Centralina di allarme

Manuale dell’utente

ZHEJIANG DAHUA VISION TECHNOLOGY CO. LTD. V2.0.0

Introduzione

Generale

Questo manuale illustra la procedura di installazione, le funzioni e l'utilizzo della centralina di allarme (di seguito denominata "la centralina"). Leggere attentamente il manuale prima di utilizzare il dispositivo e conservarlo per future consultazioni.

Istruzioni di sicurezza

Nel manuale possono comparire i seguenti indicatori di pericolo.

Indicatori di pericolo	Significato
PERICOLO	Indica una situazione ad alto rischio che, se non viene evitata, può causare il decesso o gravi lesioni.
AVVERTENZA	Indica una situazione a medio o basso rischio che, se non viene evitata, può causare lesioni di leggera o moderata entità.
ATTENZIONE	Indica un rischio potenziale che, se non evitato, può causare danni materiali, perdite di dati, riduzione delle prestazioni o altre conseguenze imprevedibili.
SUGGERIMENTI	Spiegano metodi utili per risolvere un problema o per aiutarvi a risparmiare tempo.
NOTA	Fornisce informazioni aggiuntive che sottolineano e completano quelle riportate nel testo.

Cronologia delle revisioni

Versione	Contenuto della revisione	Data di rilascio
V2.0.0	• Aggiunta delle configurazioni di rete. • inserimento. • Aggiunta dei codici e delle descrizioni degli eventi SIA.	Novembre 2022
V1.1.0	• Aggiunta delle operazioni su COS Pro e sull'app DMSS. • Aggiunta della gestione degli utenti. • Aggiornamento delle immagini. • Aggiornamento delle descrizioni dei parametri.	Febbraio 2022
V1.0.0	Prima versione.	Ottobre 2021

Informativa sulla protezione della privacy

È possibile che chi utilizza i dispositivi o gestisce i dati raccolga dati personali di altre persone, come il volto, le impronte digitali e il numero di targa dei veicoli. Gli utenti devono rispettare le norme e le leggi locali in materia di protezione della privacy per garantire il rispetto dei diritti e degli interessi legittimi di terzi. A questo scopo occorre adottare misure appropriate come, a titolo esemplificativo e non esaustivo, l'utilizzo di segnali chiari e ben visibili per informare le persone dell'esistenza di un impianto di sorveglianza nell'area, con l'indicazione delle informazioni di contatto richieste.

Informazioni sul manuale

- Questo manuale serve solo come riferimento. Possono esserci lievi differenze rispetto al prodotto effettivo.
- Decliniamo ogni responsabilita in relazione a eventuali perdite causate da utilizzi del prodotto non conformi a quanto riportato nel manuale.
- Il manuale verra aggiornato in base alle leggi e ai regolamenti pid recenti delle relative giurisdizioni. Per informazioni dettagliate, consultare il manuale d'uso in formato cartaceo, utilizzare il CD-ROM, scansionare il codice QR o visitare il nostro sito web ufficiale. Questo manuale serve solo come riferimento. E possibile che sussistano delle lievi differenze tra la versione elettronica e cartacea del manuale.
- Design e software sono soggetti a modifica senza preavviso. A seguito degli aggiornamenti del prodotto possono sorgere differenze tra il prodotto effettivo e le informazioni contenute nel manuale. Contattare il servizio di assistenza per il software e la documentazione supplementare pid recenti.
- E possibile che siano presenti errori di stampa o discrepanze nella descrizione delle funzioni, delle operazioni e dei dati tecnici. In caso di dubbi o vertenze, ci riserviamo il diritto di interpretazione finale.
- Se non é possibile aprire il manuale in formato PDF, aggiornare il programma per la lettura dei file PDF o provarne un altro.
- Tutti i marchi commerciali, i marchi registrati e i nomi di societa presenti nel manuale sono di proprieta dei rispettivi titolari.
- In caso di problemi durante l'utilizzo del dispositivo, consultare il nostro sito web oppure contattare il fornitore o il servizio di assistenza al cliente.
- In caso di dubbi o controversie, ci riserviamo il diritto di interpretazione finale.

Norme di sicurezza e avvertenze importanti

Questa sezione descrive le procedure per una corretta gestione del dispositivo e per la prevenzione dei rischi e dei danni materiali. Leggerla attentamente prima di utilizzare il dispositivo e rispettare le indicazioni fornite.

Requisiti di funzionamento

- Prima dell'uso, controllare che la fonte di alimentazione del dispositivo funzioni correttamente.
- Non scollegare il cavo di alimentazione del dispositivo mentre questo è acceso.
- Usare il dispositivo solo con tensioni comprese nell'intervallo specificato.
- Trasportare, utilizzare e conservare il dispositivo nelle condizioni di umidità e temperatura consentite.
- Evitare che il dispositivo entri in contatto con i liquidi. Non posizionare sul dispositivo contenitori pieni di liquidi, per evitare che possano entrare nell'apparecchio.
- Non smontare il dispositivo.

Requisiti per l'installazione

AVVERTENZA

- Prima di accendere il dispositivo, collegarlo all'alimentatore.
- Rispettare scrupolosamente le norme locali sulla sicurezza elettrica, verificando che la tensione sia stabile e conforme ai requisiti di alimentazione del dispositivo.
- Non collegare il dispositivo a più di un alimentatore. In caso contrario, il dispositivo potrebbe danneggiarsi.

- Osservare tutte le procedure di sicurezza e indossare i dispositivi di protezione necessari quando si lavora in quota.
- Non esporre il dispositivo alla luce solare diretta o a fonti di calore.
- Non installare il dispositivo in ambienti umidi o con presenza di polvere o fumo.
- Installare il dispositivo in un ambiente ben ventilato e non ostruire le aperture di ventilazione.
- Utilizzare l'adattatore o l'unità di alimentazione indipendente forniti dal produttore del dispositivo.
- La fonte di alimentazione deve rispondere ai requisiti ES1 dello standard IEC 62368-1 e non deve superare il livello PS2. I requisiti di alimentazione sono indicati sulla targhetta del dispositivo.
- Collegare gli apparecchi elettrici di classe I a una presa con messa a terra di protezione.

