Hub de alarmă

Manualul utilizatorului

ZHEJIANG DAHUA VISION TECHNOLOGY CO.LTD. V2.0.0

cuvânt înainte

General

Acest manual prezintă instalarea, funcțiile și operațiunile hub-ului de alarmă (denumit în continuare „hub”). Citiți cu atenție înainte de a utiliza dispozitivul și păstrați manualul în siguranță pentru referințe ulterioare.

Instructiuni de siguranta

Următoarele cuvinte de semnalizare pot apărea în manual.

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

Istoricul revizuirilor

Versiune	Conținutul revizuirii	Timpul de eliberare
V2.0.0	● S-au adăugat configurații de rețea. ● S-au adăugat evenimente și descrieri de eșec de armare. ● S-au adăugat coduri și descrieri ale evenimentelor SIA.	noiembrie 2022
V1.1.0	● S-au adăugat operațiuni în aplicația COS Pro și DMSS. ● S-a adăugat managementul utilizatorilor. ● Imagini actualizate. ● Descrieri actualizate ale parametrilor.	februarie 2022
V1.0.0	Prima aparitie.	octombrie 2021

Notificare privind protecția confidențialității

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

Despre Manual

- Manualul este doar pentru referință. Pot fi găsite mici diferențe între manual și produs.
- Nu suntem răspunzători pentru pierderile suferite din cauza utilizării produsului în moduri care nu sunt în conformitate cu manualul.
- Manualul va fi actualizat în conformitate cu cele mai recente legi și reglementări ale jurisdicțiilor aferente. Pentru informații detaliate, consultați manualul de utilizare pe hârtie, utilizați CD-ROM-ul nostru, scanați codul QR sau vizitați site-ul nostru oficial. Manualul este doar pentru referință. S-ar putea găsi mici diferențe între versiunea electronică și versiunea pe hârtie.
- Toate modelele și software-ul pot fi modificate fără notificare prealabilă în scris. Actualizările de produs pot duce la apariția unor diferențe între produsul real și manual. Vă rugăm să contactați serviciul pentru clienți pentru cel mai recent program și documentație suplimentară.
- Pot exista erori în imprimare sau abateri în descrierea funcțiilor, operațiunilor și datelor tehnice. Dacă există vreo îndoială sau dispută, ne rezervăm dreptul la explicații finale.
- Actualizați software-ul de citire sau încercați alt software de citire general dacă manualul (în format PDF) nu poate fi deschis.
- Toate mărcile comerciale, mărcile comerciale înregistrate și numele companiilor din manual sunt proprietăți ale proprietarilor respectivi.
- Vă rugăm să vizitați site-ul nostru web, să contactați furnizorul sau serviciul pentru clienți dacă apar probleme în timpul utilizării dispozitivului.
- Dacă există vreo incertitudine sau controversă, ne rezervăm dreptul la explicații finale.

Măsuri de protecție și avertismente importante

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

Cerințe de funcționare

- Asigurați-vă că sursa de alimentare a dispozitivului funcționează corect înainte de utilizare.
- Nu trageți cablul de alimentare al dispozitivului în timp ce acesta este pornit.
- Utilizați dispozitivul numai în intervalul de putere nominală.
- Transportați, utilizați și depozitați dispozitivul în condiții de umiditate și temperatură permise.
- Preveniți stropirea sau picurarea lichidelor pe dispozitiv. Asigurați-vă că nu există obiecte pline cu lichid deasupra dispozitivului pentru a evita curgerea lichidelor în el.
- Nu dezasamblați dispozitivul.

Cerințe de instalare

WARNING

- Conectați dispozitivul la adaptor înainte de pornire.
- Respectați cu strictețe standardele locale de siguranță electrică și asigurați-vă că tensiunea din zonă este constantă și este conformă cu cerințele de alimentare ale dispozitivului.
- Nu conectați dispozitivul la mai mult de o sursă de alimentare. În caz contrar, dispozitivul se poate deteriora.

- Respectați toate procedurile de siguranță și purtați echipamentul de protecție necesar pentru utilizare în timpul lucrului la înălțime.
- Nu expuneți dispozitivul la lumina directă a soarelui sau la surse de căldură.
- Nu instalați dispozitivul în locuri umede, cu praf sau cu fum.
- Instalați dispozitivul într-un loc bine ventilat și nu blocați ventilatorul dispozitivului.
- Utilizați adaptorul de alimentare sau sursa de alimentare a carcasei furnizate de producătorul dispozitivului.
- Sursa de alimentare trebuie să respecte cerințele ES1 din standardul IEC 62368-1 și să nu fie mai mare decât PS2. Rețineți că cerințele de alimentare sunt supuse etichetei dispozitivului.
- Conectați aparatele electrice de clasa I la o priză cu împământare de protecție.

Cuprins

1. Introducere

1.1 Prezentare generală

Hubul de alarmă este un dispozitiv central în sistemul de securitate, care controlează funcționarea tuturor accesoriilor conectate. Dacă sistemul de securitate detectează prezența, intrarea sau încercarea de intrare a unui intrus în zona armată, hub-ul va primi semnalele de alarmă de la detectoare și apoi va alerta utilizatorii.

1.2 Specificații tehnice

Această secțiune conține specificațiile tehnice ale dispozitivului. Vă rugăm să consultați cele care corespund modelului dvs.

Tabelul 1-1 Specificații tehnice

Tip	Parametru	Descriere
Port	Reţea	1 port Ethernet auto-adaptabil RJ-45 10 M/100 M
	GSM	SIM unic (GSM:900/1800 MHz); dual SIM single standby
	LTE	Single SIM (GSM: 900/1800 MHz, WCDMA: B1/B5/B8, LTE-FDD: B1/B3/B5/B7/B8/B20, LTE-TDD:B38/B40/B41); dual SIM single standby
	Baterie	Port baterie 12 V
	Indicator luminos	1 pentru stări multiple (alarma, armarea, dezarmarea, conectarea în rețea și funcționarea defectuoasă)
	Buton	1 × resetare, 1 × alimentare, 1 × AP
	Buzzer	Incorporat
	Tamper	1 port de manipulare a carcasei pentru panoul de control al alarmei
Funcţie	Notificare prin SMS	Alarmă prin SMS (până la 5 numere de telefon) Disponibil doar pe anumite modele.
	Apel telefonic Notificare	Da (până la 5 numere de telefon) Disponibil doar pe anumite modele.
	Legătura video	da
	Protocol de rețea	TCP/IP, inclusiv PPTP, L2TP, DHCP, UPNP și NTP
	Upgrade de la distanță	Actualizare cloud
	Configurare Metodă	App
	Înarmați și dezarmați Metodă	Aplicație, tastatură, telecomandă, program

Tip	Parametru	Descriere	
	Un numar de Periferice	Max. Periferice wireless cu 150 de canale (6 sirene, 64 telecomenzi wireless, 4 repetoare și 8 tastaturi)	
	Zonă	32 de zone (camere)	
	Putere management	Comutare automată între alimentarea principală și alimentarea de stocare	
		Alarma pentru pierderea curentului principal	
		Alarmă pentru pierderea bateriei și defecțiunea tensiunii bateriei	
	Jurnalele evenimentelor	Max. 400	
	Pana de curent Protectie pentru Configurat Parametrii	da	
	Utilizator management	Max. 8 utilizatori: 1 instalator, 1 administrator, 6 utilizatori generali	
	Interogare	Căutarea mesajelor push, starea dispozitivului și versiunea programului. Detectarea puterii semnalului.	
RF	Frecvența purtătoarei	DHI-ARA3000H-FW2 (868)/DHI-ARA3000H-GW2 (868)/DHI-ARA3000H-W2 (868): 868,0 MHz–868,6 MHz	DHI-ARA3000H-FW2/DHI-ARA3000H-GW2/DHI-ARA3000H-W2: 433,1 MHz–434,6 MHz
	Comunicare Distanţă	DHI-ARA3000H-FW2 (868)/DHI-ARA3000H-GW2 (868)/DHI-ARA3000H-W2 (868): Până la 2.000 m (6.561,68 ft) într-un spațiu deschis	DHI-ARA3000H-FW2/DHI-ARA3000H-GW2/DHI-ARA3000H-W2: Până la 1.200 m (3.937,01 ft) într-un spațiu deschis
	Transmitere Putere	DHI-ARA3000H-FW2 (868)/DHI-ARA3000H-GW2 (868)/DHI-ARA3000H-W2 (868): Limită 25 mW	DHI-ARA3000H-FW2/DHI-ARA3000H-GW2/DHI-ARA3000H-W2: Limită 10 mW
	Comunicare Mecanism	În două sensuri	
	Mod de criptare	AES128	
	Frecvență Ţopăit	da	
	Interferență RF Detectare	Pentru o detecție de 60 de secunde, dacă interferența durează mai mult de 30 de secunde, sistemul raportează informațiile despre interferența RF.	
	Wifi	2,4 G	
Putere Livra	Tip PS	Tip A	
	Puterea principala	12 VDC, 1,5 A	
	Capacitatea bateriei	2x 3,6 V/2150 mAh	

Tip	Parametru	Descriere
	Baterie Standby	Până la 12 h Când sunt îndeplinite următoarele condiții, timpul de așteptare poate ajunge la 12 ore: ● Se conectează prin Wi-Fi, GPRS/3G/4G. ● Se conectează la ARC și intervalul bătăilor inimii este de 1800 de secunde. ● Se conectează la 8 intrări și 1 sirenă. ● Se conectează la cloud.
	Tip baterie	Tip baterie: polimer litiu-ion reîncărcabil încorporat; model baterie: 18650
	Max. actual disponibil	3,5 A
	Putere Consum	Max. 15 W
	Actual Consum	Normal: 220 mA; alarma: 300 mA
	Baterie descărcată Pragul bateriei	3,5 VDC
	Restaurare baterie Prag	3,7 VDC
	Tensiune de eliberare	＜3.358 V
	Reîncărcarea bateriei Timp	80% aprox. 15 h
ARC Semnalizarea	Categoria ATS	DP2/SP2 (LAN/Wi-Fi și GPRS/4G)
	Recunoaște-mă nt Operațiunea	A trece prin
	Protocoale	SIA-DC09
	Primar Calea de transmisie	LAN/Wi-Fi (NU 50136-2)
	Secundar Calea de transmisie	GPRS/4G
	Notificare Echipamente	C/E/F

Tip	Parametru	Descriere	
Certificari		DHI-ARA3000H-FW2 (868)/DHI-ARA3000H-GW2 (868)/DHI-ARA3000H-W2 (868): EN 50131-1:2006+A1:2009+A2:2017+A3:2020 EN 50131-3:2009 EN 50131-6:2017 EN 50131-5-3:2017 EN 50131-10: 2014 EN 50136-2: 2013 Gradul de securitate 2 Clasa de mediu II CE	DHI-ARA3000H-FW2/DHI-ARA3000H-GW2/DHI-ARA3000H-W2: FCC CE

Tabelul 1-2 Categoria ATE

A MANCAT Categorie	Raportare Timp	Protocoale	Dispozitive de comunicare			Comunicare Dispozitiv de utilizat
			PSTN	2G/3G	IP	
SP2	25 h	Standard	√			Cecul marcat comunicare dispozitiv
SP3	30 minute	Standard		√	√	Doar unul dintre cele două bifate comunicare dispozitive
SP4	3 min	Criptat		√	√	Doar unul dintre cele două bifate comunicare dispozitive
SP5	90 s	Criptat		√	√	Doar unul dintre cele două bifate comunicare dispozitive
DP1	25 h	Standard	√	√	√	Doar două dintre trei bifate comunicare dispozitive
DP2	30 minute	Standard	√	√	√	Doar două dintre trei bifate comunicare dispozitive
DP3	3 min	Criptat		√	√	Cei doi verifică marcat comunicare dispozitive

A MANCAT Categorie	Raportare Timp	Protocoale	Dispozitive de comunicare			Comunicare Dispozitiv de utilizat
			PSTN	2G/3G	IP	
DP4	90 s	Criptat		√	√	Cei doi verifică marcat comunicare dispozitive

ATE: Echipament de transmisie a alarmei.

SPx (Single Path): O valoare care indică nivelul de performanță atins de un singur dispozitiv de comunicație, conform standardului EN 50136–1.

DPx (Double Path): O valoare care indică nivelul de performanță atins printr-o combinație a două dispozitive de comunicație, conform standardului EN 50136–1.

Timpul de raportare: Timpul de raportare este prescris pe baza standardului fiecărui nivel de performanță. Timpul de raportare este timpul maxim disponibil pentru a raporta atunci când un dispozitiv de transmitere a alarmei eșuează. Dispozitivele de transmisie de alarmă îndeplinesc această cerință prin raportarea regulată a stării lor printr-o funcție de testare simbolică specifică.

Protocoale: Indică nivelul de securitate al protocoalelor care vor fi utilizate pentru notificarea erorilor. Protocoalele standard și protocoalele vocale sunt criptate. Protocoalele de înaltă securitate sunt criptate cu o cheie de criptare AES pe 128 biți sau AES pe 256 biți.

Dispozitive de comunicare: Dispozitive de comunicare implementate.

Dispozitive de comunicație care urmează să fie utilizate: indică numărul și care dispozitive de comunicație vor fi utilizate în funcție de categoria ATE.

Tabelul 1-3 Specificații tehnice

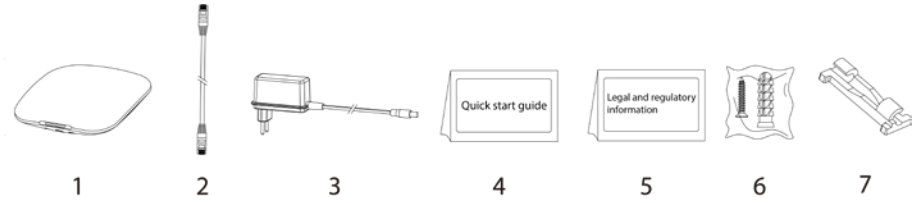
Specificație tehnică	Descriere
Clasificarea ACE	Tip A
Clasa de mediu	II
Tensiunea de alimentare	12 VDC, 1,5 A
dimensiunile produsului	163,0 mm× 163,0 mm× 32,0 mm (6,42" × 6,42" × 1,26")
Dimensiunile ambalajului	219,0 mm× 187,0 mm× 91,0 mm (8,62" × 7,36" × 3,58")
Temperatura de Operare	– 10 °C până la +50 °C (+14 °F până la +122 °F) – 10 °C până la +40 °C (+14 °F până la 104 °F) (temperatura certificată)
Umiditate	10%–90% (RH)
Greutate netă	0,38 kg (0,84 lb)
Greutate brută	0,8 kg (1,76 lb)
Carcasa	PC + ABS

1.3 Lista de verificare

Verificați pachetul conform următoarei liste de verificare. Dacă găsiți ceva deteriorat sau pierdut,

contactați serviciul pentru clienți.

