Controller de acces seria DS-K2800

Manual de utilizare

Manual de utilizare

 Acest manual este aplicat pentru controlerul de acces.

numele produsului	Seriale
Acces Controlor	Controller de acces seriale DS-K2801
	Controller de acces seriale DS-K2802
	Controller de acces seriale DS-K2804

Include instrucțiuni despre cum să utilizați produsul. Software-ul încorporat în Produs este guvernat de acordul de licență de utilizare care acoperă produsul respectiv.

Despre acest manual

Acest manual este supus protecției drepturilor de autor naționale și internaționale. Hangzhou Hikvision Digital Technology Co., Ltd. („Hikvision") își rezervă toate drepturile asupra acestui manual. Acest manual nu poate fi reprodus, modificat, tradus sau distribuit, parțial sau integral, prin niciun mijloc, fără permisiunea prealabilă scrisă a Hikvision.

Mărci comerciale

HIKVISION și alte mărci Hikvision sunt proprietatea Hikvision și sunt mărci comerciale înregistrate sau subiectul cererilor pentru aceasta de către Hikvision și/sau afiliații săi. Alte mărci comerciale menționate în acest manual sunt proprietățile deținătorilor respectivi. Nu se acordă niciun drept de licență pentru utilizarea unor astfel de mărci comerciale fără permisiunea expresă.

Disclaimer

ÎN MĂSURA MAXIMĂ PERMISĂ DE LEGEA APLICABILĂ, HIKVISION NU OFERĂ GARANȚII, EXPRESE SAU IMPLICITE, INCLUSIV, FĂRĂ LIMITAȚII, GARANȚII IMPLICITE DE VANTABILITATE ȘI ADECVENȚĂ PENTRU UN ANUMIT SCOP, CU PRIVIRE LA ACEST MANUAL. HIKVISION NU GARANTĂ, NU GARANTĂ SAU FACE NICIO DECLARAȚII CU PRIVIRE LA UTILIZAREA MANUALULUI SAU CORECTEȚIA, ACURATEȚIA SAU FIABILITATEA INFORMAȚIILOR CONȚINUTE ÎN ACEST. UTILIZAREA ACESTUI MANUAL DE CĂTRE DVS. ȘI ORICE BAZAREA ÎN ACEST MANUAL VOR FI ÎN TOTALITATE PE PROPRIUL RISC ȘI RESPONSABILITATEA DVS.

CU PRIVIRE LA PRODUSUL CU ACCES LA INTERNET, UTILIZAREA PRODUSULUI VA FI PE PROPRIUL RISCURI. COMPANIA NOASTRA NU VA ASUMA NICIO RESPONSABILITATE PENTRU OPERAREA ANORMALA, SCURTEA DE CONFIDENTIALITATE SAU ALTE DAUNE REZULTATE DIN ATAC CIBERNICE, ATAC DE HACKER, INSPECȚIA DE VIRUS SAU ALTE RISCURI DE SECURITATE A INTERNETULUI; CU toate acestea, COMPANIA NOASTRA VA FURNIZA SISTEMUL TEHNIC LA TEMPORALITATE DACĂ ESTE NECESAR.

LEGILE DE SUPRAVEGHERE VIERĂ ÎN JURISDICȚIE. VĂ RUGĂM SĂ VERIFICAȚI TOATE LEGILE RELEVANTE DIN JURISDICȚIA DVS. ÎNAINTE DE A UTILIZA ACEST PRODUS PENTRU A GARGI CĂ UTILIZAREA DVS. CONFORMĂ LEGEA APLICABĂ. COMPANIA NOASTRĂ NU VA FI RESPONSABILĂ ÎN CAZUL CĂ ACEST PRODUS ESTE UTILIZAT ÎN SCOPURI ILEGITIME.

ÎN CAZUL ORICE CONFLICTE ÎNTRE ACEST MANUAL ȘI LEGEA APLICABILĂ, PREVALEAZA TERZIUA.

A sustine

Dacă aveți întrebări, vă rugăm să nu ezitați să contactați dealerul local.

Informații de reglementare

Informații FCC

Vă rugăm să rețineți că modificările sau modificările care nu sunt aprobate în mod expres de partea responsabilă pentru conformitate ar putea anula autoritatea utilizatorului de a utiliza echipamentul.

Conformitate FCC: Acest echipament a fost testat și s-a dovedit că respectă limitele pentru un dispozitiv digital de clasă B, în conformitate cu partea 15 din Regulile FCC. Aceste limite sunt concepute pentru a oferi o protecție rezonabilă împotriva interferențelor dăunătoare într-o instalație rezidențială. Acest echipament generează, utilizează și poate radia energie de frecvență radio și, dacă nu este instalat și utilizat în conformitate cu instrucțiunile, poate provoca interferențe dăunătoare comunicațiilor radio. Cu toate acestea, nu există nicio garanție că interferențele nu vor apărea într-o anumită instalație. Dacă acest echipament provoacă interferențe dăunătoare recepției radio sau televiziunii, ceea ce poate fi determinat prin oprirea și pornirea echipamentului, utilizatorul este încurajat să încerce să corecteze interferența prin una sau mai multe dintre următoarele măsuri:

— Reorientați sau mutați antena de recepție.
— Măriți distanța dintre echipament și receptor.
— Conectați echipamentul la o priză de pe un circuit diferit de cel la care este conectat receptorul.
— Consultați distribuitorul sau un tehnician radio/TV cu experiență pentru ajutor.

Condiții FCC

Acest dispozitiv respectă partea 15 din Regulile FCC. Funcționarea este supusă următoarelor două condiții:

1. Acest dispozitiv nu poate cauza interferențe dăunătoare.
2. Acest dispozitiv trebuie să accepte orice interferență primită, inclusiv interferențe care pot cauza o funcționare nedorită.

Declarație de conformitate UE

CE Acest produs și, dacă este cazul, accesoriile furnizate sunt marcate cu „CE” și, prin urmare, respectă standardele europene armonizate aplicabile enumerate în Directiva R&TTE 1999/5/EC, Directiva EMC 2014/30/UE, Directiva LVD 2014 /35/UE, Directiva RoHS 2011/65/UE.

2012/19/UE (directiva DEEE): Produsele marcate cu acest simbol nu pot fi aruncate ca deșeuri municipale nesortate în Uniunea Europeană. Pentru o reciclare adecvată, returnați acest produs furnizorului local la achiziționarea unui echipament nou echivalent sau aruncați-l la punctele de colectare desemnate. Pentru mai multe informații, consultați: www.recyclethis.info.

2006/66/EC (directiva privind bateriile): Acest produs conține o baterie care nu poate fi aruncată ca deșeuri municipale nesortate în Uniunea Europeană. Consultați documentația produsului pentru informații specifice despre baterie. Bateria este marcată cu acest simbol, care poate include litere pentru a indica cadmiul (Cd), plumbul (Pb) sau mercurul (Hg). Pentru o reciclare adecvată, returnați bateria furnizorului dumneavoastră sau la un punct de colectare desemnat. Pentru mai multe informații vezi: www.recyclethis.info.

Conformitate Industry Canada ICES-003

Acest dispozitiv îndeplinește cerințele standardelor CAN ICES-3 (A)/NMB-3(A).

Sfaturi preventive și de precauție

Înainte de a conecta și de a utiliza dispozitivul, vă rugăm să fiți informat cu privire la următoarele sfaturi:

- Asigurați-vă că unitatea este instalată într-un mediu bine ventilat, fără praf.
- Țineți toate lichidele departe de dispozitiv.
- Asigurați-vă că condițiile de mediu îndeplinesc specificațiile din fabrică.
- Asigurați-vă că unitatea este fixată corect pe un suport sau pe un raft. Șocuri sau șocuri majore ale unității ca urmare a căderii acesteia pot cauza deteriorarea componentelor electronice sensibile din unitate.
- Utilizați dispozitivul împreună cu un UPS, dacă este posibil.
- Opriți unitatea înainte de a conecta și deconecta accesoriile și perifericele.
- Pentru acest dispozitiv trebuie utilizat un HDD recomandat din fabrică.

Utilizarea necorespunzătoare sau înlocuirea bateriei poate duce la pericol de explozie. Înlocuiți numai cu același tip sau echivalent. Aruncați bateriile uzate conform instrucțiunilor furnizate de producător.

Instrucțiuni de siguranță

Aceste instrucțiuni au scopul de a se asigura că utilizatorul poate folosi produsul corect pentru a evita pericolul sau pierderea proprietății.

Măsura de precauție se împarte în**Avertizări**și**Atenționări**: **Avertizări:**Neglijarea oricăruia dintre avertismente poate provoca vătămări grave sau deces. **Atenționări:**Neglijarea oricăreia dintre precauții poate cauza răniri sau deteriorarea echipamentului.

Avertizări Urmați acestea garanții a preveni vătămare gravă sau deces.	**Atenționări** Urma aceste măsuri de precauție pentru a preveni eventualele răni sau daune materiale.

Avertizări

-Toate operațiunile electronice trebuie să respecte strict reglementările de siguranță electrică, reglementările de prevenire a incendiilor și alte reglementări conexe din regiunea dumneavoastră locală.

-Vă rugăm să utilizați adaptorul de alimentare, care este furnizat de o companie obișnuită. Consumul de energie nu poate fi mai mic decât valoarea cerută.

-Nu conectați mai multe dispozitive la un adaptor de alimentare deoarece supraîncărcarea adaptorului poate cauza supraîncălzire sau pericol de incendiu.

-Vă rugăm să vă asigurați că alimentarea a fost deconectată înainte de a conecta, instala sau demonta dispozitivul.

-Când produsul este instalat pe perete sau tavan, dispozitivul trebuie să fie bine fixat.

-Dacă din dispozitiv se ridică fum, mirosuri sau zgomot, opriți imediat alimentarea și deconectați cablul de alimentare, apoi contactați centrul de service.

-Dacă produsul nu funcționează corect, vă rugăm să contactați dealerul sau cel mai apropiat centru de service. Nu încercați niciodată să dezasamblați singur dispozitivul. (Nu ne asumăm nicio responsabilitate pentru problemele cauzate de reparații sau întreținere neautorizate.)

Atenționări

-Nu scăpați dispozitivul și nu îl supuneți la șocuri fizice și nu îl expuneți la radiații cu electromagnetism ridicat. Evitați instalarea echipamentului pe suprafețe cu vibrații sau locuri supuse șocurilor (necunoașterea poate cauza deteriorarea echipamentului).

-Nu așezați dispozitivul în locuri extrem de fierbinți (consultați specificațiile dispozitivului pentru temperatura de funcționare detaliată), reci, prăfuite sau umede și nu îl expuneți la radiații electromagnetice ridicate. Temperatura de funcționare adecvată este 0℃la +45℃,iar temperatura de depozitare ar trebui să fie -10℃la +55℃.

-Capacul dispozitivului pentru utilizare în interior trebuie ferit de ploaie și umezeală.

-Expunerea echipamentului la lumina directă a soarelui, ventilație scăzută sau surse de căldură, cum ar fi încălzitorul sau radiatorul este interzisă (necunoașterea poate cauza pericol de incendiu).

-Nu îndreptați dispozitivul spre soare sau spre locuri foarte luminoase. În caz contrar, poate apărea o înflorire sau o pete (ceea ce nu este însă o defecțiune) și afectând în același timp rezistența senzorului.

-Vă rugăm să folosiți mănușa furnizată când deschideți capacul dispozitivului, evitați contactul direct cu capacul dispozitivului, deoarece transpirația acidă a degetelor poate eroda suprafața capacului dispozitivului.

-Vă rugăm să utilizați o cârpă moale și uscată când curățați suprafețele interioare și exterioare ale capacului dispozitivului, nu folosiți detergenți alcalini.

-Vă rugăm să păstrați toate ambalajele după ce le despachetați pentru utilizare ulterioară. În cazul în care a apărut orice defecțiune, trebuie să returnați dispozitivul la fabrică cu ambalajul original. Transportul fără ambalajul original poate duce la deteriorarea dispozitivului și la costuri suplimentare.

-Utilizarea necorespunzătoare sau înlocuirea bateriei poate duce la pericol de explozie. Înlocuiți numai cu același tip sau echivalent. Aruncați bateriile uzate conform instrucțiunilor furnizate de producătorul bateriilor.

Cuprins

Capitolul 1 Descrierea produsului

1.1 Prezentare generală

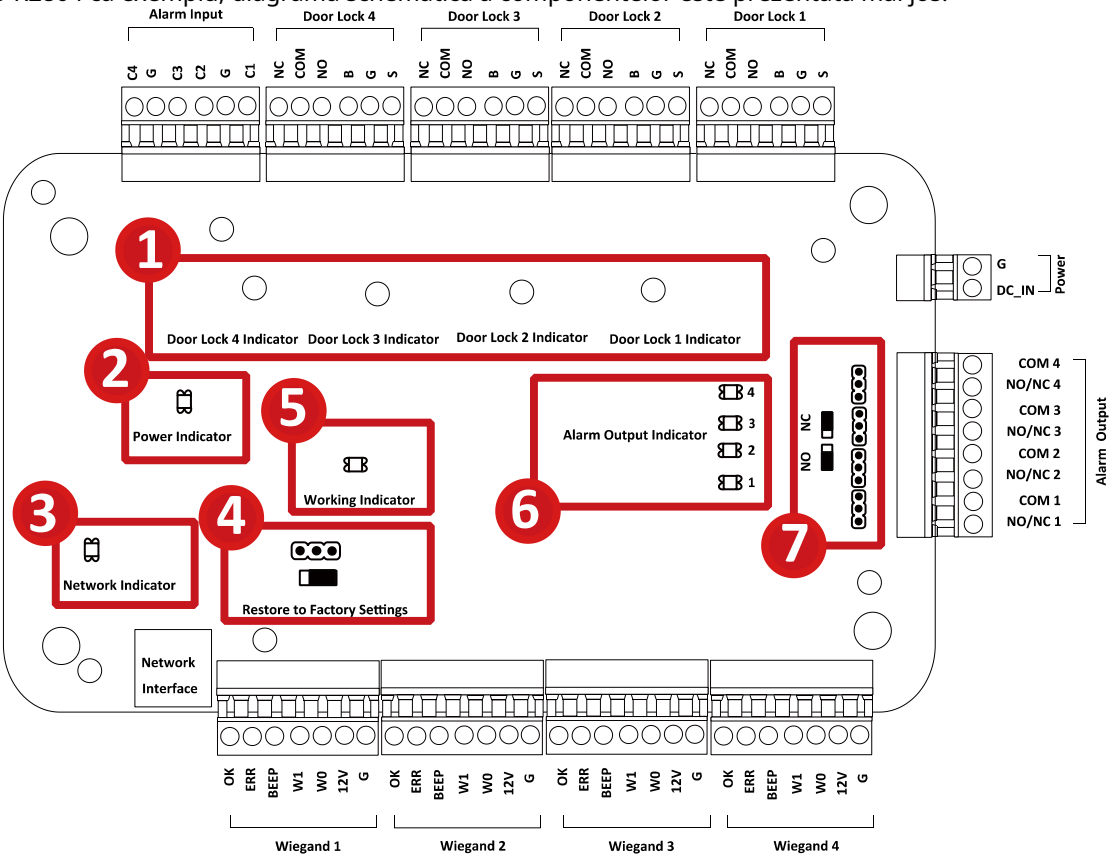
DS-K2800 este un controler de acces puternic și stabil, folosind arhitectura logică. DS-K2800 este proiectat cu interfață de rețea TCP/IP și semnalul său este procesat cu criptare specială și poate fi rulat offline. Este acceptată și funcția anti-alterare.

1.2 Caracteristici principale

- Controlerul de acces este echipat cu procesor de mare viteză pe 32 de biți
- Suporta comunicatii de retea TCP/IP, cu interfata de retea auto-adaptabila. Datele de comunicare sunt criptate special pentru a ameliora preocuparea privind scurgerile de confidențialitate.
- Acceptă recunoașterea și stocarea numărului de card cu lungimea maximă de 20
- Controlerul de acces poate stoca 10 mii de carduri legale și 50 de mii de înregistrări de glisare a cardului.
- Acceptă funcția de deschidere a primului card și funcția de autorizare a primului card, funcție super card și super parolă, funcție de upgrade online și control de la distanță al ușilor
- Suportă interfața Wiegand pentru accesarea cititorului de carduri. Interfața Wiegand acceptă W26/ W34 și este perfect compatibilă cu cititorul de carduri terță parte cu interfața Wiegand
- Suportă diferite tipuri de carduri, cum ar fi normal/listă blocată/patrulă/oaspeți/constrângere/super card, card pentru deschidere extinsă a ușii etc.
- Acceptă sincronizarea orei prin NTP, metoda manuală sau automată
- Acceptă funcția de stocare a înregistrărilor atunci când este offline și funcția de alarmă de stocare a spațiului de stocare insuficient
- Controlerul de acces are design watchdog
- Datele pot fi salvate permanent după ce controlerul de acces este oprit. Suportă
- conectarea I/O și legătura evenimentelor
- Acceptă alarma pentru evenimente offline care depășesc 90%
- Metode multiple de încărcare a evenimentelor: canal, grup central și ascultare a 500
- de grupuri de cod de autentificare
- Funcție anti-pass-back.

Capitolul 2 Descrierea componentelor

Luați DS-K2804 ca exemplu, diagrama schematică a componentelor este prezentată mai jos.

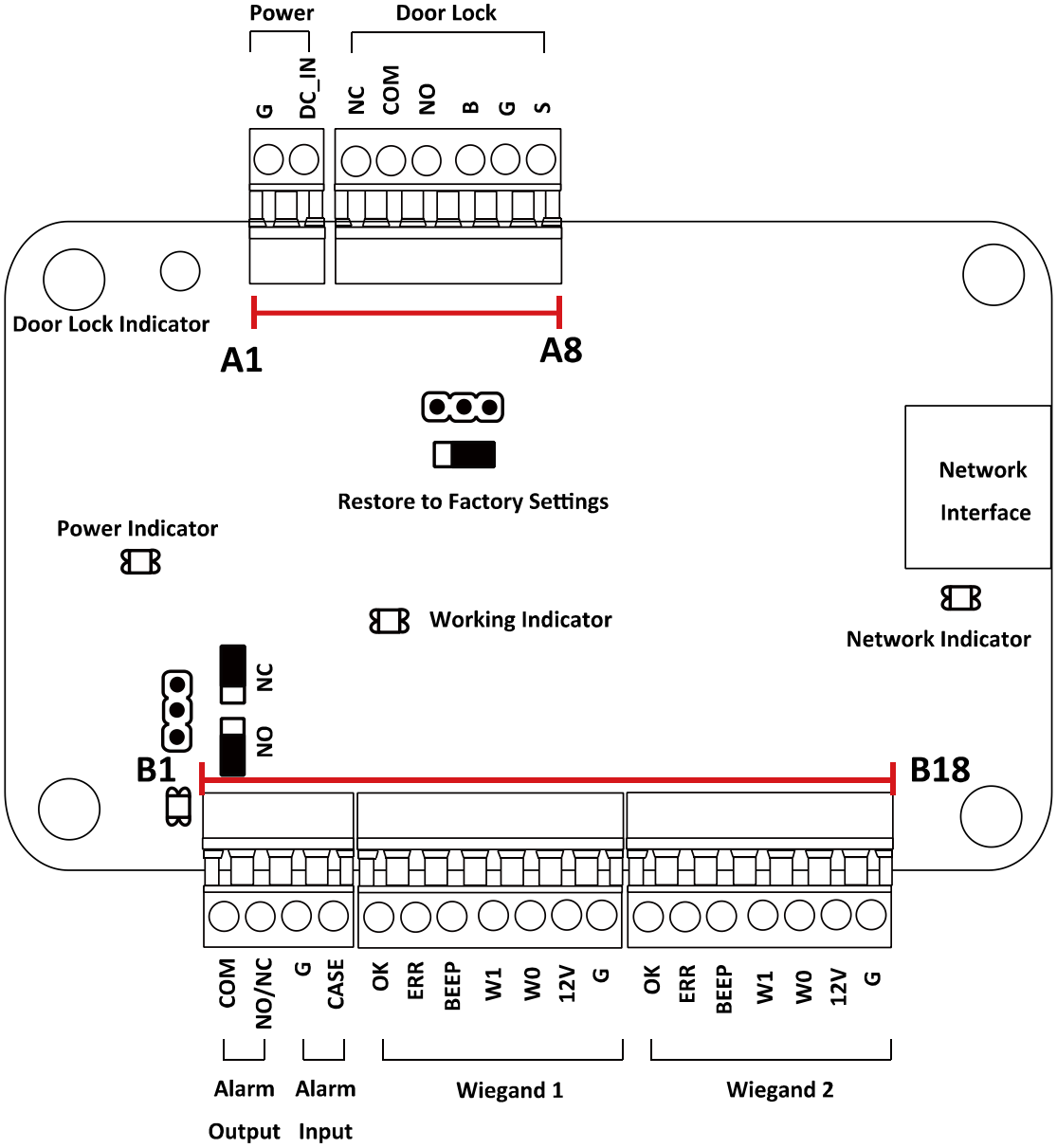


Descrierile componentelor DS-K2800 sunt după cum urmează:

Nu.	Descrierea componentelor		
	DS-K2801	**DS-K2802**	**DS-K2804**
1	Încuietoarea ușii 1 Indicator	Încuietoarea ușii 1/2 Indicator	Încuietoare ușii 1/2/3/4 Indicator
2	Indicator de putere		
3	Indicator de rețea		
4	Capac jumper pentru restabilirea setărilor din fabrică		
5	Indicator de lucru		
6	Indicator de ieșire de alarmă		
7	Capac jumper ieșire alarmă (NO/NC).		

Capitolul 3 Conexiune la terminal

3.1 Descrierea terminalului DS-K2801

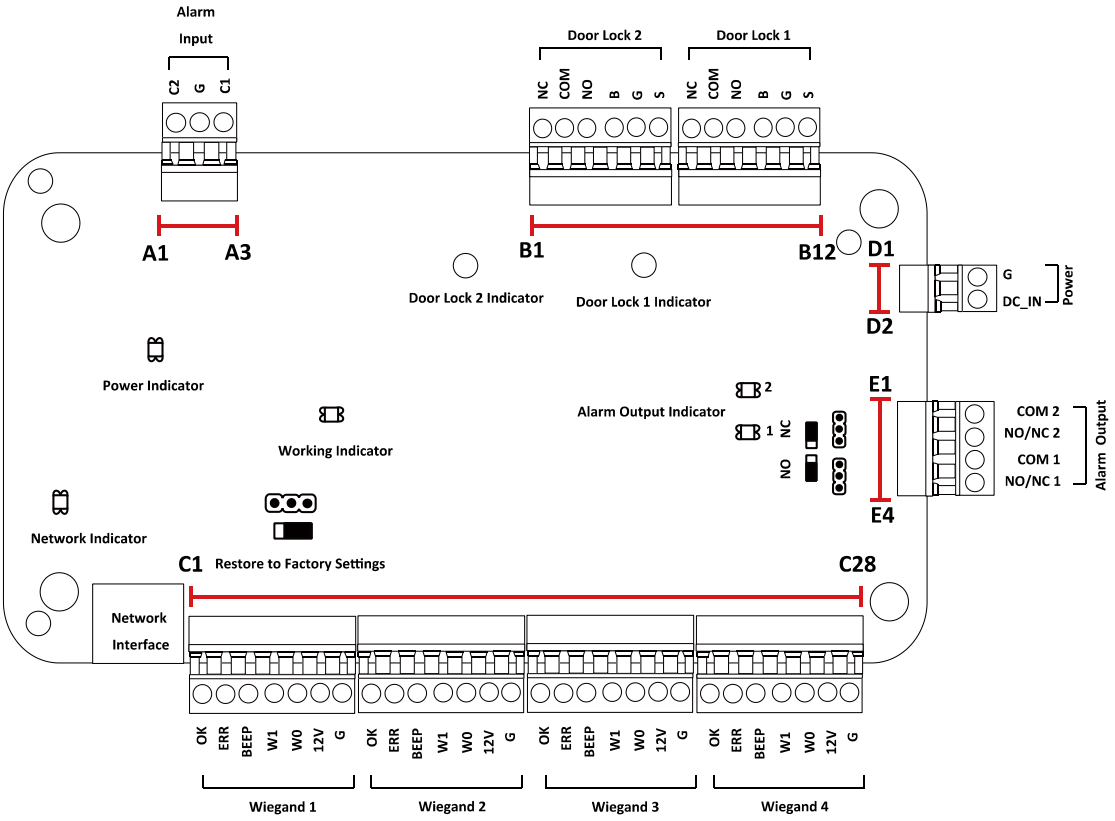


Descrierile terminalelor DS-K2801 sunt după cum urmează:

Nu.	DS-K2801		
A1	Putere	GND	Impământare DC12V
A2		+ 12V	Intrare DC12V
A3	Uşă	NC	Ieșire releu de blocare a ușii
A4		COM	
A5		NU	
A6		BUTON	Intrare buton ușă
A7		GND	Împământare

Nu.	DS-K2801		
A8		SENZOR	Detector magnetic
B1	Ieșire de alarmă	COM	Ieșire releu de alarmă (contact uscat)
B2		NU/NC	
B3	Intrare alarmă	GND	Împământare
B4		ÎN	Intrare eveniment
B5	Cardul Wiegand Cititorul 1	Bine	Indicator de ieșire de control al cititorului de carduri (ieșire validă de card)
B6		ERR	Indicator de ieșire de control a cititorului de carduri (ieșire de card invalidă)
B7		BZ	Ieșire de control a soneriei cititorului de carduri
B8		W1	Capul Wiegand Citiți datele de intrare Date1
B9		W0	Capul Wiegand Citire Date Intrare Date0
B10		PWR	Iesirea alimentarii cititorului de carduri
B11		GND	
B12	Cardul Wiegand Cititorul 2	Bine	Indicator de ieșire de control al cititorului de carduri (ieșire validă de card)
B13		ERR	Indicator de ieșire de control a cititorului de carduri (ieșire de card invalidă)
B14		BZ	Ieșire de control a soneriei cititorului de carduri
B15		W1	Capul Wiegand Citiți datele de intrare Date1
B16		W0	Capul Wiegand Citire Date Intrare Date0
B17		PWR	Iesirea alimentarii cititorului de carduri
B18		GND	

3.2 Descrierea terminalului DS-K2802

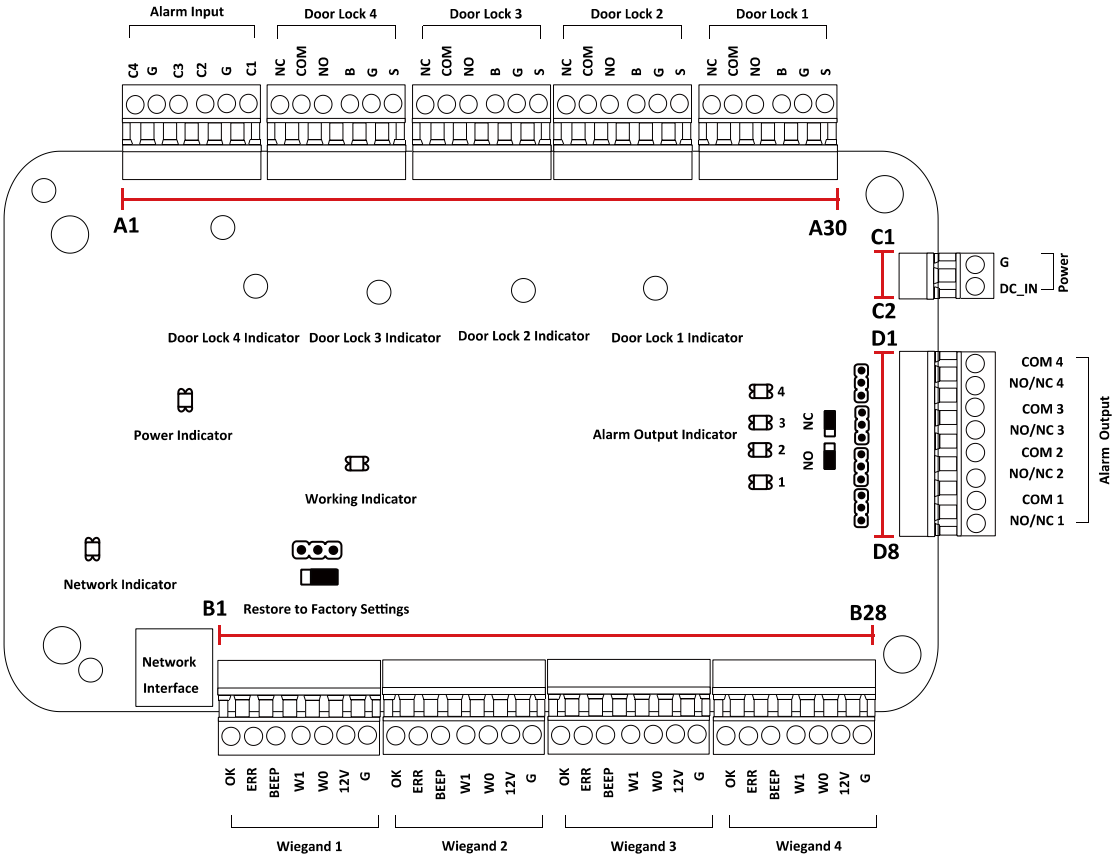


Descrierile terminalelor DS-K2802 sunt după cum urmează:

Nu.	DS-K2802		
A1	Intrare alarmă	IN2	Intrare eveniment 2
A2		GND	Împământare
A3		ÎN 1	Intrare eveniment 1
B1	Ușa 2	NC	Ieșire releu de blocare a ușii (contact uscat)
B2		COM	
B3		NU	
B4		BUTON	Intrare buton ușă
B5		GND	Împământare
B6		SENZOR	Detector magnetic
B7	Ușa 1	NC	Ieșire releu de blocare a ușii (contact uscat)
B8		COM	
B9		NU	
B10		BUTON	Intrare buton ușă
B11		GND	Împământare
B12		SENZOR	Detector magnetic
D1	Putere	GND	Impământare DC12V
D2		+ 12V	Intrare DC12V
E1	Ieșire de alarmă 2	COM2	Ieșire releu de alarmă 2 (contact uscat)
E2		NU/NC2	

Nu.	DS-K2802		
E3	Ieșire de alarmă 1	COM1	Ieșire releu de alarmă 1 (contact uscat)
E4		NU/NC1	
C1	Cardul Wiegand Cititorul 1	Bine	Indicator de ieșire de control al cititorului de carduri (ieșire validă de card)
C2		ERR	Indicator de ieșire de control a cititorului de carduri (ieșire de card invalidă)
C3		BZ	Ieșire de control a soneriei cititorului de carduri
C4		W1	Capul Wiegand Citiți datele de intrare Date1
C5		W0	Capul Wiegand Citire Date Intrare Date0
C6		PWR	Iesirea alimentarii cititorului de carduri
C7		GND	
C8	Cardul Wiegand Cititorul 2	Bine	Indicator de ieșire de control al cititorului de carduri (ieșire validă de card)
C9		ERR	Indicator de ieșire de control a cititorului de carduri (ieșire de card invalidă)
C10		BZ	Ieșire de control a soneriei cititorului de carduri
C11		W1	Capul Wiegand Citiți datele de intrare Date1
C12		W0	Capul Wiegand Citire Date Intrare Date0
C13		PWR	Iesirea alimentarii cititorului de carduri
C14		GND	
C15	Cardul Wiegand Cititorul 3	Bine	Indicator de ieșire de control al cititorului de carduri (ieșire validă de card)
C16		ERR	Indicator de ieșire de control a cititorului de carduri (ieșire de card invalidă)
C17		BZ	Ieșire de control a soneriei cititorului de carduri
C18		W1	Capul Wiegand Citiți datele de intrare Date1
C19		W0	Capul Wiegand Citire Date Intrare Date0
C20		PWR	Iesirea alimentarii cititorului de carduri
C21		GND	
C22	Cardul Wiegand Cititorul 4	Bine	Indicator de ieșire de control al cititorului de carduri (ieșire validă de card)
C23		ERR	Indicator de ieșire de control a cititorului de carduri (ieșire de card invalidă)
C24		BZ	Ieșire de control a soneriei cititorului de carduri
C25		W1	Capul Wiegand Citiți datele de intrare Date1
C26		W0	Capul Wiegand Citire Date Intrare Date0
C27		PWR	Iesirea alimentarii cititorului de carduri
C28		GND	