Indice

Introduzione.....I
Norme di sicurezza e avvertenze importanti.....III
1 Introduzione.....1
1.1 Panoramica.....1
1.2 Specifiche tecniche.....1
1.3 Contenuto della confezione.....6
2 Design.....7
2.1 Aspetto.....7
2.2 Dimensioni.....8
3 Avvio.....9
3.1 Utenti.....9
3.2 Procedura di funzionamento.....10
4 Operazioni effettuabili dagli installatori sull'app DoLynk.....13
4.1 Accesso a DoLynk.....13
4.2 Aggiunta di dispositivi.....15
4.2.1 Aggiunta della centralina.....15
4.2.1.1 Aggiunta tramite n.di serie/codice QR.....15
4.2.1.2 Aggiunta tramite configurazione AP.....16
4.2.1.3 Aggiunta tramite ricerca LAN.....18
4.2.2 Aggiunta di Accessori.....19
4.3 Gestione degli utenti.....20
4.3.1 Aggiunta di amministratori DMSS.....20
4.3.1.1 Prestito dei dispositivi agli amministratori DMSS.....20
4.3.1.2 Accettazione delle richieste di affidamento.....21
4.3.2 Eliminazione degli utenti.....23
4.3.2.1 Annullamento del prestito dei dispositivi.....23
4.3.2.2 Eliminazione dei dispositivi.....24
4.4 Richiesta delle autorizzazioni agli amministratori DMSS.....25
4.5 Consegna dei dispositivi agli amministratori DMSS.....25
4.6 Gestione del funzionamento e dello stato dei dispositivi.....26
4.6.1 Verifica dello stato dei dispositivi.....26
4.6.2 Configurazioni di base del dispositivo.....26
4.6.2.1 Visualizzazione dello stato.....27
4.6.2.2 Configurazione della centralina.....28
4.6.3 Correzione degli errori.....32

4.6.4 Visualizzazione delle valutazioni 32
5 Operazioni effettuabili dagli utenti finali sull'app DMSS 33
5.1 Accesso all'app DMSS. 33
5.2 Aggiunta di dispositivi 34
5.2.1 Aggiunta della centralina. 34
5.2.2 Aggiunta di accessori. 35
5.3 Impostazioni generali della centralina. 35
5.3.1 Configurazione della centralina. 35
5.3.2 Configurazione di rete 35
5.3.2.1 Configurazione della rete cablata. 35
5.3.2.2 Configurazione della rete Wi-Fi. 36
5.3.2.3 Configurazione della rete cellulare 36
5.4 Gestione degli utenti 37
5.4.1 Aggiunta degli utenti 37
5.4.1.1 Aggiunta di utenti DMSS generici. 37
5.4.1.2 Aggiunta degli installatori. 37
5.4.1.2.1 Affidamento dei dispositivi uno per volta 38
5.4.1.2.2 Affidamento in serie dei dispositivi. 39
5.4.2 Eliminazione degli utenti 39
5.4.2.1 Annullamento della condivisione dei dispositivi. 39
5.4.2.2 Annullamento delle richieste di affidamento 40
5.4.2.3 Eliminazione dei dispositivi. 41
6 Operazioni generali. 42
6.1 Inserimento e disinserimento singolo. 42
6.2 Inserimento e disinserimento globale. 43
6.3 Inserimento e disinserimento manuale 43
6.4 Inserimento e disinserimento programmati 43
Appendice 1 Descrizione degli errori di inserimento 45
Appendice 2 Descrizione dei codici evento SIA 47
Appendice 3 Raccomandazioni sulla sicurezza informatica 50

1 Introduzione

1.1 Panoramica

La centralina di allarme é un dispositivo adottato nei sistemi di sicurezza che controlla il funzionamento di tutti gli accessori connessi. Se viene rilevata la presenza, l'ingresso, o il tentativo di ingresso di un intruso nell'area coperta dal sistema di sicurezza, la centralina riceve i segnali di allarme da parte dei rilevatori e avvisa gli utenti.

1.2 Specifiche tecniche

Questa sezione contiene ie specifiche tecniche del dispositivo. Fare riferimento alle informazioni che corrispondono al modello in uso.

Tabella 1-1 Specifiche tecniche

Tipo	Parametro	Descrizione
Porta	Rete	1 porta Ethernet autoadattiva RJ-45 10/100 Mbps
	GSM	SIM unica (GSM: 900/1800 MHz); doppia SIM, di cui una in standby
	LTE	SIM unica (GSM: 900/1800 MHz, WCDMA: B1/B5/B8, LTE-FDD: B1/B3/BS/B7/B8/B20, LTE-TDD:B38/B40/B41); doppia SIM, di cui una in standby
	Batteria	Porta per batteria da 12 V
	Indicatore luminoso	1, con segnalazione dei vari stati (allarme, inserimento, disinserimento, traffico di rete e guasto)
	Pulsante	1 pulsante di reset, 1 pulsante di accensione, 1 pulsante AP
	Segnalatore acustico	Integrato
	Manomissione	1 porta per il rilevamento delle manomissioni dell'involucro del pannello di controllo dell'allarme
Funzione	SMS di notifica	SMS di allarme (fino a 5 numeri di telefono) Disponibile solo su alcuni modelli.
	Chiamate di notifica	Si (fino a 5 numeri di telefono) Disponibile solo su alcuni modelli.
	Collegamento video	Si
	Protocolli di rete	TCP/IP, comprendente PPTP, L2TP, DHCP, UPNP e NTP
	Aggiornamento remoto	Aggiornamento via cloud