Figura 1-1 Lista de verificare



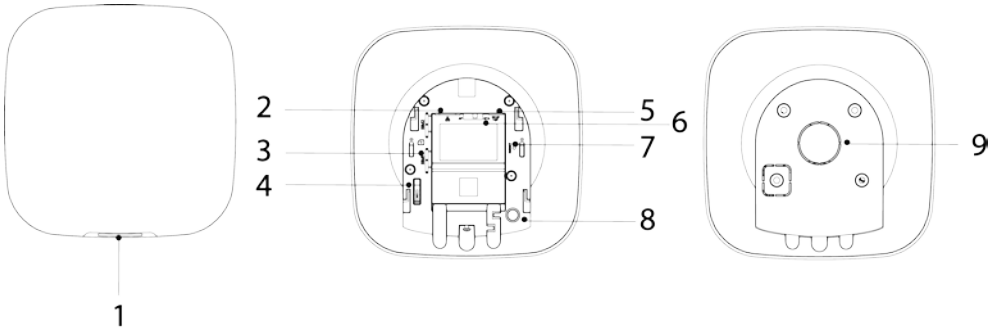
Tabelul 1-4 Lista de verificare

Nu.	Nume articol	Cantitate	Nu.	Nume articol	Cantitate
1	Hub de alarmă	1	5	Legal și de reglementare informație	1
2	Cablu	1	6	Pachet cu șuruburi	1
3	Adaptor	1	7	Clemă de fixare a firului	1
4	Ghid de inițiere rapidă	1	—	—	—

2 Proiectare

2.1 Aspectul

Figura 2-1 Aspect



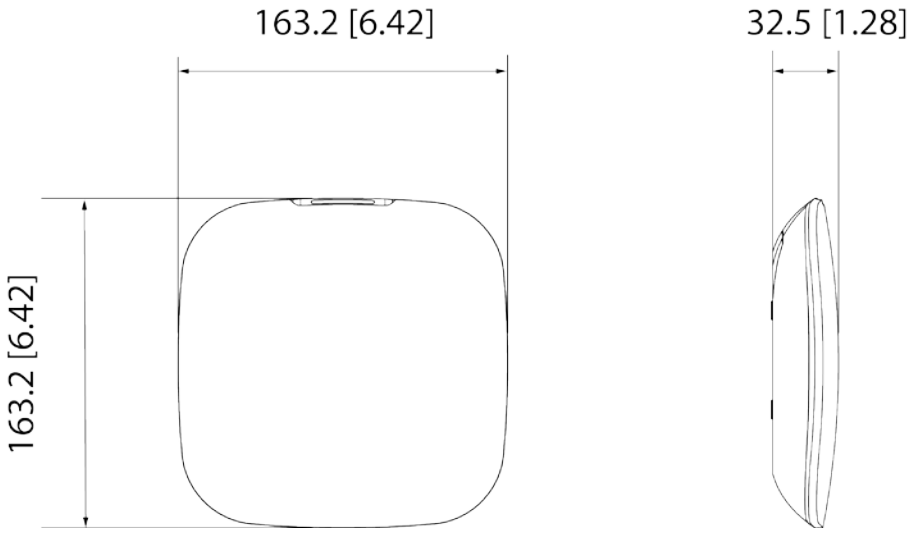
Tabelul 2-1 Structura

Nu.	Nume	Descriere
1	Indicator	● Verde intermitent lent: modul sensibilitate redusă. ● Verde intermitent: hub-ul începe să funcționeze. ● Galben continuu: Nu s-a putut conecta la cloud. ● Verde continuu: modul de dezarmare. ● Albastru continuu: modul de armare. ● Clipește roșu: evenimentul de alarmă a fost declanșat. ● Galben intermitent: a fost detectată o defecțiune. ● Se aprinde intermitent în albastru: se execută configurația AP sau hub-ul se împerechează cu periferice. ● Clipește rapid în albastru: modul de emitere a cardului.
2	Mufa cablu Ethernet	Conectați hub-ul la Ethernet.
3	Slot pentru micro SIM 1/2	Instalați cardul principal în primul slot și cardul de așteptare în al doilea slot. ● Acceptă cartele SIM duale și standby unic. ● Cardurile SIM permit hub-ului să utilizeze date celulare și să împingă notificări de alarmă. ● Cardurile SIM nu vor funcționa până când configurarea rețelei nu a făcut-o fost finalizat. ● Funcția SIM este disponibilă numai pe anumite modele.
4	Buton de manipulare	Când comutatorul de manipulare este eliberat, alarma de manipulare va fi declanșată.
5	Priză cablu de alimentare	Introduceți cablul de alimentare.
6	AP	Porniți AP, telefonul se va conecta la hotspot din hub, apoi va sincroniza numele de utilizator și parola Wi-Fi cu hub-ul.

Nu.	Nume	Descriere
7	Butonul de resetare	Apăsați și mențineți apăsat butonul timp de 10 secunde pentru a reporni hub-ul și a restabili setările implicite din fabrică.
8	Buton pornit/oprit	Apăsați și mențineți apăsat butonul timp de 2 secunde pentru a porni sau opri hub-ul.
9	Coperta din spate	Dacă capacul din spate este deschis, se va declanșa alarma de manipulare.

2.2 Dimensiuni

Figura 2-2 Dimensiuni (unitate: mm [inch])



3 Pornire

3.1 Utilizatori

Utilizatorii pot fi creați numai în aplicația DMSS și COS Pro. Clasificați utilizatorii în diferite roluri, astfel încât aceștia să poată avea diferite niveluri de acces pentru operarea dispozitivelor.

Nivel de acces utilizator

Tabelul 3-1 Nivel de acces utilizator

Utilizator	Nivel de acces
Utilizator administrator DMSS	L2
utilizator general DMSS	L2
Instalator	L3

- Instalator: instalatorii oferă utilizatorilor finali servicii de operare și întreținere. Acest rol trebuie să solicite permisiuni de la utilizatorul final (utilizator administrator DMSS) pentru a opera dispozitivul. Ei pot primi permisiuni, cum ar fi configurarea dispozitivului și gestionarea utilizatorilor.
- Utilizator administrator DMSS: utilizatorul administrator ar fi un utilizator final. Acest rol nu poate fi modificat și are permisiuni, cum ar fi configurarea dispozitivului și gestionarea utilizatorilor. Utilizatorii administratori DMSS nu au permisiunea de a configura dispozitivul atunci când instalatorii le împrumută hub-ul sau când îl încredințează instalatorului.
- Utilizator general DMSS: aceștia sunt utilizatorii cărora un utilizator administrator DMSS partajează dispozitive prin intermediul aplicației DMSS. Acest rol poate fi modificat și are numai permisiuni de bază, cum ar fi vizualizarea stării dispozitivului și armarea și dezarmarea camerelor.

Fluxul de afaceri

Mai jos este procesul de încredințare și partajare în aplicația DMSS și COS Pro. Instalatorii și utilizatorii finali pot urma procesul pentru a partaja și a încredința dispozitive.

Figura 3-1 Flux de afaceri (utilizator DMSS)

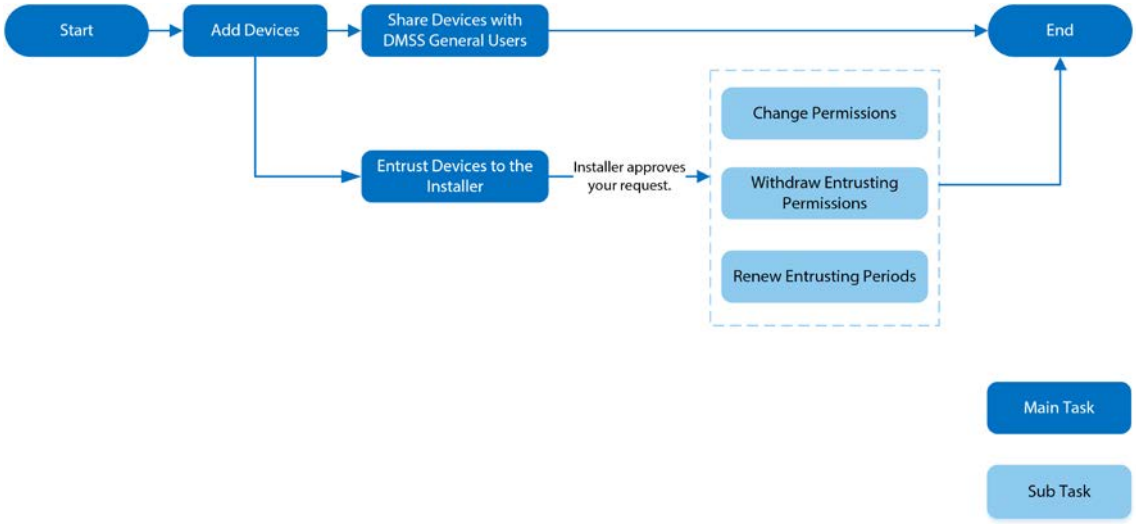
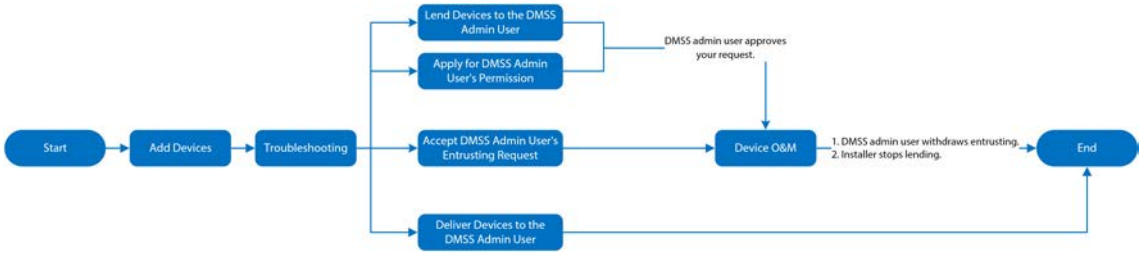


Figura 3-2 Fluxul afacerii (instalator)



3.2 Procesul de operare

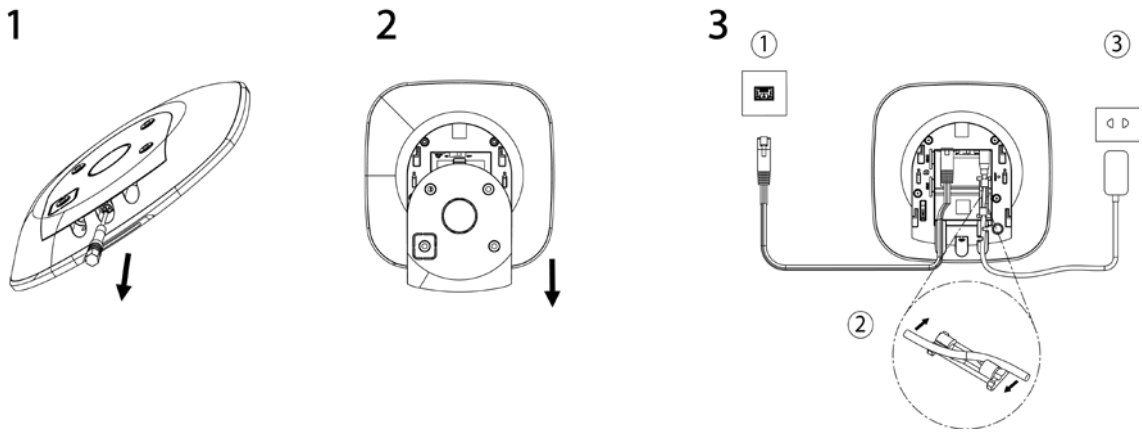
Urmați procedurile de mai jos pentru a porni sistemul de alarmă fără fir.

Figura 3-3 Procesul de operare

Aprinde

Conectați hub-ul la Ethernet și porniți hub-ul.

Figura 3-4 Pornire



Adăugarea de dispozitive

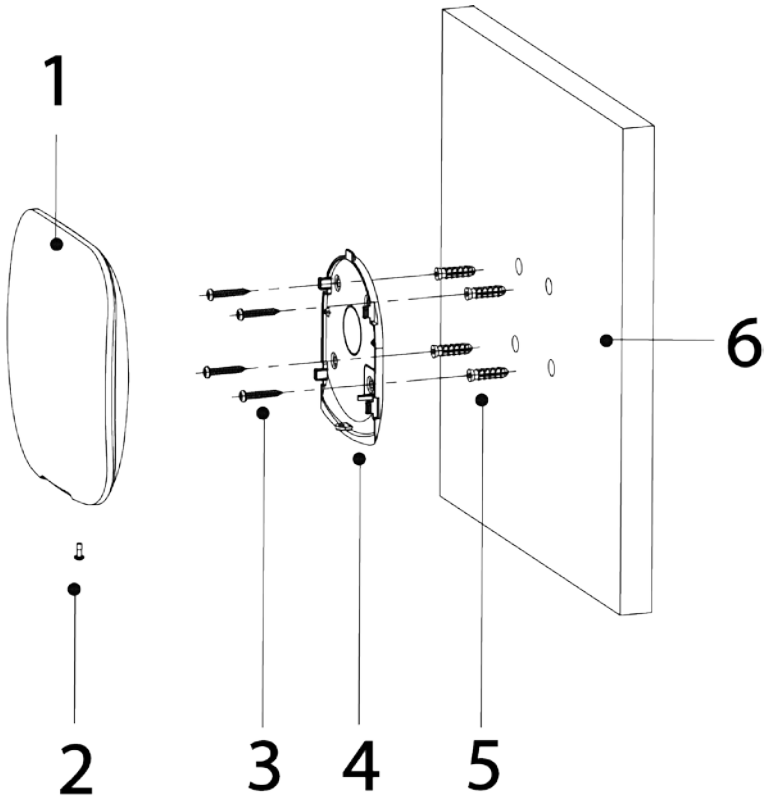
1. Adăugați hub-ul în aplicația COS Pro și DMSS. Pentru detalii, consultați „4.2 Adăugarea de dispozitive” și „5.2 Adăugarea de dispozitive”.
2. Adăugați accesoriile la butuc. Pentru detalii, consultați „4.2.2 Adăugarea accesoriilor” și „5.2.2 Adăugarea accesoriilor”.

