



Terminal de recunoaștere facială seria DS-K1T671

Manual de utilizare

Informații legale

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. Toate drepturile rezervate.

Despre acest manual

Manualul include instrucțiuni pentru utilizarea și gestionarea produsului. Imaginile, diagramele, imaginile și toate celelalte informații de mai jos sunt doar pentru descriere și explicație. Informațiile conținute în Manual pot fi modificate, fără notificare, din cauza actualizărilor de firmware sau din alte motive. Vă rugăm să găsiți cea mai recentă versiune a acestui manual pe site-ul web Hikvision ([https:// www.hikvision.com/](https://www.hikvision.com/)).

Vă rugăm să utilizați acest manual cu îndrumarea și asistența specialiștilor instruiți în sprijinirea Produsului.

Mărci comerciale

HIKVISION și alte mărci comerciale și logo-uri Hikvision sunt proprietatea Hikvision în diferite jurisdicții.

Alte mărci comerciale și logo-uri menționate sunt proprietățile deținătorilor respectivi.

Disclaimer

ÎN MĂSURA MAXIMĂ PERMISĂ DE LEGEA APLICABILĂ, ACEST MANUAL ȘI PRODUSUL DESCRIS, CU HARDWARE-UL, SOFTWARE-UL ȘI FIRMWARE-UL SUNT FURNIZATE „CA AȚIE” ȘI „CU TOATE DEFECTELE ȘI ERORILE”. HIKVISION NU OFERĂ GARANȚII, EXPRESE SAU IMPLICITE, INCLUSIV FĂRĂ LIMITĂRI, VANTABILITATE, CALITATE SATISFĂCĂTORĂ SAU ADECVENȚĂ PENTRU UN ANUMIT SCOP. UTILIZAREA PRODUSULUI DE CĂTRE DVS. ESTE PE PROPRIU RISC. HIKVISION NU VA FI RESPONSABIL ÎN NICIUN CAZ PENTRU ORICE DAUNE SPECIALE, CONSECENȚIALE, INCIDENTALE SAU INDIRECTE, INCLUSIV, PRIN ALȚELE, DAUNE PENTRU PIERDEREA PROFITURILOR AFACERII, ÎNTRERUPEREA AFACERII SAU PIERDEREA DATELOR, CORUPERA SISTEMELOR SAU PIERDEREA BAZĂRII, PIERDEREA DOCUMENTULUI. DELICITĂȚI (INCLUSUL NEGLIGENȚEI), RĂSPUNDEREA PRODUSULUI SAU ALTELE, ÎN LEGAȚIE CU UTILIZAREA PRODUSULUI, CHIAR DACĂ HIKVISION A FOST Anunțat despre POSIBILITATEA ACESTE DE DAUNE SAU PIERDERI.

RECUNOSȚI CĂ NATURA INTERNET PREVĂ RISCURI INERENTE DE SECURITATE, ȘI HIKVISION NU ÎȘI ASUMĂ NICIO RESPONSABILITATE PENTRU OPERAȚIUNEA ANORMĂ, SCURTĂRI DE CONFIDENTIALITATE SAU ALTE DAUNE REZULTATE DIN ATAC CIBERNICE, ATAC DE HACKER, ALTĂ INSPECȚIE DE VIRUS; CU toate acestea, HIKVISION VA FURNIZA SISTEMUL TEHNIC LA TEMPORUL DACĂ ESTE NECESAR.

SUNTEȚI DE ACORD SĂ UTILIZAȚI ACEST PRODUS ÎN CONFORMITATE CU TOATE LEGILE APLICABILE ȘI SUNTEȚI UNCUL RESPONSABIL PENTRU A ASIGURA CĂ UTILIZAREA DVS. CONFORM LEGEA APLICABĂ. În special, ești RESPONSABIL PENTRU UTILIZAREA ACESTUI PRODUS ÎN O MANIERĂ CARE NU ÎNCĂLCĂ DREPTURILE TERȚILOR, INCLUSIV FĂRĂ LIMITARE, DREPTURILE DE PUBLICITATE, DREPTURILE DE PROPRIETATE INTELECTUALĂ SAU PROTECȚIA DATELOR ȘI ALTE DREPTURI ȘI ALTE DREPTURI. NU UTILIZAȚI ACEST PRODUS PENTRU UTILIZĂRI FINALE INTERZISE, INCLUSIV DEZVOLTAREA SAU PRODUCȚIA DE ARME DE DISTRUCȚIE ÎN MASĂ, DEZVOLTAREA SAU

PRODUCȚIA DE ARME CHIMICE SAU BIOLOGICE, ORICE ACTIVITĂȚI ÎN CONTEXT LEGATE DE ORICE CICLU DE COMBUSTIBIL NUCLEAR EXPLOZIV SAU NUCLEAR NESICUR, SAU ÎN Sprijinirea abuzurilor drepturilor omului.

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

Protecția datelor

În timpul utilizării dispozitivului, datele personale vor fi colectate, stocate și prelucrate. Pentru a proteja datele, dezvoltarea dispozitivelor Hikvision încorporează principiile de confidențialitate prin proiectare. De exemplu, pentru dispozitivul cu caracteristici de recunoaștere facială, datele biometrice sunt stocate în dispozitivul dvs. cu metoda de criptare; pentru dispozitivul de amprentă, va fi salvat doar șablonul de amprentă, ceea ce este imposibil să reconstruiți o imagine cu amprentă.

În calitate de operator de date, vi se recomandă să colectați, să stocați, să procesați și să transferați date în conformitate cu legile și reglementările aplicabile privind protecția datelor, inclusiv, fără limitare, efectuarea de controale de securitate pentru a proteja datele cu caracter personal, cum ar fi implementarea unor controale de securitate administrative și fizice rezonabile, efectuarea de revizuiți și evaluări periodice ale eficacității controalelor dvs. de securitate.

Convenții de simboluri

Simbolurile care pot fi găsite în acest document sunt definite după cum urmează.

Simbol	Descriere
 Pericol	Indică o situație periculoasă care, dacă nu este evitată, va sau ar putea duce la moarte sau vătămări grave.
 Atenție	Indică o situație potențial periculoasă care, dacă nu este evitată, ar putea duce la deteriorarea echipamentului, pierderea datelor, degradarea performanței sau rezultate neașteptate.
 Nota	Oferă informații suplimentare pentru a sublinia sau completa punctele importante ale textului principal.

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 a se conforma cu limitele pentru un dispozitiv digital de Clasa 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 cauzează 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

Acest echipament trebuie instalat și operat la o distanță de minim 20 cm între radiator și corp.

Condiții FCC

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

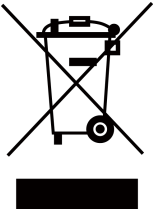
1. Acest dispozitiv nu poate cauza interferențe dăunătoare.
2. Acest dispozitiv trebuie să accepte orice interferență primită, inclusiv interferențe care pot provoca o funcționare nedorită.

Declarație de conformitate UE



Acest produs și, dacă este cazul, accesoriile furnizate sunt de asemenea marcate cu „CE” și, prin urmare, respectă standardele europene armonizate aplicabile enumerate.

în conformitate cu Directiva EMC 2014/30/UE, Directiva RE 2014/53/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, consultați: www.recyclethis.info

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 este împărțită în Pericole și Atenții: **Pericole:** Neglijarea oricăruia dintre avertismente poate provoca vătămări grave sau deces. **Atenționări:** Neglijarea oricăreia dintre precauții poate cauza răniri sau deteriorarea echipamentului.

	
Pericole: Urmați aceste măsuri de siguranță pentru a preveni rănirea gravă sau decesul.	Atenționări: Urmați aceste măsuri de precauție pentru a preveni potențialele vătămări sau daune materiale.

Pericol:

- Toate operațiunile electronice trebuie să respecte cu strictețe 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. Acest echipament este destinat să fie alimentat de la o sursă de alimentare protejată la supratensiune Clasa 2, nominală DC 12V, 3A.
- 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.
- Nu ingerați bateria, pericol de arsuri chimice.
Acest produs conține o baterie tip monedă/buton. Dacă bateria monedă/buton este înghițită, poate provoca arsuri interne severe în doar 2 ore și poate duce la moarte.
Păstrați bateriile noi și uzate departe de copii. Dacă compartimentul bateriei nu se închide bine, nu mai utilizați produsul și țineți-l departe de copii. Dacă credeți că bateriile ar fi putut fi înghițite sau plasate în orice parte a corpului, solicitați imediat asistență medicală.
- Dacă produsul nu funcționează corect, vă rugăm să contactați dealerul dumneavoastră sau cel mai apropiat centru de service. Nu încercați niciodată să dezamblați 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.

- Capacul dispozitivului pentru utilizare în interior trebuie ferit de ploaie și umezeală.
- Este interzisă expunerea echipamentului la lumina directă a soarelui, ventilație scăzută sau surse de căldură, cum ar fi încălzitorul sau radiatorul (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.
- Produsele de recunoaștere biometrică nu sunt 100% aplicabile în mediile anti-spoofing. Dacă aveți nevoie de un nivel de securitate mai ridicat, utilizați mai multe moduri de autentificare.
- Temperatura de lucru: -30 °C până la +60 °C
- Utilizare în interior și exterior. Dacă instalați dispozitivul în interior, dispozitivul trebuie să fie la cel puțin 2 metri distanță de lumină și la cel puțin 3 metri distanță de fereastră sau ușă. Dacă instalați dispozitivul în aer liber, trebuie să aplicați sigilant Sililcone printre zona cablurilor pentru a împiedica pătrunderea picăturii de ploaie.
- Nivel de protecție: IP65
- Tensiunea de intrare trebuie să îndeplinească atât SELV (Tensiune foarte joasă de siguranță) cât și sursa de alimentare limitată cu 100~240 VAC sau 12 VDC conform standardului IEC60950-1. Vă rugăm să consultați specificațiile tehnice pentru informații detaliate.

Modele disponibile

Numele produsului	Model
Terminal de recunoaștere a feței	DS-K1T671M
	DS-K1T671MF
	DS-K1T671TM
	DS-K1T671TMW
	DS-K1T671TMF
	DS-K1T671TMFW

Utilizați numai sursele de alimentare enumerate în instrucțiunile de utilizare:

Model	Producător	Standard
C2000IC12.0-24P-DE	Sursa de alimentare MOSO Technology Co., Ltd.	CEE
C2000IC12.0-24P-GB	Sursa de alimentare MOSO Technology Co., Ltd.	BS
KPL-040F-VI	Channel Well Technology Co Ltd.	CEE

Cuprins

Capitolul 1 Prezentare generală	1
1.1 Prezentare generală	1
1.2 Caracteristici	1
Capitolul 2 Aspectul	3
Capitolul 3 Instalare	5
3.1 Mediul de instalare	5
3.2 Instalare cu Gang Box	5
3.3 Instalare fără Gang Box	8
Capitolul 4 Cablaje	14
4.1 Descrierea terminalului	14
4.2 Cablare dispozitiv normal	16
4.3 Unitatea de comandă a ușii securizate prin cablu	17
Capitolul 5 Activare	19
5.1 Activare prin dispozitiv	19
5.2 Activare prin SADP	21
5.3 Activarea dispozitivului prin software-ul client	22
Capitolul 6 Operarea de bază	23
6.1 Selectarea limbii	23
6.2 Setarea modului de aplicare	23
6.3 Setarea administratorului	25
6.4 Conectare	27
6.4.1 Conectare de către administrator	27
6.4.2 Conectare prin parola de activare	28
6.5 Setări de comunicare	29
6.5.1 Setarea parametrilor rețelei cu fir	30
6.5.2 Setarea parametrilor Wi-Fi	30

6.5.3 Setarea parametrilor RS-485	32
6.5.4 Setarea parametrilor Wiegand	32
6.6 Gestionarea utilizatorilor	33
6.6.1 Adăugați imaginea feței	33
6.6.2 Adăugarea amprenteii	35
6.6.3 Adăugarea cardului	36
6.6.4 Adăugarea parolei	37
6.6.5 Setarea modului de autentificare	38
6.6.6 Căutarea și editarea utilizatorului	38
6.7 Gestionarea datelor	39
6.7.1 Ștergerea datelor	39
6.7.2 Import de date	39
6.7.3 Export de date	40
6.8 Autentificarea identității	40
6.8.1 Autentificare prin acreditare unică	40
6.8.2 Autentificare prin acreditări multiple	41
6.9 Setări de bază	41
6.10 Setarea parametrilor biometrici	43
6.11 Setarea parametrilor de control al accesului	45
6.12 Setări de oră și stare de prezență	47
6.12.1 Dezactivarea modului de participare prin dispozitiv	47
6.12.2 Setarea prezenței manuale prin intermediul dispozitivului	47
6.12.3 Setarea prezenței automate prin dispozitiv	48
6.12.4 Setați prezența manuală și automată prin intermediul dispozitivului	50
6.13 Întreținerea sistemului	51
6.14 Interfon video	52
6.14.1 Apelarea software-ului client de pe dispozitiv	52
6.14.2 Call Center de la Dispozitiv	53

6.14.3	Apelați dispozitivul din software-ul client	53
6.14.4	Apelați camera de pe dispozitiv	54
Capitolul 7 Operarea prin browser web		55
7.1	Conectare	55
7.2	Vizualizare live	55
7.3	Managementul persoanelor	56
7.4	Căutare eveniment	57
7.5	Configurare	58
7.5.1	Setarea parametrilor locali	58
7.5.2	Vizualizare informații despre dispozitiv	58
7.5.3	Setarea orei	58
7.5.4	Setați ora de oră	59
7.5.5	Actualizare și întreținere	59
7.5.6	Schimbarea parolei administratorului	61
7.5.7	Setări de rețea	61
7.5.8	Setarea parametrilor video și audio	63
7.5.9	Setarea parametrilor interfonului video	64
7.5.10	Setarea controlului accesului și parametrilor de autentificare	65
7.5.11	Setarea parametrilor RS-485	66
7.5.12	Setarea parametrilor Wiegand	67
7.5.13	Setarea parametrilor imaginii	68
7.5.14	Setarea luminozității luminii suplimentare	69
7.5.15	Setarea parametrilor biometrici	69
7.5.16	Setarea publicării notificării	71
Capitolul 8 Configurarea software-ului client		73
8.1	Fluxul de configurare al software-ului client	73
8.2	Gestionarea dispozitivelor	73
8.2.1	Adăugarea dispozitivului	73

8.2.2	Resetarea parolei dispozitivului	82
8.3	Managementul grupului	82
8.3.1	Adăugați grup	82
8.3.2	Importarea resurselor în grup	83
8.3.3	Editarea parametrilor resursei	83
8.3.4	Eliminarea resurselor din grup	84
8.4	Managementul persoanelor	84
8.4.1	Adăugați o organizație	84
8.4.2	Configurarea informațiilor de bază	85
8.4.3	Emiterea unui card prin modul local	85
8.4.4	Încărcați o fotografie a feței de pe un computer local	87
8.4.5	Realizarea unei fotografii prin client	88
8.4.6	Colectarea feței prin dispozitivul de control al accesului	88
8.4.7	Colectarea amprentei prin client	89
8.4.8	Colectarea amprentei prin intermediul dispozitivului de control al accesului	90
8.4.9	Configurarea informațiilor de control al accesului	90
8.4.10	Personalizarea informațiilor despre persoană	92
8.4.11	Configurarea informațiilor rezidenților	92
8.4.12	Configurarea informațiilor suplimentare	93
8.4.13	Importați și exportați informații de identificare a persoanei	93
8.4.14	Importați informații despre persoană	93
8.4.15	Importarea imaginilor persoanei	94
8.4.16	Exportați informații despre persoană	95
8.4.17	Exportarea imaginilor persoanei	95
8.4.18	Obține informații despre persoană de la dispozitivul de control al accesului	95
8.4.19	Mutarea persoanelor într-o altă organizație	96
8.4.20	Emite carduri către persoane din lot	96
8.4.21	Pierderea buletinului de evaluare	97

8.4.22 Setarea parametrilor de emiterie a cardului	97
8.5 Configurarea programului și șablonului	98
8.5.1 Adăugați vacanță	98
8.5.2 Adăugați un șablon	99
8.6 Setați grupul de acces pentru a atribui autorizații de acces persoanelor	101
8.7 Configurarea funcțiilor avansate	103
8.7.1 Configurarea parametrilor dispozitivului	103
8.7.2 Configurarea rămas deschis/închis	109
8.7.3 Configurați autentificarea cu mai mulți factori	110
8.7.4 Configurarea modului și programării de autentificare a cititorului de carduri	112
8.7.5 Configurați prima persoană în	114
8.7.6 Configurare Anti-Passback	115
8.7.7 Configurarea parametrilor dispozitivului	116
8.8 Configurarea acțiunilor de conectare pentru controlul accesului	122
8.8.1 Configurarea acțiunilor clientului pentru evenimentul de acces	122
8.8.2 Configurarea acțiunilor dispozitivului pentru evenimentul de acces	123
8.8.3 Configurarea acțiunilor dispozitivului pentru trecerea cardului	124
8.8.4 Configurarea acțiunilor dispozitivului pentru ID-ul persoanei	126
8.9 Controlul ușii	127
8.9.1 Starea ușii de control	127
8.9.2 Verificați înregistrările de acces în timp real	128
8.10 Centru de evenimente	129
8.10.1 Activați primirea notificărilor de evenimente de la dispozitive	129
8.10.2 Vizualizare evenimente în timp real	129
8.10.3 Căutare evenimente istorice	132
8.11 Timp și prezență	135
8.11.1 Configurarea parametrilor de prezență	135
8.11.2 Adăugarea orarului general	140

8.11.3 Adăugați Shift	142
8.11.4 Gestionarea programului schimburilor	145
8.11.5 Corectarea manuală a înregistrării de check-in/out	148
8.11.6 Adăugați concediu și călătorie de afaceri	149
8.11.7 Calcularea datelor de prezență	150
8.11.8 Statistici de prezență	151
Anexa A. Sfaturi pentru scanarea amprentei	155
Anexa B. Sfaturi la colectarea/compararea imaginii feței	157
Anexa C. Sfaturi pentru mediul de instalare	159
Anexa D. Dimensiunea	160
Anexa E. Matricea de comunicații și comanda dispozitivului	162

Capitolul 1 Prezentare generală

1.1 Prezentare generală

Terminalul de recunoaștere a feței este un fel de dispozitiv de control al accesului pentru recunoașterea feței, care este aplicat în principal în sistemele de control al accesului de securitate, cum ar fi centre logistice, aeroporturi, campusuri universitare, centrale de alarmă, locuințe etc.

1.2 Caracteristici

Caracteristicile seriei normale

- Ecran tactil LCD de 7 inch
- Lentila dublă cu unghi larg de 2 MP
- Reglează manual luminozitatea luminii suplimentare
- Distanța de recunoaștere a feței: 0,3 m până la 3 m
- Înălțimea recomandată pentru recunoașterea feței: între 1,4 m și 1,9 m
- Algoritm de învățare profundă
- Capacitate de 5.000 de fețe, 5.000 de amprente și 50.000 de evenimente



Nota

Părți ale modelelor acceptă modulul de amprentă, consultați produsele reale.

- Mai multe moduri de autentificare
- Durata recunoașterii feței $< 0,2$ s/Utilizator; Rata de precizie a recunoașterii feței $\geq 99\%$
- Transmite datele cardului și utilizatorului de la sau către software-ul client prin protocolul TCP/IP și salvează datele pe software-ul client
- Importă imagini de pe unitatea flash USB pe dispozitiv sau exportă imagini, evenimente de pe dispozitiv pe unitatea flash USB
- Gestionarea dispozitivului, căutarea în jurnal și setările parametrilor prin intermediul dispozitivului
- Funcționare de sine stătătoare
- Legătura de captură și salvarea imaginilor capturate
- Se conectează la un cititor extern de carduri sau controler de acces prin protocolul RS-485
- Se conectează la controlerul de acces extern sau la cititorul de carduri Wiegand prin protocolul Wiegand
- Se conectează la unitatea de control securizată a ușii prin protocolul RS-485 pentru a evita deschiderea ușii atunci când terminalul este distrus
- Vizualizare live de la distanță prin protocolul RTSP; mod de codare: H.264
- NTP, sincronizare manuală a timpului și sincronizare automată
- Solicitare vocală
- Design Watchdog și funcție de manipulare

Caracteristicile seriei avansate

- Ecran tactil LCD de 7 inchi
- Lentila dublă cu unghi larg de 2 MP
- Reglează manual luminozitatea luminii suplimentare
- Distanța de recunoaștere a feței: 0,3 m până la 3 m
- Înălțimea recomandată pentru recunoașterea feței: între 1,4 m și 1,9 m
- Algoritm de învățare profundă
- Capacitate de 20.000 de fețe, 5.000 de amprente și 100.000 de evenimente



Nota

Părți ale modelelor acceptă modulul de amprentă, consultați produsele reale.

- Mai multe moduri de autentificare
- Durata recunoașterii feței $< 0,2$ s/Utilizator; Rata de precizie a recunoașterii feței $\geq 99\%$
- Transmite datele cardului și utilizatorului de la sau către software-ul client prin protocolul TCP/IP și salvează datele pe software-ul client
- Importă imagini de pe unitatea flash USB pe dispozitiv sau exportă imagini, evenimente de pe dispozitiv pe unitatea flash USB
- Gestionarea dispozitivului, căutarea în jurnal și setările parametrilor prin intermediul dispozitivului
- Funcționare de sine stătătoare
- Legătura de captură și salvarea imaginilor capturate
- Se conectează la un cititor extern de carduri sau controler de acces prin protocolul RS-485
- Se conectează la unitatea de control securizată a ușii prin protocolul RS-485 pentru a evita deschiderea ușii atunci când terminalul este distrus
- Se conectează la controlerul de acces extern sau la cititorul de carduri Wiegand prin protocolul Wiegand
- Vizualizare live de la distanță prin protocolul RTSP; mod de codare: H.264
- NTP, sincronizare manuală a timpului și sincronizare automată
- Solicitare vocală
- Design Watchdog și funcție de manipulare

Capitolul 2 Aspectul

Consultați următorul conținut pentru informații detaliate despre terminalul de recunoaștere a feței:

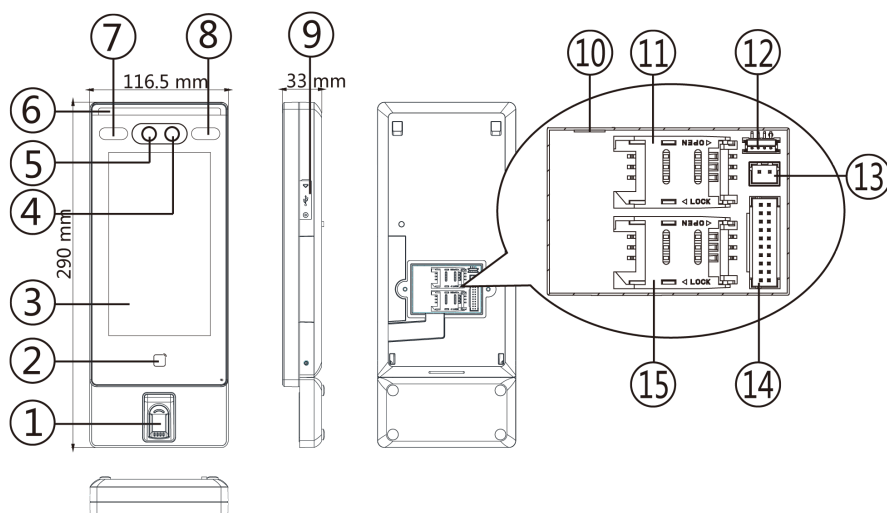


Figura 2-1 Diagrama terminalului de recunoaștere a feței

Tabelul 2-1 Descrierea terminalului de recunoaștere a feței

Nu.	Nume	Descriere
1	Modul de amprentă	Pentru recunoașterea amprenteii. Nota Doar anumite părți ale modelelor acceptă funcția de recunoaștere a amprenteii.
2	Zona de trecere a cardului	Glisați cardul în această zonă.
3	Ecran de afișare	Ecran tactil LCD de 7 inch.
4	Cameră (lumină IR)	Cameră cu lumină IR pentru înregistrarea sau captarea videoclipurilor sau imaginilor în lumină IR.
5	Cameră (lumină albă)	Cameră cu lumină albă pentru înregistrarea sau captarea videoclipurilor sau imaginilor cu lumină albă.
6	Lumină suplimentară (lumină albă)	Lumină suplimentară pentru camera cu lumină albă.
7	Lumină suplimentară (lumină IR)	Lumină suplimentară pentru camera IR.
8	Lumină suplimentară (lumină IR)	Lumină suplimentară pentru camera IR.
9	Interfață USB	Conectați-vă la unitatea flash USB.

Nu.	Nume	Descriere
10	Interfață de rețea	Conectați-vă la Ethernet.
11	Slot pentru card SIM	Rezervat
12	Port de depanare	Terminalul de depanare este folosit doar pentru depanare.
13	Interfață de alimentare	Conectați-vă la sursa de alimentare.
14	Terminale de cablare	Conectați-vă la alte dispozitive externe, inclusiv cititor de carduri RS-485, cititor de carduri Wiegand, încuietoare ușii, intrare alarmă, ieșire alarmă etc.
15	Slot pentru card PSAM	Rezervat

Capitolul 3 Instalare

3.1 Mediu de instalare

- Evitați lumina de fundal, lumina directă a soarelui și lumina indirectă a soarelui.
- Pentru o mai bună recunoaștere, ar trebui să existe o sursă de lumină în sau în apropierea mediului de instalare.



Nota

Pentru detalii despre mediul de instalare, consultați *Sfaturi pentru mediul de instalare*.

3.2 Instalați cu Gang Box

Pași

1. Conform liniei de referință de pe șablonul de montare, lipiți șablonul de montare pe perete sau pe altă suprafață, cu 1,4 metri mai înalt decât solul.

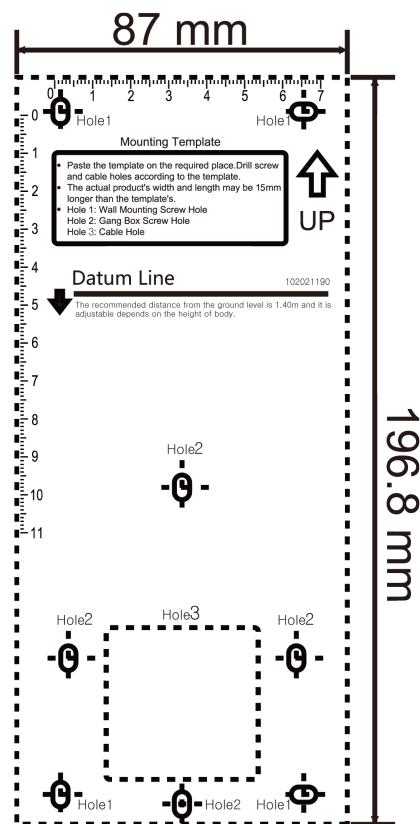


Figura 3-1 Șablon de montare

2. Găuriți găuri pe perete sau pe altă suprafață conform șablonului de montare și instalați cutia de grup.
3. Utilizați două șuruburi furnizate (4_KA4 × 22-SUS) pentru a fixa placa de montare pe cutia grupului.
4. Utilizați alte patru șuruburi furnizate pentru a fixa placa de montare pe perete.

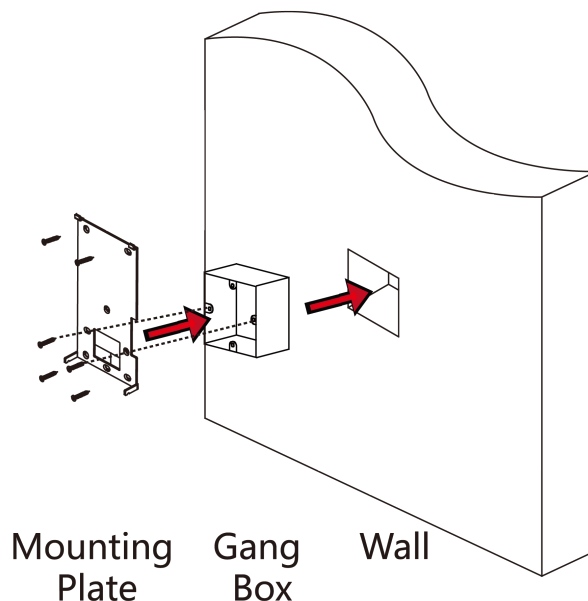


Figura 3-2 Instalarea plăcii de montare

5. Scoateți cele două șuruburi de pe panoul din spate și scoateți foaia pentru a afișa bornele cablajului.
6. Treceți cablul prin orificiul pentru cablu al plăcii de montare și conectați-l la cablurile dispozitivelor externe corespunzătoare.
7. Instalați foaia înapoi pe dispozitiv cu cele două șuruburi.
8. Aplicați etanșant siliconic printre zona cablurilor pentru a împiedica pătrunderea picăturii de ploaie.

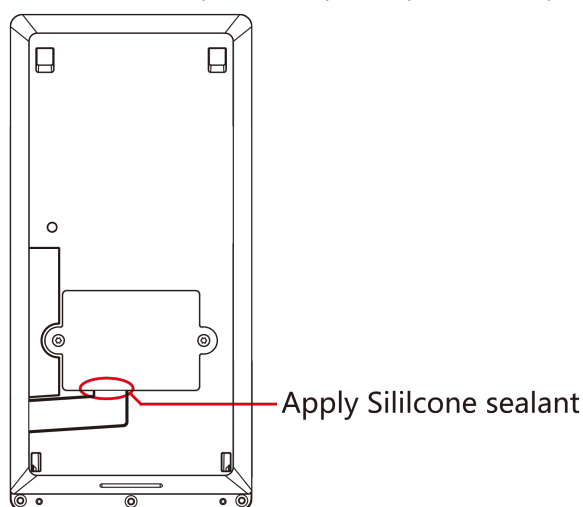


Figura 3-3 Aplicați etanșant siliconic

9. **Opțional:** Introduceți modulul de amprentă în găurile din partea de jos a părții principale.

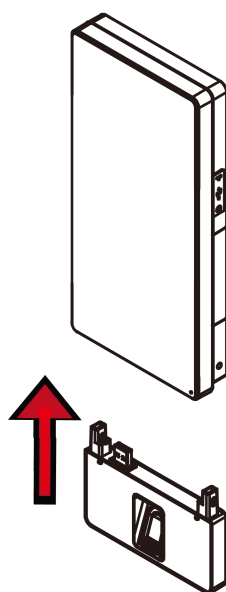


Figura 3-4 Inserați modulul de amprentă

10. Aliniați dispozitivul cu placa de montare și agățați dispozitivul pe placa de montare.

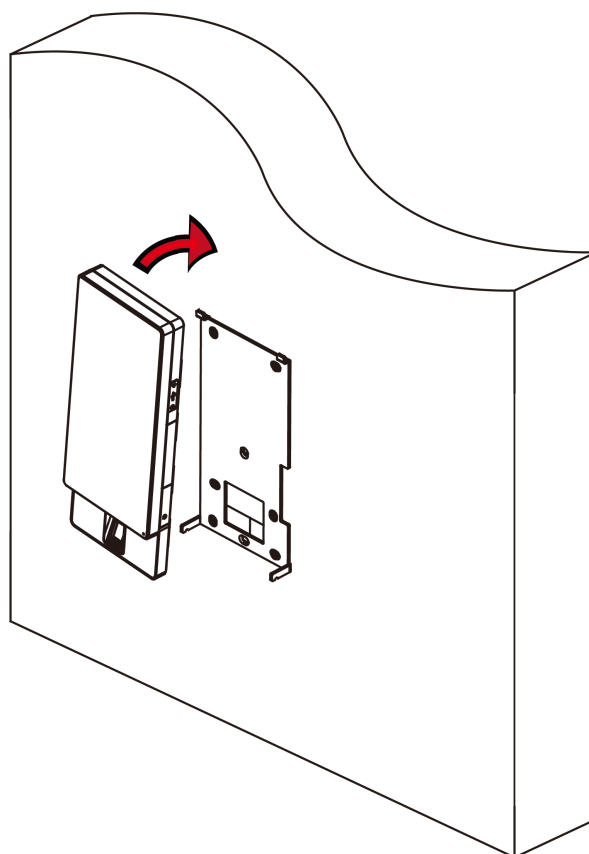


Figura 3-5 Instalare dispozitiv

11. Utilizați două șuruburi furnizate (SC-M4 × 12TP10-SUS) pentru a fixa dispozitivul și placa de montare.

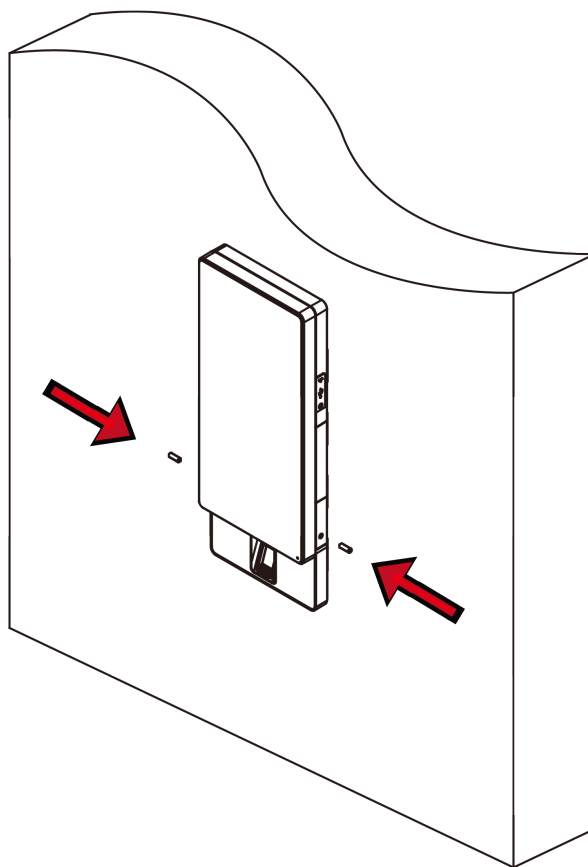


Figura 3-6 Dispozitiv securizat



Nota

- Înălțimea de instalare aici este înălțimea recomandată. Îl poți schimba în funcție de nevoile tale reale.
 - Pentru o instalare ușoară, găuriți pe suprafața de montare conform șablonului de montare furnizat.
-

3.3 Instalați fără Gang Box

Pași

- 1.** Conform liniei de referință de pe șablonul de montare, lipiți șablonul de montare pe perete sau pe altă suprafață, cu 1,4 metri mai înalt decât solul.

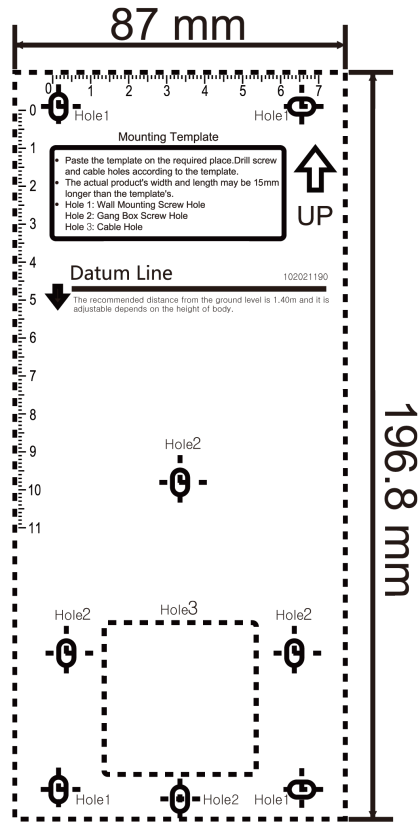


Figura 3-7 Șablon de montare

2. Găuriți 6 găuri pe perete sau pe altă suprafață conform găurii 1 și 2 din șablonul de montare.

3. Introduceți mufurile șuruburilor de fixare în găurile forate.

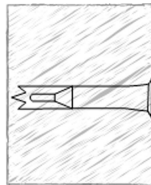


Figura 3-8 Introduceți mufa șurub

4. Aliniați cele 6 găuri la placa de montare cu găurile găurite.

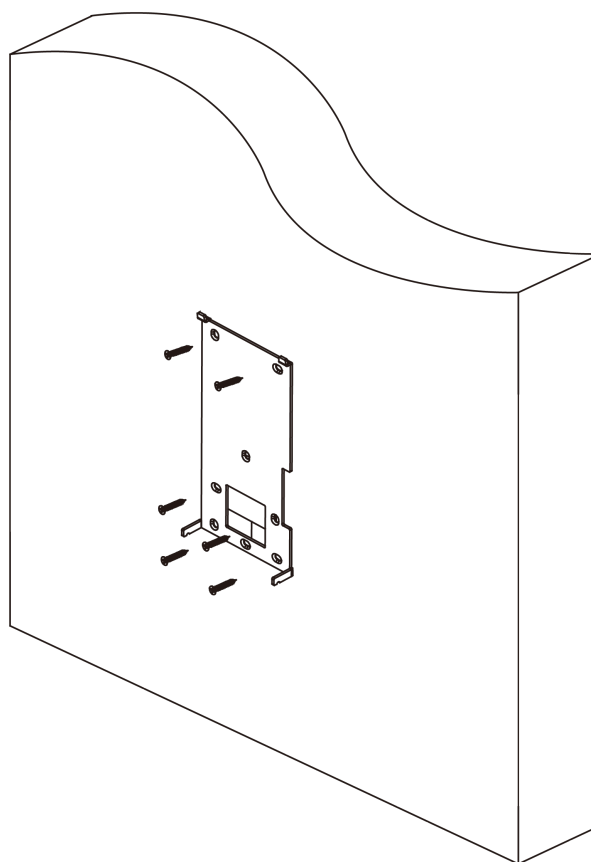


Figura 3-9 Instalarea plăcii de montare

- 5.** Scoateți cele două șuruburi de pe panoul din spate și scoateți foaia pentru a afișa bornele cablajului.
- 6.** Treceți cablul prin orificiul pentru cablu al plăcii de montare și conectați-l la cablurile dispozitivelor externe corespunzătoare.
- 7.** Instalați foaia înapoi pe dispozitiv cu cele două șuruburi.
- 8.** Aplicați etanșant siliconic printre zona cablurilor pentru a împiedica pătrunderea picăturii de ploaie.

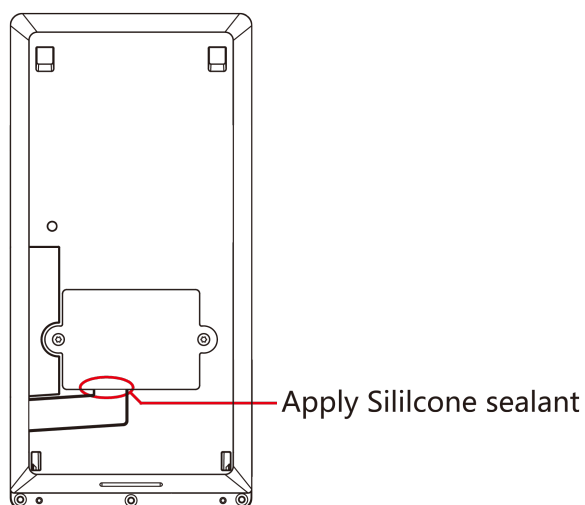


Figura 3-10 Aplicați etanșant siliconic

9.Introduceți modulul de amprentă în găurile din partea de jos a părții principale.

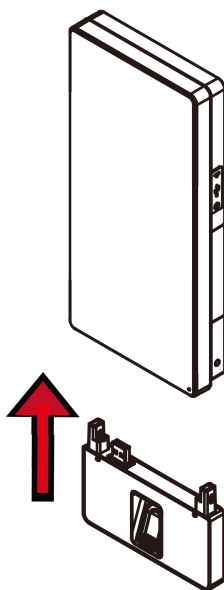


Figura 3-11 Instalarea modului de amprentă digitală

10.Aliniați dispozitivul cu placa de montare și agățați dispozitivul pe placa de montare.

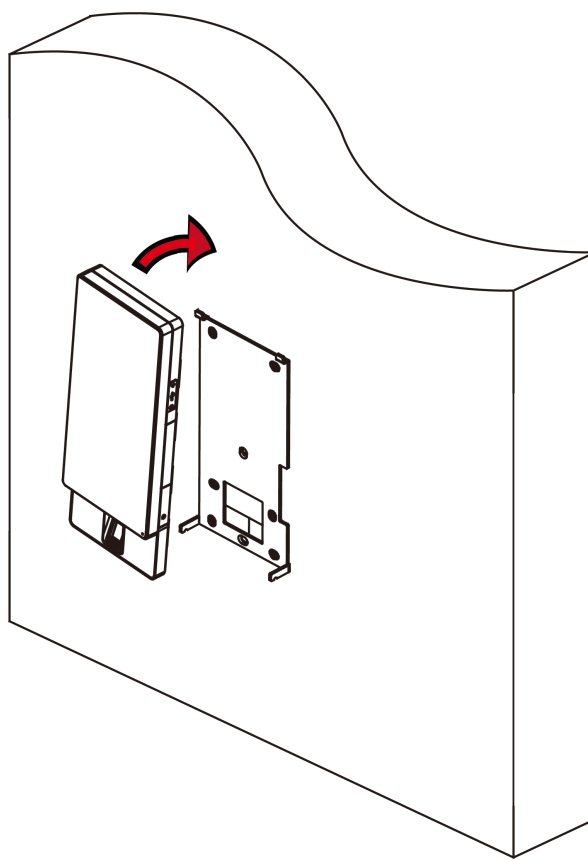


Figura 3-12 Instalare dispozitiv

11. Utilizați două șuruburi furnizate (SC-M4 × 12TP10-SUS) pentru a fixa dispozitivul și placa de montare.

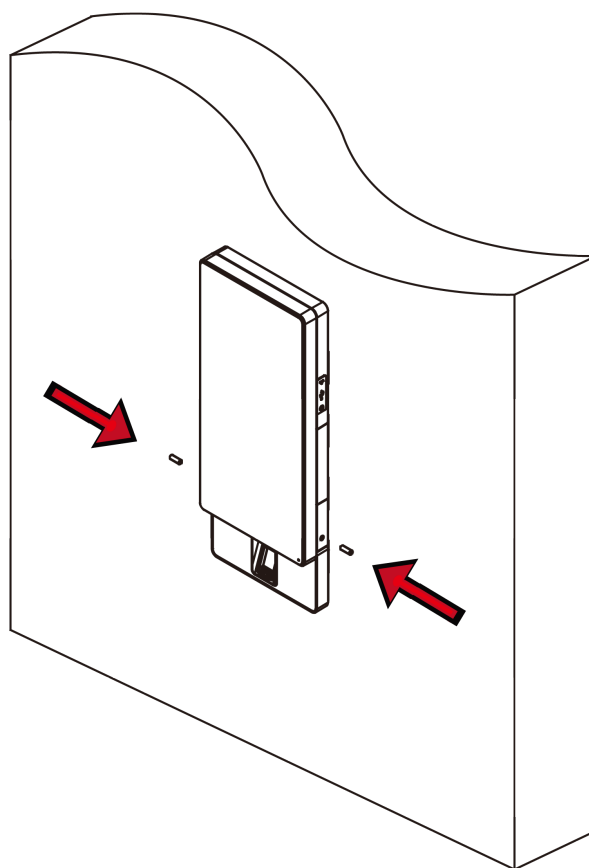


Figura 3-13 Dispozitiv securizat

 Nota

- Înălțimea de instalare aici este înălțimea recomandată. Îl poți schimba în funcție de nevoile tale reale.
 - Pentru o instalare ușoară, găuriți pe suprafața de montare conform șablonului de montare furnizat.
-

Capitolul 4 Cablaj

Puteți conecta terminalul RS-485 la cititorul de carduri RS-485, conectați terminalul NC și COM cu încuietoarea ușii, conectați terminalul SENSOR cu contactul ușii, terminalul BTN/GND cu butonul de ieșire, conectați ieșirea și terminalul de intrare de alarmă cu dispozitivele de ieșire/intrare de alarmă și conectați terminalul Wiegand cu cititorul de carduri Wiegand sau controlerul de acces.