Tipo	Parametro	Descrizione	
	Metodo di configurazione	App	
	Metodo di inserimento e disinserimento	App, tastierino, radiocomando, attivazione programmata	
	Numero di periferiche	Periferiche wireless per un massimo di 150 canali (6 sirene, 64 radiocomandi wireless, 4 ripetitori e 8 tastierini)	
	Zone	32 zone (stanze)	
	Gestione dell'alimentazione	Passaggio automatico dalla fonte di alimentazione principale a quella di riserva	
		Allarme di interruzione di corrente	
		Allarme di guasto e problemi di tensione della batteria	
	Log degli eventi	Massimo 400	
	Protezione contro le interruzioni di corrente per i parametri configurati	Si	
	Gestione utenti	Massimo 8 utenti: 1 installatore,1 amministratore, 6 utenti generici	
	Interrogazioni	Ricerca dei messaggi push, stato del dispositivo e versione del programma. Rilevamento della potenza del segnale.	
RF	Frequenza portante	DHI-ARA3000H-FW2 (868)/ DHI-ARA3000H-GW2 (868)/ DHI-ARA3000H-W2 (868): 868,0-868,6 MHz	DHI-ARA3000H-FW2/ DHI-ARA3000H-GW2/ DHI-ARA3000H-W2: 433,1-434,6 MHz
	Distanza di comunicazione	DHI-ARA3000H-FW2 (868)/ DHI-ARA3000H-GW2 (868)/ DHI-ARA3000H-W2 (868): Fino a 2000 m (6561,68 ft) in campo aperto	DHI-ARA3000H-FW2/ DHI-ARA3000H-GW2/ DHI-ARA3000H-W2: Fino a 1200 m (3937,01 ft) in campo aperto
	Potenza di trasmissione	DHI-ARA3000H-FW2 (868)/ DHI-ARA3000H-GW2 (868)/ DHI-ARA3000H-W2 (868): Limite di 25 mW	DHI-ARA3000H-FW2/ DHI-ARA3000H-GW2/ DHI-ARA3000H-W2: Limite di 10 mW
	Meccanismo di comunicazione	Bidirezionale	
	Tipo di crittografia	AES128	
	Frequency Hopping	Si	
	Rilevamento delle interferenze RF	Il sistema riporta le informazioni di interferenza RF se, durante un rilevamento di 60 secondi, l'interferenza dura più di 30 secondi.	
	Wi-Fi	2,4 GHz	

Tipo	Parametro	Descrizione
Alimen-tazione	Tipo di alimentazione	Tipo A
	Alimentazione principale	12 V CC, 1,5 A
	Capacita delle batterie	2 x 3,6 V/2150 mAh
	Durata delle batterie in standby	Fino a 12 h La durata delle batterie in standby puo raggiungere 12 ore nelle seguenti condizioni: • Connessione alla rete Wi-Fi, GPRS/3G/4G. • Connessione alia centrale di ricezione degli allarmi (ARC) e intervallo heartbeat di 1800 secondi. • Connessione a 8 ingressi e 1 sirena. • Connessione al cloud.
	Tipo di batterie	Tipo di batterie: ricaricabili ai polimeri di lito, integrate; modello: 18650
	Corrente massima disponibile	3,5 A
	Potenza assorbita	Max 15 W
	Consumo di corrente	Normale: 220 mA; allarme: 300 mA
	Soglia di batteria scarica	3,5 V CC
	Soglia di ripristino della batteria	3,7 V CC
	Tensione di rilascio	< 3,358 V
	Tempo di ricarica della batteria	80% in circa 15 h
Comuni-cazione ARC	Categoria ATS	DP2/SP2 (LAN/Wi-Fi e GPRS/4G)
	Acknowledgment	Pass-through
	Protocolli	SIA-DC09
	Canale di trasmissione primario	LAN/Wi-Fi (NO 50136-2)
	Canale di trasmissione secondario	GPRS/4G
	Apparecchiatura di notifica	C/E/F

Tipo	Parametro	Descrizione	
Certificazioni		DHI-ARA3000H-FW2 (868)/DHI-ARA3000H-GW2 (868)/DHI-ARA3000H-W2 (868): EN 50131-1:2006+A1 :2009+A2 :201 7+A3:2020 EN 50131-3:2009 EN 50131-6:2017 EN 50131-5-3:201 7 EN 50131-10: 20J 4 EN 50136-2: 2013 Grado di sicurezza 2 Classe ambientale II CE	DHI-ARA3000H-FW2/ DHI-ARA3000H-GW2/ DHI-ARA3000H-W2: FCC CE

Tabella 1-2 Categoria ATE

Categoria ATE	Tempo di segnalazione	Protocolli	Dispositivi di comunicazione			Dispositivo di comunicazione da utilizzare
			PSTN	2G/3G	IP	
SP2	25 h	Standard				Il dispositivo con il segno di spunta
SP3	30 min	Standard		√	√	Solo uno dei due dispositivi con il segno di spunta
SP4	3 min	Crittografati		√	√	Solo uno dei due dispositivi con il segno di spunta
SP5	90 s	Crittografati		√	√	Solo uno dei due dispositivi con il segno di spunta
DP1	25 h	Standard		√	√	Solo due dei tre dispositivi con il segno di spunta
DP2	30 min	Standard		√	√	Solo due dei tre dispositivi con il segno di spunta
DP3	3 min	Crittografati		√	√	I due dispositivi con il segno dispunta
DP4	90 s	Crittografati		√	√	I due dispositivi con il segno dispunta

Categoria ATE	Tempo di segnalazione	**Protocolli**	Dispositivi di **comunicazione**			Dispositivo di **comunicazione da utilizzare**
			PSTN	**2G/3G**	**iP**	
ATE: apparecchiature per la trasmissione degli allarmi. SPx (percorso singolo): valore che indica il livello di prestazioni raggiunto da un dispositivo di comunicazione singolo secondo lo standard EN 50136—1. DPx (percorso doppio): valore che indica il livello di prestazioni raggiunto dalla combinazione di due dispositivi di comunicazione, secondo lo standard EN 50136—1. Tempo di segnalazione: stabilito in base allo standard di ciascun livello di prestazioni, il tempo di segnalazione é il tempo massimo a disposizione per segnalare la mancata trasmissione di un allarme. I dispositivi per la trasmissione degli allarmi rispettano questo requisito riportando regolarmente il loro stato tramite una funzione di test simbolica specifica. Protocolli: viene indicato il livello di sicurezza dei protocolli utilizzati per la notifica degli errori. I protocolli standard e voce sono crittografati. I protocolli di elevata sicurezza sono crittografati con chiave AES a 128 bit o a 256 bit. Dispositivi di comunicazione: i dispositivi di comunicazione implementati. Dispositivi di comunicazione da utilizzare: vengono indicati il numero e il tipo di dispositivi di comunicazione che devono essere utilizzati in base alia categoria ATE.						