Instalarea Hub-ului

Vă recomandăm să utilizați șuruburi de expansiune pentru a instala butucul. Nu amplasați hub-ul în următoarele zone:

- În aer liber.
- Locuri aproape de obiecte metalice care provoacă atenuarea și ecranarea semnalului radio.
- Locuri cu un semnal GSM slab.
- Locuri în apropierea surselor de interferență radio care sunt la mai puțin de 1 metru distanță de router și cablurile de alimentare.
- Locuri unde temperatura și umiditatea depășesc limitele permise.

Figura 3-5 Instalare



Tabelul 3-2 Elemente de instalare

Nu.	Nume articol	Nu.	Nume articol
1	Hub	4	Placa de montare
2	Șurub cu cap înecat M3 × 8 mm	5	Surub de expansiune
3	Șurub autofiletant ST4 × 25 mm	6	Perete

1. Confirmați poziția orificiilor pentru șuruburi, apoi găuriți-le în placa de montare.
2. Puneți șuruburile de expansiune în găuri.
3. Atașați placa de montare în perete și apoi aliniați orificiile pentru șuruburi de pe placă cu șuruburile de expansiune.
4. Fixați placa de montare cu șuruburi autofiletante ST4 × 25 mm.
5. Puneți butucul alarmei în placa de montare de sus în jos.
6. Fixați butucul alarmei și placa de montare cu șuruburi cu cap înecat M3 × 8 mm.

Configurarea Hub-ului

Configurați hub-ul în aplicația COS Pro și DMSS. Pentru detalii, consultați „4.6.2 Configurații de bază ale dispozitivului”.

Armarea sistemului de alarmă

Puteți utiliza tastatura, telecomanda și aplicația pentru a vă arma sistemul. După ce o comandă de armare este trimisă către aplicația COS Pro și DMSS, sistemul va verifica starea sistemului. Dacă sistemul are o defecțiune, va trebui să alegeți dacă să-l forțați. Pentru detalii despre armarea și dezarmarea sistemului, consultați „6 Operații generale”. Pentru detalii despre accesorii, consultați manualul de utilizare al dispozitivului corespunzător.

4 Operațiuni COS Pro pentru instalatori

Aplicația COS Pro este concepută pentru a ajuta instalatorii, oferind servicii profesionale de operare și întreținere pentru utilizatorii finali. Oferă funcții, inclusiv gestionarea site-ului, gestionarea funcționării și a sănătății dispozitivului, examinarea încrederii dispozitivului și multe altele. Pentru detalii, vezi*Aplicația COS Pro_Manual de utilizare*.

Cifrele sunt doar pentru referință și pot diferi de interfața reală.

4.1 Conectarea la COS Pro

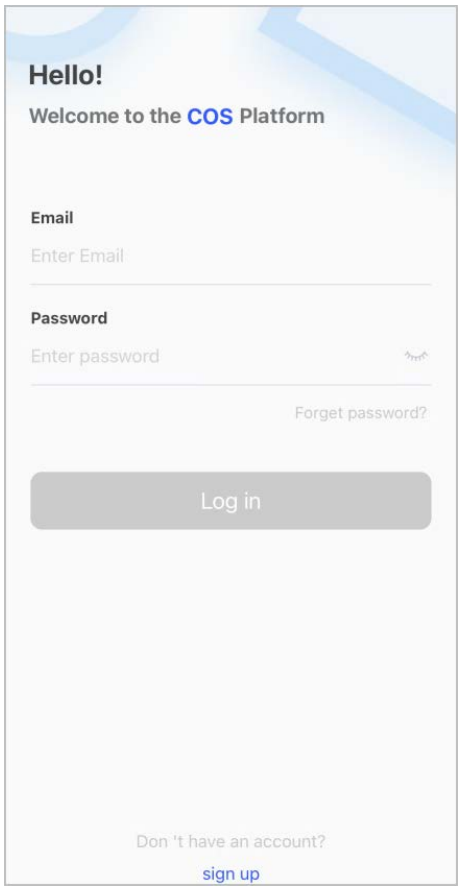
Pentru prima utilizare, trebuie să vă creați un cont. Acest manual de utilizare folosește operațiunile de pe iOS ca exemplu.

Pasul 1 Căutați COS Pro în magazinul de aplicații, apoi descărcați aplicația.

Pentru utilizatorii de Android, puteți accesa Google Play pentru a descărca COS Pro.

Pasul 2 Pe telefon, atingeți pentru a porni aplicația.

Figura 4-1 Conectare



Pasul 3 Creați un cont.

1. Pe**Log in**ecran, atingeți**Inscrie-te**.
2. Pe**Inregistreaza-te**ecran, completați informațiile pentru câmpurile obligatorii.

Dacă țara/regiunea pe care o selectați este din America de Nord, atunci**Număr de înregistrare a distribuitorului**va apărea pe**Inregistreaza-te**ecran. Pentru toate celelalte țări și regiuni,**Numele companiei**va aparea.

- **E-mail**: Introdu adresa ta de e-mail.
- **Țara/Regiune**: Selectați țara/regiunea, provincia/statul și orașul companiei dvs.
- **Abordare**: introduceți adresa detaliată a companiei dvs.
- **Numele companiei**: introduceți numele companiei dvs.
- **Număr de înregistrare a distribuitorului**: Introduceți numărul de înregistrare a distribuitorului.

  Pentru clienții din America de Nord, introduceți numărul de înregistrare a distribuitorului.
- **Codul de invitatie**: Introdu codul de invitație, care poate fi obținut de la invitator.
- **Parola**și**Confirmă parola**: Introduceți parola și confirmați-o din nou.
- **Cod de verificare**: Atingeți**Trimite**, verificați caseta de e-mail pentru a primi un cod de verificare, apoi introduceți codul**Cod de verificare**.

3. Citiți**Politica de confidențialitate**și**Protocolul de service**, apoi selectați**Am citit și sunt de acord cu Politica de confidențialitate și Protocolul de servicii**Caseta de bifat.
4. Atingeți**Inregistreaza-te**, iar apoi aplicația revine la**Log in**ecran.

Pasul 4 Introduceți adresa de e-mail și parola, apoi atingeți**Log in**.

- Pentru clienții noi, este necesară aprobarea cererii de cont. Va dura 1-3 zile pentru a primi un e-mail de aprobare a contului. După aceea, vă puteți conecta la aplicație cu contul dvs.
- Unii clienți afiliați nu trebuie să fie aprobați pentru a se înregistra pentru un cont COS Pro. Ei se pot conecta direct la aplicație după înregistrare.

4.2 Adăugarea de dispozitive

Pentru instalatori, puteți adăuga dispozitive la aplicația COS Pro pentru gestionare și întreținere. Înainte de a adăuga dispozitive, asigurați-vă că dispozitivul este conectat la alimentare și la rețea. Puteți adăuga dispozitive de alarmă, inclusiv hub-uri și mai multe accesorii în aplicație.

4.2.1 Adăugarea hub-ului

Hub-ul poate fi adăugat fie în**Modul site**sau**Modul dispozitiv**. Dacă adăugați dispozitive în**Modul dispozitiv**, trebuie să selectați mai întâi un site. Operațiunile pentru aceste două moduri sunt similare. Această secțiune folosește configurații în**Modul dispozitiv**ca exemplu.

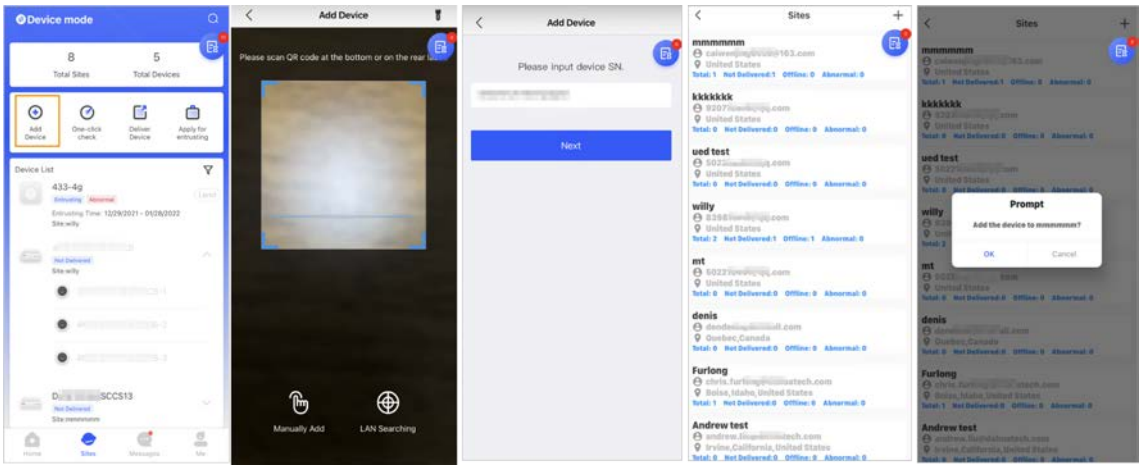
- Înainte de a adăuga hub-ul, asigurați-vă că hub-ul este conectat la alimentare și la rețea.
- Asigurați-vă că telefonul dvs. are activată funcția Wi-Fi.

4.2.1.1 Adăugarea prin cod SN/QR

Puteți adăuga hub-ul scanând codul QR al dispozitivului sau introducând manual SN-ul dispozitivului în rețeaua fără fir sau cu fir.

Pasul 1 Pe**Acasă**ecran, atingeți , apoi trece la**Site-uri**ecran.

Figura 4-2 Adăugați un dispozitiv



Pasul 2 Atingeți în colțul din stânga sus pentru a comuta**Modul dispozitiv**. pentru a

Pasul 3 Atingeți adăuga un dispozitiv.

Pasul 4 Scanați codul QR al dispozitivului sau atingeți**Adăugați manual**pentru a introduce manual SN

Pasul 5 dispozitiv. Selectați un site, apoi atingeți**Bine**.

Pasul 6 Pe**Adăugați dispozitiv**ecran, selectați un tip de dispozitiv.

Pasul 7 Conectați-vă la o rețea fără fir sau cu fir.

- **Fără fir**

1) Atingeți**Fără fir**în colțul din dreapta sus și apoi**Fără fir**devine**Cablat**.

2) Introduceți parola pentru Wi-Fi la care este conectat telefonul dvs., apoi atingeți **Conectați**.

3) Urmați instrucțiunile de pe ecran, apoi atingeți**Următorul**.

4) Așteptați împerecherea.

Dacă a eșuat, repetați procedurile de mai sus.

- **Cablat**

1) Atingeți**Cablat**în colțul din dreapta sus și apoi**Cablat**devine**Fără fir**.

2) Conectați dispozitivul la alimentare și la rețea, apoi atingeți**Următorul**.

Dacă a eșuat, repetați procedurile de mai sus.

Pasul 8 Dacă hub-ul pe care îl adăugați este neinițializat, introduceți parola și confirmați-o din nou, apoi atingeți**Inițializați dispozitivul**pentru a finaliza inițializarea.

Pasul 9 Atingeți**Efectuat**, apoi puteți vizualiza dispozitivul în lista de dispozitive.

4.2.1.2 Adăugarea prin configurarea AP

Puteți adăuga hub-ul prin configurarea AP.

Pasul 1 Pe**Acasă**ecran, atingeți , și apoi merge la**Site-uri**ecran.

Pasul 2 Atingeți în colțul din stânga sus pentru a comuta**Modul dispozitiv**. pentru a

Pasul 3 Atingeți adăuga un dispozitiv.

Figura 4-3 Adăugați un dispozitiv

Pasul 4 Scanați codul QR al dispozitivului sau atingeți**Adăugați manual**pentru a introduce manual SN

Pasul 5 dispozitiv. Pe**Adăugați dispozitiv**ecran, selectați**Stație de alarmă**.

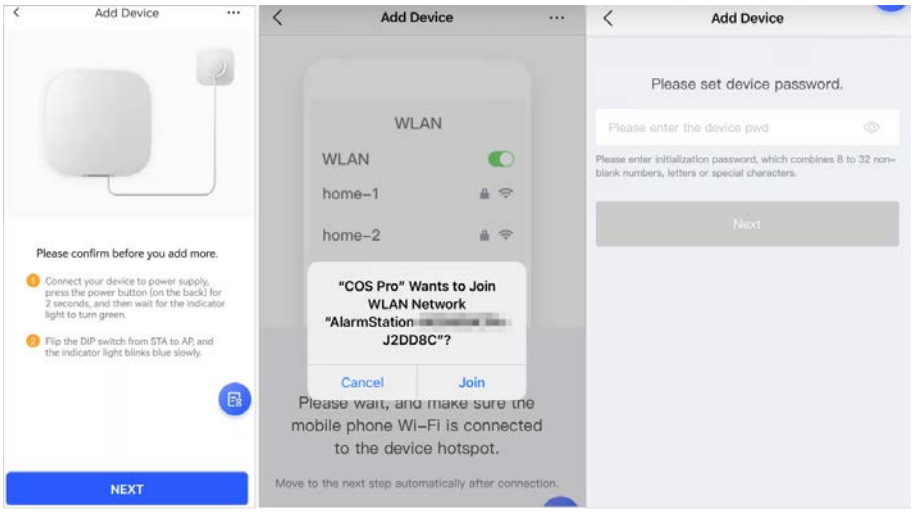
Figura 4-4 Selectați stația de alarmă

Pasul 6 Urmați instrucțiunile de pe ecran și întoarceți comutatorul DIP de la STA la AP. Atingeți**A te**

Pasul 7 **alatura**pentru a vă conecta la hotspot-ul dispozitivului.

Pasul 8 Setați parola dispozitivului pentru a inițializa dispozitivul, apoi atingeți**Următorul**.

Figura 4-5 Adăugați prin configurația AP



Pasul 9 Conectați-vă la rețea. 1)

Selectați Wi-Fi.