3.3 Descrierea terminalului DS-K2804



Descrierile terminalelor DS-K2804 sunt după cum urmează:

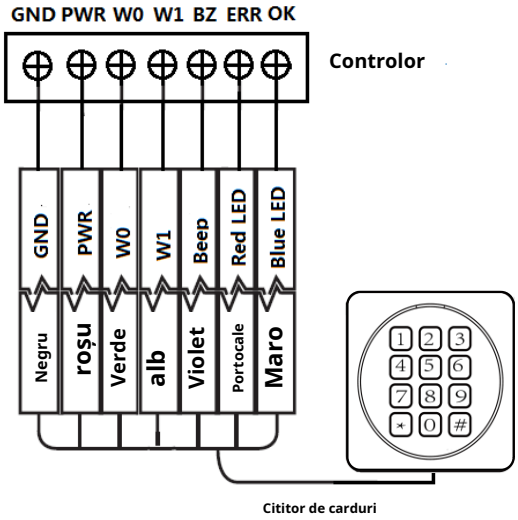
Nu.	DS-K2804		
A1	Intrare alarmă	IN4	Intrare eveniment 4
A2		GND	Împământare
A3		IN3	Intrare eveniment 3
A4		IN2	Intrare eveniment 2
A5		GND	Împământare
A6		ÎN 1	Intrare eveniment 1
A7	Ușa 4	NC	Ieșire releu de blocare a ușii (contact uscat)
A8		COM	
A9		NU	
A10		BUTON	Intrare buton ușă
A11		GND	Împământare
A12		SENZOR	Detector magnetic
A13	Ușa 3	NC	Ieșire releu de blocare a ușii (contact uscat)
A14		COM	
A15		NU	
A16		BUTON	Intrare buton ușă
A17		GND	Împământare
A18		SENZOR	Detector magnetic

Nu.	DS-K2804		
A19	Ușa 2	NC	Ieșire releu de blocare a ușii (contact uscat)
A20		COM	
A21		NU	
A22		BUTON	Intrare buton ușă
A23		GND	Împământare
A24		SENZOR	Detector magnetic
A25	Ușa 1	NC	Ieșire releu de blocare a ușii (contact uscat)
A26		COM	
A27		NU	
A28		BUTON	Intrare buton ușă
A29		GND	Împământare
A30		SENZOR	Detector magnetic
B1	Cardul Wiegand Cititorul 1	Bine	Indicator de ieșire de control al cititorului de carduri (ieșire validă de card)
B2		ERR	Indicator de ieșire de control a cititorului de carduri (ieșire de card invalidă)
B3		BZ	Ieșire de control a soneriei cititorului de carduri
B4		W1	Capul Wiegand Citiți datele de intrare Date1
B5		W0	Capul Wiegand Citire Date Intrare Date0
B6		PWR	Iesirea alimentarii cititorului de carduri
B7		GND	
B8	Cardul Wiegand Cititorul 2	Bine	Indicator de ieșire de control al cititorului de carduri (ieșire validă de card)
B9		ERR	Indicator de ieșire de control a cititorului de carduri (ieșire de card invalidă)
B10		BZ	Ieșire de control a soneriei cititorului de carduri
B11		W1	Capul Wiegand Citiți datele de intrare Date1
B12		W0	Capul Wiegand Citire Date Intrare Date0
B13		PWR	Iesirea alimentarii cititorului de carduri
B14		GND	
B15	Cardul Wiegand Cititorul 3	Bine	Indicator de ieșire de control al cititorului de carduri (ieșire validă de card)
B16		ERR	Indicator de ieșire de control a cititorului de carduri (ieșire de card invalidă)
B17		BZ	Ieșire de control a soneriei cititorului de carduri
B18		W1	Capul Wiegand Citiți datele de intrare Date1
B19		W0	Capul Wiegand Citire Date Intrare Date0
B20		PWR	Iesirea alimentarii cititorului de carduri
B21		GND	
B22	Cardul Wiegand Cititorul 4	Bine	Indicator de ieșire de control al cititorului de carduri (ieșire validă de card)
B23		ERR	Indicator de ieșire de control a cititorului de carduri (ieșire de card invalidă)

Nu.	DS-K2804		
B24		BZ	Ieșire de control a soneriei cititorului de carduri
B25		W1	Capul Wiegand Citiți datele de intrare Date1
B26		W0	Capul Wiegand Citire Date Intrare Date0
B27		PWR	Iesirea alimentarii cititorului de carduri
B28		GND	
C1	Putere	GND	Impământare DC12V
C2		+ 12V	Intrare DC12V
D1	Ieșire de alarmă 4	COM4	Ieșire releu de alarmă 4 (contact uscat)
D2		NU/NC4	
D3	Ieșire de alarmă 3	COM3	Ieșire releu de alarmă 3 (contact uscat)
D4		NU/NC3	
D5	Ieșire de alarmă 2	COM2	Ieșire releu de alarmă 2 (contact uscat)
D6		NU/NC2	
D7	Ieșire de alarmă 1	COM1	Ieșire releu de alarmă 1 (contact uscat)
D8		NU/NC1	

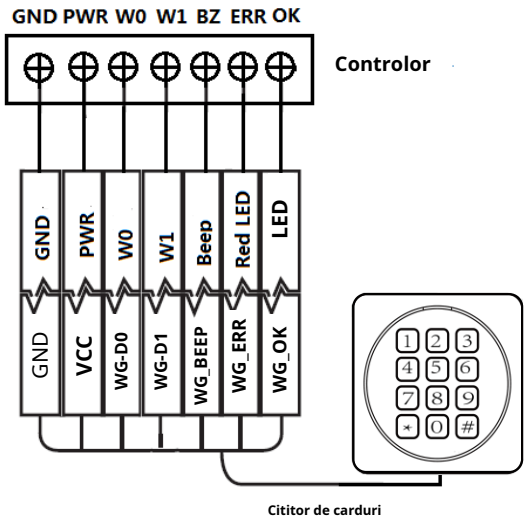
Note:

- Interfața hardware de intrare de alarmă este în mod normal deschisă implicit. Deci este permis doar semnalul normal deschis. Poate fi conectat la soneria cititorului de carduri și controlerului de acces, precum și la ieșirea releului de alarmă și la ieșirea ușii deschise.
- Pentru controlerul de acces cu o singură ușă, cititorul de carduri Wiegand 1 și respectiv 2 corespund cititoarelor de carduri de intrare și de ieșire ale ușii 1. Pentru controlerul de acces cu două uși, cititorul de carduri Wiegand 1 și respectiv 2 corespund cititoarelor de carduri de intrare și de ieșire. al ușii 1, iar cititorul de carduri Wiegand 3 și, respectiv, 4 corespund cititoarelor de carduri de intrare și de ieșire din ușa 2. Pentru controlerul de acces cu patru uși, cititorul de carduri Wiegand 1, 2, 3 și respectiv 4 corespund cititoarelor de carduri de intrare. ale ușii 1, 2, 3 și 4.



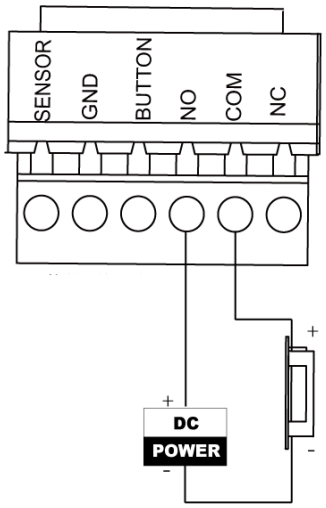
Notă: Trebuie să conectați OK/ERR/BZ, dacă utilizați controlerul de acces pentru a controla LED-ul și buzzer-ul cititorului de carduri Wiegand.

4.1.2 Cablajul cititorului de carduri seria DS-K1800

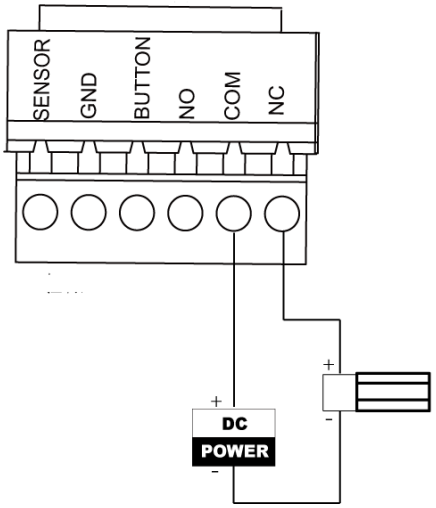


4.2 Terminale externe DS-K2801

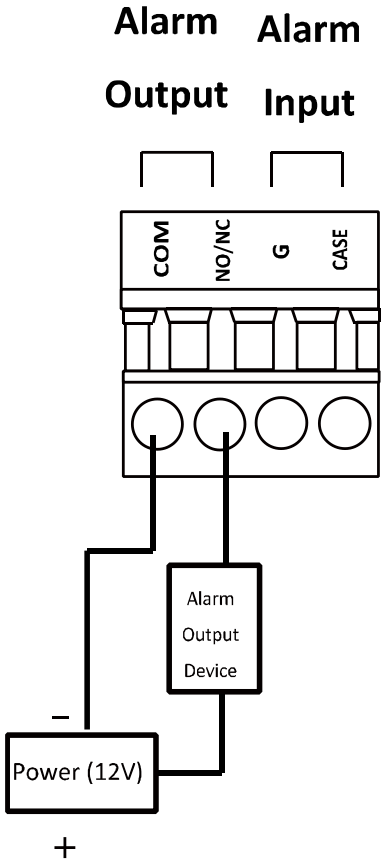
4.2.1 Instalarea blocării catodice



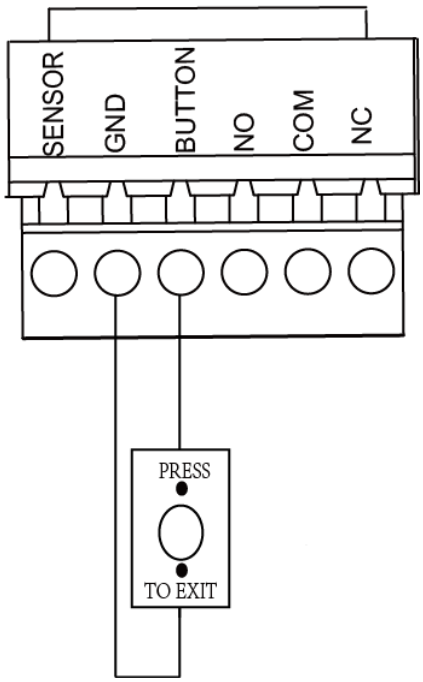
4.2.2 Instalarea blocării anodului



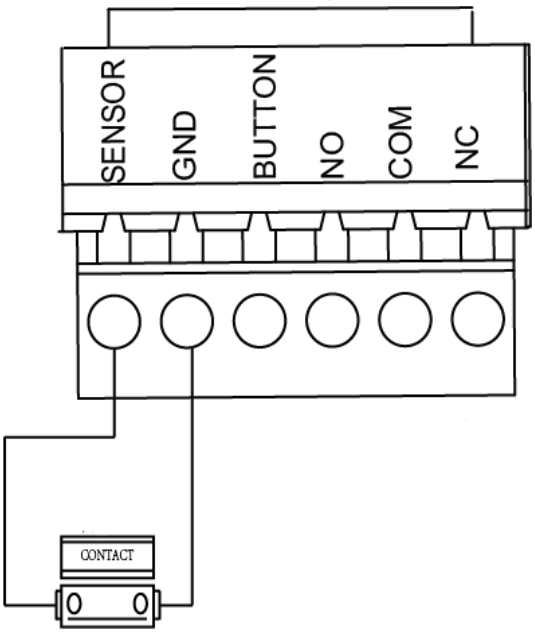
4.3 Conectarea dispozitivului extern de alarmă



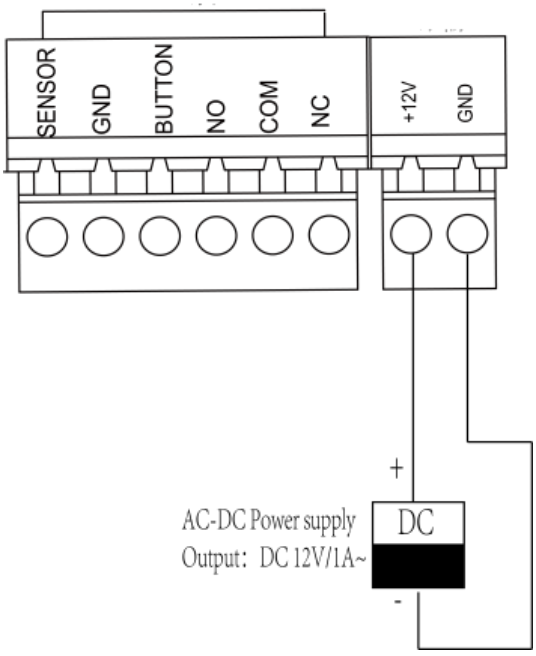
4.4 Schema electrică a butonului ușii



4.5 Conexiunea detectiei magnetice



4.6 Conectarea sursei de alimentare



Capitolul 5 Setări

5.1 Inițializarea hardware-ului

Opțiunea 1:

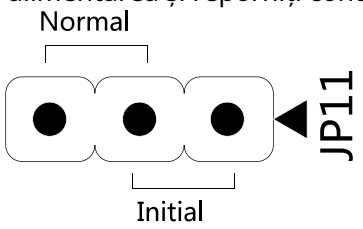
Pași:

1. Scoateți capacul jumperului de la terminalul Normal.
2. Deconectați alimentarea și reporniți controlerul de acces. Buzerul controlerului emite un bip lung.
3. Când semnalul sonor sa oprit, conectați capacul jumperului înapoi la Normal.
4. Deconectați alimentarea și reporniți controlerul de acces.

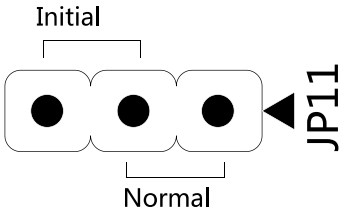
Opțiunea 2:

Pași:

1. Treceți capacul jumperului de la Normal la Inițial.
2. Deconectați alimentarea și reporniți controlerul de acces. Buzerul controlerului emite un bip lung.
3. Când semnalul sonor sa oprit, săriți capacul jumperului înapoi la Normal.
4. Deconectați alimentarea și reporniți controlerul de acces.



DS-K2801 Inițializare Dial-up



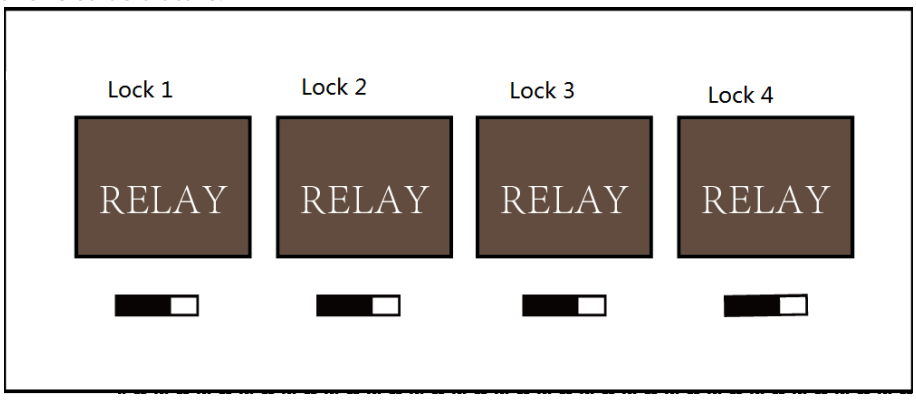
DS-K2802/DS-K2804 Inițializare Dial-up

Notă: Inițializarea hardware-ului va restabili toți parametrii la setarea implicită și toate evenimentele dispozitivului vor fi eliminate.

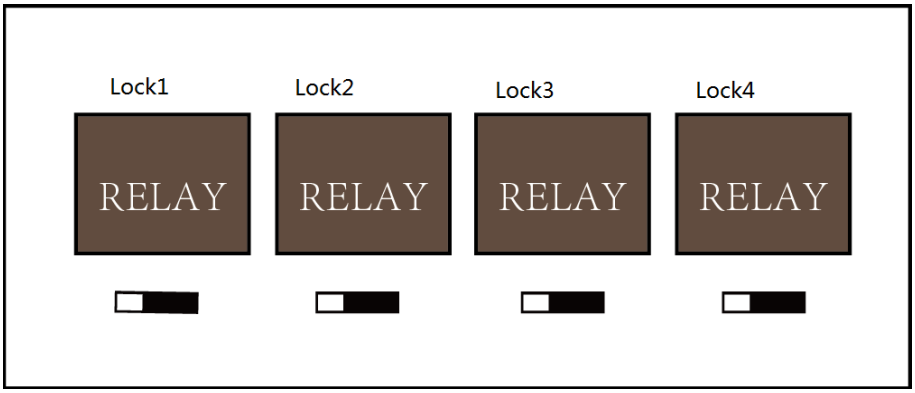
5.2 Intrare releu NO/NC

5.2.1 Blocare ieșire releu

Stare normal deschis releu de blocare:

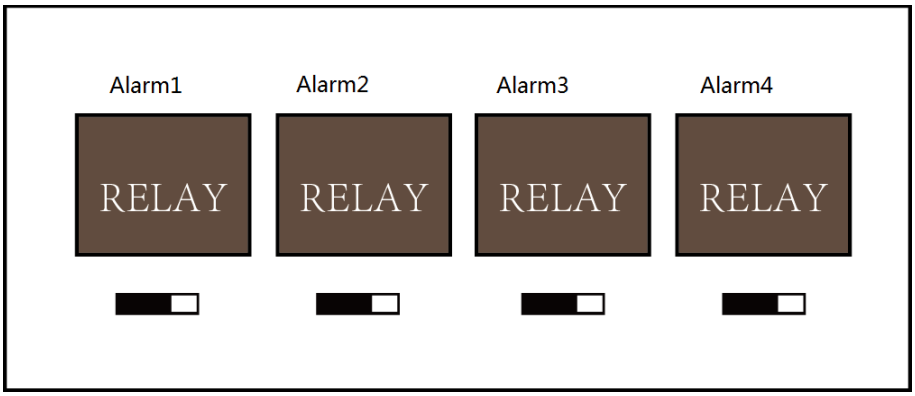


Starea releului de blocare normal închis:

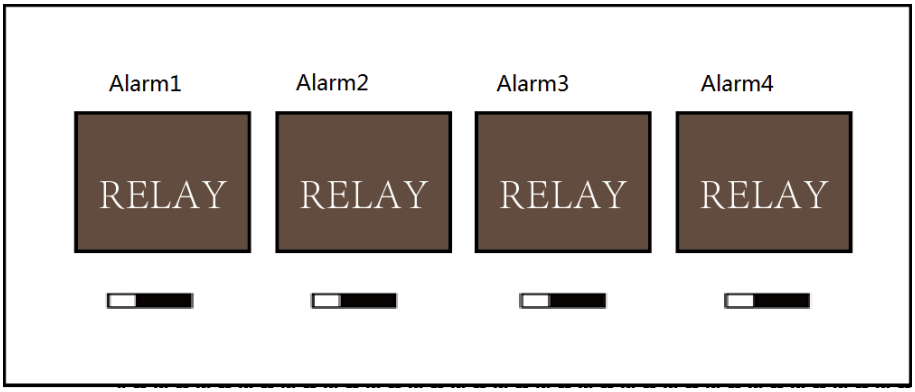


5.2.2 Stare ieșire releu de alarmă

Ieșire releu de alarmă normal deschis:



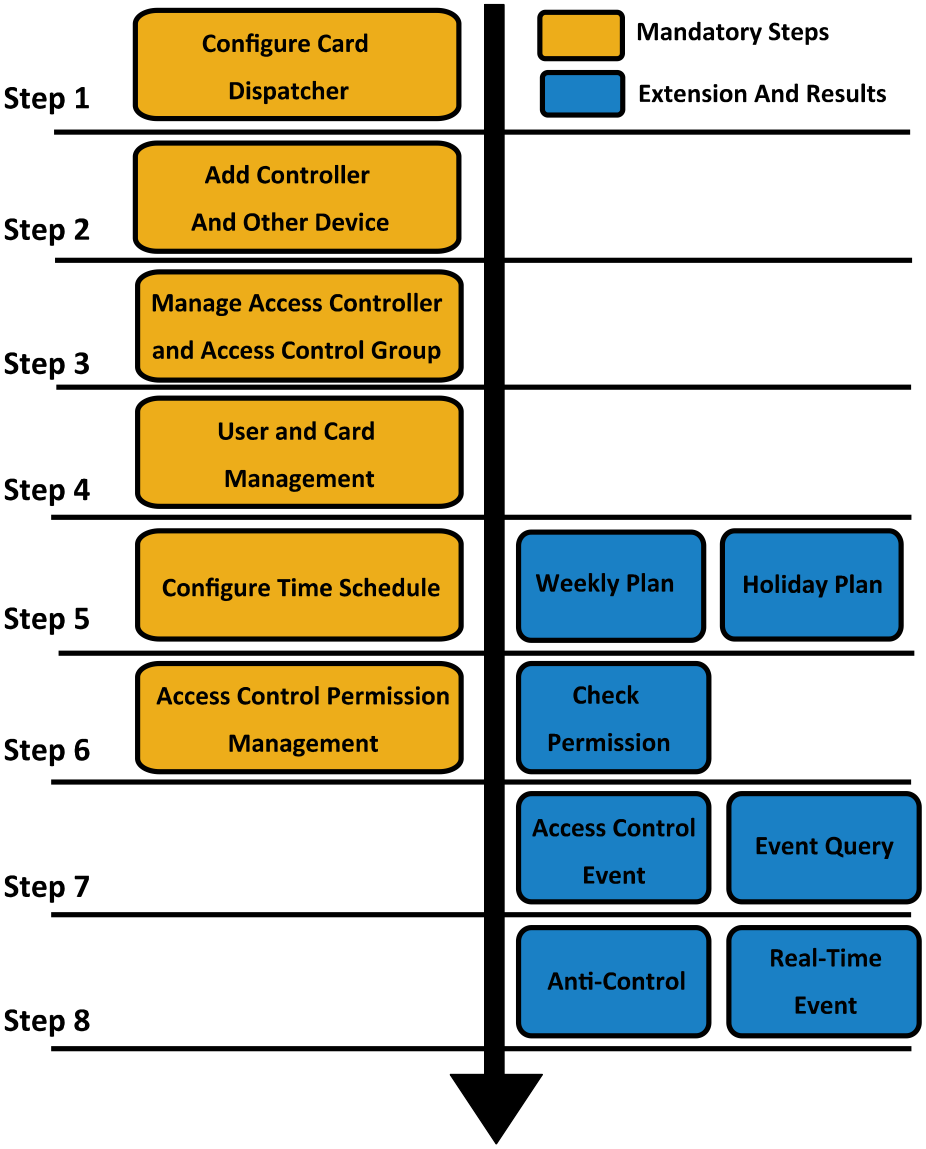
Ieșire releu de alarmă normal închis:



Fluxul de lucru al software-ului

Pentru informații detaliate, consultați manualul de utilizare al software-ului client.

Consultați următorul flux de lucru:


Mandatory Steps
Extension And Results
Step 1
Configure Card Dispatcher
Step 2
Add Controller And Other Device
Step 3
Manage Access Controller and Access Control Group
Step 4
User and Card Management
Step 5
Configure Time Schedule
Weekly Plan
Holiday Plan
Step 6
Access Control Permission Management
Check Permission
Step 7
Access Control Event
Event Query
Step 8
Anti-Control
Real-Time Event

Capitolul 6 Activarea controlului accesului Terminal

Scop:

Vi se cere să activați mai întâi terminalul înainte de a-l folosi. Activarea prin SADP și Activarea prin software-ul client sunt acceptate. Valorile implicite ale terminalului de control sunt următoarele.

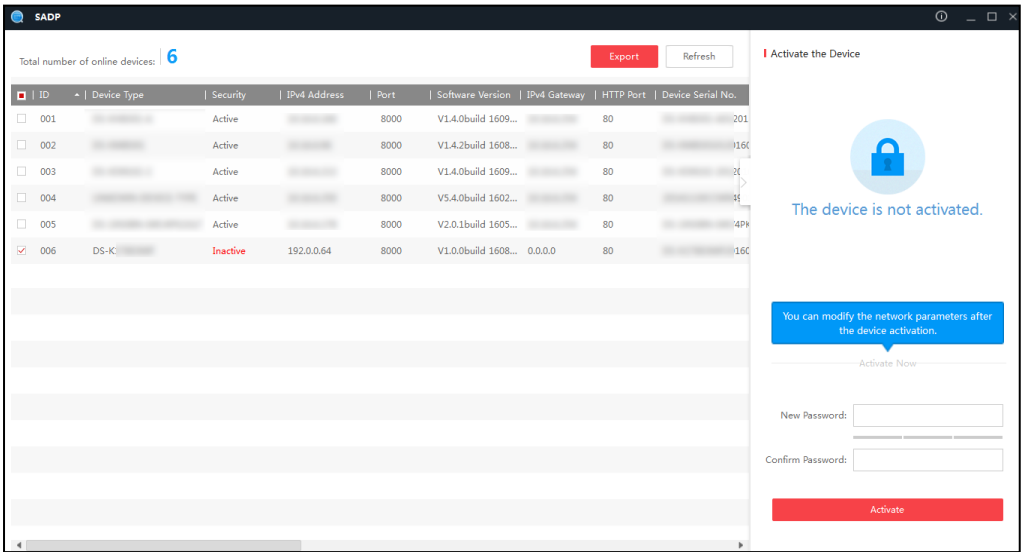
- Adresa IP implicită: 192.0.0.64.
- Portul implicit Nr.: 8000.
- Numele de utilizator implicit: admin.

6.1 Activarea prin intermediul software-ului SADP

Software-ul SADP este utilizat pentru detectarea dispozitivului online, activarea dispozitivului și resetarea parolei.

Obțineți software-ul SADP de pe discul furnizat și instalați SADP conform instrucțiunilor. Urmați pașii pentru a activa panoul de control***. Pași:***

1. Rulați software-ul SADP pentru a căuta dispozitivele online.
2. Verificați starea dispozitivului din lista de dispozitive și selectați un dispozitiv inactiv.

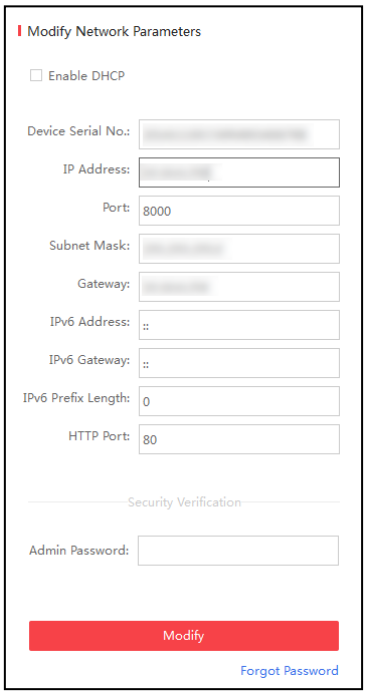


3. Creați o parolă și introduceți parola în câmpul pentru parolă și confirmați parola.

SE RECOMANDĂ PAROLA PUTERNICĂ – *Vă recomandăm să creați o parolă puternică, la alegerea dvs. (folosind minim 8 caractere, inclusiv litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dvs. Și vă recomandăm să vă resetați parola în mod regulat, mai ales în sistemul de înaltă securitate, resetarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.*

4. Faceți clic**Activati**pentru a activa dispozitivul.
5. Verificați dispozitivul activat. Puteți schimba adresa IP a dispozitivului în același segment de rețea cu computerul dvs. fie modificând adresa IP manual, fie bifând caseta de selectare a

Activați DHCP.



6. Introduceți parola și faceți clic pe **Modifica** pentru a activa modificarea adresei IP.

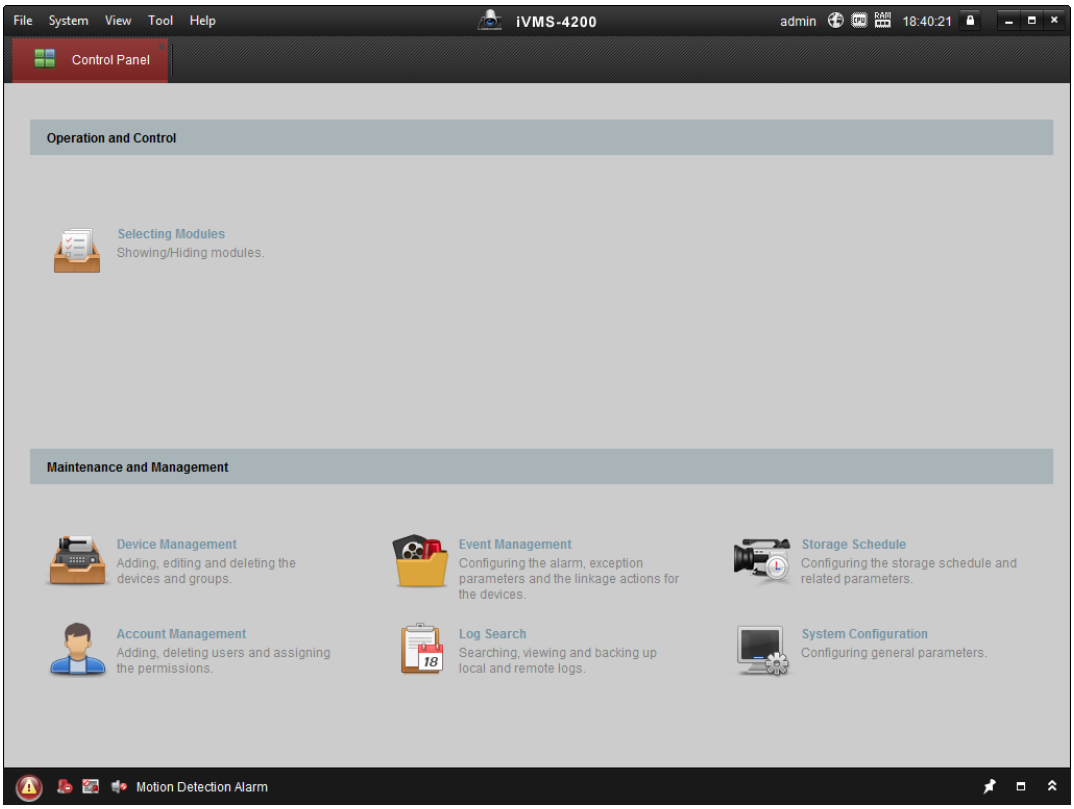
6.2 Activarea prin software-ul client

Software-ul client este un software versatil de gestionare video pentru mai multe tipuri de dispozitive.

Obțineți software-ul client de pe discul furnizat și instalați software-ul conform instrucțiunilor. Urmați pașii pentru a activa panoul de control.

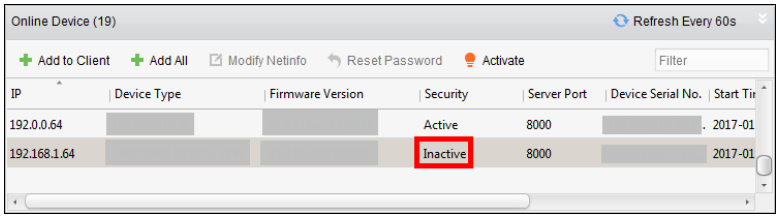
Pași:

1. Rulați software-ul client și va apărea panoul de control al software-ului, așa cum se arată în figura de mai jos.



2. Faceți clic pe **Managementul dispozitivelor** pentru a intra în interfața Device Management.

3. Verificați starea dispozitivului din lista de dispozitive și selectați un dispozitiv inactiv.



4. Faceți clic pe **Activati** pentru a deschide interfața de activare.

5. În fereastra pop-up, creați o parolă în câmpul pentru parolă și confirmați parola.

