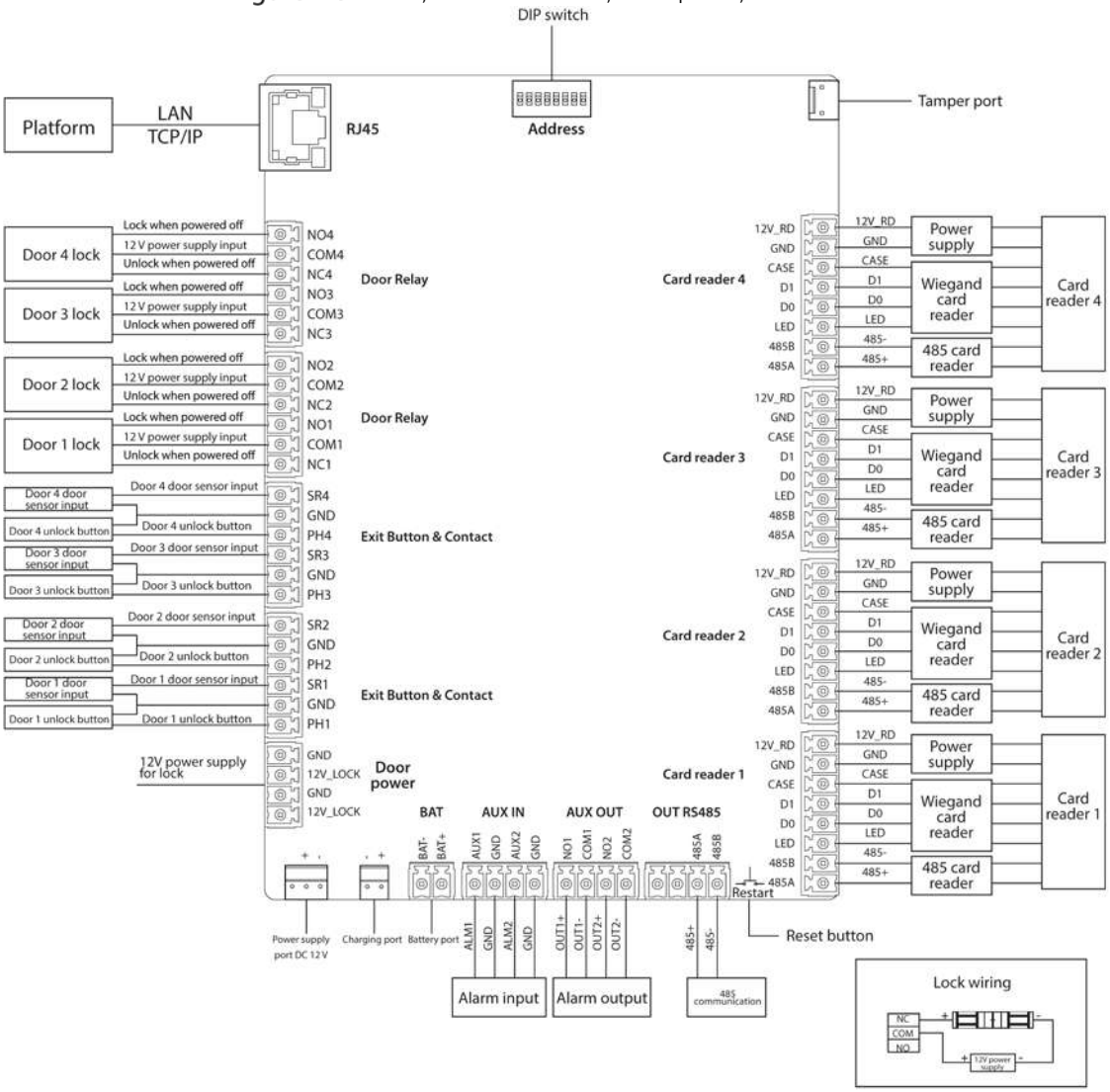
2.1.2 Două uși În două sensuri

Figure 2-2 Conectați un controler bidirecțional cu două uși



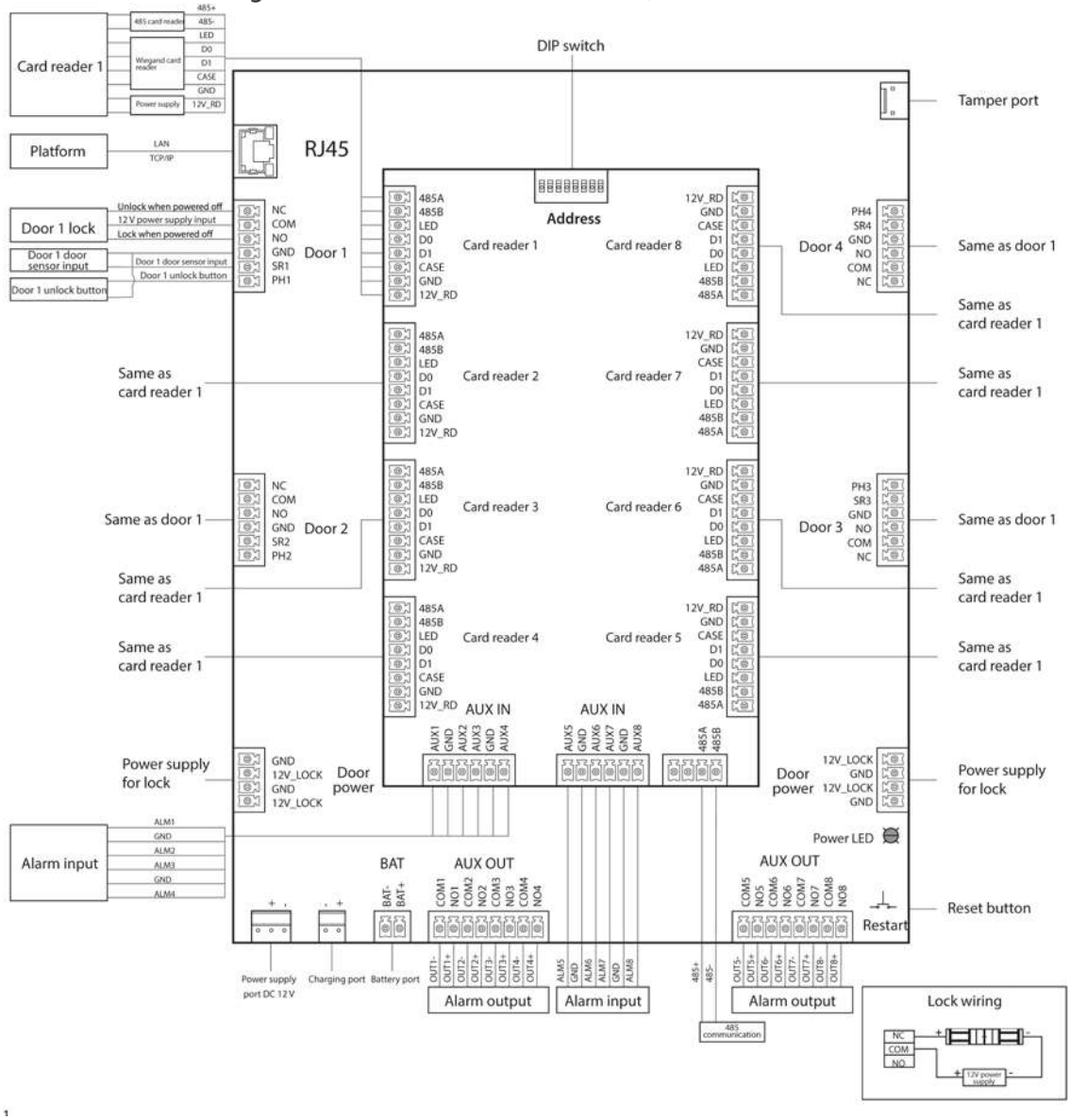
2.1.3 Un singur sens cu patru uși

Figure 2-3 Conectați un controler unidirecțional cu patru uși



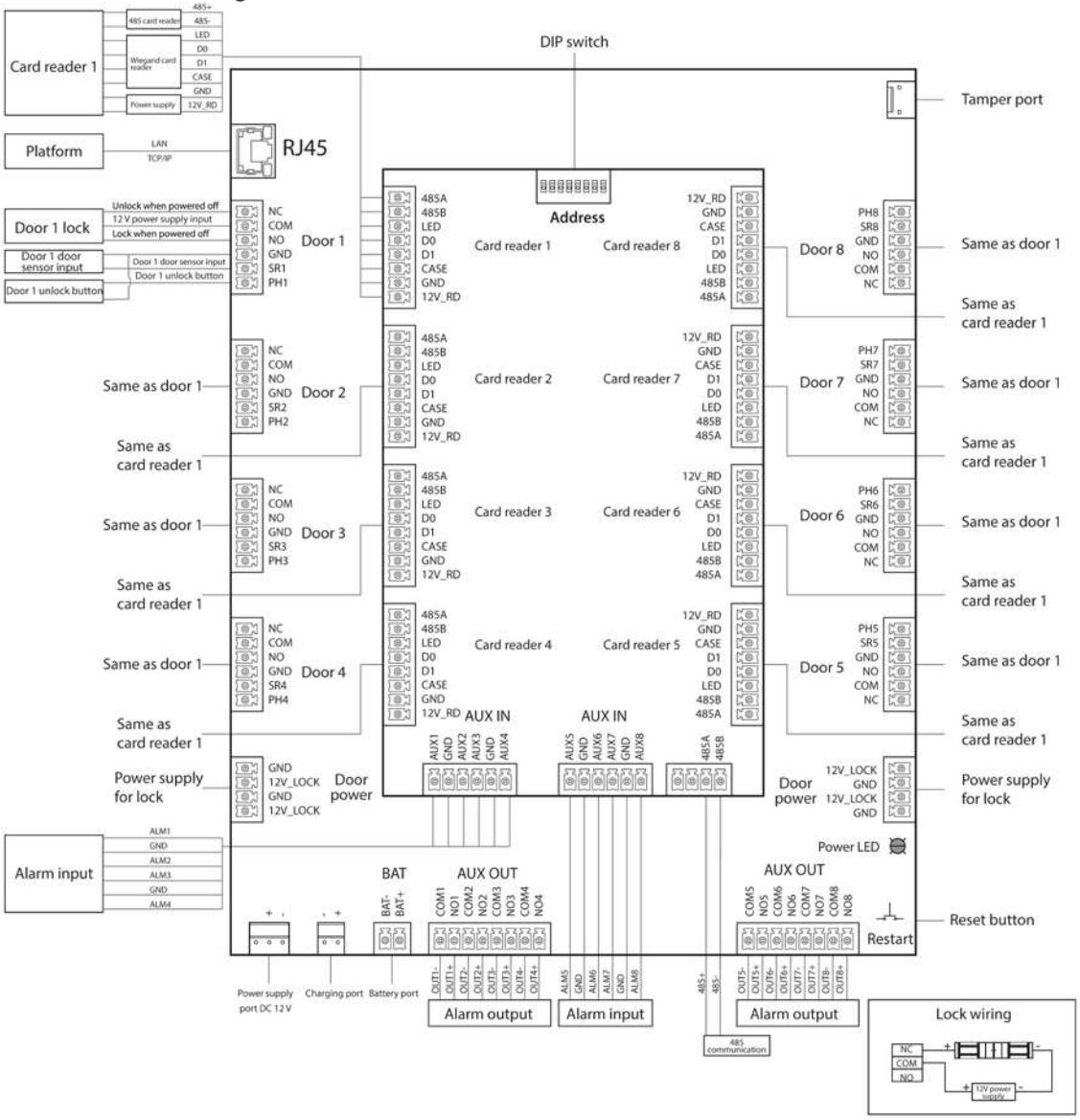
2.1.4 Cu patru uși, cu două sensuri

Figure 2-4 Conectați un controler bidirecțional cu patru uși



2.1.5 Un singur sens cu opt uși

Figure 2-5 Conectați un controler unidirecțional cu opt uși



2.1.6 Blocare

Selectați metoda de cablare în funcție de tipul dvs. de blocare.

Figure 2-6 Încuietoare electrică

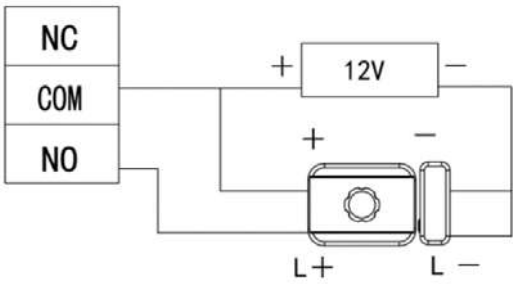


Figure 2-7 Încuietoare magnetică

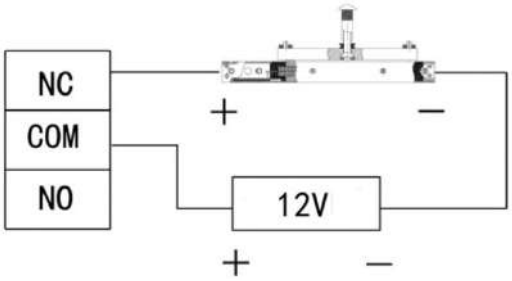
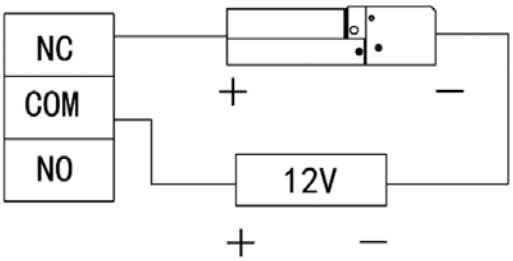


Figure 2-8 Șurub electric



2.1.7 Intrare alarmă

Portul de intrare pentru alarmă se conectează la dispozitive externe de alarmă, cum ar fi detectorul de fum și detectorul IR. Unele alarme din porturi pot lega starea de deschidere/închidere a ușii.