Dacă conectați terminalul WIEGAND cu controlerul de acces, terminalul de recunoaștere a feței poate transmite informațiile de autentificare controlerului de acces, iar controlerul de acces poate decide dacă deschide ușa sau nu.



Nota

- Dacă dimensiunea cablului este de 18 AWG, ar trebui să utilizați o sursă de alimentare de 12 V. Și distanța dintre sursa de alimentare și dispozitiv nu trebuie să fie mai mare de 20 m.
 - Dacă dimensiunea cablului este de 15 AWG, ar trebui să utilizați o sursă de alimentare de 12 V. Și distanța dintre sursa de alimentare și dispozitiv nu trebuie să fie mai mare de 30 m.
 - Dacă dimensiunea cablului este de 12 AWG, ar trebui să utilizați o sursă de alimentare de 12 V. Și distanța dintre sursa de alimentare și dispozitiv nu trebuie să fie mai mare de 40 m.
-

4.1 Descrierea terminalului

Terminalele conțin intrarea de alimentare, intrarea alarmă, ieșirea alarmei, RS-485, ieșirea Wiegand și blocarea ușii.

Schema terminalului este următoarea:

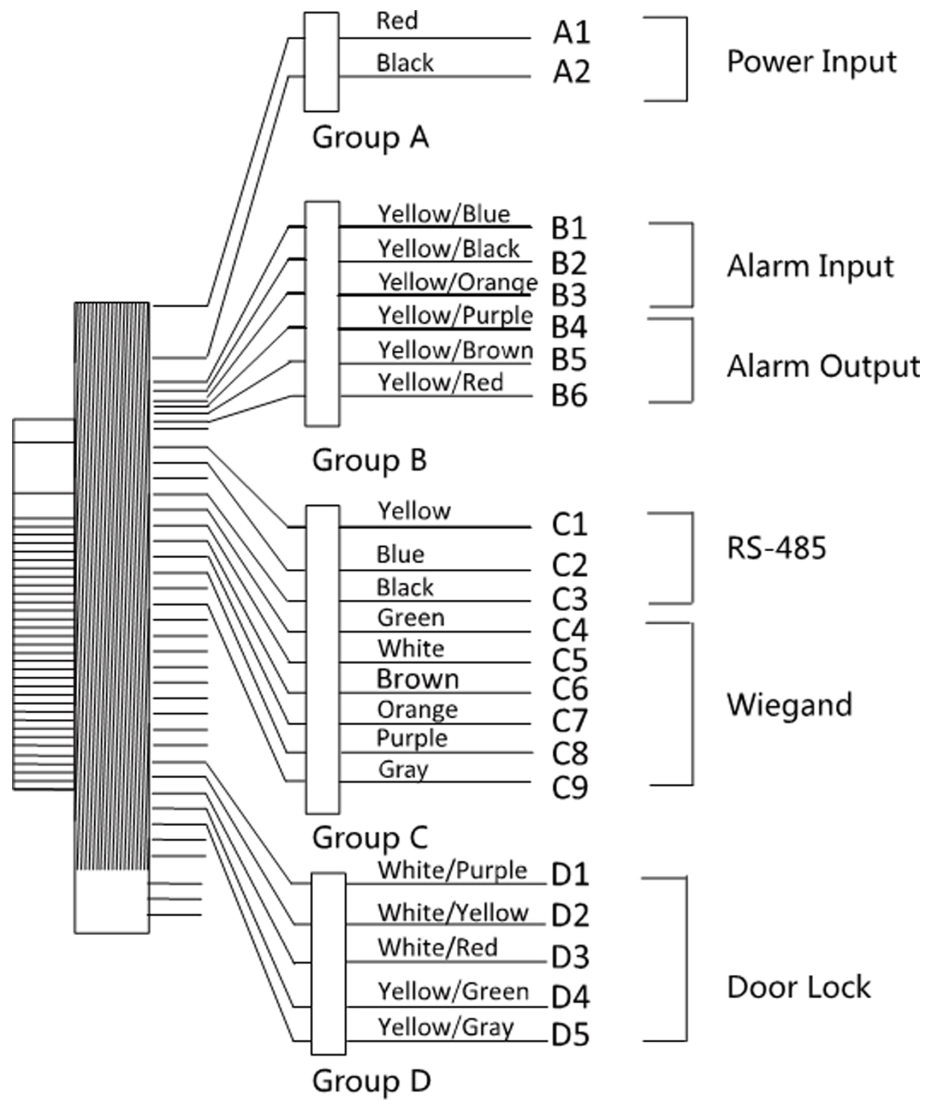


Figura 4-1 Diagrama terminalelor

Descrierile terminalelor sunt următoarele:

Tabelul 4-1 Descrieri terminale

Grup	Nu.	Funcție	Culoare	Nume	Descriere
Grupa A	A1	Intrare de putere	Roșu	+ 12 V	Alimentare 12 VDC Livra
	A2		Negru	GND	Sol
Grupa B	B1	Intrare alarmă	Galben/Albastru	IN1	Intrare alarmă 1
	B2		Galben/Negru	GND	Sol
	B3		Galben/Portocaliu	IN2	Intrare alarmă 2

Grup	Nu.	Funcție	Culoare	Nume	Descriere
	B4	Ieșire de alarmă	Galben/Mov	NC	Ieșire de alarmă Cablaj
	B5		Galben/Maro	COM	
	B6		Galben/Roșu	NU	
Grupa C	C1	RS-485	Galben	485+	Cablaj RS-485
	C2		Albastru	485-	
	C3		Negru	GND	Sol
	C4	Wiegand	Verde	W0	Wiegand Cablaj 0
	C5		Alb	W1	Wiegand Cablaj 1
	C6		Maro	WG_OK	Wiegand Autentificat
	C7		Portocale	WG_ERR	Wiegand Autentificare A eșuat
	C8		Violet	BUZZER	Cablajul soneriei
	C9		Gri	TAMPER	Falsificarea Cablaj de alarmă
Grupa D	D1	Încuietoarea ușii	Alb/Mov	NC	Cablaj de blocare (NC)
	D2		Alb/Galben	COM	Comun
	D3		Alb/Roșu	NU	Cablaj de blocare (NU)
	D4		Galben/Verde	SENSOR	Contact la ușă
	D5		Galben/gri	BTN	Ușa de ieșire Cablaj

4.2 Cablare Dispozitiv normal

Puteți conecta terminalul cu periferice normale.

Schema de cablare fără unitatea de comandă sigură a ușii este următoarea.

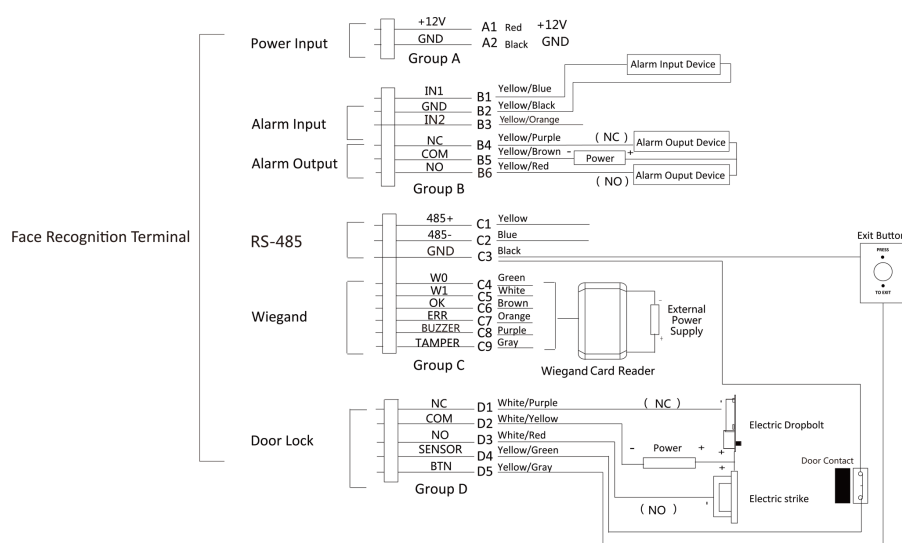


Figura 4-2 Cablajul dispozitivului

Nota

- Ar trebui să setați direcția Wiegand a terminalului de recunoaștere a feței la „Intrare” pentru a vă conecta la un cititor de carduri Wiegand. Dacă se conectează la un controler de acces, ar trebui să setați direcția Wiegand la „Ieșire” pentru a transmite informații de autentificare către controlerul de acces.
- Pentru detalii despre setările direcției Wiegand, consultați *Setarea parametrilor Wiegand* în *Setări de comunicare*.
- Sursa de alimentare externă recomandată pentru încuietoarea ușii este de 12 V, 1 A. Sursa de alimentare externă sugerată pentru cititorul de carduri Wiegand este de 12 V, 1 A.
- Diametrul sugerat al cablului de alimentare: 22 AWG. Diametrul sugerat al celuilalt cablu: 26 AWG.
- Nu conectați dispozitivul direct la sursa electrică.

Avertizare

Terminalul de recunoaștere a feței va adapta o sursă de alimentare externă de Clasa 2, cu funcție de protecție la supratensiune.

4.3 Unitatea de comandă a ușii securizate prin cablu

Puteți conecta terminalul cu unitatea de control a ușii securizate. Schema de cablare este următoarea.

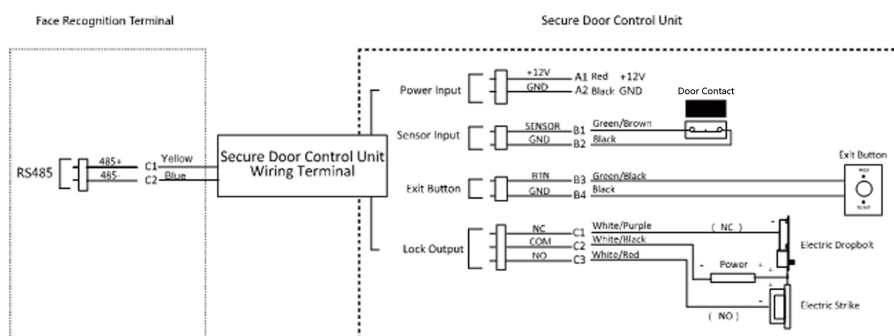


Figura 4-3 Cablajul unității de comandă a ușii securizate

Nota

Unitatea de control a ușii securizate trebuie să se conecteze separat la o sursă de alimentare externă. Sursa de alimentare externă recomandată este de 12V, 0,5A.

Capitolul 5 Activare

Ar trebui să activați dispozitivul înainte de prima conectare. După pornirea dispozitivului, sistemul va comuta la pagina Activare dispozitiv.

Activarea prin dispozitiv, instrumentul SADP și software-ul client sunt acceptate.

Valorile implicite ale dispozitivului sunt următoarele:

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

5.1 Activați prin dispozitiv

Dacă dispozitivul nu este activat, îl puteți activa după ce este pornit.

Pe pagina Activare dispozitiv, creați o parolă și confirmați-o. Robinet**Activa** iar dispozitivul se va activa.

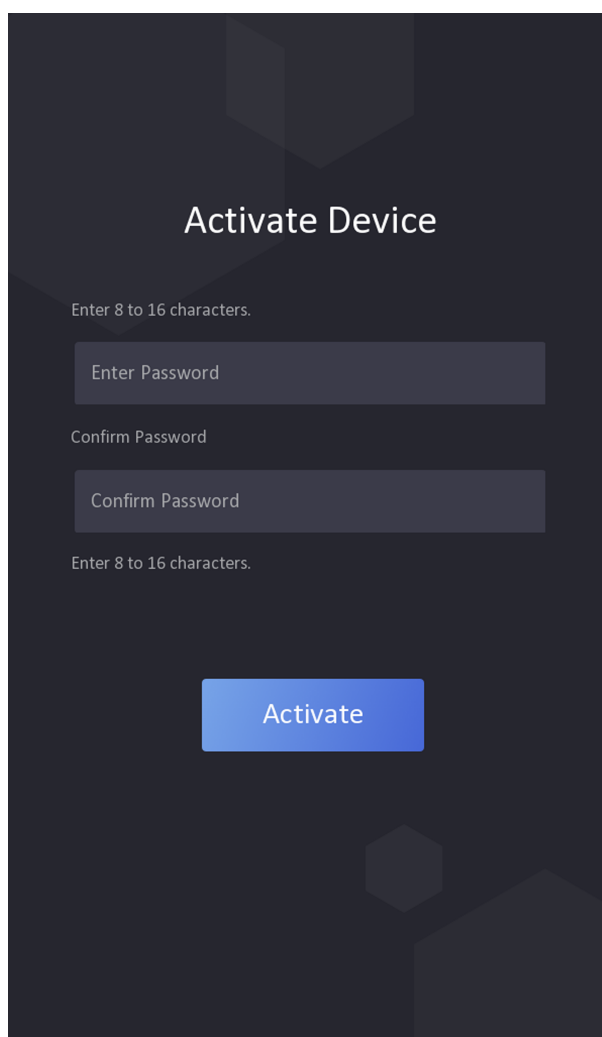


Figura 5-1 Pagina de activare

 Atenție

Puterea parolei dispozitivului poate fi verificată automat. Vă recomandăm cu căldură să schimbați parola pe care o alegeți (folosind minim 8 caractere, incluzând cel puțin trei tipuri de următoarele categorii: litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dumneavoastră. Și vă recomandăm să vă schimbați parola în mod regulat, mai ales în sistemul de înaltă securitate, schimbarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

Configurarea corectă a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau utilizatorului final.

-
- După activare, ar trebui să selectați un mod de aplicație. Pentru detalii, vezi **Setați modul de aplicare**
 - După activare, dacă trebuie să adăugați dispozitivul la software-ul client sau la alte platforme, ar trebui să editați adresa IP a dispozitivului. Pentru detalii, vezi *Setări de comunicare*.

5.2 Activați prin SADP

SADP este un instrument pentru detectarea, activarea și modificarea adresei IP a dispozitivului prin LAN.

Înainte de a începe

- Obțineți software-ul SADP de pe discul furnizat sau de pe site-ul web oficial [http:// www.hikvision.com/en/](http://www.hikvision.com/en/), și instalați SADP conform instrucțiunilor.
- Dispozitivul și computerul care rulează instrumentul SADP ar trebui să fie în aceeași subrețea.

Următorii pași arată cum să activați un dispozitiv și să modificați adresa IP a acestuia. Pentru activarea lotului și modificarea adreselor IP, consultați *Manual de utilizare al SADP* pentru detalii.

Pași

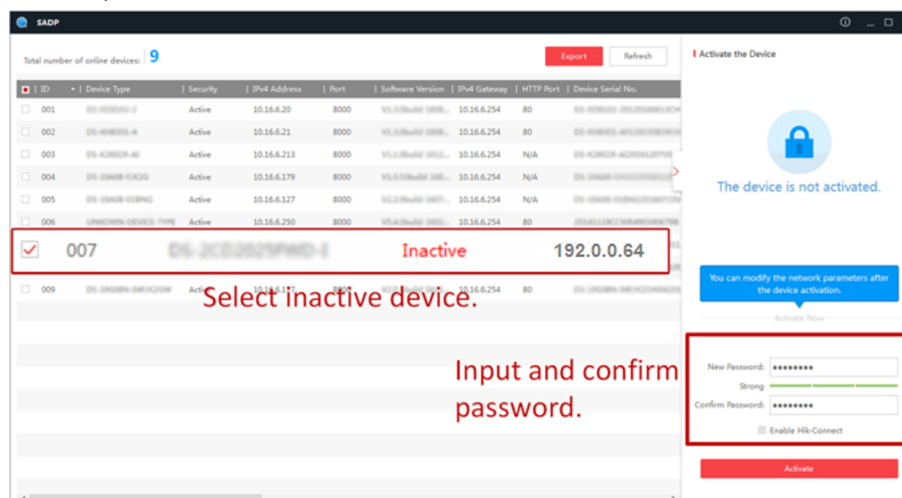
1. Rulați software-ul SADP și căutați dispozitivele online.
2. Găsiți și selectați dispozitivul dvs. în lista de dispozitive online.
3. Introduceți o nouă parolă (parolă de administrator) și confirmați parola.



Atenție

RECOMANDĂ PAROLĂ SURBA-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 dumneavoastră. 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. Clic **Activă** pentru a începe activarea.



Starea dispozitivului devine **Activ** după activarea cu succes.

5. Modificați adresa IP a dispozitivului.

- 1) Selectați dispozitivul.
- 2) Schimbați adresa IP a dispozitivului la aceeași subrețea ca și computerul dvs. fie modificând adresa IP manual, fie verificând **Activați DHCP**.
- 3) Introduceți parola de administrator și faceți clic **Modifică** pentru a activa modificarea adresei IP.

5.3 Activați dispozitivul prin software-ul client

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.

Pași



Nota

Această funcție ar trebui să fie acceptată de dispozitiv.

1. Accesați pagina Device Management.

2. Faceți clic în partea dreaptă a **Managementul dispozitivelor** și selectați **Dispozitiv**.

3. Clic **Dispozitiv online** pentru a afișa zona dispozitivului online.

Dispozitivele online căutate sunt afișate în listă.

4. Verificați starea dispozitivului (afișat pe **Nivel de securitate** coloană) și selectați un dispozitiv inactiv.

5. Clic **Activă** pentru a deschide dialogul Activare.

6. Creați o parolă în câmpul pentru parolă și confirmați parola.



Atenție

Puterea parolei dispozitivului poate fi verificată automat. Vă recomandăm cu căldură să schimbați parola pe care o alegeți (folosind minim 8 caractere, incluzând cel puțin trei tipuri de următoarele categorii: litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dumneavoastră. Și vă recomandăm să vă schimbați parola în mod regulat, mai ales în sistemul de înaltă securitate, schimbarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

Configurarea corectă a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau utilizatorului final.

7. Clic **Bine** pentru a activa dispozitivul.

Capitolul 6 Operarea de bază

6.1 Selectați limba

Puteți selecta o limbă pentru sistemul dispozitivului.

După activarea dispozitivului, puteți selecta o limbă pentru sistemul dispozitivului.

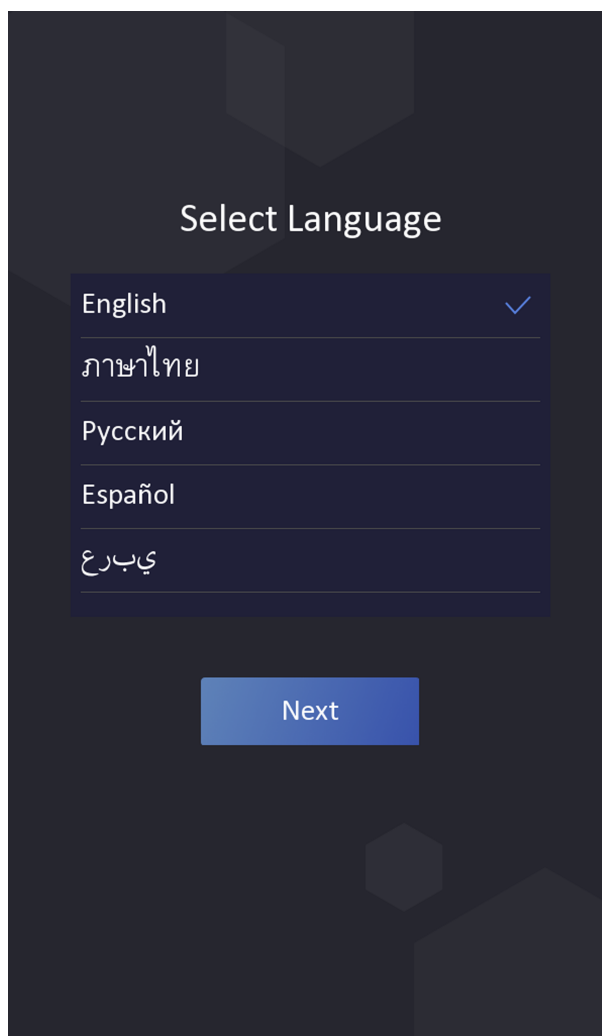


Figura 6-1 Selectați limba sistemului

În mod implicit, limba sistemului este engleza.

6.2 Setați modul de aplicare

După activarea dispozitivului, ar trebui să selectați un mod de aplicație pentru o aplicație mai bună a dispozitivului.

Pași

1. Pe pagina Bun venit, selectați **De interior** sau **Alții** din lista derulantă.

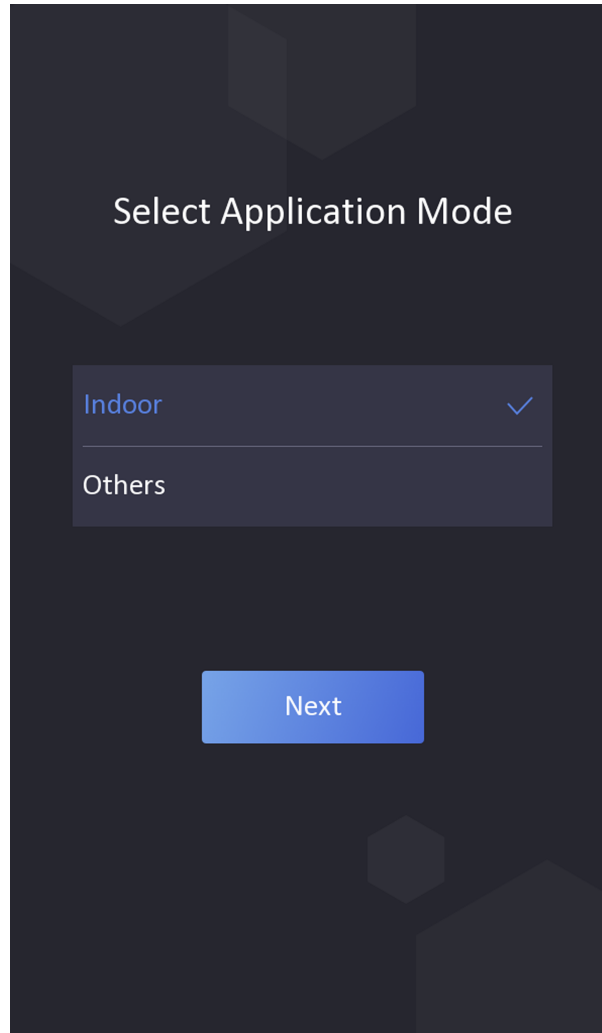


Figura 6-2 Pagina de întâmpinare

2. Robinet **B**ine a salva.



Nota

- De asemenea, puteți modifica setările în *Setări de sistem*.
 - Dacă instalați dispozitivul în interior, lângă fereastră sau dacă funcția de recunoaștere a feței nu funcționează bine, selectați **Alții**.
 - Dacă nu configurați modul de aplicație și atingeți **Următorul**, sistemul va selecta **De interior** implicit.
 - Dacă activați dispozitivul prin alte instrumente de la distanță, sistemul va selecta **De interior** ca mod implicit de aplicație.
-

6.3 Setări administrator

După activarea dispozitivului, puteți adăuga un administrator pentru a gestiona backend-ul.

Înainte de a începe

Activați dispozitivul și selectați un mod de aplicație.

Pași



Nota

RobinetSari peste pentru a sări peste adăugarea administratorului.

1.Introduceți numele administratorului (opțional) și atingeți **Următorul**.

Figura 6-3 Adăugați pagina de administrator

2.Selectați o autentificare de adăugat.

Nota

Ar trebui adăugată până la o acreditare.

-  : Cu fața în față spre cameră. Asigurați-vă că fața se află în zona de recunoaștere a feței. Faceți clic pentru a  captura și faceți clic pentru a  confirma.
-  : Apăsați cu degetul conform instrucțiunilor de pe ecranul dispozitivului. Faceți clic pentru a  confirma.
-  : Introduceți numărul cardului sau prezentați cardul în zona de prezentare a cardului. Clic **Bine**.

3. Clic **Bine**.

Veți intra pe pagina de autentificare.

Descriere pictogramă de stare



Dispozitivul este armat/



Rețeaua prin cablu a dispozitivului este conectată/nu este conectată/conectarea a eșuat.



Wi-Fi-ul dispozitivului este activat și conectat/nu este conectat/activat, dar nu este conectat. **Tastele de**

comandă rapidă **Descriere**

Nota

Puteți configura acele taste de comandă rapidă afișate pe ecran. Pentru detalii, vezi **Setări de bază**.



Scanați codul QR pentru a vă autentifica.

Nota

Codul QR poate fi obținut de la terminalul pentru vizitatori.



- Introduceți numărul camerei dispozitivului și atingeți **Bine** a suna.
- Atingeți  pentru a apela centrul.

Nota

Dispozitivul trebuie adăugat la centru, altfel operațiunea de apelare va eșua.



Introduceți parola pentru autentificare.

6.4 Conectare

Conectați-vă la backend-ul dispozitivului pentru a seta parametrii de bază ale dispozitivului.

6.4.1 Conectare de către administrator

Dacă ați adăugat un administrator pentru dispozitiv, numai administratorul se poate autentifica pe dispozitiv pentru operarea dispozitivului.

Pași

1. Atingeți lung pe pagina inițială timp de 3 secunde și glisați spre stânga/dreapta urmând gestul pentru a intra în pagina de autentificare admin.

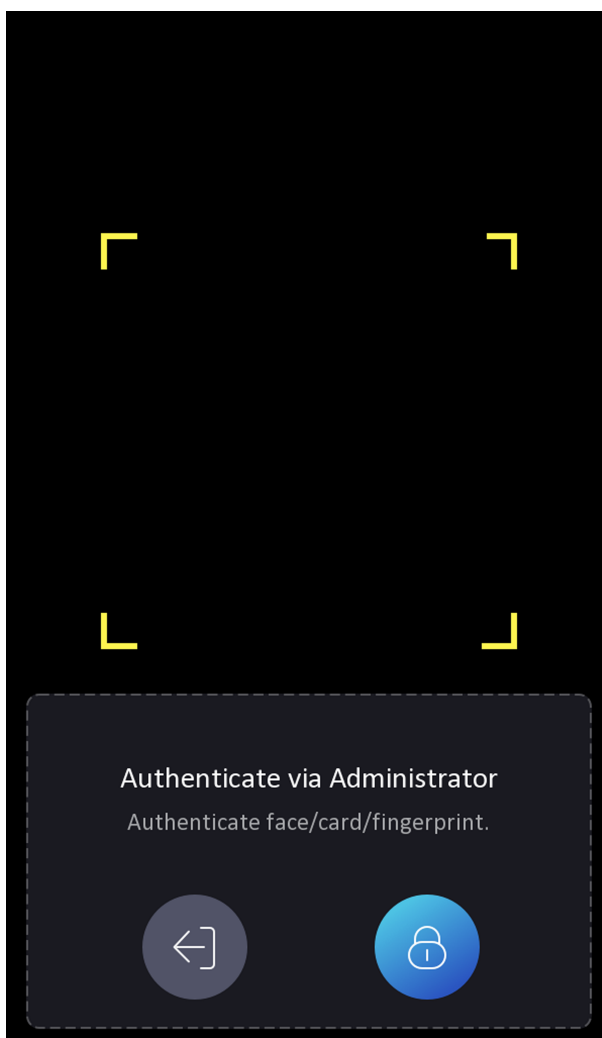


Figura 6-4 Conectare administrator

2. Autentificați fața, amprenta sau cardul administratorului pentru a intra în pagina de pornire.

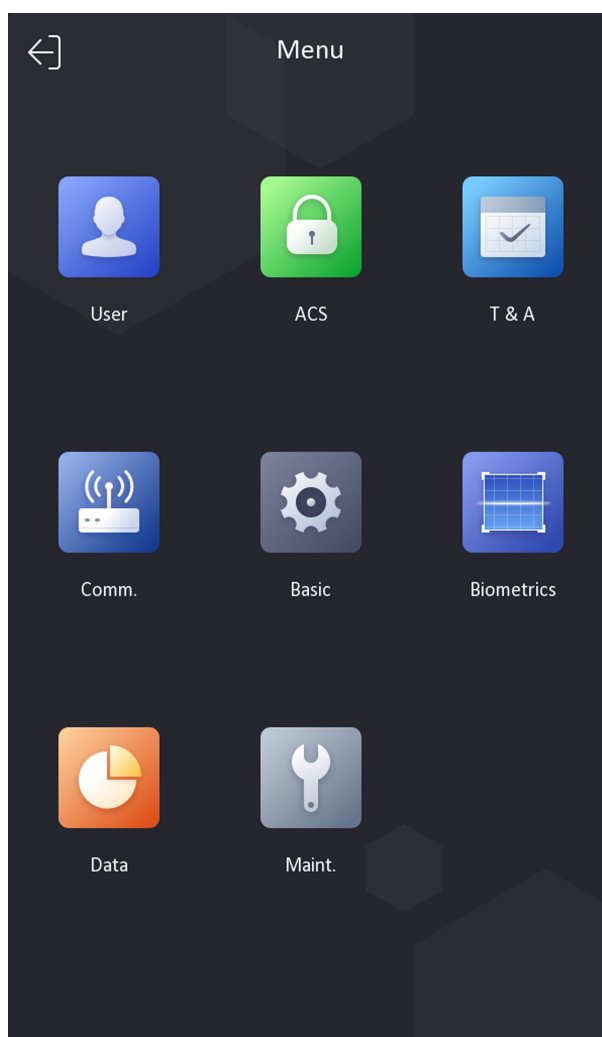


Figura 6-5 Pagina principală

Nota

Dispozitivul va fi blocat timp de 30 de minute după 5 încercări eșuate de amprentă sau card.

- 3. Opțional:** Robinet  și puteți introduce parola de activare a dispozitivului pentru autentificare. și
- 4. Opțional:** Robinet  puteți ieși din pagina de autentificare admin.

6.4.2 Conectare prin parola de activare

Ar trebui să vă conectați la sistem înainte de operațiunile altor dispozitive. Dacă nu configurați un administrator, ar trebui să urmați instrucțiunile de mai jos pentru a vă autentifica.

Pași

1. Atingeți lung pe pagina inițială timp de 3 secunde și glisați spre stânga/dreapta urmând gestul pentru a introduce pagina de introducere a parolei.

2. Atingeți câmpul Parolă și introduceți parola de activare a dispozitivului.

3. Robinet **Bine** pentru a intra pe pagina de start.

 Nota

Dispozitivul va fi blocat timp de 30 de minute după 5 încercări eșuate de parolă.

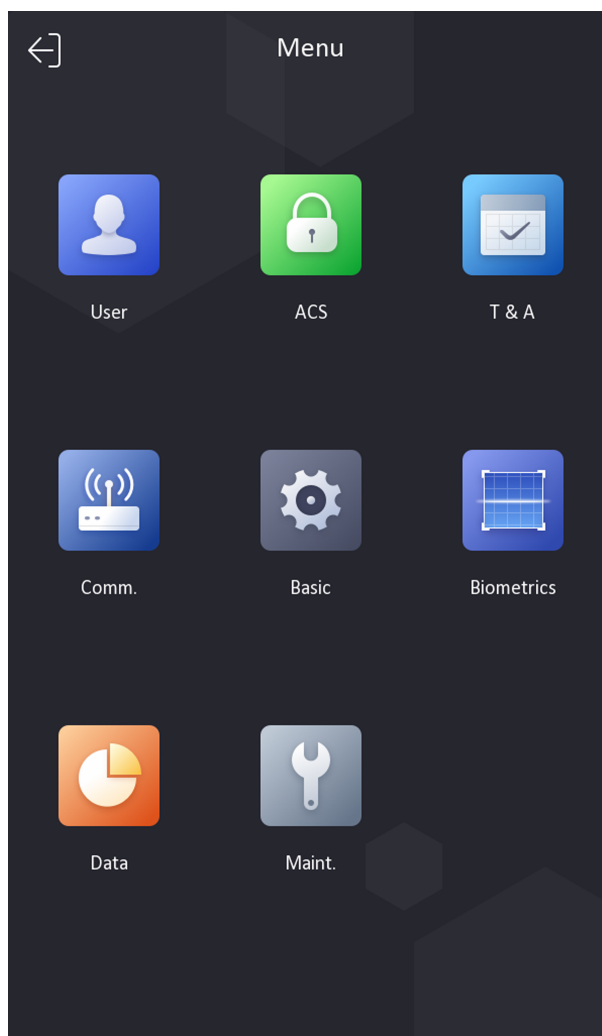


Figura 6-6 Pagina de pornire

6.5 Setări de comunicare

Puteți seta parametrii rețelei, parametrul Wi-Fi și parametrii RS-485 pe pagina de setări de comunicare.

6.5.1 Setări parametrul rețelei cu fir

Puteți seta parametrul rețelei prin cablu a dispozitivului, inclusiv adresa IP, masca de subrețea și gateway-ul.

Pași

1. Robinet**Comm.**(Communication Settings) pe pagina de pornire pentru a accesa pagina Communication Settings.

2. Pe pagina Setări de comunicare, atingeți **Rețea cu fir**.

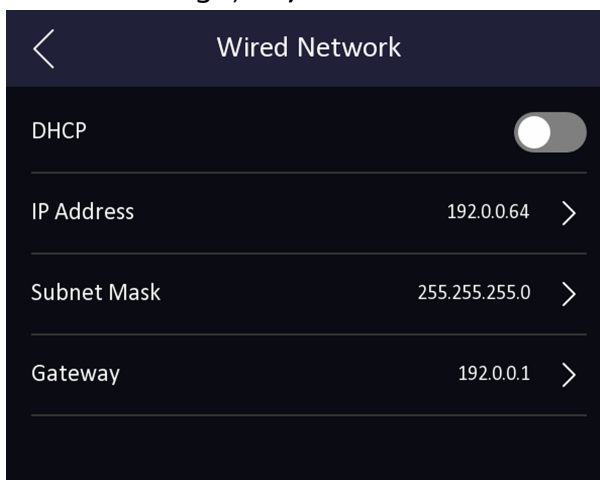


Figura 6-7 Setări de rețea cu fir

3. Setări DHCP, Adresă IP, Mască de subrețea sau Gateway.

Nota

Adresa IP a dispozitivului și adresa IP a computerului ar trebui să fie în același segment IP.

6.5.2 Setări parametrul Wi-Fi

Puteți activa funcția Wi-Fi și puteți seta parametrul aferenți Wi-Fi.

Pași

Nota

Funcția ar trebui să fie acceptată de dispozitiv.

1. Robinet**Comm.**(Communication Settings) pe pagina de pornire pentru a accesa pagina Communication Settings.

2. Pe pagina Setări de comunicare, atingeți.

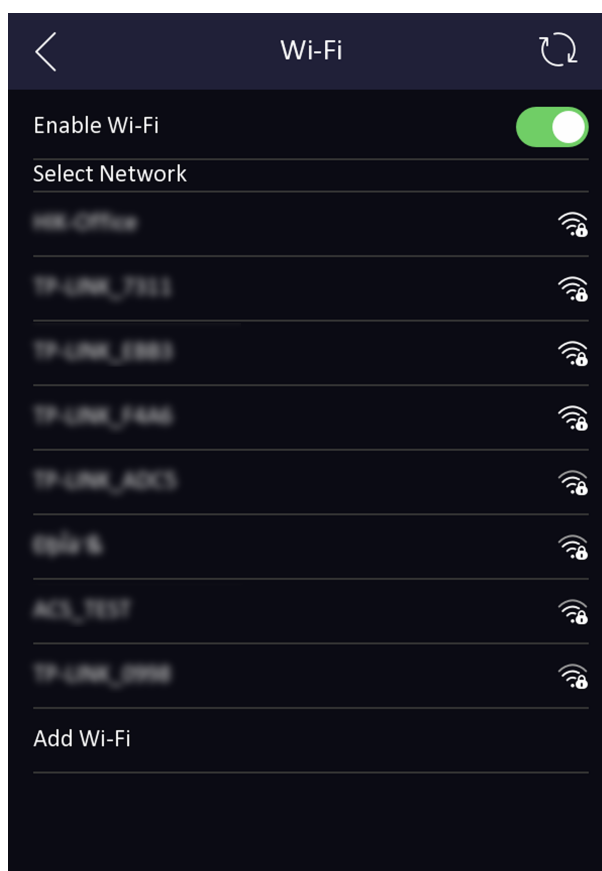


Figura 6-8 Setări Wi-Fi

3.Activați funcția Wi-Fi.

4.Configurați parametrii Wi-Fi.

- Selectați un Wi-Fi din listă și introduceți parola Wi-Fi. Robinet**Bine**.
- Dacă Wi-Fi-ul țintă nu este în listă, atingeți**Adăugați Wi-Fi**. Introduceți numele și parola Wi-Fi. Și atingeți **Bine**.



Nota

În parolă sunt permise doar cifre, litere și caractere speciale.

5.Setați parametrii Wi-Fi.

- În mod implicit, DHCP este activat. Sistemul va aloca automat adresa IP, masca de subrețea și gateway-ul.
- Dacă dezactivați DHCP, trebuie să introduceți manual adresa IP, masca de subrețea și gateway-ul.

6.Robinet**Bine**pentru a salva setările și a reveni la fila Wi-Fi.

7.Atingețipentru a salva parametrii rețelei.

6.5.3 Setarea parametrilor RS-485

Terminalul de recunoaștere a feței poate conecta controlerul de acces extern, unitatea de control a ușii securizate sau cititorul de carduri prin terminalul RS-485.

Pași

1. Robinet**Comm.**(Communication Settings) pe pagina de pornire pentru a accesa pagina Communication Settings.

2. Pe pagina Setări de comunicare, atingeți **RS-485** pentru a intra în fila RS-485.

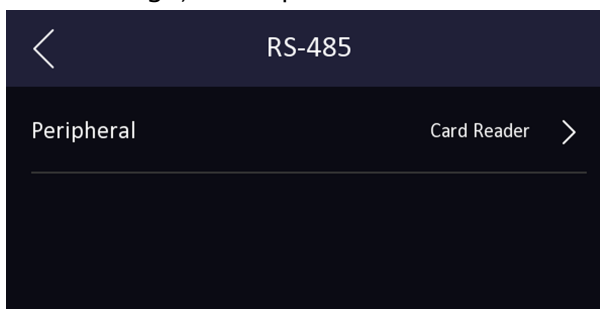


Figura 6-9 Setări parametrilor RS-485

3. Selectați un tip de periferic în funcție de nevoile dvs. reale.



Nota

Dacă selectați **Controler de acces**: Dacă conectați dispozitivul la un terminal prin interfața RS-485, setați adresa RS-485 la 2. Dacă conectați dispozitivul la un controler, setați adresa RS-485 conform ușii nr.

4. Atingeți pictograma din spate din colțul din stânga sus și ar trebui să reporniți dispozitivul dacă modificați parametrii.

6.5.4 Setarea parametrilor Wiegand

Puteți seta direcția de transmisie Wiegand.

Pași

1. Robinet**Comm.**(Communication Settings) pe pagina de pornire pentru a accesa pagina Communication Settings.

2. Pe pagina Setări de comunicare, atingeți **Wiegand** pentru a intra în fila Wiegand.

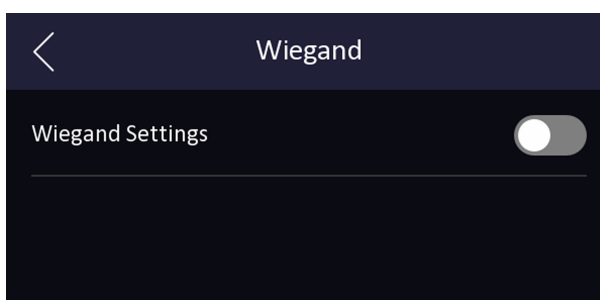


Figura 6-10 Setări Wiegand

3.Activați funcția Wiegand.

4.Selectați o direcție de transmisie.

- Ieșire: Un terminal de recunoaștere a feței poate conecta un controler de acces extern. Și cele două dispozitive vor transmite cardul nr. prin Wiegand 26 sau Wiegand 34.
- Intrare: Un terminal de recunoaștere a feței poate conecta un cititor de carduri Wiegand.

5.Atingeți  pentru a salva parametrii rețelei.



Nota

Dacă schimbați dispozitivul extern și după ce salvați parametrii dispozitivului, dispozitivul se va reporni automat.

6.6 Managementul utilizatorilor

Pe interfața de gestionare a utilizatorilor, puteți adăuga, edita, șterge și căuta utilizatorul.

6.6.1 Adăugați imaginea feței

Adăugați imaginea feței utilizatorului pe dispozitiv. Și utilizatorul poate folosi imaginea feței pentru a se autentifica.

Pași

1.Atingeți lung pe pagina inițială timp de 3 secunde și glisați spre stânga/dreapta urmând gestul și conectați-vă în backend.

2.Robinet**Utilizator** → +pentru a intra în pagina Adăugare utilizator.

3.Editați ID-ul angajatului.



Nota

- ID-ul angajatului trebuie să aibă mai puțin de 32 de caractere. Și poate fi o combinație de litere mici, litere mari și cifre.
 - ID-ul angajatului nu trebuie duplicat.
-

4.Atingeți câmpul Nume și introduceți numele de utilizator pe tastatura soft.

 Nota

- În numele de utilizator sunt permise numere, litere mari, litere mici și caractere speciale.
 - Numele de utilizator sugerat trebuie să aibă maximum 32 de caractere.
-

5. Atingeți câmpul Imagine feței pentru a intra în pagina de adăugare a imaginii feței.

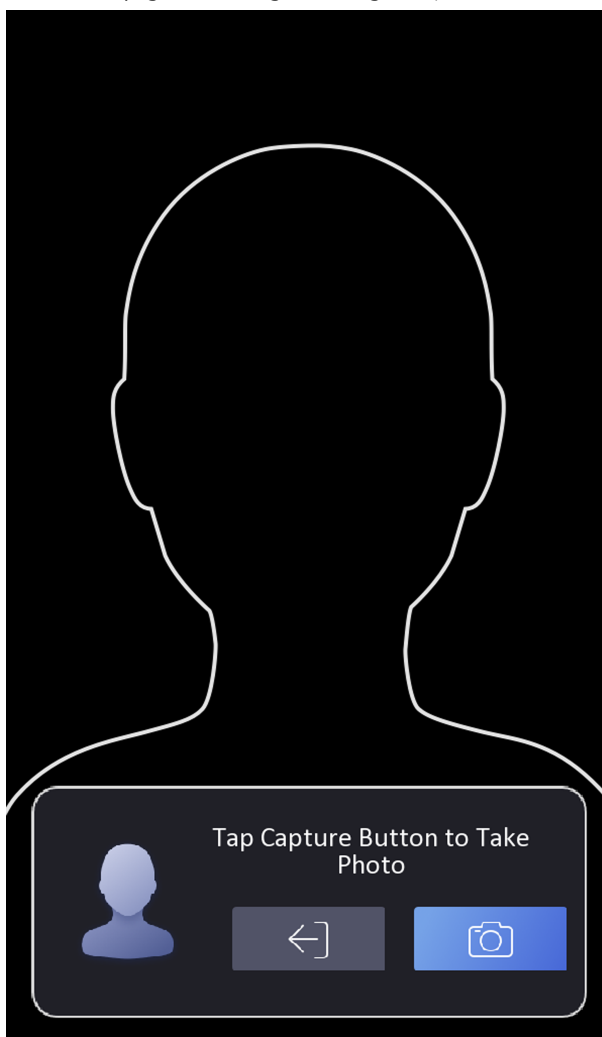


Figura 6-11 Adăugați imaginea feței

6. Uită-te la cameră.

 Nota

- Asigurați-vă că imaginea feței dvs. este în conturul imaginii feței când adăugați imaginea feței.
 - Asigurați-vă că imaginea feței capturate este de bună calitate și este exactă.
 - Pentru detalii despre instrucțiunile de adăugare a imaginilor feței, consultați ***Sfaturi atunci când colectați/comparați imaginea feței.***
-

După adăugarea completă a imaginii feței, o imagine a feței capturate va fi afișată în colțul din dreapta sus al paginii.