SE RECOMANDĂ PAROLA PUTERNICĂ – *Vă recomandăm să creați o parolă puternică, la alegerea dvs. (folosind minim 8 caractere, inclusiv litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dvs. Și vă recomandăm să vă resetați parola în mod regulat, mai ales în sistemul de înaltă securitate, resetarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.*

6. Faceți clic OK pentru a începe activarea.

7. Faceți clic pe **Modificați Netinfor** pentru a deschide interfața de modificare a parametrilor de rețea.

8. Schimbați adresa IP a dispozitivului la același segment de rețea cu computerul dvs. fie modificând manual adresa IP.

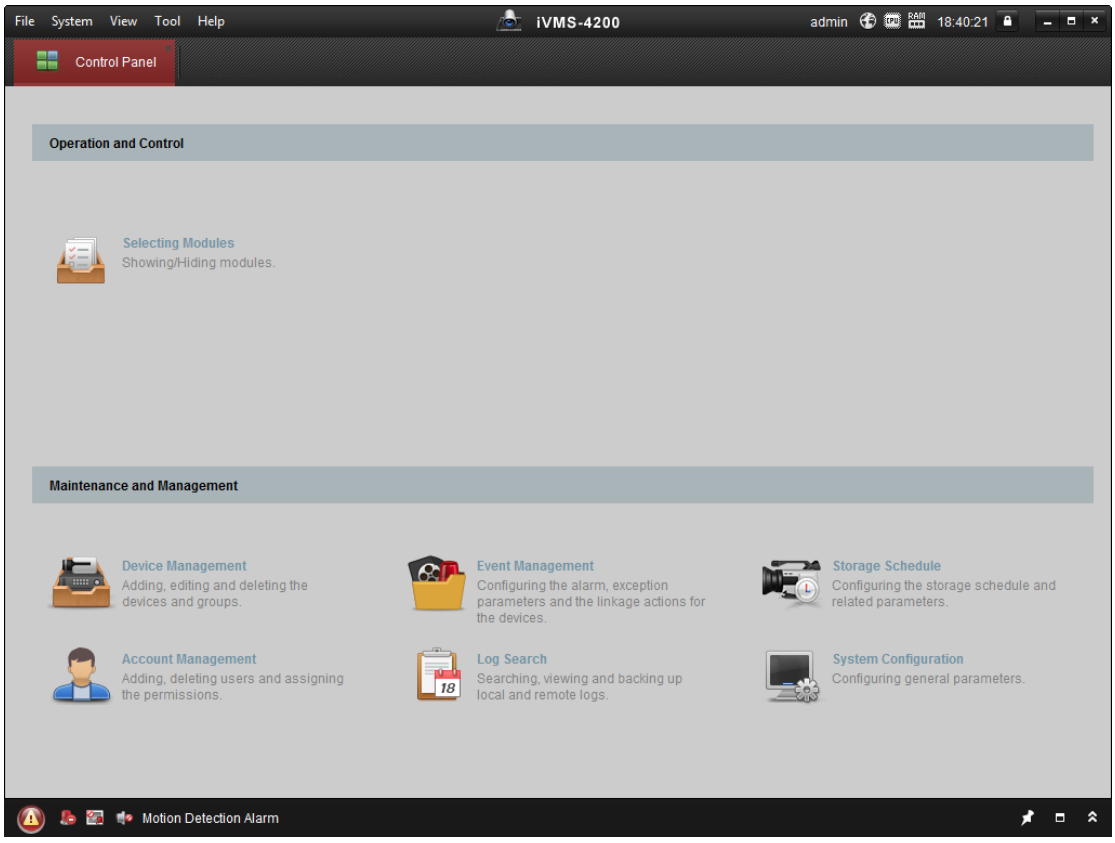
9. Introduceți parola și faceți clic pe OK pentru a salva setările.

Capitolul 7 Operarea clientului

Puteți seta și opera dispozitivele de control al accesului prin intermediul software-ului client. Acest capitol va prezenta operațiunile legate de dispozitivul de control al accesului în software-ul client. Pentru operațiuni integrate, consultați *Manual de utilizare al software-ului client iVMS-4200*.

7.1 Modulul funcțional

Panoul de control al iVMS-4200:

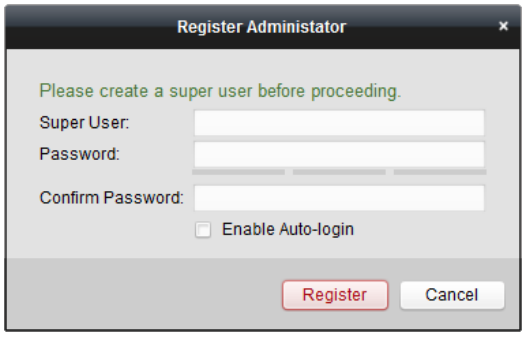


7.2 Înregistrarea și autentificarea utilizatorului

Pentru prima dată pentru a utiliza software-ul client iVMS-4200, trebuie să înregistrați un super utilizator pentru autentificare.

Pași:

1. Introduceți numele super-utilizator și parola. Software-ul va evalua puterea parolei automat și vă recomandăm să utilizați o parolă puternică pentru a vă asigura securitatea datelor.
2. Confirmați parola.
3. Opțional, bifați caseta de selectare **Activați autentificarea automată** pentru a vă conecta automat la software.
4. Faceți clic **Inregistreaza-te**. Apoi, vă puteți conecta la software ca super utilizator.



- *Un nume de utilizator nu poate conține niciunul dintre următoarele caractere: / \ : * ? „ < > |. Iar lungimea parolei nu poate fi mai mică de 6 caractere.*
- *Pentru confidențialitatea dvs., vă recomandăm insistent să schimbați parola cu ceva la alegerea dvs. (folosind minim 8 caractere, inclusiv litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dvs.*
- *Configurarea corectă a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/ sau utilizatorului final.*

Când deschideți iVMS-4200 după înregistrare, vă puteți conecta la software-ul client cu numele de utilizator și parola înregistrate.

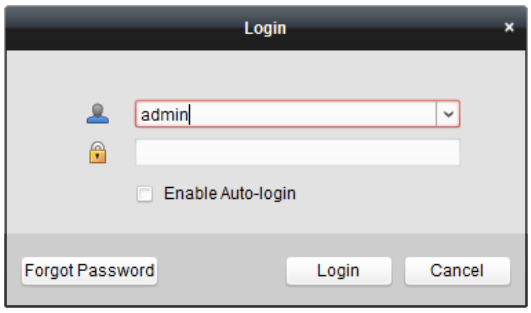
Pași:

1. Introduceți numele de utilizator și parola pe care le-ați înregistrat.

   Notă: Dacă ați uitat parola, vă rugăm să faceți clic **Aţi uitat parola** și amintiți-vă șirul criptat în fereastra pop-up. Contactați-vă dealerul și trimiteți-i șirul criptat pentru a vă reseta parola.

2. Opțional, bifați caseta de selectare **Activați autentificarea automată** pentru a vă conecta automat la software.

3. Faceți clic **Log in**.



După rularea software-ului client, puteți deschide vrăjitorii (inclusiv vrăjitor video, vrăjitor perete video, vrăjitor panou de control de securitate, vrăjitor pentru controlul accesului și interfon video și vrăjitorul de prezență), pentru a vă ghida să adăugați dispozitivul și să efectuați alte setări și operațiuni . Pentru configurarea detaliată despre vrăjitori, consultați *Ghid de pornire rapidă a iVMS-4200*.

7.3 Configurarea sistemului

Scop:

Puteți sincroniza cu client evenimentele de control al accesului ratate.

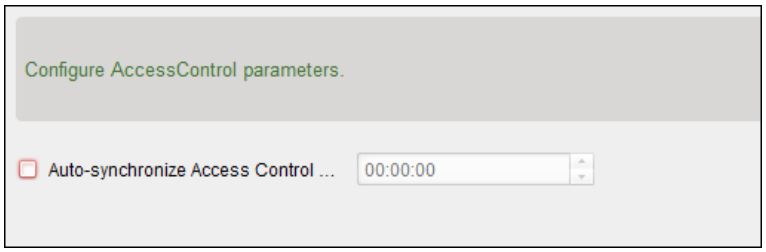
Pași:

1. Faceți clic **Instrument**–**Configurarea sistemului**.

2. În fereastra Configurare sistem, bifați **Sincronizare automată a evenimentului de control al accesului**

3. Setați ora de sincronizare.

Clientul va sincroniza automat evenimentul de control al accesului pierdut cu clientul la ora stabilită.



7.4 Managementul controlului accesului

Scop:

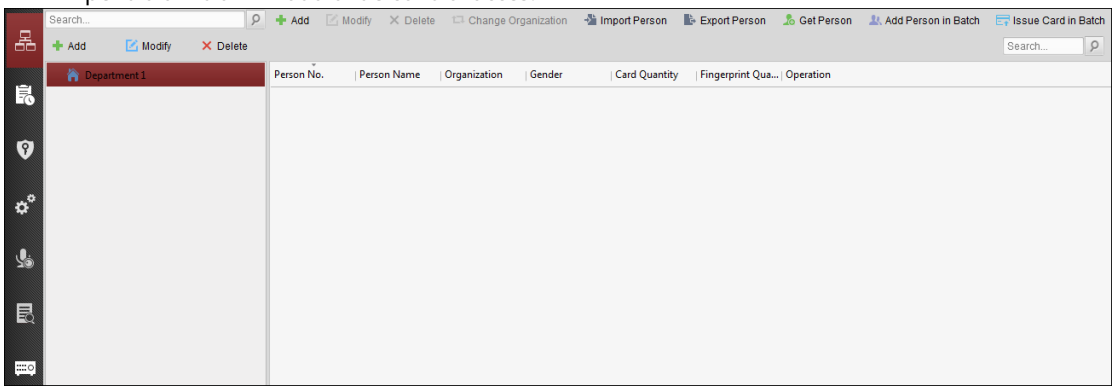
Modulul de control acces este aplicabil dispozitivelor de control acces și interfon video. Acesta oferă mai multe funcționalități, inclusiv gestionarea persoanelor și a cardurilor, configurarea permisiunilor, gestionarea stării controlului accesului, interfon video și alte funcții avansate.

De asemenea, puteți seta configurația evenimentului pentru controlul accesului și puteți afișa punctele și zonele de control al accesului pe E-map.

Notă:Pentru utilizatorul cu permisiuni pentru modulul de control al accesului, utilizatorul poate intra în modulul de control al accesului și poate configura setările de control al accesului.

Clic  în panoul de control și verificați **Controlul accesului** pentru a adăuga modulul de control acces la panou de control.

Clic  pentru a intra în modulul de control acces.



Inainte sa incepi:

Pentru prima dată când deschideți modulul Access Control, va apărea următorul dialog și vi se cere să selectați scena în funcție de nevoile reale.

Puteți selecta scena ca **Non-resedinta** și resedinta.

Note:

- Odată configurată scena, nu o puteți schimba mai târziu.
- Când selectați**Non-reședință**modul, nu puteți configura Regula de prezență atunci când adăugați o persoană.

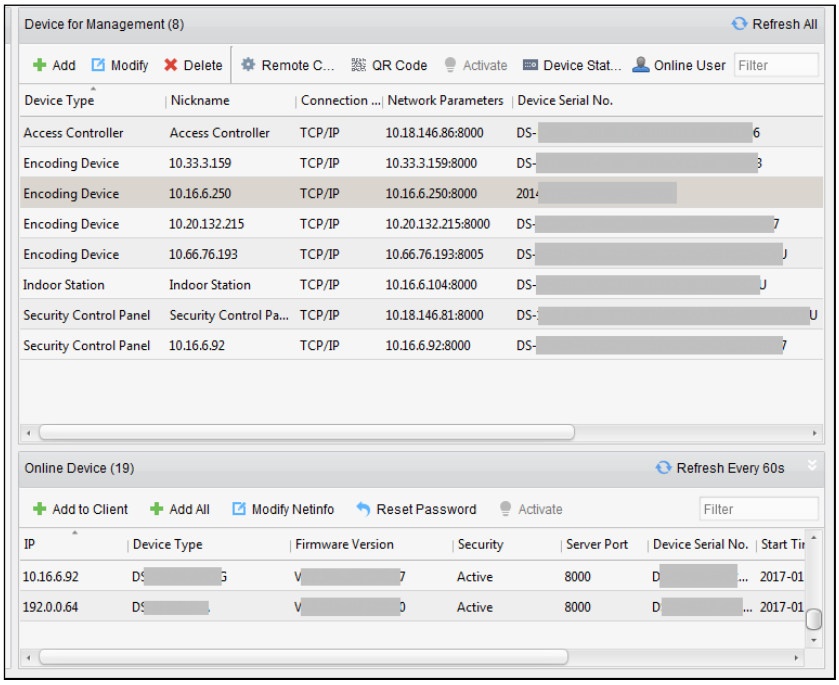
Modulul Control Acces este compus din următoarele submodule.

	Persoana si Card	Gestionarea organizațiilor, persoanelor și atribuirea cardurilor persoanelor.
	Program și Șablon	Configurarea programului săptămânal, grupul de vacanță și setarea șablonului.
	Permisiune	Atribuirea permisiunilor de control al accesului persoanelor și aplicarea dispozitivelor.
	Funcție avansată	Furnizarea de funcții avansate, inclusiv setări ale parametrilor de control al accesului, autentificarea cititorului de carduri, deschiderea ușii cu prima cartelă, anti-pasarea înapoi, interblocarea cu mai multe uși și parola de autentificare.
	Videointerfon	Interfon video între client și rezident, căutarea în jurnalul de apelare și eliberarea notificării.
	Căutare	Căutarea evenimentelor din istoricul controlului accesului; Căutarea în jurnalele de apeluri, jurnalele de deblocare și notificările lansate.
	Dispozitiv management	Gestionarea dispozitivelor de control acces și a dispozitivelor de videointerfon.

Notă:În acest capitol, prezentăm doar operațiunile despre controlul accesului.

7.4.1 Adăugarea dispozitivului de control al accesului

Clic în modulul de control acces pentru a intra în următoarea interfață.



Notă: După adăugarea dispozitivului, ar trebui să verificați starea de armare a dispozitivului **Instrument–Controlul armarii dispozitivului**. Dacă dispozitivul nu este armat, ar trebui să îl armați sau nu veți primi evenimentele prin intermediul software-ului client. Pentru detalii despre controlul armarii dispozitivului, consultați *7.12 Control armare*.

Crearea parolei

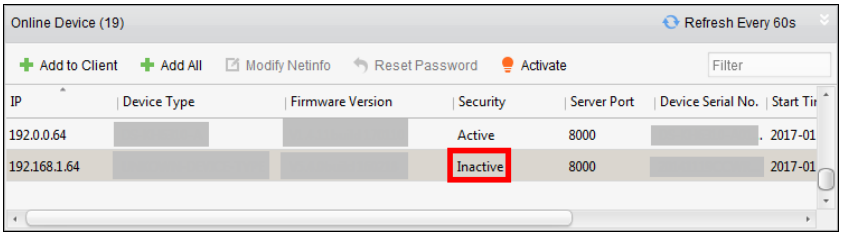
Scop:

Pentru unele dispozitive, vi se cere să creați parola pentru a le activa înainte ca acestea să poată fi adăugate la software și să funcționeze corect.

Notă: Această funcție ar trebui să fie acceptată de dispozitiv.

Pași:

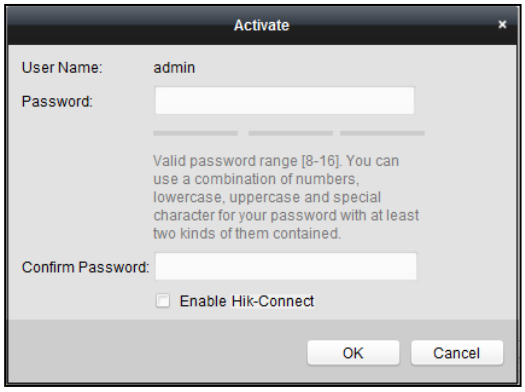
1. Accesați pagina Device Management.
2. Pe **Dispozitiv pentru management** sau **Dispozitiv online**, verificați starea dispozitivului (afișat pe **coloana Securitate**) și selectați un dispozitiv inactiv.



3. Faceți clic pe **Activati** pentru a deschide interfața de activare.
4. Creați o parolă în câmpul pentru parolă și confirmați parola.

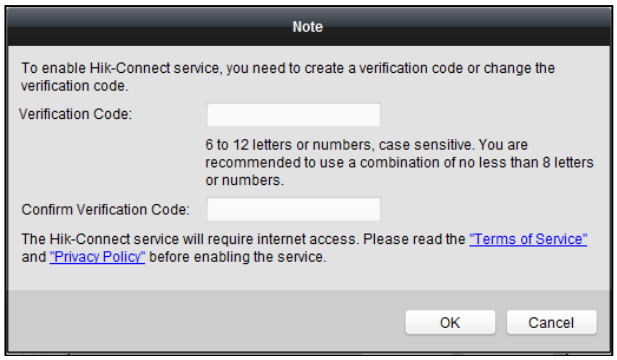
SE RECOMANDĂ PAROLA PUTERNICĂ – *Vă recomandăm să creați o parolă puternică, la alegerea dvs. (folosind minim 8 caractere, inclusiv litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dvs. Și vă recomandăm să vă resetați parola în mod regulat, mai ales în sistemul de înaltă securitate,*

resetarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.



5. (Opțional) Activați serviciul Hik-Connect atunci când activați dispozitivul dacă dispozitivul acceptă.

1) Bifați **Activați Hik-Connect** pentru a deschide caseta de dialog Notă.



2) Creați un cod de verificare.

3) Confirmați codul de verificare.

4) Faceți clic **Termenii serviciului** și **Politica de confidențialitate** pentru a citi cerințele.

5) Faceți clic **OK** pentru a activa serviciul Hik-Connect.

6. Faceți clic **OK** pentru a activa dispozitivul.

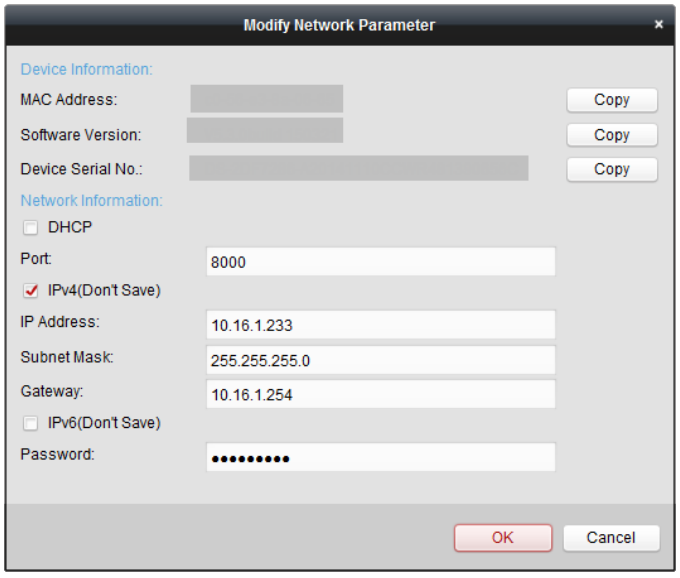
A „Dispozitivul este activat”. apare o fereastră când parola este setată cu succes.

7. Faceți clic **Modificați Netinfo** pentru a deschide interfața Modificare parametri de rețea.

Notă: Această funcție este disponibilă numai pe **Dispozitiv online** Puteți schimba adresa IP a dispozitivului la aceeași subrețea cu computerul dvs. dacă trebuie să adăugați dispozitivul la software.

8. Schimbați adresa IP a dispozitivului la aceeași subrețea cu computerul dvs. fie modificând Adresa IP manual sau bifând caseta de selectare a DHCP.

9. Introduceți parola setată la pasul 4 și faceți clic **Bine** pentru a finaliza setările de rețea.

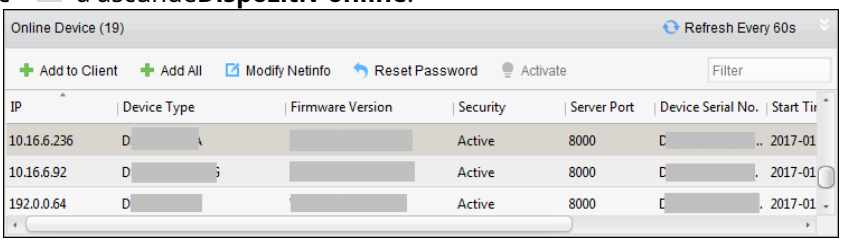


Adăugarea dispozitivului online

Scop:

Dispozitivele online active din aceeași subrețea locală cu software-ul client vor fi afișate pe **Dispozitiv online**. Puteți face clic pe **Actualizează la fiecare 60 s** pentru a reîmprospăta informațiile dispozitiveloronline.

Notă:Puteți da clic a ascunde**Dispozitiv online**.



Pași:

1. Selectați din listă dispozitivele de adăugat.

   Notă:Pentru dispozitivul inactiv, trebuie să creați parola pentru acesta înainte de a putea adăuga dispozitivul în mod corespunzător. Pentru pași detaliați, consultați*Capitolul 6 Activarea terminalului de control al accesului.*

2. Faceți clic **Adaugă la client** pentru a deschide caseta de dialog pentru adăugarea dispozitivului.

3. Introduceți informațiile necesare.

   Poreclă: Editați un nume pentru dispozitiv după cum doriți.

   Adresa: Introduceți adresa IP a dispozitivului. Adresa IP a dispozitivului este obținută automat în acest modde adăugare.

   Port: Introduceți numărul portului dispozitivului. Valoarea implicită este*8000.*

   Nume de utilizator: Introduceți numele de utilizator al dispozitivului. În mod implicit, numele de utilizator este *admin*. **Parola:**Introduceți parola dispozitivului.

   Puterea parolei dispozitivului poate fi verificată de software. Pentru confidențialitatea dvs., vă recomandăm insistent să schimbați parola cu ceva la alegerea dvs. (folosind minim 8

caractere, inclusiv litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului. Și vă recomandăm să vă resetați parola în mod regulat, mai ales în sistemul de înaltă securitate, resetarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

4. Opțional, bifați**Exportați la grup**casetă de selectare pentru a crea un grup după numele dispozitivului.

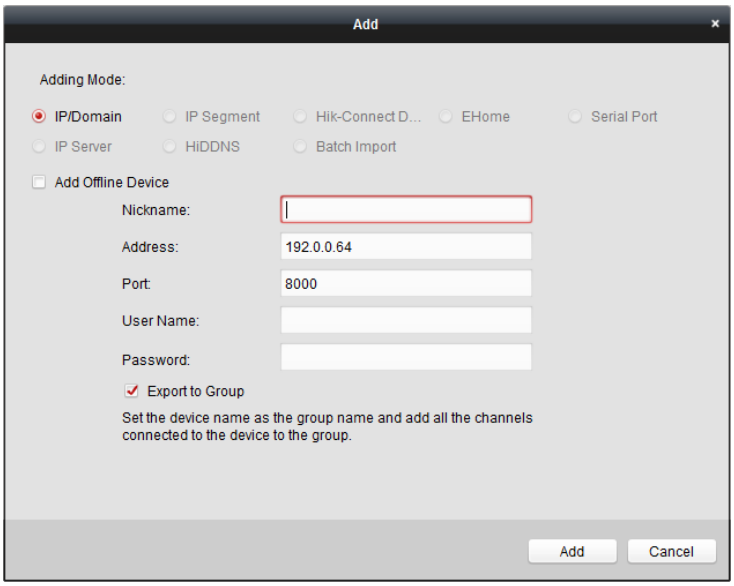
Puteți importa în mod implicit toate canalele dispozitivului în grupul corespunzător. ***Notă:***iVMS-4200 oferă, de asemenea, o metodă de adăugare a dispozitivelor offline. 1) Verificați**Adăugați dispozitiv offline**Caseta de bifat.

2) introduceți informațiile necesare, inclusiv numărul canalului dispozitivului și numărul de intrare al alarmei.

3) Faceți clic**Adăuga**.

Când dispozitivul offline este online, software-ul îl va conecta automat.

5. Faceți clic**Adăuga**pentru a adăuga dispozitivul.

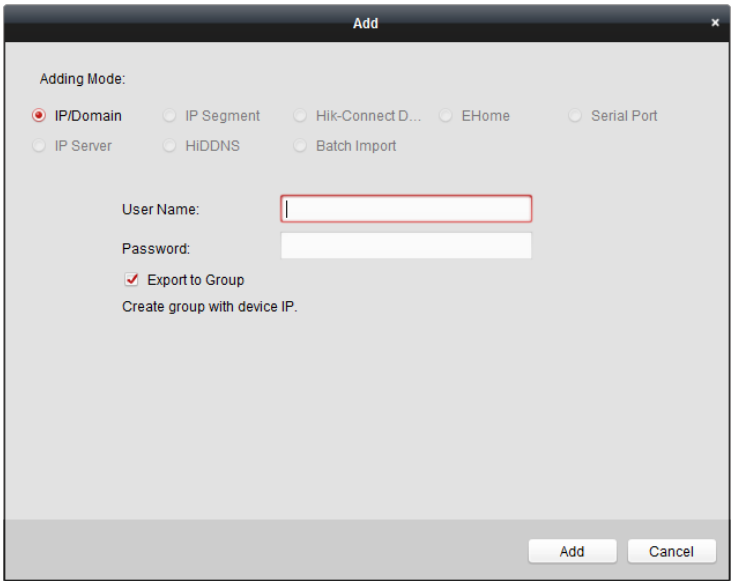


- **Adăugarea mai multor dispozitive online**

Dacă doriți să adăugați mai multe dispozitive online la software-ul client, faceți clic și mențineți apăsat*Ctrl*pentru a selecta mai multe dispozitive și faceți clic**Adaugă la client**pentru a deschide caseta de dialog pentru adăugarea dispozitivului. În caseta de mesaj pop-up, introduceți numele de utilizator și parola pentru dispozitivele de adăugat.

- **Adăugarea tuturor dispozitivelor online**

Dacă doriți să adăugați toate dispozitivele online la software-ul client, faceți clic**Adaugă totul**și faceți clic OK în caseta de mesaj pop-up. Apoi introduceți numele de utilizator și parola pentru dispozitivele de adăugat.



Adăugarea de dispozitive după IP sau Nume de domeniu

Pași:

1. Faceți clic**Adăuga**pentru a deschide caseta de dialog pentru adăugarea dispozitivului.
2. Selectați**IP/Domeniu**ca mod de adăugare.
3. Introduceți informațiile necesare.

   Poreclă: Editați un nume pentru dispozitiv după cum doriți.

   Adresa: Introduceți adresa IP sau numele domeniului dispozitivului.

   Port: Introduceți numărul portului dispozitivului. Valoarea implicită este*8000*.

   Nume de utilizator: Introduceți numele de utilizator al dispozitivului. În mod implicit, numele de utilizator este *admin*

   Parola: Introduceți parola dispozitivului.

   Puterea parolei dispozitivului poate fi verificată de software. Pentru confidențialitatea dvs., vă recomandăm insistent să schimbați parola cu ceva la alegerea dvs. (folosind minim 8 caractere, inclusiv litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dvs. Și vă recomandăm să vă resetați parola în mod regulat, mai ales în sistemul de înaltă securitate, resetarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

4. Opțional, bifați**Exportați la grup**casetă de selectare pentru a crea un grup după numele dispozitivului.

   Puteți importa în mod implicit toate canalele dispozitivului în grupul corespunzător. ***Notă:***iVMS-4200 oferă, de asemenea, o metodă de adăugare a dispozitivelor offline.

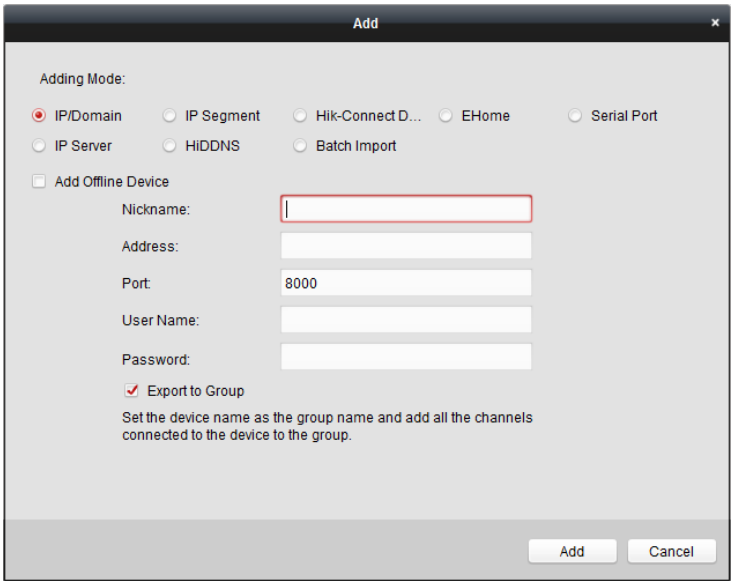
   1) Bifați **Adăugați dispozitiv offline**

   2) introduceți informațiile necesare, inclusiv numărul canalului dispozitivului și numărul de intrare al alarmei.

   3) Faceți clic**Adăuga**.

   Când dispozitivul offline este online, software-ul îl va conecta automat.

5. Faceți clic**Adăuga**pentru a adăuga dispozitivul.



Adăugarea de dispozitive după segmentul IP

Pași:

1. Faceți clic**Adăuga**pentru a deschide caseta de dialog pentru adăugarea dispozitivului.

2. Selectați**Segmentul IP**ca mod de adăugare.

3. Introduceți informațiile necesare.

IP de pornire: Introduceți o adresă IP de pornire.

IP final: Introduceți o adresă IP finală în același segment de rețea cu IP-ul de început.

Port: Introduceți numărul portului dispozitivului. Valoarea implicită este*8000*.

Nume de utilizator: Introduceți numele de utilizator al dispozitivului. În mod implicit, numele de utilizator este *admin*.

Parola: Introduceți parola dispozitivului.

Puterea parolei dispozitivului poate fi verificată de software. Pentru confidențialitatea dvs., vă recomandăm insistent să schimbați parola cu ceva la alegerea dvs. (folosind minim 8 caractere, inclusiv litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dvs. Și vă recomandăm să vă resetați parola în mod regulat, mai ales în sistemul de înaltă securitate, resetarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

4. Opțional, bifați**Exportați la grup**casetă de selectare pentru a crea un grup după numele dispozitivului.

Puteți importa în mod implicit toate canalele dispozitivului în grupul corespunzător. ***Notă:***iVMS-4200 oferă, de asemenea, o metodă de adăugare a dispozitivelor offline.

1) Bifați **Adăugați dispozitiv offline**

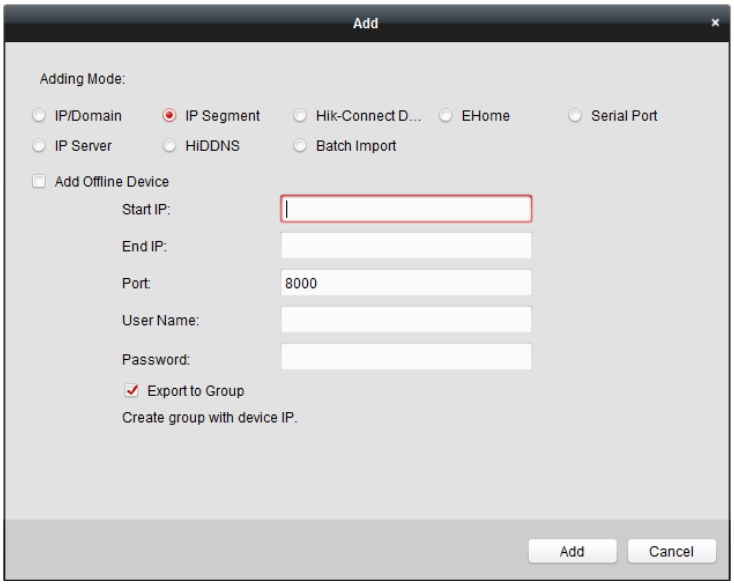
2) introduceți informațiile necesare, inclusiv numărul canalului dispozitivului și numărul de intrare al alarmei.