Tabelul 2-2 Intrare alarmă cablare

Tip	Un numar de Intrare alarmă Canale	Descriere
Cu două uși Sens unic	2	Starea ușii conectabile: ● Legături de alarmă externă AUX1 Deschis normal pentru toate ușile. ● Legături de alarmă externă AUX2 Normal închis pentru toate ușile.
Cu două uși În două sensuri	6	Starea ușii conectabile: ● Legături de alarmă externă AUX1–AUX2 Normal deschis pentru toate ușile. ● Legături de alarmă externă AUX3–A UX4 Normal închis pentru toate ușile.
Cu patru uși Sens unic	2	Starea ușii conectabile: ● Legături de alarmă externă AUX1 Deschis normal pentru toate ușile. ● Legături de alarmă externă AUX2 Normal închis pentru toate ușile.
Cu patru uși În două sensuri	8	Starea ușii conectabile: ● Legături de alarmă externă AUX1–AUX2 Normal deschis pentru toate ușile. ● Legături de alarmă externă AUX3–A UX4 Normal închis pentru toate ușile.
Cu opt uși Sens unic	8	Starea ușii conectabile: ● Legături de alarmă externă AUX1–AUX2 Normal deschis pentru toate ușile. ● Legături de alarmă externă AUX3–A UX4 Normal închis pentru toate ușile.

2.1.8 Ieșire alarmă

Când o alarmă este declanșată de la portul de intrare de alarmă intern sau extern, dispozitivul de ieșire de alarmă va raporta alarma și alarma va dura 15 s.

Când conectați dispozitivul cu două căi cu două uși la dispozitivul de ieșire de alarmă intern, selectați NC/NO în funcție de starea Întotdeauna deschis sau Întotdeauna închidere.

- NC: În mod normal, închis.
- NU: În mod normal deschis.

Tabel 2-3 Ieșire alarmă cablare

Tip	Număr de Ieșire de alarmă Canale	Descriere	
Cu două uși Sens unic	2	NUMARUL 1 COM1	● AUX1 declanșează ieșirea de alarmă. ● Timeout ușă și ieșire alarmă de efracție pentru ușa 1. ● Cititor de carduri 1 ieșire alarmă de manipulare.
		NO2 COM2	● AUX2 declanșează ieșirea de alarmă. ● Timeout ușă și ieșire alarmă de intruziune pentru ușa 2. ● Cititor de carduri 2 ieșire alarmă de manipulare.
Cu două uși În două sensuri	2	NUMARUL 1 COM1	AUX1/AUX2 declanșează ieșirea de alarmă.
		NO2 COM2	AUX3/AUX4 declanșează ieșirea de alarmă.
	2	NC1 COM1 NUMARUL 1	● Cititor de carduri 1/2 ieșire alarmă de manipulare. Timeout ● ușa 1 și ieșire pentru alarmă de intruziune.
		NC2 COM2 NO2	● Cititor de carduri 3/4 ieșire alarmă de manipulare. ● Timeout ușa 2 și ieșire alarmă de intruziune.
Cu patru uși Sens unic	2	NUMARUL 1 COM1	● AUX1 declanșează ieșirea de alarmă. ● Timeout ușă și ieșire pentru alarmă de intruziune. Ieșire ● alarmă de manipulare a cititorului de carduri.
		NO2 COM2	AUX2 declanșează ieșirea de alarmă.
Cu patru uși În două sensuri	8	NUMARUL 1 COM1	● AUX1 declanșează ieșirea de alarmă. ● Cititor de carduri 1/2 ieșire alarmă de manipulare. Timeout ● ușa 1 și ieșire pentru alarmă de intruziune. Ieșire alarmă ● de manipulare a dispozitivului.
		NO2 COM2	● AUX2 declanșează ieșirea de alarmă. ● Cititor de carduri 1/2 ieșire alarmă de manipulare. ● Timeout ușa 2 și ieșire alarmă de intruziune.
		NUMARUL 3 COM3	● AUX3 declanșează ieșirea de alarmă. ● Cititor de carduri 5/6 ieșire alarmă de manipulare. ● Timeout ușa 3 și ieșire alarmă de intruziune.
		NR4 COM4	● AUX4 declanșează ieșirea de alarmă. ● Cititor de carduri 7/8 ieșire alarmă de manipulare. ● Timeout ușa 4 și ieșire alarmă de intruziune.
		NR5 COM5	AUX5 declanșează ieșirea de alarmă.
		NR6 COM6	AUX6 declanșează ieșirea de alarmă.
		NR7 COM7	AUX7 declanșează ieșirea de alarmă.
		NR8 COM8	AUX8 declanșează ieșirea de alarmă.

Tip	Număr de Ieșire de alarmă Canale	Descriere	
Cu opt uși Sens unic	8	NUMARUL 1 COM1	● AUX1 declanșează ieșirea de alarmă. Cititor de carduri 1 ● ieșire alarmă de manipulare. Timeout ușa 1 și ieșire alarmă ● de intruziune. Ieșire alarmă de manipulare a dispozitivului. ●
		NO2 COM2	● AUX2 declanșează ieșirea de alarmă. Cititor de carduri ● 2 ieșire alarmă de manipulare. Timeout ușa 2 și ieșire ● alarmă de intruziune.
		NUMARUL 3 COM3	● AUX3 declanșează ieșirea de alarmă. Cititor de carduri ● 3 ieșire alarmă de manipulare. Timeout ușa 3 și ieșire ● alarmă de intruziune.
		NR4 COM4	● AUX4 declanșează ieșirea de alarmă. Cititor de carduri ● 4 ieșire alarmă de manipulare. Timeout ușa 4 și ieșire ● alarmă de intruziune.
		NR5 COM5	● AUX5 declanșează ieșirea de alarmă. Cititor de carduri ● 5 ieșire alarmă de manipulare. Timeout ușa 5 și ieșire ● alarmă de intruziune.
		NR6 COM6	● AUX6 declanșează ieșirea de alarmă. Cititor de carduri ● 6 ieșire alarmă de manipulare. Timeout ușa 6 și ieșire ● alarmă de intruziune.
		NR7 COM7	● AUX7 declanșează ieșirea de alarmă. Cititor de carduri ● 7 ieșire alarmă de manipulare. Timeout ușa 7 și ieșire ● alarmă de intruziune.
		NR8 COM8	● AUX8 declanșează ieșirea de alarmă. Cititor de carduri ● 8 ieșire alarmă de manipulare. Timeout ușa 8 și ieșire ● alarmă de intruziune.

2.1.9 Cititor de carduri

O singură ușă poate conecta doar cititoare de carduri de același tip, fie RS-485, fie Wiegand.

Tabelul 2-4 Descrierea specificațiilor cablului cititorului de carduri

Tip cititor de carduri	Metoda de cablare	Lungime
Cititor de carduri RS-485	Conexiune RS-485. Impedanța unui singur fir trebuie să fie de 10Ω.	100 m
Card Wiegand cititor	Conexiune Wiegand. Impedanța unui singur fir trebuie să fie de 2Ω.	80 m

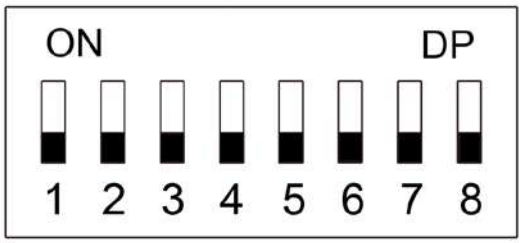
2.2 Indicator de putere

- Verde continuu: Normal.
- Roșu: Anormal.
- Verde intermitent: Se încarcă.
- Albastru: Controlerul este în modul Boot.

2.3 Comutator DIP

 (ON) indică 1;  indica 0.

Figure 2-9 Comutator DIP



- Când 1–8 sunt toate comutate la 0, controlerul pornește normal după pornire. Când 1–8
- sunt toate comutate la 1, controlerul intră în modul BOOT după ce pornește.
- Când 1, 3, 5 și 7 sunt comutate la 1, iar celelalte sunt 0, controlerul revine la valorile implicite din fabrică după ce repornește.
- Când 2, 4, 6 și 8 sunt comutate la 1 și celelalte sunt 0, controlerul revine la valorile implicite din fabrică, dar păstrează informațiile despre utilizator după ce repornește.

2.4 Alimentare electrică

2.4.1 Port de alimentare pentru blocarea ușii

Tensiunea nominală a portului de alimentare pentru încuietoarea ușii este de 12 V, iar curentul maxim de ieșire este de 2,5 A. Dacă sarcina de putere depășește curentul nominal maxim, asigurați o sursă de alimentare suplimentară.

2.4.2 Portul de alimentare al cititorului de carduri

- Controlere unidirecționale cu două uși, două uși și patru uși: Tensiunea nominală a portului de alimentare al cititorului de carduri (12V_RD) este de 12 V, iar curentul maxim de ieșire este de 1,4 A.
- Controlere cu două căi cu patru uși și cu opt uși: Tensiunea nominală a portului de alimentare al cititorului de carduri (12V_RD) este de 12 V, iar curentul maxim de ieșire este de 2,5 A.

3 Configurare SmartPSS AC

Puteți gestiona controlerul prin SmartPSS AC. Această secțiune prezintă în principal configurațiile rapide ale controlerului. 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.

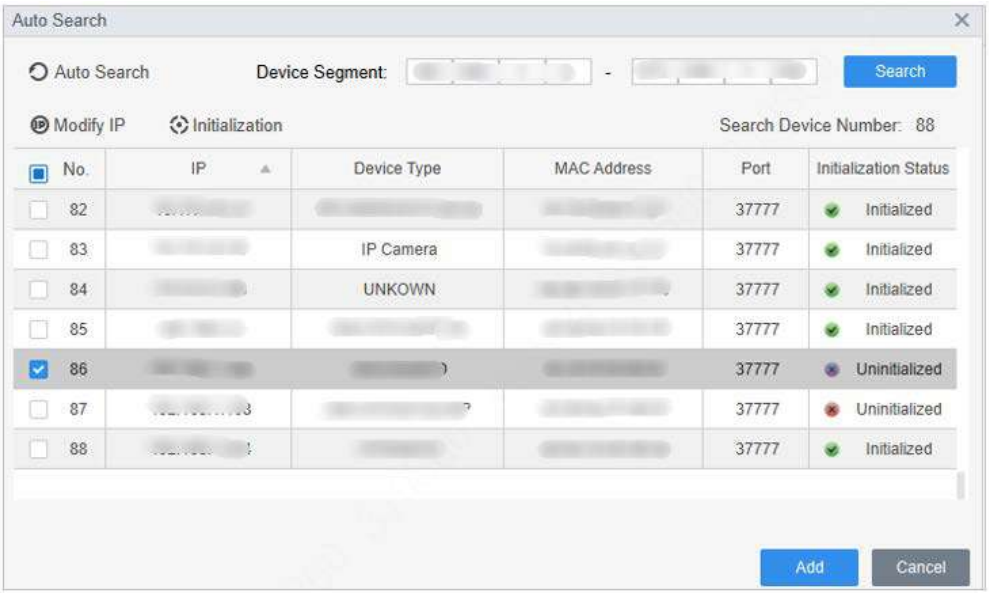
Step 2 Dublu click , apoi urmați instrucțiunile pentru a finaliza inițializarea și a vă conecta.

3.2 Inițializare

Înainte de inițializare, asigurați-vă că controlerul 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



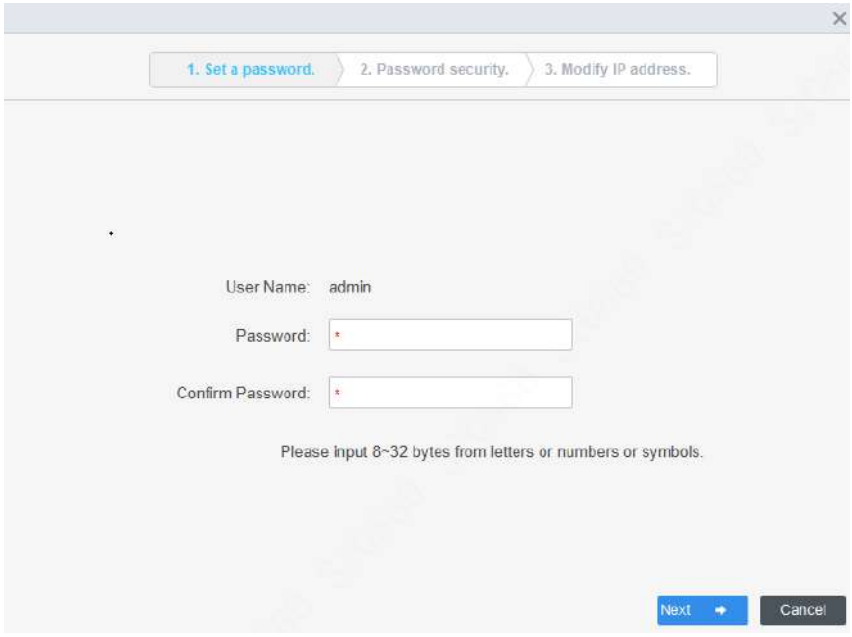
Step 2 Introduceți un interval de segment de rețea, apoi faceți clic**Căutare**.

Step 3 Selectați dispozitivul, 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.

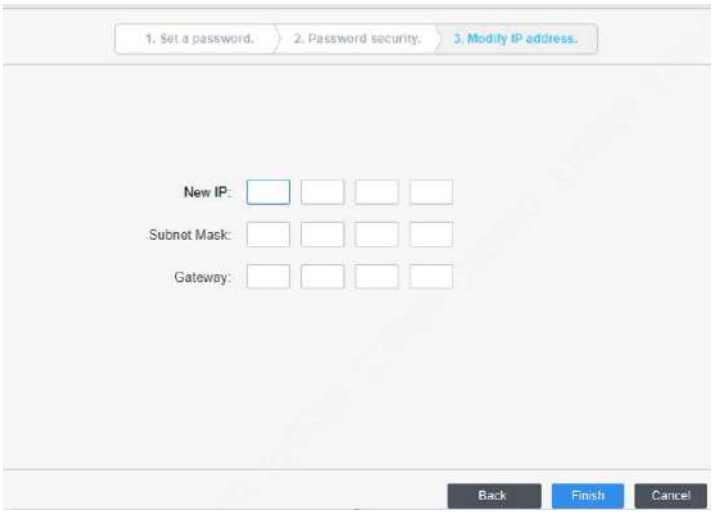
Figure 3-2 Seteaza parola



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 controlerul la SmartPSS AC. Puteți da clic**Căutare automată**pentru a adăuga și faceți clic**Adăuga**pentru a adăuga manual dispozitive.