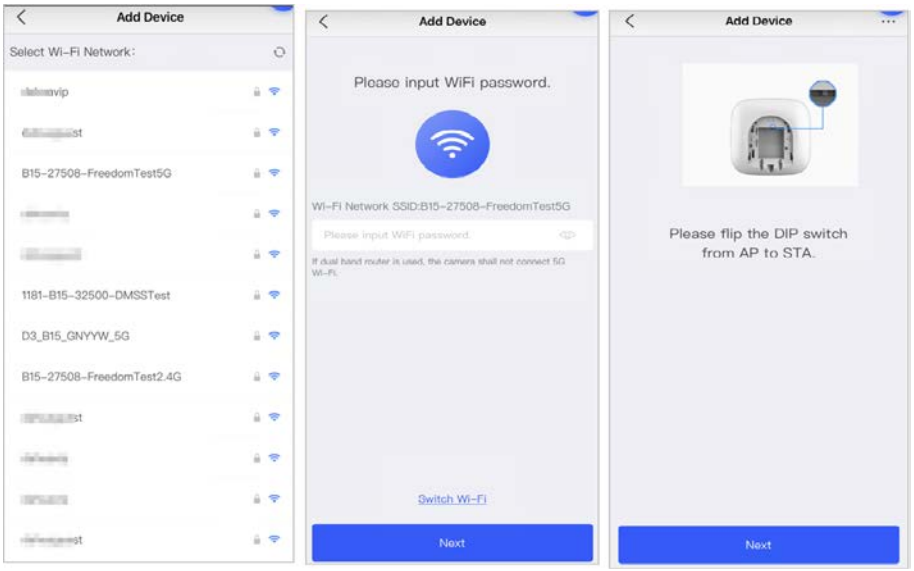
Asigurați-vă că telefonul și dispozitivul sunt conectate la aceeași rețea.

2) Introduceți parola Wi-Fi, apoi atingeți**Următorul**.

3) Întoarceți comutatorul DIP de la AP la STA, apoi atingeți**Următorul**.

4) Așteptați ca dispozitivul să finalizeze configurarea rețelei.

Figura 4-6 Conectați-vă la rețea



Pasul 10 Atingeți**Efectuat**.

4.2.1.3 Adăugarea prin căutare LAN

Puteți căuta dispozitive și le puteți adăuga. Asigurați-vă că telefonul și dispozitivele sunt conectate la aceeași rețea.

Pasul 1 Pe**Acasă**ecran, atingeți , și apoi merge la**Site-uri**ecran.

Pasul 2 Atingeți în colțul din stânga sus pentru a comuta**Modul dispozitiv**. pentru a

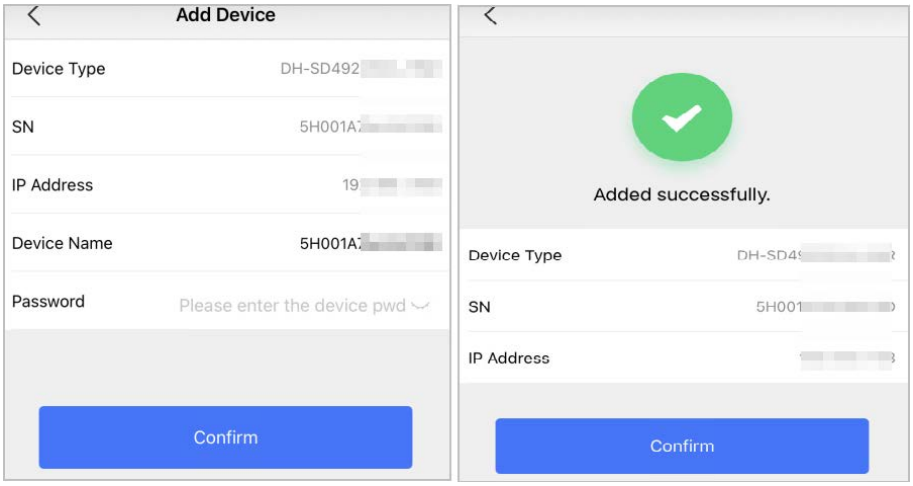
Pasul 3 Atingeți adăuga un dispozitiv.

Figura 4-7 Adăugați un dispozitiv

Pasul 4 Atingeți**Căutare LAN**.

Pasul 5 Pe**Adăugați dispozitiv**ecran, introduceți parola dispozitivului, apoi atingeți**A confirma**.

Figura 4-8 Confirmați adăugarea unui dispozitiv



4.2.2 Adăugarea accesoriilor

Puteți adăuga mai multe accesorii în hub. Secțiunea folosește detectorul de ușă ca exemplu. Pentru detalii despre adăugarea accesoriilor, consultați manualele de utilizare ale accesoriilor respective.

La un hub pot fi adăugate până la 6 sirene, 64 de brelocuri, 4 repetoare și 8 tastaturi.

Pasul 1 Pe ecranul hub, atingeți partea de în colțul din dreapta sus, apoi scanați codul QR la jos a detectorului de ușă. Atingeți

Pasul 2 **Următorul**.

Pasul 3 Urmați instrucțiunile de pe ecran și porniți detectorul de ușă, apoi atingeți**Următorul**pentru a-l adăuga la hub.

Pasul 4 Așteptați împerecherea.

Pasul 5 Personalizați numele detectorului de ușă și selectați zona, apoi atingeți**Efectuat**.

- Ștergeți accesoriul: Accesați ecranul hub, selectați accesoriul din listă, apoi glisați spre stânga pentru a-l șterge.
- Într-un hub pot fi create până la 32 de zone.

4.3 Gestionarea utilizatorilor

4.3.1 Adăugarea utilizatorilor administratori DMSS

Pentru instalator, puteți adăuga utilizatori administratori DMSS, partajând dispozitivele de încredințare cu aceștia sau acceptând cererea lor de încredințare.

Utilizatorul administrator DMSS nu are permisiunea de a configura dispozitivul atunci când instalatorii împrumută hub-ul lor, sau atunci când încredințează hub-ul instalatorului.

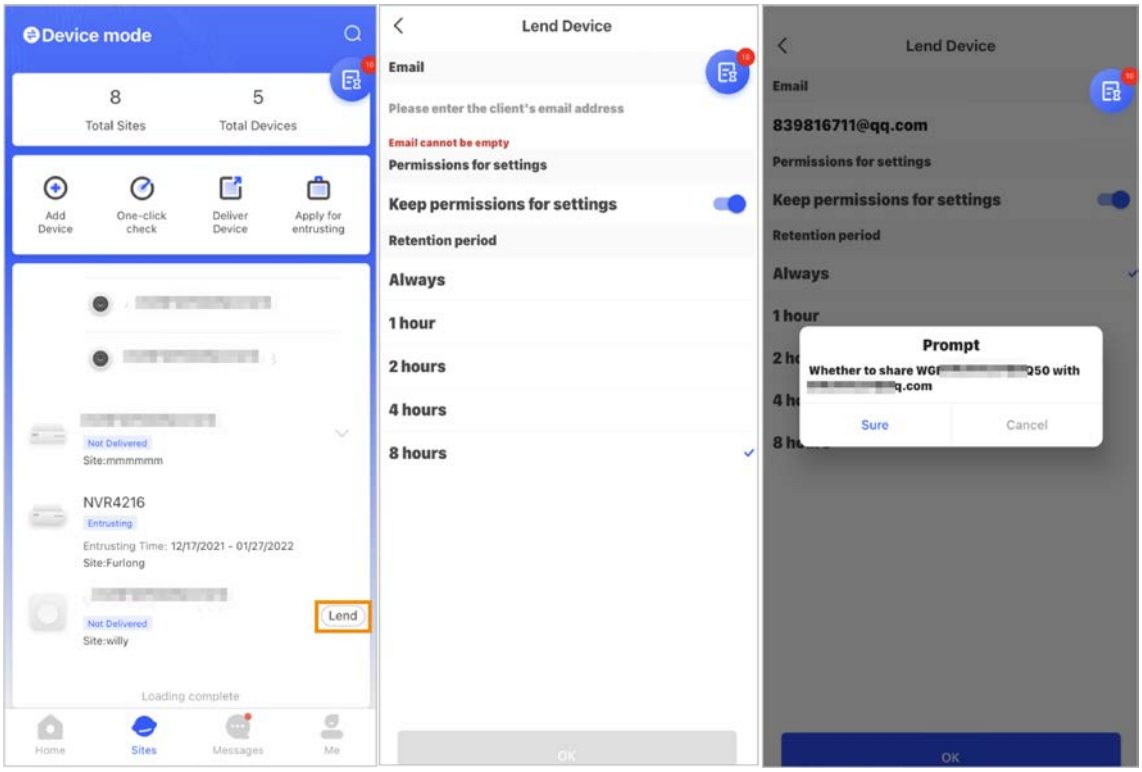
4.3.1.1 Împrumutarea dispozitivului utilizatorilor administratori DMSS

Instalatorul poate împrumuta hub-ul utilizatorului de administrator DMSS. Ulterior, instalatorul trebuie să solicite permisiuni de la utilizatorul administrator DMSS, cum ar fi configurarea dispozitivului, operațiunile de armare și dezarmare și gestionarea utilizatorilor.

Asigurați-vă că hub-ul nu a fost adăugat de alte conturi.

Pasul 1 Pe**Acasă**ecran, atingeți , apoi trece la**Site-uri**ecran.

Figura 4-9 Împrumutați hub-ul utilizatorului de administrator DMSS



Pasul 2 Atingeți în colțul din stânga sus pentru a comuta**Modul dispozitiv**.

Pasul 3 În lista de dispozitive, selectați un hub, atingeți**A împrumuta**în colțul din dreapta al butucului. Introduceți

Pasul 4 adresa de e-mail a utilizatorului administrator DMSS.

Pasul 5 Permite**Rezervați permisiunile de configurare**și selectați timpul de reținere. Atingeți**A**

Pasul 6 **confirma**.

Pasul 7 Pe ecran, atingeți**Mesaj personal**, puteți vizualiza mesajele pentru a vedea dacă administratorul DMSS a fost de acord să accepte solicitarea dvs. de a le partaja.

Un mesaj de partajare va fi trimis către contul de utilizator administrator DMSS și utilizatorul administrator DMSS poate citi mesajul în aplicația DMSS.

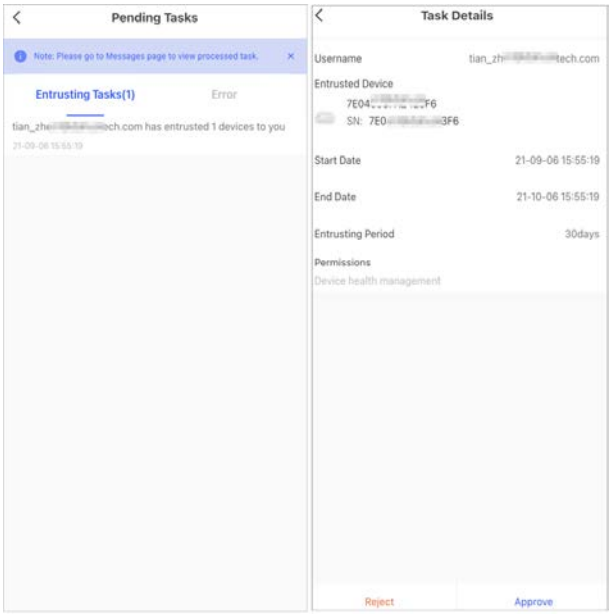
4.3.1.2 Acceptarea cererilor de încredințare

Instalatorul poate accepta cererea de încredințare a utilizatorului de administrator DMSS.

Pasul 1 Pe**Acasă**ecran, selectați**Sarcină în așteptare**>**Încrederea revizuirii**.

Pasul 2 Pe**Sarcină în așteptare**ecran, selectați o sarcină pentru a vizualiza detaliile sarcinii și pentru a gestiona aplicațiile încredințate.

Figura 4-10 Gestionați sarcinile de încredințare

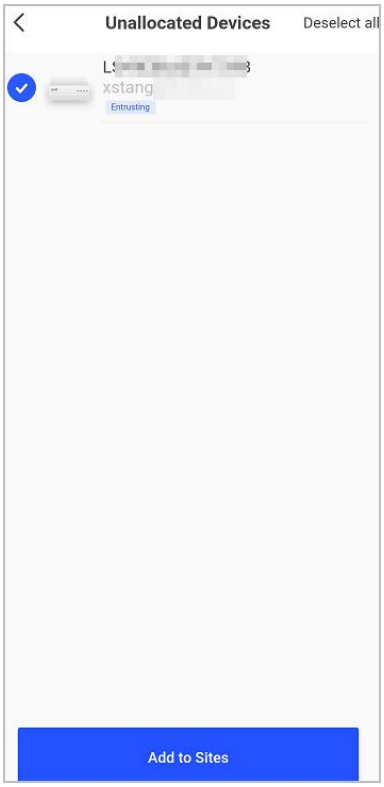


- A aproba

1) Atingeți**Aproba**, și apoi se duce la**Dispozitive nealocate**ecran.

2) Selectați dispozitivele care vor fi alocate sau atingeți**Selectează tot**, apoi atingeți**Adăugați pe site-uri**.

Figura 4-11 Adăugați dispozitiv la site-uri

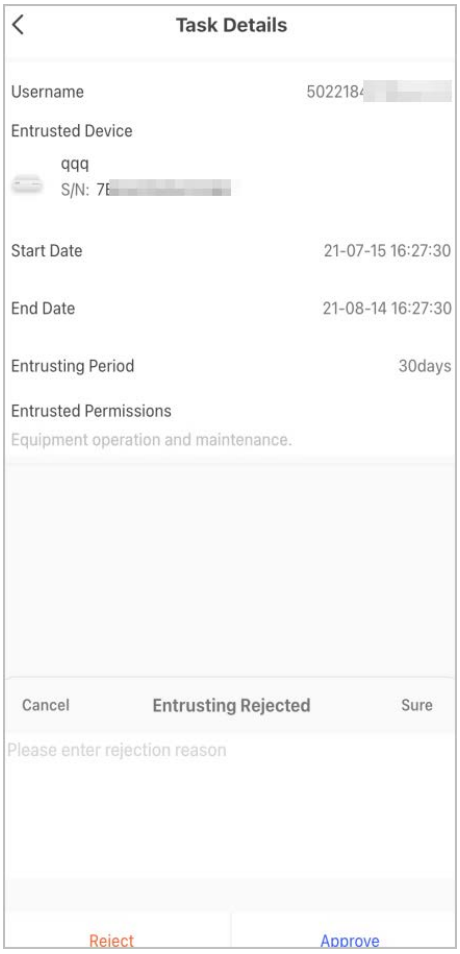


3) Pe**Site-uri**ecran, selectați un site sau adăugați un site nou.