Tabella 1-3 Specifiche tecniche

Specifiche Tecniche	**Descrizione**
Classificazione ACE	Tipo A
Classe ambientale	II
Tensione di alimentazione	12 V CC, 1,5 A
Dimensioni del prodotto	163 x 163 x 32 mm (6,42 x 6,42 x 1.26″)
Dimensioni dell'imballaggio	219 x 187 x 91 mm (8,62 x 7,36 x 3,58″)
Temperatura di funzionamento	Da -10 a +50°C (da +14 a +122 °F) Da -10 a +40 °C (da +14 a +104°F) (temperatura certificata)
Umidita	10-90% (UR)
Peso Netto	0,38 kg (0,84 lb)
Peso Lordo	0,8 kg (1,76 lb)
Alloggiamento	PC + ABS

1.3 Contenuto della confezione

Verificare il contenuto della confezione usando la lista di controllo che segue. In presenza di componenti danneggiati o rotti, contattare l'assistenza clienti.

Figura 1-1 Contenuto della confezione

1 2 3 4 5 6 7

Tabella 1-4 Contenuto della confezione

N.	Nome dell'oggetto	Quantità	N.	Nome dell'oggetto	Quantità
1	Centralina di allarme	1	5	Informazioni su leggi e normative	1
2	Cavo	1	6	Kit di viti	1
3	Alimentatore	1	7	Clip per il fissaggio dei cavi	1
4	Guida di avvio rapido	1			

2 Design

2.1 Aspetto

Figura 2-1 Aspetto

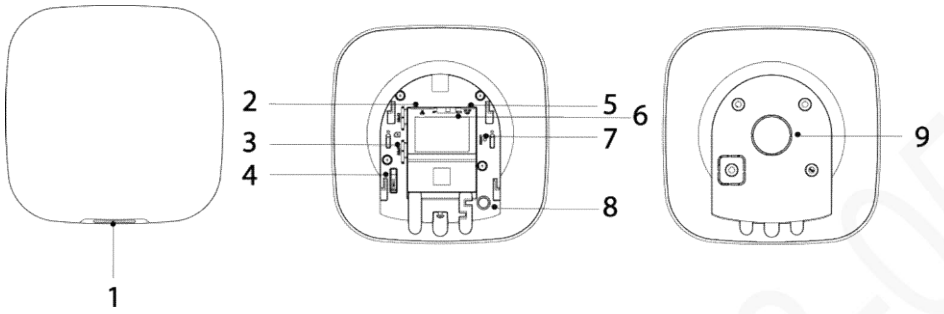


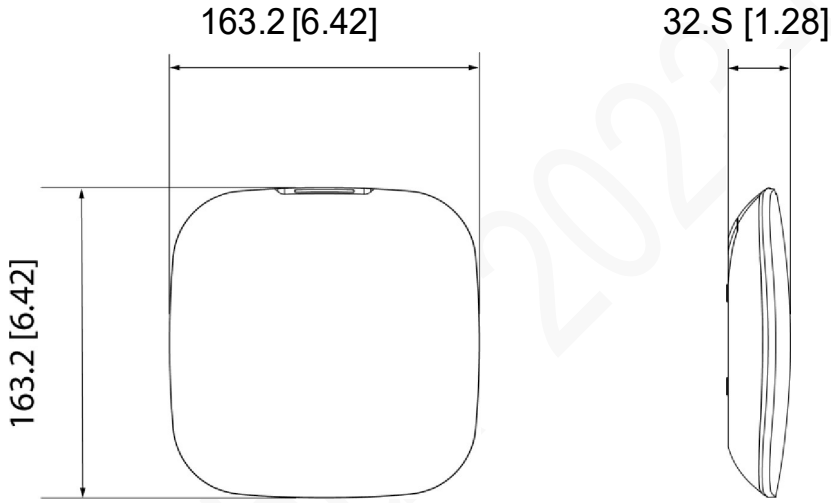
Tabella 2-1 Struttura

N.	Nome	Descrizione
1	Indicatore	• • Verde lampeggiante: la centralina inizia a funzionare. • Giallo fisso: connessione al cloud non riuscita. • Verde fisso: modalità di disinserimento. • Blu fisso: modalità di inserimento. • Rosso lampeggiante: attivazione di un evento di allarme. • Giallo lampeggiante: malfunzionamento rilevato. • centralina alle periferiche in corso. • Blu lampeggiante rapido: modalità emissione scheda.
2	Presa Ethernet	Serve a collegare la centralina a una rete Ethernet.
3	Slot micro SIM 1 e 2	Inserire la scheda principale nel primo slot e la scheda standby nel secondo. • standby. • dati cellulare e inviare notifiche push di allarme. • Le schede SIM non funzioneranno fino al completamento • La funzione SIM è disponibile solo su alcuni modelli.
4	Pulsante manomissione	Quando il pulsante viene rilasciato, si attiva l'allarme antimanomissione.
5	Presa di alimentazione	La presa a cui collegare il cavo di alimentazione.
6	AP	Attivando la funzione AP, il telefono si connetterà all'hotspot della centralina, sincronizzando il nome utente e la password Wi-Fi con quest'ultima.

N.	Nome	Descrizione
7	Pulsante di ripristino	Tenere premuto questo pulsante per 10 secondi per riavviare la centralina e ripristinare le impostazioni predefinite di fabbrica.
8	Pulsante di accensione/ spegnimento	Tenere premuto il pulsante per 2 secondi per accendere o spegnere la centralina.
9	Coperchio posteriore	Se viene aperto il coperchio posteriore, si attiva l'allarme antimanomissione.