7. Robinet **Salva** pentru a salva imaginea feței.

8. **Opțional:** Robinet **Încearcă din nou** și ajustați poziția feței pentru a adăuga din nou imaginea feței.

9. Setări rolul utilizatorului.

Administrator

Utilizatorul este administratorul. Cu excepția funcției normale de prezență, utilizatorul poate intra și pe pagina de pornire pentru a opera după autentificarea permisiunii.

Utilizator normal

Utilizatorul este utilizatorul normal. Utilizatorul se poate autentifica sau primi doar prezența pe pagina inițială.

10. Atinge  pentru a salva setările.

6.6.2 Adăugați amprentă

Adăugați o amprentă pentru utilizator și utilizatorul se poate autentifica prin amprenta adăugată.

Pași



Nota

Funcția ar trebui să fie acceptată de dispozitiv.

1. Atingeți lung pe pagina inițială timp de 3 secunde și glisați spre stânga/dreapta urmând gestul și intrați în backend-ul dispozitivului.

2. Robinet **Utilizator** → + pentru a intra în pagina Adăugare utilizator.

3. Atingeți ID-ul angajatului. câmp și editați ID-ul angajatului.



Nota

- ID-ul angajatului trebuie să aibă mai puțin de 32 de caractere. Și poate fi o combinație de litere mici, litere mari și cifre.
- ID-ul angajatului nu trebuie să înceapă cu 0 și nu trebuie să fie duplicat.

4. Atingeți câmpul Nume și introduceți numele de utilizator pe tastatura soft.



Nota

- În numele de utilizator sunt permise numere, litere mari, litere mici și caractere speciale.
- Numele de utilizator sugerat trebuie să aibă maximum 32 de caractere.

5. Atingeți câmpul Amprentă pentru a intra în pagina Adăugați amprentă.

6. Urmăriți instrucțiunile pentru a adăuga o amprentă.

Nota

- Aceeași amprentă nu poate fi adăugată în mod repetat.
 - Pentru un utilizator pot fi adăugate până la 10 amprente.
 - De asemenea, puteți utiliza software-ul client sau înregistratorul de amprente pentru a înregistra amprente. Pentru detalii despre instrucțiunile de scanare a amprentelor, consultați **Sfaturi pentru scanarea amprentei**.
-

7. Setati rolul utilizatorului.

Administrator

Utilizatorul este administratorul. Cu excepția funcției normale de prezență, utilizatorul poate intra și pe pagina de pornire pentru a opera după autentificarea permisiunii.

Utilizator normal

Utilizatorul este utilizatorul normal. Utilizatorul se poate autentifica sau primi doar prezența pe pagina inițială.

8. Atingeți  pentru a salva setările.

6.6.3 Adăugați card

Adăugați un card pentru utilizator și utilizatorul se poate autentifica prin cardul adăugat.

Pași

1. Atingeți lung pe pagina inițială timp de 3 secunde și glisați spre stânga/dreapta urmând gestul și conectați-vă în backend.

2. Robinet **Utilizator** → + pentru a intra în pagina Adăugare utilizator.

3. Conectați un cititor de carduri extern conform schemei de cablare.

4. Atingeți ID-ul angajatului. câmp și editați ID-ul angajatului.

Nota

- ID-ul angajatului trebuie să aibă mai puțin de 32 de caractere. Și poate fi o combinație de litere mici, litere mari și cifre.
 - ID-ul angajatului nu trebuie duplicat.
-

5. Atingeți câmpul Nume și introduceți numele de utilizator pe tastatura soft.

Nota

- În numele de utilizator sunt permise numere, litere mari, litere mici și caractere speciale.
 - Numele de utilizator sugerat trebuie să aibă maximum 32 de caractere.
-

6. Atingeți câmpul Card și atingeți +.

7. Configurați cardul nr.

- Introduceți manual numărul cardului.
- Prezentați cardul peste zona de prezentare a cardului pentru a obține cardul nr.



Nota

- Numărul cardului nu poate fi gol.
- Sunt permise până la 20 de caractere în cardul nr.
- Nr. card nu poate fi duplicat.

8. Configurați tipul cardului.

9. Setați rolul utilizatorului.

Administrator

Utilizatorul este administratorul. Cu excepția funcției normale de prezență, utilizatorul poate intra și pe pagina de pornire pentru a opera după autentificarea permisiunii.

Utilizator normal

Utilizatorul este utilizatorul normal. Utilizatorul se poate autentifica sau primi doar prezența pe pagina inițială.

10. Atingeți  pentru a salva setările.

6.6.4 Adăugați parola

Adăugați o parolă pentru utilizator și utilizatorul se poate autentifica prin parolă.

Pași

1. Atingeți lung pe pagina inițială timp de 3 secunde și glisați spre stânga/dreapta urmând gestul și conectați-vă în backend.

2. Robinet **Utilizator** → + pentru a intra în pagina Adăugare utilizator.

3. Atingeți ID-ul angajatului. câmp și editați ID-ul angajatului.



Nota

- ID-ul angajatului trebuie să aibă mai puțin de 32 de caractere. Și poate fi o combinație de litere mici, litere mari și cifre.
- ID-ul angajatului nu trebuie duplicat.

4. Atingeți câmpul Nume și introduceți numele de utilizator pe tastatura soft.



Nota

- În numele de utilizator sunt permise numere, litere mari, litere mici și caractere speciale.
- Numele de utilizator sugerat trebuie să aibă maximum 32 de caractere.

5. Atingeți câmpul Parolă și creați o parolă și confirmați-o.



Nota

- Numai numerele sunt permise în parolă.
- În parolă sunt permise 4 până la 8 cifre.

6. Setăți rolul utilizatorului.

Administrator

Utilizatorul este administratorul. Cu excepția funcției normale de prezență, utilizatorul poate intra și pe pagina de pornire pentru a opera după autentificarea permisiunii.

Utilizator normal

Utilizatorul este utilizatorul normal. Utilizatorul se poate autentifica sau primi doar prezența pe pagina inițială.

7. Atingeți  pentru a salva setările.

6.6.5 Setăți modul de autentificare

După ce adăugați amprenta utilizatorului, imaginea feței, parola sau alte acreditări, ar trebui să setați modul de autentificare, iar utilizatorul își poate autentifica identitatea prin modul de autentificare configurat.

Pași

1. Atingeți lung pe pagina inițială timp de 3 secunde și glisați spre stânga/dreapta urmând gestul și conectați-vă în backend.
2. Robinet **Utilizator** → **Adăugați utilizator/Editați utilizator** → **Mod de autentificare**.
3. Selectați Dispozitiv sau Personalizat ca mod de autentificare.

Dispozitiv

Dacă doriți să selectați modul dispozitiv, ar trebui să setați mai întâi modul de autentificare a terminalului în pagina Setări control acces. Pentru detalii vezi *Setarea parametrilor de control al accesului*.

Personalizat

Puteți combina diferite moduri de autentificare împreună în funcție de nevoile dvs. reale.

4. Atingeți  pentru a salva setările.

6.6.6 Căutați și editați utilizator

După adăugarea utilizatorului, puteți căuta utilizatorul și îl puteți edita.

Căutați utilizator

Pe pagina Gestionare utilizatori, Atingeți  pentru a intra în pagina Căutare utilizator. Robinet **Card** în stânga pagina și selectați un tip de căutare din lista verticală. Introduceți ID-ul angajatului, numărul cardului sau numele de utilizator pentru căutare. Atingeți per  a căuta.

Editați utilizatorul

Pe pagina User Management, selectați un utilizator din lista de utilizatori pentru a intra în pagina Edit User. Urmăți pașii din **Managementul utilizatorilor** pentru a edita parametrii utilizatorului. Atingeți per  salva setările.

Nota

ID-ul angajatului nu poate fi editat.

6.7 Gestionarea datelor

Puteți șterge date, importa și exporta date.

6.7.1 Ștergerea datelor

Ștergeți datele utilizatorului.

Pe pagina de pornire, atingeți **Date** → **Șterge date** → **Date utilizator**. Toate datele utilizatorului adăugate în dispozitiv vor fi șterse.

6.7.2 Import date

Pași

1. Conectați o unitate flash USB la dispozitiv.
2. Pe pagina de pornire, atingeți **Date** → **Import date**.
3. Robinet **Datele utilizatorului** sau **Date faciale** iar datele selectate vor fi importate pe dispozitiv.

Nota

- Dacă doriți să transferați toate informațiile despre utilizator de pe un dispozitiv (Dispozitiv A) pe altul (Dispozitiv B), ar trebui să exportați informațiile de pe Dispozitivul A pe unitatea flash USB și apoi să importați de pe unitatea flash USB pe Dispozitivul B. În acest caz, ar trebui să importați datele utilizatorului înainte de a importa fotografia de profil.
 - Formatul de unitate flash USB acceptat este FAT32.
 - Imaginile importate ar trebui să fie salvate în directorul rădăcină (enroll_pic) și numele fișierului imagine trebuie să urmeze regula de mai jos:
Card Nr._Nume_Departament_ID de angajat_Gender.jpg
 - Dacă fișierul enroll_pic nu poate salva toate imaginile importate, puteți crea alte fișiere, denumite enroll_pic1, enroll_pic2, enroll_pic3, enroll_pic4, sub directorul rădăcină.
 - ID-ul angajatului trebuie să aibă mai puțin de 32 de caractere. Poate fi o combinație de litere mici, litere mari și cifre. Nu ar trebui să fie duplicat și nu ar trebui să înceapă cu 0.
 - Cerințele pentru imaginea feței ar trebui să respecte regulile de mai jos: Ar trebui să fie luată în vedere integrală, direct cu fața către cameră. Nu purtați pălărie sau acoperire pentru cap când faceți fotografia feței. Formatul ar trebui să fie JPEG sau JPG. Rezoluția ar trebui să fie de 640 × 480 pixeli sau mai mult decât 640 × 480 pixeli. Dimensiunea imaginii trebuie să fie între 60 KB și 200 KB.
-

6.7.3 Export de date

Pași

1. Pe pagina de pornire, atingeți **Date** → **Exportați date**.

2. Robinet **Date despre eveniment**, **Datele utilizatorului**, sau **Date faciale**

3. **Opțional:** Creați o parolă pentru export. Când ar trebui să importați acele date pe alt dispozitiv, ar trebui să introduceți parola.



Nota

- Formatul de unitate flash USB acceptat este DB.
 - Sistemul acceptă unitatea flash USB cu stocare de la 1G la 32G. Asigurați-vă că spațiul liber al unității flash USB este mai mare de 512 M.
 - Datele utilizator exportate sunt un fișier DB, care nu poate fi editat.
-

6.8 Autentificarea identității

După configurarea rețelei, configurarea parametrilor sistemului și configurarea utilizatorului, puteți reveni la pagina inițială pentru autentificarea identității. Sistemul va autentifica persoana conform modului de autentificare configurat.

Puteți autentifica identitatea prin potrivire 1:1 sau potrivire 1:N.

Potrivire 1:N

Comparați imaginea feței capturată sau imaginea cu amprenta colectată cu toate imaginile feței sau cu toate imaginile cu amprenta stocate în dispozitiv.

Potrivire 1: 1

Comparați imaginea feței capturată sau imaginea cu amprenta colectată cu toate imaginile feței sau cu toate imaginile cu amprenta stocate în dispozitiv.

6.8.1 Autentificare prin acreditare unică

Setați tipul de autentificare a utilizatorului înainte de autentificare. Pentru detalii, vezi **Setați modul de autentificare**.

Autentificați fața, amprenta digitală, cardul sau codul QR. **Față**

Faceți față înainte la cameră și începeți autentificarea prin față.

Amprenta

Plasați amprenta înregistrată pe modulul de amprentă și începeți autentificarea prin amprentă.

Card

Prezentați cardul în zona de prezentare a cardului și începeți autentificarea prin card.



Nota

Cardul poate fi card IC normal sau card criptat.

Cod QR

Puneți codul QR în fața camerei dispozitivului pentru a vă autentifica prin codul QR.



Nota

Autentificarea prin cod QR ar trebui să fie acceptată de dispozitiv.

Dacă autentificarea este finalizată, va apărea mesajul „Autentificat”.

6.8.2 Autentificare prin acreditări multiple

Înainte de a începe

Setați tipul de autentificare a utilizatorului înainte de autentificare. Pentru detalii, vezi **Setați modul de autentificare**.

Pași

1. Dacă modul de autentificare este Card și Față, Parolă și Față, Card și Parolă, Card și Față și Amprentă, autentificați orice autentificare conform instrucțiunilor de pe pagina de vizualizare live.



Nota

- Cardul poate fi card IC normal sau card criptat.
 - Dacă funcția de scanare a codurilor QR este activată, puteți pune codul QR în fața camerei dispozitivului pentru a vă autentifica prin codul QR.
-

2. După ce autentificarea anterioară este autentificată, continuați autentificarea altor acreditări.
-



Nota

- Pentru informații detaliate despre scanarea amprente, consultați *Sfaturi pentru scanarea amprente*.
 - Pentru informații detaliate despre autentificarea feței, consultați *Sfaturi atunci când colectați/comparați imaginea feței*.
-

Dacă autentificarea a reușit, va apărea mesajul „Autentificat”.

6.9 Setări de bază

Puteți seta tasta de comandă rapidă, vocea, ora, limba, luminozitatea luminii albe, numărul comunității, numărul clădirii și numărul unității.

Atingeți lung pe pagina inițială timp de 3 secunde și glisați spre stânga/dreapta urmând gestul și conectați-vă pe pagina de pornire a dispozitivului. Robinet **De bază**.

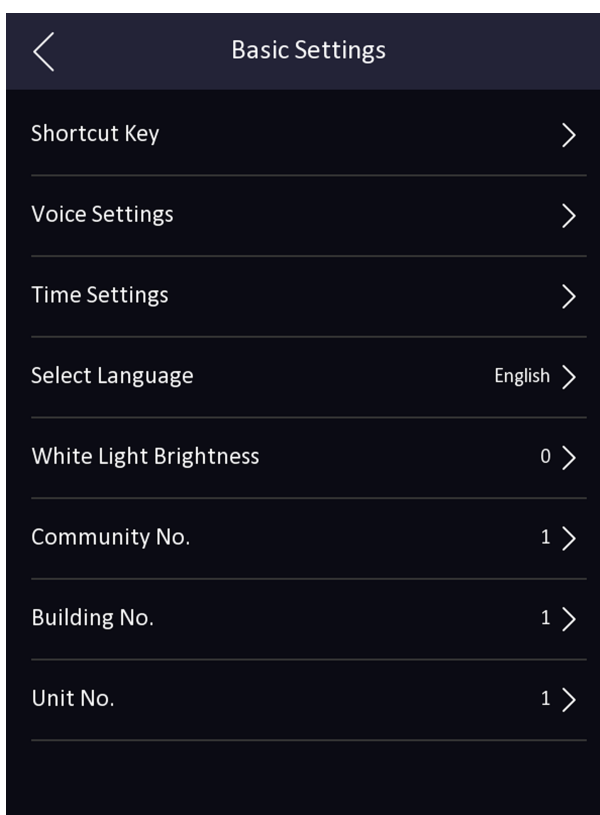


Figura 6-12 Pagina Setări de bază

tastă de comandă rapidă, voce, oră, numărul comunității, numărul clădirii și numărul unității. **Tasta de**

comandă rapidă

Alegeți tasta de comandă rapidă afișată pe pagina de autentificare, inclusiv funcția de cod QR, funcția de apel, tipul de apel și funcția de introducere a parolei.



Nota

Puteți selecta tipul de apel din **Apelați camera**, **Call Center**, și **Apelați numărul specificat de cameră**. **Apelați**

camera

Când atingeți butonul de apel de pe pagina de autentificare, ar trebui să formați un număr de cameră pentru a apela.

Call Center

Când atingeți butonul de apel de pe pagina de autentificare, puteți apela direct centrul. **Apelați camera specificată nr.**

Ar trebui să setați un număr de cameră. Când apăsați butonul de apel de pe pagina de autentificare, puteți apela direct camera configurată, fără a apela.

Setări voce

Puteți activa/dezactiva funcția de avertizare vocală și puteți regla volumul vocii.



Nota

Puteți seta volumul vocii între 0 și 10.

Setări de timp

Setați fusul orar, ora dispozitivului și ora de oră.

Selecția Limbă

Selecția limba sistemului. După ce limba este schimbată, sistemul va reporni pentru a intra în vigoare.

Luminozitatea luminii albe

Reglați luminozitatea luminii albe. 0 reprezintă dezactivarea luminii albe.

Comunitatea nr.

Setați numărul comunității instalate pe dispozitiv.

Clădirea nr.

Setați dispozitivul instalat în clădirea nr.

Unitatea nr.

Setați unitatea instalată pe dispozitiv Nr.

6.10 Setarea parametrilor biometrici

Puteți personaliza parametrii feței pentru a îmbunătăți performanța recunoașterii feței. Parametrii configurabili includ modul de aplicare, nivelul de viață al feței, distanța de recunoaștere a feței, intervalul de recunoaștere a feței, dinamica largă, nivelul de securitate 1:N, nivelul de securitate 1:1 și setările ECO.

Atingeți lung pe pagina inițială timp de 3 secunde și glisați spre stânga/dreapta urmând gestul și conectați-vă la pagina de pornire. Robinet **Biometric**.

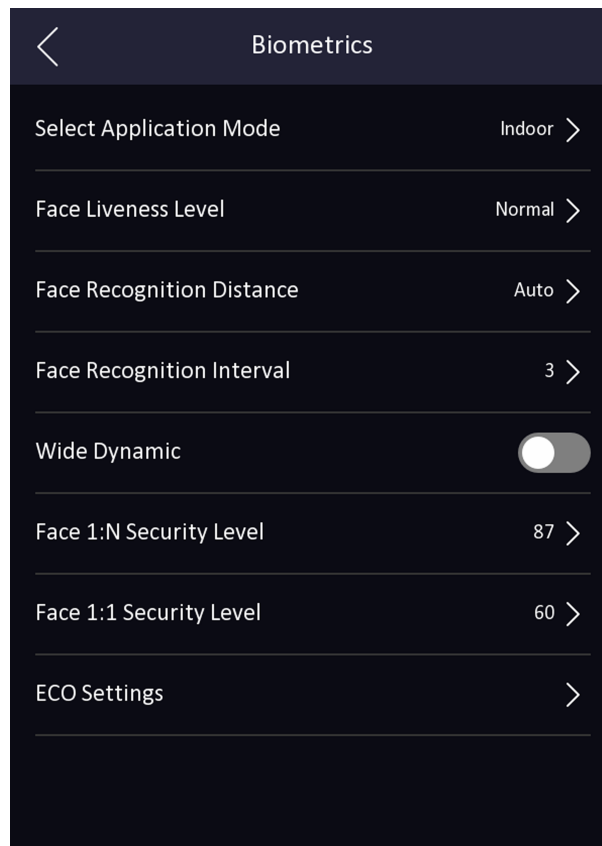


Figura 6-13 Pagina Parametrii biometrici

Tabelul 6-1 Parametrii imaginii feței

Parametru	Descriere
Selectați Aplicație Modul	Puteți selecta fie altele, fie interior în funcție de mediul real.
Nivelul de viață al feței	Puteți seta nivelul de securitate potrivit pentru anti-spoofing atunci când efectuați autentificarea live a feței.  Nota Produsele de recunoaștere biometrică nu sunt aplicabile 100% în mediile anti-spoofing. Dacă aveți nevoie de un nivel de securitate mai ridicat, utilizați mai multe moduri de autentificare.
Recunoașterea feței Distanță	Setați distanța validă dintre utilizator și cameră la autentificare.
Recunoașterea feței Interval	Intervalul de timp dintre două recunoașteri continue a feței la autentificare.

Parametru	Descriere
	 Nota Puteți introduce numărul de la 1 la 10.
Wide Dynamic	Când în vizualizare există simultan atât zone foarte luminoase, cât și foarte întunecate, puteți activa funcția dinamică largă pentru a echilibra luminozitatea întregii imagini și pentru a oferi imagini clare cu detalii.
Fața 1:N Nivel de securitate	Setați pragul de potrivire atunci când vă autentificați prin modul de potrivire 1:N. Cu cât valoarea este mai mare, cu atât rata de acceptare falsă este mai mică și rata de respingere falsă este mai mare.
Nivel de securitate 1:1	Setați pragul de potrivire atunci când vă autentificați prin modul de potrivire 1:1. Cu cât valoarea este mai mare, cu atât rata de acceptare falsă este mai mică și rata de respingere falsă este mai mare.
Modul ECO	După activarea modului ECO, dispozitivul va folosi camera IR pentru a autentifica fețele în condiții de lumină scăzută sau întuneric. Și puteți seta pragul modului ECO, modul ECO (1:N) și modul ECO (1:1).
Prag ECO	Când activați modul ECO, puteți seta pragul modului ECO. Cu cât valoarea este mai mare, cu atât dispozitivul intră mai ușor în modul ECO.
Mod ECO (1:N)	Setați pragul de potrivire atunci când vă autentificați prin modul ECO 1:N. Cu cât valoarea este mai mare, cu atât rata de acceptare falsă este mai mică și rata de respingere falsă este mai mare.
Mod ECO (1:1)	Setați pragul de potrivire atunci când vă autentificați prin modul ECO, modul de potrivire 1:1. Cu cât valoarea este mai mare, cu atât rata de acceptare falsă este mai mică și rata de respingere falsă este mai mare.

6.11 Setați parametrii de control al accesului

Puteți seta permisiunile de control al accesului, inclusiv funcțiile modului de autentificare, activarea cardului NFC, contactul ușii și timpul de deschidere a ușii.

Pe pagina de pornire, atingeți **ACS** (Setări control acces) pentru a accesa pagina Setări control acces. Editați parametrii de control acces pe această pagină.

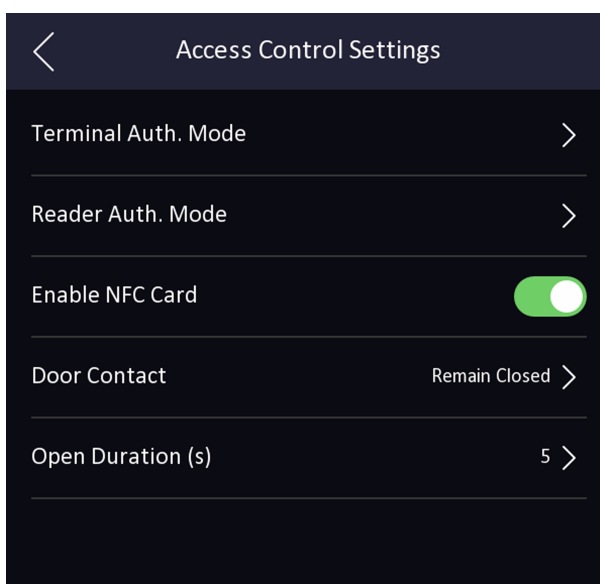


Figura 6-14 Parametrii de control al accesului

Descrierile parametrilor disponibili sunt după cum urmează:

Tabelul 6-2 Descrierile parametrilor de control al accesului

Parametru	Descriere
Terminal Auth. Mod (Modul de autentificare a terminalului)	Selectați modul de autentificare al terminalului de recunoaștere a feței. De asemenea, puteți personaliza modul de autentificare.  Nota • Numai dispozitivul cu modul de amprentă acceptă funcția legată de amprentă. • Produsele de recunoaștere biometrică nu sunt 100% aplicabile în mediile anti-spoofing. Dacă aveți nevoie de un nivel de securitate mai ridicat, utilizați mai multe moduri de autentificare. • Dacă adoptați mai multe moduri de autentificare, ar trebui să autentificați alte metode înainte de autentificarea feței.
Reader Auth. Modul (Modul de autentificare a cititorului de carduri)	Selectați modul de autentificare al cititorului de carduri.
Activați cardul NFC	Activați funcția și puteți prezenta cardul NFC pentru autentificare.

Parametru	Descriere
Contact la ușă	Puteți selecta „Open (Remain Open)” sau „Close (Remian Closed)” în funcție de nevoile dumneavoastră reale. În mod implicit, este Închidere (Remian închis).
Durata de deschidere	Setați durata de deblocare a ușii. Dacă ușa nu este deschisă în timpul stabilit, ușa va fi încuiată. Interval de timp disponibil pentru blocarea ușii: 1 până la 255 s.

6.12 Setări de oră și stare de prezență

Setați ora și starea de prezență. Puteți seta modul de prezență ca check-in, check out, breakout, break in, overtime in și overtime out, în funcție de situația dvs. reală.



Nota

Funcția ar trebui să fie utilizată în cooperare cu funcția de timp și prezență pe software-ul client.

6.12.1 Dezactivați modul de participare prin dispozitiv

Dezactivați modul de participare și sistemul nu va afișa starea de participare pe pagina inițială.

Robinet **Starea T&A** pentru a intra pe pagina de stare T&A.

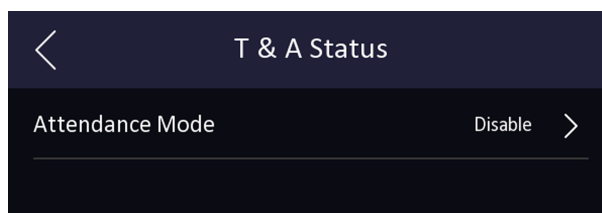


Figura 6-15 Dezactivarea modului de participare

Setați **Modul de prezență** ca **Dezactivați**.

Nu veți vedea sau configura starea de prezență pe pagina inițială. Și sistemul va respecta regula de prezență configurată pe platformă.

6.12.2 Setări prezența manuală prin dispozitiv

Setați modul de prezență ca manual și puteți selecta o stare manual când luați prezență.

Înainte de a începe

Adăugați cel puțin un utilizator și setați modul de autentificare al utilizatorului. Pentru detalii, vezi *Managementul utilizatorilor*.

Pași

1. Robinet **Starea T&A** pentru a intra pe pagina de stare T&A.

2. Setați **Modul de prezență** ca **Manual**.

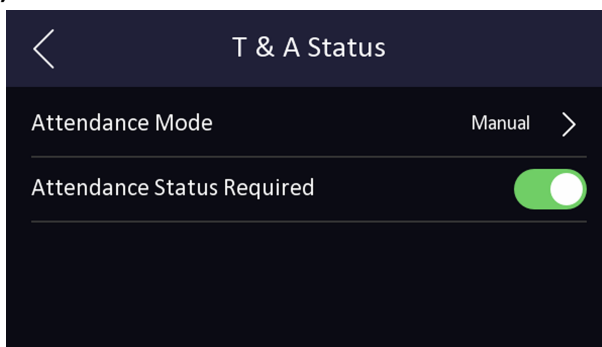


Figura 6-16 Modul de prezență manuală

3. Activați **Starea de prezență** funcție.

Rezultat

Ar trebui să selectați manual starea de prezență după autentificare.

Nota

Dacă nu selectați o stare, autentificarea va fi eșuată și nu va fi marcată ca participare validă.

6.12.3 Setați prezența automată prin dispozitiv

Setați modul de prezență ca automat și puteți seta starea de prezență și programul său disponibil. Sistemul va schimba automat starea de prezență în funcție de parametrii configurați.

Înainte de a începe

Adăugați cel puțin un utilizator și setați modul de autentificare al utilizatorului. Pentru detalii, vezi *Managementul utilizatorilor*.

Pași

1. Robinet **Starea T&A** pentru a intra pe pagina de stare T&A.

2. Setați **Modul de prezență** ca **Auto**.

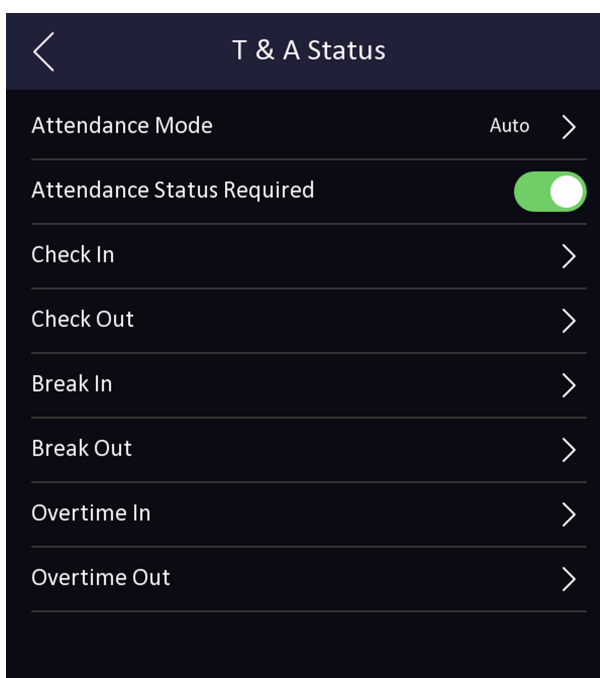


Figura 6-17 Modul de participare automată

3. Selectați o stare de prezență și setați-i programul.

- 1) Selectați **Check-in, Verifică, Izbucni, Spargere, Prelungiri In**, sau **Prelungiri Out** ca statutul de prezență.
- 2) Atingeți **Programa**.
- 3) Selectați **luni, marți, miercuri, joi, vineri, sâmbătă**, sau **duminică**.
- 4) Atingeți data selectată și setați ora de începere a stării de prezență selectate.
- 5) Atingeți **Confirma**.
- 6) Repetați pașii de la 1 la 5 în funcție de nevoile dvs. reale.



Nota

Starea de prezență va fi valabilă în cadrul programului configurat.

Rezultat

Când vă autentificați pe pagina inițială, autentificarea va fi marcată ca stare de prezență configurată conform programului configurat.

Exemplu

Dacă setați **Program de erupție** ca luni 11:00 și **Program de pauză** ca luni 12:00, autentificarea validă a utilizatorului de luni 11:00 până la 12:00 va fi marcată ca pauză.

6.12.4 Setări prezență manuală și automată prin dispozitiv

Setați modul de prezență ca **Manual și Auto**, iar sistemul va schimba automat starea de prezență în funcție de parametrii configurați. În același timp, puteți modifica manual starea de prezență după autentificare.

Înainte de a începe

Adăugați cel puțin un utilizator și setați modul de autentificare al utilizatorului. Pentru detalii, vezi *Managementul utilizatorilor*.

Pași

1. Robinet **Starea T&A** pentru a intra pe pagina de stare T&A.

2. Setați **Modul de prezență** ca **Manual și Auto**.

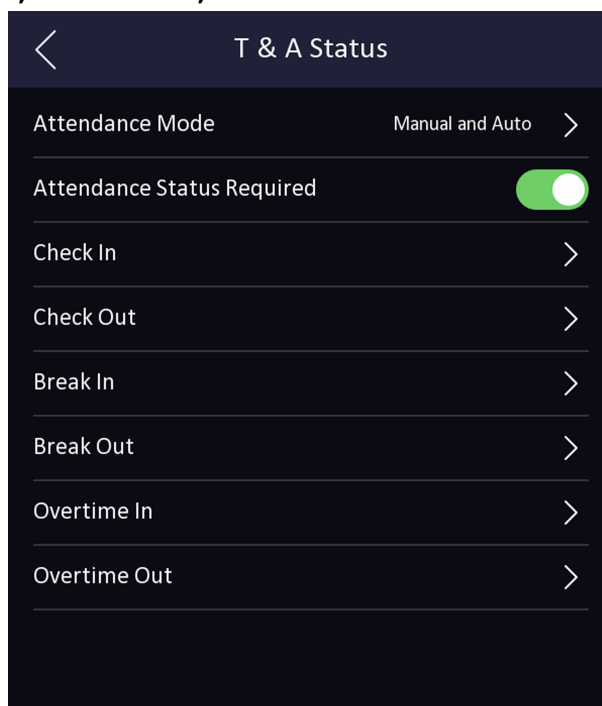


Figura 6-18 Modul manual și automat

3. Selectați o stare de prezență și setați-i programul.

- 1) Selectați **Check-in, Verifică, Izbucni, Spargere, Prelungiri In**, sau **Prelungiri Out** ca statutul de prezență.
- 2) Atingeți **Programa**.
- 3) Selectați **luni, marți, miercuri, joi, vineri, sâmbătă**, sau **duminică**.
- 4) Atingeți data selectată și setați ora de începere a stării de prezență selectate.
- 5) Atingeți **Confirma**.
- 6) Repetați pașii de la 1 la 5 în funcție de nevoile dvs. reale.



Nota

Starea de prezență va fi valabilă în cadrul programului configurat.

Rezultat

Pe pagina inițială și autentificați-vă. Dacă nu selectați o stare, autentificarea va fi marcată ca stare de prezență configurată conform programului. Dacă atingeți **Selectați Stare** și selectați un statut pentru a primi prezență, autentificarea va fi marcată ca starea de prezență selectată.

Exemplu

Dacă setați **Program de erupție** ca luni 11:00 și **Program de pauză** ca luni 12:00, autentificarea validă a utilizatorului de luni 11:00 până la 12:00 va fi marcată ca pauză.

6.13 Întreținerea sistemului

Puteți vizualiza informațiile despre sistem și capacitatea. De asemenea, puteți să faceți upgrade dispozitivul, să reveniți la setările din fabrică și să reveniți la setările implicite.

Atingeți lung pe pagina inițială timp de 3 secunde și glisați spre stânga/dreapta urmând gestul și conectați-vă la pagina de pornire. Robinet **Întreținere..**

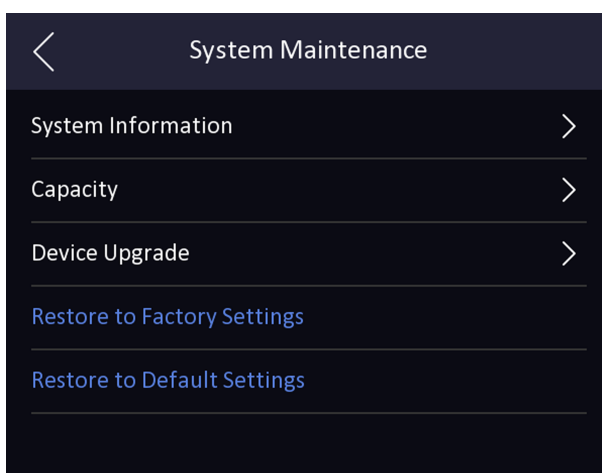


Figura 6-19 Pagina de întreținere

Informații de sistem

Puteți vizualiza modelul dispozitivului, numărul de serie, versiunile, adresa, datele de producție, codul QR și licența de cod sursă deschisă.



Nota

Pagina poate varia în funcție de diferitele modele de dispozitiv. Consultați pagina actuală pentru detalii.

Capacitate

Puteți vizualiza numărul, utilizatorul, imaginea feței, cardul, evenimentul și amprenta.

Nota

Unele părți ale modelelor de dispozitiv acceptă afișarea numărului de amprentă. Consultați pagina actuală pentru detalii.

Upgrade dispozitiv

Conectați unitatea flash USB la interfața USB a dispozitivului. Robinet **Upgrade**, iar dispozitivul va citi *digicap.dav* fișier în unitatea flash USB pentru a începe actualizarea.

Reveniți la setările implicite

Toți parametrii, cu excepția setărilor de comunicare, a informațiilor despre utilizator importate de la distanță, vor fi restabiliți la setările implicite. Sistemul se va reporni pentru a intra în vigoare.

Reveniți la setările din fabrică

Toți parametrii vor fi restabiliți la setările din fabrică. Sistemul se va reporni pentru a intra în vigoare.

6.14 Video Interfon

După adăugarea dispozitivului la software-ul client, puteți apela dispozitivul din software-ul client, puteți apela stația principală de pe dispozitiv, puteți apela software-ul client de pe dispozitiv sau puteți apela stația interioară de pe dispozitiv.

6.14.1 Apelați software-ul client de pe dispozitiv

Pași

1. Obțineți software-ul client de pe discul furnizat sau de pe site-ul web oficial și instalați software-ul conform instrucțiunilor.
2. Rulați software-ul client și va apărea panoul de control al software-ului.
3. Clic **Managementul dispozitivelor** pentru a intra în interfața Device Management.
4. Adăugați dispozitivul la software-ul client.

Nota

Pentru detalii despre adăugarea dispozitivului, consultați *Adăugați dispozitiv*.

5. Apelați software-ul client.

- 1) Atingeți **Apel** pe pagina inițială a dispozitivului.
- 2) Intrare **În** fereastra pop-up.
- 3) Atingeți **Apel** pentru a apela software-ul client.

6. Robinet **Răspuns** pe pagina pop-up a software-ului client și puteți porni audio bidirecțional între dispozitiv și software-ul client.

Nota

Dacă dispozitivul este adăugat la mai multe software-uri client și când dispozitivul apelează software-ul client, numai primul software client adăugat, dispozitivul va apărea fereastra de primire a apelurilor.

6.14.2 Call Center de la Dispozitiv

Pași

1. Obțineți software-ul client de pe discul furnizat sau de pe site-ul web oficial și instalați software-ul conform instrucțiunilor.
2. Rulați software-ul client și va apărea panoul de control al software-ului.
3. Clic **Managementul dispozitivelor** pentru a intra în interfața Device Management.
4. Adăugați stația principală și dispozitivul la software-ul client.

Nota

Pentru detalii despre adăugarea dispozitivului, consultați *Adăugați dispozitiv*.

5. Setează adresa IP și adresa SIP a stației master în pagina de configurare la distanță.

Nota

Pentru detalii despre funcționare, consultați manualul de utilizare al stației master.

6. Sună la centru.

- Dacă ați configurat pentru call center în **Setări de bază**, puteți atinge  pentru a suna centrul.
- Dacă nu ați configurat pentru call center în **Setări de bază**, ar trebui să atingeți  →  a suna centrul

7. Răspunde la apel prin stația principală și pornește sunetul bidirecțional.

Nota

Dispozitivul va apela cu prioritate stația principală.

6.14.3 Apelați dispozitivul din software-ul client

Pași

1. Obțineți software-ul client de pe discul furnizat sau de pe site-ul web oficial și instalați software-ul conform instrucțiunilor.
2. Rulați software-ul client și va apărea panoul de control al software-ului.
3. Clic **Managementul dispozitivelor** pentru a intra în pagina Device Management.
4. Adăugați dispozitivul la software-ul client.

Nota

Pentru detalii despre adăugarea dispozitivului, consultați *Adăugați dispozitiv*.

5. Introduceți **Vizualizare live** și faceți dublu clic pe dispozitivul adăugat pentru a începe vizualizarea live.



Nota

Pentru detalii despre operațiunile din **Vizualizare live** pagina, vezi *Vizualizare live* în manualul de utilizare al software-ului client.

6. Faceți clic dreapta pe imaginea de vizualizare live pentru a deschide meniul de clic dreapta.

7. Clic **Porniți audio bidirecțional** pentru a porni sunetul bidirecțional între dispozitiv și software-ul client.

6.14.4 Apelați camera de pe dispozitiv

Pași

1. Obțineți software-ul client de pe discul furnizat sau de pe site-ul web oficial și instalați software-ul conform instrucțiunilor.
 2. Rulați software-ul client și va apărea panoul de control al software-ului.
 3. Clic **Managementul dispozitivelor** pentru a intra în interfața Device Management.
 4. Adăugați stația interioară și dispozitivul la software-ul client.
-



Nota

Pentru detalii despre adăugarea dispozitivului, consultați *Adăugați dispozitiv*.

5. Conectați un utilizator la o stație interioară și setați un număr de cameră pentru stația interioară.

6. Sună la cameră.

- Dacă ați configurat un Nr. cameră specificat în **Setări de bază**, puteți atinge  a apela la camera.
- Dacă nu ați configurat un număr specificat de cameră în **Setări de bază**, ar trebui să atingeți pagina de  pe autentificare a dispozitivului. Introduceți numărul camerei de pe pagina de apelare și atingeți camera.  a suna

7. După ce stația de interior răspunde la apel, puteți porni sunetul bidirecțional cu stația de interior.

Capitolul 7 Operarea prin browser web

7.1 Autentificare

Vă puteți autentifica prin intermediul browserului web sau prin configurarea de la distanță a software-ului client.



Nota

Asigurați-vă că dispozitivul este activat. Pentru informații detaliate despre activare, consultați **Activare**.

Conectați-vă prin browser web

Introduceți adresa IP a dispozitivului în bara de adrese a browserului web și apăsați **Intră** pentru a intra în pagina de conectare.

Introduceți numele de utilizator al dispozitivului și parola. Clic **Log in**.

Conectați-vă prin configurarea de la distanță a software-ului client

Descărcați și deschideți software-ul client. După ce adăugați dispozitivul, faceți clic pe



pentru a intra în vizualizarea live

pagină.

7.2 Vizualizare live

Puteți vizualiza videoclipul în direct al dispozitivului.

După autentificare, veți intra în pagina de vizualizare live. Puteți efectua vizualizarea în direct, capturarea, înregistrarea video și alte operațiuni.

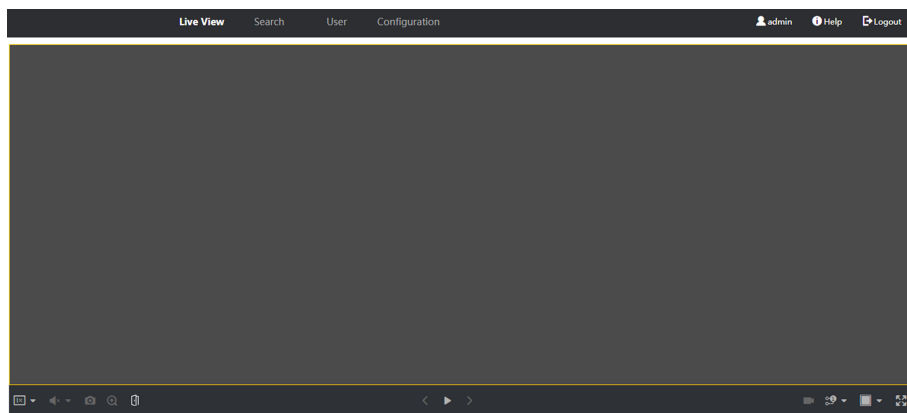


Figura 7-1 Pagina Live View

Descrieri de funcții:



Selecționați dimensiunea imaginii când porniți vizualizarea live.