4) Atingeți**Bine**pentru a confirma mutarea acestui dispozitiv pe site-ul selectat.

- Pentru a respinge: atingeți**Respinge**, introduceți motivele respingerii, apoi atingeți**Sigur**.

Figura 4-12 Respingere



4.3.2 Ștergerea utilizatorilor

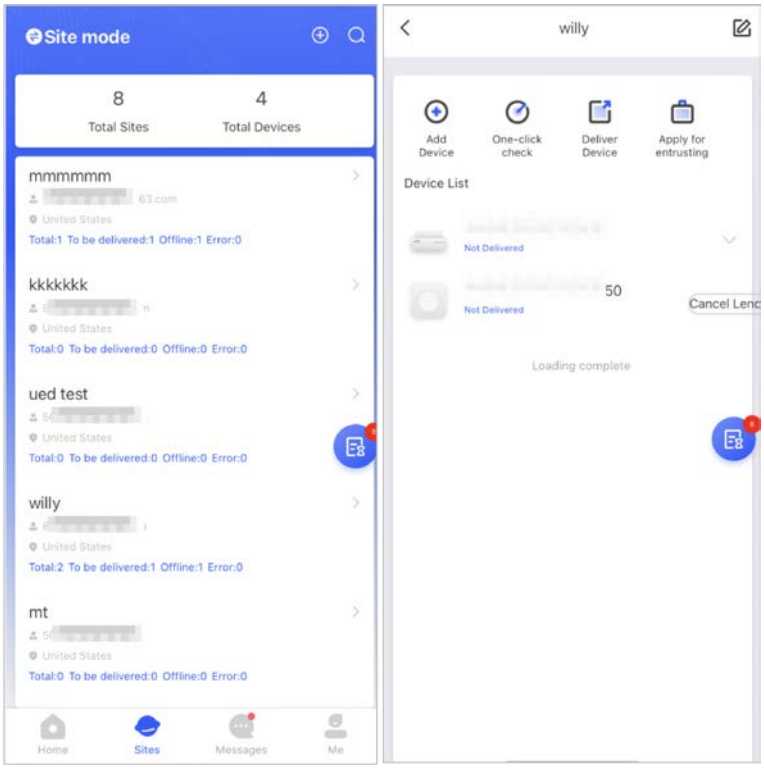
Pentru instalator, puteți șterge un utilizator anulând pentru a împrumuta dispozitivele utilizatorului administrator DMSS sau ștergând dispozitivele.

4.3.2.1 Anularea pentru a împrumuta dispozitivele

Pentru instalator, puteți șterge utilizatorii administratori DMSS anulând pentru a le împrumuta hub-ul.

Pasul 1 Pe**Acasă**ecran, atingeți , apoi trece la**Site-uri**ecran.

Figura 4-13 Împrumutați hub-ul utilizatorului de administrator DMSS



Pasul 2 Atingeți în colțul din stânga sus pentru a comuta**Modul site**.

Pasul 3 În lista de site-uri, selectați site-ul cu dispozitivul pe care îl împrumutați utilizatorului administrator DMSS, apoi selectați hub-ul și apoi atingeți**Anulează împrumutul**.

Mesajul va fi trimis către contul de utilizator de administrator DMSS, iar utilizatorul de administrator DMSS poate citiți mesajul în aplicația DMSS.

4.3.2.2 Ștergerea dispozitivelor

Pentru instalator, puteți șterge utilizatorii administratori DMSS ștergând dispozitive.

- Asigurați-vă că programul de instalare a anulat pentru a împrumuta dispozitivele utilizatorului administrator DMSS.
- Programul de instalare poate șterge toți utilizatorii DMSS dacă utilizatorul administrator DMSS a partajat dispozitivele cu DMSS utilizatorii generali.

Pasul 1 Pe**Acasă**ecran, atingeți , apoi treceți la**Site-uri**ecran. Atingeți colțul din

Pasul 2 stânga sus pentru a comuta la**Modul dispozitiv**. În lista de dispozitive,

Pasul 3 selectați dispozitivul după cum este necesar.

Pasul 4 Pe ecranul hub, atingeți , apoi atingeți**Șterge**pentru a șterge dispozitivul.

4.4 Solicitarea permisiunii utilizatorului administrator DMSS

Pentru instalatori, puteți adăuga hub-ul direct la aplicația COS Pro pentru a oferi servicii de operare și întreținere a dispozitivului pentru utilizatorii de administrator DMSS. Aveți permisiuni limitate în timp, inclusiv

configurarea dispozitivului și gestionarea utilizatorilor și trebuie să solicite din nou permisiunea la expirare.

Pasul 1 Pe **Acasă** ecran, atingeți , apoi treceți la **Site-uri** ecran. Atingeți colțul din

Pasul 2 stânga-sus pentru a comuta la **Modul dispozitiv**. În lista de dispozitive,

Pasul 3 selectați dispozitivul după cum este necesar.

Pasul 4 Pe **Hub** ecran, selectați > **Setare hub**, atingeți orice parametru pe care doriți să-l configurați, apoi va apărea o solicitare pentru a vă reaminti să solicitați permisiuni de la utilizatorul administrator DMSS.

Pasul 5 Atingeți **Sigur**.

Pasul 6 Selectați orele de autorizare, apoi atingeți **A confirma**.

Pasul 7 Pe ecran, atingeți **Mesaj personal** pentru a vizualiza mesajele pentru a vedea dacă administratorul DMSS a fost de acord să vă atribuie permisiuni.

Un mesaj de solicitare va fi trimis către contul de utilizator administrator DMSS și către utilizatorul administrator DMSS poate citi mesajul în aplicația DMSS.

4.5 Livrarea dispozitivelor către utilizatorul administrator DMSS

După depanarea dispozitivelor, puteți livra dispozitivele utilizatorului administrator DMSS. Dispozitivele offline și încredințate nu pot fi livrate.

Cerințele certificărilor En50131 nu vor fi îndeplinite dacă instalatorul livrează hub-ul unui DMSS utilizator admin.

Pasul 1 Pe **Acasă** ecran, atingeți , apoi treceți la **Site-uri** ecran. Atingeți

Pasul 2 colțul din stânga sus pentru a comuta la **Modul site**.

Pasul 3 În lista de site-uri, selectați un site cu dispozitive care trebuie livrate utilizatorului administrator DMSS.

Pasul 4 Atingeți , iar apoi treceți la **Livrați dispozitive** ecran.

Nu pot fi livrate mai mult de 5 dispozitive simultan.

Pasul 5 Introduceți e-mailurile utilizatorului administrator DMSS, apoi atingeți **Sigur** pentru a vedea rezultatele obținute. Pentru dispozitivele care nu au reușit să fie livrate utilizatorului administrator DMSS, accesați **A eșuat** ecran pentru a livra din nou.

Dacă clienții folosesc contul Imou, atunci dispozitivele lor nu vor fi livrate cu succes. Și va apărea un mesaj pe **Acasă** ecran care indică faptul că contul nu are permisiune. Vă rugăm să cereți clientului să actualizeze contul în aplicația DMSS. Pentru detalii, vedea *Aplicația DMSS_Manualul utilizatorului.*

4.6 Funcționarea și întreținerea sănătății dispozitivului

Instalatorii pot oferi servicii de operare și întreținere a sănătății dispozitivului, cum ar fi verificarea

starea de sănătate a dispozitivelor, configurarea de la distanță a dispozitivelor și remedierea erorilor.

4.6.1 Verificarea stării de sănătate a dispozitivului

Puteți verifica starea online și offline a dispozitivelor în timp real și puteți verifica starea de sănătate a dispozitivelor pe rând sau în loturi. Această secțiune folosește verificarea în loturi ca exemplu. Configurațiile pentru acestea pot fi găsite în**Modul site**și**Modul dispozitiv**. Operațiunile pentru aceste două moduri sunt similare. Această secțiune folosește configurații în**Modul dispozitiv**ca exemplu. Pasul 1

Pe**Acasă**ecran, atingeți , și apoi merge la**Site-uri**ecran.

Pasul 2 Atingeți în colțul din stânga sus pentru a comuta**Modul dispozitiv**.

Pasul 3 Atingeți .

Pasul 4 Selectați dispozitivele pe care doriți să le verificați, apoi atingeți**X dispozitive selectate. Începeți verificarea sănătății**.

Pentru a selecta toate dispozitivele, atingeți**Selectează tot**.

Pasul 5 Vizualizați rezultatele verificării, apoi atingeți**Bine**.

Dispozitivele offline nu pot fi verificate.

4.6.2 Configurații de bază ale dispozitivului

După ce adăugați dispozitive, inclusiv hub-ul de alarmă și accesorii, puteți vizualiza și edita informații generale despre dispozitiv.

Pasul 1 Pe**Acasă**ecran, atingeți , apoi treceți la**Site-uri**ecran. Atingeți colțul din

Pasul 2 stânga sus pentru a comuta la**Modul dispozitiv**. În lista de dispozitive,

Pasul 3 selectați dispozitivul după cum este necesar.

Pasul 4 Pe ecranul hub, atingeți pentru a vedea și edita informațiile generale de pe dispozitiv.

Tabelul 4-1 Descrierea parametrilor

Parametru	Descriere
Configurarea dispozitivului	● Vizualizați numele dispozitivului, tipul și SN. ● Editați numele dispozitivului, apoi atingeți**Salvați**pentru a salva configurația.
Stare hub	Pentru detalii, consultați „4.6.2.2 Configurarea hub-ului”.
Setare hub	Pentru detalii, consultați „4.6.2.1 Stare de vizualizare”.
Fus orar	Atingeți**Fus orar**pentru a vă selecta fusul orar și pentru a activa DST (ora de vară), dacă este necesar. ● **Fus orar**: Selectați fusul orar în care funcționează hub-ul. ● **DST**: Selectați data sau săptămâna, apoi selectați ora de începere și ora de încheiere.
Configurarea Rețelei	Atingeți**Configurarea Rețelei**pentru a vizualiza informațiile actuale ale rețelei.

Parametru	Descriere
Partajarea dispozitivului	Atingeți**Partajarea dispozitivului**pentru a partaja starea hub-ului cu ceilalți utilizatori. Pentru detalii, consultați „4.3.1.1 Împrumutarea dispozitivului utilizatorilor administratori DMSS”.
Actualizare în cloud	Actualizați online. Actualizarea nu este permisă când hub-ul este în starea armată sau nivelul bateriei este scăzut.
Buturuga	Jurnalele pentru dispozitive și aplicații. ● Jurnal dispozitiv: Selectați**Buturuga**>**Jurnalul dispozitivului**pentru a vizualiza jurnalele de alarmă ale dispozitivului. De asemenea, puteți apăsa pe**Jurnalul dispozitivului**ecran pentru a trimite jurnalele de alarmă către e-mailul legat. ● Jurnal de aplicații: Selectați**Buturuga**>**Jurnalul aplicației**pentru a vizualiza jurnalele de alarmă ale COS Pro. De asemenea, puteți atinge pe**Jurnalul aplicației**ecran pentru a trimite jurnalele de alarmă e-mailul legat.

4.6.2.1 Stare de vizualizare

Pe**Hub**ecran, selectați > **Stare hub**pentru a vedea starea hub-ului.

Tabelul 4-2 Stare

Parametru	Descriere
Puterea semnalului GSM	Puterea semnalului rețelei mobile pentru cartela SIM activă. ● : Ultra scăzut. ● : Scăzut. ● : Moderat. ● : Înalt. ● : Nu.
Puterea semnalului Wi-Fi	Starea conexiunii la internet a hub-ului prin Wi-Fi. Pentru o mai mare fiabilitate, vă recomandăm să instalați hub-ul în locuri cu puterea semnalului de cel puțin 2 bare. ● : Ultra scăzut. ● : Scăzut. ● : Moderat. ● : Înalt. ● : Nu.
Acumulator	Arată electricitatea rămasă din baterie. ● : Incarcat complet. ● : Suficient. ● : Moderat. ● : Insuficient.
Anti-manipulare	Modul tamper al accesoriului, care reacționează la detașarea corpului.
Stare alimentare principală	Afișează starea alimentării principale.

Parametru	Descriere
Starea conexiunii GSM	Starea conexiunii la internet a hub-ului prin cartela SIM, Wi-Fi și Ethernet. ● : Conectat. ● : Deconectat.
Starea conexiunii Wi-Fi	
Starea conexiunii cablului de rețea	
Starea cartelei SIM	Starea conexiunii cartelei SIM. ● : cartela SIM 1 este activă. ● : cartela SIM 2 este activă. ● : Fără cartelă SIM.
Versiunea programului	Versiunea de program a hub-ului.

4.6.2.2 Configurarea Hub-ului

Pe**Hub**ecran, selectați > **Setare hub**pentru a configura parametrii hub-ului.

Tabelul 4-3 Descrierea parametrului hub

Parametru	Descriere
Global Armare/Dezarmare	Armați sau dezarmați toate detectoarele din toate zonele cu o singură atingere.
Programa Armare/Dezarmare	Armați sau dezarmați zonele după program. ● **Zonă**: Selectați zona în care funcționează hub-ul. ● **Setarea comenzii**: Selectați un mod armat după cum este necesar atingând **Acasă**,**Departe**, sau**Dezarma**. ● **Timp**: Selectați perioada de timp în care funcționează hub-ul. ● **Repeta**: Copiați programul de armare sau dezarmare. ● **Forța Armată**: Puteți arma sistemul atunci când apar erori în zone.
Setarea tonului de apel	Tonul de apel la intrarea sau ieșirea din modul de armare.
Indicator cu LED	**Indicator cu LED**este activat implicit. Pentru detalii despre comportamentul indicatorului, consultați „2.1 Aspect”. ● Dacă**Indicator cu LED**este dezactivat, indicatorul LED va rămâne stins indiferent dacă hub-ul funcționează normal sau nu. ● Funcția este disponibilă numai când versiunea aplicației DMSS este 1.96 sau mai recent, iar hub-ul este V1.001.0000000.4.R.211014 sau mai recent.
Modul de testare	Atingeți**start**pentru a testa starea accesoriilor care se conectează la hub în diferite zone, apoi atingeți**Stop**pentru a finaliza detectarea.
Sensibilitate redusă Modul	Permite**Mod de sensibilitate redusă**, iar apoi puterea de transmisie a hub-ului va fi redusă. Funcția este disponibilă numai atunci când versiunea aplicației DMSS este 1.97 sau o versiune ulterioară, iar hub-ul este V1.001.0000000.6.R.211215 sau o versiune ulterioară.