2.2 Dimensioni

Figura 2-2 Dimensioni (unita di misura: mm [pollici])



3 Avvio

3.1 Utenti

Gli utenti possono essere creati solo sulle app DMSS e COS Pro. È opportuno classificare gli utenti in base al ruolo, così da poter assegnare loro livelli di accesso differenti per l'utilizzo dei dispositivi.

Livelli di accesso degli utenti

Tabella 3-1 Livelli di accesso degli utenti

Utente	Livello di accesso
Amministratore DMSS	L2
Utente DMSS generico	L2
Installatore	L3

- Installatore: gli installatori forniscono servizi operativi e di manutenzione agli utenti finali. Devono richiedere le autorizzazioni per l'utilizzo dei dispositivi agli utenti finali (amministratori DMSS). Possono ottenere le autorizzazioni per operazioni come la configurazione dei dispositivi e la gestione degli utenti.
- Amministratore DMSS: l'amministratore è un utente finale. Questo ruolo non può essere modificato e possiede autorizzazioni per operazioni come la configurazione dei dispositivi e la gestione degli utenti. Gli amministratori DMSS non possiedono le autorizzazioni per configurare il dispositivo quando affidano la centralina all'installatore o quando gli installatori prestano loro la centralina.
- Utente DMSS generico: sono utenti con cui gli amministratori DMSS condividono i dispositivi tramite l'app DMSS. Questo ruolo può essere modificato e possiede solo autorizzazioni di base, come la visualizzazione dello stato del dispositivo o l'inserimento e il disinserimento degli allarmi nelle stanze.

Procedura operativa

Di seguito vengono illustrate le procedure di affidamento e condivisione sulle app DMSS e COS Pro. Gli installatori e gli utenti finali possono seguirle per condividere e affidare i dispositivi.

Figura 3-1 Procedura operativa (utente DMSS)

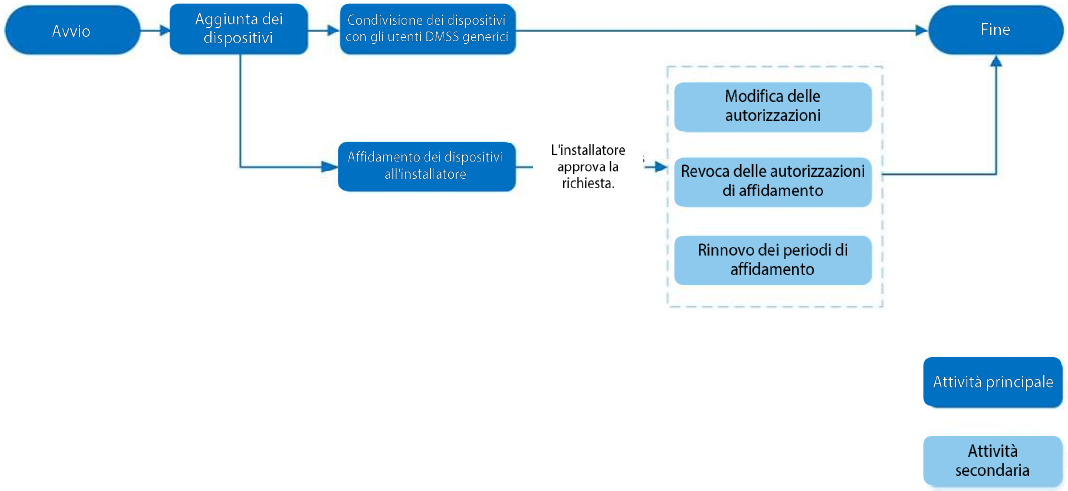
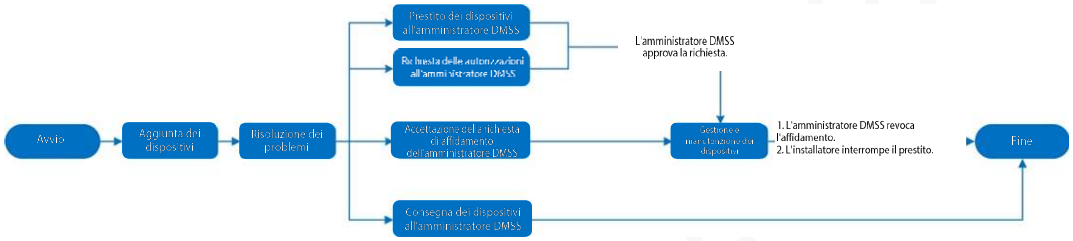


Figura 3-2 Procedura operativa (installatore)



3.2 Procedura di funzionamento

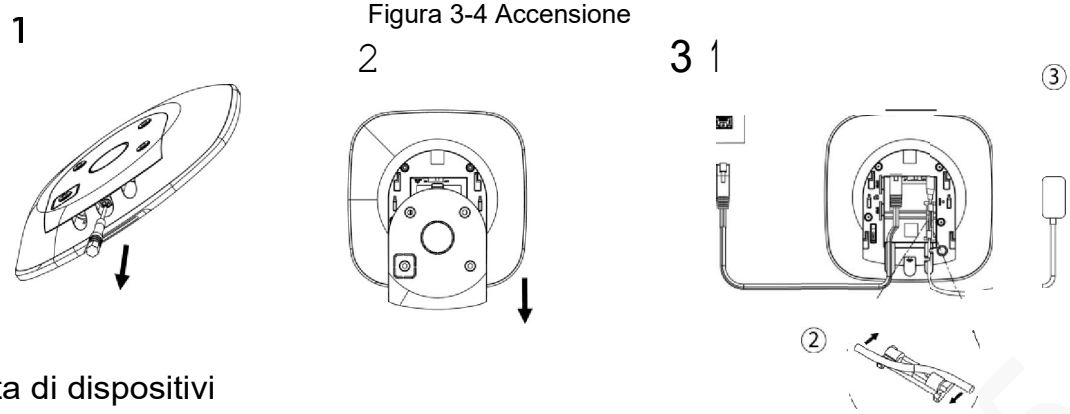
Attenersi alle procedure illustrate di seguito per attivare il sistema di allarme wireless.