3.3.1 Căutare automată

Vă recomandăm să adăugați dispozitive prin căutare automată atunci când trebuie să adăugați dispozitive în loturi în cadrul aceluiași segment de rețea sau când segmentul de rețea este clar, dar adresa IP a dispozitivului este neclară.

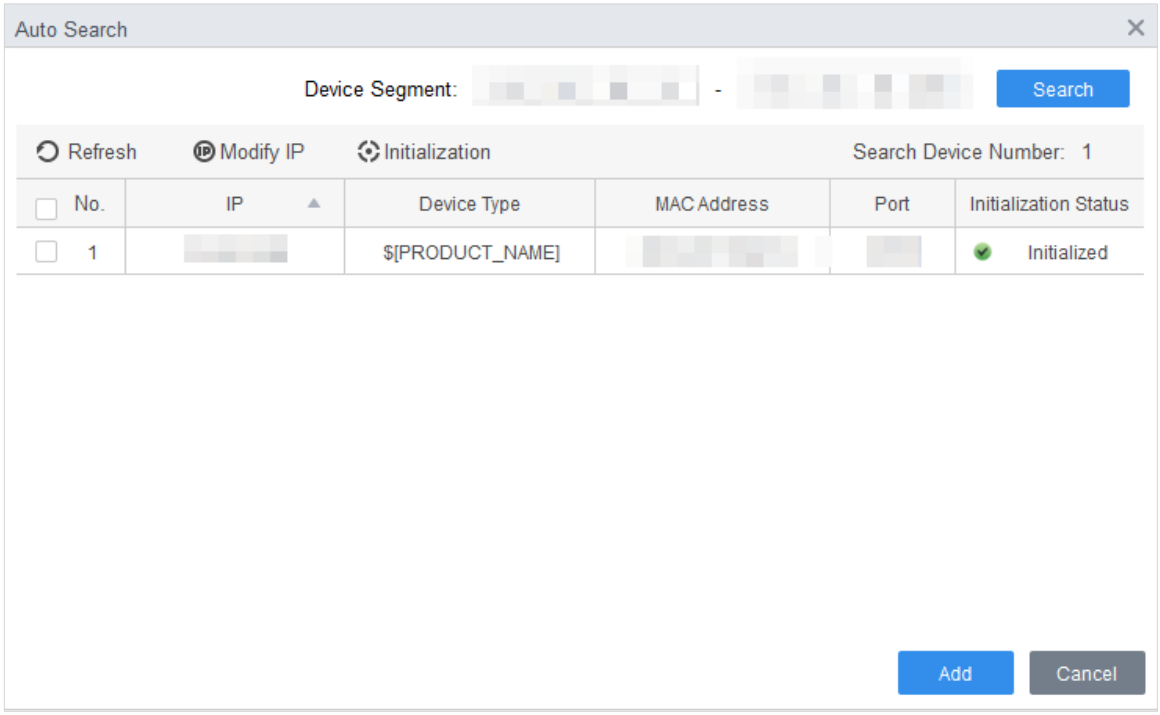
Step 1 Conectați-vă la SmartPSS AC.

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**. Va fi afișată o listă cu rezultatele căutării.

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

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.

Puteți vedea dispozitivele adăugate pe**Dispozitive**pagină.

- Numele de utilizator este admin și parola este admin123 în mod implicit. Recomandăm schimbarea parola după conectare.
- După adăugare, SmartPSS AC se conectează automat la dispozitiv. După conectarea cu succes, afișează stare**Pe net**. În caz contrar, se afișează**Deconectat**.

3.3.2 Adăugarea manuală

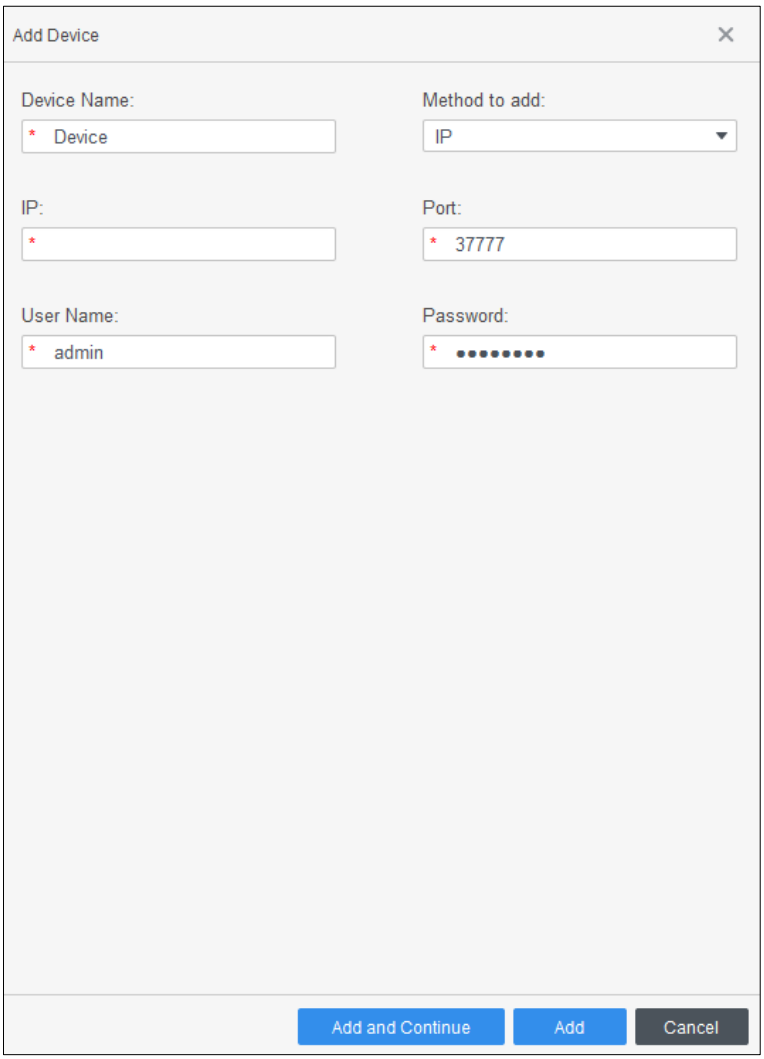
Puteți adăuga dispozitive manual. Trebuie să știți adresele IP și numele de domenii ale controlorilor de acces pe care doriți să le adăugați.

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 informații detaliate despre controlor.

Tabelul 3-1 Parametri

Parametru	Descriere
Nume dispozitiv	Introduceți un nume pentru controler. Vă recomandăm să numiți controlerul după zona de instalare pentru o identificare ușoară.
Metoda de adaugat	Selectați**IP**pentru a adăuga controlerul prin adresa IP.
IP	Introdu adresa IP a controlerului. Este implicit 192.168.1.108.
Port	Introduceți numărul portului dispozitivului. Numărul portului este 37777 implicit.
Nume de utilizator, Parola	Introduceți numele de utilizator și parola controlerului. Numele de utilizator este admin și parola este admin123 în mod implicit. Vă recomandăm să schimbați parola după autentificare.

Step 5 Clic**Adăuga**.

Dispozitivul adăugat este pe**Dispozitive**pagină.

După adăugare, SmartPSS AC se conectează automat la dispozitiv. După conectarea cu succes, afișează stareaPe net. În caz contrar, se afișeazăDeconectat.

3.4 Managementul utilizatorilor

Adăugați utilizatori, atribuiți-le carduri și configurați-le permisiunile de acces.

3.4.1 Setarea tipului cardului

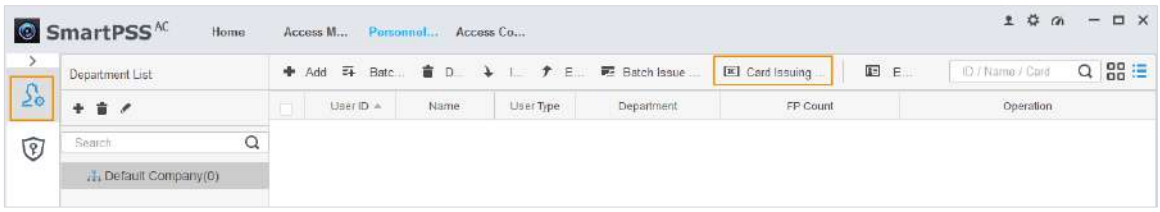
Înainte de a atribui cardul, setați mai întâi tipul cardului. De exemplu, dacă cardul alocat este carte de identitate, selectați tipul ca carte de identitate.

Tipul de card selectat trebuie să fie același cu tipul de card alocat efectiv; 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

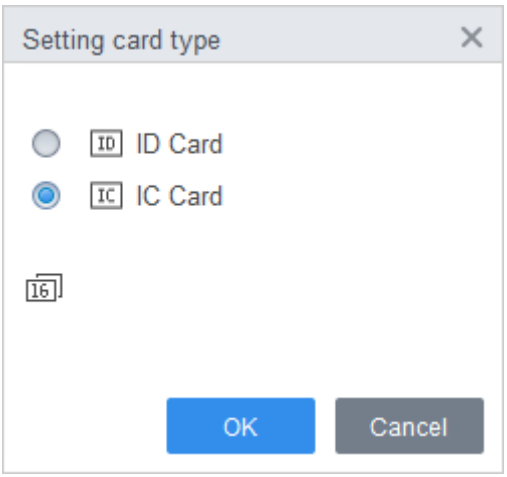


Step 3 Pe**Manager de personal**pagina, faceți clic , apoi apasa .

Step 4 Pe**Setarea tipului cardului**fereastra, 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 individuală

Puteți adăuga utilizatori individual.

Step 1 Conectați-vă la SmartPSS AC.

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

Step 3 Adăugați informații de bază ale utilizatorului.

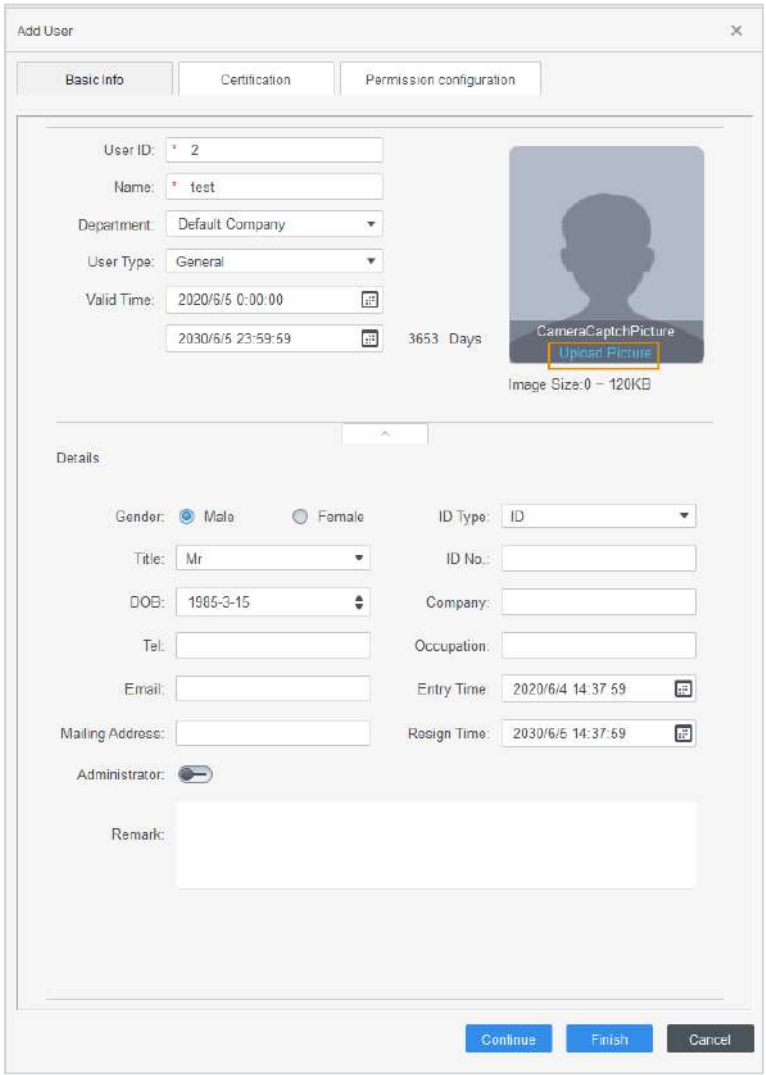
1) Faceți clic pe**Informatii de baza**fila de pe**Adăugați utilizator**pagina și apoi adăugați informații de bază despre utilizator.

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 introdus manual. Pentru a citi numărul cardului automat, selectați un cititor de carduri, apoi plasați cardul pe cititorul de carduri.

1) Faceți clic a setaDispozitivsauEmitentul cardului la cititorul de carduri.

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

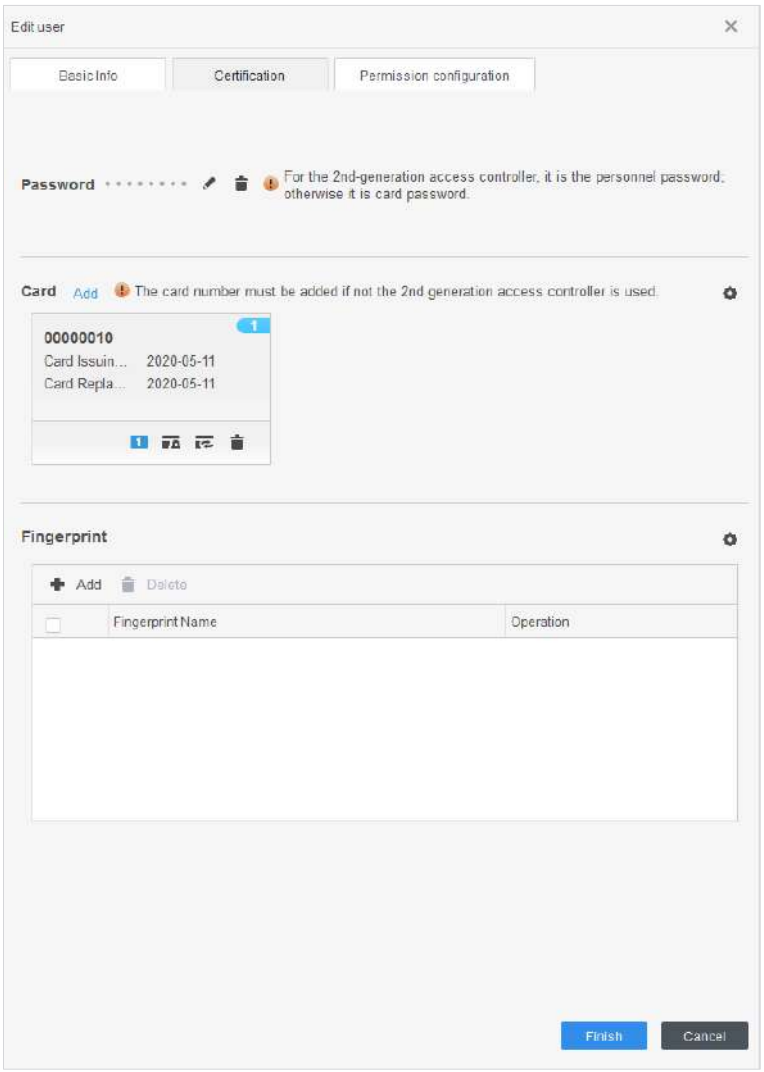
3) După adăugare, puteți seta cardul pe cardul principal sau pe cardul de constrângere sau puteți înlocui cardul cu unul nou sau ștergeți cardul.