3) Faceți clic**Adăuga**.

Când dispozitivul offline este online, software-ul îl va conecta automat.

5. Faceți clic**Adăuga**.

Puteți adăuga dispozitivul care are adresa IP între IP-ul de început și IP-ul final la lista de dispozitive.



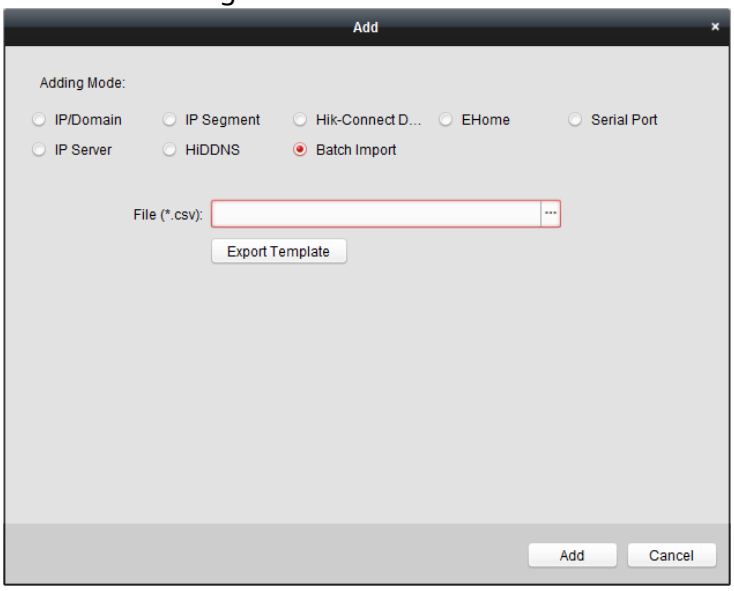
Importarea dispozitivelor în lot

Scop:

Dispozitivele pot fi adăugate la software în lot prin introducerea informațiilor despre dispozitiv în fișierul CSV predefinit.

Pași:

1. Faceți clic**Adăuga**pentru a deschide caseta de dialog pentru adăugarea dispozitivului.
2. Selectați**Import lot**ca mod de adăugare.



3. Faceți clic**Export șablon**și salvați șablonul predefinit (fișier CSV) pe computer.
4. Deschideți fișierul șablon exportat și introduceți informațiile necesare despre dispozitivele care vor fi adăugate în coloana corespunzătoare.

   Poreclă: Editați un nume pentru dispozitiv după cum doriți.

   Mod de adăugare: Puteți introduce 0, 2, 3, 4, 5 sau 6 care au indicat diferite moduri de adăugare. 0 indică faptul că dispozitivul este adăugat prin adresa IP sau numele de domeniu; 2 indică faptul că dispozitivul este adăugat prin server IP; 3 indică faptul că dispozitivul este adăugat prin HiDDNS; 4 indică faptul că dispozitivul

este adăugat prin protocolul EHome; 5 indică faptul că dispozitivul este adăugat prin portul serial; 6 indică faptul că dispozitivul este adăugat prin Hik-Connect Domain.

Adresa : Editați adresa dispozitivului. Dacă setați 0 ca mod de adăugare, ar trebui să introduceți adresa IP sau numele de domeniu al dispozitivului; dacă setați 2 ca mod de adăugare, ar trebui să introduceți adresa IP a PC-ului care instalează IP Server; dacă setați 3 ca mod de adăugare, ar trebui să introduceți *www.hik-online.com*.

Port: Introduceți numărul portului dispozitivului. Valoarea implicită este*8000*.

Informatie despre dispozitiv: Dacă setați 0 ca mod de adăugare, acest câmp nu este obligatoriu; dacă setați 2 ca mod de adăugare, introduceți ID-ul dispozitivului înregistrat pe serverul IP; dacă setați 3 ca mod de adăugare, introduceți numele domeniului dispozitivului înregistrat pe serverul HiDDNS; dacă setați 4 ca mod de adăugare, introduceți contul EHome; dacă setați 6 ca mod de adăugare, introduceți numărul de serie al dispozitivului.

Nume de utilizator: Introduceți numele de utilizator al dispozitivului. În mod implicit, numele de utilizator este *admin*.

Parola: Introduceți parola dispozitivului.

Puterea parolei dispozitivului poate fi verificată de software. Pentru confidențialitatea dvs., vă recomandăm insistent să schimbați parola cu ceva la alegerea dvs. (folosind minim 8 caractere, inclusiv litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dvs. Și vă recomandăm să vă resetați parola în mod regulat, mai ales în sistemul de înaltă securitate, resetarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

Adăugați dispozitiv offline: Puteți introduce 1 pentru a activa adăugarea dispozitivului offline, iar apoi software-ul îl va conecta automat când dispozitivul offline este online. 0 indică dezactivarea acestei funcții.

Exportați în grup: Puteți introduce 1 pentru a crea un grup după numele dispozitivului (porecla). Toate canalele dispozitivului vor fi importate implicit în grupul corespunzător. 0 indică dezactivarea acestei funcții.

Numărul canalului: Dacă setați 1 pentru Adăugare dispozitiv offline, introduceți numărul canalului dispozitivului. Dacă setați 0 pentru Adăugare dispozitiv offline, acest câmp nu este obligatoriu.

Număr de intrare de alarmă: Dacă setați 1 pentru Adăugare dispozitiv offline, introduceți numărul de intrare de alarmă al dispozitivului. Dacă setați 0 pentru Adăugare dispozitiv offline, acest câmp nu este obligatoriu.

Nr. port serial: Dacă setați 5 ca mod de adăugare, introduceți numărul portului serial pentru dispozitivul de control al accesului.

Rata baud: Dacă setați 5 ca mod de adăugare, introduceți viteza de transmisie a dispozitivului de control al accesului. **DIP:**Dacă setați 5 ca mod de adăugare, introduceți adresa DIP a dispozitivului de control al accesului. **Cont Hik-Connect:**Dacă setați 6 ca mod de adăugare, introduceți contul Hik-Connect. **Parola Hik-Connect:**Dacă setați 6 ca mod de adăugare, introduceți parola Hik-Connect.

5. Faceți clic și selectați fișierul șablon.

6. Faceți clic**Adăuga**pentru a importa dispozitivele.

Dispozitivele vor fi afișate în lista de dispozitive pentru gestionare după ce sunt adăugate cu succes. Puteți verifica utilizarea resurselor, starea HDD-ului, starea înregistrării și alte informații despre dispozitivele adăugate din listă.

Clic**Reîmprospătați toate**pentru a reîmprospăta informațiile tuturor dispozitivelor adăugate. De asemenea, puteți introduce numele dispozitivului în câmpul de filtrare pentru căutare.

7.4.2 Vizualizarea stării dispozitivului

În lista de dispozitive, puteți selecta dispozitivul și apoi faceți clic**Starea dispozitivului**butonul pentru a vedea starea acestuia. ***Notă:***Interfața poate fi diferită de imaginea afișată mai sus. Consultați interfața reală când adoptați această funcție.

Starea ușii: starea ușii conectate.

Stare gazdă: starea gazdei, inclusiv tensiunea de alimentare a bateriei de stocare, starea sursei de alimentare a dispozitivului, starea interblocării cu mai multe uși, starea anti-trecere înapoi și starea anti-modificare gazdă.

Stare cititor de carduri: Starea cititorului de carduri.

Notă:Dacă utilizați cititorul de carduri cu conexiune RS-485, puteți vedea starea online sau offline. Dacă utilizați cititorul de carduri cu conexiune Wiegand, puteți vedea starea offline.

Stare ieșire alarmă: Starea ieșirii de alarmă a fiecărui port.

Stare senzor de eveniment: starea senzorului de eveniment al fiecărui port.

Stare de armare: Starea dispozitivului.

7.4.3 Editarea informațiilor de bază

Scop:

După adăugarea dispozitivului de control al accesului, puteți edita informațiile de bază ale dispozitivului.

Pași:

1. Selectați dispozitivul din lista de dispozitive.
2. Faceți clic**Modifica**pentru a deschide fereastra de modificare a informațiilor despre dispozitiv.
3. Faceți clic**Informatii de baza**pentru a intra în interfața Informații de bază.

4. Editați informațiile despre dispozitiv, inclusiv modul de adăugare, numele dispozitivului, adresa IP a dispozitivului, numărul portului, numele de utilizator și parola.

7.4.4 Configurare la distanță

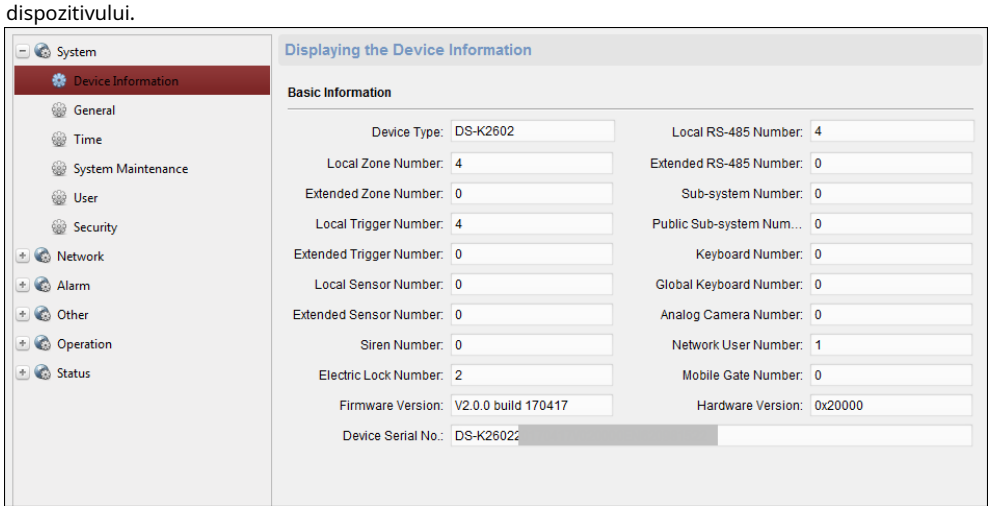
Scop:

În lista de dispozitive, selectați dispozitivul și faceți clic **Configurare la distanță** pentru a intra în interfața de configurare la distanță. Puteți seta parametrii detaliați ai dispozitivului selectat.

Verificarea informațiilor despre dispozitiv

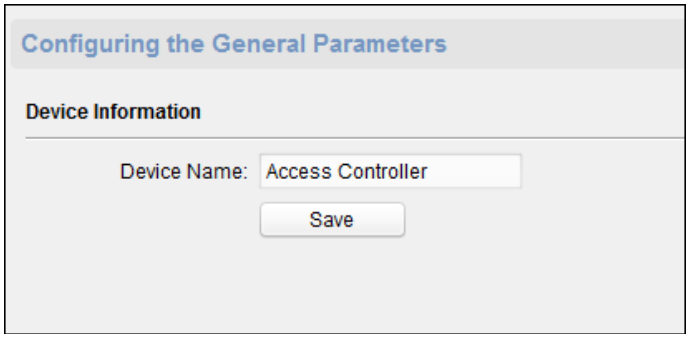
Pași:

1. În lista de dispozitive, puteți face clic**Configurare la distanță**pentru a intra în interfața de configurare la distanță.
2. Faceți clic**Sistem**->**Informatie despre dispozitiv**pentru a verifica informațiile de bază ale dispozitivului și informațiile despre versiunea dispozitivului.



Editarea numelui dispozitivului

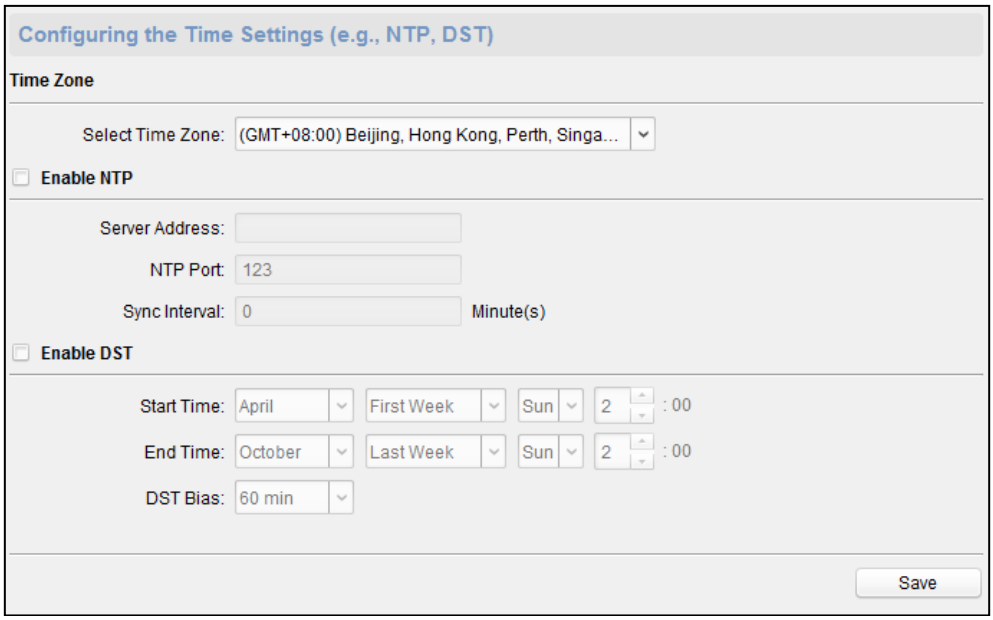
În interfața Configurare la distanță, faceți clic **Sistem**->**General** pentru a configura numele dispozitivului. Clic **Salvați** pentru a salva setările.



Timp de editare

Pași:

1. În interfața Configurare la distanță, faceți clic pe **Sistem**->**Timp** pentru a configura fusul orar.
2. (Opțional) Verificați **Activați NTP** și configurați adresa serverului NTP (sau domeniul serverului), portul NTP și intervalul de sincronizare.
3. (Opțional) Verificați **Activați ora de oră** și configurați ora stea DST, ora de încheiere și părtinirea.
4. Faceți clic **Salvați** pentru a salva setările.



Setarea întreținere a sistemului

Pași:

1. În interfața Configurare la distanță, faceți clic pe **Sistem**->**Întreținerea sistemului**.

2. Faceți clic **Reporniți** pentru a reporni dispozitivul.

   Sau faceți clic **Restabilește setările implicite** pentru a restabili setările dispozitivului la cele implicite, excluzând adresa IP.

   Sau faceți clic **Restabileste tot** pentru a restabili parametrii dispozitivului la cei impliciti. Dispozitivul trebuieactivat după restaurare.

   Notă: Fișierul de configurare conține parametrii dispozitivului.

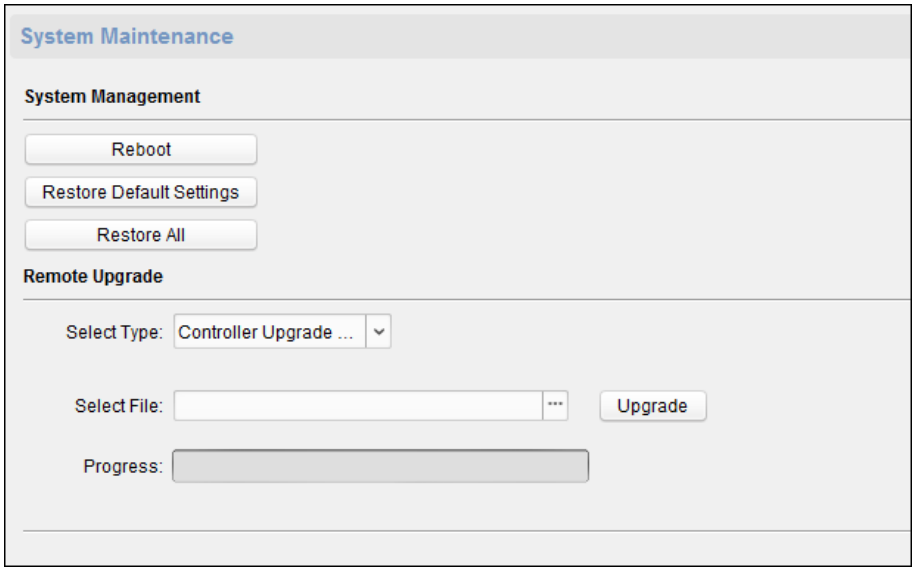
3. De asemenea, puteți actualiza dispozitivul de la distanță.

   1) În secțiunea Actualizare la distanță, selectați un tip de fișier de actualizare din lista verticală. Puteți selecta Controller Upgrade File sau Card Reader Upgrade din lista derulantă.

   2) Faceți clic pentru a selecta fișierul de actualizare.

   3) Faceți clic **Actualizare** pentru a începe actualizarea.

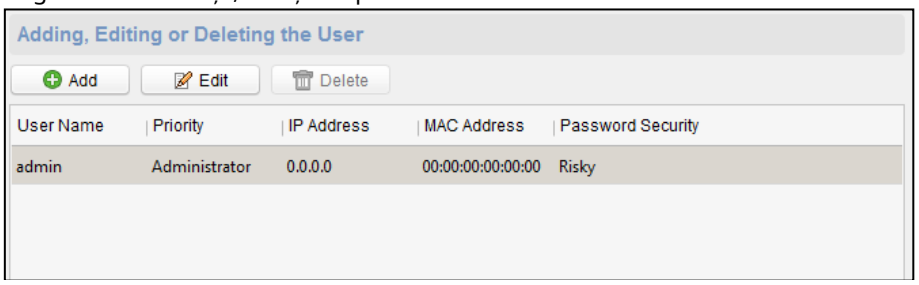
      Notă: Numai cititoarele de carduri conectate prin RS-485 pot fi actualizate. Controlerul de acces seria DS-K2800 acceptă doar cititorul de carduri Wiegand.



Administrator utilizator

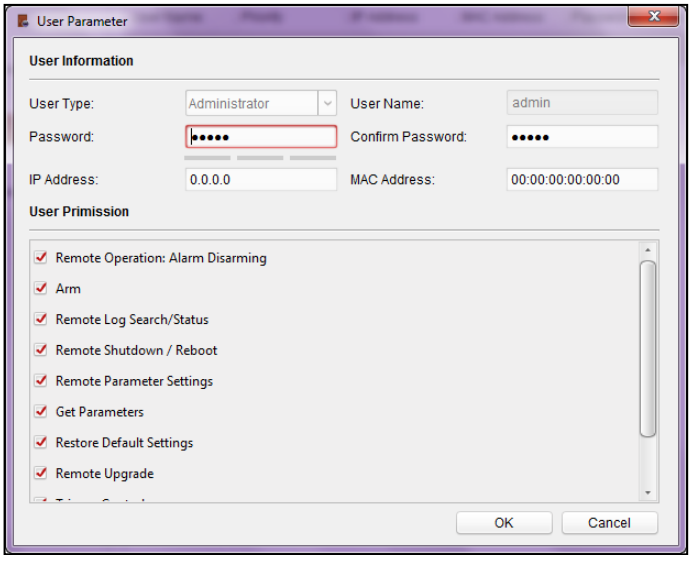
Pași:

1. În interfața Configurare la distanță, faceți clic pe **Sistem**->**Utilizator**.



2. Faceți clic**Adăuga**pentru a adăuga utilizatorul.

Sau selectați un utilizator din lista de utilizatori și faceți clic **Editați** pentru a edita utilizatorul. Puteți edita parola utilizatorului, adresa IP, adresa MAC și permisiunea utilizatorului. Clic **OK** pentru a confirma editarea.



Setarea Securității

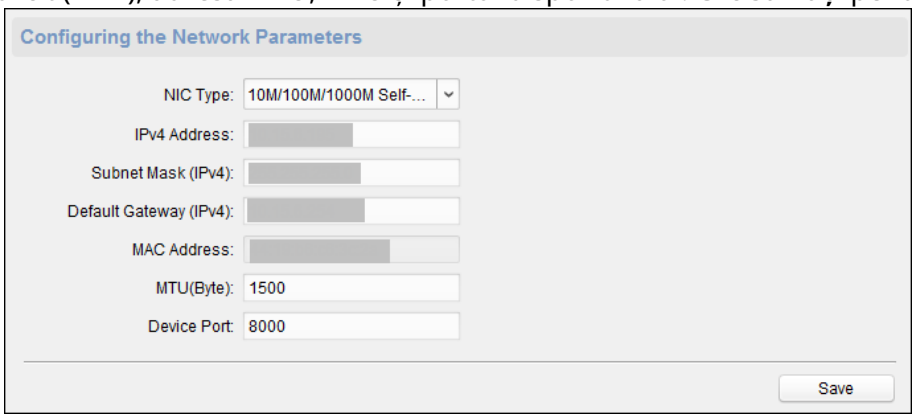
Pași:

1. Faceți clic **Sistem**->**Securitate**.

2. Selectați modul de criptare din lista verticală. Puteți selecta Modul compatibil sau Modul de criptare.
3. Faceți clic **Salvați** pentru a salva setările.

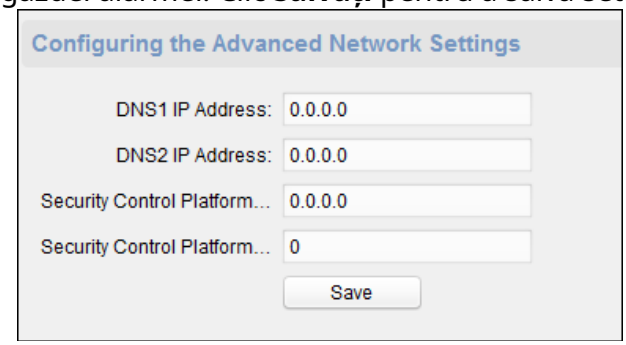
Configurarea parametrilor de rețea

Clic **Reţea**->**General**. Puteți configura tipul NIC, adresa IPv4, masca de subrețea (IPv4), gateway-ulimplicit (IPv4), adresa MTU, MTU și portul dispozitivului. Clic **Salvați** pentru a salva setările.



Configurarea rețelei avansate

Clic **Reţea**->**Setari avansate**. Puteți configura adresa DNS 1, adresa DNS 2, IP-ul gazdeialarmei și portul gazdei alarmei. Clic **Salvați** pentru a salva setările.

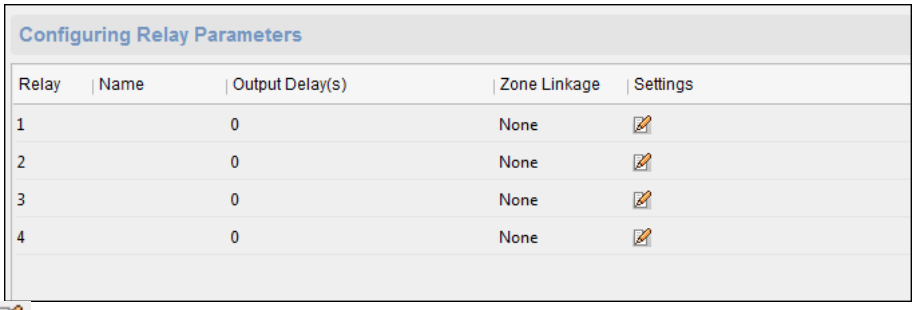


Configurarea parametrilor releului

Pași:

1. Faceți clic **Alarma**->**Releu**.

   Puteți vizualiza parametrii releului.



2. Faceți clic pe pentru a deschide fereastra Setări parametri releu.
3. Setați numele releului și întârzierea de ieșire.
4. Faceți clic **Salvați** pentru a salva parametrii.

Sau faceți clic **Copiaza in...** pentru a copia informațiile despre releu în alte relee.

Configurarea parametrilor de control al accesului

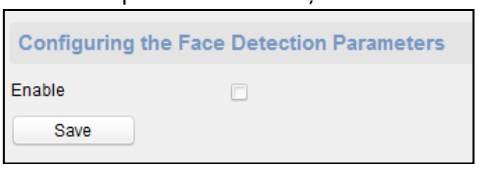
Pași:

1. În interfața Configurare la distanță, faceți clic pe **Alte**->**Parametrii de control al accesului**.
2. Selectați și bifați **Apăsați tasta pentru a introduce numărul cardului.**
3. Faceți clic **Salvați** pentru a salva setările.

Configurarea parametrilor de detectare a feței

Clic **Alte**->**Detectare facială**. Puteți verifica **Permite** pentru a activa funcția de detectare a feței.

Notă:Numai dispozitivele cu funcție video acceptă această funcție.



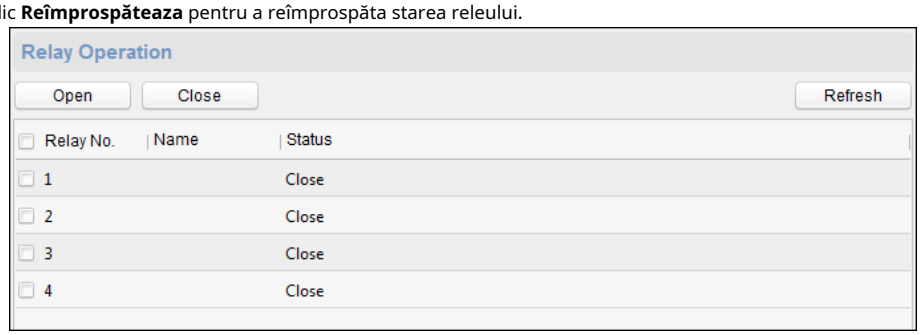
Releu de operare

Pași:

1. Faceți clic **Operațiune**->**Releu**.

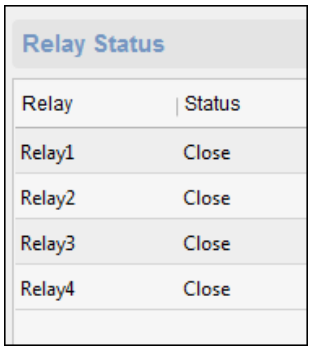
Puteți vizualiza starea releului.

2. Bifați caseta de validare a releului
3. Faceți clic **Deschis** sau **Închis** pentru a deschide/închide releul.
4. (Opțional) Faceți clic **Reîmprospăteaza** pentru a reîmprospăta starea releului.



Vizualizarea stării releului

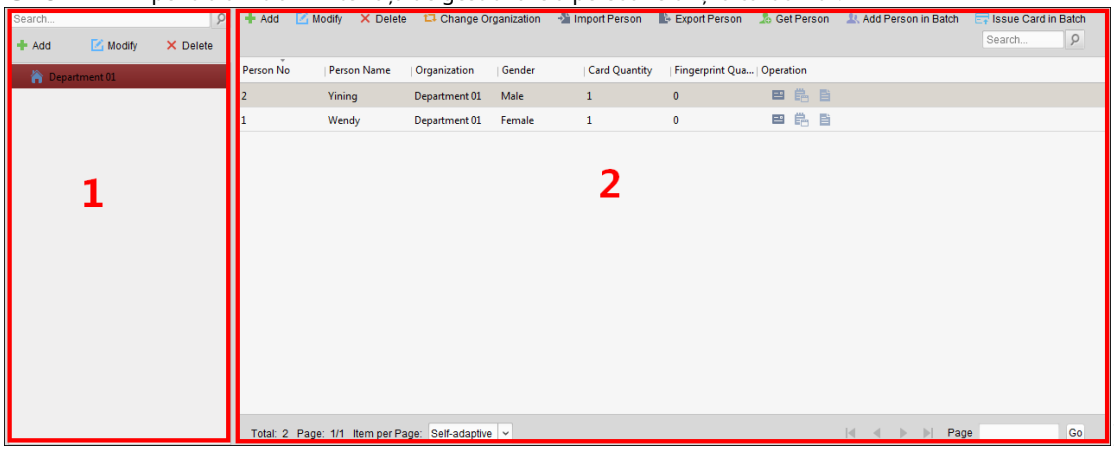
Clic **stare**->**Releu** pentru a vizualiza starea releului.



7.5 Gestionarea persoanelor și a cardurilor

Puteți adăuga, edita și șterge organizația și persoana în modulul de gestionare a persoanelor și a cardurilor.

Clic  pentru a intra în interfața de gestionare a persoanelor și a cardurilor.



Interfața este împărțit în două părți: Managementul organizației și Managementul persoanelor.

1	**Organizare management**	Puteți adăuga, edita sau șterge organizația după cum doriți.
2	**Managementul persoanelor**	După adăugarea organizației, puteți adăuga persoana la organizație și puteți elibera cardul persoanelor pentru gestionarea ulterioară.

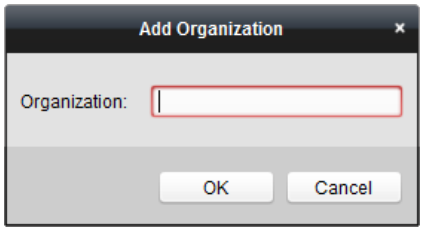
7.5.1 Managementul organizației

Adăugarea organizației

Pași:

1. În lista de organizații din stânga, ar trebui să adăugați o organizație de top ca organizație-mamă a tuturor organizațiilor.

Clic**Adăuga**butonul pentru a deschide interfața de adăugare a organizației.



2. Introduceți numele organizației după cum doriți.

3. Faceți clic **OK** pentru a salva adăugarea.

4. Puteți adăuga mai multe niveluri de organizații în funcție de nevoile reale.

Pentru a adăuga suborganizații, selectați organizația părinte și faceți clic**Adăuga**.

Repeta*Pasul 2*și*3*pentru a adăuga suborganizația.

Apoi organizația adăugată va fi suborganizația organizației de nivel superior. ***Notă:*** Pot fi create până la 10 niveluri de organizații.

Modificarea și ștergerea organizației

Puteți selecta organizația adăugată și faceți clic**Modifica**pentru a-i modifica numele.

Puteți selecta o organizație și faceți clic**Șterge**butonul pentru a-l șterge. ***Note:***

- Organizațiile de nivel inferior vor fi șterse și dacă ștergeți o organizație.
- Asigurați-vă că nu există nicio persoană adăugată în cadrul organizației sau organizația nu poate fi ștearsă.

7.5.2 Managementul persoanelor

După adăugarea organizației, puteți adăuga o persoană la organizație și puteți gestiona persoana adăugată, cum ar fi emiterea de carduri în lot, importul și exportul de informații despre persoane în lot etc.

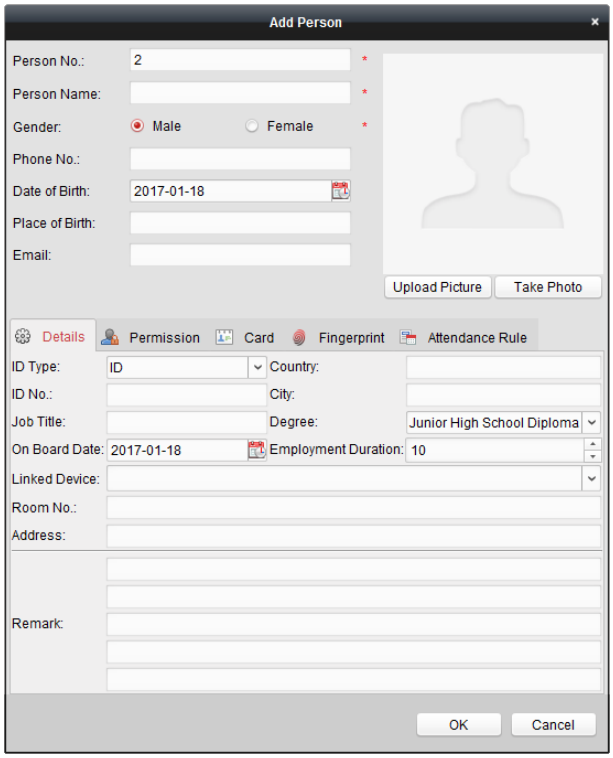
Notă:Se pot adăuga până la 10.000 de persoane sau carduri.

Adăugarea unei persoane

Adăugarea unei persoane (informații de bază)

Pași:

1. Selectați o organizație din lista de organizații și faceți clic**Adăuga**butonul din panoul Persoană pentru a deschide caseta de dialog pentru adăugarea persoanei.