Figura 3-3 Procedura di funzionamento

Accensione

Connettere la centralina a una rete Ethernet e accenderla.

Figura 3-4 Accensione



Aggiunta di dispositivi

1. Aggiungere la centralina alle app DoLynk e DMSS. Per ulteriori dettagli, consultare le sezioni "4.2 Aggiunta dei dispositivi" e "5.2 Aggiunta dei dispositivi".
2. Aggiungere gli accessori alia centralina. Per ulteriori dettagli, consultare ie sezioni "4.2.2 Aggiunta di accessori" e "5.2.2 Aggiunta di accessori".

Installazione della centralina

Consigliamo di installare la centralina utilizzando viti con tasselli a espansione. Non posizionare la centralina nelle seguenti zone:

- All'esterno.
- Vicino a oggetti metallici in grado di attenuare o schermare il segnale radio.
- In luoghi con una scarsa ricezione del segnale GSM.
- In luoghi vicino a fonti di interferenze radio che si trovino a meno di 1 metro di distanza dal router e dai cavi di alimentazione.
- In ambienti con temperatura o umidita superiori ai livelli consentiti.

Figura 3-5 Installazione

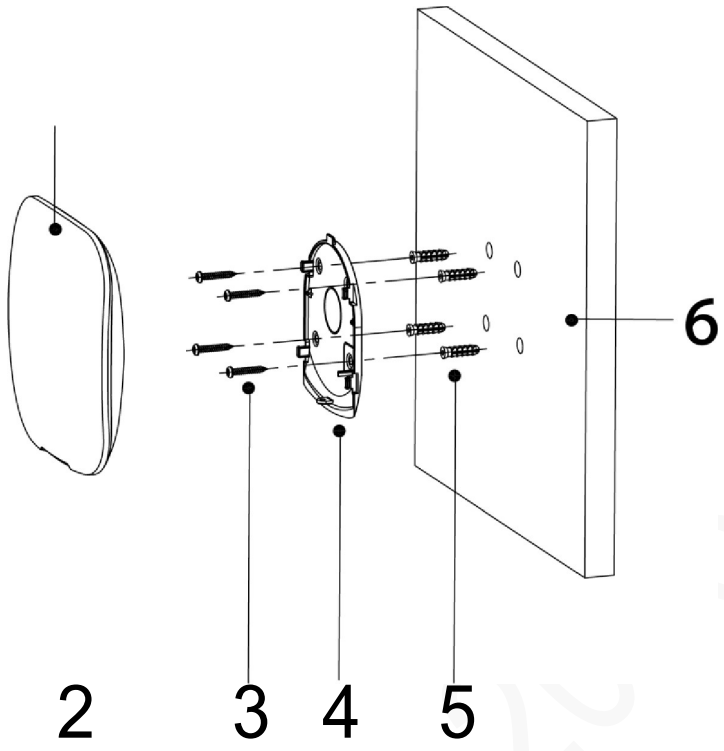


Tabella 3-2 Elementi della procedura di installazione

N.	Nome dell'oggetto	N.	Nome dell'oggetto
1	Centralina	4	Piastra di montaggio
2	Viti a testa svasata M3 x 8 mm	5	Bullone di espansione
3	Viti autofilettanti ST4 x 25 mm	6	Parete

1. Dopo averne confermato la posizione, praticare i fori per le viti sulla piastra di montaggio.
2. Inserire i tasselli a espansione nei fori.
3. Posizionare la piastra di montaggio sul muro, quindi allineare i fori per ie viti sulla piastra ai tasselli a espansione.
4. Fissare la piastra di montaggio con le viti autofilettanti ST4 x 25 mm.
5. Posizionare la centralina di allarme sulla piastra di montaggio, facendola scorrere dall'alto verso il basso.
6. Fissare la centralina di allarme con le viti a testa svasata M3 x 8 mm.

Configurazione della centralina

Configurare la centralina sulle app DoLynk e DMSS. Per ulteriori dettagli, consultare la sezione "4.6.2 Configurazioni di base del dispositivo".

Inserimento del sistema di allarme

Per inserire il sistema di allarme, é possibile utilizzare il tastierino, il radiocomando e l'app. Quando un comando di inserimento viene inviato alle app DoLynk e DMSS, il sistema verifica il proprio stato. In presenza di un guasto, é necessario scegliere se procedere con l'inserimento forzato. Per ulteriori dettagli sull'inserimento e il disinserimento del sistema, consultare la sezione "6 Operazioni generali". Per informazioni dettagliate sugli accessori, consultare i relativi manuali d'uso.

4 Operazioni effettuabili dagli installatori sull'app DoLynk

L'app DoLynk é pensata per aiutare gli installatori a fornire servizi professionali per l'utilizzo e la manutenzione dei dispositivi agli utenti finali. Inoltre, offre funzioni che comprendono la gestione dei siti, la gestione del funzionamento e dello stato dei dispositivi, la revisione delle procedure di affidamento dei dispositivi e molto altro. Per ulteriori dettagli, consultare il manuale d'uso dell'app *DoLynk.*

Le figure servono unicamente a scopo illustrativo e potrebbero differire dall'interfaccia reale.

4.1 Accesso a DoLynk

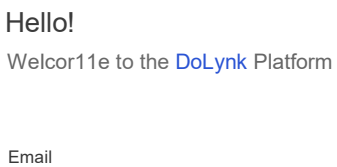
Al primo utilizzo, é necessario creare un account. Gli esempi illustrati in questo manuale d'uso si basano sul sistema operativo iOS.

Passaggio 1: Cercare l'app DoLynk nell'App Store e scaricarla.

Gli utenti Android possono scaricare l'app DoLynk da Google Play.