Parametru	Descriere
Serviciu cloud Conexiune	Setați intervalul de ping server-hub cu un interval de la 150 la 900 de secunde (150 de secunde în mod implicit). Dacă D-cloud detectează că durata offline a hub-ului depășește 150 de secunde, va raporta utilizatorului starea hub-ului prin intermediul aplicației. Funcția este disponibilă numai atunci când versiunea aplicației DMSS este 1.96 sau o versiune ulterioară, iar hub-ul este V1.001.0000000.6.R.211215 sau o versiune ulterioară.
Bătăile inimii	Configurați intervalul de ping hub-detector. Setările determină cât de des comunică hub-ul cu accesoriile și cât de repede este detectată pierderea conexiunii. ● **Intervalul de ping al detectorului**: Frecvența accesoriilor conectate operate de hub este configurată în intervalul de la 12 secunde la 300 de secunde (60 de secunde în mod implicit). Cu cât intervalul de ping al detectorului este mai scurt, cu atât durata de viață este mai scurtă bateria. ● **Numărul de pachete nelivrate pentru a determina eșecul conexiunii**: Un contor de pachete nelivrate este configurat în intervalul de la 3 la 60 (15 pachete în mod implicit). ◇ Cu cât numărul este mai mic, cu atât starea offline este mai frecventă de accesorii este detectată și raportată. ◇ Dacă butucul pierde constant legătura cu accesoriile și nu le poate detecta bătăile definite ale inimii, va raporta sistemului lor starea offline.
Anti-manipulare Difuzor	Alertă cu o sirenă dacă capacul din spate al accesoriilor și al butucului este deschis.
Integritatea sistemului Verifica	Când este activat, hub-ul verifică starea tuturor detectorilor înainte de armare, cum ar fi nivelul de încărcare a bateriei, incidentele de manipulare și conectivitatea. Dacă sunt detectate erori, vor fi afișate avertismente. ● Pentru telecomandă, indicatorul clipește în verde și apoi devine roșu. ● Pentru aplicație, apare un mesaj de alarmă. ● Pentru tastatură, emite un bip timp de 1 secundă, la armare și dezarmare indicatorul luminează intermitent în verde timp de 2 secunde, apoi se întoarce la stare normală.
CMS	Introduceți adresa IP, portul și ID-ul dispozitivului, apoi puteți înregistra hub-ul în D-cloud. Funcția este disponibilă numai atunci când versiunea aplicației DMSS este 1.96 sau o versiune ulterioară, iar hub-ul este V1.001.0000000.6.R.211215 sau o versiune ulterioară.

Parametru	Descriere
Stația de monitorizare	Permite**Stația de monitorizare**, apoi setați parametrii protocolului SIA pentru centrul de recepție a alarmelor (ARC). ● **Adresă IP preferată**: Introduceți adresa IP și numărul portului ARC. ● **Adresă IP alternativă**: Introduceți adresa IP alternativă și numărul portului ARC. ◇ Mesajele vor fi trimise la adresa IP alternativă numai când adresa IP preferată nu reușește să primească mesajul. ◇ Dacă**Intervalul bătăilor inimii**este activat, sistemul va decide dacă trimite mesajul la adresa IP preferată sau alternativă. ● **Protocolul IP**: Selectați**TCP**în mod implicit. ● **Intervalul bătăilor inimii**: Setați intervalul bătăilor inimii cu un interval de la 0 secundă la 24 de ore (60 de secunde în mod implicit). 0 secunde înseamnă**Intervalul bătăilor inimii**este dezactivat. ● **Cont central**: Introduceți numărul de cont creat de ARC, care va fi utilizat pentru a identifica hub-ul atunci când hub-ul trimite informații către ARC. ● **Criptare**: hub-ul folosește un format de criptare pentru securitatea informațiilor când configurați ARC.**AES128**este setat implicit. ● **Încărcați evenimentul**: Atingeți lângă un eveniment pentru a-l încărca. ◇ **Alarma**: Mesaj de alarmă. ◇ **Eroare**: întrerupere de curent, subtensiune a bateriei, manipulare și offline. ◇ **Eveniment**: interziceți utilizarea perifericelor, adăugați sau ștergeți periferice și adăugați sau ștergeți utilizatori. ◇ **Armare/Dezarmare**: Mesaj de notificări privind armarea și dezarmarea sistemului.

4.6.3 Remedierea erorilor

Puteți remedia erorile după ce dispozitivele anormale sunt verificate. Erorile sunt găsite în două moduri, inclusiv raportarea automată a dispozitivului și verificarea manuală.

Pasul 1 Pe**Acasă**ecran, selectați**Sarcină în așteptare**>**Remedierea erorilor**. În lista de

Pasul 2 erori, atingeți o sarcină de eroare, apoi atingeți**Începeți procesarea**. Remediați

Pasul 3 eroarea conform sugestiilor.

Pasul 4 Atingeți**Eroare remediată**dacă eroarea este remediată, apoi așteptați ca clientul să o confirme.

Clienții vor fi informați cu privire la starea de remediere a erorilor. Dacă confirmă că eroarea are au fost reparate, li se va cere să evalueze serviciul.

4.6.4 Vizualizarea evaluărilor

După ce au configurat dispozitivele de la distanță și au remediat erori, clienții vor evalua modul în care operatorii s-au comportat în remedierea erorilor și întreținerea sănătății dispozitivului. Contul de administrator poate vizualiza detalii despre erori, cum ar fi tipul de eroare, ora în care a apărut eroarea, sugestii și operațiuni, numele operatorului și evaluări.

Pasul 1 Pe ecran, atingeți**Notificare de eroare**.

Pasul 2 În lista de mesaje, atingeți un mesaj pentru a vizualiza detaliile mesajului, inclusiv numele de utilizator al clientului, numele de utilizator al operatorului, detaliile dispozitivului, detaliile erorilor, detaliile de remediere a erorilor și evaluarea.

5 Operațiuni DMSS pentru utilizatorii finali

Aplicația DMSS oferă servicii profesionale de supraveghere a securității pentru utilizatorii finali. Pentru utilizatorii administratori DMSS, puteți partaja hub-ul cu până la 6 utilizatori generali DMSS și îl puteți încredința unei singure întreprinderi. Accesoriile care vin cu hub-ul pot fi partajate și încredințate în același timp. Pentru a partaja și a încredința hub-ul singur, trebuie să instalați cea mai recentă versiune a aplicației DMSS.

Cifrele sunt doar pentru referință și pot diferi de interfața reală.

5.1 Conectarea la DMSS

Sistemul de securitate este configurat și controlat prin aplicația DMSS. Puteți accesa aplicația DMSS pe iOS și Android. Această secțiune folosește operațiunile de pe iOS ca exemplu.

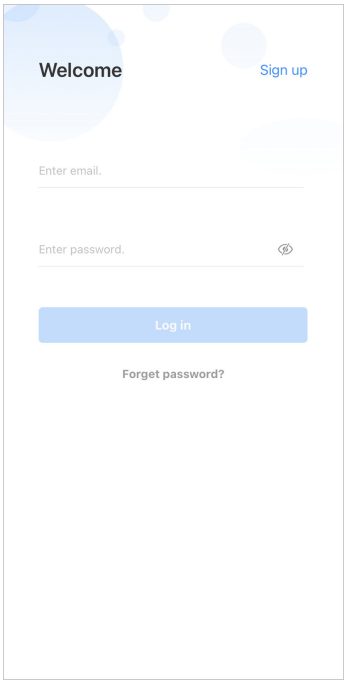
Asigurați-vă că ați instalat cea mai recentă versiune a aplicației.

Pasul 1 Căutați DMSS în magazinul de aplicații, apoi descărcați aplicația.

Pentru utilizatorii de Android, puteți accesa Google Play pentru a descărca DMSS.

Pasul 2 Pe telefon, atingeți pentru a porni aplicația.

Figura 5-1 Conectare



Pasul 3 Creați un cont.

1) Pe**Log in**ecran, atingeți**Inscrie-te**.

2) Introduceți adresa dvs. de e-mail și parola.

Atingeți pentru a afișa parola, iar pictograma va deveni .

3) Citiți**Acordul Utilizatorului**și**Politica de confidențialitate**, apoi selectați**Am citit și sunt de acord** Caseta de bifat.

4) Atingeți**Obțineți codul de verificare**, verificați caseta de e-mail pentru codul de verificare, apoi introduceți codul.

Utilizați codul de verificare în 60 de secunde de la primire. În caz contrar, codul de verificare va deveni invalid.

5) Atingeți**Bine**.

Pasul 4 Pe**Log in**ecran, introduceți adresa de e-mail și parola, apoi atingeți**Log in**.

Puteți modifica parola de pe**Pe mine**>**Managementul contului**>**Modificați parola**.

5.2 Adăugarea de dispozitive

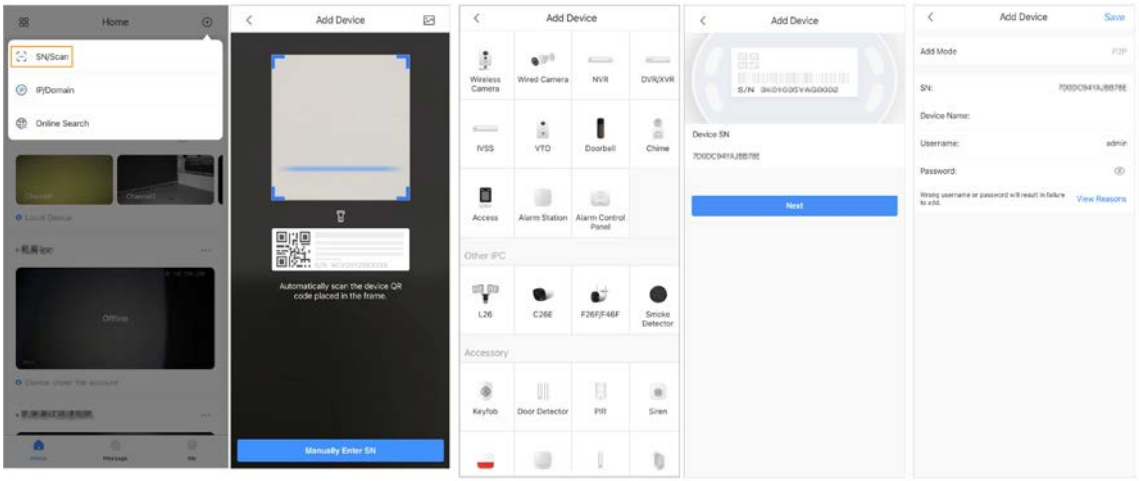
Pentru utilizatorii finali, puteți adăuga dispozitive de alarmă la aplicația DMSS.

5.2.1 Adăugarea hub-ului

Puteți adăuga hub-ul introducând manual SN-ul dispozitivului și scanând codul QR.

Pasul 1 Pe**Acasă**ecran, atingeți și apoi selectați**SN/Scanare**.

Figura 5-2 Adăugați după codul SN/QR



Pasul 2 Adaugă un dispozitiv.

- Scanați direct codul QR al dispozitivului sau atingeți și importați imaginea codului QR pentru a adăuga un dispozitivul.
- Atingeți**Introduceți manual SN**, apoi introduceți SN-ul dispozitivului pentru a adăuga manual un dispozitiv.

Pasul 3 Selectați tipul de dispozitiv, apoi atingeți**Următorul**.

Atingeți**Următorul**dacă sistemul identifică automat tipul de dispozitiv.

Pasul 4 Pe**Adăugați dispozitiv**ecran, personalizați numele dispozitivului, introduceți numele de utilizator și parola dispozitivului, apoi atingeți**Salvați**.

5.2.2 Adăugarea accesoriilor

Pentru utilizatorii finali, puteți adăuga mai multe accesorii în hub. Operațiunile de adăugare a accesoriilor pe DMSS sunt aceleași cu cele de pe COS Pro. Pentru detalii, consultați „4.2.2 Adăugarea accesoriilor”.

5.3 Setări generale hub

5.3.1 Configurare hub

Pe**Detalii despre dispozitiv**ecran, atingeți , iar apoi puteți vizualiza și edita informațiile generale ale hub. Informațiile generale ale dispozitivului afișate în aplicația DMSS sunt aceleași cu cele din aplicația COS Pro. Pentru detalii, consultați „4.6.2 Configurații de bază ale dispozitivului”.

5.3.2 Configurarea rețelei

În**Configurare generală**pe**Detalii despre dispozitiv**ecran, atingeți**Configurarea Rețelei**, apoi puteți selecta un tip de conexiune la rețea pentru hub: rețea cu fir, rețea fără fir sau rețea celulară.

5.3.2.1 Configurarea rețelei cu fir

Pasul 1 Selectați**Setari de retea**>**Configurare rețea cu fir**.

Pasul 2 Configurați parametrii de conexiune la rețea cu fir.

Tabelul 5-1 Descrierea parametrilor rețelei cu fir

Parametru	Descriere
DHCP	Când există un server DHCP în rețea, puteți activa **DHCP**, iar apoi hub-ul primește automat o adresă IP dinamică.
Adresa IP	Setați manual adresa IP: setați manual adresa IP, masca de subrețea, gateway-ul implicit și DNS pentru hub.
Mască de rețea	
Hub de alarmă	
DNS	
DNS 2	

5.3.2.2 Configurarea rețelei Wi-Fi

Pasul 1 Selectați**Setari de retea**>**Configurarea rețelei Wi-Fi**.

Pasul 2 Selectați o rețea Wi-Fi disponibilă în zonă, apoi introduceți parola rețelei pentru a vă conecta la rețea.

5.3.2.3 Configurare celulară

Pasul 1 Selectați**Setari de retea**>**Celular**.

Pasul 2 Configurați parametrii celulari.