2. Numărul de persoană va fi generat automat și nu poate fi editat.

3. Introduceți informațiile de bază, inclusiv numele persoanei, numărul de telefon, detaliile zilei de naștere și adresa de e-mail.

4. Faceți clic**Încarcă imagine**pentru a selecta imaginea persoanei de pe computerul local pentru a o încărca pe client. ***Notă:***Imaginea trebuie să fie în format *.jpg.

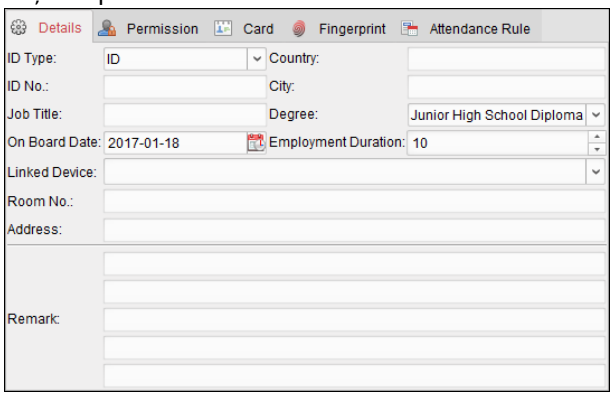
5. (Opțional) Puteți, de asemenea, să faceți clic**Luați telefonul**pentru a face fotografia persoanei cu camera PC-ului.

6. Faceți clic**Bine**pentru a termina de adăugat.

Adăugarea unei persoane (informații detaliate)

Pași:

1. În interfața Add Person, faceți clic pe **Detalii**.



2. Introduceți informațiile detaliate ale persoanei, inclusiv tipul de identitate al persoanei, numărul ID, țara etc., în funcție de nevoile reale.

- **Dispozitiv conectat:**Puteți lega stația interioară de persoană.
  Notă:Dacă selectați**Stație interioară analogică**în Dispozitivul conectat,**Stația de ușă** câmpul va fi afișat și vi se cere să selectați stația de ușă pentru a comunica cu analogul

statie interioara.

- **Camera nr.:**Puteți introduce numărul de cameră al persoanei.

3. Faceți clic**Bine**pentru a salva setările.

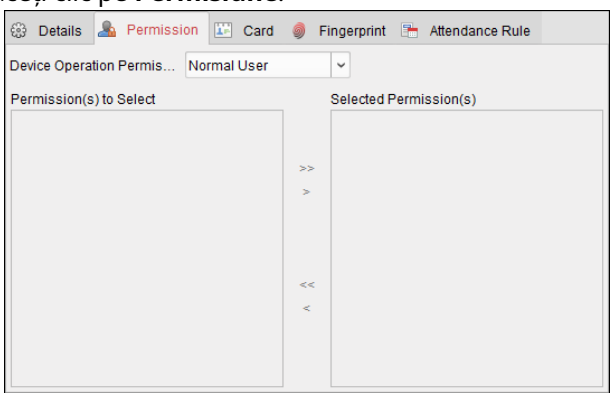
Adăugarea unei persoane (permisiune)

Puteți atribui permisiunile (inclusiv permisiunile de operare ale dispozitivului de control al accesului și permisiunile de control al accesului) persoanei atunci când adăugați o persoană.

Notă:Pentru setarea permisiunii de control al accesului, consultați*Capitolul 7.7 Configurarea permisiunilor.*

Pași:

1. În interfața Add Person, faceți clic pe **Permisiune**.



2. În câmpul Device Operation Role, selectați rolul de operare a dispozitivului de control acces.

Utilizator normal: Persoana are permisiunea de a face check-in/out pe dispozitiv, trece punctul de control accesetc.

Administrator: Persoana are permisiunea de utilizator normală, precum și permisiunea de a configura dispozitivul, inclusiv adăugarea unui utilizator normal etc.

3. În lista Permisiuni de selectare, se afișează toate permisiunile configurate.

Bifați caseta (permisiunile) și faceți clic**>**pentru a adăuga la lista de permisiuni selectate. (Opțional) Puteți face clic**>>**pentru a adăuga toate permisiunile afișate la lista de permisiuni selectate. (Opțional) În lista Permisiuni selectate, selectați permisiunea selectată și faceți clic**<**pentru a-l elimina. De asemenea, puteți face clic**<<** pentru a elimina toate permisiunile selectate.

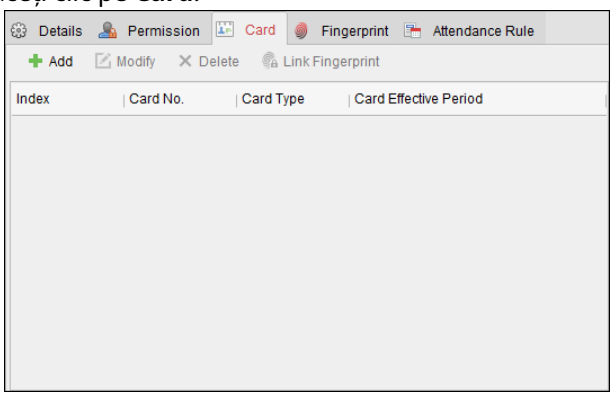
4. Faceți clic **OK** pentru a salva setările.

Adăugarea unei persoane (card)

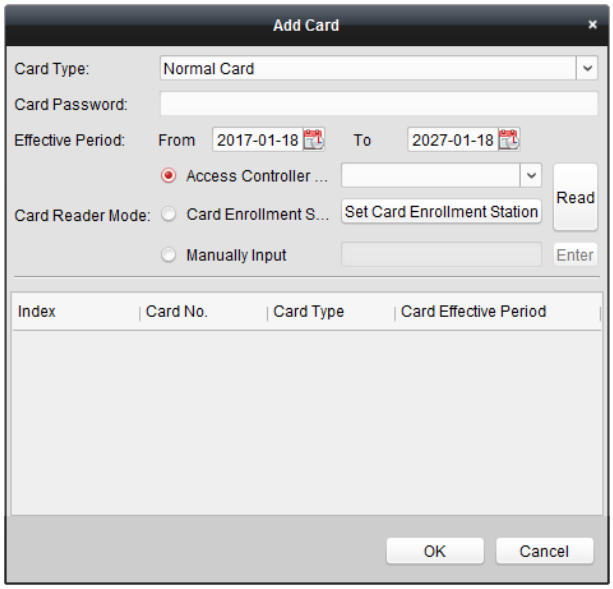
Puteți adăuga card și emite cardul persoanei.

Pași:

1. În interfața Add Person, faceți clic pe **Card**.



2. Faceți clic **Adăuga** pentru a deschide caseta de dialog Adăugați card.



3. Selectați tipul de card în funcție de nevoile reale.
   - **Card normal**
   - **Card pentru deschidere extinsă a ușii**: Ușa va rămâne deschisă pentru perioada de timp configurată pentru deținătorul cardului.
   - **Card în Blocklist**: Acțiunea de glisare a cardului va fi încărcată și ușa nu poate fi deschisă.
   - **Card de patrulare**: Acțiunea de glisare a cardului poate fi utilizată pentru verificarea stării de lucru a personalului de inspecție. Permisul de acces al personalului de inspecție este configurabil. **Cardul de constrângere**: Ușa se poate
   - deschide prin glisarea cardului de constrângere atunci când există constrângere. În același timp, clientul poate raporta evenimentul de constrângere.
   - **Super Card**: Cardul este valabil pentru toate ușile controlerului în timpul programului configurat.
   - **Card de vizitator**: Cardul este atribuit vizitatorilor. Pentru Cardul de vizitator, puteți seta**Max. Timp de glisare**.

     Note:
     - Max. Timpii de glisare ar trebui să fie între 0 și 255. Când timpul de glisare a cardului este mai mare decât timpul configurat, glisarea cardului va fi invalidă.
     - Când setați timpii la 0, înseamnă că glisarea cardului este nelimitată.

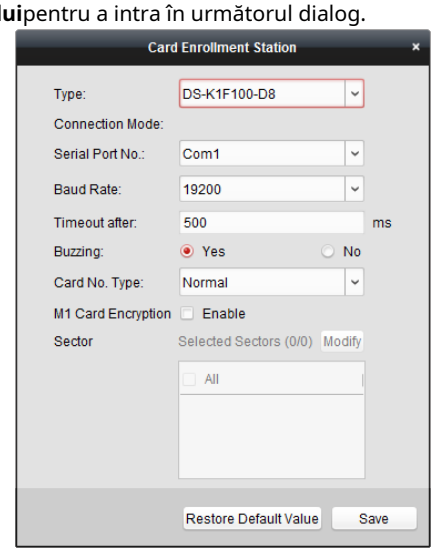
4. Introduceți parola cardului în câmpul Parola cardului. Parola cardului trebuie să conțină 4 până la 8 cifre.

   Notă:Parola va fi necesară atunci când deținătorul cardului glisează cardul pentru a intra sau a ieși din ușă dacă activați modul de autentificare a cititorului de carduri ca**Card și Parolă**, **Parolă și amprentă**, și**Card, parolă și amprentă**. Pentru detalii,*Capitolul 7.8.2 Autentificarea cititorului de carduri.*

5. Faceți clic pentru a seta timpul efectiv și timpul de expirare a cardului.
6. Selectați modul cititor de carduri pentru citirea cardului nr.
   - **Cititor de controler de acces:**Așezați cardul pe cititorul controlerului de acces și faceți clic **Citit** pentru a obține cardul nr.

- **Stație de înregistrare a cardurilor:**Așezați cardul pe stația de înregistrare a cardului și faceți clic**Citit**pentru a obține cardul nr.

  Notă:Stația de înregistrare a cardului ar trebui să se conecteze la computerul care rulează clientul. Puteți da clic**Setați stația de înregistrare a cardului**pentru a intra în următorul dialog.



2) Selectați tipul de stație de înregistrare card.

Notă:În prezent, tipurile de cititoare de carduri acceptate includ DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E și DS-K1F180-D8E.

3) Setați numărul portului serial, viteza de transmisie, valoarea timeout, bâzâitul sau tipul de nr.

Notă:Controlerul de acces seria DS-K2800 nu acceptă funcția de criptare a cardului M1.

4) Faceți clic **Salvați** pentru a salva setările.

Puteți da clic **Restabiliți valoarea implicită** pentru a restabili valorile implicite.
Introducere manuală: Introduceți numărul cardului și faceți clic**introduce**pentru a introduce cardul nr.

7. Faceți clic **OK** iar cardurile vor fi eliberate persoanei.

8. (Opțional) Puteți selecta cardul adăugat și faceți clic**Editați** sau **Șterge**pentru a edita sau șterge cardul.9.

Faceți clic **OK** pentru a salva setările.

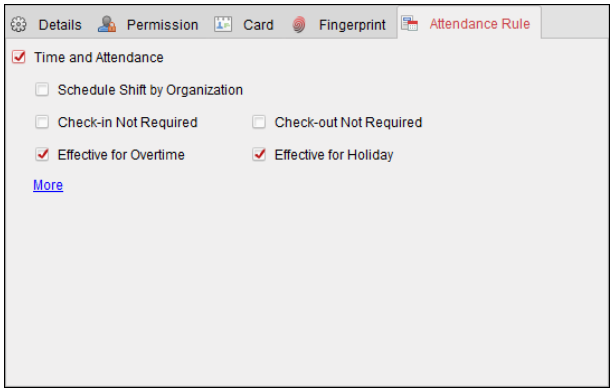
Adăugarea unei persoane (regula de prezență)

Puteți seta regula de prezență pentru persoană.

Notă:Această pagină cu filă se va afișa când selectați**Non-reședință**modul în scena aplicației atunci când rulați software-ul pentru prima dată.

Pași:

1. În interfața Add Person, faceți clic pe**Regula de prezență**fila.



2. Dacă persoana se alătură în timp și prezență, verificați**Timp și prezență**casetă de selectare pentru a activa această funcție pentru persoană. Apoi, înregistrările de trecere a cardului persoanei vor fi înregistrate și analizate pentru timp și prezență.

   Pentru detalii despre timp și prezență, faceți clic **Mai mult** pentru a merge la modulul Timp și prezență.

3. Faceți clic **OK** pentru a salva setările.

Importarea și exportarea informațiilor despre persoană

Informațiile despre persoană pot fi importate și exportate în lot.

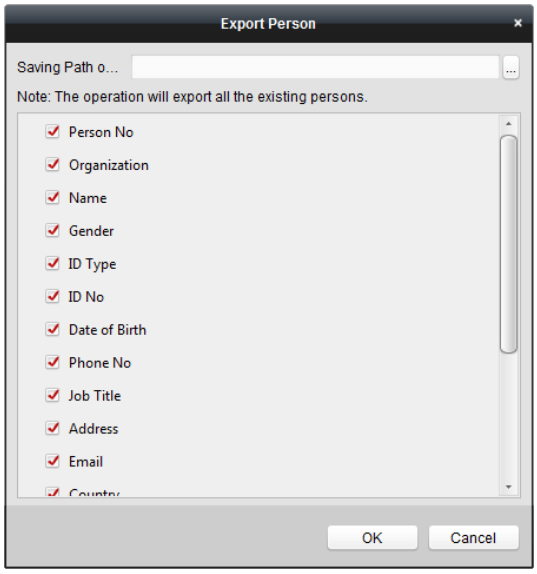
Pași:

1.**Persoana exportatoare:**Puteți exporta informațiile despre persoanele adăugate în format Excel în local PC.

   1) După ce ați adăugat persoana, puteți face clic **Persoana de export** din fila Persoană și card pentru a afișa următorul dialog.

   2) Faceți clic ... pentru a selecta calea de salvare a fișierului Excel exportat.

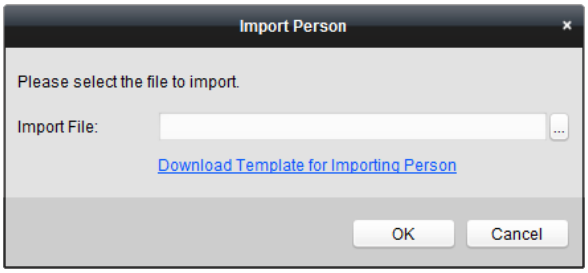
   3) Bifați casetele de selectare pentru a selecta informațiile despre persoană de exportat.



   4) Faceți clic **OK** pentru a începe exportul.

2.**Persoana importatoare:** Puteți importa fișierul Excel cu informații despre persoane în lot de pe computerul local

   1) faceți clic **Persoană de import** din fila Persoană și card.



2) Puteți face clic**Descărcați șablonul pentru persoana care importă**pentru a descărca mai întâi șablonul.

3) Introduceți informațiile despre persoană în șablonul descărcat.

4) Faceți clic ... pentru a selecta fișierul Excel cu informații despre persoană.

5) Faceți clic**Bine**pentru a începe importul.

Obținerea informațiilor despre persoane de la dispozitivul de control al accesului

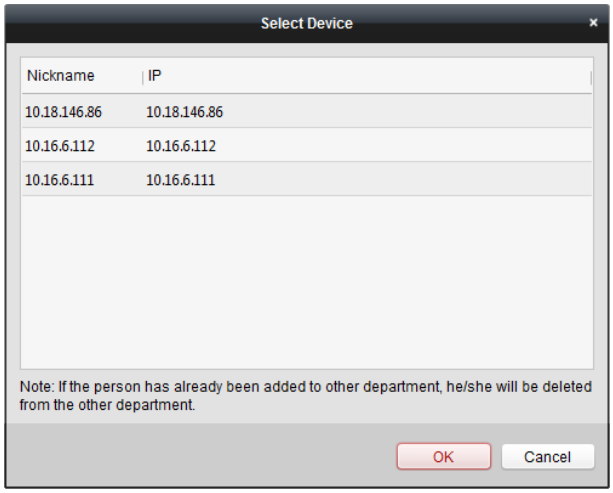
Dacă dispozitivul de control al accesului adăugat a fost configurat cu informații despre persoană (inclusiv detalii despre persoană, amprentă, informații despre cardul emis), puteți obține informațiile despre persoană de pe dispozitiv și le puteți importa în client pentru operațiuni ulterioare.

Notă:Această funcție este acceptată numai de dispozitivul a cărui metodă de conectare este TCP/IP la adăugarea dispozitivului.

Pași:

1. În lista de organizații din stânga, faceți clic pentru a selecta o organizație pentru a importa persoanele.

2. Faceți clic**Obțineți Persoană**butonul pentru a deschide următoarea casetă de dialog.



3. Dispozitivul de control al accesului adăugat va fi afișat.

4. Faceți clic pentru a selecta dispozitivul și apoi faceți clic **OK** pentru a începe să obțineți informații despre persoană de pe dispozitiv.

De asemenea, puteți face dublu clic pe numele dispozitivului pentru a începe să obțineți informațiile despre persoană.

Note:

- Informațiile despre persoană, inclusiv detaliile despre persoană, informațiile despre amprenta persoanei (dacă este configurată) și cardul conectat (dacă este configurat), vor fi importate în organizația selectată. Dacă numele
- persoanei stocate în dispozitiv este gol, numele persoanei va fi completat cu numărul cardului emis după importare către client.
- Pot fi importate până la 10000 de persoane cu până la 5 carduri fiecare.

Persoana Conducătoare

Modificarea și ștergerea persoanei

Pentru a modifica informațiile despre persoană și regula de prezență, faceți clic pe sau în coloanaOperație sau selectați persoana și faceți clic**Modifica**pentru a deschide dialogul persoanei de editare. Puteți face clic pentru a vedea înregistrările de trecere a cardului persoanei.

Pentru a șterge persoana, selectați o persoană și faceți clic**Șterge**pentru a-l șterge.

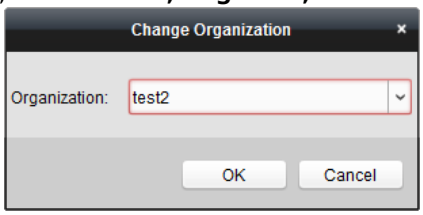
Notă:Dacă un card este emis persoanei curente, legătura va fi invalidă după ce persoana respectivă este ștearsă.

Schimbarea persoanei în altă organizație

Dacă este necesar, puteți muta persoana într-o altă organizație.

Pași:

1. Selectați persoana din listă și faceți clic**Schimbați organizația**buton.



2. Selectați organizația la care să mutați persoana.
3. Faceți clic **OK** pentru a salva setările.

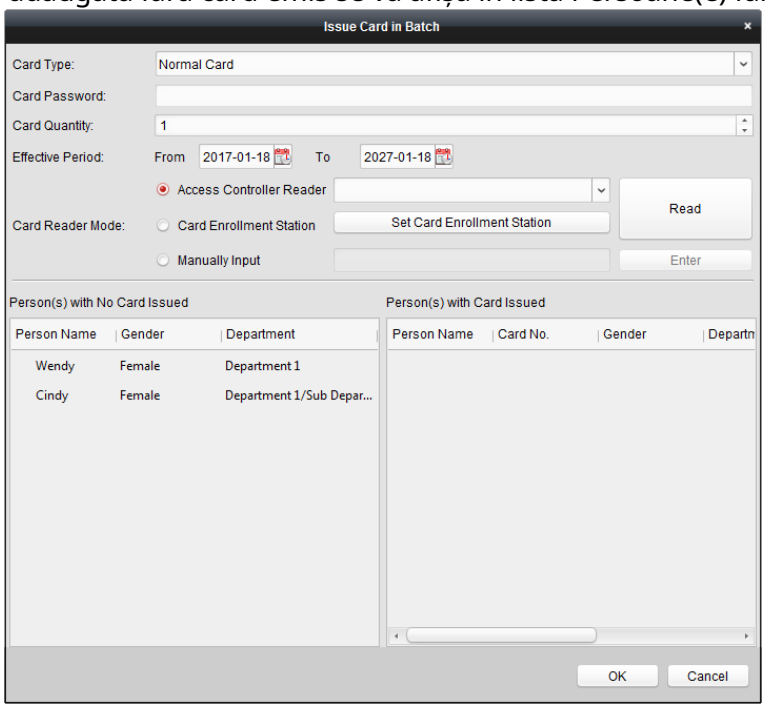
Emiterea cardului în lot

Puteți emite mai multe carduri pentru persoana fără card emis în lot.

Pași:

1. Faceți clic**Emite card în lot**butonul pentru a intra în următorul dialog.

Toată persoana adăugată fără card emis se va afișa în lista Persoane(e) fără card emis.



2. Selectați tipul de card în funcție de nevoile reale.

Notă:Pentru detalii despre tipul de card, consultați*Adăugarea unei persoane.*

3. Introduceți parola cardului în câmpul Parola cardului. Parola cardului trebuie să conțină 4 până la 8 cifre.

   Notă:Parola va fi necesară atunci când deținătorul cardului glisează cardul pentru a intra sau a ieși din ușă dacă activați modul de autentificare a cititorului de carduri ca**Card și Parolă**, **Parolă și amprentă**, și**Card, parolă și amprentă**. Pentru detalii, consultați*Capitolul 7.8.2 Autentificarea cititorului de carduri.*

4. Introduceți cantitatea de card emisă pentru fiecare persoană.

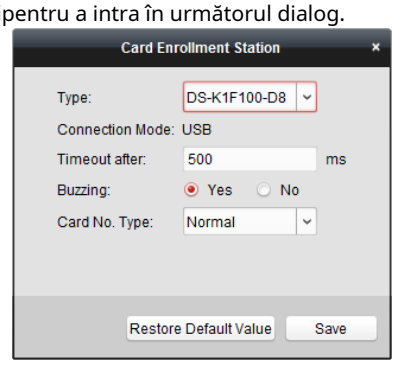
   De exemplu, dacă Cantitatea cardului este 3, puteți citi sau introduce trei Nr. card pentru fiecare persoană.

5. Faceți clic pentru a seta timpul efectiv și timpul de expirare a cardului.

6. Selectați modul cititor de carduri pentru citirea cardului nr.

   - **Cititor de controler de acces:**Așezați cardul pe cititorul controlerului de acces și faceți clic **Citit** pentru a obține cardul nr.
   - **Stație de înregistrare a cardurilor:**Așezați cardul pe stația de înregistrare a cardului și faceți clic**Citit**pentru a obține cardul nr.

     Notă:Stația de înregistrare a cardului ar trebui să se conecteze la computerul care rulează clientul. Puteți da clic**Setați stația de înregistrare a cardului**pentru a intra în următorul dialog.



     1) Selectați tipul de stație de înregistrare card.

        Notă:În prezent, tipurile de cititoare de carduri acceptate includ DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E și DS-K1F180-D8E.

     2) Setați parametrii despre stația de înregistrare card conectată.

     3) Faceți clic**Salvați**butonul pentru a salva setările.

        Puteți da clic**Restabiliți valoarea implicită**butonul pentru a restabili valorile implicite.

Introducere manuală: Introduceți numărul cardului și faceți clic**introduce**pentru a introduce cardul nr.

7. După emiterea cardului persoanei respective, persoana și informațiile despre card vor fi afișate în lista Persoane(e) cu cardul emis.

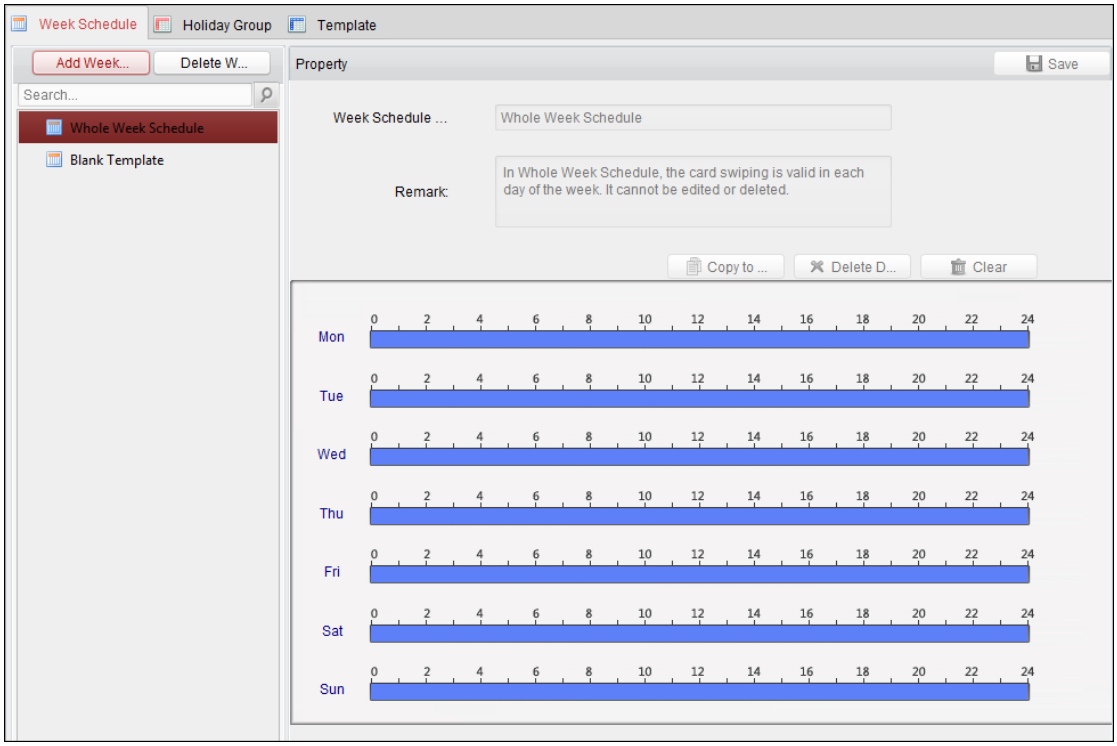
8. Faceți clic**Bine**pentru a salva setările.

7.6 Program și șablon

Scop:

Puteți configura șablonul, inclusiv programul săptămânal și programul de vacanță. După setarea șabloanelor, puteți adopta șabloanele configurate pentru permisiunile de control al accesului atunci când setați permisiunea, astfel încât permisiunea de control al accesului să intre în vigoare în duratele de timp ale șablonului.

Clic pentru a intra în interfața de program și șablon.



Puteți gestiona programul de permisiuni de control al accesului, inclusiv programul săptămânal, programul de vacanță și șablonul. Pentru setările de permisiuni, consultați *Capitolul 7.7 Configurarea permisiunilor.*

7.6.1 Programul săptămânii

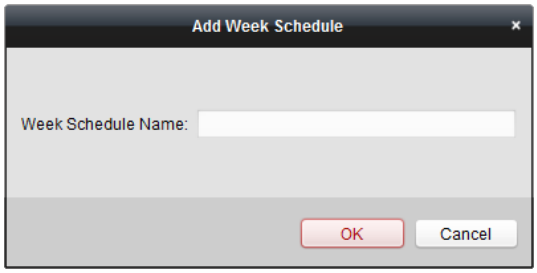
Clic**Programul săptămânii**pentru a intra în interfața de gestionare a programului săptămânal.

Clientul definește implicit două tipuri de plan de săptămână:**Programul întregii săptămâni**și**Program gol**, care nu poate fi șters și editat.

- **Programul întregii săptămâni:**Glisarea cardului este valabilă în fiecare zi a săptămânii.
- **Program necompletat:**Glisarea cardului este invalidă în fiecare zi a săptămânii.

Puteți efectua următorii pași pentru a defini programe personalizate la cererea dvs. ***Pași:***

1. Faceți clic**Adăugați programul săptămâniibutonul** pentru a deschide interfața de adăugare a programului.



2. Introduceți numele programului săptămânii și faceți clic **OK** pentru a adăuga programul săptămânal.
3. Selectați programul săptămânal adăugat în lista de program și puteți vedea proprietatea acestuia în partea dreaptă. Puteți edita numele programului săptămânal și puteți introduce informațiile despre observație.
4. În programul săptămânal, faceți clic și trageți pe o zi pentru a desena programul, ceea ce înseamnă că

perioada de timp, permisiunea configurată este activată.

Notă: În program pot fi setate până la 8 perioade de timp pentru fiecare zi.

5. Când cursorul setransforma în , puteți muta bara de timp selectată pe care tocmai ați editat-o. De asemenea, puteți edita punctul de timp afișat pentru a seta perioada de timp exactă.

Când cursorul setransformaîn , puteți prelungi sau scurta bara de timp selectată.

6. Opțional, puteți selecta bara de timp pentru programare,

și apoi faceți clic**Șterge durata**pentru a șterge bara de timp selectată sau faceți

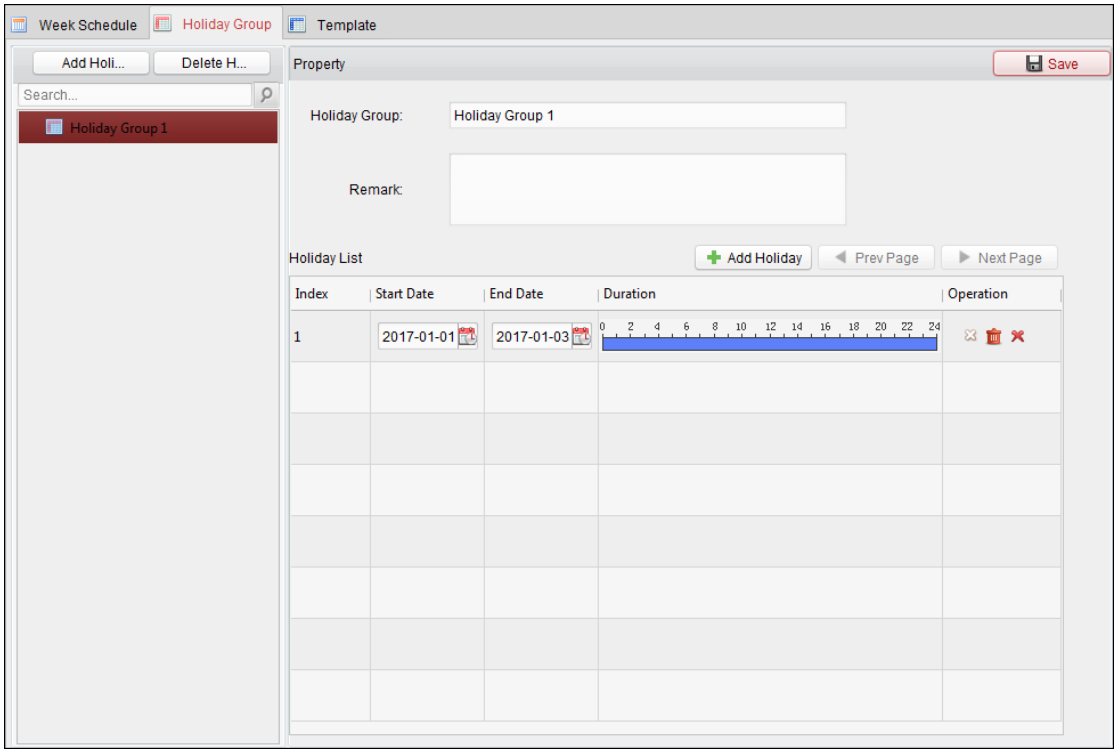
clic**clar**pentru a șterge toate barele de timp,

sau faceți clic**Copiați în Săptămâna**pentru a copia setările barei de timp în întreaga săptămână.

7. Faceți clic**Salvați**pentru a salva setările.

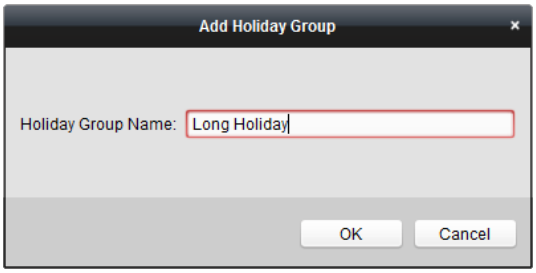
7.6.2 Grup de vacanță

Clic**Grup de vacanță**pentru a intra în interfața de gestionare a grupului de vacanță.



Pași:

1. Faceți clic**Adăugați un grup de vacanță**butonul din stânga pentru a deschide interfața pentru adăugarea grupului de vacanță.