Setați volumul când începeți vizualizarea live.



Nota

Dacă reglați volumul la pornirea sunetului bidirecțional, este posibil să auziți sunete repetate.



Puteți captura o imagine când începeți vizualizarea live.



Funcție rezervată. Puteți mări imaginea live view.



Deblocați ușa conectată.



Porniți sau opriți vizualizarea live.



Porniți sau opriți înregistrarea video.



Selectați tipul de streaming când începeți vizualizarea live. Puteți selecta dintre fluxul principal și fluxul secundar.



Selectați tipul de diviziune a ferestrei când începeți vizualizarea live.



Vizualizare pe tot ecranul.

7.3 Managementul persoanelor

Faceți clic și adăugați informațiile persoanei, inclusiv informațiile de bază, cardul, modul de autentificare și

Clic **Bine** pentru a salva persoana.

Adăugați informații de bază

Clic **Utilizator** → **Adăugați** pentru a intra în pagina Adăugare persoană.

Adăugați informațiile de bază ale persoanei, inclusiv ID-ul angajatului, numele persoanei, sexul și rolul de utilizator.

Clic **Salva** pentru a salva setările.

Adăugați card

Clic **Utilizator** → **Adăugați** pentru a intra în pagina Adăugare persoană.

Clic **Adăugați card** și introduceți un număr de card.

Clic **Salva** pentru a salva setările.

Adăugați imaginea feței

Clic **Utilizator** → **Adăugați** pentru a intra în pagina Adăugare persoană.

Clic **+din dreapta** pentru a încărca o imagine a feței de pe computerul local.



Nota

Formatul imaginii trebuie să fie JPEG, iar dimensiunea trebuie să fie mai mică de 200K.

Clic **Salva** pentru a salva setările.

Adăugați modul de autentificare

Clic **Utilizator** → **Adăugați** pentru a intra pe pagina Adăugare persoană. Setati modul de autentificare.

Clic **Salva** pentru a salva setările.

7.4 Căutare eveniment

Clic **Căutare** pentru a intra pe pagina de căutare.

Employee ID

Name

Card No.

Start Time

End Time

Search

Figura 7-2 Pagina de căutare

Introduceți condițiile de căutare, inclusiv ID-ul angajatului, numele, numărul cardului, ora de începere și ora de încheiere și faceți clic **Căutare**.

Rezultatele vor fi afișate în panoul din dreapta.

7.5 Configurare

7.5.1 Setarea parametrilor locali

Setați parametrii de vizualizare live, calea de salvare a fișierului de înregistrare și calea de salvare a imaginilor capturate.

Setați parametrii Live View

Clic **Configurare** → **Local** pentru a intra pe pagina locală. Configurați tipul fluxului și formatul imaginii și faceți clic **Salva**.

Setați calea de salvare a fișierului de înregistrare

Clic **Configurare** → **Local** pentru a intra pe pagina locală. Selectați o cale de salvare de pe computerul local și faceți clic **Salva**.

De asemenea, puteți face clic **Deschide** pentru a deschide folderul de fișiere pentru a vedea detaliile.

Setați calea de salvare a imaginilor capturate

Clic **Configurare** → **Local** pentru a intra pe pagina locală. Selectați o cale de salvare de pe computerul local și faceți clic **Salva**.

De asemenea, puteți face clic **Deschide** pentru a deschide folderul de fișiere pentru a vedea detaliile.

7.5.2 Vizualizați informații despre dispozitiv

Vizualizați numărul dispozitivului, modelul, numărul de serie, versiunea, capacitatea dispozitivului etc.

Clic **Configurare** → **Sistem** → **Setări sistem** → **Informații de bază** pentru a intra în pagina de configurare.

Puteți vizualiza numărul dispozitivului, modelul, numărul de serie, versiunea, capacitatea dispozitivului etc.

7.5.3 Setare Ora

Setați fusul orar al dispozitivului, modul de sincronizare și ora dispozitivului. Clic **Configurare** → **Sistem** → **Setări sistem** → **Setări oră**.

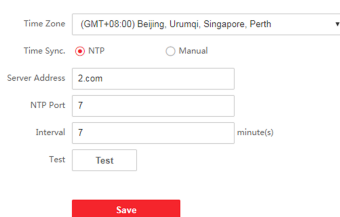


Figura 7-3 Setări de timp

Clic **Salva** pentru a salva setările după configurare.

Fus orar

Selectați fusul orar al dispozitivului din lista verticală.

Sincronizare oră.

NTP

Ar trebui să setați adresa IP, numărul portului și intervalul serverului NTP.

Manual

În mod implicit, ora dispozitivului ar trebui să fie sincronizată manual. Puteți seta manual ora dispozitivului sau puteți verifica **Sincronizare. cu Computer Time** pentru a sincroniza ora dispozitivului cu cea a computerului.

7.5.4 Setări ora de oră

Pași

1. Clic **Configurare** → **Sistem** → **Setări sistem** → **DST**.

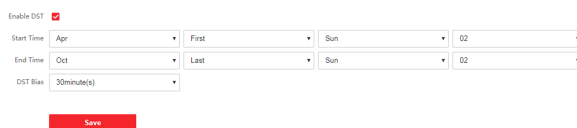


Figura 7-4 Pagina DST

2. Verificați **Activați ora de oră**.

3. Setări ora de începere a DST, ora de încheiere și ora de polarizare.

4. Clic **Salva** pentru a salva setările.

7.5.5 Actualizare și întreținere

Reporniți dispozitivul, restaurați parametrii dispozitivului și actualizați versiunea dispozitivului.

Reporniți dispozitivul

Clic **Configurare** → **Sistem** → **Întreținere** → **Upgrade și întreținere**.



Reboot

Reboot the device.

Restore Parameters

Restore all parameters t...

Restore all parameters, ...

Export

Import

Upgrade

Note: The upgrading process will last 1 to 10 min. Do not power the device off during the upgrading. The device will reboot automatically after the upgrading.

Figura 7-5 Pagina de actualizare și întreținere

Clic **Reporniți** pentru a începe repornirea dispozitivului.

Restaurarea parametrilor

Clic **Configurare → Sistem → Întreținere → Upgrade și întreținere**.

Fabrică

Toți parametrii vor fi restabiliți la setările din fabrică. Ar trebui să activați dispozitivul înainte de utilizare.

Implicit

Dispozitivul va reveni la setările implicite, cu excepția adresei IP a dispozitivului și a informațiilor despre utilizator.

Parametri de import și export

Clic **Configurare → Sistem → Întreținere → Upgrade și întreținere**.

Export

Clic **Export** pentru a exporta jurnalele sau parametrii dispozitivului.



Nota

Puteți importa parametrii dispozitivului exportați pe alt dispozitiv.

Import

Clic  și selectați fișierul de importat. Clic **Import** pentru a începe importul fișierului de configurare.

Upgrade

Clic **Configurare → Sistem → Întreținere → Upgrade și întreținere**.

Selectați un tip de upgrade din lista verticală. Faceți clic și selectați  fișierul de actualizare de pe computerul local. Clic **Upgrade** pentru a începe actualizarea.

Nota

Nu opriți în timpul actualizării.

7.5.6 Schimbarea parolei administratorului

Pași

1.Clic**Configurare** → **Gestionare utilizatori**.

2.Faceți clic  **pe** .

3.Introduceți vechea parolă și creați o nouă parolă.

4.Confirmați noua parolă.

5.Clic **Bine**.



Atenție

Puterea parolei dispozitivului poate fi verificată automat. Vă recomandăm cu căldură să schimbați parola pe care o alegeți (folosind minim 8 caractere, incluzând cel puțin trei tipuri de următoarele categorii: litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dumneavoastră. Și vă recomandăm să vă schimbați parola în mod regulat, mai ales în sistemul de înaltă securitate, schimbarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

Configurarea corectă a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau utilizatorului final.

7.5.7 Setări de rețea

Setați parametrii TCP/IP, portul și Wi-Fi.

Nota

Unele modele de dispozitive nu acceptă setări Wi-Fi. Consultați produsele reale atunci când configurați.

Setați parametrii de bază de rețea

Setați parametrii TCP/IP

Clic**Configurare** → **Rețea** → **Setări de bază** → **TCP/IP**.

☐ DHCP

IPv4 Address

IPv4 Subnet Mask ✓

IPv4 Default Gateway ✓

Mac Address

MTU ✓

DNS Server

Preferred DNS Server ✓

Alternate DNS Server ✓

Save

Figura 7-6 Pagina Setări TCP/IP

Clic **Salva** pentru a salva setările.

Tip NIC

Selectați un tip de NIC din lista verticală. În mod implicit, este **Auto**.

DHCP

Dacă debifați funcția, ar trebui să setați adresa IPv4, masca de subrețea IPv4, gateway-ul implicit IPv4, MTU și portul dispozitivului.

Dacă verificați funcția, sistemul va alocă automat adresa IPv4, masca de subrețea IPv4 și gateway-ul implicit IPv4.

Server DNS

Setați serverul DNS preferat și serverul DNS alternativ în funcție de nevoia dvs. reală.

Setați parametrii EHome

Setați parametrii EHome pentru accesarea dispozitivului prin protocolul EHome.

Pași



Nota

Funcția ar trebui să fie acceptată de dispozitiv.

1. Clic **Configurare** → **Rețea** → **Setări avansate** → **Platformă**.

2. Selectați **EHome** din lista derulantă a modului de acces la platformă.

3. Verificați **Permite**.

4. Setați versiunea EHome, adresa serverului, ID-ul dispozitivului și starea EHome.



Nota

Dacă selectați 4.0 ca versiune, ar trebui să setați și tasta EHome.

5. Clic **Salva**.

Setați parametrii Wi-Fi

Setați parametrii Wi-Fi pentru conexiunea wireless a dispozitivului.

Pași



Nota

Funcția ar trebui să fie acceptată de dispozitiv.

1. Clic **Configurare** → **Rețea** → **Setări de bază** → **Wi-Fi**.



Figura 7-7 Pagina Setări Wi-Fi

2. Verificați **Wifi**.

3. Selectați un Wi-Fi

- Faceți clic pe un Wi-Fi din listă și introduceți parola Wi-Fi.
- Clic **Adăuga** și introduceți numele unui Wi-Fi, parola și tipul de criptare. Clic **Conectați-vă**. Când Wi-Fi este conectat, faceți clic **Bine**.

4. Opțional: Setați parametrii WLAN.

- 1) Faceți clic **Setări TCP/IP**.
- 2) Setați adresa IP, masca de subrețea și gateway-ul implicit. Sau verificați **Activați DHCP** iar sistemul va alocă automat adresa IP, masca de subrețea și gateway-ul implicit.

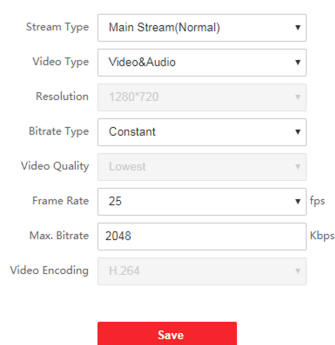
5. Clic **Salva**.

7.5.8 Setați parametrii video și audio

Setați calitatea imaginii, rezoluția și volumul dispozitivului.

Setați parametrii video

Clic **Configurare** → **Video/Audio** → **Video**.



Stream Type	Main Stream(Normal)	▼
Video Type	Video&Audio	▼
Resolution	1280*720	▼
Bitrate Type	Constant	▼
Video Quality	Lowest	▼
Frame Rate	25	▼ fps
Max. Bitrate	2048	Kbps
Video Encoding	H.264	▼

Save

Figura 7-8 Pagina Setări video

Setați tipul fluxului, tipul video, tipul bitrate, frame rate și Max. rata de biți. Clic **Salva** pentru a salva setările după configurare.

Setați parametrii audio

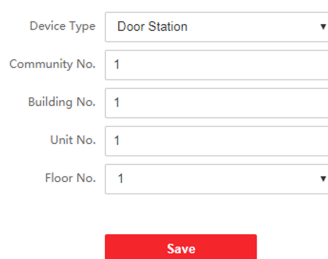
Clic **Configurare** → **Video/Audio** → **Audio**. Trageți blocul pentru a regla volumul de ieșire al dispozitivului. Clic **Salva** pentru a salva setările după configurare.

7.5.9 Setați parametrii interfonului video

Dispozitivul poate fi folosit ca stație de ușă sau stație de ușă exterioară. Trebuie să setați numărul dispozitivului înainte de utilizare.

Setați numărul dispozitivului.

Clic **Configurare** → **Interfon video** → **Nr..**



Device Type	Door Station	▼
Community No.	1	
Building No.	1	
Unit No.	1	
Floor No.	1	▼

Save

Figura 7-9 Setări Nr. dispozitiv

Clic **Salva** pentru a salva setările după configurare. **Tip de dispozitiv**

Dispozitivul poate fi folosit ca stație de usa sau stație de usa exterioara. Selectați un tip de dispozitiv din lista verticală.

Comunitatea nr.

Setați numărul comunității instalate pe dispozitiv.

Clădirea nr.

Setați dispozitivul instalat în clădirea nr.

Unitatea nr.

Setați unitatea instalată pe dispozitiv Nr.

Etajul nr.

Setați podeaua instalată a dispozitivului Nr.

Nu.

Dacă selectați stația exterioară ca tip de dispozitiv, ar trebui să introduceți un număr între **1** și **99**.



Nota

Dacă schimbați numărul, ar trebui să reporniți dispozitivul.

Setați setările rețelei conectate

Clic **Configurare** → **Interfon video** → **Setări rețea conectată**.

Puteți seta tipul de dispozitiv, adresa IP a serverului SIP și adresa IP a stației master. După setarea parametrilor, puteți comunica între dispozitivul de control acces, stația de ușă, stația interioară, stația principală și platforma.

Clic **Salva** pentru a salva setările după configurare.

7.5.10 Setări controlul accesului și parametrii de autentificare

Setați parametrii de control acces și parametrii de autentificare.

Setări parametrii uși

Clic **Configurare** → **Control acces** → **Parametri uși**.

Door Contact ☒ Remain Closed ☐ Remain Open

Open Duration S

Open Timeout Alarm S

Save

Figura 7-10 Pagina Setări parametri uși

Clic **Salva** pentru a salva setările după configurare.

Contact la ușă

Puteți selecta **Rămâi deschis** sau **Rămâi închis** conform nevoilor tale reale. În mod implicit, este **Rămâi închis**.

Durata de deschidere

Setați durata de deblocare a ușii. Dacă ușa nu este deschisă în timpul stabilit, ușa va fi încuiată.

Deschidere Timeout Alarm (Alarmă Door Open Timeout)

O alarmă va fi declanșată dacă ușa nu a fost închisă în timpul configurat.

Setați parametrii de autentificare

Clic**Configurare** → **Control acces** → **Setări de autentificare**.

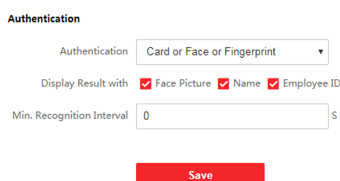


Figura 7-11 Setări parametrii de autentificare

Clic**Salva** pentru a salva setările după configurare.

Autentificare

Selectați un mod de autentificare în funcție de nevoile dvs. reale din lista derulantă.

Afișează rezultatul cu

Verifica **Poza feței**, **Nume**, sau **ID de angajat**. Când autentificarea este finalizată, sistemul va afișa conținutul selectat în rezultat.

Min. Interval de recunoaștere

Dacă intervalul dintre prezentarea cardului aceluiași card este mai mic decât valoarea configurată, prezentarea cardului este invalidă.

7.5.11 Setați parametrii RS-485

Puteți seta parametrii RS-485, inclusiv perifericul, adresa, rata de transmisie și tipul de ieșire.

Clic**Configurare** → **Sistem** → **Setări sistem** → **Setări RS-485**.

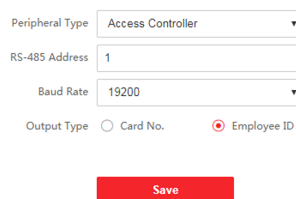


Figura 7-12 Pagina RS-485

Clic**Salva** pentru a salva setările după configurare.

Tipul periferic

Selecțai un periferic din lista derulantă în funcție de situația actuală. Puteți alege din **Cititor de carduri**, **Modul de extensie**, **Controler de acces**, sau **Dezactivați**.



Nota

După ce perifericul este schimbat și salvat, dispozitivul se va reporni automat.

Adresa RS-485

Setați adresa RS-485 în funcție de nevoile dvs. reale.



Nota

Dacă selecțai **Controler de acces**: Dacă conectați dispozitivul la un terminal prin interfața RS-485, setați adresa RS-485 la 2. Dacă conectați dispozitivul la un controler, setați adresa RS-485 conform ușii nr.

Baud Rate

Rata baud atunci când dispozitivele comunică prin protocolul RS-485.

Tip ieșire

Dacă selecțai **Controler de acces** ca tip de periferic, ar trebui să setați parametrul. Dispozitivul va scoate numărul cardului sau ID-ul angajatului către controlerul de acces.

7.5.12 Setări parametrul Wiegand

Puteți seta direcția de transmisie Wiegand.

Pași



Nota

Unele modele de dispozitive nu acceptă această funcție. Consultați produsele reale atunci când configurați.

1. Clic **Configurare** → **Sistem** → **Setări sistem** → **Setări Wiegand**.

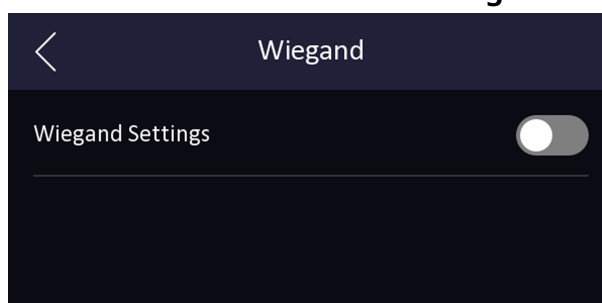


Figura 7-13 Pagina Wiegand

2. Verificați **Wiegand** pentru a activa funcția Wiegand.

3. Setați o direcție de transmisie.

Intrare

Dispozitivul poate conecta un cititor de carduri Wiegand.

Ieșire

Se poate conecta un controler de acces extern. Și cele două dispozitive vor transmite cardul nr. prin Wiegand 26 sau 34.

4. Clic **Salva** pentru a salva setările.



Nota

Dacă schimbați perifericul și după ce salvați parametrii dispozitivului, dispozitivul se va reporni automat.

7.5.13 Setări parametrilor imaginii

Setați standardul video, WDR, luminozitatea, contrastul, saturația și claritatea.

Pași

1. Clic **Configurare** → **Imagine**.

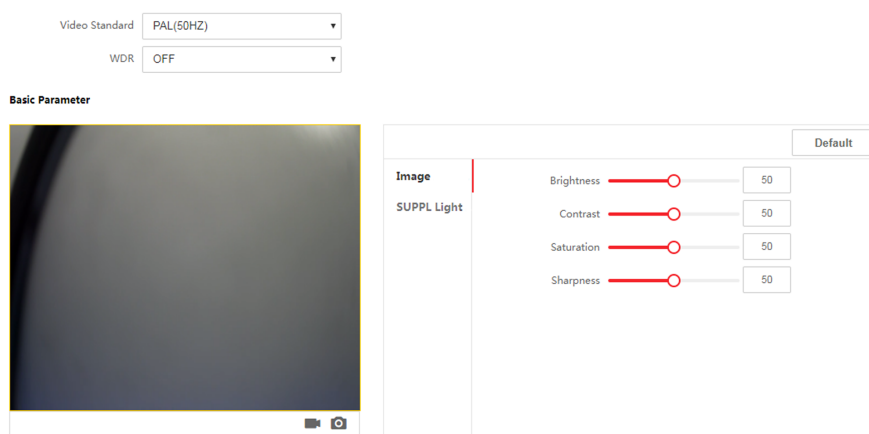


Figura 7-14 Pagina Setări imagine

2. Configurați parametrii pentru a regla imaginea.

Standard video

Setați rata de cadre video atunci când efectuați vizualizarea live de la distanță. După modificarea standardului, ar trebui să reporniți dispozitivul pentru a intra în vigoare.

PAL

25 de cadre pe secundă. Potrivit pentru China continentală, Hong Kong (China), țările din Orientul Mijlociu, țările din Europa etc.

NTSC

30 de cadre pe secundă. Potrivit pentru SUA, Canada, Japonia, Taiwan (China), Coreea, Filipine etc.

WDR

Activați sau dezactivați funcția WDR.

Atunci când în vizualizare există atât zone foarte luminoase, cât și foarte întunecate simultan, WDR echilibrează nivelul de luminozitate al întregii imagini și oferă imagini clare cu detalii.

Luminozitate/Contrast/Saturație/Sharpness

Trageți blocul sau introduceți valoarea pentru a regla luminozitatea, contrastul, saturația și claritatea videoclipului în direct.



Începe/termină înregistrarea video.



Capturați imaginea.

7.5.14 Setări luminozitatea luminii suplimentare

Setați luminozitatea luminii suplimentare a dispozitivului.

Pași

1. Clic **Configurare** → **Imagine**.

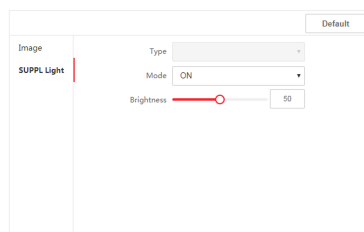


Figura 7-15 Pagina Setări lumini suplimentare

2. Clic **SUPPL Lumină** (Supliment Light) în panoul Basic Parameter.

3. Selectați un tip și un mod de lumină suplimentară din lista derulantă. Dacă selectați modul **caPE**, ar trebui să setați luminozitatea.

4. **Opțional**: Clic **Implicit** pentru a restabili parametrii la setările implicite.

7.5.15 Setarea parametrilor biometrici

Setați parametrii de bază

Clic **Configurare** → **Smart** → **Smart**.

Face Parameters Settings

Face Anti-spoofing ☒

Live Face Detection Sec... ☒ Normal ☐ High ☐ Highest

Recognition Distance ☐ 0.5 ☐ 1.0 ☐ 1.5 ☐ 2.0 ☒ Auto

Application Mode ☒ Indoor ☐ Other

Continuous Recognition... 3 s

Pitch Angle 45 °

Yaw Angle 45 °

1:1 Matching Threshold 60

1:N Matching Threshold 87

ECO Mode ☒

4

ECO Mode (1:1) 60

ECO Mode (1:N) 70

Fingerprint

Fingerprint Security Level ▼

Save

Figura 7-16 Pagina Setări inteligente

Clic **Salva** pentru a salva setările după configurare. **Față**

Anti-spoofing

Activați sau dezactivați funcția de detectare a feței în direct. Dacă activați funcția, dispozitivul poate recunoaște dacă persoana este în viață sau nu.



Nota

Produsele de recunoaștere biometrică nu sunt aplicabile 100% în mediile anti-spoofing. Dacă aveți nevoie de un nivel de securitate mai ridicat, utilizați mai multe moduri de autentificare.

Live Face Detection Nivel de securitate

După activarea funcției anti-spoofing facială, puteți seta nivelul de securitate potrivit atunci când efectuați autentificarea facială live.

Distanța de recunoaștere

Selectați distanța dintre utilizatorul care se autentifică și camera dispozitivului.

Modul de aplicare

Selectați fie altele, fie interior, în funcție de mediul real. **Interval**

continuu de recunoaștere a feței

Setați intervalul de timp dintre două recunoașteri continue a feței la autentificare.

Unghiul de înclinare

Unghiul maxim de înclinare la pornirea autentificării feței. **Unghiul de rotire**

Unghiul maxim de rotire la pornirea autentificării feței.

Prag de potrivire 1:1

Setați pragul de potrivire atunci când vă autentificați prin modul de potrivire 1:1. Cu cât valoarea este mai mare, cu atât rata de acceptare falsă este mai mică și rata de respingere falsă este mai mare.

Pragul de potrivire 1:N

Setați pragul de potrivire atunci când vă autentificați prin modul de potrivire 1:N. Cu cât valoarea este mai mare, cu atât rata de acceptare falsă este mai mică și rata de respingere falsă este mai mare.

Modul ECO

După activarea modului ECO, dispozitivul va folosi camera IR pentru a autentifica fețele în condiții de lumină scăzută sau întuneric. Și puteți seta pragul modului ECO, modul ECO (1:N) și modul ECO (1:1).

Mod ECO (1:1)

Setați pragul de potrivire atunci când vă autentificați prin modul ECO, modul de potrivire 1:1. Cu cât valoarea este mai mare, cu atât rata de acceptare falsă este mai mică și rata de respingere falsă este mai mare.

Mod ECO (1:N)

Setați pragul de potrivire atunci când vă autentificați prin modul ECO 1:N. Cu cât valoarea este mai mare, cu atât rata de acceptare falsă este mai mică și rata de respingere falsă este mai mare.

Nivel de securitate a amprente

Selectați nivelul de securitate a amprente.

Cu cât este mai mare nivelul de securitate, cu atât este mai mică rata de acceptare falsă (FAR). Cu cât este mai mare nivelul de securitate, cu atât este mai mare rata de respingere falsă (FRR).

Setați zona de recunoaștere

Clic **Configurare** → **Smart** → **Configurare zonă**.

Trageți cadrul galben în videoclipul live pentru a regla zona de recunoaștere. Doar fața din zonă poate fi recunoscută de sistem.

Clic **Salva** pentru a salva setările.

Faceți clic pe  sau  pentru a înregistra videoclipuri sau a face fotografii.

7.5.16 Setări publicarea notificării

Puteți seta economizorul de ecran și timpul de somn pentru dispozitiv. Clic **Configurare** → **Publicare avis**.

Sleep ☐

Sleep after 60 S

Customize Screen Saver ☒

Screen Saver Picture Only JPEG format is allowed. Up to 16 pictures can be added.

Upload

Slide Show Interval 15 S

Save

Figura 7-17 Pagina de notificare

Dormi

Permite **Dormi** iar dispozitivul va intra în modul de repaus când nu există nicio operațiune cu timpul de repaus configurat.

Personalizați Screen Saver

Activați funcția și puteți încărca imaginile de economizor de ecran de pe computerul local. De asemenea, puteți seta intervalul de prezentare de diapozitive pentru economizorul de ecran.

Capitolul 8 Configurarea software-ului client

8.1 Fluxul de configurare al software-ului client

Urmați diagrama de flux de mai jos pentru a configura software-ul client.

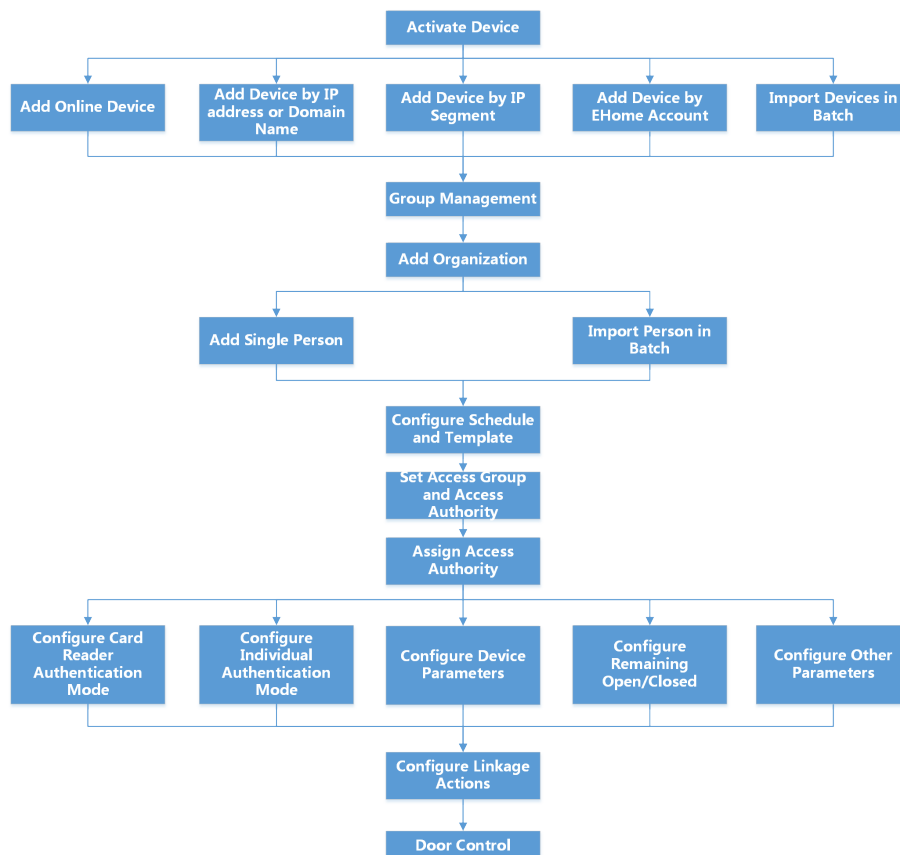


Figura 8-1 Diagrama de flux a configurației pe software-ul client

8.2 Managementul dispozitivelor

Puteți gestiona dispozitivele pe client, inclusiv adăugarea, editarea și ștergerea dispozitivelor. De asemenea, puteți efectua operațiuni precum verificarea stării dispozitivului.

8.2.1 Adăugați dispozitiv

Clientul oferă trei moduri de adăugare a dispozitivului, inclusiv prin IP/domeniu, segment IP și protocol ISUP. Clientul acceptă, de asemenea, importarea mai multor dispozitive într-un lot atunci când există o cantitate mare de dispozitive de adăugat.

Adăugați dispozitiv online

Dispozitivele online active din aceeași subrețea locală cu software-ul client vor fi afișate pe **Dispozitiv online**zonă.



Nota

- Puteți face clic **Reîmprospătare la 60 de secunde** pentru a reîmprospăta informațiile dispozitivelor online.
 - Funcția de jurnal SADP poate fi activată sau dezactivată făcând clic dreapta **Dispozitiv online**.
-

Adăugați un singur dispozitiv online

Puteți adăuga un singur dispozitiv online la software-ul client.

Pași

1. Intrați în modulul Device Management.
 2. **Opțional:** Faceți clic în partea dreaptă a **Managementul dispozitivelor** și selectați **Dispozitiv**.
 3. Clic **Dispozitiv online** pentru a afișa zona dispozitivului online.
Dispozitivele online căutate sunt afișate în listă.
 4. Selectați un dispozitiv online din **Dispozitiv online**zonă.
-



Nota

Pentru dispozitivul inactiv, trebuie să creați parola pentru acesta înainte de a putea adăuga dispozitivul în mod corespunzător. Pentru pași detaliați, consultați **Activare**.

5. Clic **Adăuga** pentru a deschide fereastra de adăugare a dispozitivului.

6. Introduceți informațiile necesare.

Nume

Introduceți un nume descriptiv pentru dispozitiv.

Adresa

Adresa IP a dispozitivului este obținută automat în acest mod de adăugare. **Port**

Numărul portului este obținut automat. **Nume de utilizator**

În mod implicit, numele de utilizator este

admin. **Parolă**

Introduceți parola dispozitivului.



Atenție

Puterea parolei dispozitivului poate fi verificată automat. Vă recomandăm cu căldură să schimbați parola pe care o alegeți (folosind minim 8 caractere, incluzând cel puțin trei tipuri de următoarele categorii: litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dumneavoastră. Și vă recomandăm să vă schimbați parola în mod regulat, mai ales în sistemul de înaltă securitate, schimbarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

Configurarea corectă a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau utilizatorului final.

7. Opțional: Verifica Sincronizarea timpului pentru a sincroniza ora dispozitivului cu computerul care rulează clientul după adăugarea dispozitivului la client.

8. Opțional: Verifica Import în grup pentru a crea un grup după numele dispozitivului.



Nota

Puteți importa în mod implicit toate canalele dispozitivului în grupul corespunzător.

9. Clic Bine pentru a adăuga dispozitivul.

Adăugați mai multe dispozitive online

Puteți adăuga mai multe dispozitive online la software-ul client.

Pași

1. Intrați în modulul Device Management.

2. Faceți clic în partea dreaptă a **Managementul dispozitivelor** și selectați **Dispozitiv**.

3. Clic Dispozitiv online pentru a afișa zona dispozitivului online.

Dispozitivele online căutate sunt afișate în listă.

4. Selectați mai multe dispozitive.



Nota

Pentru dispozitivul inactiv, trebuie să creați parola pentru acesta înainte de a putea adăuga dispozitivul în mod corespunzător. Pentru pași detaliați, consultați **Activare**.

5. Clic Adăuga pentru a deschide fereastra de adăugare a dispozitivului.

6. Introduceți informațiile necesare.

Nume de utilizator

În mod implicit, numele de utilizator este

admin. **Parolă**

Introduceți parola dispozitivului.



Atenție

Puterea parolei dispozitivului poate fi verificată automat. Vă recomandăm cu căldură să schimbați parola pe care o alegeți (folosind minim 8 caractere, incluzând cel puțin trei tipuri de următoarele categorii: litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dumneavoastră. Și vă recomandăm să vă schimbați parola în mod regulat, mai ales în sistemul de înaltă securitate, schimbarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

Configurarea corectă a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau utilizatorului final.

7. Opțional: Verificați **Sincronizarea timpului** pentru a sincroniza ora dispozitivului cu computerul care rulează clientul după adăugarea dispozitivelor la client.

8. Opțional: Verificați **Import în grup** pentru a crea un grup după numele dispozitivului.



Nota

Puteți importa în mod implicit toate canalele dispozitivului în grupul corespunzător.

9. Clic Bine pentru a adăuga dispozitivele.

Adăugați dispozitivul după adresa IP sau numele domeniului

Când știți adresa IP sau numele de domeniu al dispozitivului de adăugat, puteți adăuga dispozitive la client specificând adresa IP (sau numele domeniului), numele de utilizator, parola etc.

Pași

1. Accesați modulul de gestionare a dispozitivelor.

2. Clic **Dispozitiv** fila din partea de sus a panoului din dreapta.

Dispozitivele adăugate sunt afișate în panoul din dreapta.

3. Clic **Adăugare** pentru a deschide fereastra Adăugare, apoi selectați **IP/Domeniu** ca mod de adăugare.

4. Introduceți informațiile necesare.

Nume

Creați un nume descriptiv pentru dispozitiv. De exemplu, puteți utiliza o poreclă care poate arăta locația sau caracteristica dispozitivului.

Adresa

Adresa IP sau numele de domeniu al dispozitivului.

Port

Dispozitivele de adăugat partajează același număr de port. Valoarea implicită este **8000**. **Nume**

de utilizator

Introduceți numele de utilizator al dispozitivului. În mod implicit, numele de utilizator este

admin. **Parolă**

Introduceți parola dispozitivului.



Atenție

Puterea parolei dispozitivului poate fi verificată automat. Vă recomandăm cu căldură să schimbați parola pe care o alegeți (folosind minim 8 caractere, incluzând cel puțin trei tipuri de următoarele categorii: litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dumneavoastră. Și vă recomandăm să vă schimbați parola în mod regulat, mai ales în sistemul de înaltă securitate, schimbarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

Configurarea corectă a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau utilizatorului final.

5. Opțional: Verificați criptarea transmisiei (TLS) pentru a activa criptarea transmisiei folosind protocolul TLS (Transport Layer Security) în scop de securitate.



Nota

- Această funcție ar trebui să fie acceptată de dispozitiv.
- Vă puteți conecta la dispozitiv pentru a obține fișierul certificat prin browser web.

6. Verificați sincronizarea timpului pentru a sincroniza ora dispozitivului cu computerul care rulează clientul după adăugarea dispozitivului la client.

7. Opțional: Verificați importul în grup pentru a crea un grup după numele dispozitivului.

8. Finalizați adăugarea dispozitivului.

- Clic **Adăugă** pentru a adăuga dispozitivul și înapoi la pagina cu lista de dispozitive.
- Clic **Adăugați și Nou** pentru a salva setările și pentru a continua să adăugați alt dispozitiv.

9. Opțional: Efectuați următoarele operații.

Telecomanda

Configurare

Clic  pe coloana Operație pentru a seta configurația de la distanță a dispozitivul corespunzător.



Nota

Pentru pașii de operare detaliați pentru configurarea de la distanță, consultați manualul de utilizare al dispozitivului.

Stare dispozitiv

Clic  pe coloana Operațiune pentru a vedea starea dispozitivului, inclusiv camere, starea înregistrării, starea semnalului, starea hardware-ului etc.

Editați dispozitivul

Informații

Faceți clic  pe coloana Operațiune pentru a edita informațiile despre dispozitiv, cum ar fi adresa IP, numele de utilizator și parola.

Verificați utilizatorul online

Faceți clic  pe coloana Operațiune pentru a verifica utilizatorii online care accesează dispozitivul, cum ar fi numele de utilizator, tipul de utilizator, adresa IP a utilizatorului și ora de conectare.

Reimprospăta

Clic  pe coloana Operațiune pentru a obține cele mai recente informații despre dispozitiv.

Ștergeți dispozitivul

Selecțați unul sau mai multe dispozitive și faceți clic **Șterge** pentru a șterge dispozitivul(e) selectat(e) de la client.

Adăugați dispozitive după segmentul IP

Dacă dispozitivele partajează același număr de port, nume de utilizator și parolă și adresele lor IP partajează un segment IP. Puteți specifica adresa IP de început și adresa IP de final, numărul de port, numele de utilizator, parola etc. ale dispozitivelor pentru a le adăuga la client.

Pași

1. Intrați în modulul Device Management.

2. Clic **Dispozitiv** fila din partea de sus a panoului din dreapta.

Dispozitivele adăugate sunt afișate în panoul din dreapta.

3. Clic **Adăuga** pentru a deschide fereastra Adăugare.

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

5. Introduceți informațiile necesare.

IP de pornire

Introduceți o adresă IP de pornire.

Încheiere IP

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

În mod implicit, numele de utilizator este

admin. Parolă

Introduceți parola dispozitivului.



Atenție

Puterea parolei dispozitivului poate fi verificată automat. Vă recomandăm cu căldură să schimbați parola pe care o alegeți (folosind minim 8 caractere, incluzând cel puțin trei tipuri de următoarele categorii: litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dumneavoastră. Și vă recomandăm să vă schimbați parola în mod regulat, mai ales în sistemul de înaltă securitate, schimbarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

Configurarea corectă a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau utilizatorului final.

6. Opțional: Verificați **Criptare transmisie (TLS)** pentru a activa criptarea transmisiei folosind protocolul TLS (Transport Layer Security) în scop de securitate.

Nota

- Această funcție ar trebui să fie acceptată de dispozitiv.
- Vă puteți conecta la dispozitiv pentru a obține fișierul certificat prin browser web.

7. Verificați **Sincronizarea timpului** pentru a sincroniza ora dispozitivului cu computerul care rulează clientul după adăugarea dispozitivului la client.

8. **Opțional:** Verificați **Import în grup** pentru a crea un grup după numele dispozitivului.

9. Finalizați adăugarea dispozitivului.

- Clic **Adăuga** pentru a adăuga dispozitivul și înapoi la pagina cu lista de dispozitive.
- Clic **Adăugați și Nou** pentru a salva setările și pentru a continua să adăugați alt dispozitiv.

10. **Opțional:** Efectuați următoarele operații.

Telecomanda

Configurare

Clic  pe coloana Operație pentru a seta configurația de la distanță a dispozitivul corespunzător.

Nota

Pentru pașii de operare detaliați pentru configurarea de la distanță, consultați manualul de utilizare al dispozitivului.

Stare dispozitiv

Clic  pe coloana Operațiune pentru a vedea starea dispozitivului, inclusiv camere, starea înregistrării, starea semnalului, starea hardware-ului etc.

Editați dispozitivul

Informații

Faceți clic  pe coloana Operațiune pentru a edita informațiile despre dispozitiv, cum ar fi adresa IP, numele de utilizator și parola.

Verificați utilizatorul online

Faceți clic  pe coloana Operațiune pentru a verifica utilizatorii online care accesează dispozitivul, cum ar fi numele de utilizator, tipul de utilizator, adresa IP a utilizatorului și ora de conectare.

Reîmprospăta

Faceți clic  pe coloana Operațiune pentru a obține cele mai recente informații despre dispozitiv.

Ștergeți dispozitivul

Selectați unul sau mai multe dispozitive și faceți clic **Șterge** pentru a șterge dispozitivul(e) selectat(e) de la client.

Adăugați dispozitiv prin contul EHome

Pentru dispozitivele de control acces care acceptă protocolul EHome 5.0, le puteți adăuga la client prin protocolul EHome după ce ați introdus ID-ul și cheia dispozitivului, dacă le-ați configurat adresele serverului, numărul portului și ID-urile dispozitivului.

Înainte de a începe

Asigurați-vă că dispozitivele s-au conectat corect la rețea.

Pași

1. Accesați modulul de gestionare a dispozitivelor.

Dispozitivele adăugate sunt afișate în panoul din dreapta.

2. Clic **Adăugă** pentru a deschide fereastra Adăugare.

3. Selecta **EHome** ca mod de adăugare.

4. Introduceți informațiile necesare.

Cont de dispozitiv

Introduceți numele contului înregistrat pe protocolul EHome. **Cheia**

EHome

Pentru dispozitivele EHome 5.0, introduceți cheia EHome dacă ați setat-o când configurați parametrul centrului de rețea pentru dispozitiv.



Nota

Această funcție ar trebui să fie acceptată de dispozitiv.

5. **Opțional:** Verifica **Sincronizarea timpului** pentru a sincroniza ora dispozitivului cu computerul care rulează clientul după adăugarea dispozitivului la client.

6. **Opțional:** Verifica **Import în grup** pentru a crea un grup după numele dispozitivului și pentru a importa toate canalele dispozitivului în grup.

7. Finalizați adăugarea dispozitivului.

- Clic **Adăugă** pentru a adăuga dispozitivul și a reveni la lista de dispozitive.
- Clic **Adăugați și Nou** pentru a salva setările și pentru a continua să adăugați alt dispozitiv.



Nota

Imaginile feței nu pot fi aplicate dispozitivelor adăugate de contul EHome.

8. **Opțional:** Efectuați următoarele operații. **Stare**

dispozitiv

Editați dispozitivul

Informații

Verificați utilizatorul online

Reîmprospăta

Ștergeți dispozitivul

Clic  pe coloana Operațiune pentru a vedea starea dispozitivului.

Clic  pe coloana Operație pentru a edita informațiile despre dispozitiv, cum ar fi numele dispozitivului, contul dispozitivului și cheia EHome.

Faceți clic  pe coloana Operațiune pentru a verifica utilizatorii online care accesează dispozitivul, cum ar fi numele de utilizator, tipul de utilizator, adresa IP a utilizatorului și ora de conectare.

Clic  pe coloana Operațiune pentru a obține cele mai recente informații despre dispozitiv.

Selectați unul sau mai multe dispozitive și faceți clic **Șterge** pentru a șterge dispozitivul(ele) selectat(e) de la client.

Importați dispozitive într-un lot

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

Pași

1. Accesați pagina Device Management

2. Clic **Adăugă** pentru a deschide fereastra de adăugare a dispozitivului.

3. Selectați **Import lot** ca mod de adăugare.

4. Clic **Export șablon** și apoi salvați șablonul predefinit (fișier CSV) pe computer.

5. Deschideți fișierul șablon exportat și introduceți informațiile necesare despre dispozitivele care vor fi adăugate în coloana corespunzătoare.