- Configurați amprenta digitală.

1) Faceți clic a setaDispozitivsauScaner de amprentela colectorul de amprente.

2) Faceți clicAdăugați amprentași apăsați degetul pe scaner de trei ori continuu.

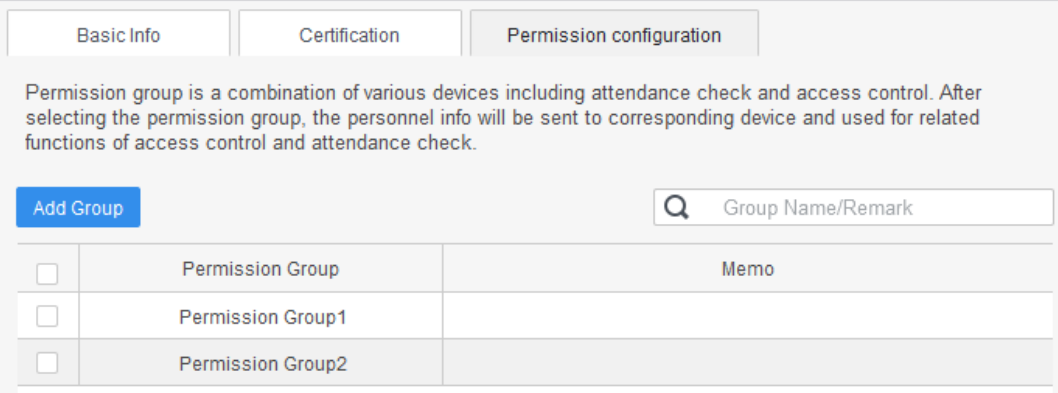
Figure 3-10 Configurați certificarea



Step 5 Configurați permisiunile 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.

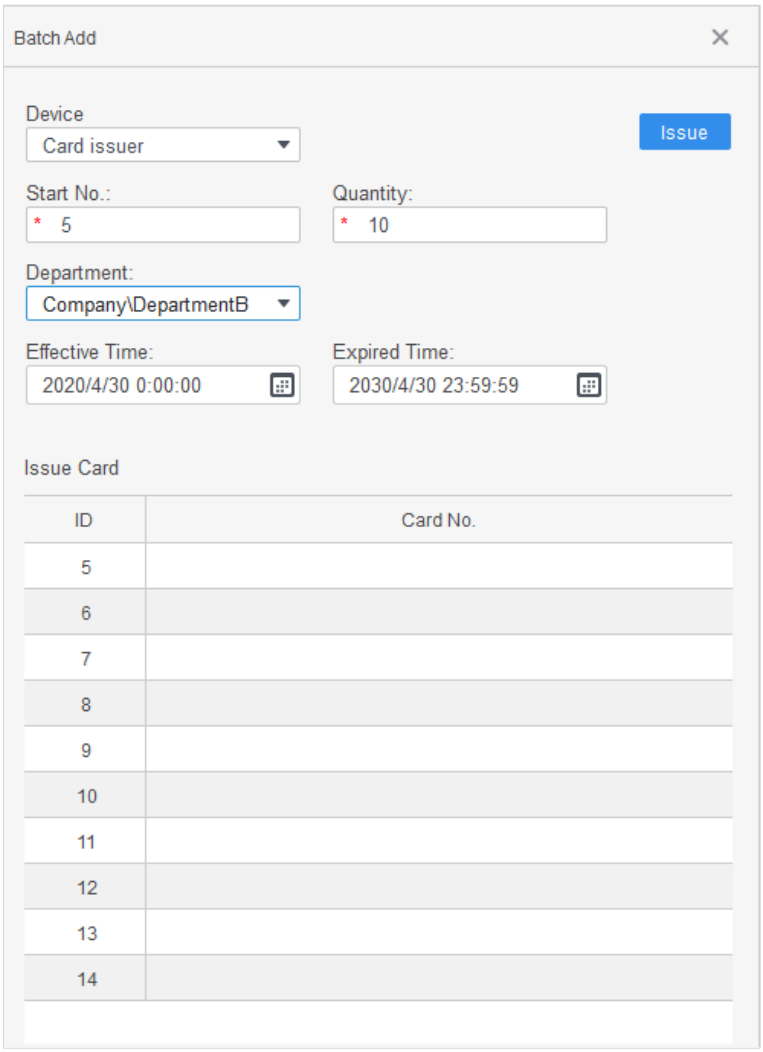
Step 2 Clic**Manager de personal**>**Utilizator**>**Adăugare lot**.

Step 3 Selectați cititorul de carduri și departamentul de utilizator. Setați numărul de început, cantitatea cardului, timpul efectiv și timpul expirat al cardului.

Step 4 Clic**Emisiune**la atribuirea cardurilor.

Step 5 Numărul cardului va fi citit automat. Clic**Stop**după atribuirea cardului, apoi faceți clic**Bine**.

Figure 3-12 Adăugați utilizatori în loturi



3.5 Configurarea permisiunii

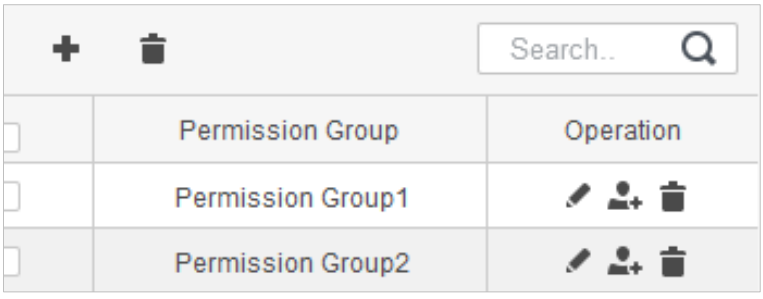
3.5.1 Adăugarea unui grup de permisiuni

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.

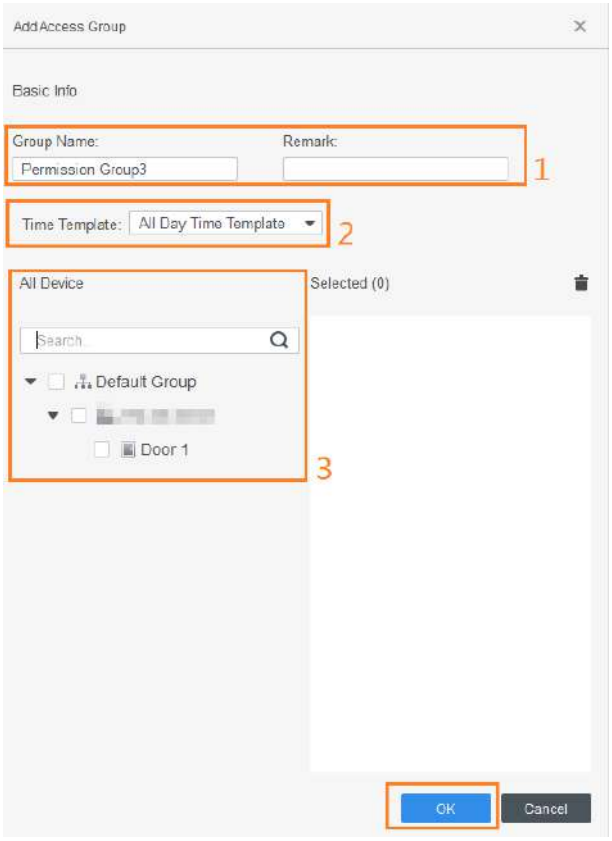
1) Introduceți numele grupului și observația.

2) Selectați șablonul de timp.

Pentru detalii despre setarea șablonului de timp, consultați manualul utilizatorului SmartPSS AC.

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

Figure 3-14 Adăugați un grup de permisiuni



Step 5 Clic**Bine**.

Operație aferentă

Pe**Lista grupurilor de permisiuni**pagina, puteți:

- Faceți 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 permisiunii de acces

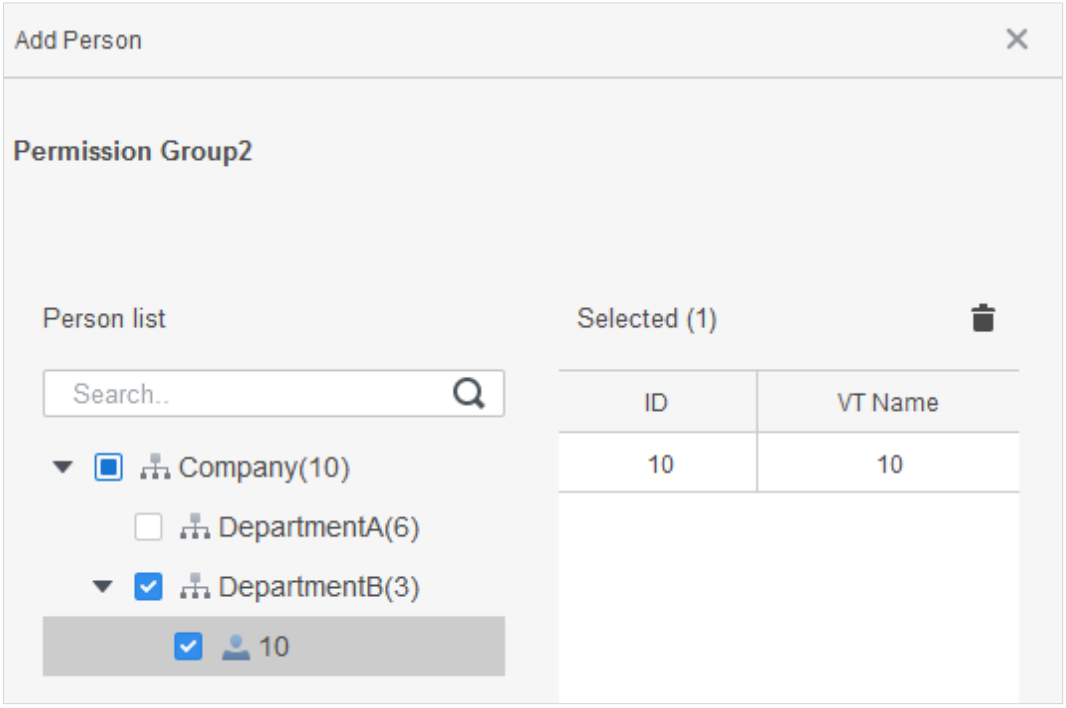
Asociați utilizatorii cu grupurile de permisiuni dorite, iar apoi utilizatorilor li se vor atribui permisiuni de acces la ușile definite.

Step 1 Conectați-vă la SmartPSS AC.

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

Step 3 Selectați grupul de permisiuni țintă, 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 Configurarea funcţiilor 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 prima permisiune de deblocare a cardului ar trebui să fie din**General**utilizator tastați și aveți permisiuni pentru anumite uși. Setați tipul când adăugați utilizatori. Pentru detalii, vezi „3.3.2 Adăugarea unui utilizator”.
- Pentru detalii despre atribuirea permisiunilor, consultați „3.5 Configurarea permisiunii”.

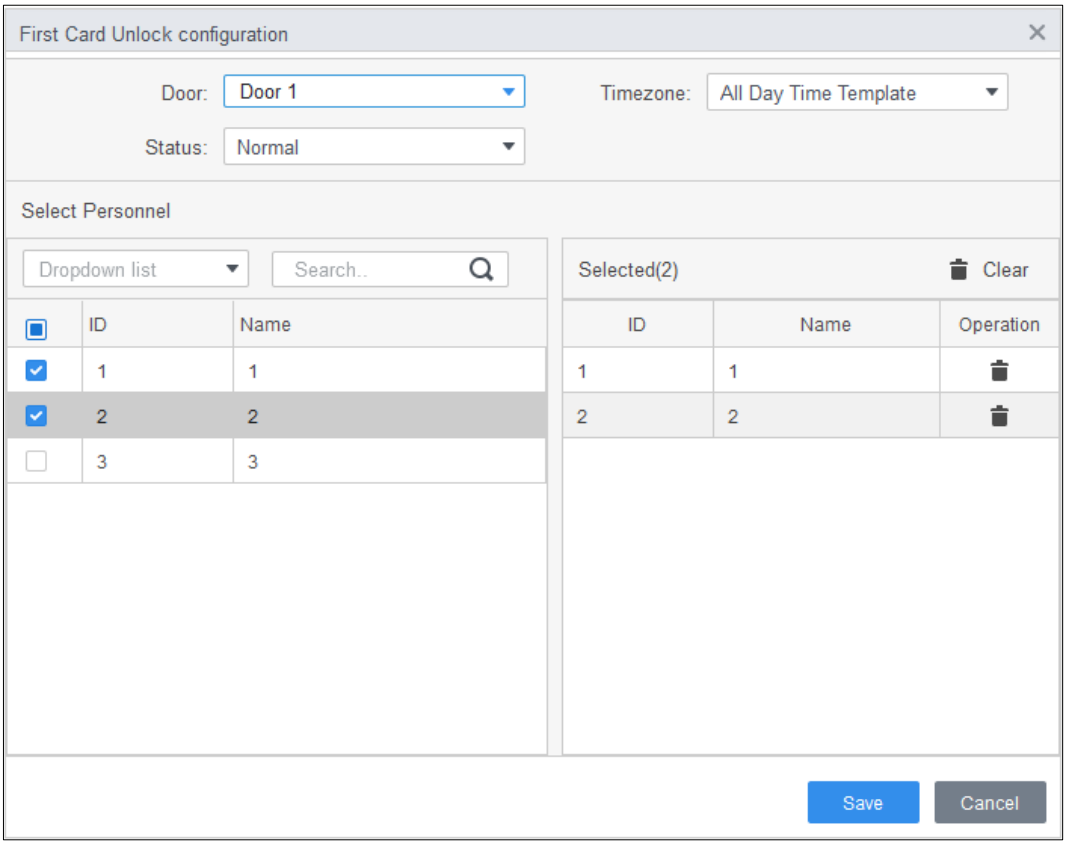
Step 1 Selectați**Configurare acces**>**Configurare avansată**. Apasă pe

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

Step 3

Step 4 Configurați**Prima deblocare a cardului**parametri, apoi faceți clic**Salvați**.