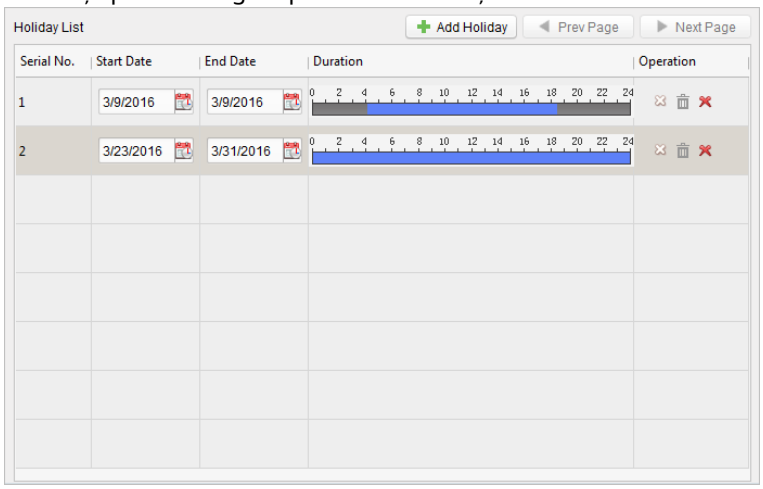
2. Introduceți numele grupului de vacanță în textul depus și faceți clic OK butonul pentru a adăuga grupul de vacanță.

3. Selectați grupul de vacanță adăugat și puteți edita numele grupului de vacanță și puteți introduce observația

informație.

4. Faceți clic**Adăugați vacanță**pictograma din dreapta pentru a adăuga o perioadă de vacanță la lista de vacanțe și a configura durata vacanței.

Notă:La un grup de vacanțe pot fi adăugate până la 16 vacanțe.



1) În programul perioadei, faceți clic și trageți pentru a desena perioada, ceea ce înseamnă că în acea perioadă de timp este activată permisiunea configurată.

Notă:Pot fi setate până la 8 durate de timp pentru fiecare perioadă din program.

2) Când cursorul se transforma în , puteți muta bara de timp selectată pe care tocmai ați editat-o. De asemenea, puteți edita punctul de timp afișat pentru a seta perioada de timp exactă.

3) Când cursorul se întoarce în , puteți prelungi sau scurta bara de timp selectată.

4) Opțional, puteți selecta bara de timp a programului,

și apoi faceți clic pentru a șterge bara de timp selectată,

sau faceți clic pentru a șterge toate barele de timp ale vacanței,

sau faceți clic pentru a șterge direct vacanța.

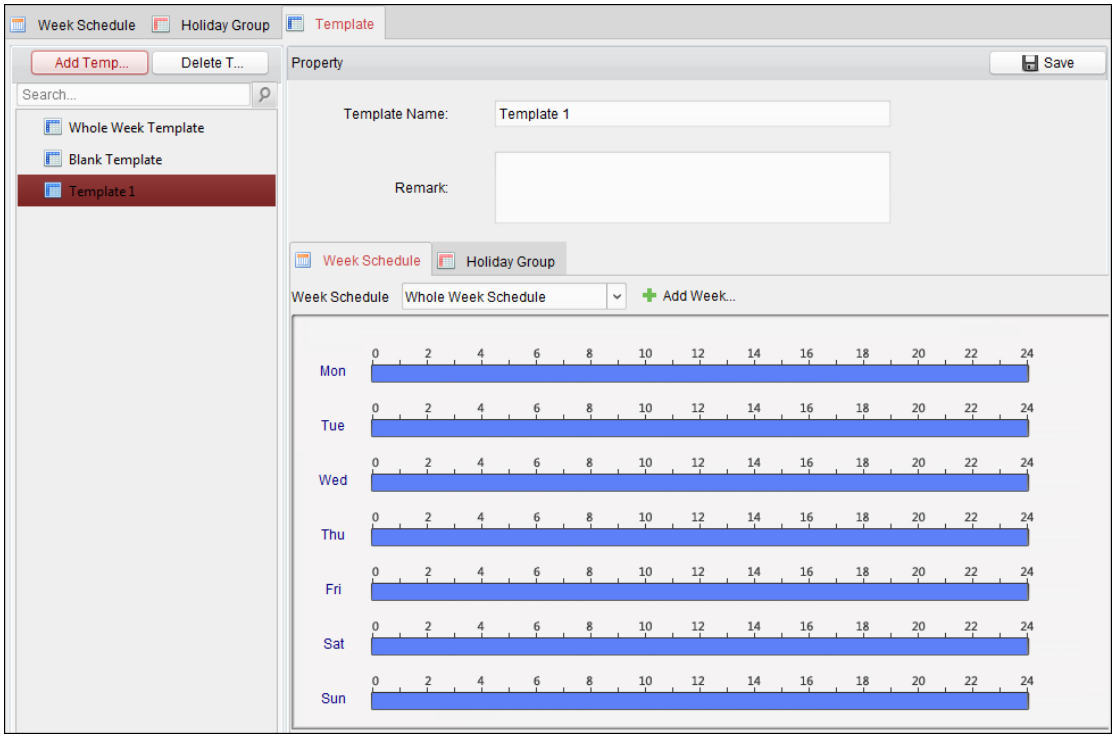
5. Faceți clic**Salvați**pentru a salva setările.

Notă:Sărbătorile nu pot fi suprapuse între ele.

7.6.3 Șablon

După setarea programului săptămânal și a grupului de vacanță, puteți configura șablonul care conține programul săptămânal și programul grupului de vacanță.

Notă:Prioritatea programului de grup de vacanță este mai mare decât programul săptămânal. Clic**Șablon**pentru a intra în interfața de gestionare a șabloanelor.



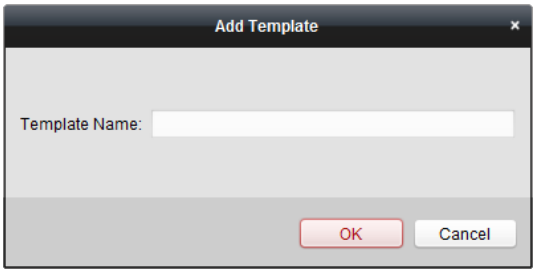
Există două șabloane predefinite în mod implicit:**Șablon pentru întreaga săptămână**și**Șablon gol**, care nu poate fi șters și editat.

- **Șablon pentru întreaga săptămână:**Glisarea cardului este valabilă în fiecare zi a săptămânii și nu are program de grup de vacanță.
- **Șablon gol:**Glisarea cardului este invalidă în fiecare zi a săptămânii și nu are program de grup de vacanță.

Puteți defini șabloane personalizate la cererea dvs.

Pași:

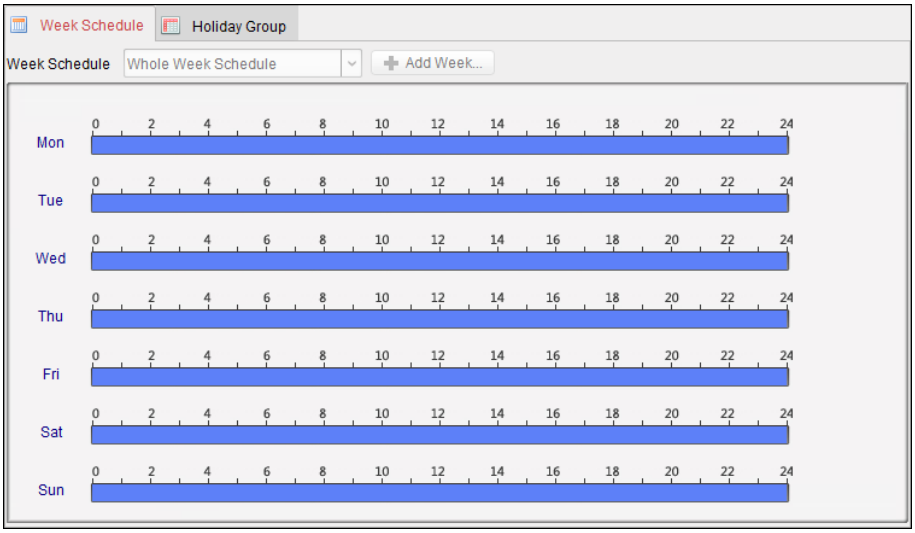
1. Faceți clic**Adăugați șablon**pentru a deschide interfața de adăugare a șablonului.



2. Introduceți numele șablonului în textul înregistrat și faceți clic**Bine**butonul pentru a adăuga șablonul.
3. Selectați șablonul adăugat și puteți edita proprietatea acestuia din dreapta. Puteți edita numele șablonului și puteți introduce informațiile despre observație.
4. Selectați un program săptămânal pentru a aplica programului.

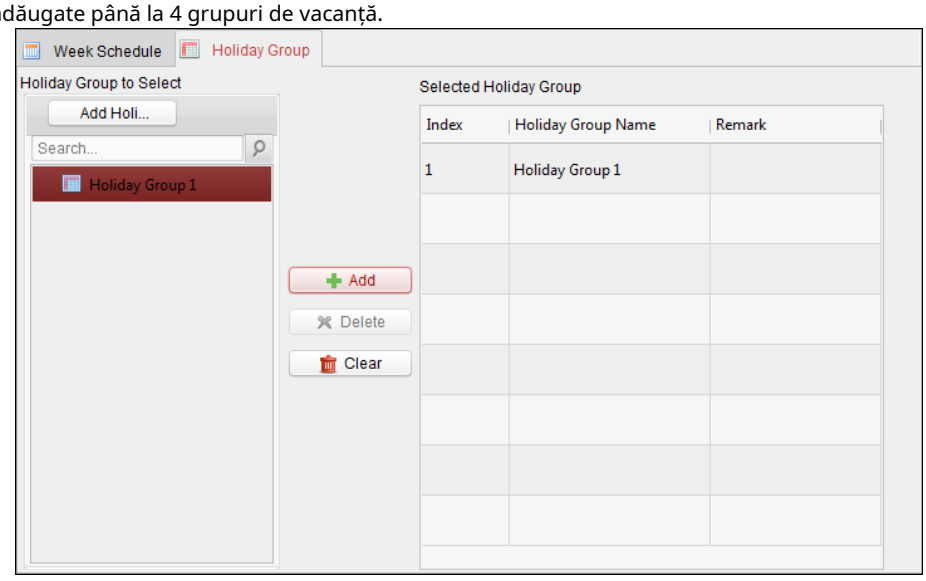
   Clic**Programul săptămâniifila și selectați un program din lista verticală.**

   De asemenea, puteți face clic**Adăugați programul săptămâniipentru a adăuga un nou program de săptămână. Pentru detalii, consultați***Capitolul 7.6.1 Program săptămânal.*



5. Selectați grupurile de vacanță pentru a aplica programului.

Notă: Pot fi adăugate până la 4 grupuri de vacanță.



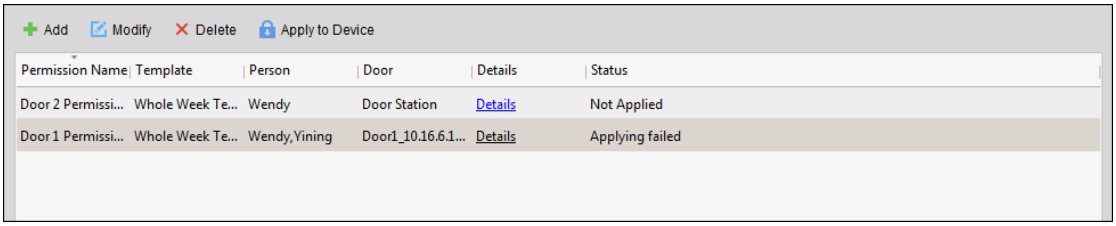
Faceți clic pentru a selecta un grup de vacanță din listă și faceți clic **Adăuga** pentru a-l adăuga la șablon. De asemenea, puteți face clic **Adăugați un grup de vacanță** pentru a adăuga unul nou. Pentru detalii, consultați *Capitolul 7.6.2 Grup de vacanță.* Puteți face clic pentru a selecta un grup de vacanță adăugat în lista din dreapta și faceți clic **Șterge** pentru a-l șterge. Puteți da clic **clar** pentru a șterge toate grupurile de vacanță adăugate.

6. Faceți clic **Salvați** butonul pentru a salva setările.

7.7 Configurarea permisiunii

În modulul de configurare a permisiunii, puteți adăuga, edita și șterge permisiunea de control al accesului, apoi puteți aplica setările de permisiuni pe dispozitiv pentru a intra în vigoare.

Faceți clic pe pictograma pentru a intra în interfața de permisiuni de control acces.

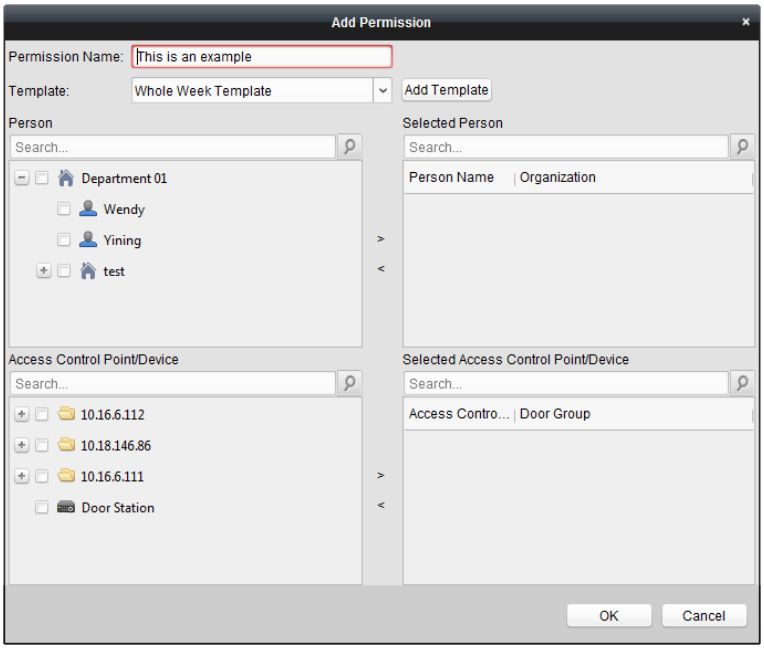


7.7.1Adăugarea permisiunii

Scop:

Puteți acorda permisiunea persoanelor de a intra/existe punctele de control acces (uși) în această secțiune. ***Pași:***

1. Faceți clic**Adăuga**pictograma pentru a intra în următoarea interfață.



2.În câmpul Nume permisiunea, introduceți numele permisiunii, după cum doriți.

3. Faceți clic pe meniul derulant pentru a selecta un șablon pentru permisiune.

Notă:Ar trebui să configurați șablonul înainte de setările de permisiuni. Puteți da clic**Adăugați șablon** pentru a adăuga șablonul. A se referi la*Capitolul 7.6 Program și șablon*pentru detalii.

4. În lista de persoane, se afișează toate persoanele adăugate.

Bifați casetele de selectare pentru a selecta persoane și faceți clic**>**pentru a adăuga la lista de persoane selectate. (Opțional) Puteți selecta persoana din lista Persoane selectate și faceți clic**<**pentru a anula selecția.

5. În lista Punct de control acces/Dispozitiv, se vor afișa toate punctele de control acces (ușile) și stațiile de ușă adăugate.

Bifați casetele de selectare pentru a selecta ușile sau stațiile de ușă și faceți clic**>**pentru a adăuga la lista selectată. (Opțional) Puteți selecta ușa sau stația de ușă din lista selectată și faceți clic**<**pentru a anula selecția.

6. Faceți clic**Bine**butonul pentru a finaliza adăugarea permisiunii. Persoana selectată va avea permisiunea de a intra/ieși din ușa/stația de ușă selectată cu cardul(ele) sau amprentele digitale asociate.

7. (Opțional) după adăugarea permisiunii, puteți face clic**Detalii**să-l modifice. Sau puteți selecta

permisiunea și faceți clic**Modifica**a modifica.

Puteți selecta permisiunea adăugată din listă și faceți clic**Șterge**pentru a-l șterge.

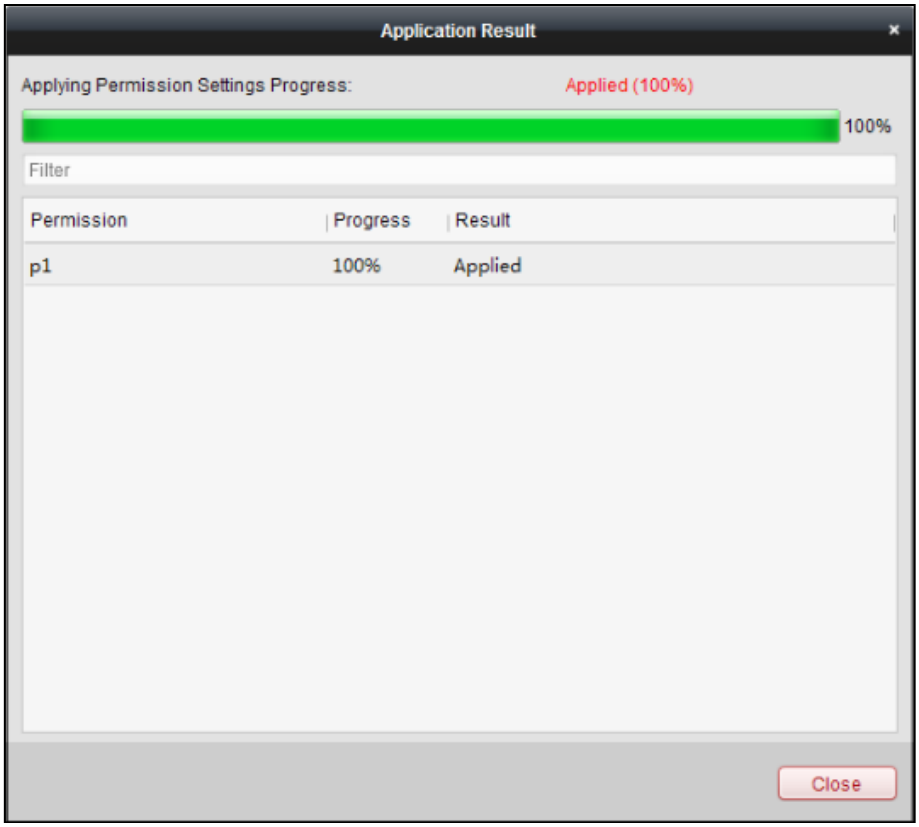
7.7.2 Aplicarea permisiunii

Scop:

După configurarea permisiunilor, ar trebui să aplicați permisiunea adăugată dispozitivului de control al accesului pentru a intra în vigoare.

Pași:

1. Selectați permisiunea (permisiunile) de aplicat dispozitivului de control al accesului. Pentru a selecta mai multe permisiuni, poți ține tasta *Ctrl* sau *Alt* și selectați permisiunile.
2. Faceți clic**Aplicați pe dispozitiv**pentru a începe aplicarea permisiunii selectate la dispozitivul de control al accesului sau la stația de ușă.
3. Va apărea următoarea fereastră, indicând rezultatul aplicării permisiunii.



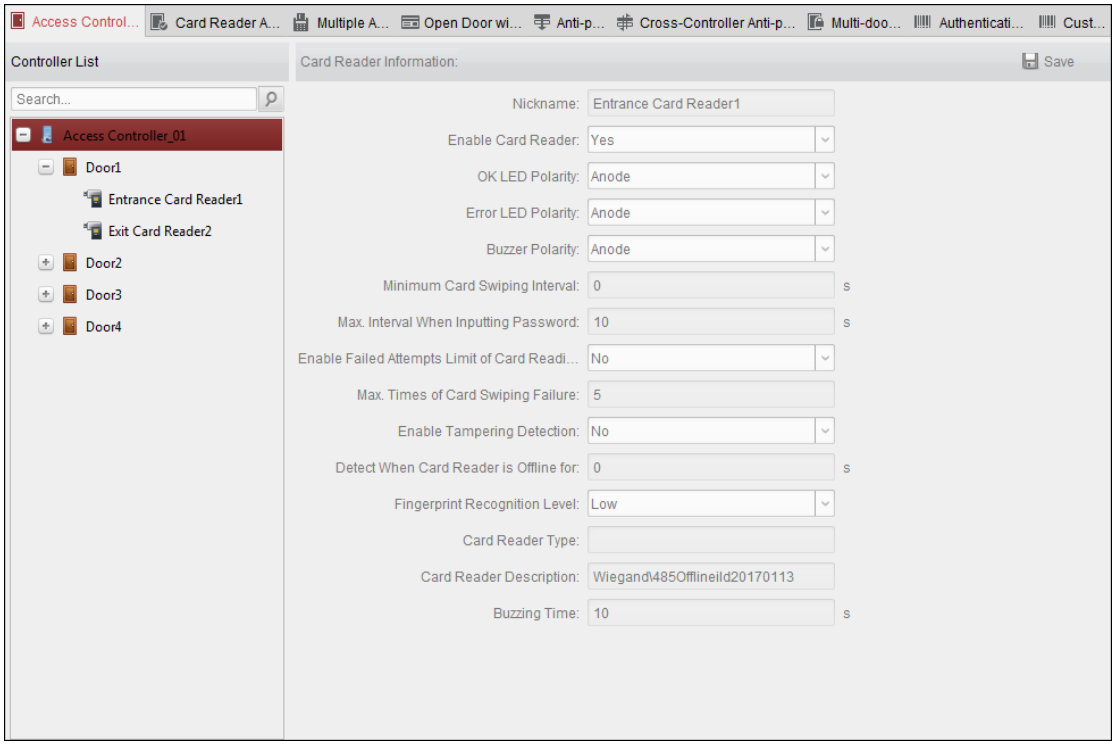
7.8 Funcții avansate

Scop:

După ce configurați persoana, șablonul și permisiunea de control al accesului, puteți configura funcțiile avansate ale aplicației de control al accesului.

Notă:Funcțiile avansate ar trebui să fie acceptate de dispozitiv.

Faceți clic pe pictograma  pentru a intra în următoarea interfață.



7.8.1 Parametrii de control al accesului

Scop:

După ce configurați persoana, șablonul și permisiunea de control al accesului, puteți configura funcțiile avansate ale aplicației de control al accesului.

Clic**Parametrii de control al accesului**pentru a intra în interfața de setări a parametrilor.

Parametrii ușii

Pași:

1. În lista de controlere din stânga, faceți clic pe pentru a extinde dispozitivul de control acces, selectați ușa (punct de control acces) și puteți edita informațiile ușii selectate din dreapta.
2. Puteți edita următorii parametri:

   Ușă magnetică: Ușa Magnetică este în starea de**Rămâi închis**(cu excepția condițiilor speciale).

   Tip buton de ieșire: Tipul butonului de ieșire este în starea de**Rămâi deschis**(cu excepția condițiilor speciale).

   Ușa Încuiată Timp: După ce glisați cardul normal și acțiunea releului, temporizatorul pentru blocarea ușii începe să funcționeze.

   Durata deschiderii ușii cu cardul pentru deschiderea extinsă a ușii:Ușa magnetică poate fi activată cu întârziere corespunzătoare după ce titularul cardului glisează cardul.

   Alarmă de expirare a ușii deschise: Alarma poate fi declanșată dacă ușa nu a fost închisă **Activați încuierea ușii când ușa este închisă (rezervat)**: Ușa poate fi blocată odată ce este închisă, chiar dacă nu este atins Timpul de blocare a ușii.

   Codul de constrângere: Ușa se poate deschide prin introducerea codului de constrângere atunci când există constrângere. La acelasi

timp, clientul poate raporta evenimentul de constrângere.

Super Parolă: Persoana specifică poate deschide ușa introducând superparola. **Cod de respingere:** Introduceți codul de respingere pentru a opri semnalul sonor al cititorului de carduri. ***Note:***

- Codul de constrângere, parola super și codul de respingere ar trebui să fie diferite.
- Codul de constrângere, super parola și codul de respingere ar trebui să fie diferite de parola de autentificare.
- Codul de constrângere, parola super și codul de respingere ar trebui să conțină 4 până la 8 cifre.

3. Faceți clic**Salvați**butonul pentru a salva parametrii.

Parametrii cititorului de carduri

Pași:

1. În lista de dispozitive din stânga, faceți clic pe pentru a extinde ușa, selectați numele cititorului de carduri și dvs poate edita parametrii cititorului de carduri din dreapta.
2. Puteți edita următorii parametri: **Poreclă:**Editați numele cititorului de carduri după cum doriți. **Activați cititorul de carduri:**Selectați**da** pentru a activa cititorul de carduri.

   Polaritate LED OK: Selectați polaritatea LED-ului OK a plăcii de bază a cititorului de carduri. **Polaritate LED de eroare:**Selectați polaritatea LED-ului de eroare a plăcii de bază a cititorului de carduri. **Polaritatea soneriei:**Selectați Polaritatea LED-ului Buzzer de pe placa de bază a cititorului de carduri.

   Interval minim de trecere a cardului: Dacă intervalul dintre trecerea cardului cu același card este mai mic decât valoarea setată, trecerea cardului este invalidă. Îl puteți seta de la 0 la 255.

   Max. Interval la introducerea parolei:Când introduceți parola pe cititorul de carduri, dacă intervalul dintre apăsarea a două cifre este mai mare decât valoarea setată, cifrele pe care le-ați apăsat înainte vor fi șterse automat.

   Activați Limita încercărilor eșuate de citire a cardului: Activați pentru raportarea alarmei atunci când încercările de citire a cardului ating valoarea setată.

   Max. Perioadele de eșec la trecerea cardului: Setați valoarea maximă. încercări eșuate de citire a cardului. **Activați detectarea falsificării:**Activați detectarea anti-manipulare pentru cititorul de carduri. ***Notă:***Pentru controlerul de acces seria DS-K2800, funcția nu este încă acceptată.

   Detectați când cititorul de carduri este offline pentru:Când dispozitivul de control al accesului nu se poate conecta la cititorul de carduri mai mult decât timpul stabilit, cititorul de carduri se va opri automat. ***Notă:*** Pentru controlerul de acces seria DS-K2800, funcția nu este încă acceptată.

   Timp de zgomot: Setați timpul de sunet al cititorului de carduri. Timpul disponibil variază de la 0 la 5999 de secunde. 0 reprezintă bâzâit continuu.

   Descrierea cititorului de carduri: Citiți descrierea cititorului de carduri.
3. Faceți clic pe**Salvați**butonul pentru a salva parametrii.

7.8.2 Autentificare cititor de carduri

Scop:

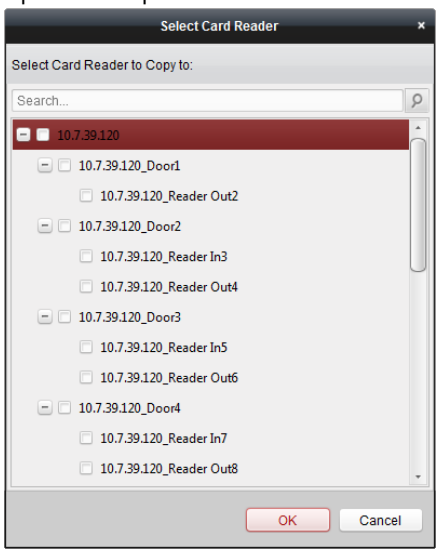
Puteți seta regulile de trecere pentru cititorul de carduri al dispozitivului de control al accesului.

Pași:

1. Faceți clic**Autentificare cititor de carduri**fila și selectați un cititor de carduri din stânga.
2. Selectați un mod de autentificare a cititorului de carduri. Modurile de autentificare disponibile depind de tipul de cititor de carduri:
   - **Card și Parolă**: Ușa se poate deschide atât prin introducerea parolei cardului, cât și prin glisarea cardului.
     Notă:Aici parola se referă la parola setată la emiterea cardului persoanei. *Capitolul 7.5.2 Managementul persoanelor.*
   - **Card sau parola de autentificare**: Ușa se poate deschide introducând autentificarea parola sau trecerea cardului.
     Notă:Aici parola de autentificare se referă la parola setată pentru deschiderea ușii. A se referi la *Capitolul 7.8.5 Parola de autentificare.* **Card**: Ușa se poate deschide doar prin glisarea cardului.
   -
3. Faceți clic și trageți mouse-ul într-o zi pentru a desena o bară de culoare pe program, ceea ce înseamnă că în acea perioadă de timp, autentificarea cititorului de carduri este valabilă.
4. Repetați pasul de mai sus pentru a seta alte perioade de timp.

   Sau puteți selecta o zi configurată și faceți clic**Copiați în Săptămâna**butonul pentru a copia aceleași setări în întreaga săptămână.

   (Opțional) Puteți face clic**Șterge**butonul pentru a șterge perioada de timp selectată sau faceți clic**clar**butonul pentru a șterge toate perioadele de timp configurate.
5. (Opțional) Faceți clic**Copiaza in**butonul pentru a copia setările în alte cititoare de carduri.



6. Faceți clic**Salvați**butonul pentru a salva parametrii.

7.8.3 Deschideți ușa cu primul card

Scop:

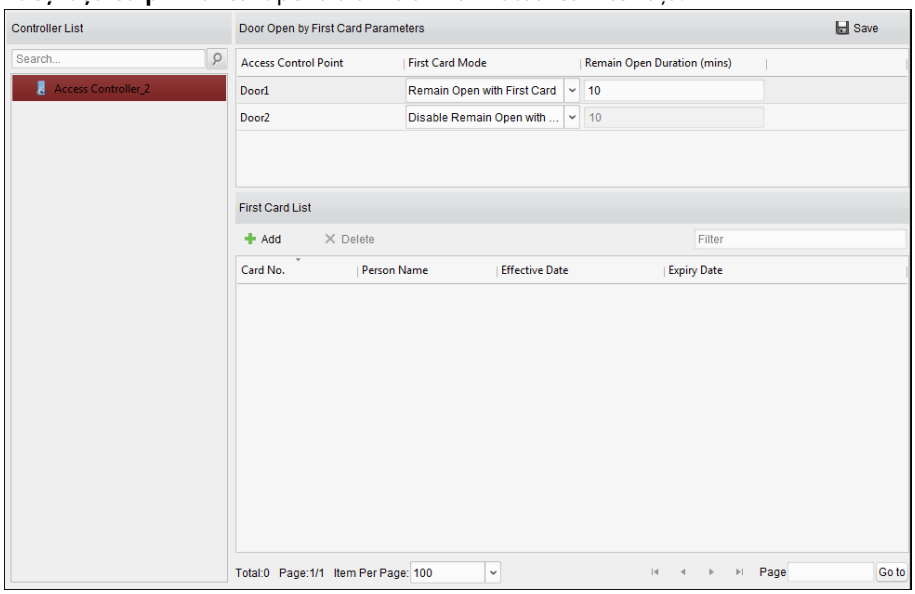
Puteți seta mai multe prime carduri pentru un punct de control al accesului. După prima trecere a cardului, permite accesul mai multor persoane la ușă sau alte acțiuni de autentificare. Primul mod de card conține Rămâne deschis cu primul card, Dezactivare Rămâne deschis cu primul card și Autorizarea primului card.

Rămâi deschis cu primul card:Ușa rămâne deschisă pentru durata de timp configurată după trecerea primului card până când se încheie durata de rămâne deschisă.

Prima autorizare cu card: Toate autentificările, cu excepția autentificărilor supercard, cardului de constrângere și codului de constrângere, sunt permise numai după prima autorizare a cardului.

Pași:

1. Faceți clic**Deschideți ușa cu primul card**pentru a intra în următoarea interfață.

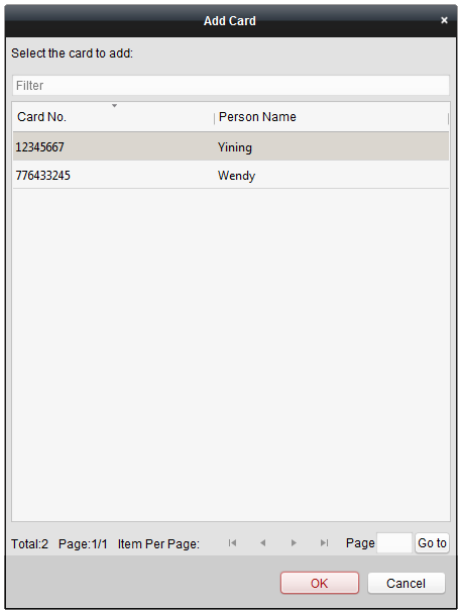


2. Selectați un dispozitiv de control al accesului din lista din stânga.
3. Selectați primul mod card din lista derulantă pentru punctul de control acces.
4. (Opțional) Dacă selectați Rămâne deschis cu primul card, ar trebui să setați durata de a rămâne deschis.