Tabelul 5-2 Descrierea parametrilor celulari

Parametru	Descriere
Celular	Atingeți Alături de**Celular**pentru a activa celula.
Prioritate	Atingeți Alături de**Prioritate**pentru a seta celula ca prioritate la selectarea rețelei.
SIM 1	● Suportă cartele SIM duale și standby unic. ● Cardurile SIM permit hub-ului să utilizeze date celulare și să împingă notificări de alarmă.
SIM 2	
APN	Numele punctului de acces (APN) este numele setărilor pe care le citește dispozitivul dvs. pentru a configura o conexiune pentru gateway-ul între rețeaua celulară a operatorului dvs. și internetul public.
Modul de autentificare	Modul de autentificare al rețelei celulare.
Nume de utilizator	Numele de utilizator și parola rețelei celulare.
Parola	
Formeaza numarul	Numărul pe care trebuie să îl sune hub-ul.
Utilizarea datelor mobile	Vedeți modul de utilizare a datelor mobile.
Resetează statisticile	Resetați utilizarea datelor mobile pentru a reporni contorizarea.

5.4 Gestionarea utilizatorilor

5.4.1 Adăugarea utilizatorilor

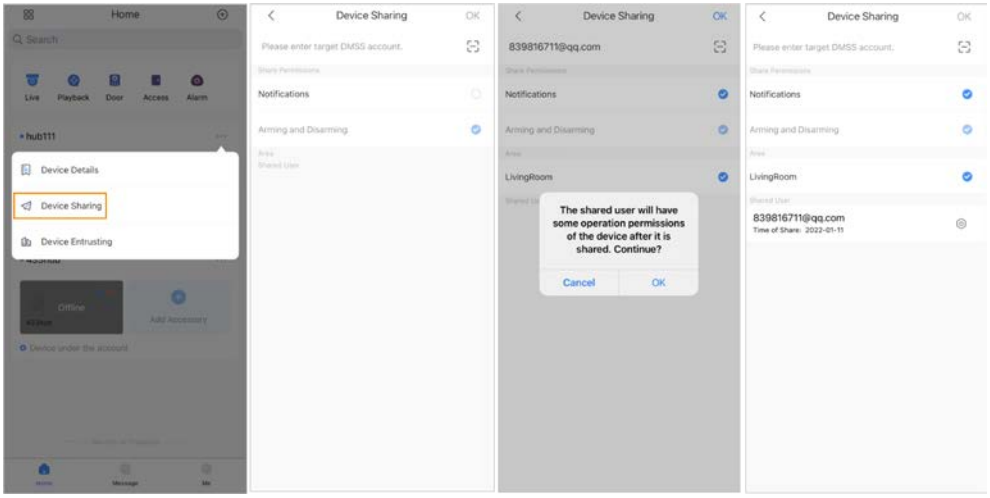
Pentru utilizatorii administratori DMSS, puteți adăuga atât instalatori, cât și utilizatori generali DMSS.

5.4.1.1 Adăugarea utilizatorilor generali DMSS

Puteți partaja dispozitive cu până la 6 utilizatori generali DMSS. Poti sa te duci la ••• > **Detalii despre dispozitiv**> , sau ••• > **Detalii despre dispozitiv**>**Partajarea dispozitivului**a împărtăși dispozitivul. Aceste metode sunt similare. Această secțiune folosește partajarea ••• > **Partajarea dispozitivului** dispozitivelor ca exemplu.

Pasul 1 Pe**Acasă**ecran, atingeți ••• lângă un dispozitiv, apoi atingeți**Partajarea dispozitivului**.

Figura 5-3 Partajare dispozitiv



Pasul 2 Pe**Partajarea dispozitivului**ecran, partajați dispozitivul cu utilizatorul introducând contul DMSS sau scanând codul QR.

Pasul 3 Selectați permisiunile dispozitivului pentru utilizatori în funcție de nevoile dvs. reale.

Pasul 4 Atingeți**Bine**.

Contul cu care ați partajat dispozitivul va apărea pe**Utilizator partajat**secțiunea **Partajarea dispozitivului**ecran.

5.4.1.2 Adăugarea instalatorilor

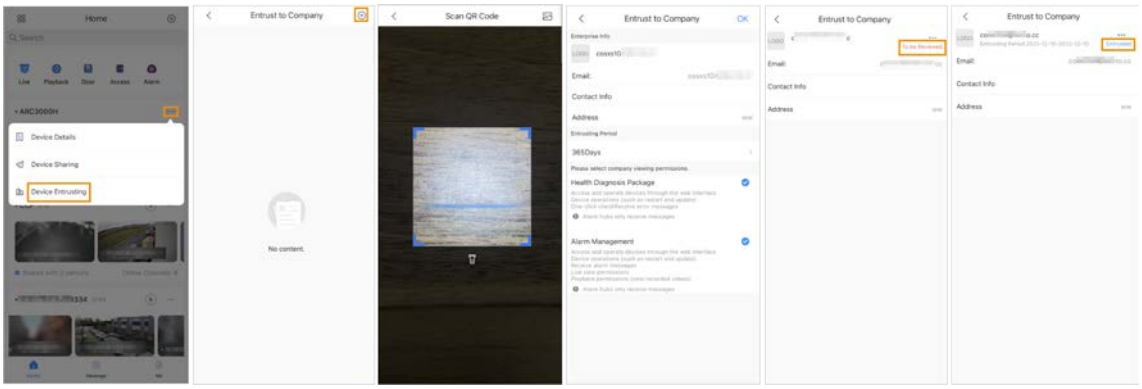
Pentru utilizatorii administratori DMSS, puteți adăuga instalatori, încredințându-le dispozitive. Puteți încredința dispozitivele instalatorului unul câte unul sau în loturi.

5.4.1.2.1 Încredințarea dispozitivului unul câte unul

Procedură

Pasul 1 Pe**Acasă**ecran, atingeți ••• lângă un dispozitiv, apoi atingeți**Încredințarea dispozitivului**.

Figura 5-4 Încrederea unui dispozitiv



Pasul 2 Pe**Încredințați companiei**ecran, atingeți , apoi scanați codul QR corespunzător al instalatorului sau atingeți și importați imaginea codului QR pentru a încredința dispozitivul instalatorului.

Puteți cere instalatorilor codurile QR.

Pasul 3 Pe**Încredințați companiei**ecran, selectați perioadele de încredințare și permisiunile de vizualizare ale companiei, apoi atingeți**Bine**.

- Trebuie să selectați cel puțin o permisiune de vizualizare din**Pachetul de diagnostic de sănătate**și **Managementul alarmelor**.
- Informațiile companiei vor fi recunoscute automat după ce scanați codul QR al instalatorul.

Pasul 4 Vedeți detalii de încredințare pe**Încredințați companiei**ecran.

Când a fost încredințat cu succes,**A fi revizuit**se va schimba în**Livrat**.

După ce o solicitare de încredințare a fost trimisă cu succes, va apărea un mesaj pe ecran**Acasă** ecran. Trebuie să așteptați un răspuns de la programul de instalare, care va fi afișat pe **Pe mine**>**Cutie poștală**>**Personal**ecran.

Operațiuni conexe

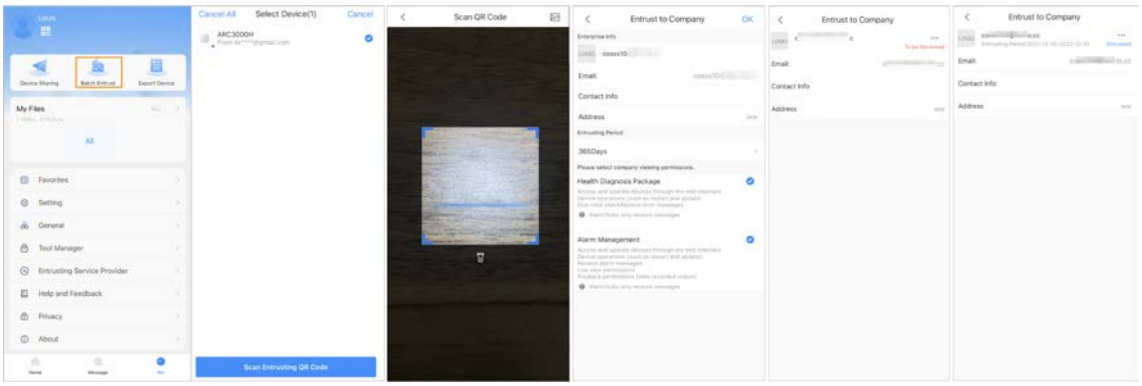
- Pentru a schimba permisiunile, accesați**Încredințați companiei**ecran, apoi atingeți**Schimbați permisiunile**.
- Pentru a retrage permisiunile de încredințare, accesați**Încredințați companiei**ecran, apoi atingeți **Retrage**.
- Pentru a reînnoi perioadele de încredințare, accesați**Încredințați companiei**ecran, apoi atingeți**Reînnoi**.

5.4.1.2.2 Încredințarea dispozitivelor în loturi

Puteți încredința dispozitivele unei singure întreprinderi în loturi. Pasul

1 Pe**Acasă**ecran, selectați**Pe mine**>**Batch Entrust**.

Figura 5-5 Încredeți dispozitivele în loturi



Pasul 2 Pe**Selecteaza dispozitivul**ecran, selectați dispozitivele care urmează să fie încredințate și apoi încredințați-le întreprinderii. Procesul de încredințare a mai multor dispozitive este același cu încredințarea unui singur dispozitiv. Pentru detalii, consultați „5.4.1.2.1 Încredințarea dispozitivului unul câte unul”.

5.4.2 Ștergerea utilizatorilor

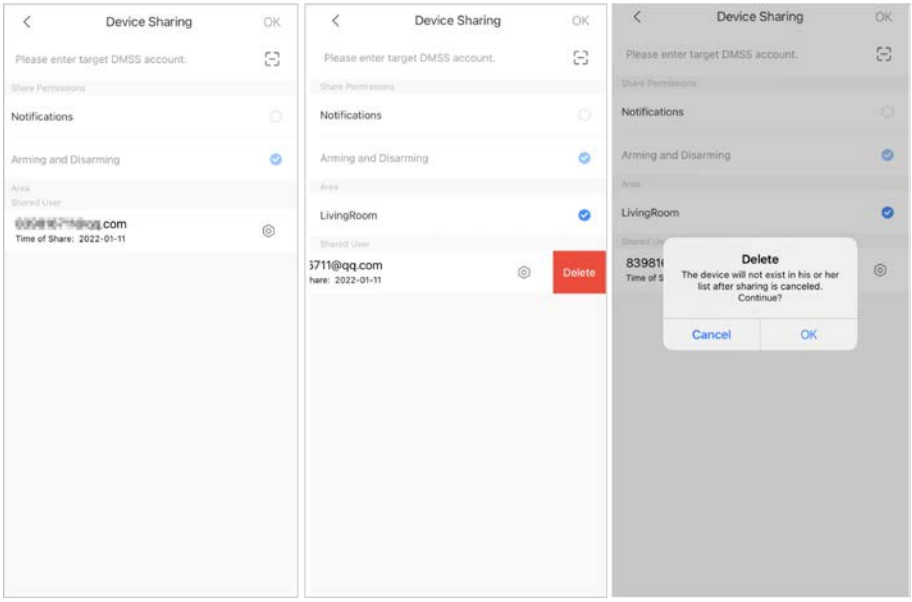
Pentru utilizatorii administratori DMSS, puteți șterge atât instalatorii, cât și utilizatorii generali DMSS.

5.4.2.1 Anularea pentru a partaja dispozitivele

Pentru utilizatorul administrator DMSS, puteți șterge utilizatorii generali DMSS anulând pentru a partaja dispozitivele cu ei pe **Partajarea dispozitivului**ecran. Pentru detalii despre a merge la**Partajarea dispozitivului**ecran, consultați „5.4.1.1 Adăugarea utilizatorilor generali DMSS”. Această secțiune folosește metode pe > **Partajarea dispozitivului**ca o exemplu.

Pasul 1 Pe**Acasă**ecran, atingeți lângă un dispozitiv, apoi atingeți**Partajarea dispozitivului**.

Figura 5-6 Partajare dispozitiv



Pasul 2 În lista de conturi a**Partajarea dispozitivului**ecran, selectați un cont, glisați blocul spre stânga, apoi atingeți**Șterge**. Atingeți**Bine**pentru a anula partajarea.

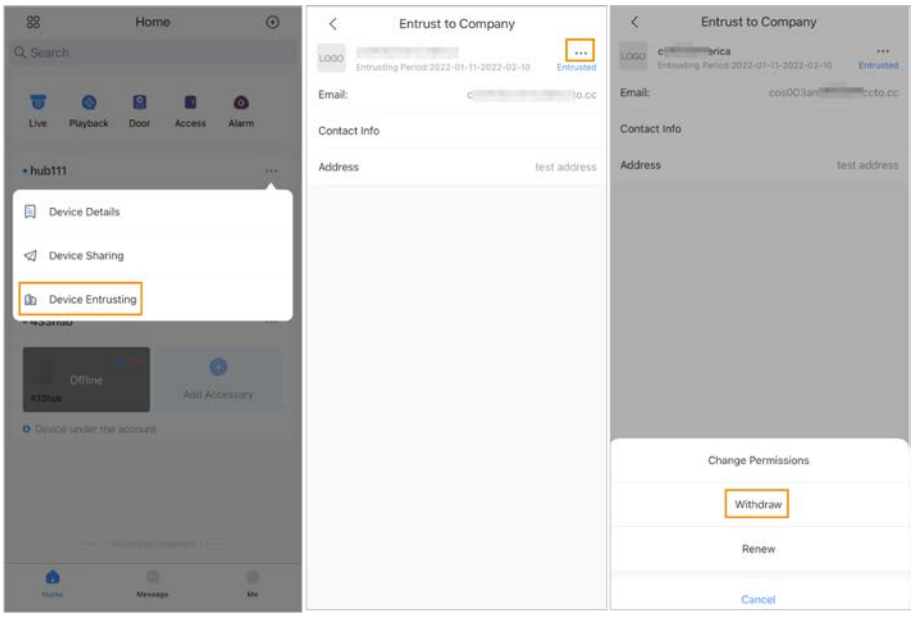
Pasul 3

5.4.2.2 Anularea aplicației de încredințare

Pentru utilizatorii administratori DMSS, puteți șterge un program de instalare prin anularea aplicației de încredințare.

Pasul 1 Pe**Acasă**ecran, atingeți lângă un dispozitiv, apoi atingeți**Încredințarea dispozitivului**.

Figura 5-7 Retragerea cererii de încredințare



Pasul 2 Pe**Încredințarea dispozitivului**ecran, selectați > **Retrage**, apoi atingeți**Bine**.