Figure 3-16 Prima configurație de deblocare a cardului



Tabelul 3-2 Parametrii deblocării primei cărți

Parametru	Descriere
Ușă	Selectați canalul de control al accesului țintă pentru a configura prima deblocare a cardului.
Fus orar	**Prima deblocare a cardului**este valabilă în perioada șablonului de timp selectat.
stare	După**Prima deblocare a cardului**este activată, ușa este fie în**Mod normal**sau **Modul Întotdeauna Deschis**.
Utilizator	Selectați utilizatorul care să dețină primul card. Acceptă selectarea unui număr de utilizatori care să dețină primele cărți. Oricare dintre ei trecând pe primul card înseamnă că primul card este deblocat.

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**VIP**sau**Patrulare**tastați pentru persoanele din grupul de utilizatori. Pentru detalii, consultați „3.3.2 Adăugarea unui utilizator”.

- Pentru detalii despre atribuirea permisiunii, consultați „3.4 Configurarea permisiunii”.

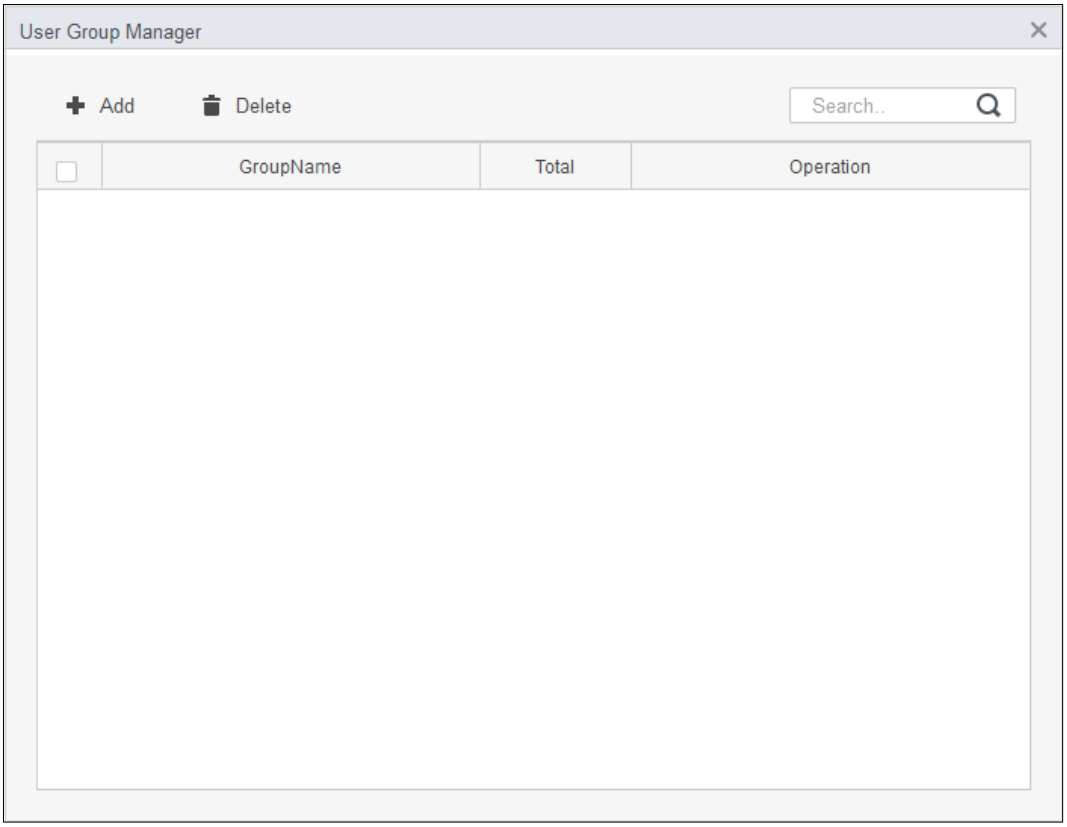
Step 1 Selectați**Configurare acces**>**Configurare avansată**. Apasă pe

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

Step 3

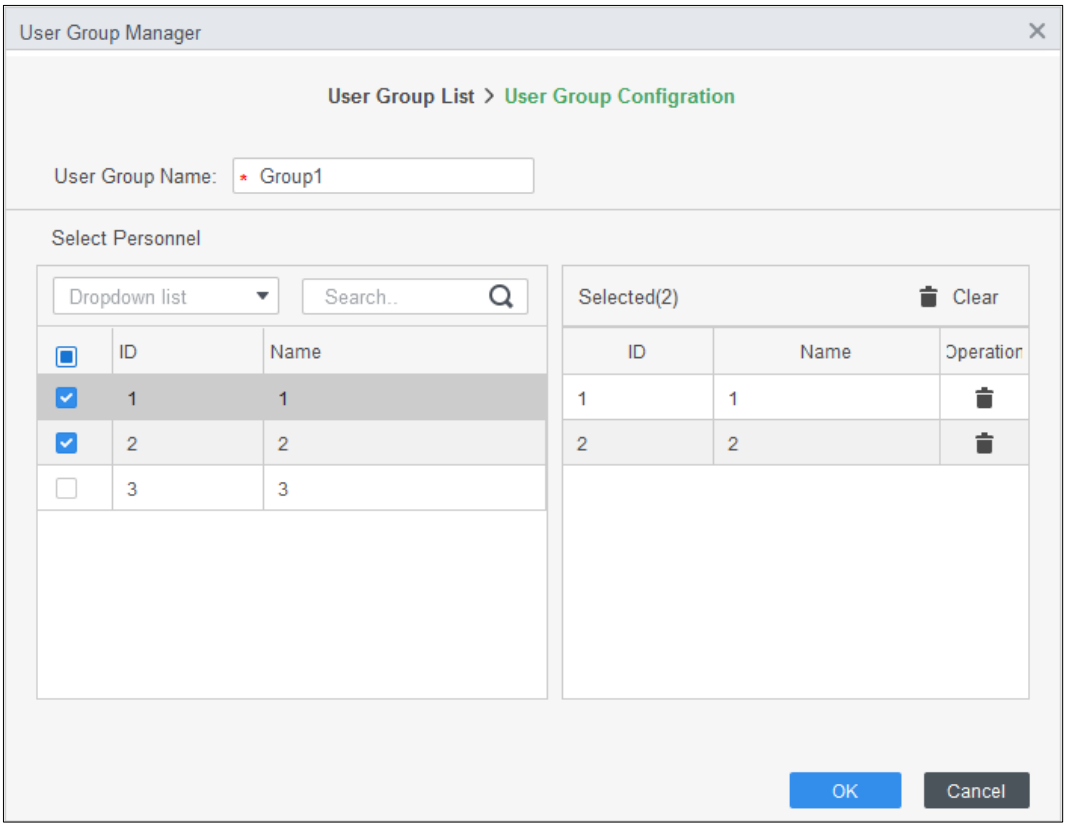
1) Faceți clic**Grup de utilizatori**.

Figure 3-17 Manager de grup de utilizatori



2) Faceți clic**Adăuga**.

Figure 3-18 Configurarea grupului de utilizatori



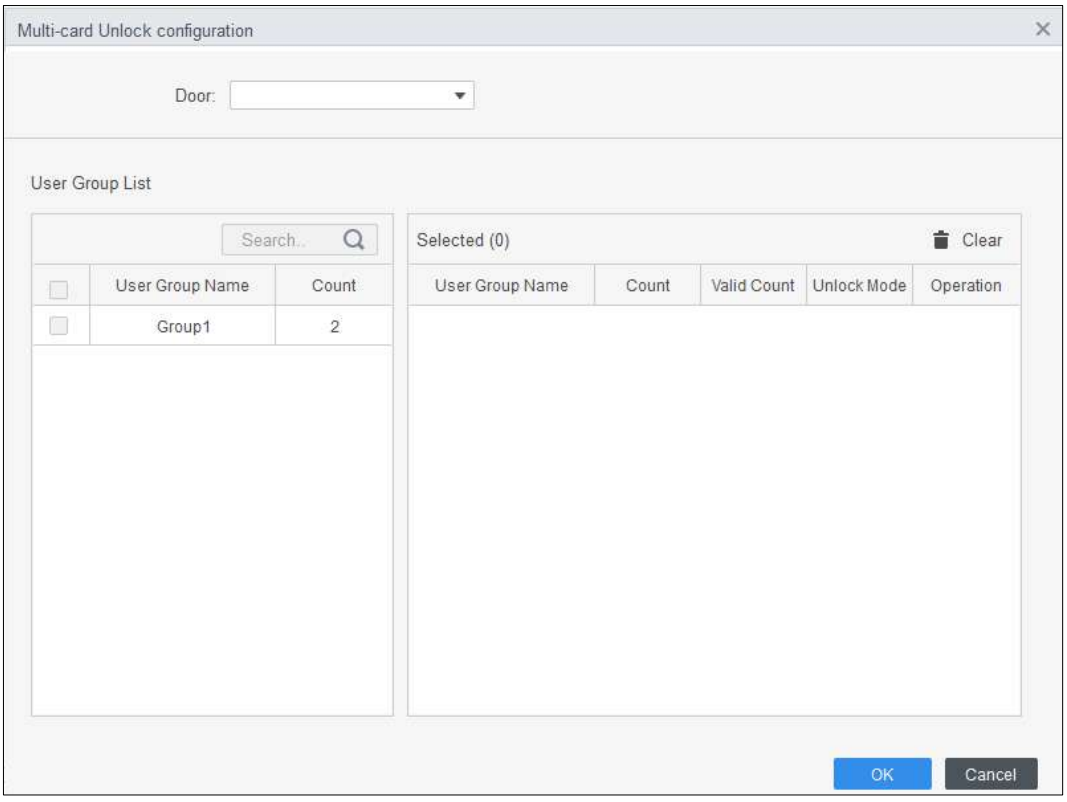
3) Configurați**Numele grupului de utilizatori**. Selectați utilizatori din**Lista de utilizatori**și faceți clic**Bine**. Puteți selecta până la 50 de utilizatori.

4) Faceți clic în colțul din dreapta sus al**Manager de grup de utilizatori**pagină. Configurați parametrii deblocării cu mai multe carduri.

Step 4

1) Faceți clic**Adăuga**.

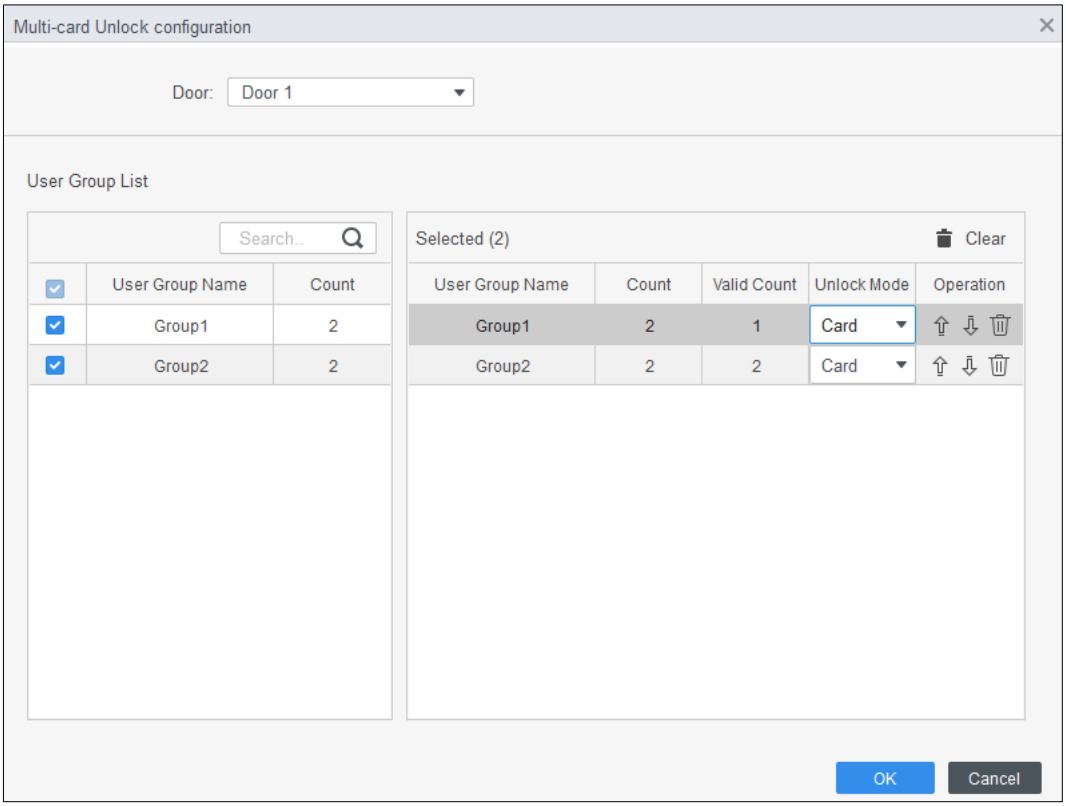
Figure 3-19 Configurație de deblocare cu mai multe carduri (1)



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**pentru ca fiecare grup să fie la fața locului, apoi selectați**Modul de deblocare**.