Mod de adăugare

Poti intra **0** sau **1** care indica diferite moduri de adăugare. **0** indică faptul că dispozitivul este adăugat prin adresa IP sau numele de domeniu; **1** indică faptul că dispozitivul este adăugat prin EHome.

Adresa

Editați adresa dispozitivului. Dacă setați **0** ca mod de adăugare, ar trebui să introduceți adresa IP sau numele de domeniu al dispozitivului; dacă ai setat **1** ca mod de adăugare, acest fișier nu este necesar.

Port

Introduceți numărul portului dispozitivului. Valoarea implicită este 8000.

Informații despre dispozitiv

Dacă setați **0** ca mod de adăugare, acest câmp nu este obligatoriu. Dacă setați **1** ca mod de adăugare, introduceți contul EHome.

Nume de utilizator

Introduceți numele de utilizator al dispozitivului. În mod implicit, numele de utilizator este

admin. **Parolă**

Dacă setați **0** ca mod de adăugare, introduceți parola. Dacă setați **1** ca mod de adăugare, introduceți tasta EHome.



Atenție

Puterea parolei dispozitivului poate fi verificată automat. Vă recomandăm cu căldură să schimbați parola pe care o alegeți (folosind minim 8 caractere, incluzând cel puțin trei tipuri de următoarele categorii: litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dumneavoastră. Și vă recomandăm să vă schimbați parola în mod regulat, mai ales în sistemul de înaltă securitate, schimbarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

Configurarea corectă a tuturor parolelelor și a altor setări de securitate este responsabilitatea instalatorului și/sau utilizatorului final.

Import în grup

Poti intra **1** pentru a crea un grup după numele dispozitivului. Toate canalele dispozitivului vor fi importate implicit în grupul corespunzător. **0** indică dezactivarea acestei funcții.

6. Faceți clic și selectați fișierul șablon.

7. Clic **Adăugă** pentru a importa dispozitivele.

8.2.2 Resetează parola dispozitivului

Dacă ați uitat parola dispozitivelor online detectate, puteți reseta parola dispozitivului prin client.

Pași

1. Accesați pagina Device Management.

2. Clic **Dispozitiv online** pentru a afișa zona dispozitivului online.

Toate dispozitivele online din aceeași subrețea se vor afișa în listă.

3. Selectați dispozitivul din listă și faceți clic pe coloana Operație.

4. Clic **Export** pentru a salva fișierul dispozitivului pe computer și apoi a trimite fișierul la suportul nostru tehnic.



Nota

Pentru următoarele operațiuni de resetare a parolei, contactați suportul nostru tehnic.



Atenție

Puterea parolei dispozitivului poate fi verificată automat. Vă recomandăm cu căldură să schimbați parola pe care o alegeți (folosind minim 8 caractere, incluzând cel puțin trei tipuri de următoarele categorii: litere mari, litere mici, cifre și caractere speciale) pentru a crește securitatea produsului dumneavoastră. Și vă recomandăm să vă schimbați parola în mod regulat, mai ales în sistemul de înaltă securitate, schimbarea parolei lunar sau săptămânal vă poate proteja mai bine produsul.

Configurarea corectă a tuturor parolelor și a altor setări de securitate este responsabilitatea instalatorului și/sau utilizatorului final.

8.3 Managementul grupului

Clientul oferă grupuri pentru a gestiona resursele adăugate în diferite grupuri. Puteți grupa resursele în diferite grupuri în funcție de locațiile resurselor.

Exemplu

De exemplu, la etajul 1, au fost montate 16 uși, 64 de intrări de alarmă și 16 ieșiri de alarmă. Puteți organiza aceste resurse într-un singur grup (numit 1st Floor) pentru o gestionare convenabilă. Puteți controla starea ușii și puteți efectua alte operațiuni ale dispozitivelor după gestionarea resurselor pe grupuri.

8.3.1 Adăugați grup

Puteți adăuga grup pentru a organiza dispozitivul adăugat pentru o gestionare convenabilă.

Pași

1. Intrați în modulul Device Management.

2. **Clic Gestionare dispozitive → Grup** pentru a intra pe pagina de gestionare a grupului.

3. Creați un grup.

- Clic **Adăugați grup** și introduceți un nume de grup după cum doriți.
- Clic **Creați grup după numele dispozitivului** și selectați un dispozitiv adăugat pentru a crea un grup nou după numele dispozitivului selectat.



Nota

Resursele (cum ar fi intrările/ieșirile de alarmă, punctele de acces etc.) ale acestui dispozitiv vor fi importate în grup în mod implicit.

8.3.2 Importați resurse în grup

Puteți importa resursele dispozitivului (cum ar fi intrări/ieșiri de alarmă, puncte de acces etc.) în grupul adăugat într-un lot.

Înainte de a începe

Adăugați un grup pentru gestionarea dispozitivelor. Consultați **Adăugați grup**.

Pași

1. Intrați în modulul Device Management.

2. **Clic Gestionare dispozitive → Grup** pentru a intra pe pagina de gestionare a grupului.

3. Selectați un grup din lista de grupuri și selectați tipul de resursă ca **Punct de acces**, **Intrare alarmă**, **Ieșire de alarmă**, etc.

4. **Clic Import**.

5. Selectați miniaturile/numele resurselor în vizualizarea miniatură/listă.



Nota

Puteți da clic  **Sa**  pentru a comuta modul de afișare a resurselor la vizualizarea în miniatură sau la vizualizarea listă.

6. **Clic Import** pentru a importa resursele selectate în grup.

8.3.3 Editați parametrul resursei

După importarea resurselor în grup, puteți edita parametrul resursei. Pentru punctul de acces, puteți edita numele punctului de acces. Pentru intrarea alarmei, puteți edita numele intrării alarmei. Aici luăm ca exemplu punctul de acces.

Înainte de a începe

Importați resursele în grup. Consultați **Importă resurse în grup**.

Pași

1. Intrați în modulul Device Management.

2. **Clic Gestionare dispozitive → Grup** pentru a intra pe pagina de gestionare a grupului.

Toate grupurile adăugate sunt afișate în stânga.

3. Selectați un grup din lista de grupuri și faceți clic **Punct de**

acces. Se vor afișa punctele de acces importate în grup.

4. Faceți clic  în coloana Operație pentru a deschide fereastra Editare resurse.

5. Editați numele resursei.

6. Clic **Bine** pentru a salva noile setări.

8.3.4 Eliminarea resurselor din grup

Puteți elimina resursele adăugate din grup.

Pași

1. Intrați în modulul Device Management.

2. Clic **Gestionare dispozitive** → **Grup** pentru a intra pe pagina de gestionare a grupului.

Toate grupurile adăugate sunt afișate în stânga.

3. Faceți clic pe un grup pentru a afișa resursele adăugate acestui grup.

4. Selectați resursa (resursele) și faceți clic **Șterge** pentru a elimina resursa (resursele) din grup.

8.4 Managementul persoanelor

Puteți adăuga informații despre persoană în sistem pentru operațiuni ulterioare, cum ar fi controlul accesului, interfon video, ora și prezența etc. Puteți gestiona persoanele adăugate, cum ar fi emiterea de carduri către acestea într-un lot, importarea și exportarea informațiilor despre persoană într-un lot etc.

8.4.1 Adăugați organizație

Puteți adăuga o organizație și importa informații despre persoane în organizație pentru gestionarea eficientă a persoanelor. De asemenea, puteți adăuga o organizație subordonată pentru cea adăugată.

Pași

1. Intrați **Persoană** modul.

2. Selectați o organizație părinte în coloana din stânga și faceți clic **Adăuga** în colțul din stânga sus pentru a adăuga o organizație.

3. Creați un nume pentru organizația adăugată.



Nota

Pot fi adăugate până la 10 niveluri de organizații.

4. **Opțional:** Efectuați următoarele operații.

Editați organizația

Plasați mouse-ul pe o organizație adăugată și faceți clic pe  pentru a-i edita nume.

Șterge Organizare

Plasați mouse-ul pe o organizație adăugată și faceți clic



pentru a-l șterge.



Nota

- 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.

Afișați Persoane în Suborganizație

Verificați și selectați o organizație pentru a afișa persoanele din suborganizațiile sale.

8.4.2 Configurarea informațiilor de bază

Puteți adăuga o persoană la software-ul client una câte una și puteți configura informațiile de bază ale persoanei, cum ar fi numele, sexul, numărul de telefon etc.

Pași

1. Întrați în modul Persoană.

2. Selectați o organizație din lista de organizații pentru a adăuga persoana respectivă.

3. Clic **Adăugă** pentru a deschide fereastra de adăugare a persoanei.

ID-ul persoanei va fi generat automat.

4. Introduceți informațiile de bază, inclusiv numele persoanei, sexul, telefonul, adresa de e-mail etc.

5. Opțional: Setati perioada efectivă a persoanei. Odată expirat, acreditările și setările de control al accesului ale persoanei vor fi invalide, iar persoana respectivă nu va avea autorizație pentru a accesa ușile/etajele.

Exemplu

De exemplu, dacă persoana respectivă este un vizitator, perioada sa efectivă poate fi scurtă și temporară.

6. Confirmați pentru a adăuga persoana.

- Clic **Adăugă** pentru a adăuga persoana și pentru a închide fereastra Adăugare persoană.
- Clic **Adăugați și Nou** pentru a adăuga persoana și pentru a continua să adăugați alte persoane.

8.4.3 Emite un card prin modul local

Dacă este disponibilă o stație de înregistrare a cardului, puteți emite un card prin modul local. Pentru a citi numărul cardului, trebuie să conectați stația de înregistrare a cardului la computerul care rulează clientul prin interfața USB sau COM și așezați cardul pe stația de înregistrare a cardului.

Pași

1. Întrați în modul Persoană.

2. Selectați o organizație din lista de organizații pentru a adăuga persoana și faceți clic **Adăugă** pentru a intra în panoul Adăugare persoană.

**Nota**

- 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.

Afișați Persoane în Suborganizație

Verificați **Afișați persoanele din suborganizație** și selectați o organizație pentru a afișa persoanele din suborganizațiile sale.

8.4.2 Configurarea informațiilor de bază

Puteți adăuga o persoană la software-ul client una câte una și puteți configura informațiile de bază ale persoanei, cum ar fi numele, sexul, numărul de telefon etc.

Pași**1. Întră Persoană modul.**

2. Selectați o organizație din lista de organizații pentru a adăuga persoana respectivă.

3. Clic **Adăugă** pentru a deschide fereastra de adăugare a persoanei.

ID-ul persoanei va fi generat automat.

4. Introduceți informațiile de bază, inclusiv numele persoanei, sexul, telefonul, adresa de e-mail etc.

5. Opțional: Setati perioada efectivă a persoanei. Odată expirat, acreditările și setările de control al accesului ale persoanei vor fi invalide, iar persoana respectivă nu va avea autorizație pentru a accesa ușile/etajele.

Exemplu

De exemplu, dacă persoana respectivă este un vizitator, perioada sa efectivă poate fi scurtă și temporară.

6. Confirmați pentru a adăuga persoana.

- Clic **Adăugă** pentru a adăuga persoana și pentru a închide fereastra Adăugare persoană.
- Clic **Adăugați și Nou** pentru a adăuga persoana și pentru a continua să adăugați alte persoane.

8.4.3 Emite un card prin modul local

Dacă este disponibilă o stație de înregistrare a cardului, puteți emite un card prin modul local. Pentru a citi numărul cardului, trebuie să conectați stația de înregistrare a cardului la computerul care rulează clientul prin interfața USB sau COM și așezați cardul pe stația de înregistrare a cardului.

Pași**1. Întră Persoană modul.**

2. Selectați o organizație din lista de organizații pentru a adăuga persoana și faceți clic **Adăugă** pentru a intra în panoul Adăugare persoană.

Nota

Introduceți mai întâi informațiile de bază ale persoanei respective. Pentru detalii despre configurarea informațiilor de bază ale persoanei, consultați **Configurați informațiile de bază**.

3.În **Credențială** → **Card** zonă, faceți clic+.

4.Clic **Setări** pentru a intra în pagina Setări.

5.Selecta **Local** ca modul de emiteră a cardului.

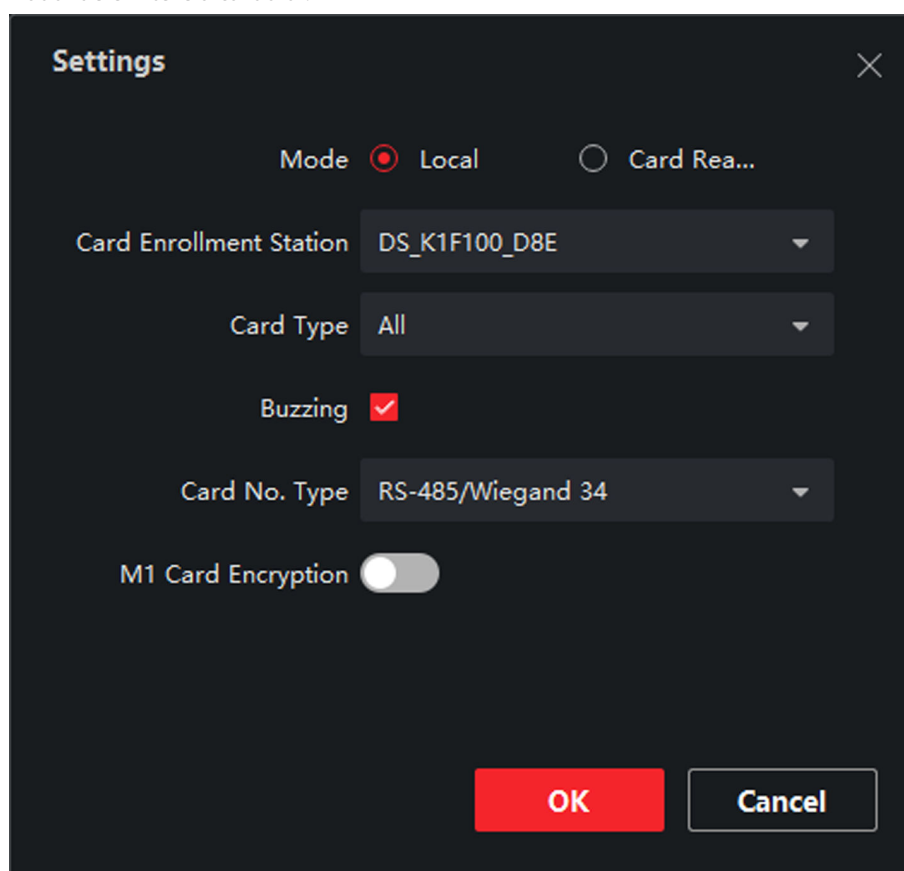


Figura 8-2 Emiterea unui card în modul local

6.Setați alți parametri corelați. **Stația de**

înregistrare a cardurilor

Selectați modelul stației de înregistrare a cardului conectat.

Nota

În prezent, modelele de stații de înregistrare a cardurilor acceptate includ DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E și DS-K1F180-D8E.

Tip card

Acest câmp este disponibil numai când modelul este DS-K1F100-D8E sau DS-K1F180-D8E. Selectați tipul cardului ca card EM sau card Mifare în funcție de tipul de card real.

Zumzet

Activați sau dezactivați sunetul când numărul cardului este citit cu succes.

Tip card nr

Selectați tipul numărului de card în funcție de nevoile reale.

Criptare card M1

Acest câmp este disponibil numai când modelul este DS-K1F100-D8, DS-K1F100-D8E sau DS-K1F180-D8E. Dacă cardul este un card M1, atunci puteți activa funcția M1 Card Encryption și puteți selecta sectorul cardului de criptat.

7.ClicBine pentru a confirma operația.

8.Așezați cardul pe stația de înregistrare a cardului și faceți clic **Citire** pentru a obține numărul cardului.

Numărul cardului va fi afișat automat în câmpul Nr. card.

9.ClicAdăuga.

Cardul va fi eliberat persoanei.

8.4.4 Încărcați o fotografie a feței de pe computerul local

Când adăugați o persoană, puteți încărca pe client o fotografie a feței stocată pe computerul local ca profil al persoanei.

Pași

1.Intră **Persoană** modul.

2.Selectați o organizație din lista de organizații pentru a adăuga persoana și faceți clic **Adăuga**.



Nota

Introduceți mai întâi informațiile de bază ale persoanei respective. Pentru detalii despre configurarea informațiilor de bază ale persoanei, consultați **Configurați informațiile de bază**.

3.ClicAdăugați Fața în panoul Informații de bază.

4.Selecta **Încărcați**.

5.Selectați o imagine de pe computerul care rulează clientul.



Nota

Imaginea trebuie să fie în format JPG sau JPEG și mai mică de 200 KB.

6. Opțional: Permite **Verificați după dispozitiv** pentru a verifica dacă dispozitivul de recunoaștere facială gestionat în client poate recunoaște fața din fotografie.

7.Confirmați pentru a adăuga persoana.

- Clic **Adăuga** pentru a adăuga persoana și pentru a închide fereastra Adăugare persoană.
- Clic **Adăugați și Nou** pentru a adăuga persoana și pentru a continua să adăugați alte persoane.

8.4.5 Faceți o fotografie prin client

Când adăugați o persoană, puteți face o fotografie a persoanei de către camera web a computerului care rulează clientul și puteți seta această fotografie ca profil al persoanei.

Înainte de a începe

Adăugați cel puțin un dispozitiv de control al accesului verificând dacă fața din fotografie poate fi recunoscută de dispozitivul de recunoaștere facială gestionat de client.

Pași

1. Întrați în **Persoană** modul.

2. Selectați o organizație din lista de organizații pentru a adăuga persoana și faceți clic **Adăuga**.



Nota

Introduceți mai întâi informațiile de bază ale persoanei respective. Pentru detalii despre configurarea informațiilor de bază ale persoanei, consultați **Configurați informațiile de bază**.

3. Clic **Adăugați Fața** în panoul Informații de bază.

4. Selectați **Faceți o fotografie**.

5. Conectați scannerul facial la computerul care rulează clientul.

6. **Opțional:** Permiteți **Verificați după dispozitiv** pentru a verifica dacă dispozitivul de recunoaștere facială gestionat în client poate recunoaște fața din fotografie.

7. Faceți o fotografie.

1) Îndreptați-vă către camera web a computerului și asigurați-vă că fața dvs. este în mijlocul ferestrei de colectare.

2) Faceți clic **Centru** pentru a captura o fotografie a feței.

3) **Opțional:** Faceți clic pe **Centru** pentru a captura din nou.

4) Faceți clic **Bine** pentru a salva fotografia capturată.

8. Confirmați pentru a adăuga persoana.

- Clic **Adăuga** pentru a adăuga persoana și pentru a închide fereastra Adăugare persoană.
- Clic **Adăugați și Nou** pentru a adăuga persoana și pentru a continua să adăugați alte persoane.

8.4.6 Colectați fața prin intermediul dispozitivului de control al accesului

Când adăugați o persoană, puteți colecta fața persoanei prin intermediul dispozitivului de control al accesului adăugat clientului, care acceptă funcția de recunoaștere facială.

Pași

1. Întrați în **Persoană** modul.

2. Selectați o organizație din lista de organizații pentru a adăuga persoana și faceți clic **Adăuga**.



Nota

Introduceți mai întâi informațiile de bază ale persoanei respective. Pentru detalii despre configurarea informațiilor de bază ale persoanei, consultați **Configurați informațiile de bază**.

3. **Clic Adăugați Fața** în panoul Informații de bază.

4. **Selecta Colectare de la distanță**.

5. **Selectați** un dispozitiv de control al accesului care acceptă funcția de recunoaștere a feței din lista derulantă.

6. **Adună fața**.

- 1) Îndreptați-vă spre camera dispozitivului de control al accesului selectat și asigurați-vă că fața dvs. se află în mijlocul ferestrei de colectare.
- 2) Faceți clic  pentru a face o fotografie.
- 3) Faceți clic **Bine** pentru a salva fotografia capturată.

7. **Confirmați** pentru a adăuga persoana.

- **Clic Adăuga** pentru a adăuga persoana și pentru a închide fereastra Adăugare persoană.
- **Clic Adăugați și Nou** pentru a adăuga persoana și pentru a continua să adăugați alte persoane.

8.4.7 Colectați amprenta prin client

Colectarea amprentelor la nivel local înseamnă că puteți colecta amprenta prin intermediul înregistratorului de amprente conectat direct la computerul care rulează clientul. Ampretele înregistrate pot fi folosite ca acreditări ale persoanelor care accesează ușile autorizate.

Înainte de a începe

Conectați înregistratorul de amprentă la computerul care rulează clientul.

Pași

1. **Intră Persoană** modul.

2. **Selectați** o organizație din lista de organizații pentru a adăuga persoana și faceți clic **Adăuga**.



Nota

Introduceți mai întâi informațiile de bază ale persoanei respective. Pentru detalii despre configurarea informațiilor de bază ale persoanei, consultați **Configurați informațiile de bază**.

3. **În Acreditare → Amprentă** panou, faceți clic **+**.

4. **În** fereastra pop-up, **selectați** modul de colectare ca **Local**.

5. **Selectați** modelul înregistratorului de amprente conectat.



Nota

Dacă înregistrarea de amprente este DS-K1F800-F, puteți face clic **Setări** pentru a selecta COM la care se conectează înregistratorul de amprentă.

6. **Colectați amprenta**.

- 1) Faceți clic **Început**.
- 2) Așezați și ridicați-vă amprenta pe înregistratorul de amprentă pentru a colecta amprenta.
- 3) Faceți clic **Adăuga** pentru a salva amprenta înregistrată.

7. **Confirmați** pentru a adăuga persoana.

- **Clic Adăuga** pentru a adăuga persoana și pentru a închide fereastra Adăugare persoană.
- **Clic Adăugați și Nou** pentru a adăuga persoana și pentru a continua să adăugați alte persoane.

Nota

Odată ce amprenta este adăugată, tipul de amprentă nu poate fi schimbat.

8.4.8 Colectați amprenta prin intermediul dispozitivului de control al accesului

Când adăugați o persoană, puteți colecta informații despre amprentă prin intermediul modulului de amprentă al dispozitivului de control al accesului. Ampretele înregistrate pot fi folosite ca acreditări ale persoanelor care accesează ușile autorizate.

Înainte de a începe

Asigurați-vă că colectarea amprentelor digitale este acceptată de dispozitivul de control al accesului.

Pași

1. În **Persoană** modul.

2. Selectați o organizație din lista de organizații pentru a adăuga persoana și faceți clic **Adăuga**.

Nota

Introduceți mai întâi informațiile de bază ale persoanei respective. Pentru detalii despre configurarea informațiilor de bază ale persoanei, consultați **Configurați informațiile de bază**.

3. În **Acreditare** → **Amprentă** panou, faceți clic **+**.

4. În fereastra pop-up, selectați modul de colectare ca **Telecomanda**.

5. Selectați un dispozitiv de control al accesului care acceptă funcția de recunoaștere a amprente din lista verticală.

6. Colectați amprenta.

1) Faceți clic **Început**.

2) Așezați și ridicați-vă amprenta pe scannerul de amprentă al dispozitivului de control al accesului selectat pentru a colecta amprenta.

3) Faceți clic **Adăuga** pentru a salva amprenta înregistrată.

7. Confirmați pentru a adăuga persoana.

- Clic **Adăuga** pentru a adăuga persoana și pentru a închide fereastra Adăugare persoană.
- Clic **Adăugați și Nou** pentru a adăuga persoana și pentru a continua să adăugați alte persoane.

Nota

Odată ce amprenta este adăugată, tipul de amprentă nu poate fi schimbat.

8.4.9 Configurați informațiile de control acces

Când adăugați o persoană, îi puteți seta proprietățile de control al accesului, cum ar fi setarea persoanei ca vizitator sau pe lista neagră sau ca super utilizator care are super-autorizare.

Pași

1. În **Persoană** modul.

2. Selectați o organizație din lista de organizații pentru a adăuga persoana și faceți clic **Adăuga**.

3. În **Control acces** zonă, setați proprietățile de control al accesului persoanei.

Grup de acces

Puteți selecta unul sau mai multe grupuri de acces pentru ca persoana respectivă să-i dea autorizația pentru punctele de acces selectate. Pentru detalii, consultați **Setați grupul de acces pentru a atribui autorizație de acces persoanelor**.

Parolă

Persoana trebuie să introducă parola după ce glisează cardul sau amprenta digitală la accesare. Nu poate fi utilizat independent și ar trebui să conțină 4 până la 8 cifre.

Super utilizator

Dacă persoana este setată ca super utilizator, va avea autorizație de a accesa toate ușile/ etajele și va fi scutită de restricțiile rămase închise, de toate regulile anti-passback și de autorizarea primei persoane.

Timp de deschidere extins al ușii

Când persoana care accesează ușa, acordați acestei persoane mai mult timp pentru a trece prin ușile care au fost configurate cu o durată de deschidere extinsă. Utilizați această funcție pentru persoanele cu mobilitate redusă.

Pentru detalii despre setarea duratei de deschidere a ușii, consultați **Configurați parametrii pentru ușă. Adăugați la**

lista neagră

Adăugați persoana în lista neagră și atunci când persoana încearcă să acceseze uși/pardoseli, se va declanșa un eveniment și se va trimite clientului pentru a anunța personalul de securitate.

Marcați ca vizitator

Dacă persoana respectivă este un vizitator, setați timpii maximi de autentificare, inclusiv accesul prin card și amprenta digitală pentru a limita timpii de acces ale vizitatorului.



Nota

Timpul maxim de autentificare ar trebui să fie între 1 și 100.

Operator de dispozitiv

Pentru persoana cu rol de operator de dispozitiv, aceasta este autorizată să opereze pe dispozitivele de control acces.



Nota

Funcțiile Super User, Extended Door Open Time, Add to Blacklist și Mark as Visitor nu pot fi activate simultan. De exemplu, dacă o persoană este setată ca super utilizator, nu puteți activa durata extinsă a ușii pentru ea/ea, nu o puteți adăuga pe lista neagră sau nu o puteți seta ca vizitator.

4. Confirmați pentru a adăuga persoana.

- Clic **Adăuga** pentru a adăuga persoana și pentru a închide fereastra Adăugare persoană.
- Clic **Adăugați și Nou** pentru a adăuga persoana și pentru a continua să adăugați alte persoane.

8.4.10 Personalizați informații despre persoană

Puteți personaliza proprietățile persoanei care nu sunt predefinite în client în funcție de nevoile reale, de exemplu, locul nașterii. După personalizare, atunci când adăugați o persoană, puteți introduce informațiile personalizate pentru a completa informațiile despre persoană.

Pași

1. Intră în **Persoană** modul.

2. Setează câmpurile de informații personalizate.

- 1) Faceți clic **Proprietate personalizată**.
- 2) Faceți clic **Adăuga** pentru a adăuga o nouă proprietate.
- 3) Introduceți numele proprietății.
- 4) Faceți clic **Bine**.

3. Setează informațiile personalizate atunci când adăugați o persoană.

- 1) Selectați o organizație din lista de organizații pentru a adăuga persoana și faceți clic **Adăuga**.



Nota

Introduceți mai întâi informațiile de bază ale persoanei respective. Pentru detalii despre configurarea informațiilor de bază ale persoanei, consultați **Configurați informațiile de bază**.

- 2) În **Informații personalizate** panoul, introduceți informațiile despre persoană.

- 3) Faceți clic **Adăuga** pentru a adăuga persoana și pentru a închide fereastra Adăugare persoană sau faceți clic **Adăugați și Nou** pentru a adăuga persoana și pentru a continua să adăugați alte persoane.

8.4.11 Configurați informațiile rezidenților

Dacă persoana este rezidentă, în scopul interfonului video, trebuie să setați numărul camerei pentru ea și să legați o stație interioară. După legat, puteți apela această persoană sunând la postul de interior și efectuați interfon video cu ea.

Pași

1. Intră în **Persoană** modul.

2. Selectați o organizație din lista de organizații pentru a adăuga persoana și faceți clic **Adăuga**.



Nota

Introduceți mai întâi informațiile de bază ale persoanei respective. Pentru detalii despre configurarea informațiilor de bază ale persoanei, consultați **Configurați informațiile de bază**.

3. În **Informații despre rezidenți** panou, selectați stația interioară pentru a o lega de persoana respectivă.



Nota

Dacă selectați **Stație interioară analogică**, cel **Stația de ușă** câmpul va fi afișat și vi se cere să selectați stația de ușă pentru a comunica cu stația interioară analogică.

4. Introduceți numărul etajului și numărul camerei persoanei.

5. Confirmați pentru a adăuga persoana.

- Clic **Adăuga** pentru a adăuga persoana și pentru a închide fereastra Adăugare persoană.
- Clic **Adăugați și Nou** pentru a adăuga persoana și pentru a continua să adăugați alte persoane.

8.4.12 Configurați informații suplimentare

Când adăugați o persoană, puteți configura informații suplimentare pentru persoana respectivă, cum ar fi tipul de identitate al persoanei, numărul de identitate, țara etc., în funcție de nevoile reale.

Pași

1. Întrați în modulul Persoană.

2. Selectați o organizație din lista de organizații pentru a adăuga persoana și faceți clic **Adăuga**.



Nota

Introduceți mai întâi informațiile de bază ale persoanei respective. Pentru detalii despre configurarea informațiilor de bază ale persoanei, consultați **Configurați informațiile de bază**.

3. În **Informații suplimentare** panoul, introduceți informațiile suplimentare ale persoanei, inclusiv tipul ID persoanei, nr ID, titlul postului etc., în funcție de nevoile reale.

4. Confirmați pentru a adăuga persoana.

- Clic **Adăuga** pentru a adăuga persoana și pentru a închide fereastra Adăugare persoană.
- Clic **Adăugați și Nou** pentru a adăuga persoana și pentru a continua să adăugați alte persoane.

8.4.13 Importați și exportați informații de identificare a persoanei

Puteți importa informațiile și imaginile mai multor persoane în software-ul client într-un lot. Între timp, puteți, de asemenea, să exportați informațiile despre persoană și imaginile și să le salvați pe computer.

8.4.14 Importați informații despre persoană

Puteți introduce informațiile mai multor persoane într-un șablon predefinit (un fișier CSV) pentru a importa informațiile către client într-un lot.

Pași

1. Intrați în modulul Persoană.

2. Selectați o organizație adăugată în listă sau faceți clic **Adăuga** în colțul din stânga sus pentru a adăuga o organizație și apoi selectați-o.

3. Clic **Import** pentru a deschide panoul Import.

4. Selectați **Informații despre persoană** ca mod de import.

5. Clic **Descărcați șablonul pentru persoana care importă** pentru a descărca șablonul.

6. Introduceți informațiile despre persoană în șablonul descărcat.

Nota

- Dacă persoana are mai multe cărți, separați numărul cardului cu punct și virgulă.
 - Elementele cu asterisc sunt obligatorii.
 - În mod implicit, Data Închirierii este data curentă.
-

7. Faceți clic  pentru a selecta fișierul CSV cu informații despre persoană.

8. Clic **Import** pentru a începe importul.

Nota

- Dacă o persoană Nr. există deja în baza de date a clientului, ștergeți informațiile existente înainte de a le importa.
 - Puteți importa informații de cel mult 10.000 de persoane.
-

8.4.15 Importați imagini persoane

După importarea imaginilor feței pentru persoanele adăugate către client, persoanele din imagini pot fi identificate printr-un terminal de recunoaștere facială adăugat. Puteți fie să importați imaginile unei persoane una câte una, fie să importați mai multe imagini simultan, în funcție de nevoile dvs.

Înainte de a începe

Asigurați-vă că ați importat informații despre persoană către client în prealabil.

Pași

1. Intrați în modulul Persoană.

2. Selectați o organizație adăugată în listă sau faceți clic **Adăuga** în colțul din stânga sus pentru a adăuga o organizație și apoi selectați-o.

3. Clic **Import** pentru a deschide panoul Import și verificați **Față**.

4. **Opțional:** Permite **Verificați după dispozitiv** pentru a verifica dacă dispozitivul de recunoaștere a feței gestionat în client poate recunoaște fața din fotografie.

5. Faceți clic  pentru a selecta un fișier imagine a feței.

Nota

- (dosarul) imaginilor feței trebuie să fie în format ZIP.
 - Fiecare fișier imagine trebuie să fie în format JPG și nu trebuie să fie mai mare de 200 KB.
 - Fiecare fișier imagine trebuie denumit „Person ID_Name”. ID-ul persoanei ar trebui să fie același cu cel al informațiilor importate despre persoană.
-

6. Clic **Import** pentru a începe importul.

Progresul importului și rezultatul vor fi afișate.

8.4.16 Exportați informații despre persoană

Puteți exporta informațiile despre persoane adăugate pe computerul local ca fișier CSV.

Înainte de a începe

Asigurați-vă că ați adăugat persoane la o organizație.

Pași

1. Intrați în modulul Persoană.
2. **Opțional:** Selectați o organizație din listă.



Nota

Toate informațiile despre persoane vor fi exportate dacă nu selectați nicio organizație.

3. Clic **Export** pentru a deschide panoul Export și verificați **Informații despre persoană** ca conținut de exportat.
4. Verificați articolele dorite de exportat.
5. Clic **Export** pentru a salva fișierul CSV exportat pe computer.

8.4.17 Exportați imagini persoane

Puteți exporta fișierul cu imaginea feței persoanelor adăugate și puteți salva pe computer.

Înainte de a începe

Asigurați-vă că ați adăugat persoane și imaginile feței acestora la o organizație.

Pași

1. Intrați în modulul Persoană.
2. **Opțional:** Selectați o organizație din listă.



Nota

Imaginile feței tuturor persoanelor vor fi exportate dacă nu selectați nicio organizație.

3. Clic **Export** pentru a deschide panoul Export și verificați **Față** ca conținut de exportat.
4. Clic **Export** pentru a începe exportul.



Nota

- Fișierul exportat este în format ZIP.
 - Imaginea feței exportată este numită „Person ID_Name_0” („0” este pentru o față integrală).
-

8.4.18 Obțineți informații despre persoană 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 și informații despre cardul emis), puteți obține informațiile despre persoană de pe dispozitiv și le puteți importa în client pentru operațiuni ulterioare.

Pași

Nota

- Dacă numele persoanei stocate în dispozitiv este gol, numele persoanei va fi completat cu numărul cardului emis după importare către client.
 - Genul persoanelor va fi **Bărbat** implicit.
 - Dacă numărul cardului sau ID-ul persoanei (ID-ul angajatului) stocat pe dispozitiv există deja în baza de date a clienților, persoana cu acest număr de card sau ID-ul persoanei nu va fi importată în client.
-

1. Intră în Modul Persoană.

2. Selectați o organizație pentru a importa persoanele.

3. Clic Obțineți de pe dispozitiv.

4. Selectați dispozitivul de control al accesului din lista verticală.

5. Clic Obțineți pentru a începe importarea informațiilor despre persoană către client.

Informațiile despre persoană, inclusiv detaliile persoanei, informațiile despre amprenta persoanei (dacă sunt configurate) și cardurile conectate (dacă sunt configurate), vor fi importate în organizația selectată.

8.4.19 Mutați persoane într-o altă organizație

Dacă aveți nevoie, puteți muta persoanele adăugate într-o altă organizație.

Înainte de a începe

- Asigurați-vă că ați adăugat cel puțin două organizații.
- Asigurați-vă că ați importat informații despre persoană.

Pași

1. Intră în Modul Persoană.

2. Selectați o organizație în panoul din stânga.

Persoanele din cadrul organizației vor fi afișate în panoul din dreapta.

3. Selectați persoana de mutat.

4. Clic Schimbați organizația.

5. Selectați organizația în care să mutați persoanele.

6. Clic Bine.

8.4.20 Emite carduri persoanelor din lot

Clientul oferă o modalitate convenabilă de a emite carduri pentru mai multe persoane dintr-un lot.

Pași

1. Intră în Modul Persoană.

2. Clic Carduri de emisiune lot.

Se vor afișa toate persoanele adăugate fără card.

3. Setări parametrii de emisie a cardului. Pentru detalii, consultați *Setări parametrii de emisie a cardului*.

4. **Clic** **Inițializați** pentru a inițializa stația de înregistrare a cardurilor sau cititorul de carduri pentru a-l pregăti pentru emiterea cardurilor.

5. Faceți clic pe coloana cu numărul cardului și introduceți numărul cardului.

- Puneți cardul pe stația de înregistrare a cardului.
- Glisați cardul pe cititorul de carduri.
- Introduceți manual numărul cardului și apăsați **Intră** tasta de pe tastatură.

Numărul cardului va fi citit automat și cardul va fi eliberat persoanei din listă.

6. Repetați pasul de mai sus pentru a emite cardurile persoanelor din listă în ordine.

8.4.21 Pierderea buletinului de raportare

Dacă persoana și-a pierdut cardul, puteți raporta pierderea cardului, astfel încât autorizația de acces aferentă cardului să fie inactivă.

Pași

1. **Intră** **Persoană** modul.

2. Selectați persoana pentru care doriți să raportați pierderea cardului și faceți clic **Edita** pentru a deschide fereastra Editare persoană.

3. În **Credențială** → **Card** panoul, faceți clic pe cardul  adăugat pentru a seta acest card ca fiind pierdut.

După pierderea cardului de raportare, autorizația de acces a acestui card va fi invalidă și inactivă. O altă persoană care primește acest card nu poate accesa ușile glisând acest card pierdut.

4. **Opțional:** Dacă cardul pierdut este găsit, puteți face clic pe  a anula pierderea.

După anularea pierderii cardului, autorizația de acces a persoanei va fi valabilă și activă.

5. Dacă cardul pierdut este adăugat într-un grup de acces și grupul de acces este deja aplicat dispozitivului, după raportarea pierderii cardului sau anularea pierderii cardului, va apărea o fereastră pentru a vă anunța să aplicați modificările pe dispozitiv. După aplicarea pe dispozitiv, aceste modificări pot avea efect asupra dispozitivului.

8.4.22 Setări parametrilor de emiteră a cardului

Clientul oferă două moduri de citire a numărului unui card: prin stația de înregistrare a cardului sau prin cititorul de carduri al dispozitivului de control acces. Dacă este disponibilă o stație de înregistrare a cardului, conectați-o la computerul care rulează clientul prin interfața USB sau COM și plasați cardul pe cardul de înregistrare pentru a citi numărul cardului. Dacă nu, puteți, de asemenea, să glisați cardul pe cititorul de carduri al dispozitivului de control al accesului adăugat pentru a obține numărul cardului. Ca urmare, înainte de a emite un card unei persoane, trebuie să setați parametrilor de emiteră a cardului, inclusiv modul de emiteră și parametrilor aferenți.

Când adăugați un card unei persoane, faceți clic **Setări** pentru a deschide fereastra Setări de emiteră a cardului.

Mod local: Emite card de către stația de înregistrare card

Conectați o stație de înregistrare a cardului la computerul care rulează clientul. Puteți plasa cardul pe stația de înregistrare a cardului pentru a obține numărul cardului.

Stația de înregistrare a cardurilor

Selectați modelul stației de înregistrare a cardului conectat



Nota

În prezent, modelele de stații de înregistrare a cardurilor acceptate includ DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E și DS-K1F180-D8E.

Tip card

Acest câmp este disponibil numai când modelul este DS-K1F100-D8E sau DS-K1F180-D8E.

Selectați tipul cardului ca card EM sau card IC în funcție de tipul de card real. **Port serial**

Este disponibil numai când modelul este DS-K1F100-M. Selectați

COM la care se conectează stația de înregistrare a cardului. **Zumzet**

Activați sau dezactivați sunetul când numărul cardului este citit cu succes.

Tip card nr

Selectați tipul numărului de card în funcție de nevoile reale.

Criptare card M1

Acest câmp este disponibil numai când modelul este DS-K1F100-D8, DS-K1F100-D8E sau DS-K1F180-D8E.

Dacă cardul este un card M1 și dacă trebuie să activați funcția M1 Card Encryption, ar trebui să activați această funcție și să selectați sectorul cardului de criptat.

Mod de la distanță: Emite card cu cititorul de carduri

Selectați un dispozitiv de control al accesului adăugat în client și glisați cardul pe cititorul său de carduri pentru a citi numărul cardului.

8.5 Configurați programul și șablonul

Puteți configura șablonul, inclusiv programul de vacanță și săptămâna. După setarea șablonului, puteți adopta șablonul configurat pentru a accesa grupurile atunci când setați grupurile de acces, astfel încât grupul de acces să aibă efect în duratele de timp ale șablonului.



Nota

Pentru setările grupului de acces, consultați **Setați grupul de acces pentru a atribui autorizație de acces persoanelor**.

8.5.1 Adăugați vacanță

Puteți crea sărbători și puteți seta zilele din sărbători, inclusiv data de începere, data de încheiere și durata vacanței într-o singură zi.

Pași



Nota

Puteți adăuga până la 64 de sărbători în sistemul software.

1. Clic **Control acces** → **Program** → **Vacanță** pentru a intra pe pagina Sărbători.
 2. Clic **Adăuga** pe panoul din stânga.
 3. Creați un nume pentru vacanță.
 4. **Opțional:** Introduceți descrierile sau unele notificări ale acestei sărbători în caseta Observații.
 5. Adăugați o perioadă de vacanță la lista de vacanțe și configurați durata vacanței.
-



Nota

La o vacanță pot fi adăugate până la 16 perioade de vacanță.

- 1) Faceți clic **Adăuga** în câmpul Listă de vacanțe.
 - 2) Trageți cursorul pentru a desena durata de timp, ceea ce înseamnă că în acea durată de timp este activat grupul de acces configurat.
-



Nota

Până la 8 durate pot fi setate pentru o perioadă de vacanță.

- 3) **Opțional:** Efectuați următoarele operații pentru a edita duratele de timp.
 - Mutați cursorul la durata de timp și trageți durata de timp pe bara cronologică în poziția dorită când cursorul se întoarce în .
 - Faceți clic pe durata timpului și editați direct ora de începere/terminare în dialogul apărut.
 - Mutați cursorul la începutul sau la sfârșitul duratei de timp și trageți pentru a prelungi sau a scurta durata de timp când cursorul se întoarce în .
- 4) **Opțional:** Selectați durata de timp care trebuie ștearsă, apoi faceți clic pe  în coloana Operație pentru a șterge durata de timp selectată.
- 5) **Opțional:** Clic  în coloana Operație pentru a șterge toate duratele de timp din bara de timp.
- 6) **Opțional:** Clic  în coloana Operație pentru a șterge această perioadă de vacanță adăugată din lista de sarbatori.

6. Clic Salva.

8.5.2 Adăugați șablon

Șablonul include programul săptămânal și vacanța. Puteți seta programul săptămânal și alocă durata de timp a autorizației de acces pentru o persoană sau un grup diferit. De asemenea, puteți selecta vacanțele adăugate pentru șablon.

Pași



Nota

Puteți adăuga până la 255 de șabloane în sistemul software.

1. Clic Control acces → Program → Șablon pentru a intra în pagina Șablon.

 Nota

Există două șabloane implicite: Autorizat toată ziua și Refuzat toată ziua și nu pot fi editate sau șterse.

Autorizat toată ziua

Autorizația de acces este valabilă în fiecare zi a săptămânii și nu are sărbătoare. **Toată**

ziua refuzată

Autorizația de acces este invalidă în fiecare zi a săptămânii și nu are sărbătoare.