Un mesaj va fi trimis în contul instalatorului. După ce instalatorul citește mesajul și aprobă cererea dvs. de a anula cererea de încredințare în COS Pro, dvs cererea va fi anulată.

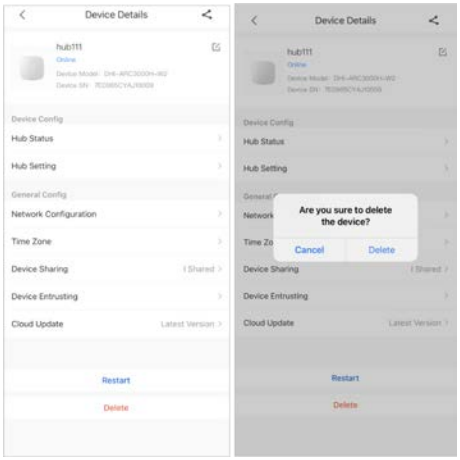
5.4.2.3 Ștergerea dispozitivelor

Pentru utilizatorul administrator DMSS, puteți șterge atât instalatorii, cât și utilizatorii generali DMSS ștergând dispozitive.

Utilizatorul administrator DMSS nu poate șterge un program de instalare dacă dispozitivele sunt partajate de instalator.

Pasul 1 Pe**Acasă**ecran, selectați > **Detalii despre dispozitiv**.

Figura 5-8 Ștergeți dispozitivul



Pasul 2 Pe**Detalii despre dispozitiv**ecran, atingeți**Șterge**.

Pasul 3 Atingeți**Șterge**pentru a șterge dispozitivele.

6 Operațiuni generale

Utilizatorul de la nivelul 2 sau 3 are permisiunea de a arma și dezarma sistemul. Această secțiune folosește operațiunea utilizatorului final pe DMSS ca exemplu.

Cerințe preliminare

- Asigurați-vă că ați adăugat un hub înainte de a efectua configurații.
- Asigurați-vă că hub-ul are o conexiune stabilă la internet.
- Asigurați-vă că hub-ul este dezarmat.

Informații generale

Puteți gestiona centrele de alarmă și accesoriile și puteți efectua operațiuni precum armarea și dezarmarea, configurarea dispozitivelor de alarmă.

Procedură

Pasul 1 Pe ecranul hub, atingeți**Accesorii**pentru a adăuga accesoriile. Pentru detalii despre adăugarea accesoriilor, consultați manualul de utilizare al dispozitivului corespunzător.

Pasul 2 Armați și dezarmați detectoarele într-o singură zonă sau în toate zonele prin operațiuni manuale sau programate.

- Armare și dezarmare unică: Armați și dezarmați detectoarele într-o singură zonă. Pentru detalii, consultați „6.1 Armare și dezarmare unică”.
- Armare și dezarmare globală: Armați și dezarmați detectoarele în toate zonele. Pentru detalii, consultați „6.2 Armare și dezarmare globală”.
- Armare și dezarmare manuală: Armați sistemul de securitate prin aplicația DMSS, tastatură sau telecomandă.
- Programare armare și dezarmare: Armați și dezarmați detectoarele după program. Pentru detalii, consultați „6.4 Armare și dezarmare programată”.

6.1 Armare și dezarmare unică

Puteți arma și dezarma detectoarele într-o singură zonă.

Pasul 1 Pe ecranul hub, atingeți**Zonă**.

Pasul 2 Atingeți o zonă, apoi selectați din**Acasă**,**Departe**,**Dezarma**, și**Dezactivați**în fereastra pop-up.

- **Acasă**: Un mod de armare care vă permite să armați sistemul atunci când vă aflați în zona sistemului de alarmă.
- **Departe**: Armați sistemul când părăsiți zona sistemului de alarmă.
- **Dezarma**: Opriți sistemul de securitate. Opusul armarii.
- **Dezactivați**: Închideți ecranul curent.

6.2 Armarea și dezarmarea globală

Cerințe preliminare

Asigurați-vă că ați activat**Armare/Dezarmare globală**funcţie. Pe ecranul hub, selectați > **Setare hub**, apoi activați**Armare/Dezarmare globală**.

Informații generale

Puteți arma și dezarma detectoarele în toate zonele.

Procedură

Pasul 1 Accesați ecranul hub.

Pasul 2 Alege din**Acasă**,**Departe**, și**Dezarma**pe ecranul de sus.

6.3 Armare și dezarmare manuală

Puteți arma sistemul de securitate prin aplicația DMSS sau telecomandă.

- Pentru a arma și dezarma detectoarele într-o singură zonă sau în toate zonele, consultați „6.1 Armare și dezarmare unică” și „6.2 Armare și dezarmare globală”.
- Pentru a opera prin telecomandă și tastatură, trebuie să atribuiți mai întâi permisiunile de control ale zonelor pentru telecomandă și tastatură. Pentru detalii, consultați manualul utilizatorului pentru telecomandă și tastatură corespunzătoare.

6.4 Armare și dezarmare programate

Puteți seta un program pentru armarea și dezarmarea detectoarelor. Puteți configura planuri de armare, inclusiv zona de armare, moduri și perioade.

Pasul 1 Pe ecranul hub, selectați > **Setare hub**>**Armare/Dezarmare programată**.

Pasul 2 Pe**Armare/Dezarmare programată**ecran, atingeți**Adăuga**, apoi configurați planurile de armare.

- **Nume**: Personalizați un nume pentru planurile de armare.
- **Zonă**: Selectați o singură zonă sau mai multe zone pe care doriți să le armați.
- **Setarea comenzii**: Alege din**Acasă**,**Departe**, și**Dezarma**.
- **Timp**: Setați un timp de armare.

  Pentru a aplica timpul de armare altor zile, atingeți**Repeta**și selectați zilele dorite.
- **Armare forțată**: Selectați după cum este necesar.

Anexa 1 Evenimente de eșec de armare și Descriere

Anexă Tabelul 1-1 Evenimentele de defecțiune a armarii și descrierea (accesorii)

Nu.	Motiv	Descriere
1	ModuleLoss	Accesoriul era offline.
2	HeartErrore	Nu au fost trimise pachete de bătăi inimii de mai mult de 18 minute.
3	Alarma	Alarma (24 ore).
4	Deschis	Capacul din spate al dispozitivului era deschis.
5	exOpen	Capacul din spate al dispozitivului extern era deschis.
6	Tamper	Alarma de manipulare a accesoriilor a fost declanșată.
7	Baterie descarcata	Bateria scăzută a dispozitivului a fost detectată.
8	PriPowerLoss	A fost detectată o întrerupere a alimentării principale a accesoriilor.
9	Pierdere baterie	A fost detectată defecțiunea bateriei.
10	Supratensiune	S-a detectat supratensiune.
11	Supracurent	S-a detectat supracurent.
12	Supraîncălzi	S-a detectat supraîncălzire.
13	Alarma de incendiu	Alarma de incendiu a fost declanșată.
14	Alarmă medicală	Alarma medicală a fost declanșată.
15	SOSAlarm	Alarma SOS a fost declanșată.
16	Alarmă de panică	Alarma de panică a fost declanșată.
17	Alarmă de gaz	Alarma de scurgere de gaz a fost declanșată.
18	IntrusionAlarm	Alarma de intruziune a fost declanșată.
19	HoldUpAlarm	Alarma de panică a fost declanșată.

Anexă Tabelul 1-2 Evenimentele de eșec de armare și descrierea (hub)

Nu.	Motiv	Descriere
1	Alertă SOS	Alarma de panică poate fi declanșată prin aplicația DMSS.
2	Tamper	A fost declanșată alarma de manipulare a centrului de alarmă.
3	Eroare de conectare la server	Hub-ul era offline.
4	Eroare de conectare SIAServer	Există o eroare la conexiunea dintre hub și centrul de recepție a alarmelor SIA.
5	Baterie descarcata	Baterie descărcată a fost detectată.
6	Principala Loss	A fost detectată o întrerupere a alimentării principale.
7	Pierdere baterie	A fost detectată defecțiunea bateriei.

Nu.	Motiv	Descriere
8	NoGSM	Au fost detectate erori ale modulelor 2G/4G.
9	Defecțiune ATS	A fost detectată defecțiunea sistemului de transmisie a alarmei.
10	Defecțiune ATP în rețeaua celulară	A fost detectată o eroare a căii de transmisie a alarmei (defecțiune a rețelei celulare).
11	Defecțiune rețea cu fir/Wi-Fi ATP	A fost detectată o eroare a căii de transmisie a alarmei (defecțiune a rețelei wireless sau Wi-Fi).

Anexa 2 Codurile evenimentului SIA și descrierea

Anexă Tabelul 2-1 Codurile evenimentului SIA și descrierea

Nu.	Eveniment	Cod CID	Descriere
1	Alarmă de mișcare	130 133 134	130: Alarma efractie. 133: Alarmă de 24 de ore (sigură). 134: Alarmă de intrare/ieșire.
2	Detector de ușă de alarmă Restabili	130 133 134	130: Alarma efractie. 133: Alarmă de 24 de ore (sigură). 134: Alarmă de intrare/ieșire.
3	Alarmă de intrare externă Restabili	130 133 134	130: Alarma efractie. 133: Alarmă de 24 de ore (sigură). 134: Alarmă de intrare/ieșire.
4	Alarmă de constrângere	121	Alarmă de constrângere.
5	Alarmă SOS	120	Alarmă de panică.
6	Alarmă de intruziune	130 133 134	130: Alarma efractie. 133: Alarmă de 24 de ore (sigură). 134: Alarmă de intrare/ieșire.
7	Alarma de incendiu	110	Alarma de incendiu.
8	Alarma de scurgere de gaz	151	Gaz detectat Alarmă.
9	Alarma medicala	100	Alarma medicala.
10	Alarmă de reținere	120	Alarmă de panică.
11	Controller Tamper Rezolvat	137	Tamper.
12	Tamper periferic Rezolvat	383	Tamper senzor.
13	Dispozitiv extern Modificarea a fost rezolvată	383	Tamper senzor.
14	Voltajul bateriei Restaurat	302	Baterie de sistem scăzută.
15	Recuperarea defecțiunii bateriei	311	Baterie lipsă/ moartă.
16	Putere restabilită	301	Pierderea AC.
17	Bruiaj RF	344	Detectare blocaj receptor RF.
18	Transmisie de alarmă Eroare de sistem restaurată	350	Probleme de comunicare.
19	Transmisie de alarmă Defect de cale Erori restaurate/Wi-Fi Recuperare	350	Probleme de comunicare.

Nu.	Eveniment	Cod CID	Descriere
20	Transmisie de alarmă Defect de cale Restaurat/Wireless Erori de rețea Recuperare	350	Probleme de comunicare.
21	Periferic Nu Conectat restaurat	381	Pierderea supravegherii - RF.
22	Periferic Scăzut Alarma baterie Recuperare	302	Baterie de sistem scăzută.
23	Baterie periferică Recuperare defecțiuni	311	Baterie lipsă/ moartă.
24	Principalul periferic Pana de curent Restaurat	301	Pierderea AC.
25	Defecțiunea RF-HD a fost restaurată	354	Eșecul comunicării evenimentului.
26	Dispozitiv blocat și Deblocat	501	Acces cititor dezactivat.
27	Supratensiune Protecție restaurată	319	Supratensiune sursă de alimentare.
28	Supracurent Protecție restaurată	312	Supracurent sursă de alimentare.
29	Protecție la supraîncălzire Restaurat	318	Supraîncălzirea sursei de alimentare.
30	Temperatura ridicata Alarma restabilită	158	Temperatură înaltă.
31	Temperatura scazuta Alarma restabilită	159	Temperatură scăzută.
32	Braţ	400 (aplicație) 401 (Tastatură) 403 (programat armare) 407 (Bloc pentru chei) 408 (armare globală)	400: Deschis/Închidere. 401: O/C de către utilizator. 403: O/C automată. 407: Armare/dezarmare la distanță. 408: Braț rapid.
33	Dezarma	400 (aplicație) 401 (Tastatură) 403 (programat armare) 407 (Bloc pentru chei) 408 (Fără parolă armare)	400 Deschis/Închidere. 401 O/C de către utilizator. 403 O/C automată. 407 Armare/dezarmare la distanță. 408 Braț rapid.
34	Armare acasă	441	STAY înarmat.

Nu.	Eveniment	Cod CID	Descriere
35	Eșec de armare	454 (Eșec la armare) 455 (programat eșec de armare) 457 (Întârziere la ieșire eșec de armare)	454 Închiderea eșuată. 455 Armarea automată a eșuat. 457 Eroare de ieșire (utilizator).
36	Armare forțată	450	Excepție O/C.
37	Dezactivare periferică Recuperare	502	Dezactivat temporar.
38	Dezactivați doar manipularea Recuperare alarmă	503	Dezactivat temporar.
39	Raport de testare manuală	601	Raport de testare a declanșării manuale.

Anexa 3 Recomandări de securitate cibernetică

Securitatea cibernetică este mai mult decât un cuvânt la modă: este ceva care se referă la fiecare dispozitiv care este conectat la internet. Supravegherea video IP nu este imună la riscurile cibernetice, dar luarea unor pași de bază pentru protejarea și consolidarea rețelelor și a dispozitivelor în rețea le va face mai puțin susceptibile la atacuri. Mai jos sunt câteva sfaturi și recomandări de la Dahua despre cum să creați un sistem de securitate mai securizat.

Acțiuni obligatorii care trebuie întreprinse pentru securitatea de bază a rețelei dispozitivului:

1.**Utilizați parole puternice**

Consultați următoarele sugestii pentru a seta parole:

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

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

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

Recomandări „Îmi place” pentru a îmbunătăți securitatea rețelei dispozitivului dvs.:

1.**Protecție fizică**

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

2.**Schimbați parolele în mod regulat**

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

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

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

4.**Activați Blocarea contului**

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

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

Vă sugerăm să schimbați HTTP implicit și alte porturi de serviciu în orice set de numere între

1024–65535, reducând riscul ca persoanele din afară să poată ghici ce porturi utilizați.

6.**Activați HTTPS**

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

7.**Legarea adresei MAC**

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

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

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

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

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

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

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

10.**Transmisie criptată audio și video**

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

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

11.**Audit securizat**

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

12.**Jurnal de rețea**

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

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

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

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

dispozitiv.

Mai multe informatii

Vă rugăm să vizitați site-ul oficial Dahua Centrul de răspuns în caz de urgență pentru anunțuri de securitate și cele mai recente recomandări de securitate.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883