Clic sau pentru a regla secvența grupului pentru a debloca ușa.

- Numărul valid se referă la numărul de utilizatori din fiecare grup pentru care trebuie să fie pe site glisează-le cardurile. Luați ca exemplu Figura 3-17. Ușa poate fi descuiată numai după ce o persoană din grupul 1 și 2 persoane din grupul 2 și-au trecut cardurile.
- Sunt permise până la cinci utilizatori validi.

5) Faceți clic**Bine**.

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

Cel nou adăugat**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 și unitatea este minute.

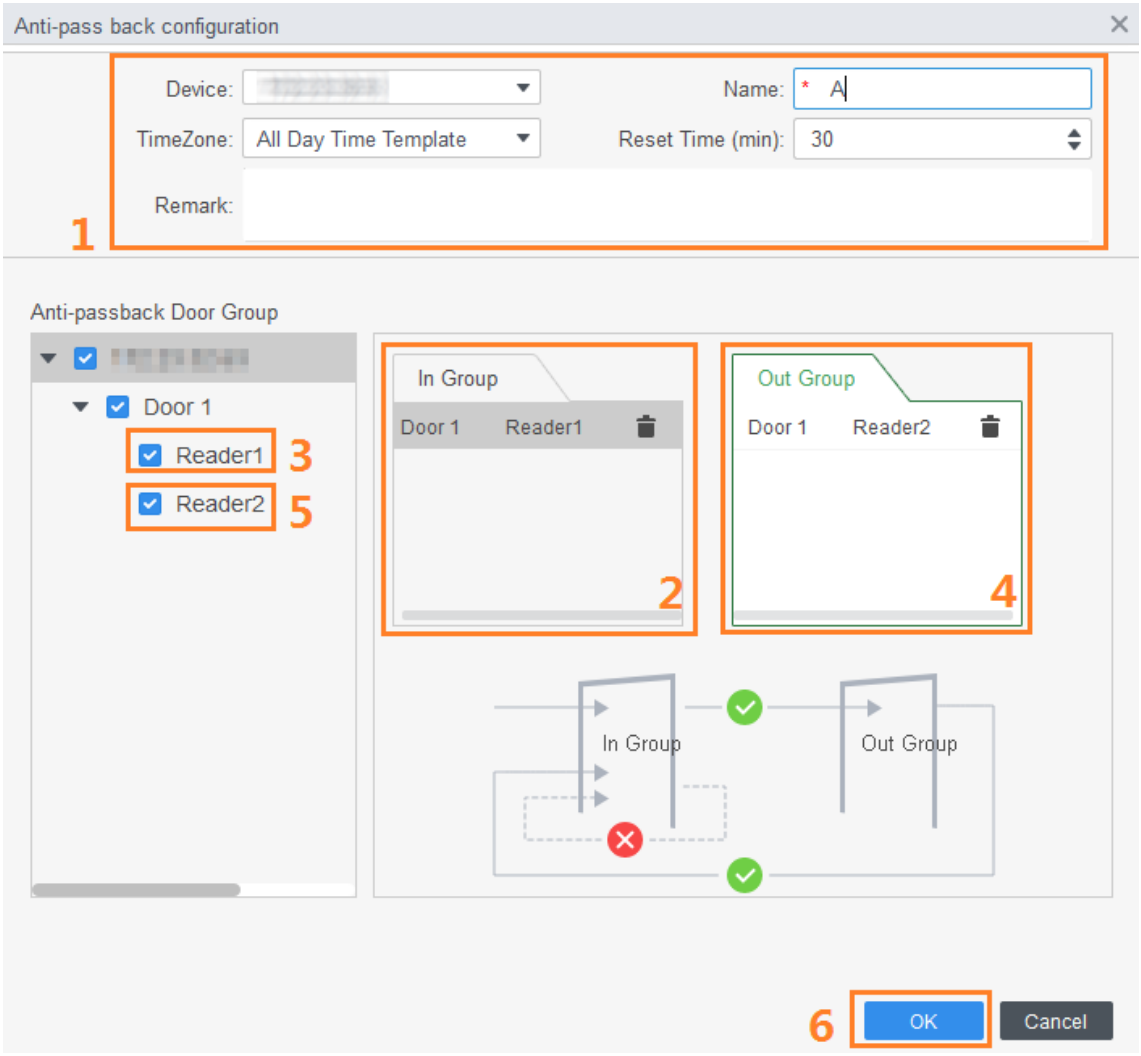
De exemplu, setați timpul de resetare la 30 de minute. Dacă un personal a trecut, dar nu a trecut, alarma anti-pass back va fi declanșată atunci când acest personal tinde să treacă din nou înăuntru în decurs de 30 de minute. Cea de-a doua înregistrare a acestui personal este valabilă numai după 30 de minute mai târziu.

4) Faceți clic**In grup**și selectați cititorul corespunzător. Și apoi faceți clic**Out Group**și selectați cititorul corespunzător.

5) Faceți clic**Bine**.

Configurația va fi trimisă pe dispozitiv și va intra în vigoare.

Figure 3-21 Configurație anti-pass back



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

Cel nou adăugat**Anti-passback**este activat implicit.

3.6.1.4 Încuietoare inter-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 dispozitivul și introduceți numele dispozitivului.

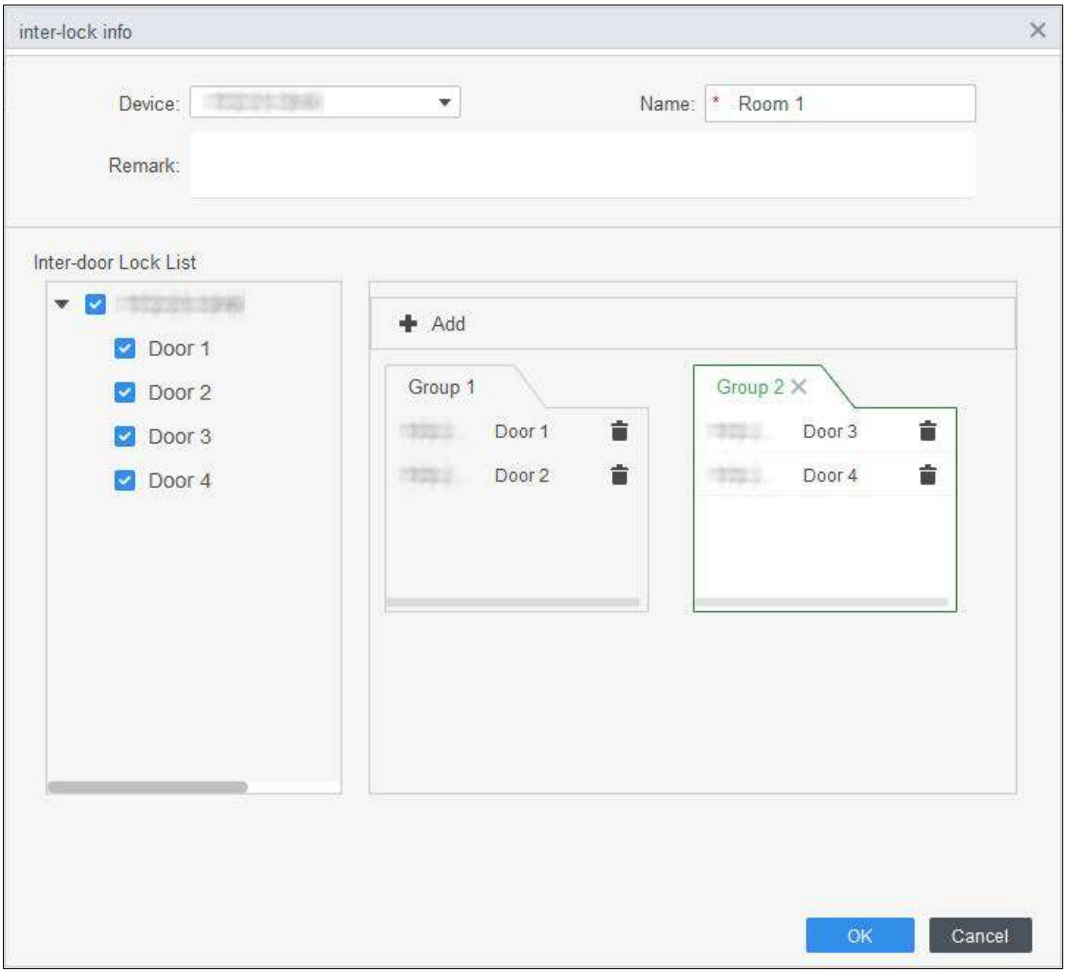
2) Introduceți observația.

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

4) Adăugați ușile controlerului de acces la grupul de uși necesar. Faceți clic pe un grup de uși, apoi faceți clic pe uși pentru a adăuga.

5) Faceți clic**Bine**.

Figure 3-22 Configurație încuietoare inter-uși



Step 5 (Opțional) Faceți clic . Pictograma se schimbă în , ceea ce indică**Încuietoare inter-uși**este activat.

Cel nou adăugat**Încuietoare inter-uși**este activat implicit.

3.6.2 Configurarea controlerului de acces

Puteți configura ușa de acces, cum ar fi direcția cititorului, starea ușii și modul de deblocare.

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

Step 2 Faceți clic pe ușa care trebuie configurată.

Step 3 Configurați parametrii.

Figure 3-23 Configurați ușa de acces

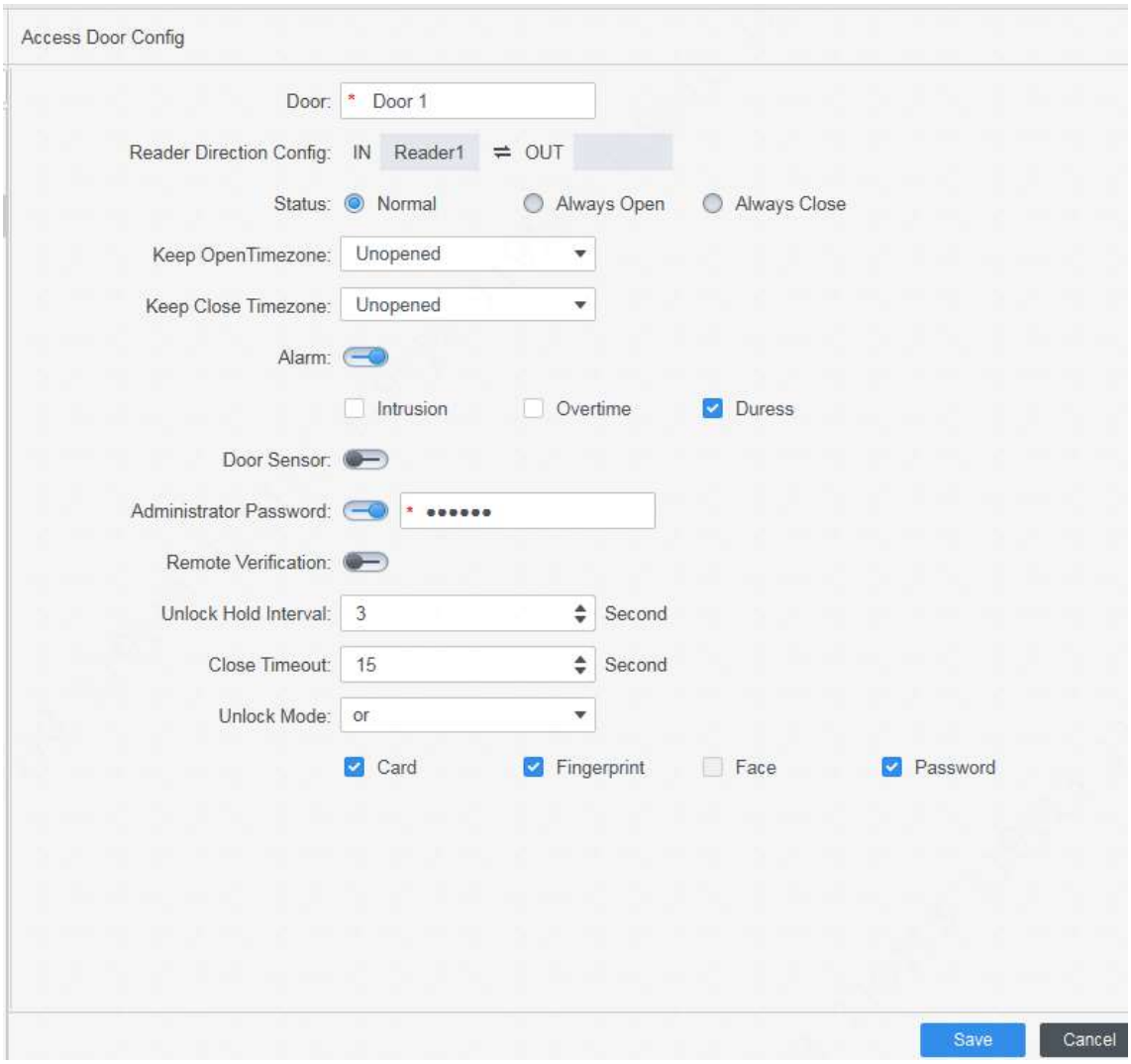
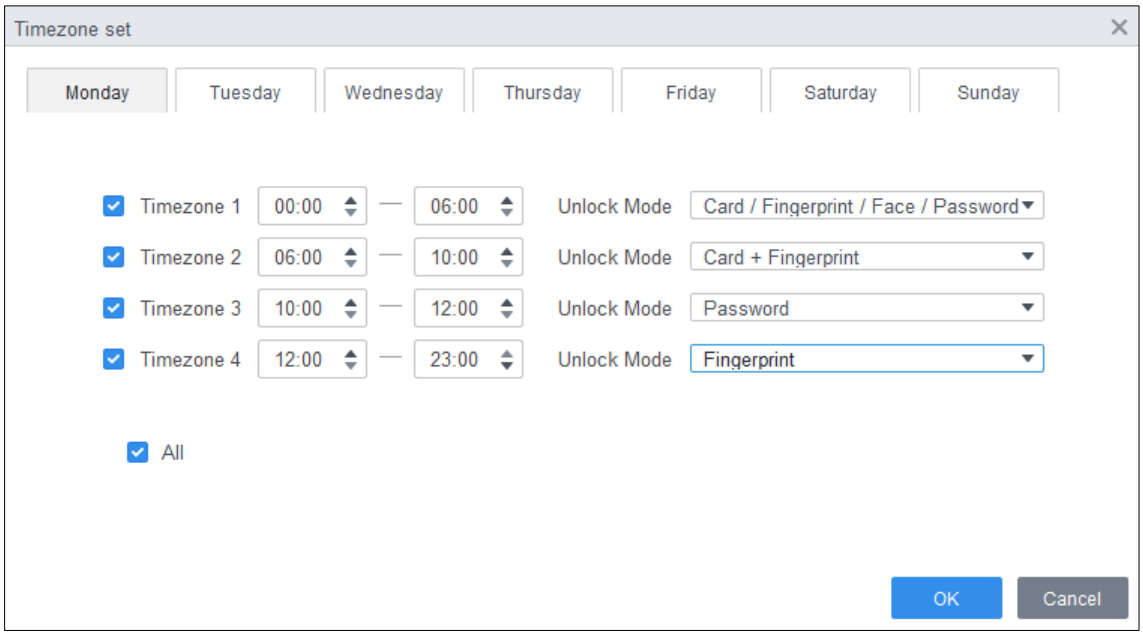