2. Clic Adăuga în panoul din stânga pentru a crea un șablon nou.

3. Creați un nume pentru șablon.

4. Introduceți descrierile sau unele notificări ale acestui șablon în caseta Observație.

5. Editați programul săptămânal pentru a-l aplica șablonului.

1) Faceți clic **Programul săptămânii** fila din panoul inferior.

2) Selectați o zi a săptămânii și trageți duratele de timp pe bara cronologică.

 Nota

Pot fi setate până la 8 durate de timp pentru fiecare zi din programul săptămânii.

3) Opțional: Efectuați următoarele operații pentru a edita duratele de timp.

- Mutați cursorul la durata de timp și trageți durata de timp pe bara cronologică în poziția dorită când cursorul se întoarce în .
- Faceți clic pe durata timpului și editați direct ora de începere/terminare în dialogul apărut.
- Mutați cursorul la începutul sau la sfârșitul duratei de timp și trageți pentru a prelungi sau a scurta durata de timp când cursorul se întoarce în .

4) Repetați cei doi pași de mai sus pentru a desena mai multe durate de timp în celelalte zile ale săptămânii.

6. Adăugați o vacanță pentru a o aplica șablonului.

 Nota

La un șablon pot fi adăugate până la 4 sărbători.

1) Faceți clic **Vacanță** fila.

2) Selectați o vacanță din lista din stânga și va fi adăugată la lista selectată din panoul din dreapta.

3) **Opțional:** Clic **Adăuga** pentru a adăuga o nouă vacanță.

 Nota

Pentru detalii despre adăugarea unei sărbători, consultați **Adăugați vacanță**.

4) **Opțional:** Selectați o vacanță selectată din lista din dreapta și faceți clic sau faceți  pentru a-l elimina pe cel selectat, clic **Clar** pentru a șterge toate vacanțele selectate din lista din dreapta.

7. Clic Salvă pentru a salva setările și pentru a finaliza adăugarea șablonului.

8.6 Setări grupul de acces pentru a atribui autorizație de acces persoanelor

După adăugarea persoanei și configurarea acreditărilor persoanei, puteți crea grupuri de acces pentru a defini care persoană(e) poate(e) să aibă acces la ce ușă(e) și apoi să aplicați grupul de acces la dispozitivul de control al accesului pentru a intra în vigoare.

Pași

Când setările grupului de acces sunt modificate, trebuie să aplicați din nou grupurile de acces la dispozitive pentru a intra în vigoare. Modificările grupului de acces includ modificări ale șablonului, setărilor grupului de acces, setările grupului de acces ale persoanei și detaliile persoanei asociate (inclusiv numărul cardului, amprenta digitală, imaginea feței, legătura dintre numărul cardului și amprenta digitală, legătura dintre numărul cardului și amprenta digitală, parola cardului, perioada de valabilitate a cardului etc.).

1.ClicControl acces → Autorizare → Grup de acces pentru a intra în interfața Grupului de acces.

2.ClicAdăugă pentru a deschide fereastra Adăugare.

3.ÎnNume câmp de text, creați un nume pentru grupul de acces după cum doriți.

4.Selectați un șablon pentru grupul de acces.



Nota

Ar trebui să configurați șablonul înainte de a accesa setările grupului. Consultați **Configurați programul și șablonul** pentru detalii.

5.În lista din stânga a câmpului Selectare persoană, selectați persoana(e) pentru a atribui autorizarea de acces.

6.În lista din stânga a câmpului Selectare punct de acces, selectați ușile, stațiile de ușă sau etajele pentru accesul persoanelor selectate.

7.ClicSalva.

Puteți vizualiza persoanele selectate și punctele de acces selectate în partea dreaptă a interfeței.

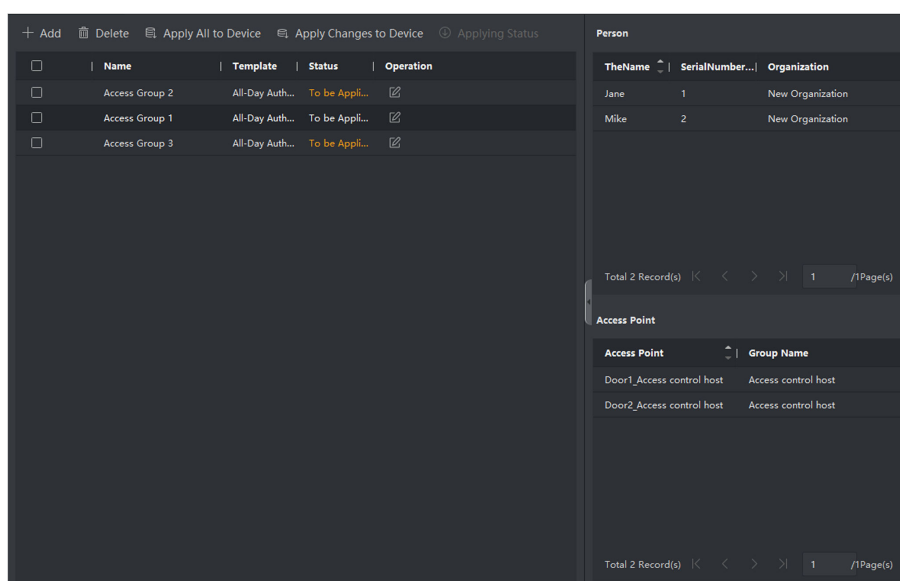


Figura 8-3 Afișează Persoana (Persoanele) și Punctele de Acces selectate

8. După adăugarea grupurilor de acces, trebuie să le aplicați dispozitivului de control al accesului pentru a intra în vigoare.

- 1) Selectați grupul (grupurile) de acces de aplicat dispozitivului de control al accesului.
- 2) Faceți clic **Aplicați totul la dispozitive** începeți să aplicați toate grupurile de acces selectate la dispozitivul de control al accesului sau la stația de acces.
- 3) Faceți clic **Aplicați totul la dispozitive** sau **Aplicați modificări la dispozitive**.

Aplicați totul la dispozitive

Această operațiune va șterge toate grupurile de acces existente ale dispozitivelor selectate și apoi va aplica noul grup de acces la dispozitiv.

Aplicați modificări la dispozitive

Această operațiune nu va șterge grupurile de acces existente ale dispozitivelor selectate și va aplica doar partea modificată a grupurilor de acces selectate dispozitivului (dispozitivelor).

- 4) Vizualizați starea aplicării în coloana Stare sau faceți clic **Starea de aplicare** pentru a vizualiza toate grupurile de acces aplicate.



Nota

Puteți verifica **Numai eșec de afișare** pentru a filtra rezultatele aplicării.

Persoanele selectate din grupurile de acces aplicate vor avea autorizația de a intra/ieși din ușile/stațiile de ușa selectate cu cardul(ele) sau amprentele lor conectate.

9. **Opțional:** Faceți clic pe  pentru a edita grupul de acces dacă este necesar.



Nota

Dacă modificați informațiile de acces ale persoanelor sau alte informații conexe, veți vedea solicitarea **Grup de acces care urmează să fie aplicat** în colțul din dreapta al clientului.

Puteți face clic pe solicitare pentru a aplica datele modificate pe dispozitiv. Puteți selecta oricare **Aplica acum** sau **Aplicați mai târziu**.

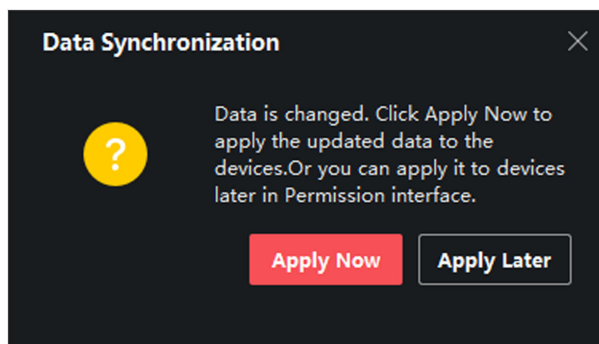


Figura 8-5 Sincronizarea datelor

8.7 Configurați funcții avansate

Puteți configura funcțiile avansate de control al accesului pentru a îndeplini anumite cerințe speciale în diferite scene.

Nota

- Pentru funcțiile legate de card (tipul cardului de control acces), numai cardul(ele) cu grupul de acces aplicat vor fi afișate atunci când adăugați carduri.
 - Funcțiile avansate ar trebui să fie acceptate de dispozitiv.
 - Plasați cursorul pe Funcția avansată, apoi Faceți clic pentru a personaliza funcția (funcțiile) avansate care urmează să fie afișate.
-

8.7.1 Configurarea parametrilor dispozitivului

După adăugarea dispozitivului de control acces, puteți configura parametrii dispozitivului de control acces, puncte de control acces.

Configurați parametrii pentru dispozitivul de control al accesului

După adăugarea dispozitivului de control acces, puteți configura parametrii acestuia.

Pași

1. Clic Control acces → Funcție avansată → Parametru dispozitiv.

Nota

Dacă nu găsiți Parametrul dispozitivului în lista Funcție avansată, plasați cursorul pe Funcția avansată, apoi faceți clic pentru a selecta parametrul dispozitivului care va fi afișat.

2. Selectați un dispozitiv de acces pentru a-și afișa parametrii pe pagina din dreapta.

3. Rotiți comutatorul în poziție ON pentru a activa funcțiile corespunzătoare.



Nota

- Parametrii afișați pot varia pentru diferite dispozitive de control al accesului.
 - Unii dintre următorii parametri nu sunt listați în pagina Informații de bază, faceți clic **Mai mult** pentru a edita parametrii.
-

Solicitare vocală

Dacă activați această funcție, promptul vocal este activat în dispozitiv. Puteți auzi solicitarea vocală când utilizați dispozitivul.

Încărcați poza. După capturarea legată

Încărcați automat imaginile capturate de camera conectată în sistem. **Salvați**

imaginea. După capturarea legată

Dacă activați această funcție, puteți salva pe dispozitiv fotografia capturată de camera conectată. **Modul de recunoaștere a feței**

Mod normal: recunoașteți fața prin intermediul camerei în mod normal.

Activați cardul NFC

Dacă activați funcția, dispozitivul poate recunoaște cardul NFC. Puteți prezenta cardul NFC pe dispozitiv.

Activați cardul M1

Dacă activați funcția, dispozitivul poate recunoaște cardul M1. Puteți prezenta cardul M1 pe dispozitiv.

Activați cardul EM

Dacă activați funcția, dispozitivul poate recunoaște cardul EM. Puteți prezenta cardul EM pe dispozitiv.

Activați cardul CPU

Dacă activați funcția, dispozitivul poate recunoaște placa CPU. Puteți prezenta cardul CPU pe dispozitiv.

Activați cartea de identitate

Dacă activați funcția, dispozitivul poate recunoaște cartea de identitate. Puteți prezenta cartea de identitate pe dispozitiv.

4. Clic Bine.

5. **Opțional:** Clic **Copiați în**, apoi selectați dispozitivul(ele) de control al accesului pentru a copia parametrii din pagină pe dispozitivul(ele) selectat(e).

Configurați parametrii pentru ușă

După adăugarea dispozitivului de control al accesului, puteți configura parametrii ușii punctului de acces al acestuia.

Pași

1.ClicControl acces → Funcție avansată → Parametru dispozitiv.

2. Selectați un dispozitiv de control al accesului în panoul din stânga, apoi faceți clic  pentru a afișa ușile dispozitivului selectat.

3. Selectați o ușă pentru a-și afișa parametrii pe pagina din dreapta.

4. Editați parametrii ușii.



Nota

- Parametrii afișați pot varia pentru diferite dispozitive de control al accesului.
- Unii dintre următorii parametri nu sunt listați în pagina Informații de bază, faceți clic **Mai mult** pentru a edita parametrii.

Nume

Editați numele cititorului de carduri după cum

doriți. **Contact la ușă**

Puteți seta senzorul ușii ca să rămână închis sau să rămână deschis. De obicei, acesta rămâne închis.

Tip buton de ieșire

Puteți seta butonul de ieșire ca să rămână închis sau să rămână deschis. De obicei, acesta rămâne deschis.

Ușa Încuiată Timp

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

Durată de deschidere extinsă

Contactul ușii poate fi activat cu o întârziere corespunzătoare după ce persoana cu acces extins are nevoie să-și gliseze cardul.

Alarmă de expirare ușă stângă deschisă

Alarma poate fi declanșată dacă ușa nu a fost închisă într-o perioadă de timp configurată. Dacă este setată la 0, nu va fi declanșată nicio alarmă.

Încuie ușa când ușa este închisă

Ușa poate fi încuiată odată ce este închisă, chiar dacă **Ușa Încuiată Timp** nu este atins. **Codul de constrângere**

Ușa se poate deschide prin introducerea codului de constrângere atunci când există constrângere. În același timp, clientul poate raporta evenimentul de constrângere.

Super Parolă

Persoana specifică poate deschide ușa introducând superparola.

Nota

- Codul de constrângere și codul super ar trebui să fie diferite.
 - Codul de constrângere și parola super ar trebui să fie diferite de parola de autentificare.
 - Lungimea codului de constrângere și a parolei super este în funcție de dispozitiv, de obicei ar trebui să conțină 4 până la 8 cifre.
-

5.ClicBine.

6. Opțional:ClicCopiați în,apoi selectați ușa/etajele pentru a copia parametrul din pagină în ușile/etajele selectate.

Nota

Setările privind durata stării ușii vor fi copiate și în ușile selectate.

Configurați parametrul pentru cititorul de carduri

După adăugarea dispozitivului de control al accesului, puteți configura parametrul cititorului de carduri.

Pași

1.ClicControl acces → Funcție avansată → Parametru dispozitiv.

2.În lista de dispozitive din stânga, faceți **clic** pentru a extinde ușa, selectați un cititor de carduri și puteți edita parametrul cititorului de carduri din dreapta.

3.Editați parametrul de bază al cititorului de carduri în pagina Informații de bază.

Nota

- Parametrii afișați pot varia pentru diferite dispozitive de control al accesului. Există o parte din parametri enumerați după cum urmează. Consultați manualul de utilizare al dispozitivului pentru mai multe detalii.
 - Unii dintre următorii parametri nu sunt listați în pagina Informații de bază, faceți clic**Mai mult**pentru a edita parametrul.
-

Nume

Editați numele cititorului de carduri după cum doriți.

OK Polaritate LED/Eroare Polaritate LED/Polaritate sonerie

Setați polaritatea LED-ului OK/polaritatea LED-ului de eroare/ Polaritatea LED-ului sonerie a plăcii principale în funcție de parametrul cititorului de carduri. În general, adoptă setările implicite.

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 PWD

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 apăsător înainte vor fi șterse automat.

Alarma de max. Încercări eșuate

Activați pentru raportarea alarmei atunci când încercările de citire a cardului ating valoarea

setată. **Max. Momente de eșec card**

Setați valoarea maximă. Încercări eșuate de citire a

cardului. **Detectare falsificare**

Activați detectarea anti-manipulare pentru cititorul de

carduri. **Comunicați cu Controller Every**

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.

Tip cititor card/Descriere card cititor

Obțineți tipul și descrierea cititorului de carduri. Sunt doar pentru citire.

Nivel de recunoaștere a amprentei

Selectați nivelul de recunoaștere a amprentei din lista derulantă. **Modul**

de autentificare implicit al cititorului de carduri

Vizualizați modul de autentificare implicit al cititorului de carduri.

Capacitate de amprentă

Vizualizați numărul maxim de amprente disponibile.

Numărul de amprentă existent

Vedeți numărul de amprente existente pe dispozitiv. **Nivel de**

recunoaștere a amprentei

Selectați nivelul de recunoaștere a amprentei din lista verticală. **Valoarea**

de expirare a recunoașterii feței

Dacă timpul de recunoaștere este mai mare decât timpul configurat, dispozitivul vă va reaminti.

Fața 1:N Pragul de potrivire

Setați pragul de potrivire atunci când vă autentificați prin modul de potrivire 1:N. Cu cât valoarea este mai mare, cu atât rata de acceptare falsă este mai mică și rata de respingere falsă mai mare la autentificare.

Interval de recunoaștere a feței

Intervalul de timp dintre două recunoașteri continue a feței la autentificare. **Detectarea**

feței în direct

Activați sau dezactivați funcția de detectare a feței în direct. Dacă activați funcția, dispozitivul poate recunoaște dacă persoana este în viață sau nu.

Pragul de potrivire 1:1

Setați pragul de potrivire atunci când vă autentificați prin modul de potrivire 1:1. Cu cât valoarea este mai mare, cu atât rata de acceptare falsă este mai mică și rata de respingere falsă mai mare la autentificare.

Modul de aplicare

Puteți selecta modurile de aplicare interioare sau altele în funcție de mediul real.

Blocare autentificare a eșuat față

După activarea funcției Live Face Detection, sistemul va bloca fața utilizatorului timp de 5 minute dacă detectarea live a feței nu reușește mai mult decât încercările configurate. Același utilizator nu se poate autentifica prin chipul fals în 5 minute. În cele 5 minute, utilizatorul se poate autentifica prin intermediul feței reale de două ori în mod continuu pentru a debloca.

Live Face Detection Nivel de securitate

După activarea funcției Live Face Detection, puteți seta nivelul de securitate potrivit atunci când efectuați autentificarea live a feței.

Max. Încercări eșuate de autentificare facială.

Setați numărul maxim de încercări eșuate de detectare a feței în direct. Sistemul va bloca fața utilizatorului timp de 5 minute dacă detectarea feței live nu reușește mai mult decât încercările configurate. Același utilizator nu se poate autentifica prin chipul fals în 5 minute. În cele 5 minute, utilizatorul se poate autentifica prin intermediul feței reale de două ori în mod continuu pentru a debloca.

4.ClicBine.

5. Opțional:ClicCopiați în, apoi selectați cititoarele de carduri pentru a copia parametrii din pagină în cititoarele de carduri selectate.

Configurați parametrii pentru ieșirea alarmei

După adăugarea dispozitivului de control acces, dacă dispozitivul se conectează la ieșirile de alarmă, puteți configura parametrii.

Pași

- 1.ClicControl acces → Funcție avansată → Parametru dispozitiv pentru a accesa pagina de configurare a parametrilor de control al accesului.
- 2.În lista de dispozitive din stânga, faceți clic pentru a extinde ușa, selectați o intrare de alarmă și puteți edita parametrii intrării de alarmă din dreapta.
- 3.Setați parametrii de ieșire a alarmei.

Nume

Editați numele cititorului de carduri după cum doriți. **Timp activ ieșire alarmă**

Cât timp va dura ieșirea alarmei după declanșare.

4.ClicBine.

5. Opțional:Setați comutatorul din colțul din dreapta sus laPE pentru a declanșa ieșirea de alarmă.

8.7.2 Configurare rămas deschis/închis

Puteți seta starea ușii ca deschisă sau închisă. De exemplu, puteți seta ușa să rămână închisă în vacanță și puteți seta ușa să rămână deschisă în perioada specificată a zilei de lucru.

Înainte de a începe

Adăugați dispozitivele de control acces la sistem.

Pași

1. Clic **Control acces** → **Funcție avansată** → **Rămâne deschis/închis** pentru a intra în pagina Rămâne deschis/închis.
2. Selectați ușa care trebuie configurată pe panoul din stânga.
3. Pentru a seta starea ușii în timpul zilei de lucru, faceți clic pe **Programul săptămânii** și efectuați următoarele operații.

- 1) Faceți clic **Rămâi deschis** sau **Rămâi închis**.
- 2) Trageți cursorul pentru a desena durata de timp, ceea ce înseamnă că în acea durată de timp este activat grupul de acces configurat.



Nota

Pentru fiecare zi din programul săptămânal pot fi setate până la 8 durate de timp.

- 3) **Opțional:** Efectuați următoarele operații pentru a edita duratele de timp.

- Mutați cursorul la durata de timp și trageți durata de timp pe bara cronologică în poziția dorită când cursorul se întoarce în .
- Faceți clic pe durata timpului și editați direct ora de începere/terminare în dialogul apărut.
- Mutați cursorul la începutul sau la sfârșitul duratei de timp și trageți pentru a prelungi sau a scurta durata de timp când cursorul se întoarce în .

- 4) Faceți clic **Salva**.

Operațiuni conexe

Copiați în întreg

săptămână

Selectați o durată pe bara de timp, faceți clic **Copiați în săptămâna întreagă** pentru a copia toate setările de durată din această bară de timp în alte zile ale săptămânii.

Ștergeți selectat

Selectați o durată pe bara de timp, faceți clic **Ștergeți selectat** pentru a șterge această durată.

Clar

Clic **Clar** pentru a șterge toate setările de durată din programul săptămânal.

4. Pentru a seta starea ușii în timpul vacanței, faceți clic pe **Vacanță** și efectuați următoarele operații.

- 1) Faceți clic **Rămâi deschis** sau **Rămâi închis**.
- 2) Faceți clic **Adăuga**.
- 3) Introduceți data de început și data de încheiere.
- 4) Trageți cursorul pentru a desena durata de timp, ceea ce înseamnă că în acea durată de timp este activat grupul de acces configurat.

Nota

Până la 8 durate pot fi setate pentru o perioadă de vacanță.

5) Efectuați următoarele operații pentru a edita duratele de timp.

- Mutați cursorul la durata de timp și trageți durata de timp pe bara cronologică în poziția dorită când cursorul se întoarce în .
- Faceți clic pe durata timpului și editați direct ora de începere/terminare în dialogul apărut.
- Mutați cursorul la începutul sau la sfârșitul duratei de timp și trageți pentru a prelungi sau a scurta durata de timp când cursorul se întoarce în .

6) **Opțional:** Selectați durata de timp care trebuie ștearsă, apoi faceți clic pe  în coloana Operație pentru a șterge durata de timp selectată.

7) **Opțional:** Clic  în coloana Operație pentru a șterge toate duratele de timp din bara de timp.

8) **Opțional:** Clic  în coloana Operațiune pentru a șterge această perioadă de vacanță adăugată din lista de sarbatori.

9) Faceți clic **Salva**.

5. Opțional: Clic **Copiați în** pentru a copia setările de stare a ușii acestei uși către alte uși.

8.7.3 Configurați autentificarea cu mai mulți factori

Puteți gestiona persoanele în funcție de grup și puteți seta autentificarea pentru mai multe persoane dintr-un punct de control acces (ușă).

Înainte de a începe

Setați grupul de acces și aplicați grupul de acces la dispozitivul de control al accesului. Pentru detalii, consultați **Setați grupul de acces pentru a atribui autorizație de acces persoanelor**.

Efectuați această sarcină atunci când doriți să setați autentificări pentru mai multe carduri ale unui punct de control acces (ușă).

Pași

1. Clic Control acces → Funcție avansată → Autentificare multifactor.

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

3. Adăugați o persoană/grup de carduri pentru dispozitivul de control al accesului.

- 1) Faceți clic **Adăuga** pe panoul din dreapta.
- 2) Creați un nume pentru grup după cum doriți.
- 3) Specificați ora de începere și ora de încheiere a perioadei efective pentru persoana/grupul de carduri.
- 4) Selectați membrii și cardurile din lista Disponibil, iar membrii și cardurile selectate vor fi adăugate la lista Selectate.

Nota

Asigurați-vă că aveți un card de emisiune pentru persoana respectivă.

Asigurați-vă că ați setat grupul de acces și aplicați cu succes grupul de acces la dispozitivul de control al accesului.

5) Faceți clic **Salva**.

6) **Opțional:** Selectați persoana/grupurile de carduri, apoi faceți clic **Ștergea-l** șterge (le).

- 7) **Opțional:** Selectați persoana/grupurile de carduri, apoi faceți clic **Aplicați** pentru a reaplica un grup de acces care nu a putut fi aplicat anterior dispozitivului de control al accesului.
4. Selectați un punct de control al accesului (ușa) al dispozitivului selectat pe panoul din stânga.
5. Introduceți intervalul maxim când introduceți parola.
6. Adăugați un grup de autentificare pentru punctul de control acces selectat.
- 1) Faceți clic **Adăuga** în panoul Grupuri de autentificare.
 - 2) Selectați un șablon configurat ca șablon de autentificare din lista derulantă.

Nota

Pentru setarea șablonului, consultați **Configurați programul și șablonul**.

- 3) Selectați tipul de autentificare ca **Autentificare locală**, **Autentificare locală și ușă deschisă de la distanță**, sau **Autentificare locală și Super Parolă** din lista derulantă.

Autentificare locală

Autentificare prin dispozitivul de control acces.

Autentificare locală și ușă deschisă de la distanță

Autentificare de către dispozitivul de control acces și de către client. Când persoana trece cardul pe dispozitiv, va apărea o fereastră. Poți deschide ușa prin intermediul clientului.

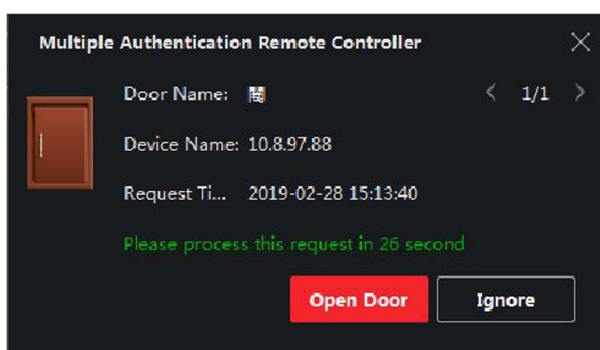


Figura 8-6 Ușă deschisă de la distanță

Nota

Puteți verifica **Autentificare offline** pentru a activa autentificarea superparolă atunci când dispozitivul de control al accesului este deconectat de client.

Autentificare locală și Super Parolă

Autentificare prin dispozitivul de control acces și prin super parolă.

- 4) Selectați persoana/grupul de carduri adăugate în lista din stânga de mai jos și va fi adăugată în lista Selectate din dreapta ca grup de autentificare.
- 5) Faceți clic pe grupul de autentificare adăugat din lista din dreapta pentru a seta timpii de autentificare în coloana Auth Times.

Nota

- Timpul de autentificare ar trebui să fie mai mari decât 0 și mai mici decât cantitatea de personal adăugată în grupul de personal.
- Valoarea maximă a timpilor de autentificare este 16.

6) Faceți clic **Salva**.

Nota

- Pentru fiecare punct de control acces (ușă), pot fi adăugate până la patru grupuri de autentificare.
- Pentru grupul de autentificare al cărui tip de autentificare este **Autentificare locală**, la grupul de autentificare pot fi adăugate până la 8 persoane/grupuri de carduri.
- Pentru grupul de autentificare al cărui tip de autentificare este **Autentificare locală și Super Parolă** sau **Autentificare locală și ușă deschisă de la distanță**, la grupul de autentificare pot fi adăugate până la 7 persoane/grupuri de carduri.

7. Clic **Salva**.

8.7.4 Configurați modul și programarea de autentificare a cititorului de carduri

Puteți seta regulile de trecere pentru cititorul de carduri al dispozitivului de control acces în funcție de nevoile dvs. reale.

Pași

1. Clic **Control acces** → **Funcție avansată** → **Autentificare** pentru a intra în pagina de configurare a modului de autentificare.
2. Selectați un cititor de carduri din stânga pentru a configura.
3. Setări modul de autentificare a cititorului de carduri.
 - 1) Faceți clic **Configurare**.

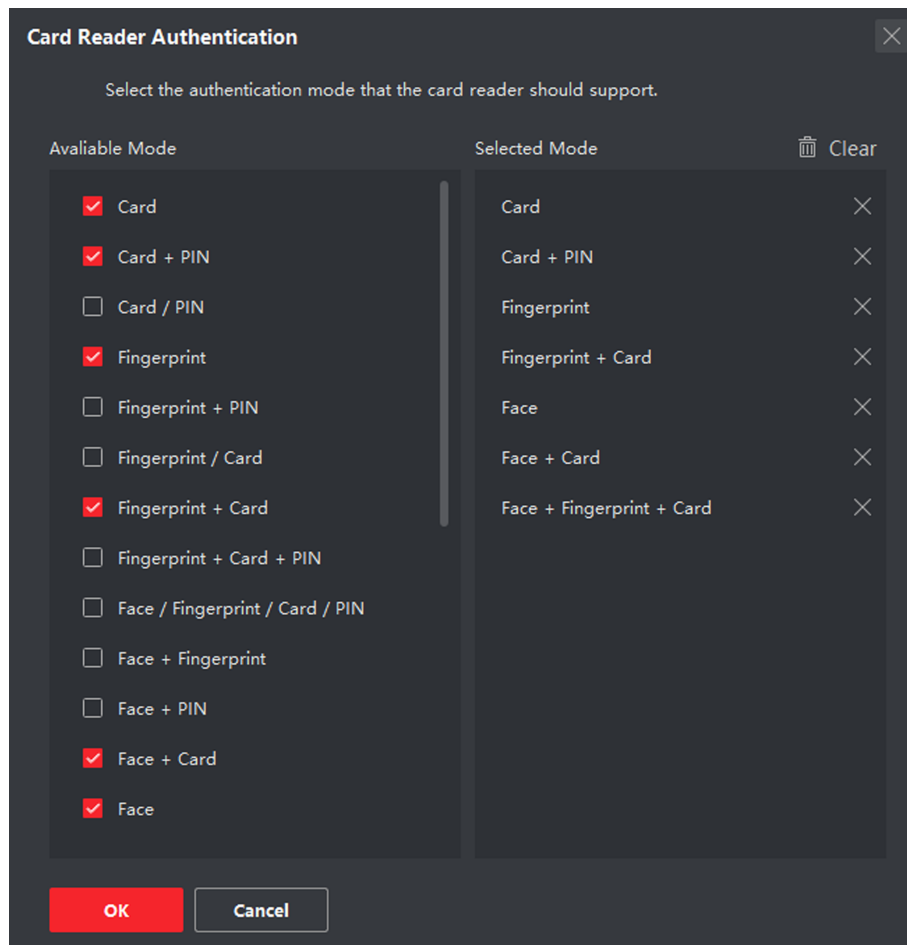


Figura 8-7 Selectați modul de autentificare a cititorului de carduri

Nota

PIN se referă la codul PIN setat pentru a deschide ușa. Consultați **Configurați informațiile de control al accesului**.

2) Verificați modurile din lista Moduri disponibile și acestea vor fi adăugate la lista modurilor selectate.

3) Faceți clic **Bine**.

După selectarea modurilor, modurile selectate se vor afișa ca pictograme cu culori diferite.

4. Faceți clic pe pictogramă pentru a selecta un mod de autentificare a cititorului de carduri și trageți cursorul pentru a desena o bară de culoare pe program, ceea ce înseamnă că în acea perioadă de timp, autentificarea cititorului de carduri este valabilă.

5. Repetați pasul de mai sus pentru a seta alte perioade de timp.

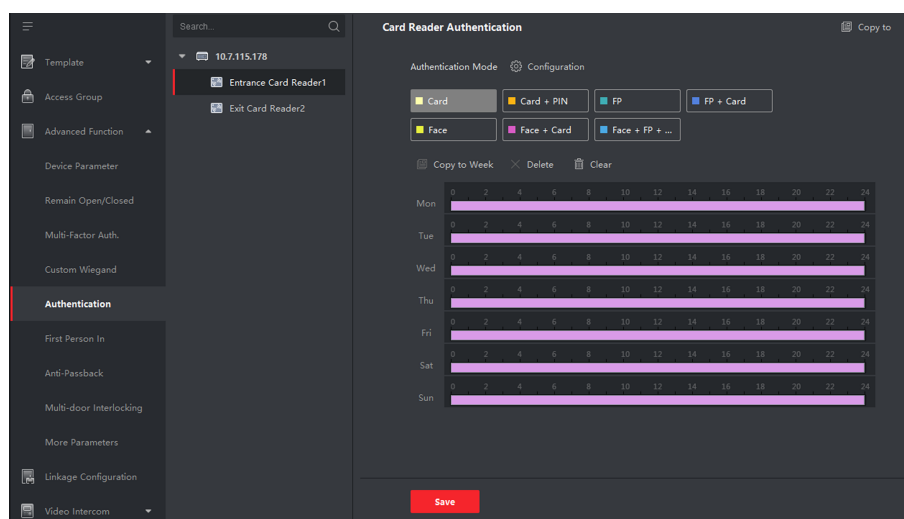


Figura 8-8 Setarea modurilor de autentificare pentru cititoarele de carduri

6. Opțional: Selectați o zi configurată și faceți clic **Copiați în Săptămână** pentru a copia aceleași setări în întreaga săptămână.

7. Opțional: Clic **Copiați în** pentru a copia setările în alte cititoare de carduri.

8. Clic Salva.

8.7.5 Configurați prima persoană în

Puteți seta mai multe prime persoane pentru un punct de control al accesului. După ce prima persoană este autorizată, permite accesul mai multor persoane la ușă sau alte acțiuni de autentificare.

Înainte de a începe

Setați grupul de acces și aplicați grupul de acces dispozitivului de control acces. Pentru detalii, consultați **Setați grupul de acces pentru a atribui autorizație de acces persoanelor**.

Efectuați această sarcină atunci când doriți să configurați deschiderea ușii cu prima persoană.

Pași

1. Clic Control acces → Funcție avansată → Prima persoană în pentru a intra în pagina Persoana întâi.

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

3. Selectați modul curent ca **Activați Rămânerea deschisă după persoana întâi sau **Dezactivați Rămânerea deschisă după persoana întâi** din lista derulantă pentru fiecare punct de control al accesului al dispozitivului selectat.**

Activați Rămânerea deschisă după persoana întâi

Ușa rămâne deschisă pentru durata de timp configurată după ce prima persoană este autorizată până când se încheie durata de rămânere deschisă. Dacă selectați acest mod, ar trebui să setați durata de a rămâne deschisă.

Nota

Durata rămasă deschisă ar trebui să fie între 0 și 1440 de minute. În mod implicit, durata rămâne deschisă este de 10 minute.

Dezactivați Rămânerea deschisă după persoana întâi

Dezactivați funcția de prima persoană în, și anume autentificarea normală.

Nota

Vă puteți autentifica din nou de către prima persoană pentru a dezactiva modul prima persoană.

4.ClicAdăugape panoul Lista Persoanei întâi.

5.Selectați persoana (persoanele) din lista din stânga și persoana (persoanele) vor fi adăugate la persoanele selectate ca prima persoană (persoane) a ușilor.

Prima persoană adăugată (primele persoane) va fi listată în Lista de prima persoană

6. Opțional: Selectați prima persoană din listă și faceți clic**Șterge** pentru a elimina persoana din lista primei persoane.

7.ClicSalva.

8.7.6 Configurați Anti-Passback

Puteți seta să treacă numai punctul de control al accesului conform căii specificate și doar o persoană ar putea trece de punctul de control al accesului după ce glisați cardul.

Înainte de a începe

Activați funcția anti-retrie a dispozitivului de control acces.

Efectuați această sarcină atunci când doriți să configurați anti-retrimiteră pentru dispozitivul de control al accesului.

Pași

Nota

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. Pentru configurarea interblocării cu mai multe uși, consultați .

1.ClicControl acces → Funcție avansată → Anti-Passback pentru a intra în pagina Setări Anti-Passpack.

2. Selectați un dispozitiv de control al accesului pe panoul din stânga.

3. Selectați un cititor de carduri ca început al căii în **Primul cititor de carduri** din meniul.

4. Faceți clic pe primul cititor de carduri selectat în **Cititor de carduri După aceea** pentru a deschide dialogul de selectare a cititorului de carduri.

5. Selectați apoi cititoarele de carduri pentru primul cititor de carduri.

Nota

Până la patru cititoare de carduri pot fi adăugate ulterior ca cititoare de carduri pentru un cititor de carduri.

6.ClicBineîn caseta de dialog pentru a salva selecțiile.

7.ClicSalvaîn pagina Setări Anti-Passback pentru a salva setările și a intra în vigoare.

Exemplu

Setați calea de glisare a cardului

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.

8.7.7 Configurarea parametrilor dispozitivului

După adăugarea dispozitivului de control al accesului, puteți seta parametrii acestuia, cum ar fi parametrii de rețea.

Setați mai mulți parametri NIC

Dacă dispozitivul acceptă mai multe interfețe de rețea, puteți seta parametrii de rețea ai acestor NIC prin intermediul clientului, cum ar fi adresa IP, adresa MAC, numărul portului etc.

Pași



Nota

Această funcție ar trebui să fie acceptată de dispozitiv.

1.Intrați în modulul de control acces.

2.În bara de navigare din stânga, introduceți**Funcție avansată → Mai mulți parametri**.

3.Selectați un dispozitiv de control al accesului din lista de dispozitive și faceți clic**NIC**pentru a intra pe pagina Setări NIC multiple.

4.Selectați o NIC pe care doriți să o configurați din lista derulantă.

5.Setați parametrii rețelei, cum ar fi adresa IP, gateway-ul implicit, masca de subrețea etc.

Adresa MAC

O adresă de control al accesului media (adresă MAC) este un identificator unic atribuit interfeței de rețea pentru comunicații pe segmentul fizic al rețelei.

MTU

Unitatea de transmisie maximă (MTU) a interfeței de rețea.

6.ClicSalva.

Setați parametrii de rețea

După adăugarea dispozitivului de control al accesului, puteți seta modul de încărcare a jurnalului dispozitivului și puteți crea un cont EHome prin intermediul rețelei prin cablu.

Setați modul de încărcare a jurnalului

Puteți seta modul pentru ca dispozitivul să încarce jurnale prin protocolul EHome.

Pași



Nota

Asigurați-vă că dispozitivul nu este adăugat de EHome.

1. Intrați în modulul de control acces.
2. În bara de navigare din stânga, introduceți **Funcție avansată** → **Mai mulți parametri**.
3. Selectați un dispozitiv de control al accesului din lista de dispozitive și intrați **Rețea** → **Mod de încărcare**.
4. Selectați grupul central din lista verticală.
5. Verificați **Permite** pentru a permite setarea modului de încărcare.
6. Selectați modul de încărcare din lista verticală.
 - Permite **N1** sau **G1** pentru canalul principal și canalul de rezervă.
 - Selectați **Aproape** pentru a dezactiva canalul principal sau canalul de rezervă



Nota

Canalul principal și canalul de rezervă nu pot activa N1 sau G1 în același timp.

7. Clic **Salva**.

Creați un cont EHome în modul de comunicare prin cablu

Puteți seta contul pentru protocolul EHome în modul de comunicare prin cablu. Apoi puteți adăuga dispozitive prin protocolul EHome.

Pași



Nota

- Această funcție ar trebui să fie acceptată de dispozitiv.
- Asigurați-vă că dispozitivul nu este adăugat de EHome.

1. Intrați în modulul de control acces.
2. În bara de navigare din stânga, introduceți **Funcție avansată** → **Mai mulți parametri**.
3. Selectați un dispozitiv de control al accesului din lista de dispozitive și intrați **Rețea** → **Centru de rețea**.
4. Selectați grupul central din lista verticală.
5. Selectați **Tip de adresă** ca **Adresa IP** sau **Nume de domeniu**.
6. Introduceți adresa IP sau numele domeniului în funcție de tipul adresei.
7. Introduceți numărul portului pentru protocol.

Nota

Numărul portului rețelei fără fir și al rețelei cu fir ar trebui să fie în concordanță cu numărul portului EHome.

8. Selectați Tipul protocolului EHome.

9. Setați un nume de cont pentru centrul de rețea.

10. Clic Salva.

Setați parametrii de capturare a dispozitivului

Puteți configura parametrii de capturare ai dispozitivului de control al accesului, inclusiv capturarea manuală și capturarea declanșată de evenimente.

Nota

- Funcția de captură ar trebui să fie acceptată de dispozitiv.
 - Înainte de a seta parametrii de captură, ar trebui să setați mai întâi stocarea imaginilor pentru a defini unde sunt salvate imaginile declanșate de eveniment. Pentru detalii, consultați *Setați stocarea imaginilor* în manualul de utilizare al software-ului client. .
-

Setați parametrii de captură declanșați

Când are loc un eveniment, camera dispozitivului de control al accesului poate fi declanșată pentru a captura imagini pentru a înregistra ce se întâmplă atunci când are loc evenimentul. Puteți vizualiza imaginile capturate când verificați detaliile evenimentului în Centrul de evenimente. Înainte de aceasta, trebuie să setați parametrii pentru captură, cum ar fi numărul de imagini capturate pentru o singură dată.

Înainte de a începe

Înainte de a seta parametrii de captură, ar trebui să setați mai întâi stocarea imaginilor pentru a defini unde sunt salvate imaginile capturate. Pentru detalii, consultați *Setați stocarea imaginilor* în manualul de utilizare al software-ului client.

Pași

Nota

Această funcție ar trebui să fie acceptată de dispozitiv

1. Intrați în modulul de control acces.
2. În bara de navigare din stânga, introduceți **Funcție avansată** → **Mai mulți parametri** → **Captură**.
3. Selectați un dispozitiv de control al accesului din lista de dispozitive și selectați **Captură conectată**.
4. Setați dimensiunea și calitatea imaginii.
5. Setați timpii de captură odată declanșați, ceea ce definește câte imagini vor fi capturate pentru o singură dată.
6. Dacă timpul de captură este mai mare de 1, setați intervalul pentru fiecare captură.

7.ClicSalva.

Setați parametrii de captură manuală

În modulul de monitorizare a stării, puteți face o imagine manual cu camera dispozitivului de control al accesului făcând clic pe un buton. Înainte de aceasta, trebuie să setați parametrii pentru captură, cum ar fi calitatea imaginii.

Înainte de a începe

Înainte de a seta parametrii de captură, ar trebui să setați mai întâi calea de salvare pentru a defini unde sunt salvate imaginile capturate. Pentru detalii, consultați *Setați stocarea imaginilor* în manualul de utilizare al software-ului client.

Pași



Nota

Această funcție ar trebui să fie acceptată de dispozitiv

- 1.Intrați în modulul de control acces.
- 2.În bara de navigare din stânga, introduceți **Funcție avansată** → **Mai mulți parametri** → **Captură**.
- 3.Selectați un dispozitiv de control al accesului din lista de dispozitive și selectați **Captură manuală**.
- 4.Selectați rezoluția imaginilor capturate din lista verticală.
- 5.Selectați calitatea imaginii ca **Ridicat**, **Mediu**, sau **Scăzut**. Cu cât calitatea imaginii este mai mare, cu atât imaginea va avea dimensiunea mai mare.
- 6.ClicSalva.

Setați parametrii pentru terminalul de recunoaștere a feței

Pentru terminalul de recunoaștere a feței, puteți seta parametrii acestuia, inclusiv baza de date a imaginilor feței etc.

Pași



Nota

Această funcție ar trebui să fie acceptată de dispozitiv.

- 1.Intrați în modulul de control acces.
- 2.În bara de navigare din stânga, introduceți **Funcție avansată** → **Mai mulți parametri**.
- 3.Selectați un dispozitiv de control al accesului din lista de dispozitive și faceți clic **Terminal de recunoaștere a feței**.
- 4.Setați parametrii.



Nota

Acești parametri afișați variază în funcție de diferitele modele de dispozitiv.

Algoritm

Selectați **Învățare profundă** ca baza de date a imaginilor feței.

Salvați imaginea feței de autentificare

Dacă este activată, imaginea feței capturată la autentificare va fi salvată pe dispozitiv.