Passaggio 2: Sul telefono, toccare @ per avviare l'app.

Figura 4-1 Accesso



sign up

Passaggio 3: Creare un account.

1. Nella schermata Accesso (Login), toccare registrazione (sign up).
2. Nella schermata Registrazione (Register), inserire le informazioni nei campi obbligatori.
   Se come Paese/area geografica viene selezionata l'America del Nord, nella schermata Registrazione (Register) comparira il campo Numero di registrazione del rivenditore (Dealer Registration Number). Selezionando un qualsiasi altro Paese o area geografica, comparira il campo Nome dell'azienda (Company Name).
   - E-mail: inserire il proprio indirizzo e-mail.
   - Paese/area geografica: selezionare il Paese o l'area geografica, la provincia o lo Stato e la citta in cui risiede la propria azienda.
   - Indirizzo: inserire l'indirizzo completo della propria azienda.
   - Nome azienda: inserire il nome della propria azienda.
   - Numero di registrazione del rivenditore: inserire il numero di registrazione del rivenditore.

     I clienti che risiedono in America del Nord devono inserire il numero di registrazione del rivenditore.
   - Codice di invito: inserire il codice di invito, che puo essere ottenuto dalla persona da cui si é ricevuto l'invito.
   - Password e Conferma password: inserire la password e confermarla nuovamente.

- **Codice di verifica:** toccare **Invia** (Send) e controllare di avere ricevuto il codice di verifica sulla propria casella di posta elettronica, quindi inserirlo nel campo **Codice di verifica** (Verification Code).

3. Leggere la **Politica sulla privacy** (Privacy Policy) e il **Protocollo del servizio** (Service Protocol), quindi selezionare la casella di spunta **Dichiaro di avere letto e di accettare la Politica sulla privacy e il Protocollo del servizio** (I have read and agree to Privacy Policy and Service Protocol).
4. Toccare **Registra** (Register): l'app tornerà alla schermata **Accesso** (Login).

Passaggio 4: Inserire l'indirizzo e-mail e la password, quindi toccare **Accedi** (Log in).

- Per i nuovi clienti, la richiesta di registrazione dell'account deve essere approvata. L'e-mail di approvazione dell'account viene spedita entro 1-3 giorni. Una volta approvata la richiesta, è possibile accedere all'app con il proprio account.
- La procedura di approvazione dell'account COS Pro non è necessaria per alcuni clienti affiliati, che possono accedere direttamente all'app subito dopo essersi registrati.

4.2 Aggiunta di dispositivi

Gli installatori possono aggiungere dispositivi all'app COS Pro per gestirli e occuparsi della loro manutenzione. Prima di procedere, accertarsi che il dispositivo sia alimentato e connesso alla rete. È possibile aggiungere dispositivi di allarme, comprese le centraline e vari accessori, all'app.

4.2.1 Aggiunta della centralina

La centralina può essere aggiunta in **Modalità sito** (Site mode) o in **Modalità dispositivo** (Device mode). Per aggiungere i dispositivi in **Modalità dispositivo** (Device mode), è necessario selezionare prima un sito. La procedura è simile per entrambe le modalità. L'esempio in questa sezione si basa sulla configurazione in **Modalità dispositivo** (Device mode).

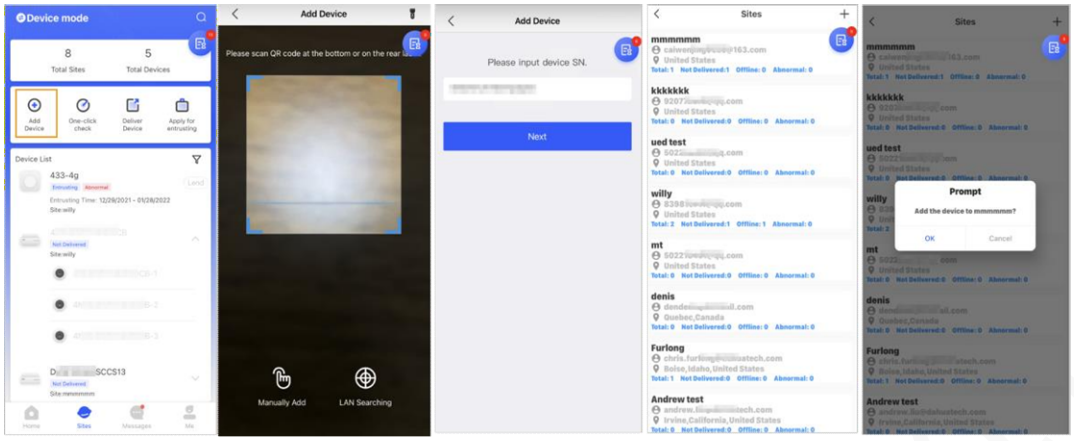
- Prima di aggiungere la centralina, accertarsi che sia alimentata e connessa alla rete.
- Verificare che sul telefono sia attiva la funzione Wi-Fi.

4.2.1.1 Aggiunta tramite n. di serie/codice QR

È possibile aggiungere la centralina a una rete wireless o cablata scansionandone il codice QR o inserendone il numero di serie manualmente.

Passaggio 1: Nella schermata **Home**, toccare per accedere all'interfaccia **Siti** (Sites).

Figura 4-2 Aggiunta di un dispositivo



Passaggio 2: Toccare nell'angolo in alto a sinistra per passare alla **Modalità dispositivo** (Device mode).

Passaggio 3: Toccare per aggiungere un dispositivo.

Passaggio 4: Scansionare il codice QR del dispositivo o toccare **Aggiungi manualmente** (Manually Add) per inserire il numero di serie del dispositivo manualmente.

Passaggio 5: Selezionare un sito, quindi toccare **OK**.

Passaggio 6: Nella schermata **Aggiungi dispositivo** (Add Device), selezionare un tipo di dispositivo.

Passaggio 7: Effettuare la connessione a una rete wireless o cablata.