Note:

- Durata rămâne deschisă ar trebui să fie între 0 și 1440 de minute. În mod implicit, este de 10 minute.
- În modul First Card Authorization, puteți accesa ușa când glisați super cardul, cardul de constrângere sau introduceți codul de constrângere fără a glisa primul card.
- Puteți glisa din nou primul card pentru a dezactiva modul primul card.
- Prima autorizare a cardului este valabilă numai în ziua curentă. Autorizația va fi expirată după ora 24:00 în ziua curentă.

5. În lista First Card, Faceți clic**Adăuga**butonul pentru a deschide următoarea casetă de dialog.



1) Selectați cărțile de adăugat ca primă carte pentru ușă

Notă: Vă rugăm să setați permisiunea cardului și să aplicați mai întâi setarea de permisiuni la dispozitivul de control al accesului. Pentru detalii, consultați *Capitolul 7.7 Configurarea permisiunilor.*

2) Faceți clic **Bine** butonul pentru a salva adăugarea cardului.

6. Puteți face clic **Șterge** butonul pentru a elimina cardul din prima listă de carduri.

7. Faceți clic **Salvați** pentru a salva și a intra în vigoare noile setări.

7.8.4 Anti-Passing Back

Scop:

Puteți seta anti-passing back pentru cititoarele de carduri în același controler de acces. Ar trebui să glisați cardul în funcție de traseul configurat pentru cardul de glisare. Și doar o singură persoană putea trece de punctul de control al accesului după ce glisează cardul.

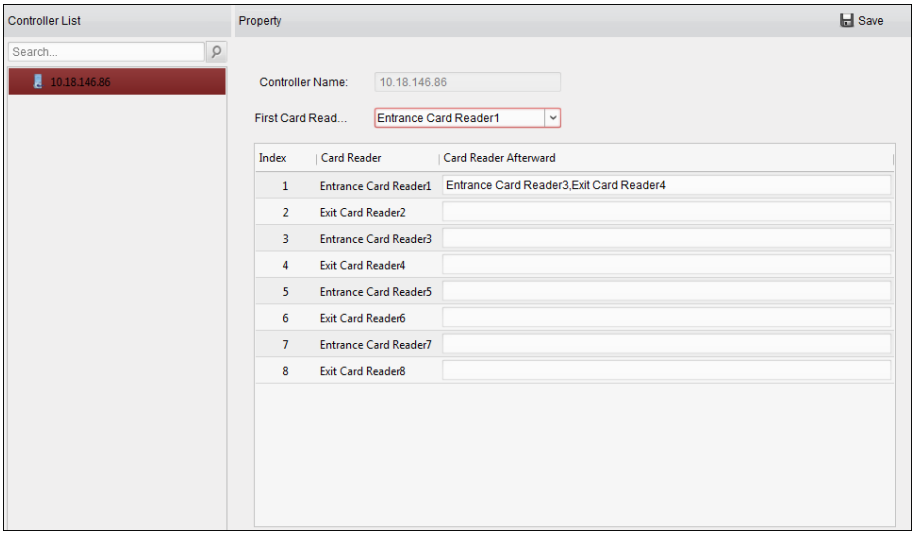
Note:

- Fie funcția anti-trecere în spate, fie funcția de interblocare cu mai multe uși pot fi configurate în același timp pentru un dispozitiv de control al accesului.
- Ar trebui să activați mai întâi funcția anti-retorcare pe dispozitivul de control al accesului.

Setarea căii de glisare a cardului (Ordinea cititorului de carduri)

Pași:

1. Faceți clic **Anti-trecerea înapoi** pentru a intra în următoarea interfață.

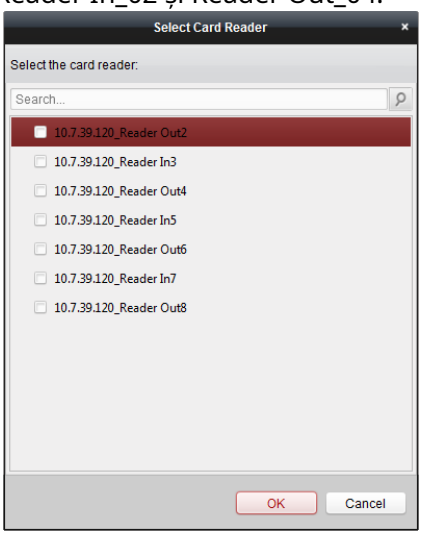


2. Selectați un dispozitiv de control al accesului din lista de dispozitive din stânga.

3. În câmpul First Card Reader, selectați cititorul de carduri ca început al căii.

4. În listă, faceți clic pe textul arhivat de**Cititor de carduri După aceea**și selectați cititoarele de carduri conectate.

Exemplu:Dacă selectați Reader In_01 ca început și selectați Reader In_02, Reader Out_04 ca cititoare de carduri conectate. Apoi, puteți trece prin punctul de control al accesului doar glisând cardul în ordinea Reader In_01, Reader In_02 și Reader Out_04.



Notă:Ulterior pot fi adăugate până la patru cititoare de carduri pentru un cititor de carduri.

5. (Opțional) Puteți intra din nou în caseta de dialog Select Card Reader pentru a edita ulterior cititoarele de carduri.

6. Faceți clic**Salvați**pentru a salva și a intra în vigoare noile setări.

7.8.5 Parola de autentificare

Scop:

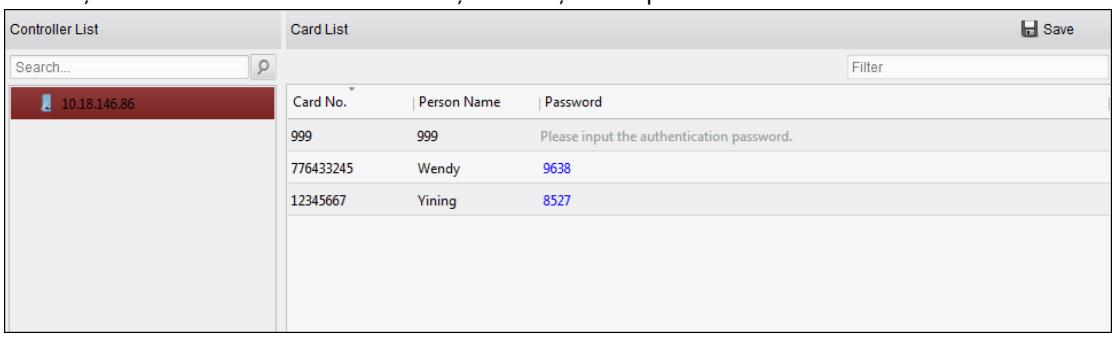
Puteți deschide ușa introducând parola de autentificare pe tastatura cititorului de carduri după terminarea operațiunii de setare a parolei de autentificare.

Note:

- Această funcție de parolă de autentificare este valabilă numai în timpul programărilor când modul de autentificare a cititorului de carduri pentru dispozitivul de control acces este setat ca**Card sau parola de autentificare**. Pentru detalii, vă rugăm să consultați*Capitolul 7.8.2 Autentificarea cititorului de carduri.* Această funcție ar trebui să fie suportată de
- dispozitivul de control al accesului.

Pași:

1. Faceți clic**Parola de autentificare**fila și selectați un dispozitiv de control al accesului din listă.



Vor fi afișate toate cardurile și persoanele care au fost aplicate pe dispozitiv.

Notă:Pentru setarea și aplicarea permisiunilor dispozitivului, consultați*Capitolul 7.7 Configurarea permisiunilor.*

2. Faceți clic pe **Parola** cardului și introduceți parola de autentificare pentru card. ***Notă:*** Parola de autentificare trebuie să conțină 4 până la 8 cifre.
3. După setarea parolei de autentificare, funcția de parolă de autentificare a cardului va fi activat implicit.
4. (Opțional) Puteți introduce cuvintele cheie ale Nr. card, numele persoanei sau parola de autentificare pentru a căuta.

Note:

- La un dispozitiv de control acces pot fi adăugate până la 500 de carduri cu parolă de autentificare. Parola
- ar trebui să fie unică și nu poate fi aceeași cu parola super, codul de constrângere și codul de respingere din parametrii de control al accesului.

7.8.6 Wiegand personalizat

Scop:

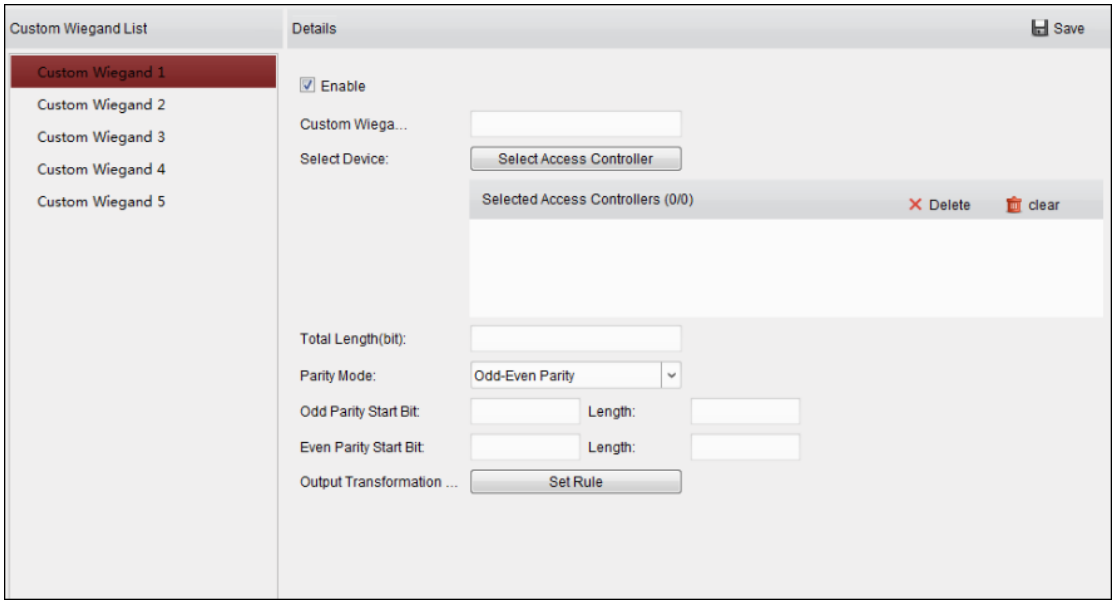
Pe baza cunoștințelor regulii de încărcare pentru Wiegand terță parte, puteți seta mai multe protocoale Wiegand personalizate pentru a comunica între controler și cititoarele de carduri terță parte.

Inainte sa incepi:

Conectați cititoarele de carduri terță parte la controler.

Pași:

1. Faceți clic**Wiegand personalizat**pentru a intra în fila Custom Wiegand.



2. Selectați un wiegand personalizat din stânga interfeței.

3. Verificați**Permite**casetă de selectare pentru a activa Wiegand personalizat.

4. Setați numele wiegand.

5. Selectați dispozitivul.

1) Faceți clic**Selecteaza dispozitivul**.

2) Selectați dispozitivul care trebuie să utilizeze Wiegand personalizat.

3) Faceți clic **OK** pentru a salva setările.

6. Introduceți lungimea totală și selectați modul de paritate din lista verticală.

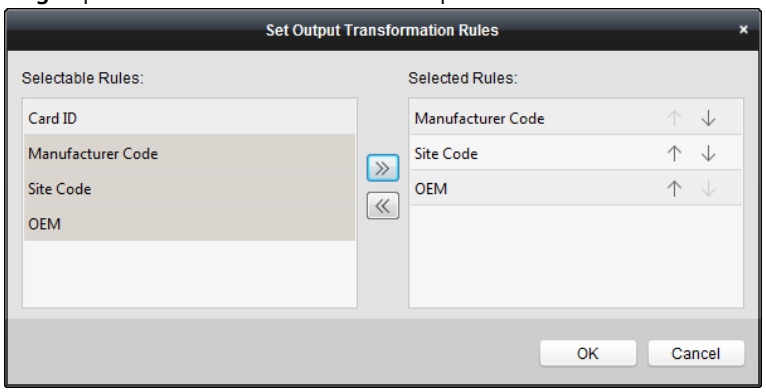
Dacă selectați Odd-Even Parity, ar trebui să setați bitul de început al parității impare, lungimea parității impare, bitul de început al parității par și lungimea parității par.

Dacă selectați XOR Parity, ar trebui să setați bitul de pornire al parității XOR, lungimea per grup și lungimea totală.

Dacă selectați Niciunul, nu este nevoie să setați modul de paritate.

7. Setați regula de transformare a ieșirii.

1) Faceți clic**Setează o regulă**pentru a deschide fereastra Set Output Transformation Rules.



2) Selectați regulile din lista din stânga.

Notă:apasă pe*Schimb*tasta pentru a selecta mai multe reguli.

3) Faceți clic pentru a muta regulile selectate în lista din dreapta.

4) (Opțional) Faceți clic pe sau pentru a schimba ordinea regulilor.

5) (Opțional) Selectați regulile din lista Reguli selectate și faceți clic pe pentru a elimina regula din lista din dreapta.

6) Faceți clic **OK** pentru a salva setările.

7) În fila Custom Wiegand, setați bitul de început al regulii, lungimea și cifra zecimală.

8. Faceți clic**Salvați**în colțul din dreapta sus al interfeței pentru a salva setările.

Note:

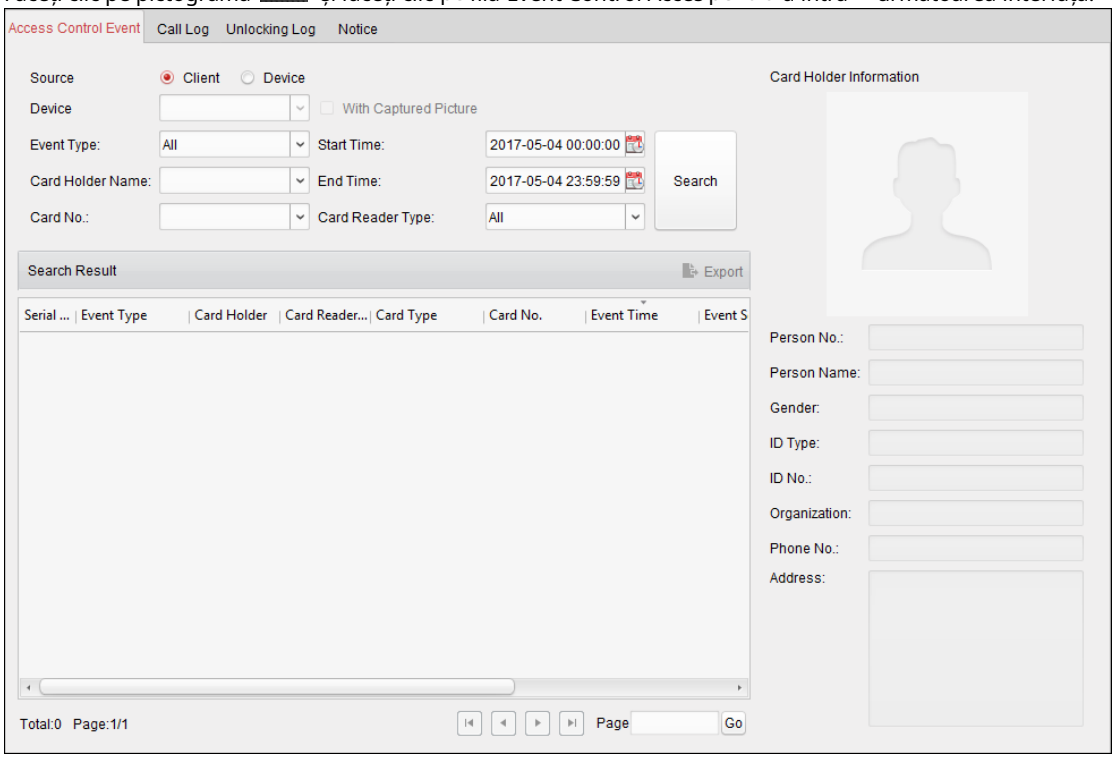
- În mod implicit, dispozitivul dezactivează funcția personalizată Wiegand.
- Dacă dispozitivul activează funcția wiegand personalizată, toate interfețele wiegand din dispozitiv vor folosi protocolul wiegand personalizat.
- Pot fi setate până la 5 wiegand-uri personalizate.
- Sunt permise până la 32 de caractere în numele wiegand personalizat. Până
- la 80 de biți sunt disponibili în lungimea totală.
- Bitul de pornire al parității impare, lungimea parității impare, bitul de pornire al parității par și lungimea parității par sunt cuprinse între 1 și 80 de biți.
- Bitul de pornire al ID-ului cardului, codul producătorului, codul site-ului și OEM-ul ar trebui să varieze de la 1 la 80 de biți.
- Pentru detalii despre wiegand personalizat, consultați Anexa.

7.9 Căutarea evenimentului de control acces

Scop:

Puteți căuta evenimentele din istoricul controlului accesului, inclusiv evenimentul de excepție al dispozitivului, evenimentul ușii, intrarea alarmei și evenimentul cititorului de carduri.

Faceți clic pe pictograma și faceți clic pe fila Event Control Acces pentru a intra în următoarea interfață.



Pași:

1. Selectați sursa.

   Puteți selecta Client sau Dispozitiv.

2. Introduceți condiția de căutare (sursă, tipul evenimentului/numele titularului cardului/numărul cardului/capturarea/ora de începere și sfârșit).

3. Faceți clic**Căutare**pentru a obține rezultatele căutării.

4. Vizualizați informațiile despre eveniment în lista de evenimente.

5. Faceți clic pe un eveniment pentru a vedea informațiile deținătorului cardului pe**Informații despre titularul cardului**panoul din partea stângă a paginii.

6. Puteți face clic**Export**butonul pentru a exporta rezultatele căutării pe computerul local.

7.10 Configurare eveniment control acces

Scop:

Pentru dispozitivul de control al accesului adăugat, puteți configura legătura de control al accesului, inclusiv legătura evenimentului de control al accesului, legătura intrării alarmei de control acces, legătura cardului de evenimente și legătura între dispozitive.

Apasă pe  pictograma de pe panoul de control,

sau faceți clic**Instrument**->**Management de evenimente**pentru a deschide pagina de gestionare a evenimentelor.

7.10.1 Legătura evenimentelor pentru controlul accesului

Scop:

Puteți atribui acțiuni de conectare evenimentului de control acces prin stabilirea unei reguli. De exemplu, când este detectat evenimentul de control al accesului, apare un avertisment sonor sau au loc alte acțiuni de conectare.

Notă:Legătura aici se referă la conectarea acțiunilor proprii ale software-ului client. ***Pași:***

1. Faceți clic pe**Eveniment de control al accesului**fila.

2. Dispozitivele de control al accesului adăugate se vor afișa în panoul Dispozitiv de control al accesului din stânga. Selectați dispozitivul de control al accesului sau intrarea de alarmă sau punctul de control al accesului (uşă) sau cititorul de carduri pentru a configura legătura evenimentului.

3. Selectați tipul de eveniment pentru a seta legătura.

4. Selectați camera declanșată. Imaginea sau videoclipul de la camera declanșată va apărea când are loc evenimentul selectat.

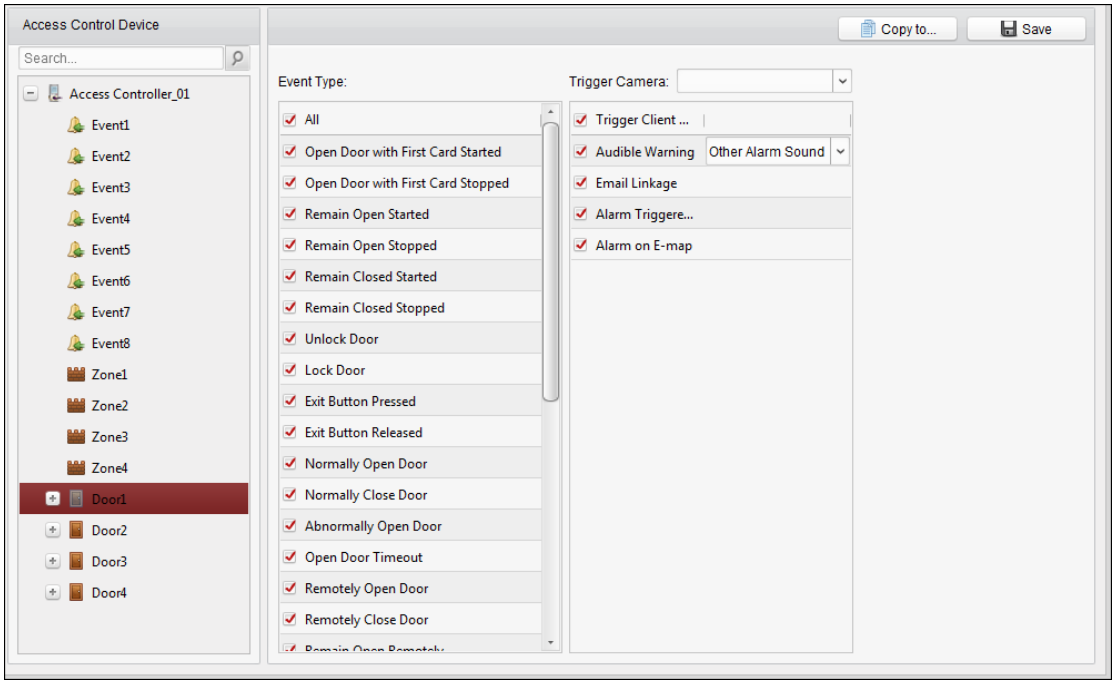
   Pentru a captura imaginea camerei declanșate atunci când are loc evenimentul selectat, puteți seta, de asemenea, programul de captură și stocarea în Program de stocare.

5. Bifați casetele de selectare pentru a activa acțiunile de conectare. Pentru detalii, consultați*Tabelul 14.1 Acțiuni de conectare pentru evenimentul de control al accesului*.

6. Faceți clic**Salvați**pentru a salva setările.

7. Puteți face clic pe butonul Copiere în pentru a copia evenimentul de control al accesului pe alt dispozitiv de control al accesului, intrare de alarmă, punct de control acces sau cititor de carduri.

   Selectați parametrii pentru copiere, selectați ținta în care să copiați și faceți clic OK pentru a confirma.



Tabelul 1. 1 Acțiuni de conectare pentru evenimentul de control acces

Acțiuni de legătură	Descrieri
Avertizare sonoră	Software-ul client emite un avertisment sonor atunci când alarma este declanșată. Puteți selecta sunetul alarmei pentru avertizare sonoră.
Legătura de e-mail	Trimiteți o notificare prin e-mail cu informațiile de alarmă către unul sau mai mulți receptori.
Alarma pe hartă electronică	Afișați informațiile despre alarmă pe E-harta. ***Notă:***Această legătură este disponibilă numai pentru a accesa punctul de control și intrarea alarmei.
Alarma declanșată Imagine pop-up	Imaginea cu informații despre alarmă apare când alarma este declanșată.

7.10.2 Conexiune intrare alarmă control acces

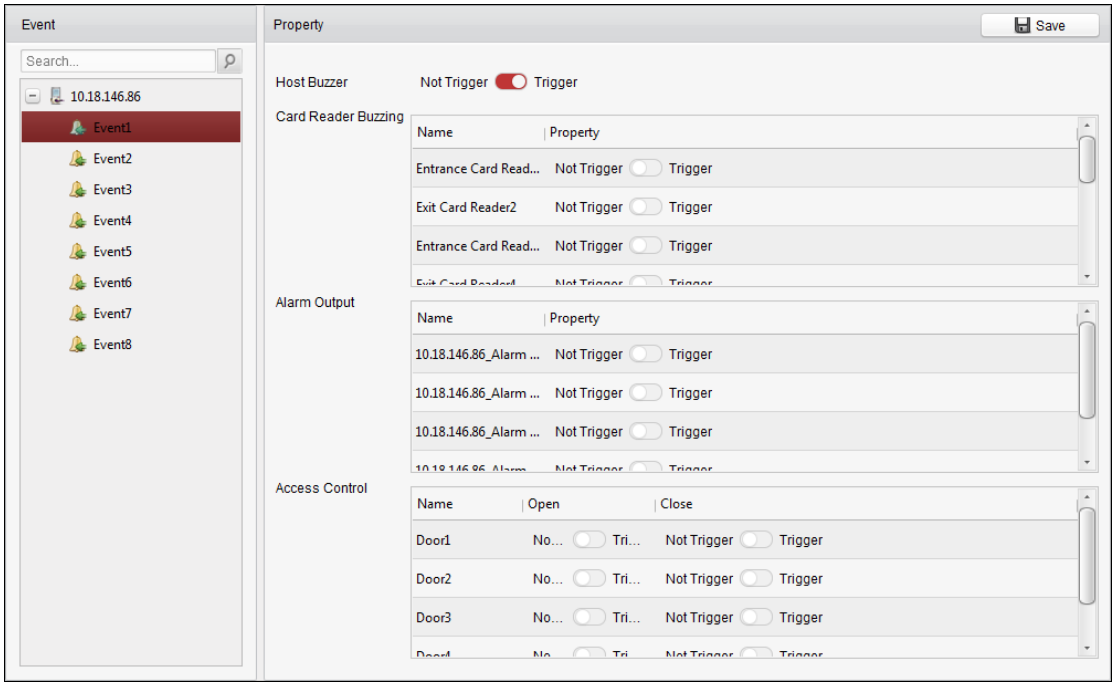
Scop:

Intrările de alarmă pentru controlul accesului pot fi legate de unele acțiuni (de exemplu, ieșire de alarmă, sonerie gazdă) atunci când este declanșată.

Notă:Legătura aici se referă la conectarea acțiunilor proprii ale software-ului client.

Pași:

1. Faceți clic**Intrare alarmă control acces**pentru a intra în următoarea interfață.



2. În lista de evenimente din stânga, selectați o intrare de alarmă.

3. Comutați proprietatea de la la  pentru a activa această acțiune.

Gazdă Buzzer: Avertismentul sonor al controlerului va fi declanșat. **Buzzer pentru cititor de carduri**: Avertismentul sonor al cititorului de carduri va fi declanșat. **Ieșire de alarmă**: Ieșirea de alarmă va fi declanșată pentru notificare.

Punct de control acces (Deschis/Închidere): Ușa va fi deschisă sau închisă atunci când carcasa este declanșată. ***Notă:***Ușa nu poate fi configurată ca deschisă sau închisă în același timp.

4. Faceți clic**Salvați**butonul pentru a salva setările.

7.10.3 Conectare card de eveniment

Clic**Conectare card de eveniment**pentru a intra în următoarea interfață.

Note:

- Conectarea cardului de evenimente ar trebui să fie acceptată de dispozitiv.
- Legătura aici se referă la conectarea acțiunilor proprii ale software-ului client.

Selectați dispozitivul de control al accesului din lista din stânga.

Clic**Adăuga**butonul pentru a adăuga o nouă legătură. Puteți selecta sursa evenimentului ca**Legătura evenimentului**sau**Conectarea cardului**.

Legătura evenimentului

Pentru conectarea evenimentului, evenimentul de alarmă poate fi împărțit în patru tipuri: eveniment dispozitiv, intrare alarmă, eveniment ușă și eveniment cititor de carduri.

Pași:

1. Faceţi clic pentru a selecta tipul de legătură ca**Legătura evenimentului**și selectați tipul de eveniment din meniul drop-down listă.

-Pentru Eveniment dispozitiv, selectați tipul de eveniment detaliat din lista verticală.

- Pentru Intrare alarmă, selectați tipul ca alarmă sau recuperare alarmă și selectați numele intrării alarmei din tabel.
- Pentru Eveniment ușă, selectați tipul de eveniment detaliat și selectați ușa sursă din tabel. Pentru
- Card Reader Event, selectați tipul de eveniment detaliat și selectați cititorul de carduri din tabel.

2. Setați ținta de legătură și comutați proprietatea de la la  pentru a activa această funcție.
   - **Buzzer gazdă:**Avertismentul sonor al controlerului va fi activat/dezactivat.
   - **Captură:**Captarea în timp real va fi activată.
   - **Buzzer cititor de carduri:**Avertismentul sonor al cititorului de carduri va fi activat/dezactivat.
   - **Ieșire alarmă:**Ieșirea alarmei va fi activată/dezactivată pentru notificare.
   - **Punct de control acces:**Starea ușii deschisă, închisă, rămâne deschisă și rămâne închisă va fi activată.

     Note:
     - Starea ușii deschisă, închisă, rămâne deschisă și rămâne închisă nu poate fi declanșată în același timp.
     - Ușa țintă și ușa sursă nu pot fi aceeași.
3. Faceți clic**Salvați**butonul pentru a salva și a lua efectul parametrilor.

Conectarea cardului

Pași:

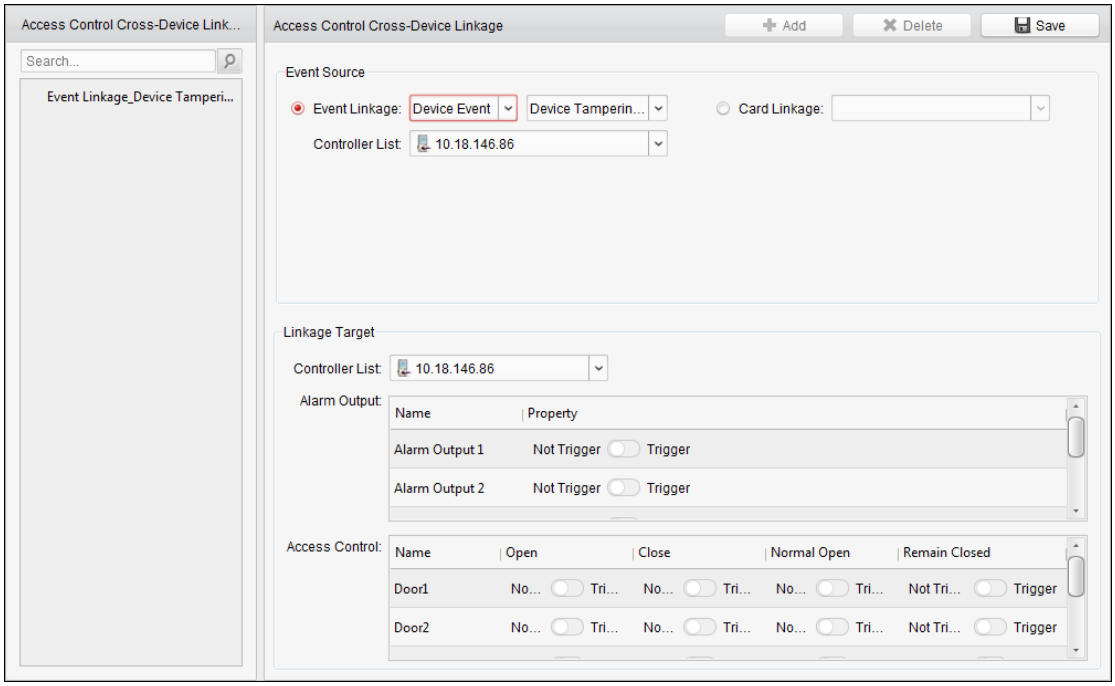
1. Faceţi clic pentru a selecta tipul de legătură ca**Conectarea cardului**.
2. Introduceți numărul cardului sau selectați cardul din lista verticală.
3. Selectați cititorul de carduri din tabel pentru declanșare.
4. Setați ținta de legătură și comutați proprietatea de la la  pentru a activa această funcție.
   - **Buzzer gazdă:**Avertismentul sonor al controlerului va fi activat/dezactivat.
   - **Captură:**Captarea în timp real va fi activată.
   - **Buzzer cititor de carduri:**Avertismentul sonor al cititorului de carduri va fi activat/dezactivat.
   - **Ieșire alarmă:**Ieșirea alarmei va fi activată/dezactivată pentru notificare.
   - **Punct de control acces:**Starea ușii deschisă, închisă, rămâne deschisă și rămâne închisă va fi activată.
5. Faceți clic**Salvați**butonul pentru a salva și a lua efectul parametrilor.