Figure 3-24 Deblocați după perioadă de timp



Tabelul 3-3 Parametrii ușii de acces

Parametru	Descriere
Uşă	Introduceți numele ușii.
Direcția cititorului Config	Clic ⇌ pentru a seta direcția cititorului în funcție de situațiile reale.
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 când ușa este întotdeauna deschisă.
Păstrați în apropiere fusul orar	Selectați șablonul de timp când ușa este întotdeauna închisă.
Alarma	Activați funcția de alarmă și setați tipul de alarmă, inclusiv intruziune, ore suplimentare și constrângere. Când alarma este activată, SmartPSS-AC va primi mesajul încărcat când alarma este declanșată.
Senzor de ușă	Activați senzorul ușii, astfel încât să puteți cunoaște starea reală a ușii. Vă recomandăm să activați funcția.
Administrator Parola	Activați și setați parola de administrator. Puteți accesa introducând parola.
Verificare de la distanță	Activați funcția și setați șablonul de timp, iar apoi accesul persoanei trebuie verificat de la distanță prin SmartPSS-AC în timpul perioadelor de șablon.
Deblocați intervalul de așteptare	Setați intervalul de deblocare. Ușa se va închide automat când timpul se termină.
Închideți Timeout	Setați timeout-ul pentru alarmă. De exemplu, setați timeout de închidere la 60 de secunde. Dacă ușa nu este închisă mai mult de 60 de secunde, mesajul de alarmă va fi încărcat.
Modul de deblocare	Selectați modul de deblocare după cum este necesar. ● Selectați**Și**și selectați metodele de deblocare. Puteți deschide ușa combinând metodele de deblocare selectate. ● Selectați**Sau**și selectați metodele de deblocare. Puteți deschide ușa într-unul din modurile pe care le-ați configurat. ● Selectați**Deblocați după perioadă de timp**și selectați modul de deblocare pentru fiecare perioadă de timp. Ușa poate fi deschisă numai prin metoda(ele) selectată(e) în perioada definită.

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 Adăugați personalul necesar la SmartPSS-AC.

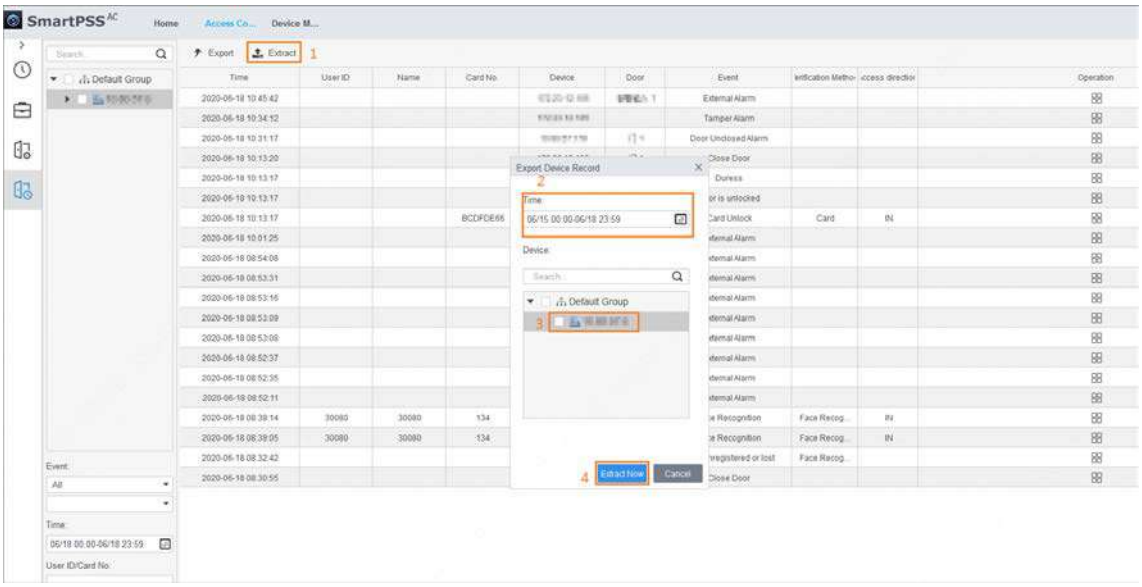
Step 2 Clic**Configurare acces**>**Eveniment istoric**pe pagina de start. Faceți

Step 3 clic pe**Manager de acces**pagină.

Step 4 Extrageți evenimentele de la dispozitivul de ușă în local. Clic**Extrage**, setați ora, selectați dispozitivul ușii, apoi faceți clic**Extrage acum**.

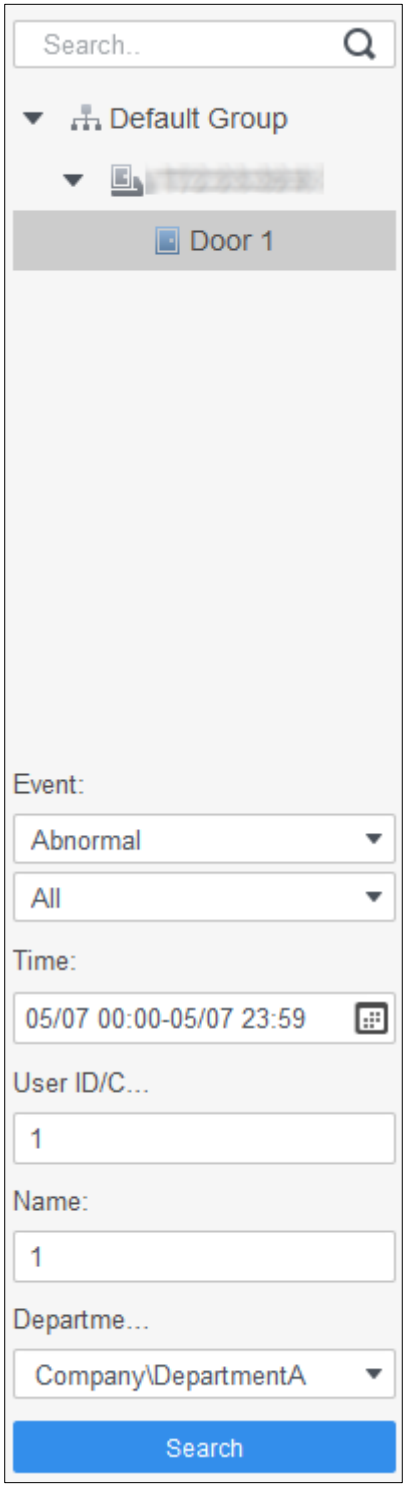
Puteți selecta mai multe dispozitive simultan pentru a extrage evenimente.

Figure 3-25 Extrage evenimente



Step 5 Setați condițiile de filtrare, apoi faceți clic**Căutare**.

Figure 3-26 Căutați evenimente prin filtrarea condițiilor



3.7 Managementul accesului

3.7.1 Deschiderea și închiderea ușii de la distanță

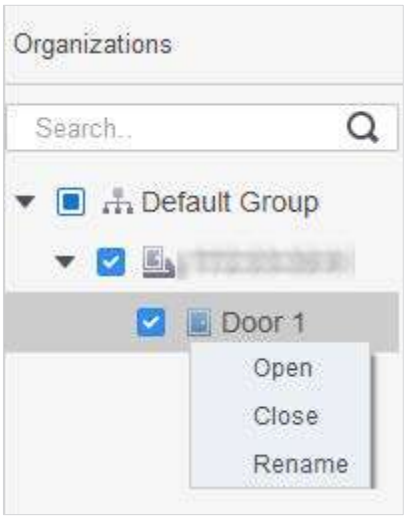
Puteți controla ușa de la distanță prin SmartPSS AC.

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

Step 2 Controlați ușa de la distanță. 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.

Figure 3-28 Control de la distanță (metoda 2)

Step 3 Vedeți starea ușii după**Informații despre eveniment**listă.

- Filtrarea evenimentelor: Selectați tipul de eveniment în**Informații despre eveniment**, iar lista de evenimente afișează evenimente dintre tipurile selectate. De exemplu, selectați**Alarma**, iar lista de evenimente afișează doar alarma evenimente.
- Blocarea reîmprospătării evenimentului: faceți clic chiar lângă**Informații despre eveniment**pentru a bloca sau debloca lista de evenimente și atunci evenimentele în timp real nu pot fi vizualizate.
- Ștergerea evenimentului: faceți clic chiar lângă**Informații despre eveniment**pentru a șterge toate evenimentele din lista de evenimente.

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

3.7.3 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

Pentru funcția anti-pass back, setați modul anti-pass back în**Anormal**de**Configurare eveniment**, și apoi configurați parametrii în**Configurare avansată**. Pentru detalii, consultați „3.5.1 Configurarea avansată Funcții”.

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

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

Step 3 chiar lângă**Alarmă de intruziune**pentru a activa funcția.

Step 4 Configurați acțiunile de conectare a alarmei de intruziune după cum este necesar.

- Activați sunetul alarmei.

  Apasă pe**Notifică**fila și faceți clic chiar lângă**Sunet de alarmă**. Când evenimentul de intruziune se întâmplă, controlerul de acces avertizează cu un sunet de alarmă.

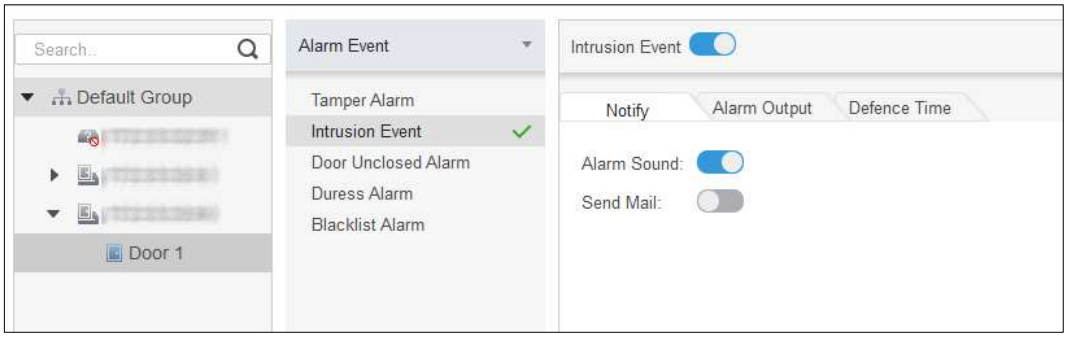
- Trimite e-mail de alarmă.

  1) Activați**Trimite e-mail**și confirmați pentru a seta SMTP. The**Setarile sistemului**este afișată pagina.

  2) Configurați parametrii 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 I/O alarmă.

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

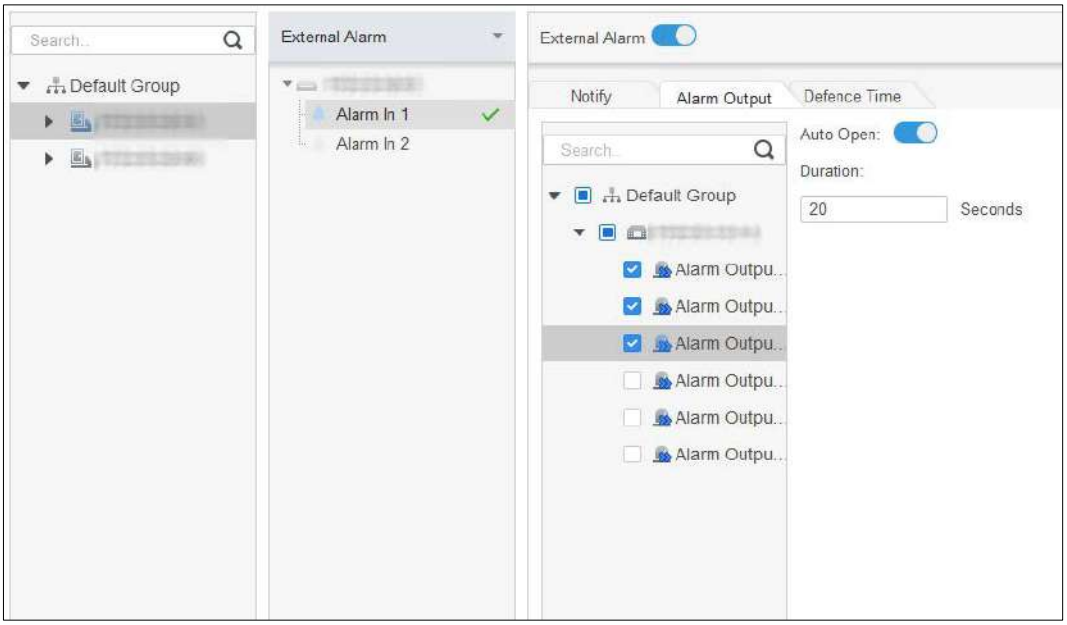
2) Selectați dispozitivul care acceptă alarma, selectați interfața de alarmă și apoi activați **Alarmă externă**.

3) Selectați dispozitivul care acceptă ieșirea alarmei, apoi selectați interfața de ieșire alarmă.

4) Activați**Deschidere automată**pentru conectarea alarmei.