Modul ECO

După activarea modului ECO, dispozitivul poate autentifica fețele în condiții de lumină scăzută sau întuneric. Și puteți seta pragul modului ECO, modul ECO (1:N) și modul ECO (1:1).

Mod ECO (1:1)

Setați pragul de potrivire atunci când vă autentificați prin modul ECO, modul de potrivire 1:1. Cu cât valoarea este mai mare, cu atât rata de acceptare falsă este mai mică și rata de respingere falsă este mai mare.

Mod ECO (1:N)

Setați pragul de potrivire atunci când vă autentificați prin modul ECO 1:N. Cu cât valoarea este mai mare, cu atât rata de acceptare falsă este mai mică și rata de respingere falsă este mai mare.

Pragul modului ECO

Când activați modul ECO, puteți seta pragul modului ECO. Cu cât valoarea este mai mare, cu atât dispozitivul intră mai ușor în modul ECO. Interval disponibil: de la 0 la 8.

Modul de lucru

Setați modul de lucru al dispozitivului ca Mod control acces. Modul de control al accesului este modul normal al dispozitivului. Ar trebui să vă autentificați acreditările pentru accesare.

5.ClicSalva.

Activați criptarea cardului M1

Criptarea cardului M1 poate îmbunătăți nivelul de securitate al autentificării.

Pași



Nota

Funcția ar trebui să fie suportată de dispozitivul de control al accesului și de cititorul de carduri.

- 1.Intrați în modulul de control acces.
 - 2.În bara de navigare din stânga, introduceți**Funcție avansată → Mai mulți parametri**.
 - 3.Selectați un dispozitiv de control al accesului din lista de dispozitive și faceți clic**Criptare card M1**pentru a intra pe pagina M1 Card Encryption.
 - 4.Setați comutatorul pe pornit pentru a activa funcția de criptare a cardului M1.
 - 5.Setați ID-ul sectorului.
-



Nota

- ID-ul sectorului variază de la 1 la 100.
 - În mod implicit, Sectorul 13 este criptat. Se recomandă criptarea sectorului 13.
-

6.ClicSalvapentru a salva setările.

Setați parametrii RS-485

Puteți seta parametrii RS-485 ai dispozitivului de control acces, inclusiv rata de transmisie, bitul de date, bitul de oprire, tipul de paritate, tipul de control al fluxului, modul de comunicare, modul de lucru și modul de conectare.

Pași



Nota

Setările RS-485 ar trebui să fie acceptate de dispozitiv.

1. Intrați în modulul de control acces.
 2. În bara de navigare din stânga, introduceți **Funcție avansată → Mai mulți parametri**.
 3. Selectați un dispozitiv de control al accesului din lista de dispozitive și faceți clic **RS-485** pentru a intra pe pagina Setări RS-485.
 4. Selectați numărul portului serial din lista verticală pentru a seta parametrii RS-485.
 5. Setați rata de transmisie, bitul de date, bitul de oprire, tipul de paritate, modul de comunicare, modul de lucru și modul de conectare în lista derulantă.
-



Nota

Când modul de conectare este **Conectați dispozitivul de control al accesului**, puteți selecta **Card Nr.** sau **ID persoana** ca tip de ieșire.

6. Clic Salva.

- Parametrii configurați vor fi aplicați automat dispozitivului.
- Când schimbați modul de lucru sau modul de conectare, dispozitivul se va reporni automat.

Setați parametrii Wiegand

Puteți seta canalul Wiegand al dispozitivului de control al accesului și modul de comunicare. După setarea parametrilor Wiegand, dispozitivul se poate conecta la cititorul de carduri Wiegand prin comunicare Wiegand.

Pași



Nota

Această funcție ar trebui să fie acceptată de dispozitiv.

1. Intrați în modulul de control acces.
2. În bara de navigare din stânga, introduceți **Funcție avansată → Mai mulți parametri**.
3. Selectați un dispozitiv de control al accesului din lista de dispozitive și faceți clic **Wiegand** pentru a intra pe pagina Setări Wiegand.
4. Setați comutatorul pe pornit pentru a activa funcția Wiegand pentru dispozitiv.
5. Selectați numărul canalului Wiegand și modul de comunicare din lista verticală.



Nota

Dacă setați **Direcția de comunicare** ca **Trimiterea**, vi se cere să setați **Modul Wiegand** ca **Wiegand 26** sau **Wiegand 34**.

6. Verificați Activarea Wiegand pentru a activa funcția Wiegand.

7. Clic Salva.

- Parametrii configurați vor fi aplicați automat dispozitivului.
- După schimbarea direcției de comunicare, dispozitivul se va reporni automat.

8.8 Configurarea acțiunilor de conectare pentru controlul accesului

Puteți configura diferite acțiuni de conectare pentru evenimentul detectat de dispozitivul de control al accesului. După aceea, acțiunile de conectare vor fi declanșate odată ce evenimentul are loc. Acest mecanism este utilizat pentru notificarea personalului de securitate asupra evenimentului sau declanșarea controlului automat al accesului în timp real.

Sunt acceptate două tipuri de acțiuni de legătură:

- **Acțiuni ale clienților:** Când evenimentul este detectat, acesta va declanșa acțiunile asupra clientului, cum ar fi clientul care face un avertisment sonor.
- **Acțiuni ale dispozitivului:** Când evenimentul este detectat, acesta va declanșa acțiunile unui anumit dispozitiv, cum ar fi bătăitul unui cititor de carduri și, deschiderea/închiderea unei uși, ..

8.8.1 Configurați acțiunile clientului pentru evenimentul de acces

Chiar dacă sunteți departe de un punct de acces, puteți ști totuși ce se întâmplă și cât de urgent este evenimentul prin configurarea acțiunilor legate de evenimentul de acces pe client. Veți fi notificat pe client odată ce un eveniment este declanșat, astfel încât să puteți răspunde instantaneu la eveniment. De asemenea, puteți configura acțiunile client ale punctelor de acces într-un lot la un moment dat.

Pași



Nota

Acțiunile de conectare de aici se referă la conectarea acțiunilor proprii ale software-ului client, cum ar fi avertismentul sonor, legătura de e-mail etc.

1. Clic Gestionare evenimente → Eveniment de control acces.

Dispozitivele de control al accesului adăugate se vor afișa în lista de dispozitive.

2. Selectați o resursă (inclusiv dispozitiv, intrare de alarmă, ușă/lift și cititor de carduri) din lista de dispozitive.

Tipurile de evenimente pe care le suportă resursa selectată se vor afișa.

3. Selectați evenimentul (evenimentele) și faceți clic Editare prioritate pentru a defini prioritatea pentru eveniment(e), care poate fi folosită pentru a filtra evenimentele din Centrul de evenimente.

4. Setati acțiunile de conectare ale evenimentului.

1) Selectați evenimentul (evenimentele) și faceți clic **Editați legătura** pentru a seta acțiunile clientului la declanșarea evenimentelor.

Avertizare sonoră

Software-ul client emite un avertisment sonor atunci când alarma este declanșată. Puteți selecta sunetul alarmei pentru avertizare sonoră.



Nota

Pentru setarea sunetului alarmei, consultați *Setați sunetul alarmei* în manualul de utilizare al software-ului client..

Trimite e-mail

Trimiteți o notificare prin e-mail cu informațiile de alarmă către unul sau mai mulți receptori.

Pentru detalii despre setarea parametrilor de e-mail, consultați *Setați parametrii de e-mail* în manualul de utilizare al software-ului client..

2) Faceți clic **Bine**.

5. Activați evenimentul astfel încât, atunci când evenimentul este detectat, evenimentul va fi trimis clientului și acțiunile de conectare să fie declanșate.

6. Opțional: Clic **Copiați în...** pentru a copia setările evenimentului pe alt dispozitiv de control al accesului, intrare de alarmă, ușă sau cititor de carduri.

8.8.2 Configurați acțiunile dispozitivului pentru evenimentul de acces

Puteți seta acțiunile de conectare ale dispozitivului de control al accesului pentru evenimentul declanșat al dispozitivului de control al accesului. După aceea, atunci când este declanșat un eveniment, acesta poate declanșa ieșirea de alarmă, soneria pe controlerul de acces și alte acțiuni.

Pași



Nota

Acțiunile de conectare ar trebui să fie suportate de dispozitiv.

1. Clic **Control acces → Configurare legături**.

2. Selectați dispozitivul de control al accesului din lista din stânga.

3. Clic **Adăugă** pentru a adăuga o nouă legătură.

4. Selecta **Legătura evenimentului** ca sursă de eveniment.

5. selectați tipul de eveniment și evenimentul detaliat pentru a seta legătura.

6. În zona țintă de legătură, setați ținta proprietății pentru a activa această acțiune.

Buzzer pe controler

Avertismentul sonor al dispozitivului de control al accesului va fi declanșat.

Capta

O fotografie legată de eveniment va fi capturată atunci când are loc evenimentul selectat.

Înregistrare

O fotografie legată de eveniment va fi capturată atunci când are loc evenimentul selectat.

Nota

Dispozitivul ar trebui să accepte înregistrarea.

Buzzer pe Reader

Avertismentul sonor al cititorului de carduri va fi declanșat.

Ieșire de alarmă

Ieșirea de alarmă va fi declanșată pentru notificare atunci când are loc evenimentul selectat

Intrare alarmă

Armați sau dezarmați intrarea alarmei.

Nota

Dispozitivul ar trebui să accepte funcția de intrare de alarmă.

Punct de acces

Se va declanșa starea ușii deschisă, închisă, rămâne deschisă sau rămâne închisă.

Nota

Ușa țintă și ușa sursă nu pot fi aceeași.

Redare audio

Promptul audio va fi declanșat. Și conținutul audio legat de indexul audio selectat va fi redat conform modului de redare configurat.

7.ClicSalva.

8. Opțional:După adăugarea conexiunii dispozitivului, puteți efectua una sau mai multe dintre următoarele:

Editați legătura

Setări

Selectați setările de conectare configurate din lista de dispozitive și puteți edita parametrii sursei evenimentului, inclusiv sursa evenimentului și ținta de conectare.

Șterge legătura

Setări

Selectați setările de conectare configurate din lista de dispozitive și faceți clic**Șterge** pentru a-l șterge.

8.8.3 Configurați acțiunile dispozitivului pentru trecerea cardului

Activați acțiunile de conectare ale dispozitivului de control al accesului (cum ar fi dezarmarea unei zone și declanșarea promptului audio) pentru trecerea unui anumit card. În acest fel, puteți monitoriza comportamentul și locația titularului cardului.

Pași

Nota

Ar trebui să fie suportat de dispozitiv.

1.Clic **Control acces** → **Configurare legături**.

2.Selectați dispozitivul de control al accesului din lista din stânga.

3.Clic **Adăugă** pentru a adăuga o nouă legătură.

4.Selectați **Conectarea cardului** ca sursă de eveniment.

5.Introduceți numărul cardului sau selectați cardul din lista derulantă.

6.Selectați cititorul de carduri de unde trece cardul.

7.În zona țintă de legătură, setați ținta proprietății pentru a activa această acțiune.

Buzzer pe controler

Avertismentul sonor al dispozitivului de control al accesului va fi declanșat.

Buzzer pe Reader

Avertismentul sonor al cititorului de carduri va fi declanșat.

Capta

O fotografie legată de eveniment va fi capturată atunci când are loc evenimentul selectat.

Înregistrare

O fotografie legată de eveniment va fi capturată atunci când are loc evenimentul selectat.



Nota

Dispozitivul ar trebui să accepte înregistrarea.

Ieșire de alarmă

Ieșirea de alarmă va fi declanșată pentru notificare.

Intrare alarmă

Armați sau dezarmați intrarea alarmei.



Nota

Dispozitivul ar trebui să accepte funcția de intrare de alarmă.

Punct de acces

Starea ușii deschisă, închisă, rămâne deschisă sau rămâne închisă va fi declanșată. **Redare**

audio

Promptul audio va fi declanșat. Și conținutul audio legat de indexul audio selectat va fi redat conform modului de redare configurat.

8.Clic **Salva**.

Când cardul (configurat la Pasul 5) trece prin glisare pe cititorul de carduri (configurat la Pasul 6), acesta poate declanșa acțiunile legate (configurat la pasul 7).

9. **Opțional:** După adăugarea conexiunii dispozitivului, puteți efectua una sau mai multe dintre următoarele:

Șterge legătura Setări

Selectați setările de conectare configurate din lista de dispozitive și faceți clic **Șterge** pentru a-l șterge.

Editați legătura Setări

Selectați setările de conectare configurate din lista de dispozitive și puteți edita parametrii sursei evenimentului, inclusiv sursa evenimentului și ținta de conectare.

8.8.4 Configurați acțiunile dispozitivului pentru ID-ul persoanei

Puteți seta acțiunile de conectare ale dispozitivului de control al accesului pentru ID-ul de persoană specificat. Când dispozitivul de control al accesului detectează ID-ul persoanei specificate, acesta poate declanșa ieșirea de alarmă, soneria pe cititorul de carduri și alte acțiuni, astfel încât să implementeze o monitorizare specială asupra persoanei specificate.

Pași



Nota

Ar trebui să fie suportat de dispozitiv.

1.ClicControl acces → Configurare legături.

2.Selectați dispozitivul de control al accesului din lista din stânga.

3.Clic**Adăuga**pentru a adăuga o nouă legătură.

4.Selecta**Legătura persoanei**ca sursă de eveniment.

5.Introduceți numărul angajatului sau selectați persoana din lista verticală.

6.Selectați cititorul de carduri de unde trece cardul.

7.În zona țintă de legătură, setați ținta proprietății pentru a activa această acțiune.

Buzzer pe controler

Avertismentul sonor al dispozitivului de control al accesului va fi declanșat.

Buzzer pe Reader

Avertismentul sonor al cititorului de carduri va fi declanșat.

Capta

O fotografie legată de eveniment va fi capturată atunci când are loc evenimentul selectat.

Înregistrare

O fotografie legată de eveniment va fi capturată atunci când are loc evenimentul selectat.



Nota

Dispozitivul ar trebui să accepte înregistrarea.

Ieșire de alarmă

Ieșirea de alarmă va fi declanșată pentru notificare.

Intrare alarmă

Armați sau dezarmați intrarea alarmei.



Nota

Dispozitivul ar trebui să accepte funcția de zonă.

Punct de acces

Starea ușii deschisă, închisă, rămâne deschisă sau rămâne închisă va fi declanșată. **Redare**

audio

Promptul audio va fi declanșat. Și conținutul audio legat de indexul audio selectat va fi redat conform modului de redare configurat.

8.ClicSalva.

9. Opțional:După adăugarea conexiunii dispozitivului, puteți efectua una sau mai multe dintre următoarele:

Șterge legătura Setări

Selectați setările de conectare configurate din lista de dispozitive și faceți clic**Șterge** pentru a-l șterge.

Editați legătura Setări

Selectați setările de conectare configurate din lista de dispozitive și puteți edita parametrii sursei evenimentului, inclusiv sursa evenimentului și ținta de conectare.

8.9 Controlul ușii

În modulul de monitorizare, puteți vizualiza starea în timp real a ușilor gestionate de dispozitivul de control acces adăugat. De asemenea, puteți controla ușile, cum ar fi deschiderea/închiderea ușii, sau rămâneți ușa deschisă/închisă prin intermediul clientului de la distanță. Evenimentele de acces în timp real sunt afișate în acest modul. Puteți vizualiza detaliile de acces și detaliile persoanei.



Nota

Pentru utilizatorul cu permisiunea de control al ușii, utilizatorul poate intra în modulul de monitorizare și poate controla ușa. Sau pictogramele folosite pentru control nu se vor afișa. Pentru setarea permisiunii utilizatorului, consultați **Managementul persoanelor**.

8.9.1 Starea ușii de control

Puteți controla starea unei singure ușii, inclusiv deschiderea ușii, închiderea ușii, menținerea ușii deschisă și rămânerea ușii închise.

Pași

- 1.Clic**Monitorizare**pentru a intra pe pagina de monitorizare a stării.
- 2.Selectați un grup de puncte de acces în colțul din dreapta sus.



Nota

Pentru gestionarea grupului de puncte de acces, consultați*Managementul grupului*în manualul de utilizare al software-ului client.

Se vor afișa ușile din grupul de control acces selectat.

- 3.Faceți clic pe pictograma unei ușii pentru a selecta o ușă sau apăsați**Ctrl**și selectați mai multe ușii.
- 4.Faceți clic pe următoarele butoane pentru a controla ușa.

Ușa Deschisă

Când ușa este încuiată, deblocați-o și va fi deschisă o dată. După durata de deschidere, ușa va fi închisă și blocată din nou automat.

Închide Ușa

Când ușa este descuiată, încuiați-o și va fi închisă. Persoana care are autorizația de acces poate accesa ușa cu acreditări.

Rămâi deschis

Ușa va fi descuiată (indiferent de închisă sau deschisă). Toate persoanele pot accesa ușa fără a fi necesare acreditări.

Rămâi închis

Ușa va fi închisă și încuiată. Nicio persoană nu poate accesa ușa chiar dacă are acreditările autorizate, cu excepția super utilizatorilor.

Capta

Capturați o fotografie manual.



Nota

The **Capta** butonul este disponibil când dispozitivul acceptă funcția de captură. Imaginea este salvată pe computerul care rulează clientul. Pentru setarea căii de salvare, consultați *Setați calea de salvare a fișierului* în manualul de utilizare al software-ului client.

Rezultat

Pictograma ușilor se va schimba în timp real în funcție de operațiune dacă operațiunea este reușită.

8.9.2 Verificați înregistrările de acces în timp real

Înregistrările de acces se vor afișa în timp real, inclusiv înregistrările de trecere a cardului, înregistrările de recunoaștere a feței, înregistrările de comparare a amprentelor etc. Puteți vizualiza informațiile despre persoană și puteți vizualiza imaginea capturată în timpul accesului.

Pași

1. Clic Monitorizare și selectați un grup din lista derulantă din colțul din dreapta sus.

Înregistrările de acces declanșate la ușile din grupul selectat se vor afișa în timp real. Puteți vizualiza detaliile înregistrărilor, inclusiv numărul cardului, numele persoanei, organizația, ora evenimentului etc.

2. Opțional: Verificați tipul evenimentului și starea evenimentului, astfel încât aceste evenimente să apară în listă dacă evenimentele sunt detectate. Evenimentele de tip sau stare nebifate nu vor fi afișate în listă.

3. Opțional: Verificați **Afișează cel mai recent eveniment** iar cea mai recentă înregistrare de acces va fi selectată și afișată în partea de sus a listei de înregistrări.

- 4. Opțional:** Faceți clic pe eveniment pentru a vedea detaliile persoanei accesate, inclusiv fotografiile persoanei (imaginea și profilul capturat), numărul persoanei, numele persoanei, organizația, telefonul, adresa de contact etc.



Nota

Puteți face dublu clic pe imaginea capturată pentru a o mări pentru a vedea detaliile.

- 5. Opțional:** Faceți clic dreapta pe numele coloanei tabelului de evenimente de acces pentru a afișa sau ascunde coloana în funcție de nevoile reale.

8.10 Centru de evenimente

Puteți configura evenimentul resurselor adăugate și puteți seta acțiunile de conectare astfel încât, atunci când evenimentul este declanșat, clientul software să poată notifica personalul de securitate și să înregistreze detaliile evenimentului pentru a le verifica ulterior.

În pagina de gestionare a evenimentelor, puteți configura evenimentul de control al accesului. Pentru detalii despre configurarea evenimentului de control al accesului, consultați **Configurați acțiunile de conectare pentru controlul accesului**.

În centrul de evenimente, puteți vizualiza evenimentele în timp real și puteți căuta evenimentele istorice. Pentru detalii, consultați **Vizualizați evenimente în timp real** și **Căutați evenimente istorice**.

8.10.1 Activați primirea notificărilor de evenimente de la dispozitive

Înainte ca software-ul client să poată primi notificări de evenimente de la dispozitiv, mai întâi trebuie să armați dispozitivul.

Pași

- 1. Clic**  → **Instrument** → **Control armare dispozitiv** pentru a deschide pagina Device Arming Control.

Toate dispozitivele adăugate apar pe această pagină.

- 2. În coloana Armare automată, porniți comutatorul pentru a activa armarea automată.**

După pornire, dispozitivul (dispozitivele) vor fi armate. Iar notificările despre evenimentele declanșate de dispozitivul(e) armat(e) vor fi trimise automat către software-ul client în timp real.

8.10.2 Vizualizare evenimente în timp real

În modulul Eveniment în timp real al paginii centrului de evenimente, puteți vizualiza informațiile despre eveniment în timp real, inclusiv sursa evenimentului, ora evenimentului, prioritate, cuvinte cheie ale evenimentului etc.

Înainte de a începe

Activați primirea evenimentelor de pe dispozitive înainte ca clientul să poată primi informații despre evenimente de pe dispozitiv, a se vedea **Activați Primirea notificărilor de eveniment de la dispozitive** pentru detalii.

Pași

1. **Clic Centru de evenimente → Eveniment în timp real** pentru a intra pe pagina de evenimente în timp real și puteți vizualiza evenimentele în timp real primite de client.

Ora evenimentului

Pentru dispozitivul video, ora evenimentului este ora clientului când primește evenimentul. Pentru dispozitivele fără video, ora evenimentului este momentul în care evenimentul este declanșat.

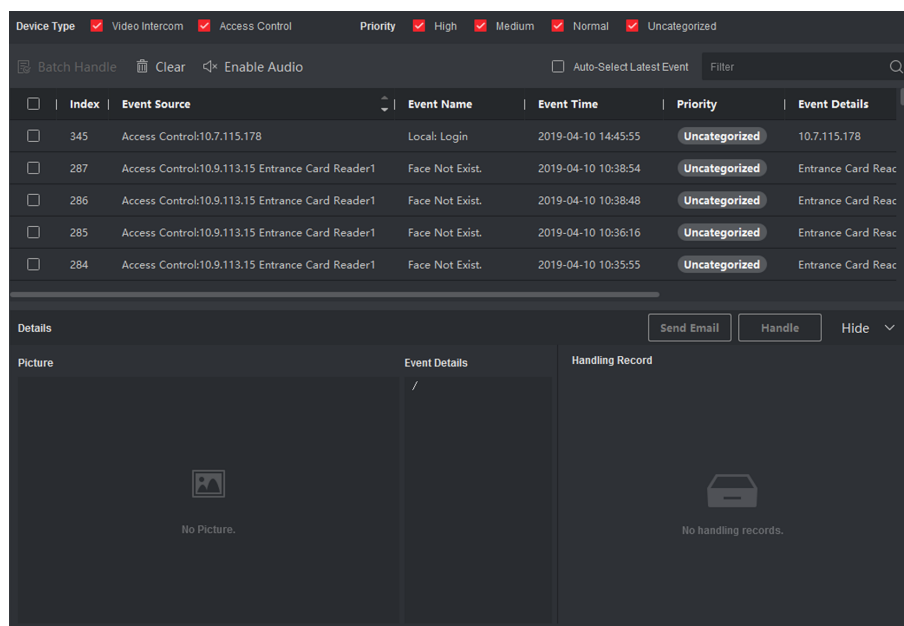


Figura 8-9 Vizualizare evenimente în timp real

2. Setăți condițiile de filtrare sau introduceți cuvântul cheie pentru eveniment în câmpul de text Filtru pentru a afișa numai evenimentele necesare.

Tip de dispozitiv

Tipul de dispozitiv care a avut loc evenimentul.

Prioritate

Prioritatea evenimentului care indică gradul de urgență al evenimentului.

3. **Opțional:** Faceți clic dreapta pe antetul tabelului din lista de evenimente pentru a personaliza elementele legate de eveniment care urmează să fie afișate în lista de evenimente.

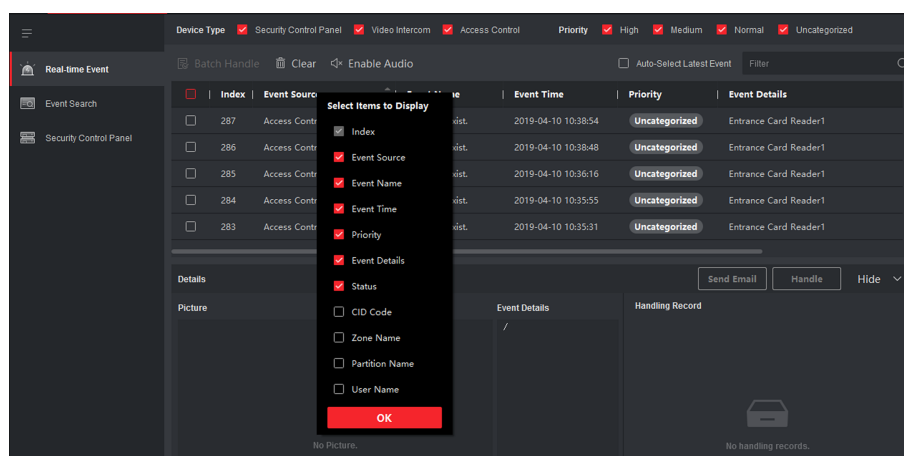


Figura 8-10 Personalizarea elementelor legate de eveniment care urmează să fie afișate

4. Vedeți detaliile informațiilor despre eveniment.

- 1) Selectați un eveniment din lista de evenimente.
- 2) Faceți clic **Extinde** în colțul din dreapta-jos al paginii.
- 3) Vizualizați imaginea aferentă, descrierea detaliată și înregistrările de înmânare ale evenimentului.
- 4) **Opțional:** Treceți cursorul pe imaginea asociată, apoi faceți clic pe pictograma de descărcare din colțul din dreapta sus al imaginii pentru a o descărca pe computerul local. Puteți seta manual calea de salvare.

5. Opțional: Efectuați următoarele operații dacă este necesar.

Gestionați un singur eveniment

Clic **Mâner** pentru a introduce sugestia de procesare, apoi faceți clic **Angajează-te**.



Nota

După ce un eveniment este gestionat, **Mâner** butonul va deveni **Adăugați observație**, faceți clic **Adăugați observație** pentru a adăuga mai multe remarci pentru acest eveniment gestionat.

Gestionați evenimente într-un lot

Selectați evenimentele care trebuie procesate, apoi faceți clic **Mâner în lot**. Introduceți sugestia de procesare, apoi faceți clic **Angajează-te**.

Activați/Dezactivați Alarmă audio

Clic **Activați audio/Dezactivați audio** pentru a activa/dezactiva audio-ul evenimentului.

Selectați Cel mai recent Eveniment automat

Verificați **Selectați automat cel mai recent eveniment** pentru a selecta cel mai recent eveniment automat și sunt afișate detaliile informațiilor despre eveniment.

Ștergeți evenimentele

Clic **Clar** pentru a șterge toate evenimentele din lista de evenimente.

Trimite e-mail

Selectați un eveniment și apoi faceți clic **Trimite e-mail**, iar detaliile informative ale acestui eveniment vor fi trimise prin e-mail.

Nota

Ar trebui să configurați mai întâi parametrii de e-mail, vezi *Setați parametrii de e-mail* în manualul de utilizare al software-ului client pentru detalii.

8.10.3 Căutare evenimente istorice

În modulul Căutare evenimente din pagina centrului de evenimente, puteți căuta evenimentele istorice prin oră, tip de dispozitiv și alte condiții în funcție de tipul de dispozitiv specificat și apoi procesați evenimentele.

Înainte de a începe

Activați primirea de evenimente de la dispozitive înainte ca clientul să poată primi informații despre evenimente de pe dispozitiv, vezi **Activați Primirea notificărilor de eveniment de la dispozitive** pentru detalii.

Pași

1. Clic **Centru de evenimente** → **Căutare evenimente** pentru a intra în pagina de căutare a evenimentelor.

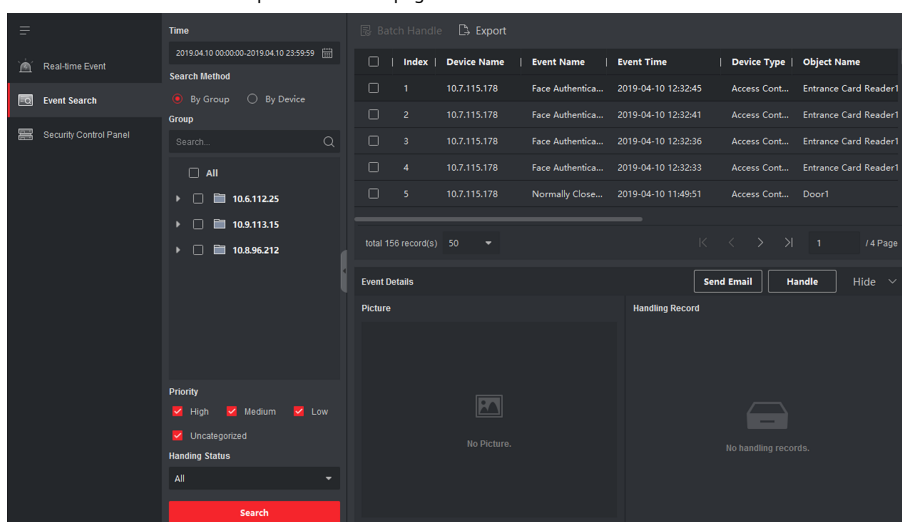


Figura 8-11 Eveniment istoric de căutare

2. Setați condițiile de filtrare pentru a afișa numai evenimentele necesare.

Timp

Ora clientului la care începe evenimentul.

Căutați după

Grup: Căutați evenimentele care au avut loc pe resursele din grupul selectat. **Dispozitiv:**

Căutați evenimentele care au avut loc pe dispozitivul selectat. **Tip de dispozitiv**

Tipul de dispozitiv care a avut loc evenimentul.

Toate

Toate tipurile de dispozitive și puteți seta următoarele condiții de filtrare: grup, prioritate și stare.

Videointerfon

Pentru evenimentele de interfon video, trebuie să selectați domeniul de căutare: Toate înregistrările și numai deblocarea.

- **Toate înregistrările:** Puteți filtra evenimentele din toate evenimentele video interfon și trebuie să setați următoarele condiții de filtrare: dispozitiv, prioritate, stare.
- **Doar Deblocare:** Puteți filtra evenimentele din toate evenimentele de deblocare a interfonului video și trebuie să setați următoarele condiții de filtrare: dispozitiv, tip de deblocare.

Control acces

Pentru evenimentele de control acces, puteți seta următoarele condiții de filtrare: dispozitiv, prioritate, stare, tip eveniment, tip cititor card, nume persoane, nr card, organizație.



Nota

Clic **Arată mai mult** pentru a seta tipul evenimentului, tipul cititorului de carduri, numele persoanei, nr. cardului, organizarea.

Grup

Grupul dispozitivului care a avut loc evenimentul. Ar trebui să setați grupul ca condiție numai atunci când selectați Tipul dispozitivului ca **Toate**.

Dispozitiv

Dispozitivul care a avut loc evenimentul.

Prioritate

Prioritatea include scăzută, medie, mare și necategorizată, ceea ce indică gradul de urgență al evenimentului.

Stare

Starea de gestionare a evenimentului.

3. Clic **Căutare** pentru a căuta evenimentele conform condițiilor pe care le-ați stabilit.

4. **Opțional:** Faceți clic dreapta pe antetul tabelului din lista de evenimente pentru a personaliza elementele legate de eveniment care urmează să fie afișate în lista de evenimente.

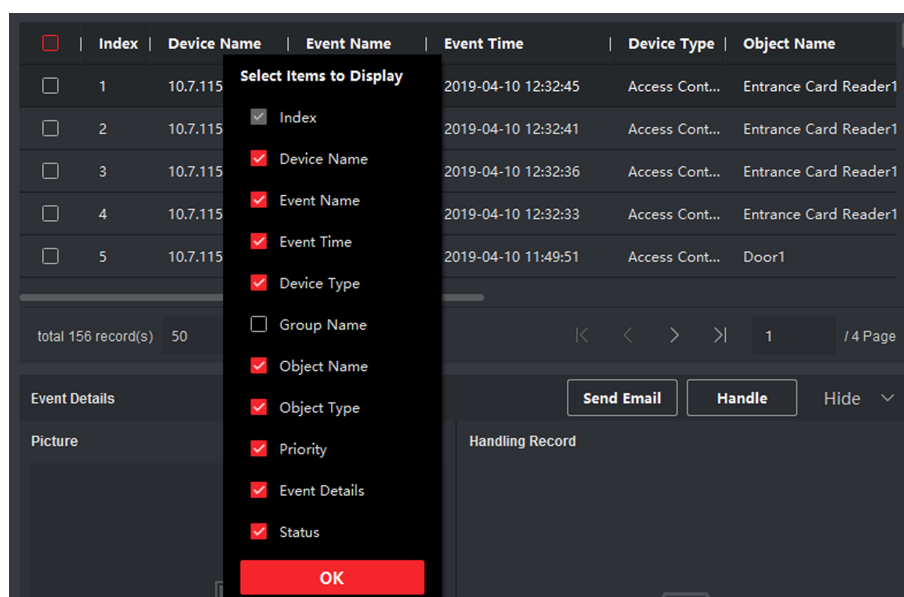


Figura 8-12 Particularizarea elementelor legate de eveniment care urmează să fie afișate

5. Opțional: Gestionati evenimentul(e).

- Gestionati un singur eveniment: selectati un eveniment care trebuie procesat, apoi faceti clic **Măner** în pagina cu detalii despre informații despre eveniment și introduceți sugestia de procesare.
- Gestionati evenimentele într-un lot: selectati evenimentele care trebuie procesate, apoi faceti clic **Măner în lot** și introduceți sugestia de procesare.

 Nota

După ce un eveniment este gestionat, **Măner** butonul va deveni **Adăugați observație**, faceti clic **Adăugați observație** pentru a adăuga mai multe remarci pentru acest eveniment gestionat.

6. Opțional: Selectati un eveniment și apoi faceti clic **Trimite e-mail**, iar detaliile informative ale acestui eveniment vor fi trimise prin e-mail.
 Nota

Ar trebui să configurați mai întâi parametrii de e-mail, vezi *Setați parametrii de e-mail* în manualul de utilizare al software-ului client pentru detalii.

7. Opțional: Clic **Export** pentru a exporta jurnalul de evenimente sau imaginile evenimentului pe computerul local în format CSV. Puteți seta manual calea de salvare.**8.** Treceți cursorul pe imaginea asociată, apoi faceti clic pe pictograma de descărcare din colțul din dreapta sus al imaginii pentru a o descărca pe computerul local. Puteți seta manual calea de salvare.

8.11 Timp și prezență

Modulul Timp și prezență oferă mai multe funcționalități pentru a urmări și monitoriza momentul în care angajații încep și încetează lucrul, precum și control deplin asupra orelor de lucru ale angajaților, cum ar fi sosiri întârziate, plecări anticipate, timpul acordat în pauze și absenteism.



Nota

În această secțiune, vă prezentăm configurațiile înainte de a putea obține rapoartele de prezență. Înregistrările de acces înregistrate după aceste configurații vor fi calculate în statistici.

8.11.1 Configurarea parametrilor de prezență

Puteți configura parametrii de prezență, inclusiv regula generală, parametrii orelor suplimentare, punctul de verificare a prezenței, vacanța, tipul de concediu etc.

Setați weekendul

Zilele de weekend pot varia în diferite țări și regiuni. Clientul oferă funcția de definire a weekendurilor. Puteți selecta una sau mai multe zile ca weekend-uri în funcție de cerințele reale și puteți stabili reguli diferite de prezență pentru weekend-uri față de zilele lucrătoare.

Pași



Nota

Parametrii configurați aici vor fi setați implicit pentru perioada de timp nou adăugată. Nu le va afecta pe cele existente(e).

1. Intrați în modulul Timp și prezență.
2. Clic **Setări de prezență** → **Regulă generală**.
3. Selectați ziua (zile) ca weekend, cum ar fi sâmbătă și duminică.
4. Clic **Salva**.

Configurați parametrii orelor suplimentare

Puteți configura parametrii orelor suplimentare pentru ziua de lucru și pentru weekend, inclusiv nivelul orelor suplimentare, rata orelor de lucru, statutul de prezență pentru orele suplimentare etc.

Pași

1. Clic **Timp și prezență** → **Setări de prezență** → **Orele suplimentare**.
2. Setați informațiile necesare.

Nivelul orelor suplimentare pentru ziua de lucru

Când lucrați pentru o anumită perioadă după terminarea orei de lucru în ziua lucrătoare, veți atinge un nivel diferit de ore suplimentare: nivelul 1 pentru ore suplimentare, nivelul 2 și nivelul 3 pentru orele suplimentare. Puteți seta o rată diferită pentru orele suplimentare, respectiv, pentru trei niveluri de ore suplimentare.

Rata oră de lucru

Rata oră de lucru este utilizată pentru a calcula orele de lucru prin înmulțirea acestuia cu orele suplimentare. Când lucrați pentru o anumită perioadă după terminarea orei de lucru în ziua lucrătoare, veți ajunge la un nivel diferit de ore suplimentare. Puteți seta diferite rate pentru orele de lucru (1-10, poate fi o zecimală) pentru trei niveluri de ore suplimentare. De exemplu, orele suplimentare valabile sunt de o oră (în orele suplimentare nivelul 1), iar rata orelor suplimentare de la nivelul 1 este setată la 2, apoi orele de lucru din perioada vor fi calculate ca 2 ore.

Regula orelor suplimentare pentru weekend

Puteți activa regula orelor suplimentare pentru weekend și puteți seta modul de calcul.

3.ClicSalva.

Configurați punctul de verificare a prezenței

Puteți seta cititoarele de carduri ale punctului de acces ca punct de verificare a prezenței, astfel încât autentificarea cititoarelor de carduri să fie înregistrată pentru prezență.

Înainte de a începe

Ar trebui să adăugați un dispozitiv de control al accesului înainte de a configura punctul de control al prezenței. Pentru detalii, consultați

Adăugați dispozitiv.

Pași



Nota

În mod implicit, toate cititoarele de carduri ale dispozitivelor de control al accesului adăugate sunt setate ca punct de control al prezenței.

1.Intrați în modulul Timp și prezență.

2.Clic**Setări de prezență** → **Punct de verificare a prezenței**pentru a intra în pagina Setări punct de verificare a prezenței.

3. **Opțional:**Set**Setați toate cititoarele de carduri ca puncte de verificare**comuta la oprit.

Doar cititorii de carduri din listă vor fi setate ca puncte de verificare a prezenței.

4.Verificați cititoarele de carduri dorite în lista de dispozitive ca punct(e) de verificare a prezenței.

5.Setați funcția punct de control ca**Început/Sfârșit-Lucrare,Începe-Lucrare**sau**Sfârșitul lucrării**.

6.Clic**Setați ca punct de verificare**.

Punctul de verificare a prezenței configurat este afișat în lista din dreapta.

Configurați vacanța

Puteți adăuga vacanța în care nu va fi înregistrată check-in sau check-out.

Adăugați vacanță obișnuită

Puteți configura o sărbătoare care va intra în vigoare anual în zilele obișnuite din perioada efectivă, cum ar fi Anul Nou, Ziua Independenței, Ziua de Crăciun etc.

Pași

1. Intrați în modulul Timp și prezență.
2. Clic **Setări de prezență** → **Vacanță** pentru a intra în pagina Setări de vacanță.
3. Verificați **Sărbătoare obișnuită** ca tip de vacanță.
4. Personalizați un nume pentru vacanță.
5. Stabiliți prima zi de vacanță.
6. Introduceți numărul zilelor de vacanță.
7. Setati statutul de prezență dacă angajatul lucrează în vacanță.
8. **Opțional:** Verificați **Repetati Anual** pentru a face acest cadru de vacanță eficient în fiecare an.
9. Clic **Bine**.

Sărbătoarea adăugată va fi afișată în lista de sărbători și în calendar.

Dacă data este selectată ca sărbători diferite, va fi înregistrată ca prima sărbătoare adăugată.

10. **Opțional:** După adăugarea vacanței, efectuați una dintre următoarele operațiuni.

Editați vacanța

Clic  pentru a edita informațiile despre vacanță.

Șterge vacanța

Selectați una sau mai multe sărbători adăugate și faceți clic **Șterge** pentru a șterge vacanțele din lista sărbătorilor.

Adăugați vacanță neregulată

Puteți configura o vacanță care va intra în vigoare anual în zilele neregulate din perioada efectivă, cum ar fi sărbătoarea bancară.

Pași

1. Intrați în modulul Timp și prezență.
2. Clic **Setări de prezență** → **Vacanță** pentru a intra în pagina Setări de vacanță.
3. Clic **Adăuga** pentru a deschide pagina Adăugați vacanță.
4. Verificați **Vacanță neregulată** ca tip de vacanță.
5. Personalizați un nume pentru vacanță.
6. Setati data de începere a vacanței.

Exemplu

Dacă doriți să setați a patra zi de joi din noiembrie 2019 ca sărbătoare de Ziua Recunoștinței, ar trebui să selectați 2019, 4 noiembrie și joi din cele patru liste derulante.

7. Introduceți numărul zilelor de vacanță.
8. Setati statutul de prezență dacă angajatul lucrează în vacanță.
9. **Opțional:** Verificați **Repetati Anual** pentru a face acest cadru de vacanță eficient în fiecare an.
10. Clic **Bine**.

Sărbătoarea adăugată va fi afișată în lista de sărbători și în calendar.

Dacă data este selectată ca sărbători diferite, va fi înregistrată ca prima sărbătoare adăugată.

11. Opțional: După adăugarea vacanței, efectuați una dintre următoarele operațiuni.

- | | |
|------------------------|--|
| Editați vacanța | Clic  pentru a edita informațiile despre vacanță. |
| Șterge vacanța | Selectați una sau mai multe sărbători adăugate și faceți clic Șterge pentru a șterge vacanțele din lista sărbătorilor. |

Configurați tipul de concediu

Puteți personaliza tipul de concediu (tip de concediu major și tip de concediu minor) în funcție de nevoile reale. De asemenea, puteți edita sau șterge tipul de concediu.

Pași

1. Intrați în modulul Timp și prezență.

2. Clic **Setări de prezență** → **Tip de concediu** pentru a intra în pagina Setări tip de părăsire.

3. Clic **Adăuga** din stânga pentru a adăuga un tip de concediu major.

4. Opțional: Efectuați una dintre următoarele operațiuni pentru tipul de concediu major.

- | | |
|---------------|--|
| Edita | Mutați cursorul peste tipul principal de concediu și faceți clic pe  pentru a edita concediul major tip. |
| Șterge | Selectați un tip de concediu major și faceți clic Șterge din stânga pentru a șterge tipul principal de concediu. |

5. Clic **Adăuga** din dreapta pentru a adăuga un tip de concediu minor.

6. Opțional: Efectuați una dintre următoarele operațiuni pentru tipul de concediu minor.

- | | |
|---------------|---|
| Edita | Mutați cursorul peste tipul de concediu minor și faceți clic pe  pentru a edita concediul minor tip. |
| Șterge | Selectați unul sau mai multe tipuri majore de concediu și faceți clic Șterge din dreapta pentru a șterge tipul (tipurile) de concediu minor selectat(e). |

Sincronizați înregistrarea de autentificare cu baza de date terță parte

Datele de prezență înregistrate în software-ul client pot fi utilizate de către alt sistem pentru calcule sau alte operațiuni. Puteți activa funcția de sincronizare pentru a aplica automat înregistrarea de autentificare din software-ul client la baza de date terță parte.