7.10.4 Conectare între dispozitive

Scop:

Puteți declanșa acțiunea altui dispozitiv de control al accesului prin stabilirea unei reguli atunci când evenimentul de control al accesului este declanșat.

Clic**Conectare între dispozitive**pentru a intra în următoarea interfață.



Clic**Adăuga**butonul pentru a adăuga o nouă legătură cu clientul. Puteți selecta sursa evenimentului ca**Legătura evenimentului**sau **Conectarea cardului**.

Legătura evenimentului

Pentru conectarea evenimentului, evenimentul de alarmă poate fi împărțit în patru tipuri: eveniment dispozitiv, intrare alarmă, eveniment ușă și eveniment cititor de carduri.

Pași:

1. Faceţi clic pentru a selecta tipul de legătură ca**Legătura evenimentului**, selectați dispozitivul de control al accesului ca sursă de eveniment, și selectați tipul de eveniment din lista verticală.
   - Pentru Eveniment dispozitiv, selectați tipul de eveniment detaliat din lista verticală.
   - Pentru Intrare alarmă, selectați tipul ca alarmă sau recuperare alarmă și selectați numele intrării alarmei din tabel.
   - Pentru Eveniment ușă, selectați tipul de eveniment detaliat și selectați ușa din tabel.
   - Pentru Card Reader Event, selectați tipul de eveniment detaliat și selectați cititorul de carduri din tabel.
2. Setați ținta de legătură, selectați dispozitivul de control al accesului din lista verticală ca țintă de legătură și comutați proprietatea de la la  pentru a activa această funcție.
   - **Ieșire de alarmă**: Ieșirea de alarmă va fi declanșată pentru notificare.
   - **Punct de control acces**: Starea ușii deschis, închidere, rămâne deschisă și rămâne închisă va fi declanșată.***Notă:***Starea ușii deschisă, închisă, rămâne deschisă și rămâne închisă nu poate fi declanșată în același timp.
3. Faceți clic**Salvați**butonul pentru a salva parametrii.

Conectarea cardului

Pași:

1. Faceţi clic pentru a selecta tipul de legătură ca**Conectarea cardului**.

2. Selectați cardul din lista verticală și selectați dispozitivul de control al accesului ca sursă de evenimente.
3. Selectați cititorul de carduri din tabel pentru declanșare.
4. Setați ținta de legătură, selectați dispozitivul de control al accesului din lista verticală ca țintă de legătură și comutați proprietatea de la la  pentru a activa această funcție.

   Ieșire de alarmă: Ieșirea de alarmă va fi declanșată pentru notificare.

5. Faceți clic**Salvați**butonul pentru a salva parametrii.

7.11 Managementul stării ușii

Scop:

Starea ușii dispozitivului de control al accesului adăugat va fi afișată în timp real. Puteți verifica starea ușii și evenimentul(e) asociat(e) ușii selectate. Puteți controla starea ușii și puteți seta și durata stării ușilor.

7.11.1 Managementul grupului de control acces

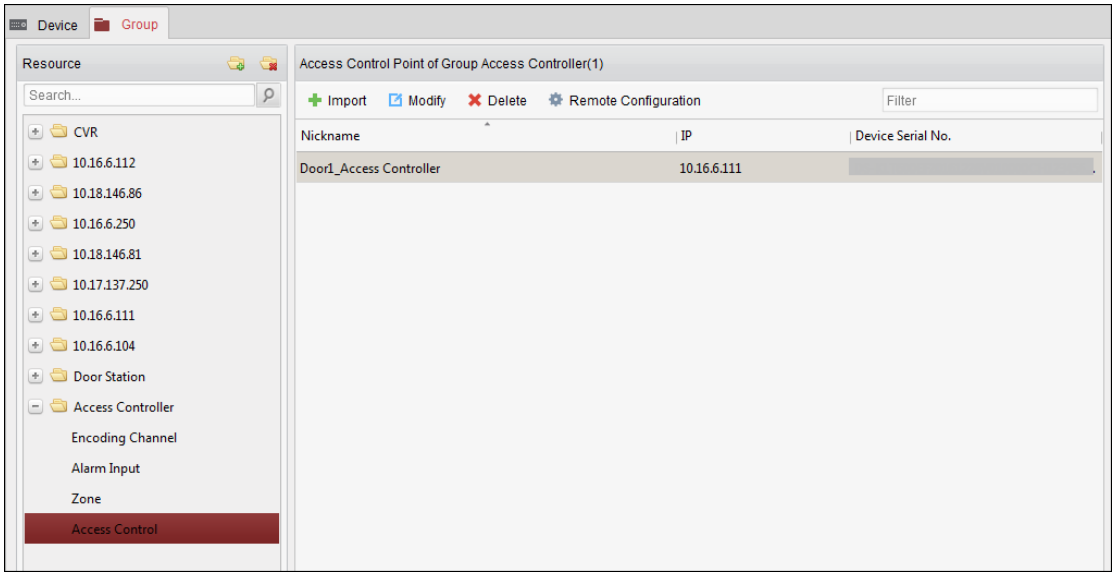
Scop:

Înainte de a controla starea ușii și a seta durata stării, trebuie să o organizați în grupuri pentru o gestionare convenabilă.

Efectuați următorii pași pentru a crea grupul pentru dispozitivul de control acces:

Pași:

1. Faceți clic  pe panoul de control pentru a deschide pagina Device Management.
2. Faceți clic**grup**pentru a intra în interfața de gestionare a grupului.



3. Efectuați următorii pași pentru a adăuga grupul.

   1) Faceți clic  pentru a deschide caseta de dialog Adăugare grup.

   2) Introduceți un nume de grup după cum doriți.

   3) Faceți clic**Bine**pentru a adăuga noul grup la lista de grupuri.

      De asemenea, puteți bifa caseta de selectare**Creați grup după numele dispozitivului**pentru a crea noul grup prin

numele dispozitivului selectat.

4. Efectuați următorii pași pentru a importa punctele de control acces în grup:

1) Faceți clic**Import**pe interfața de gestionare a grupului, apoi faceți clic pe**Controlul accesului**pentru a deschide pagina Import Access Control.

Note:

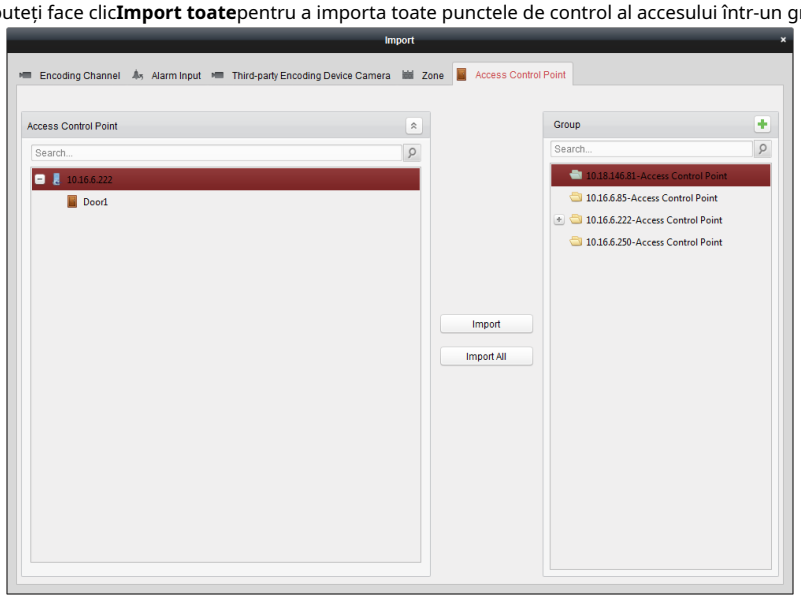
- De asemenea, puteți selecta**Intrare alarmă**și importați intrările de alarmă în grup.
- Pentru terminalul de control al accesului video, puteți adăuga camerele ca canal de codificare la grup.

2) Selectați numele punctelor de control acces din listă.

3) Selectați un grup din lista de grupuri.

4) Faceți clic**Import**pentru a importa punctele de control acces selectate în grup.

De asemenea, puteți face clic**Import toate**pentru a importa toate punctele de control al accesului într-un grup selectat.



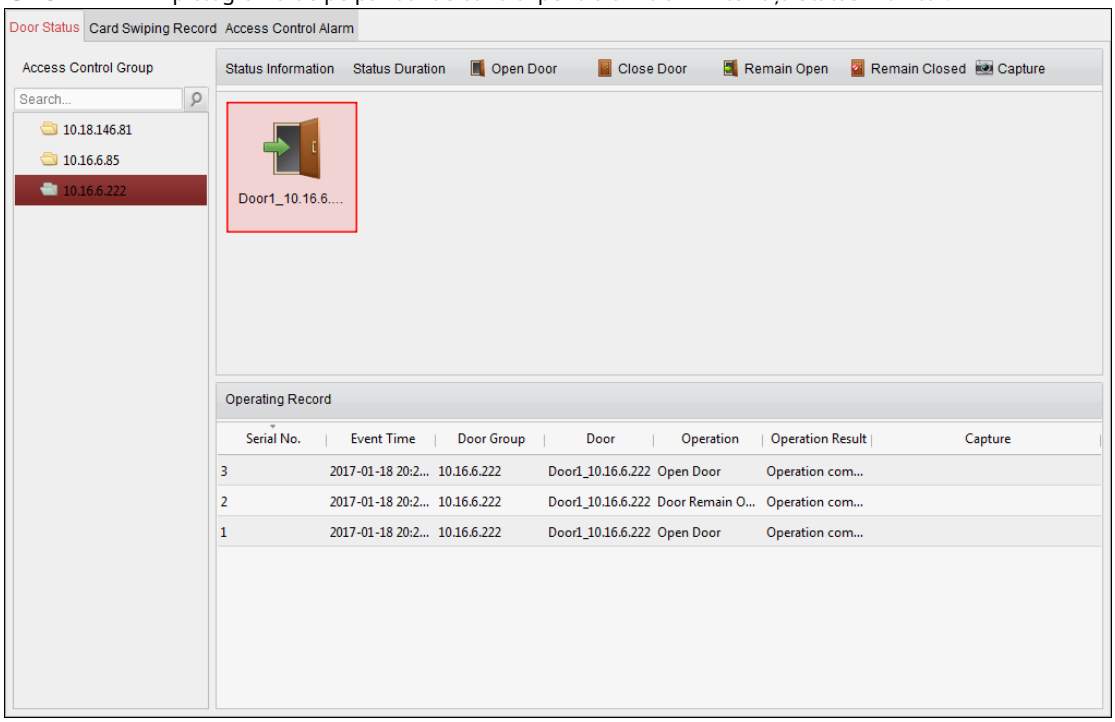
5. După importarea punctelor de control al accesului în grup, puteți face clic pe sau faceți dublu clic pe numele grupului/ punctului de control al accesului pentru a-l modifica.

7.11.2 Anti-controlul punctului de control al accesului (uşă)

Scop:

Puteți controla starea unui singur punct de control al accesului (o ușă), inclusiv deschiderea ușii, închiderea ușii, rămânerea deschisă și rămânerea închisă.

Clic  pictograma de pe panoul de control pentru a intra în interfața Status Monitor.



Pași:

1. Selectați un grup de control acces din stânga. Pentru gestionarea grupului de control acces, consultați *Capitolul 7.11.1 Managementul grupului de control acces.*
2. Punctele de control acces ale grupului de control acces selectat vor fi afișate în partea dreaptă.

Faceți clic pe pictograma  pe panoul Informații de stare pentru a selecta o ușă.

3. Faceți clic pe următorul buton listat pe**Informații despre stare**panou pentru controlul ușii.

Open Door : Faceți clic pentru a deschide ușa o dată. :

Close Door Faceți clic pentru a închide ușa o dată. :

Remain Open Faceți clic pentru a menține ușa deschisă.

Remain Closed : Faceți clic pentru a ține ușa închisă.

Capture : Faceți clic pentru a captura imaginea manual.

4. Puteți vizualiza rezultatul operațiunii anti-control în panoul Jurnal operațiuni.

Note:

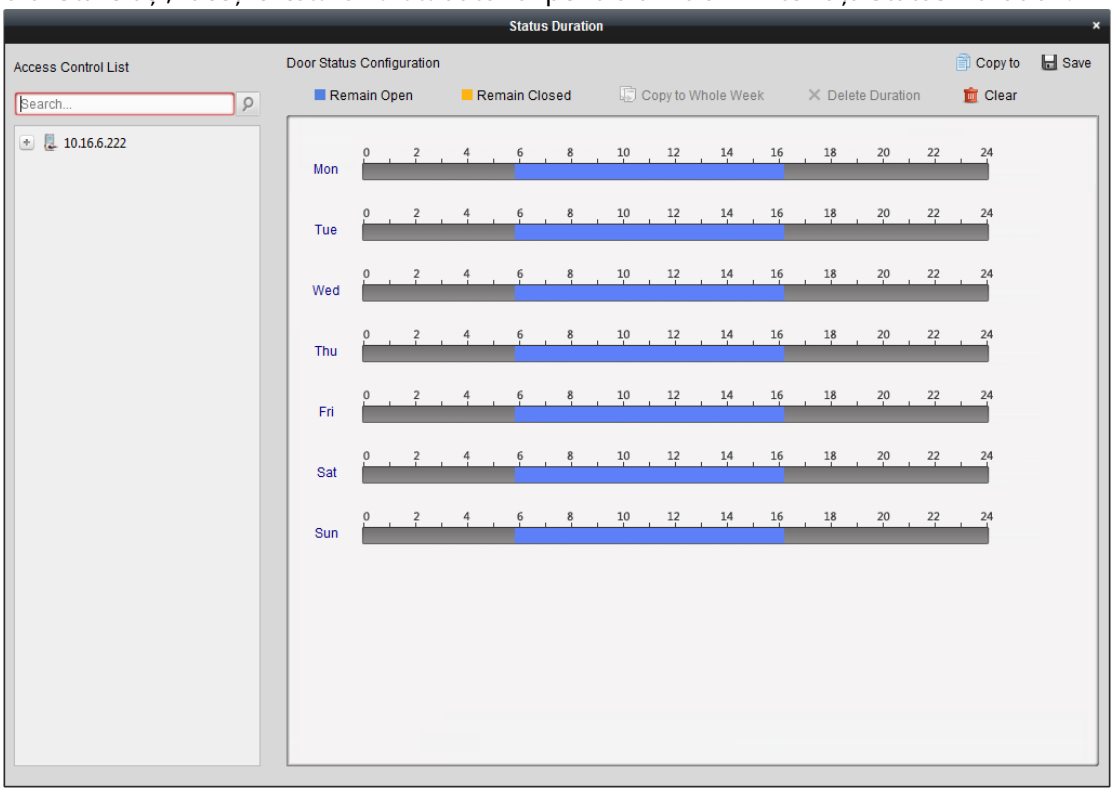
- Dacă selectați starea ca**Rămâne deschis/Rămâne închis**, ușa va rămâne deschisă/închisă până la efectuarea unei noi comenzi anti-control.
- The**Capturăbutonul** este disponibil când dispozitivul acceptă funcția de captură. Și nu poate fi realizat până când serverul de stocare este configurat.
- Dacă ușa este în starea de rămâne închisă, numai super cardul poate deschide ușa sau deschide ușa prin intermediul software-ului client.

7.11.3 Configurare durată stare

Scop:

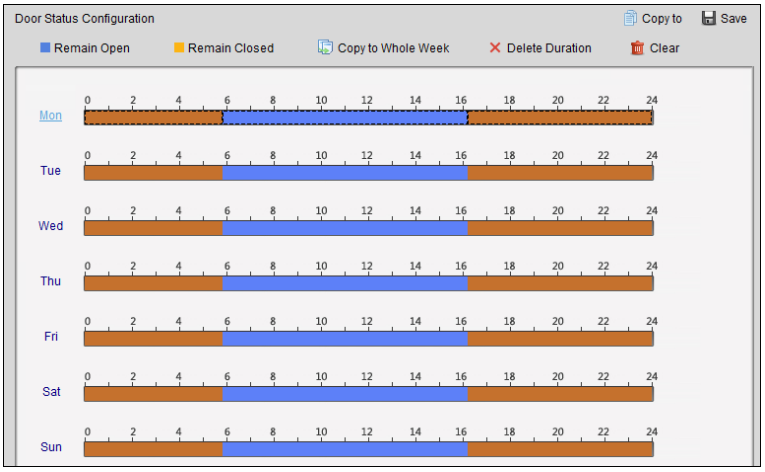
Puteți programa perioade de timp săptămânale pentru ca un punct de control acces (ușă) să rămână deschis sau să rămână închis.

În modulul Stare uși, faceți clic**Stare Durata**butonul pentru a intra în interfața Status Duration.



Pași:

1. Faceți clic pentru a selecta o ușă din lista de dispozitive de control acces din stânga.
2. În panoul Configurare stare uși din dreapta, desenați un program pentru ușa selectată.
   1) Selectați o perie pentru starea ușii ca Remain Open sau Remain Closed.
      Rămâi deschis: Ușa va rămâne deschisă în perioada de timp configurată. Peria este marcată ca .
      Rămâi închis: Ușa va rămâne închisă pe durata configurată. Peria este marcată ca .
   2) Faceți clic și trageți pe cronologia pentru a desena o bară de culoare pe program pentru a seta durata.



3) Când cursorul setransforma în , puteți muta bara de timp selectată pe care tocmai ați editat-o. De asemenea, putețiedita punctul de timp afișat pentru a seta perioada de timp exactă.

Când cursorul se transforma în , puteți prelungi sau scurta bara de timp selectată.

3. Opțional, puteți selecta bara de timp a programului și faceți clic **Copiați în săptămâna întreagă** pentru a copia setările barei de timp în celelalte zile ale săptămânii.

4. Puteți selecta bara de timp și faceți clic **Șterge durata** pentru a șterge perioada de timp. Sau

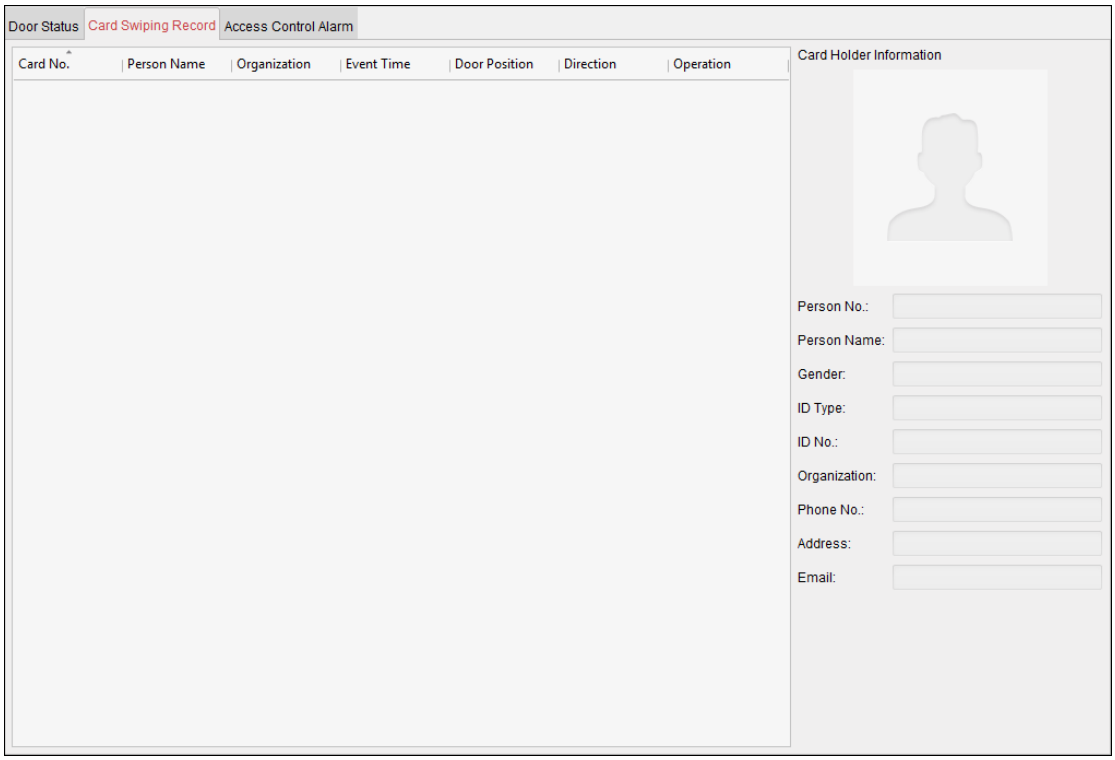
puteți face clic **clar** pentru a șterge toate duratele configurate în program.

5. Faceți clic **Salvați** pentru a salva setările.

6. Puteți face clic **Copiaza in** pentru a copia programul la alte uși.

7.11.4 Înregistrare de glisare a cardului în timp real

Clic **Înregistrare de trecere a cardului** pentru a intra în următoarea interfață.



Jurnalele înregistrărilor de glisare a cardurilor pentru toate dispozitivele de control al accesului se vor afișa în timp real. Puteți vizualiza detaliile evenimentului de trecere a cardului, inclusiv numărul cardului, numele persoanei, organizația, ora evenimentului etc.

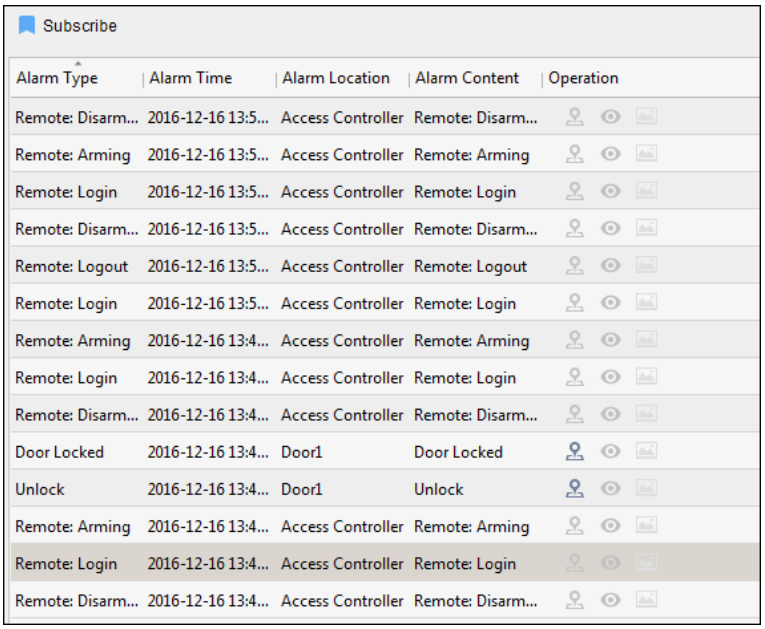
De asemenea, puteți face clic pe eveniment pentru a vedea detaliile deținătorului cardului, inclusiv numărul persoanei, numele persoanei, organizația, telefonul, adresa de contact etc.

7.11.5 Alarmă de control al accesului în timp real

Scop:

Jurnalele evenimentelor de control al accesului vor fi afișate în timp real, inclusiv excepția dispozitivului, evenimentul ușii, evenimentul cititorului de carduri și intrarea alarmei.

Clic **Alarmă de control acces** pentru a intra în următoarea interfață.



Pași:

1. Toate alarmele de control al accesului vor fi afișate în listă în timp real.

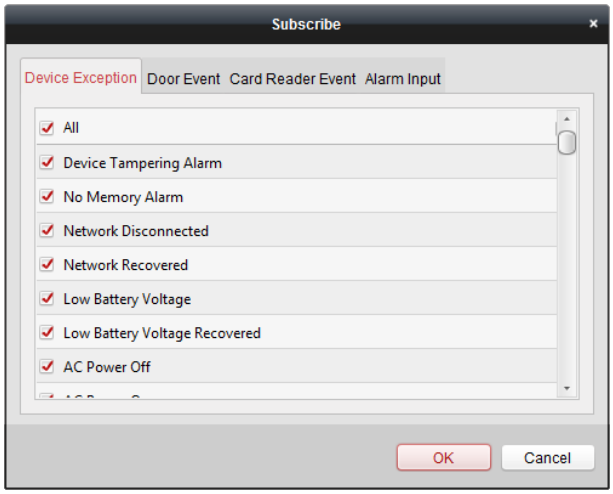
   Puteți vizualiza tipul alarmei, ora alarmei, locația etc.

2. Faceți clic pentru a vizualiza alarma pe E-map.

3. Puteți face clic pe sau pentru a vizualiza vizualizarea live sau imaginea capturată a camerei declanșate atunci când alarma estedeclanșată.

   Notă:Pentru setarea camerei declanșate, consultați*Capitolul 7.10.1 Legătura evenimentelor de control al accesului.*

4. Faceți clic**Abonati-va**pentru a selecta alarma pe care clientul o poate primi atunci când alarma este declanșată.



   1) Bifați casetele de selectare pentru a selecta alarmele, inclusiv alarma de excepție a dispozitivului, alarma de eveniment de ușă, alarma cititorului de carduri și intrarea alarmei.

   2) Faceți clic**Bine**pentru a salva setările.

7.12 Control armare

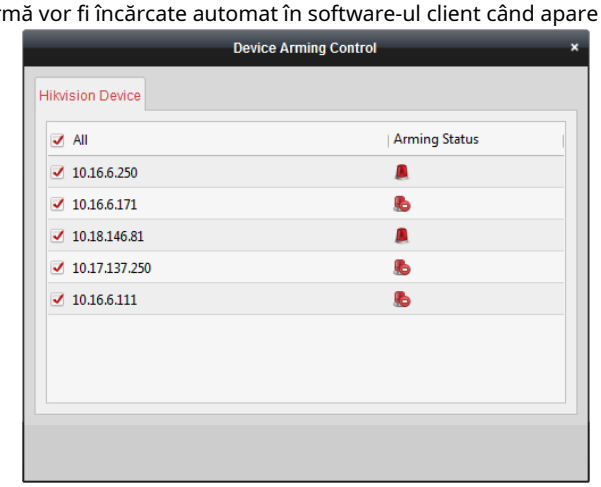
Scop:

Puteți arma sau dezarma dispozitivul. După armarea dispozitivului, clientul poate primi informațiile de alarmă de la dispozitiv.

Pași:

1. Faceți clic**Instrument->Control armare dispozitiv**pentru a deschide fereastra de control al armarii dispozitivului.
2. Armați dispozitivul bifând caseta de selectare corespunzătoare.

   Apoi, informațiile despre alarmă vor fi încărcate automat în software-ul client când apare alarma.



Anexa A Sunet și indicator

După ce cititorul de carduri este pornit, indicatorul LED de stare va deveni albastru și va clipi o dată. Apoi va deveni roșu și va clipi de 3 ori. În cele din urmă, soneria va emite un bip care indică finalizarea procesului de pornire. În timpul utilizării cititorului de carduri, acesta va emite sunete diferite, iar indicatorul LED de pe acesta va avea stări diferite. Puteți consulta tabelele de mai jos pentru informații detaliate.

Tabelul 7-1 Descrierea sunetului prompt

Sunet prompt	Descriere
Un bip	Protocol RS-485: Apăsarea tastelor prompt; Swiping card prompt; Time out prompt pentru apăsarea tastelor sau glisarea cardului. Protocolul Wiegand: Apăsarea tastelor prompt; Solicitare de glisare a cardului.
Două bipuri rapide	Operația de apăsare a tastelor sau de glisare a cardului este valabilă.
Trei bipuri lente	Operația de apăsare a tastelor sau de glisare a cardului este invalidă.
Rapid continuu bipuri	Alarma de falsificare.
Încet continuu bipuri	Cititorul de carduri este necriptat.

Tabelul 7-2 Descrierea indicatorului LED

Stare indicator LED	Descriere
Verde și clipește	Cititorul de carduri funcționează normal.
Verde solid	Operația de apăsare a tastelor sau de glisare a cardului este valabilă.
Roșu continuu	Operația de apăsare a tastelor sau de glisare a cardului este invalidă.
Roșu și clipește	Pentru protocolul RS-485: Înregistrarea a eșuat sau cititorul de carduri este offline. Nu s-au putut obține fișierele cheie ale cardului PSAM; Nu s-a detectat cardul PSAM.
roșu și rapid clipind	Păstrarea Disponibil pentru modul de citire fișier al cardului CPU: PSAM nu este introdus sau nedetectat.

Anexa B Regula Wiegand personalizată

Luați Wiegand 44 ca exemplu, valorile setărilor din fila Custom Wiegand sunt după cum urmează:

Nume Wiegand personalizat:	Wiegand 44					
Lungime totală	44					
Regula de transformare (cifra zecimală)	byFormatRule[4]=[1][4][0][0]					
Modul de paritate	Paritate XOR					
Bit de început de paritate impară		Lungime				
Chiar și bitul de pornire al parității		Lungime				
Bit de pornire de paritate XOR	0	Lungimea per grup	4	Lungime totală	40	
Bit de pornire ID card	0	Lungime	32	Cifră zecimală		10
Bit de pornire cod site		Lungime		Cifră zecimală		
Bit de pornire OEM		Lungime		Cifră zecimală		
Bit de pornire cod de producător	32	Lungime	8	Cifră zecimală		3

Date Wiegand = Date valide + Date de paritate

Lungime totală: Lungimea datelor Wiegand.

Regula de transport:4 octeți. Afișați tipurile de combinații de date valide. Exemplul afișează combinația de ID card și cod de producător. Datele valide pot fi o singură regulă sau o combinație de mai multe reguli.

Mod paritate: Paritate valabilă pentru datele Wiegand. Puteți selecta fie paritate impară, fie paritate pară.

Bit de început de paritate impară și lungime: Dacă selectați Paritate impară, aceste elemente sunt disponibile. Dacă bitul de pornire al parității impare este 1 și lungimea este 12, atunci sistemul va începe calculul parității impare de la bitul 1. Va calcula 12 biți. Rezultatul va fi în bitul 0. (Bitul 0 este primul bit.)

Bit de început paritate și lungime: Dacă selectați Paritate egală, aceste elemente sunt disponibile. Dacă bitul de pornire al parității par este 12, iar lungimea este 12, atunci sistemul va începe calculul parității par de la bitul 12. Va calcula 12 biți. Rezultatul va fi în ultimul bit.

Bit de început de paritate XOR, lungime per grup și lungime totală: Dacă selectați XOR Parity, aceste elemente sunt disponibile. În funcție de tabelul afișat mai sus, bitul de început este 0, lungimea per grup este 4 și lungimea totală este 40. Înseamnă că sistemul va calcula de la bitul 0, va calcula la fiecare 4 biți și va calcula 40 de biți în total (10 grupuri în total). Rezultatul va fi în ultimii 4 biți. (Lungimea rezultatului este aceeași cu lungimea per grup.)

Bit de pornire ID card, lungime și cifră zecimală: Dacă utilizați regula de transformare, aceste elemente sunt disponibile. În funcție de tabelul afișat mai sus, bitul de pornire al ID-ului cardului este 0, lungimea este 32 și cifra zecimală este 10. Reprezintă că din bitul 0, există 32 de biți care reprezintă ID-ul cardului. (Lungimea aici este calculată pe biți.) Și lungimea cifrei zecimale este de 10 biți.

Bit de început codul site-ului, lungime și cifră zecimală: Dacă utilizați regula de transformare, aceste elemente sunt disponibile. Pentru informații detaliate, consultați explicația ID-ului cardului.

Bit de început OEM, lungime și cifră zecimală: Dacă utilizați regula de transformare, aceste elemente sunt disponibile. Pentru informații detaliate, consultați explicația ID-ului cardului.

Bit de început al codului de producător, lungime și cifră zecimală: Dacă utilizați regula de transformare, aceste elemente sunt disponibile. În funcție de tabelul afișat mai sus, bitul de pornire al codului producătorului este 32, lungimea este 8 și cifra zecimală este 3. Reprezintă că din bitul 32 există 8 biți care sunt codul producătorului. (Lungimea aici este calculată pe biți.) Și lungimea zecimală este 3.

020000001080620


See Far, Go Further