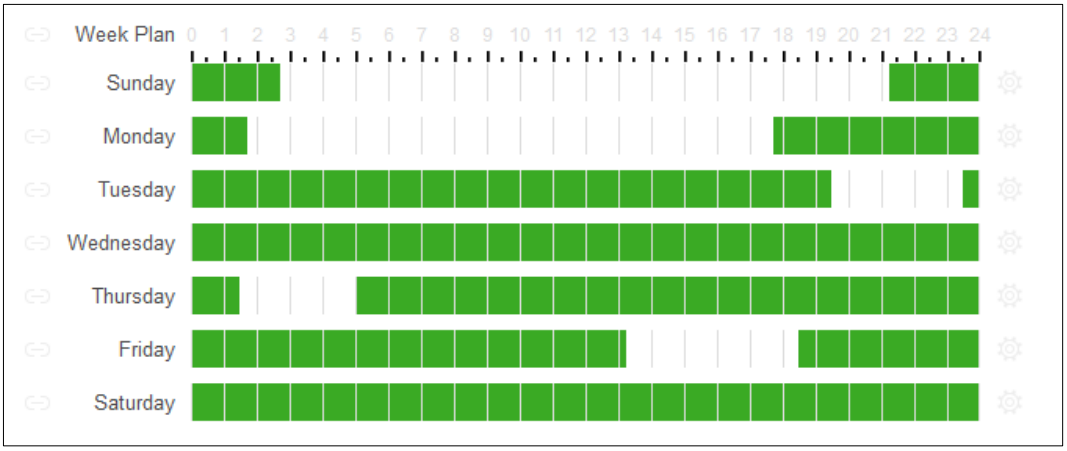
5) Setați durata.

Figure 3-31 Configurați conexiunea alarmei



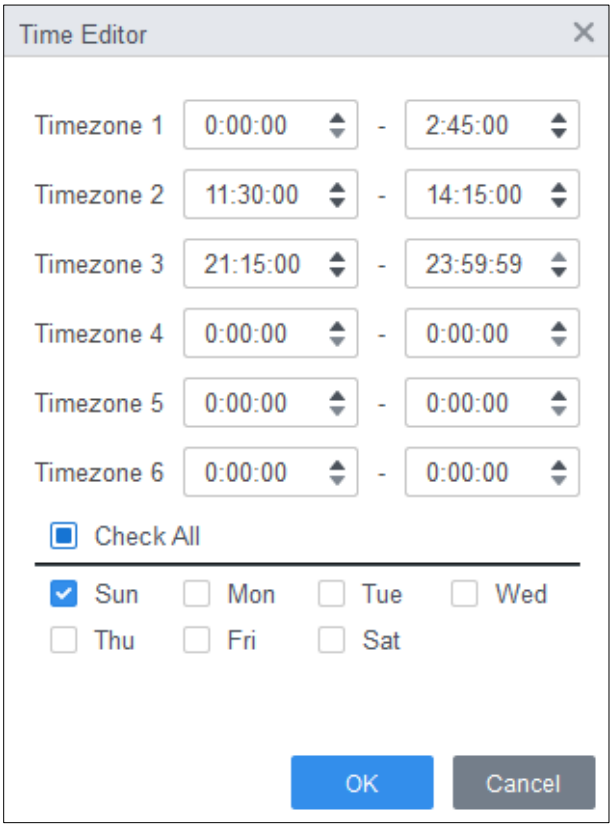
- Setați timpul de armare. Există două metode.
  - Metoda 1: Mutați cursorul pentru a seta perioade. Când cursorul este creion, faceți clic pentru a adăuga puncte; când cursorul este șters, faceți clic pentru a elimina punctele. Zona verde sunt perioadele de armare.

Figure 3-32 Setați timpul de armare (metoda 1)



-Metoda 2: Faceți clic pentru a seta perioade, 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 utilizat 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

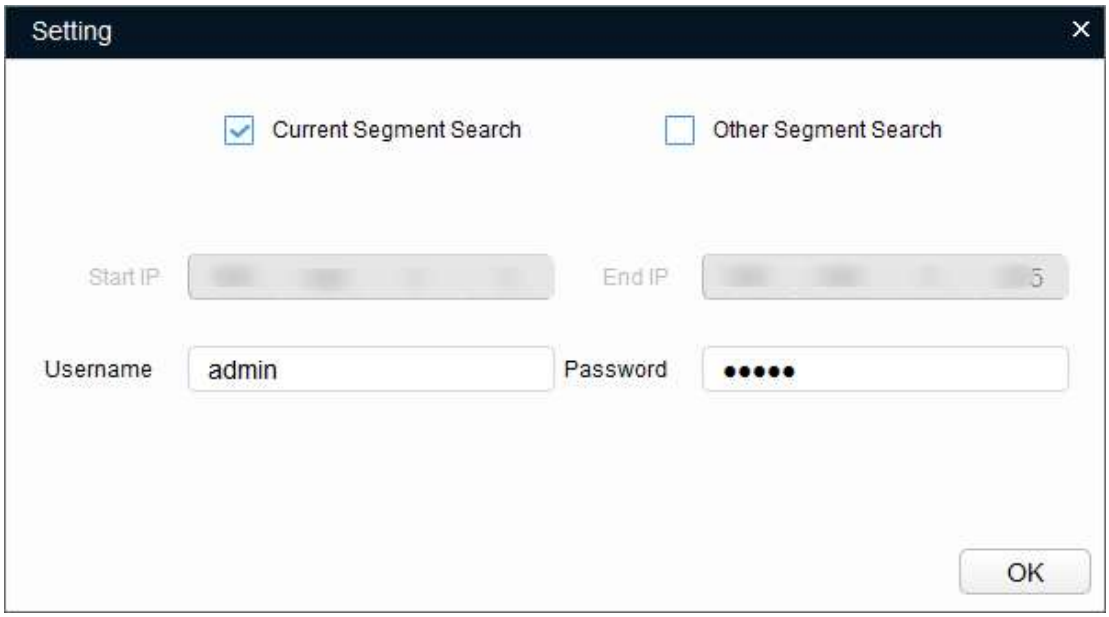
Înainte de inițializare, asigurați-vă că controlerul și computerul sunt în aceeași rețea.

Step 1 Căutați controlerul 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 pe OK.

3) Selectați controlerul neinițializat, apoi faceți clic pe Inițializare.

Figure 4-1 Căutați dispozitivul



Step 2 Selectați controlerul neinițializat, apoi faceți clic**Inițializați.** Clic

Step 3 **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 în funcție de nevoile dvs. reale.

Asigurați-vă că dispozitivul și computerul pe care este instalat ConfigTool sunt conectate; altfel cel instrumentul nu poate găsi dispozitivul.

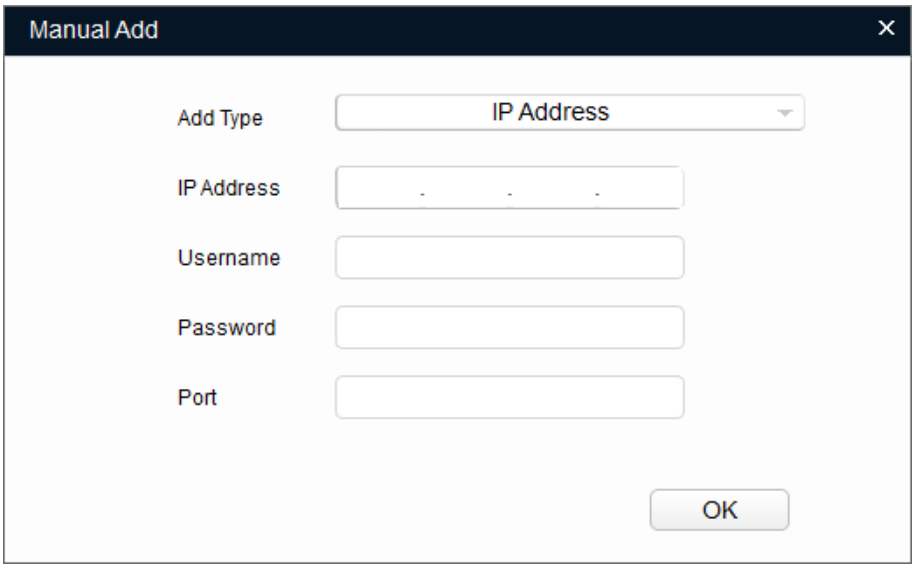
4.2.1 Adăugarea dispozitivului individual

Step 1 Clic .

Step 2 Clic**Adăugați manual**.

Step 3 Selectați**Adresa IP**din**Adăugați tip**.

Figure 4-2 Adăugarea manuală (adresă IP)



Step 4 Setați parametrii controlerului.

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.
	Nume de utilizator	Numele de utilizator și parola pentru autentificarea dispozitivului.
	Parola	
	Port	Numărul portului dispozitivului.

Step 5 Clic**Bine**.

Dispozitivul nou adăugat este afișat în lista de dispozitive.

4.2.2 Adăugarea de dispozitive în loturi

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

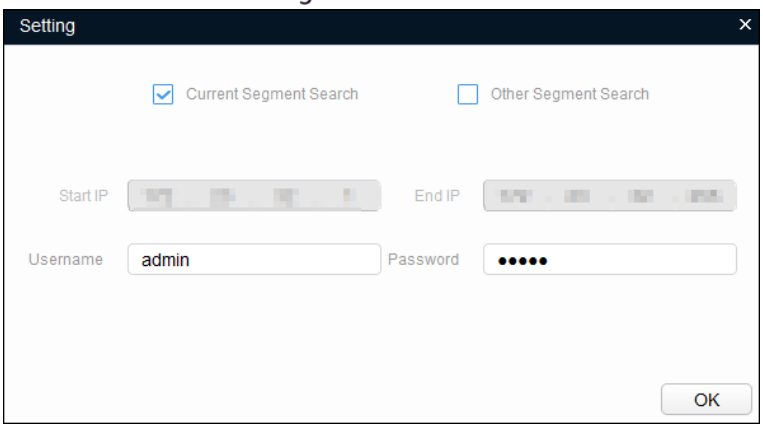
4.2.2.1 Adăugarea prin căutare

Puteți adăuga mai multe dispozitive prin căutarea segmentului curent sau a altor segmente.

Puteți seta condițiile de filtrare pentru a căuta rapid dispozitivul dorit.

Step 1 Clic Search setting.

Figure 4-3 Setare



Step 2 Selectați modalitatea de căutare. Ambele următoarele două moduri sunt selectate implicit.

- Căutați segmentul curent

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

- Căutați 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 începe căutarea dispozitivelor.

Dispozitivele căutate vor fi afișate în lista de dispozitive.

- Clic pentru a reîmprospăta lista de dispozitive.
- Sistemul salvează condițiile de căutare la ieșirea din software și reutiliza 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.

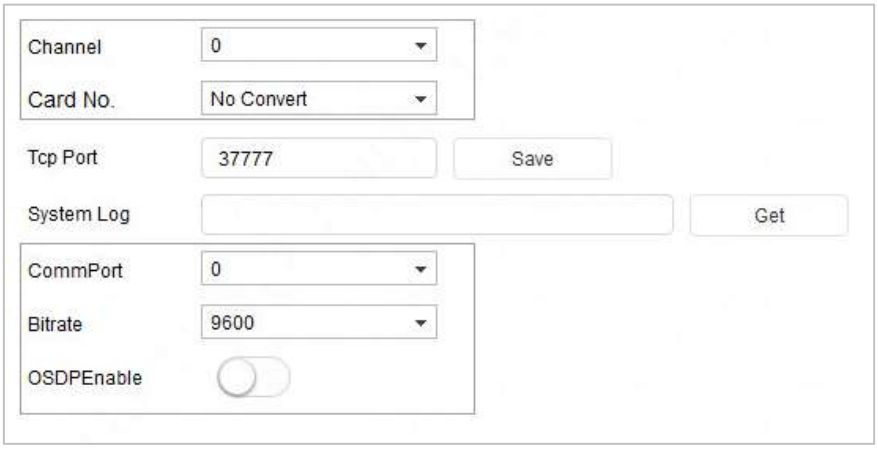
Step 1 Clic pe meniul principal.

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 4-4 Configurați controlerul de acces



Tabelul 4-2 Parametrii controlerului de acces

Parametru
Canal
Card Nr.
Port TCP

Parametru
SysLog
CommPort
Rata de biți
Activare OSDP

Step 5 (Opțional) Faceți clic**Aplica pentru**, selectați dispozitivele cu care aveți nevoie pentru a sincroniza parametrii configurați, apoi faceți clic**Config**.

Dacă a reușit, este afișat în partea dreaptă a dispozitivului; dacă nu a reușit, puteți face clic pe este afisat. Tu pictogramă pentru a vizualiza informații detaliate.

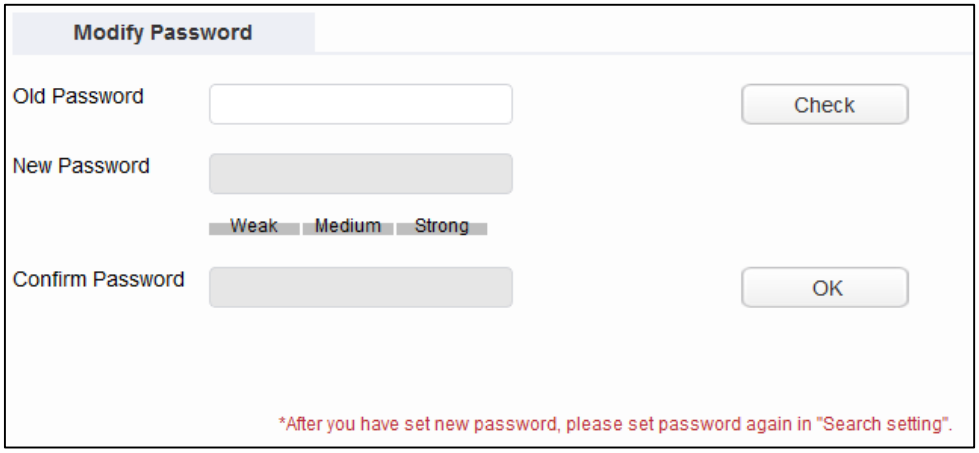
4.4 Schimbarea parolei dispozitivului

Puteți modifica parola de conectare a dispozitivului.

Step 1 Clic pe bara de meniu.

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

Figure 4-5 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 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 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.