Pași

1. Intrați în modulul Timp și prezență.

2. Clic **Setări de prezență** → **Bază de date terță parte**.

3. Set **Aplicați la baza de date** comutați la pornit pentru a activa funcția de sincronizare.

4. Selectați tipul bazei de date ca **SQL Server** sau **MySql**.

Nota

Dacă selectați **MySQL**, ar trebui să importați fișierul de configurare (libmysql.dll) de pe computerul local.

5. Setați ceilalți parametri necesari ai bazei de date terță parte, inclusiv adresa IP a serverului, numele bazei de date, numele de utilizator și parola.
6. Setați parametrii tabelului bazei de date în funcție de configurația actuală.
 - 1) Introduceți numele tabelului bazei de date terță parte.
 - 2) Setați câmpurile de tabel mapate între software-ul client și baza de date terță parte.
7. Clic **Salva** pentru a testa dacă baza de date poate fi conectată și pentru a salva setările pentru conexiunea cu succes.
 - Datele de prezență vor fi scrise în baza de date terță parte.
 - În timpul sincronizării, dacă clientul se deconectează de la baza de date terță parte, clientul va începe reconectarea la fiecare 30 de minute. După reconectare, clientul va sincroniza datele înregistrate în perioada de deconectare cu baza de date terță parte.

Configurați timpul de pauză

Puteți adăuga timpul de pauză și puteți seta ora de începere, ora de încheiere, durata, modul de calcul și alți parametri pentru pauză. Timpul de pauză adăugat poate fi, de asemenea, editat sau șters.

Pași

1. Clic **Timp și prezență → **Orar**.**

Orarele adăugate sunt afișate în listă.

2. Selectați un orar adăugat sau faceți clic **Adăuga** pentru a intra pe pagina de setare a orarului.

3. Clic **Timp de pauză** pentru a intra pe pagina Pauza.

4. Clic **Setări de pauză.**

5. Adăugați timpul de pauză.

- 1) Faceți clic **Adăuga**.
- 2) Introduceți un nume pentru timpul de pauză.
- 3) Setați parametrii corespunzători pentru timpul de pauză.

Ora de început / Ora de sfârșit

Setați ora la care începe și se termină pauza. **Nu**

mai devreme / nu mai târziu

Setați cea mai devreme oră de glisare pentru începerea pauzei și cea mai recentă oră de glisare pentru încheierea pauzei.

Durata pauzei

Durata de la ora de început până la ora de încheiere a pauzei. **Calcul**

Deducere automată

Durata fixă a pauzei va fi exclusă din programul de lucru. **Trebuie verificat**

Durata pauzei va fi calculată și exclusă din orele de lucru în funcție de ora reală de check-in și check-out.



Nota

Dacă selectați **Trebuie verificat** ca metodă de calcul, trebuie să setați statutul de prezență pentru întoarcerea târziu sau devreme din pauză.

6. Clic Salvă pentru a salva setările.

7. Opțional: Clic **Adăugă** pentru a continua să adăugați timp de pauză.

Configurați afișarea raportului

Puteți configura conținutul afișat în raportul de prezență, cum ar fi numele companiei, sigla, formatul datei, formatul orei și marcajul.

Pași

1. Intrați în modulul Timp și prezență.

2. Clic **Statistici de prezență → Afișare raport**.

3. Setări setările de afișare pentru raportul de prezență.

Numele companiei

Introduceți un nume de companie pentru a afișa numele în raport. **Format dată / Format oră**

Setați formatul de dată și formatul orei în funcție de nevoile reale. **Marcaj**

de stare de prezență în raport

Introduceți marcajul și selectați culoarea. Câmpurile aferente stării de prezență din raport vor fi afișate cu marcajul și culoarea.

Marcaj de weekend în raport

Introduceți marcajul și selectați culoarea. Câmpurile de weekend din raport vor fi afișate cu marcajul și culoarea.

4. Clic Salva.

8.11.2 Adăugați orarul general

Pe pagina de orar, puteți adăuga un orar general pentru angajați, care necesită timpul fix de începere a lucrului și ora de terminare a lucrului. De asemenea, puteți seta o oră valabilă de check-in/out, un orar permis pentru a întârzia și a pleca devreme.

Pași

1. Clic **Timp și prezență → Orar** pentru a intra în pagina de setări orar.

2. Clic **Adăugă** pentru a intra în pagina de adăugare a orarului.

Basic Settings

Name: Timetable 1

Timetable Type: General

Calculated by: Each Check-In/Out

Valid Authentication Interval: 1 min

Enable T&A Status: ☐

Attendance Time

Start-Work Time: 9:00

End-Work Time: 18:00

Valid Check-in Time: 8:30 to 9:30

Valid Check-out Time: 17:30 to 18:30

Calculated as: 540 min

Late Allowable: 10 min

Early Leave Allowable: 10 min

Configuration Result

24 00 02 04 06 08 10 12 14 16 18 20 22 24 00 02

Valid Time of Check-In/Out Work Time Late/Early Leave Allowable

Absence Settings

Save

Figura 8-13 Adăugați orar

3. Creați un nume pentru orar.



Nota

Puteti face clic pe pictograma de culoare de langa nume pentru a personaliza culoarea pentru orarul valabil din bara de timp din zona Rezultate configuratie.

4. Selectați tipul de orar ca general.

5. Selectați metoda de calcul.

Primul intrat și ultimul ieșit

Prima oră de check-in este înregistrată ca oră de începere a lucrului, iar ultima oră de check-out este înregistrată ca oră de sfârșit de lucru.

Fiecare check-in/out

Fiecare oră de check-in și check-out este valabilă, iar suma tuturor perioadelor dintre ora adiacentă de check-in și check-out va fi înregistrată ca durată de lucru valabilă.

Trebuie să setați **Interval de autentificare valid** pentru această metodă de calcul. De exemplu, dacă intervalul dintre trecerea cardului a aceluiași card este mai mic decât valoarea setată, trecerea cardului este invalidă.

6. Opțional: Set **Activați starea T&A** comutați la pornit pentru a calcula în funcție de starea de prezență a dispozitivului.

Nota

Această funcție ar trebui să fie acceptată de dispozitiv.

7. Setează parametrii aferenți timpului de prezență după cum urmează: **Ora de**

începere/sfârșit de lucru

Setați ora de începere a lucrului și ora de terminare a lucrului.

Ora valabilă de check-in/out

Pe bara de timp, reglați bara galbenă pentru a seta orarul în care este valabil check-in sau check-out.

Calculat ca

Setați durata calculată ca durata reală de lucru. **Concediu**

târziu/devreme permis

Stabiliți orarul pentru concediu târziu sau devreme.

8. Setează parametrii legați de absență.

Check-in, târziu pentru

Puteți seta durata de întârziere pentru angajatul care s-a înregistrat, dar întârzie la serviciu. În cazul în care angajatul depășește perioada de timp cerută, datele sale de prezență vor fi marcate ca absent.

Check-out, concediu devreme pentru

Puteți seta durata concediului anticipat pentru angajatul care pleacă mai devreme decât timpul normal de concediu, iar datele de prezență ale acestuia vor fi marcate ca absente.

Fără check-in

Dacă angajatul nu se înregistrează, datele sale de prezență pot fi marcate ca absent sau întârziat.

Fără check-out

Dacă angajatul nu face check-out, datele sale de prezență pot fi marcate ca absent sau concediu anticipat.

9. **Clic Salvă** pentru a adăuga orarul.

10. **Opțional:** Efectuați una sau mai multe operațiuni următoare după adăugarea orarului.

Editați orarul

Selectați un orar din listă pentru a edita informațiile conexe.

Ștergeți orarul

Selectați un orar din listă și faceți clic **Șterge** pentru a-l șterge.

8.11.3 Adăugați Shift

Puteți adăuga tură pentru angajați, inclusiv setarea perioadei de schimb (zi, săptămână, lună) și timpul efectiv de prezență. În conformitate cu cerințele actuale, puteți adăuga mai multe orare într-o tură pentru angajați, ceea ce le cere să se înregistreze și să iasă pentru fiecare orar.

Înainte de a începe

Adăugați mai întâi un orar. Vedeți **Adăugați orarul general** pentru detalii.

Pași

1. Clic **Timp și prezență** → **Schimb** pentru a intra în pagina de setări a turelor.
2. Clic **Adăugare** pentru a intra în pagina Adăugare schimb.
3. Introduceți numele pentru schimb.
4. Selectați perioada de schimb din lista derulantă.
5. Selectați orarul adăugat și faceți clic pe bara de timp pentru a aplica orarul.

The screenshot displays the 'Shift' configuration page. At the top, there's a 'Name' field with 'Default Shift' and a 'Period' dropdown set to '1'. Below this is a 'Week(s)' dropdown. A 'Timetable 1' section contains a 'Delete' button and a 'Clear' button. The main part of the interface is a grid with days of the week (Mon. to Sun.) on the y-axis and time slots (00:00 to 24:00) on the x-axis. Blue bars are present from 09:00 to 18:00 for all days. At the bottom, there are 'Save' and 'Assign' buttons.

Figura 8-14 Add Shift

**Nota**

Puteți selecta mai multe orare. Ora de începere și de sfârșit de lucru și ora de check-in și de ieșire valabilă în diferite tabele orare nu pot fi suprapuse.

Shift

Name: New Shift 1

Period: 1 Week(s)

☒ Timetable 1 ☐ Timetable 2

✕ Delete 🗑️ Clear Timetable 1 : 09:00 - 18:00

Time	00:00	02:00	04:00	06:00	08:00	10:00	12:00	14:00	16:00	18:00	20:00	22:00	24:00
Mon.													
Tue.													
Wed.													
Thu.													
Fri.													
Sat.													
Sun.													

Save **Assign**

Figura 8-15 Adăugați mai multe orare

6. ClicSalva.

Listele de schimburi adăugate în panoul din stânga paginii. Pot fi adăugate cel mult 64 de schimburi.

7. Opțional: Atribuiți schimbul către organizație sau persoană pentru un program rapid de schimb.

1) Faceți clic **Atribui**.

2) Selectați **Organizare** sau **Persoană** fila și bifați caseta organizației sau persoanei dorite.

Organizațiile sau persoanele selectate vor fi listate pe pagina din dreapta.

3) Setati data de expirare pentru programul de schimb.

4) Setati alți parametri pentru program.

Înregistrarea nu este necesară

Persoanele din acest program nu trebuie să se înregistreze când vin la serviciu.

Check-out nu este necesar

Persoanele din acest program nu trebuie să facă check-out când își încheie munca.

Programat de sărbători

De sărbători, acest program este încă în vigoare, iar persoanele trebuie să meargă la serviciu conform programului.

Eficient pentru ore suplimentare

Orele suplimentare ale persoanelor vor fi înregistrate pentru acest program.

5) Faceți clic **Salva** pentru a salva programul rapid al schimburilor.

8.11.4 Gestionarea programului schimburilor

Munca în schimburi este o practică de angajare concepută pentru a folosi toate cele 24 de ore ale ceasului în fiecare zi a săptămânii. Practica vede de obicei ziua împărțită în ture, perioade stabilite de timp în care diferitele ture își îndeplinesc sarcinile.

Puteți seta programul departamentului, programul persoanelor și programul temporar.

Stabiliți programul departamentului

Puteți seta programul de ture pentru un departament și toate persoanele din departament vor fi alocate cu programul de ture.

Înainte de a începe

În modulul Time & Attendance, lista departamentelor este aceeași cu organizația. Ar trebui să adăugați mai întâi organizația și persoanele în modulul Persoană. Vedeți **Managementul persoanelor** pentru detalii.

Pași

1. Clic **Timp și prezență** → **Programul schimburilor** pentru a intra în pagina de gestionare a programului de schimb.
2. Clic **Programul departamentului** pentru a intra pe pagina Programul departamentului.
3. Selectați departamentul din lista organizației din stânga.



Nota

Dacă **Includeți suborganizație** este bifat, la selectarea organizației, suborganizațiile acesteia sunt selectate în același timp.

4. Selectați schimbarea din lista verticală.
5. **Opțional:** Permite **Programe de schimburi multiple** și selectați perioada (perioadele) de timp efectivă din orele adăugate pentru persoane.



Nota

Acesta este disponibil doar pentru ture cu un singur orar.

Programe de schimburi multiple

Conține mai mult de un orar. Persoana poate face check-in/out în oricare dintre ore și prezența va fi efectivă.

În cazul în care programul de schimburi multiple conține trei ore: 00:00 - 07:00, 08:00 - 15:00 și 16:00 - 23:00. Prezența persoanei care adoptă acest program în schimburi multiple va fi efectivă în oricare dintre cele trei ore. Dacă persoana face check-in la ora 07:50, se va aplica cel mai apropiat orar 08:00 - 15:00 pentru prezența persoanei.

6. Setati data de început și data de încheiere.

7. Setati alți parametri pentru program.

Înregistrarea nu este necesară

Persoanele din acest program nu trebuie să se înregistreze când vin la serviciu.

Check-out nu este necesar

Persoanele din acest program nu trebuie să facă check-out când își încheie munca.

Programat de sărbători

De sărbători, acest program este încă în vigoare, iar persoanele trebuie să meargă la serviciu conform programului.

Efficient pentru ore suplimentare

Orele suplimentare ale persoanelor vor fi înregistrate pentru acest program.

8.ClicSalva.

Setați programul persoanei

Puteți atribui programul de schimb uneia sau mai multor persoane. De asemenea, puteți vizualiza și edita detaliile programului persoanei.

Înainte de a începe

Adăugați departament și persoană în modulul Persoană. Vedeți *Managementul persoanelor* pentru detalii.

Pași



Nota

Programul persoanei are prioritate mai mare decât programul departamentului.

- 1.Clic**Timp și prezență** → **Programul schimburilor** pentru a intra în pagina Programul schimburilor.
 - 2.Clic**Programul persoanei** pentru a intra pe pagina Programul persoanei.
 - 3.Selectați organizația și selectați persoana (persoanele).
 - 4.Selectați schimbarea din lista verticală.
 5. **Opțional:** Permite **Programe de schimburi multiple** și selectați perioada (perioadele) de timp efectivă din orele adăugate pentru persoane.
-



Nota

Acesta este disponibil doar pentru ture cu un singur orar.

Programe de schimburi multiple

Conține mai mult de un orare. Persoana poate face check-in/out în oricare dintre orare și prezența va fi efectivă.

În cazul în care programul de schimburi multiple conține trei orare: 00:00 - 07:00, 08:00 - 15:00 și 16:00 - 23:00. Prezența persoanei care adoptă acest program în schimburi multiple va fi efectivă în oricare dintre cele trei orare. Dacă persoana face check-in la ora 07:50, se va aplica cel mai apropiat orar 08:00 - 15:00 pentru prezența persoanei.

6.Setați data de început și data de încheiere.

7.Setați alți parametri pentru program.

Înregistrarea nu este necesară

Persoanele din acest program nu trebuie să se înregistreze când vin la serviciu.

Check-out nu este necesar

Persoanele din acest program nu trebuie să facă check-out când își încheie munca.

Programat de sărbători

De sărbători, acest program este încă în vigoare, iar persoanele trebuie să meargă la serviciu conform programului.

Efficient pentru ore suplimentare

Orele suplimentare ale persoanelor vor fi înregistrate pentru acest program.

8.ClicSalva.

Setați programul temporar

Puteți adăuga un program temporar pentru persoana respectivă, iar persoanei i se va atribui temporar programul de schimb. De asemenea, puteți vizualiza și edita detaliile programului temporar.

Înainte de a începe

Adăugați departament și persoană în modulul Persoană. Vedeți *Managementul persoanelor* pentru detalii.

Pași



Nota

Programul temporar are prioritate mai mare decât orarul departamentului și orarul personal.

- 1.Clic**Timp și prezență** → **Programul schimburilor** pentru a intra în pagina de gestionare a programului de schimb.
- 2.Clic**Program temporar** pentru a intra pe pagina Program temporar.
- 3.Selectați organizația și selectați persoana (persoanele).
- 4.Faceți clic pe o dată sau faceți clic și trageți pentru a selecta mai multe date pentru programarea temporară.
- 5.Selectați **Zi de lucru** sau **Non-zi de lucru** din lista derulantă.

Dacă **Non-zi de lucru** este selectat, trebuie să setați următorii parametri.

Calculat ca

Selectați nivelul normal sau orele suplimentare pentru a marca starea de prezență pentru programul temporar.

Orarul

Selectați un orar din lista derulantă. **Program**

de schimburi multiple

Conține mai mult de un orare. Persoana poate face check-in/out în oricare dintre orare și prezența va fi efectivă.

În cazul în care programul de schimburi multiple conține trei orare: 00:00 - 07:00, 08:00 - 15:00 și 16:00 - 23:00. Prezența persoanei care adoptă acest program de ture multiple va fi

efectiv în oricare dintre cele trei orare. Dacă persoana face check-in la ora 07:50, se va aplica cel mai apropiat orar 08:00 - 15:00 pentru prezența persoanei.

Regulă

Setați altă regulă pentru program, cum ar fi **Înregistrarea nu este necesară**, și **Check-out nu este necesar**.

6. Clic Salva.

Verificați programul schimburilor

Puteți verifica programul de schimb în modul calendar sau listă. De asemenea, puteți edita sau șterge programul de schimb.

Pași

1. Clic **Timp și prezență** → **Programul schimburilor** pentru a intra în pagina de gestionare a programului de schimb.
2. Selectați organizația și persoana (persoanele) corespunzătoare.
3. Faceți clic pe  sau  pentru a vizualiza programul turelor în modul calendar sau listă.

Calendaristic

În modul calendar, puteți vizualiza programul de schimb pentru fiecare zi dintr-o lună. Puteți face clic pe programul temporar pentru o zi pentru a-l edita sau șterge.

Listă

În modul listă, puteți vizualiza detaliile programului de ture despre o persoană sau organizație, cum ar fi numele schimbului, tipul, perioada efectivă și așa mai departe. Verificați programul(e) turelor și faceți clic **Șterge** pentru a șterge programul(e) de schimb selectat(e).

8.11.5 Corecți manual înregistrarea de check-in/out

Dacă starea de prezență nu este corectă, puteți corecta manual înregistrarea de check-in sau check-out. De asemenea, puteți edita, șterge, căuta sau exporta înregistrarea de check-in sau check-out.

Înainte de a începe

- Ar trebui să adăugați organizații și persoane în modulul Persoană. Pentru detalii, consultați **Managementul persoanelor**.
- Starea de prezență a persoanei este incorectă.

Pași

1. Clic **Timp și prezență** → **Gestionarea prezenței** pentru a intra pe pagina de gestionare a prezenței.
2. Clic **Check-in/out corect** pentru a intra adăugând pagina de corecție de check-in/out.
3. Selectați persoana din lista din stânga pentru corectare.
4. Selectați data corectării.
5. Setări parametrii de corecție de check-in/out.
 - Selecta **Check-in** și setați ora efectivă de începere a lucrului.
 - Selecta **Verifică** și setați ora reală de sfârșit de lucru.

Nota

Puteți da clic  pentru a adăuga mai multe articole de check-in/out. Pot fi cel mult 8 articole de check-in/out sprijinit.

6. Opțional: Introduceți informațiile despre observație după cum doriți.

7. Clic **Salva**.

8. Opțional: După adăugarea corecției de check-in/out, efectuați una dintre următoarele operațiuni.

Vedere Clic  sau  pentru a vizualiza informațiile adăugate privind gestionarea prezenței în calendar sau listă modul.

Nota

În modul calendar, trebuie să faceți clic **Calcula** pentru a obține statutul de prezență al persoanei într-o lună.

Edita

- În modul calendar, faceți clic pe eticheta aferentă datei pentru a edita detaliile.
- În modul listă, faceți dublu clic pe fișierul aferent în coloana Data, Tip de manipulare, Ora sau Observație pentru a edita informațiile.

Șterge Ștergeți elementele selectate.

Export Exportați detaliile de gestionare a prezenței pe computerul local.

Nota

Detaliile exportate sunt salvate în format CSV.

8.11.6 Adăugați concediu și călătorie de afaceri

Puteți adăuga concediu și călătorie de afaceri atunci când angajatul dorește să ceară concediu sau să plece într-o călătorie de afaceri.

Înainte de a începe

Ar trebui să adăugați organizații și persoane în modulul Persoană. Pentru detalii, consultați **Managementul persoanelor**.

Pași

1. Clic **Timp și prezență** → **Gestionarea prezenței** pentru a intra pe pagina de gestionare a prezenței.
 2. Clic **Aplicați pentru concediu/călătorie de afaceri** pentru a intra adăugând pagina concediu/călătorie de afaceri.
 3. Selectați o persoană din lista din stânga.
 4. Setati data(le) concediului sau călătoriei dvs. de afaceri.
 5. Selectați tipul de concediu major și tipul de concediu minor din lista derulantă.
-

Nota

Puteți seta tipul de concediu în Setări de prezență. Pentru detalii, consultați **Configurați tipul de concediu**.

6. Stabiliți timpul pentru concediu.

7. **Opțional:** Introduceți informațiile despre observație după cum doriți.

8. ClicSalva.

9. **Opțional:** După adăugarea concediului și călătoriei de afaceri, efectuați una dintre următoarele operațiuni.

Vedere Clic  **Salva**  pentru a vizualiza informațiile adăugate privind gestionarea prezenței în calendar sau listă modul.



Nota

În modul calendar, trebuie să faceți clic **Calcula** pentru a obține statutul de prezență al persoanei într-o lună.

Edita

- În modul calendar, faceți clic pe eticheta aferentă datei pentru a edita detaliile.
- În modul listă, faceți dublu clic pe coloana înregistrată în Data, Tipul de manipulare, Ora sau Observație pentru a edita informațiile aferente.

Șterge Ștergeți elementele selectate.

Export Exportați detaliile de gestionare a prezenței pe computerul local.



Nota

Detaliile exportate sunt salvate în format CSV.

8.11.7 Calculați datele de prezență

Trebuie să calculați datele de prezență înainte de a căuta și vizualiza prezentarea generală a datelor de prezență, a datelor detaliate de prezență ale angajaților, a datelor de prezență anormale ale angajaților, a datelor de lucru suplimentare ale angajaților și a jurnalului de trecere a cardului.

Calculați automat datele de prezență

Puteți seta un program astfel încât clientul să poată calcula automat datele de prezență la ora pe care ați configurat-o în fiecare zi.

Pași



Nota

Acesta va calcula datele de prezență până în ziua precedentă.

1. Intrați în modulul Timp și prezență.

2. Clic **Setări de prezență** → **Regulă generală**.

3. În zona Auto-Calculate Attendance, setați ora la care doriți ca clientul să calculeze datele în fiecare zi.

4. Clic **Salva**.

Calculați manual datele de prezență

Puteți calcula manual datele privind prezența setând intervalul de date.

Pași

1. Intrați în modulul Timp și prezență.

2. Clic **Statistici de prezență** → **Calcul**.

3. Setați ora de începere și ora de încheiere pentru a defini intervalul de date de prezență.

4. Setați alte condiții, inclusiv departamentul, numele, ID-ul persoanei și statutul de prezență.

5. Clic **Calcula**.



Nota

Poate calcula datele de prezență numai în termen de trei luni.

6. Efectuați una dintre următoarele operații.

Check-in/out corect

Clic **Check-in/out corect** pentru a adăuga o corecție de check-in/out.

Selecționați Elemente către

Afișa

Faceți clic pe sau faceți clic dreapta pe titlurile diferitelor articole pentru a selecta elementele care vor fi afișate în raport.

Generați raport

Clic **Raport** pentru a genera raportul de prezență. Clic **Export**

Raport de export

pentru a exporta datele de prezență pe computerul local.



Nota

Detaliile exportate sunt salvate în format .CSV.

8.11.8 Statistici de prezență

Puteți verifica înregistrarea originală de prezență, puteți genera și exporta raportul de prezență pe baza datelor de prezență calculate.

Obțineți o prezentare generală a datelor privind prezența angajaților

Puteți căuta și vizualiza înregistrările de prezență ale angajatului pe client, inclusiv timpul de prezență, starea prezenței, punctul de control etc.

Înainte de a începe

- Ar trebui să adăugați organizații și persoane în modulul Persoană, iar persoanele au carduri glisate. Pentru detalii, consultați **Managementul persoanelor**.
- Calculați datele de prezență.

Nota

- Clientul va calcula automat datele de prezență din ziua precedentă la ora 1:00 a doua zi.
 - Mențineți clientul în funcțiune la 1:00 am sau acesta nu poate calcula automat datele de prezență din ziua precedentă. Dacă nu sunt calculate automat, puteți calcula manual datele de prezență. Pentru detalii, consultați **Calculați manual datele de prezență**.
-

Pași

1. Intrați în modulul Timp și prezență.

2. Clic **Statistici de prezență** → **Înregistrare de prezență**.

3. Setați ora de începere a prezenței și ora de încheiere pe care doriți să le căutați.

4. Setați alte condiții de căutare, inclusiv departamentul, numele și ID-ul persoanei.

5. Selectați sursa de date ca **Înregistrări originale pe dispozitiv** sau **Înregistrări de manipulare manuală**.

6. Opțional: Clic **Obțineți evenimente de pe dispozitiv** pentru a obține datele de prezență de pe dispozitiv.

7. Opțional: Clic **Resetați** pentru a reseta toate condițiile de căutare și a edita din nou condițiile de căutare.

8. Clic **Căutare**.

Rezultatul este afișat pe pagină. Puteți vedea starea de prezență necesară a angajatului și punctul de control.

9. Opțional: După căutarea rezultatului, efectuați una dintre următoarele operații.

Generați raport	Clic Raport pentru a genera raportul de prezență. Clic
Raport de export	Export pentru a exporta rezultatele pe computerul local.
Export personalizat	Pentru detalii, consultați .

Generați un raport instantaneu

Acceptă generarea manuală a unei serii de rapoarte de prezență pentru a vizualiza rezultatele prezenței angajaților.

Înainte de a începe

Calculați datele de prezență.

Nota

Puteți calcula datele de prezență manual sau puteți seta programul astfel încât clientul să poată calcula datele automat în fiecare zi. Pentru detalii, consultați **Calculați datele de prezență**.

Pași

1. Intrați în modulul Timp și prezență.

2. Clic **Statistici de prezență** → **Raport**.

3. Selectați un tip de raport.

4. Selectați departamentul sau persoana pentru a vizualiza raportul de prezență.

5.Setați ora de începere și ora de încheiere în care datele de prezență vor fi afișate în raport.

6.Clic**Raport**pentru a genera raportul de statistici și a-l deschide.

Trimiteți raportul în mod regulat

Clientul acceptă mai multe tipuri de rapoarte și puteți predefini conținutul raportului și poate trimite raportul automat la adresa de e-mail pe care ați configurat-o.

Pași

1.Intrați în modulul Timp și prezență.

2.Clic**Statistici de prezență** → **Trimiteți periodic raport**.

3.Clic**Adăugap**pentru a intra în pagina de adăugare a raportului personalizat.

4.Setați conținutul raportului.

Numele raportului

Introduceți un nume pentru raport.

Tipul de raport

Selectați un tip de raport și acest raport va fi generat. **Ora raportului**

Ora care trebuie selectată poate varia în funcție de tipul de raport diferit.

Persoană

Selectați persoana (persoanele) adăugate ale căror înregistrări de prezență vor fi generate pentru raport.



Nota

Puteți vizualiza persoanele selectate în partea dreaptă a zonei Persoană.

5.Setați programul pentru a trimite automat raportul la adresa(e) de e-mail.



Nota

The**Trimitere automată a e-mailului**funcția este activată implicit.

1) Setați Perioada efectivă în timpul căreia clientul va trimite raportul la data(le) de trimitere selectată(e).

2) Selectați Data (Datele) de trimitere la care clientul va trimite raportul.

3) Setați ora de trimitere la care clientul va trimite raportul.

Exemplu

Dacă setați perioada efectivă ca**2018/3/10 până la 2018/4/10**, selectați**vineri**ca dată de trimitere și setați ora de trimitere ca**20:00:00**, clientul va transmite raportul la ora 20.00 în zilele de vineri în perioada 2018/3/10 până în 2018/4/10.



Nota

Asigurați-vă că înregistrările de prezență sunt calculate înainte de ora de trimitere. Puteți calcula datele de prezență manual sau puteți seta programul astfel încât clientul să poată calcula datele automat în fiecare zi. Pentru detalii, consultați **Calculați datele de prezență**.

4) Introduceți adresa de e-mail a destinatarului.



Nota

Pot fi adăugate până la 5 adrese de e-mail. Puteți da clic+pentru a adăuga o nouă adresă de e-mail.

5) **Opțional:** Clic **Previzualizare** pentru a vedea detaliile de e-mail.

6. Clic **Bine**.

7. **Opțional:** După adăugarea raportului personalizat, puteți efectua una sau mai multe dintre următoarele:

Editați raportul	Selectați un raport adăugat și faceți clic Edita pentru a-i edita setările.
Ștergeți raportul	Selectați un raport adăugat și faceți clic Șterge pentru a-l șterge.
Generați raport	Selectați un raport adăugat și faceți clic Raport pentru a genera raportul instantaneu și puteți vizualiza detaliile raportului.

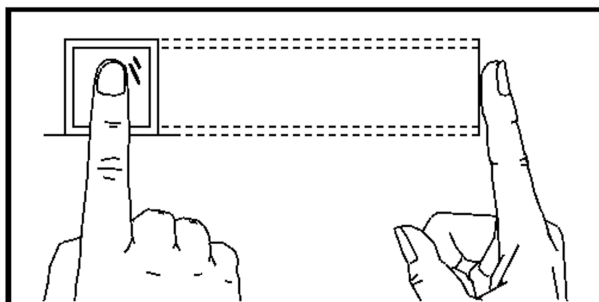
Anexa A. Sfaturi pentru scanarea amprente

Degetul recomandat

Degetul arătător, degetul mijlociu sau al treilea deget.

Scanare corectă

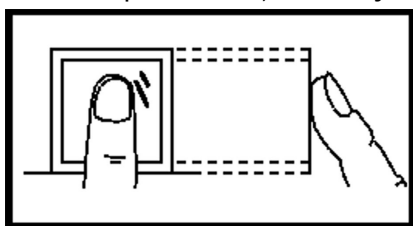
Figura afișată mai jos este modalitatea corectă de scanare a degetului:



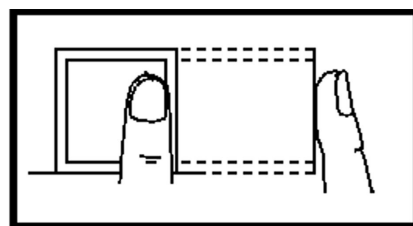
Ar trebui să apăsați cu degetul pe scanner pe orizontală. Centrul degetului scanat trebuie să se alinieze cu centrul scannerului.

Scanare incorectă

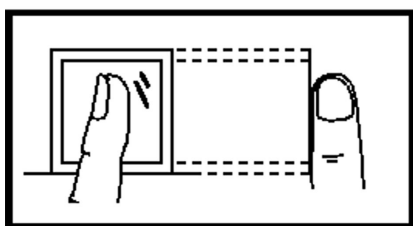
Cifrele de scanare a amprente afișate mai jos sunt incorecte:



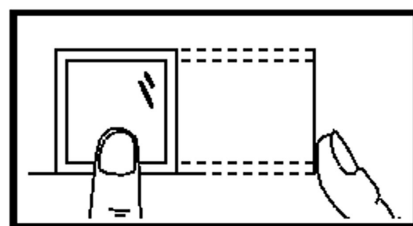
Vertical



Edge I



Side



Edge II

Mediu

Scannerul trebuie să evite lumina directă a soarelui, temperaturile ridicate, condițiile umede și ploaia. Când este uscat, este posibil ca scannerul să nu recunoască cu succes amprenta dvs. Puteți sufla cu degetul și puteți scana din nou.

Alții

Dacă amprenta dvs. este superficială sau este dificil să vă scanați amprenta, vă recomandăm să utilizați alte metode de autentificare.

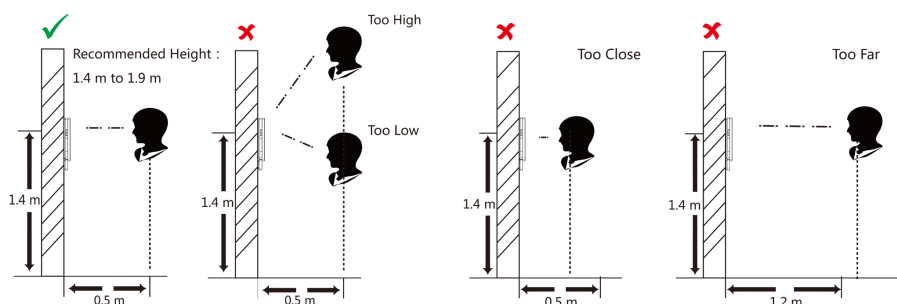
Dacă aveți răni la degetul scanat, este posibil ca scanerul să nu recunoască. Puteți schimba un alt deget și puteți încerca din nou.

Anexa B. Sfaturi la colectarea/compararea feței

Imagine

Poziția la colectarea sau compararea imaginii feței este următoarea:

Poziții (Distanța recomandată: 0,5 m)



Expresie

- Păstrează-ți expresia naturală atunci când colectezi sau compari imagini cu fețe, la fel ca expresia din imaginea de mai jos.



- Nu purtați pălărie, ochelari de soare sau alte accesorii care pot afecta funcția de recunoaștere facială.
- Nu vă lăsați părul să vă acopere ochii, urechile etc. și nu este permis machiajul intens.

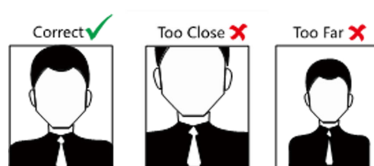
Postură

Pentru a obține o imagine a feței de bună calitate și precisă, poziționați-vă fața privind la camera atunci când colectați sau comparați imaginile feței.



Dimensiune

Asigurați-vă că fața dvs. este în mijlocul ferestrei de colectare.



Anexa C. Sfaturi pentru mediul de instalare

1. Valoarea de referință a iluminării sursei de lumină



Lumanare: 10 lux

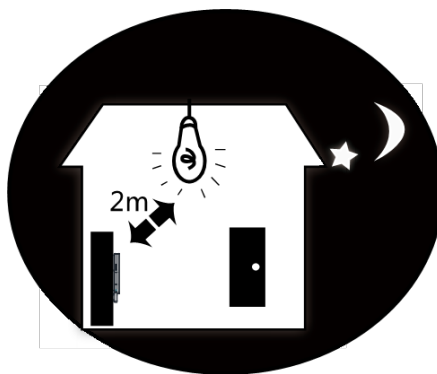
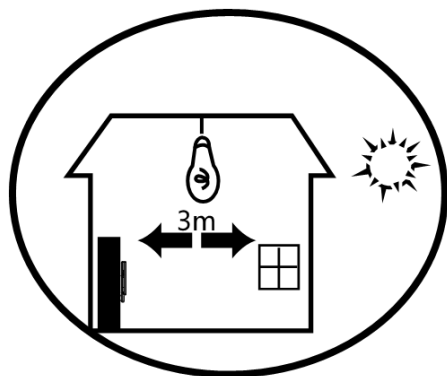


Bec: 100~850Lux

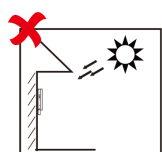


Lumina soarelui: peste 1200 lux

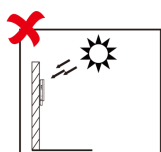
2. Instalați dispozitivul la cel puțin 2 metri distanță de lumină și la cel puțin 3 metri distanță de fereastră sau ușă.



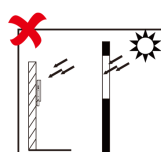
3. Evitați lumina de fundal, lumina directă și indirectă a soarelui



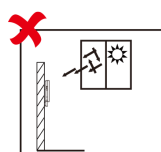
Backlight



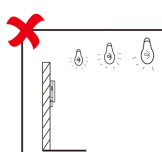
Direct Sunlight



Direct Sunlight through Window



Indirect Sunlight through Window



Close to Light

Anexa D. Dimensiunea

Dispozitiv cu modul de amprentă digitală

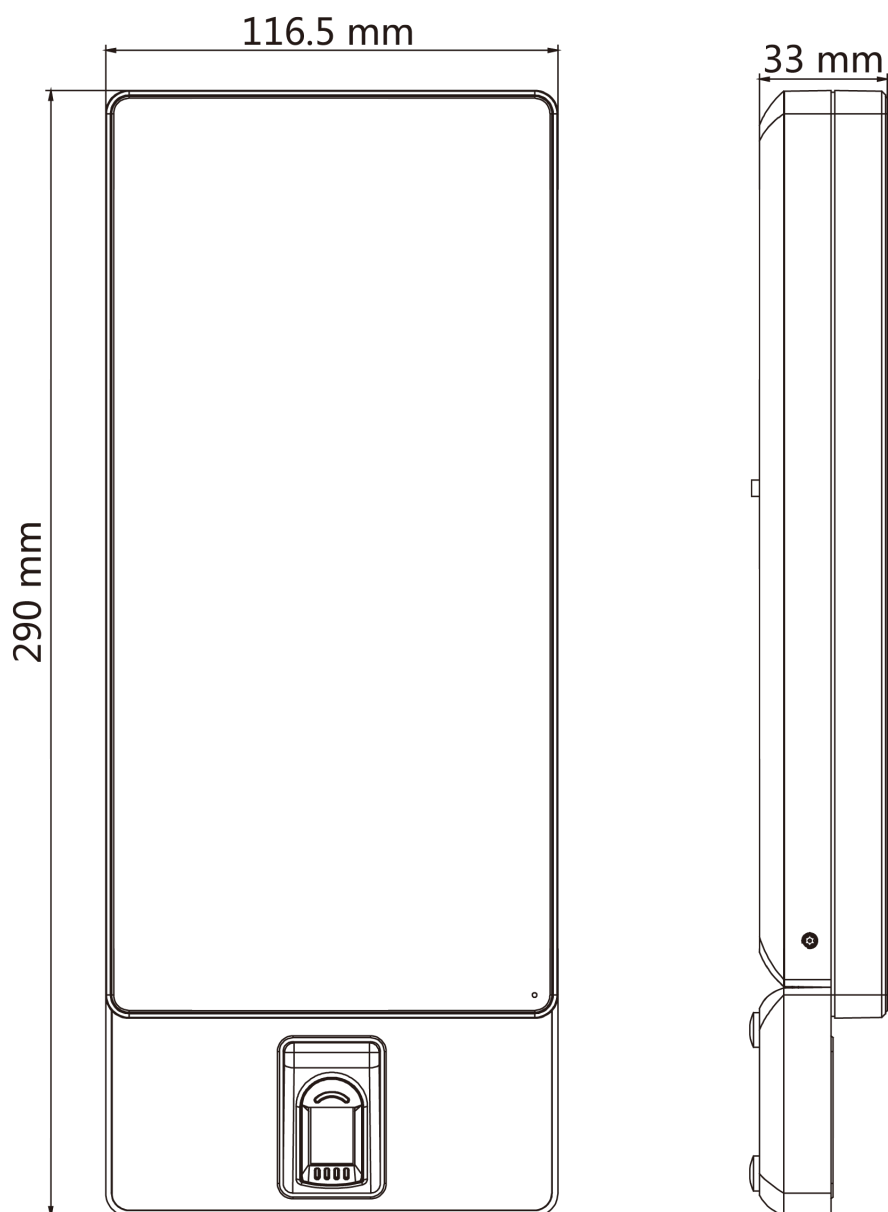


Figura D-1 Dispozitiv cu modul de amprentă digitală

Dispozitiv fără modul de amprentă

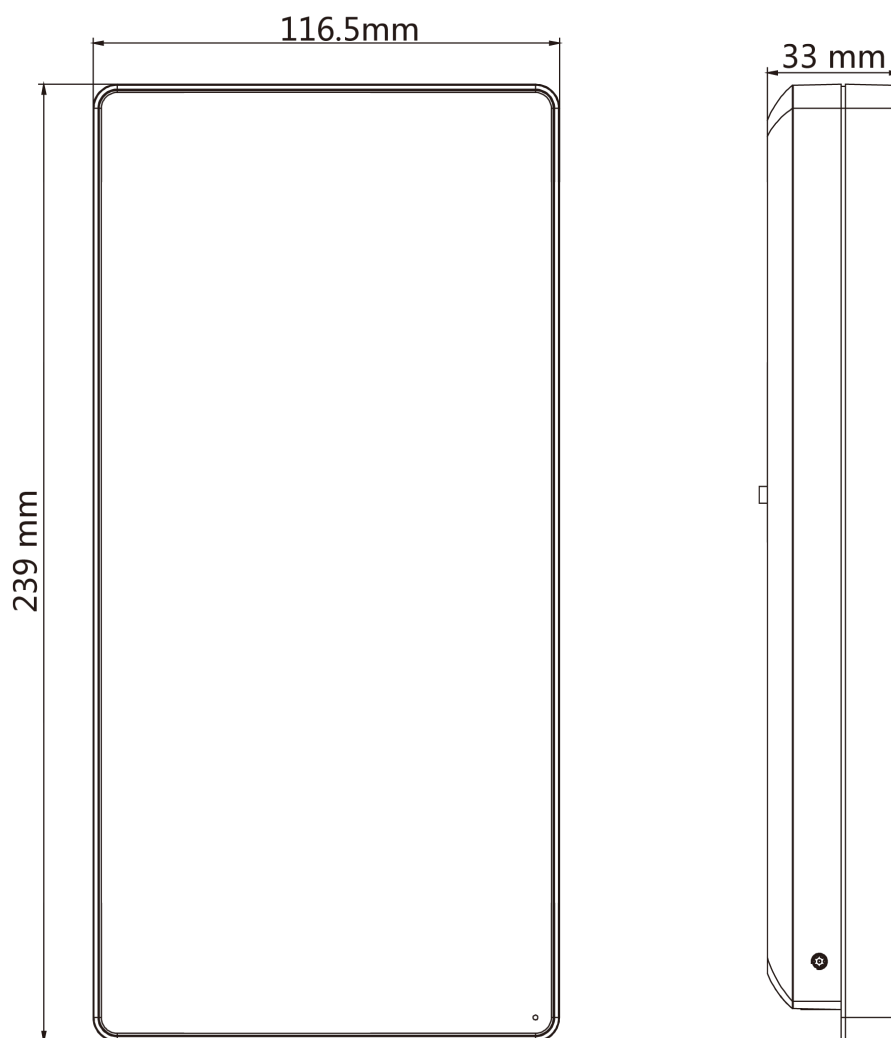


Figura D-2 Dispozitiv fără modul de amprentă

Anexa E. Matricea și dispozitivul de comunicare Comanda

Matricea de comunicare

Scanați următorul cod QR pentru a obține matricea de comunicare a dispozitivului.

Rețineți că matricea conține toate porturile de comunicație ale dispozitivelor de control acces și video interfon Hikvision.



Figura E-1 Matricea de comunicare a codului QR

Comanda dispozitivului

Scanați următorul cod QR pentru a obține comenzile comune ale portului serial al dispozitivului.

Rețineți că lista de comenzi conține toate comenzile de porturi seriale utilizate în mod obișnuit pentru toate dispozitivele de control al accesului și videointerfon Hikvision.



Figura E-2 Comanda dispozitivului



See Far, Go Further