- **Wireless**

1) Nell'angolo in alto a destra, toccare l'opzione **Wireless**, che passerà da **Wireless** a **Cablata** (Wired).
2) Inserire la password della rete Wi-Fi a cui è connesso il telefono e toccare **Connetti** (Connect).
3) Seguire le istruzioni sullo schermo, quindi toccare **Avanti** (Next).
4) Attendere il completamento dell'abbinamento.

Se la procedura non riesce, ripetere i passaggi illustrati sopra.

- **Cablata**

1) Nell'angolo in alto a destra, toccare l'opzione **Cablata** (Wired), che passerà da **Cablata** (Wired) a **Wireless**.
2) Connettere il dispositivo a una fonte di alimentazione e alla rete, quindi toccare **Avanti** (Next).

Se la procedura non riesce, ripetere i passaggi illustrati sopra.

Passaggio 8: Se la centralina che si sta aggiungendo non è inizializzata, inserire la password e confermarla, quindi toccare **Inizializza il dispositivo** (Initialize the device) per procedere.

Passaggio 9: Toccare **Fine** (Completed) e il dispositivo comparirà nell'elenco.

4.2.1.2 Aggiunta tramite configurazione AP

È possibile aggiungere la centralina usando la configurazione AP.

Passaggio 1: Nella schermata **Home**, toccare per accedere all'interfaccia **Siti** (Sites).

Passaggio 2: Toccare nell'angolo in alto a sinistra per passare alla **Modalità dispositivo** (Device mode).

Passaggio 3: Toccare per aggiungere un dispositivo.

Figura 4-3 Aggiunta di un dispositivo

Passaggio 4: Scansionare il codice QR del dispositivo o toccare **Aggiungi manualmente** (Manually Add) per inserire il numero di serie del dispositivo manualmente.

Passaggio 5: Nella schermata **Aggiungi dispositivo** (Add Device), selezionare **Postazione di allarme** (Alarm Station).

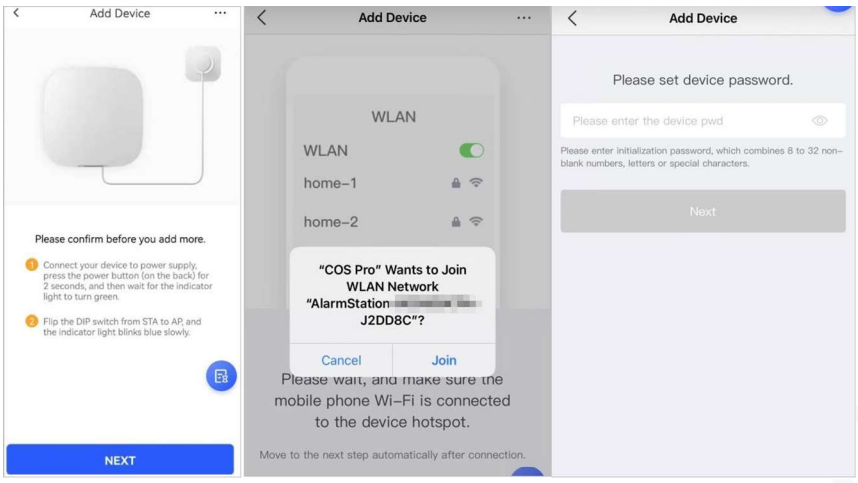
Figura 4-4 Selezione di una postazione di allarme

Passaggio 6: Seguire le istruzioni sullo schermo e spostare l'interruttore DIP dalla posizione STA alla posizione AP.

Passaggio 7: Toccare **Collega** (Join) per effettuare la connessione all'hotspot del dispositivo.

Passaggio 8: Impostare la password del dispositivo per inizializzarlo, quindi toccare **Avanti** (Next).

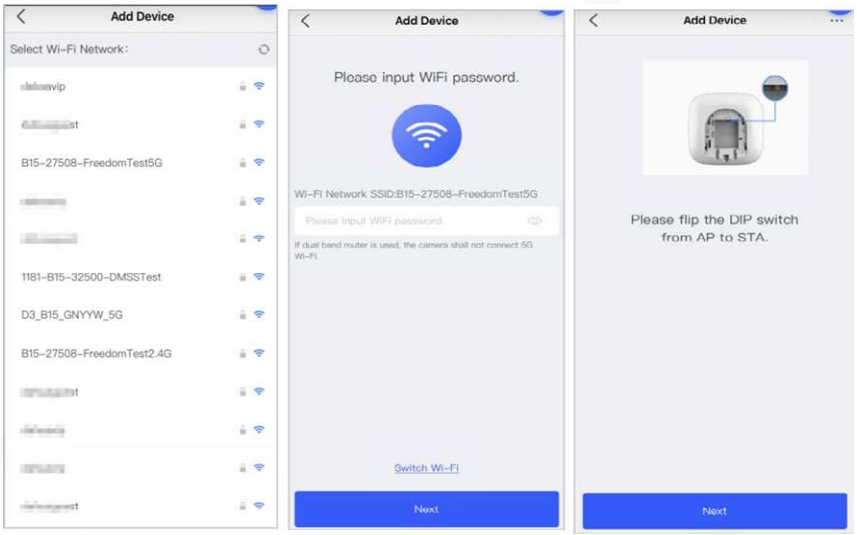
Figura 4-5 Aggiunta tramite configurazione AP



Passaggio 9: Effettuare la connessione alla rete.

1) Selezionare la rete Wi-Fi.
   Accertarsi che il telefono e il dispositivo siano connessi alla stessa rete.
2) Inserire la password Wi-Fi e toccare **Avanti** (Next).
3) Spostare l'interruttore DIP dalla posizione AP a quella STA, quindi toccare **Avanti** (Next).
4) Attendere che il dispositivo completi la configurazione di rete.

Figura 4-6 Connessione alla rete



Fase 10: Toccare **Fine** (Completed).

4.2.1.3 Aggiunta tramite ricerca LAN

È possibile cercare i dispositivi e aggiungerli. Accertarsi che il telefono e i dispositivi siano connessi alla stessa rete.

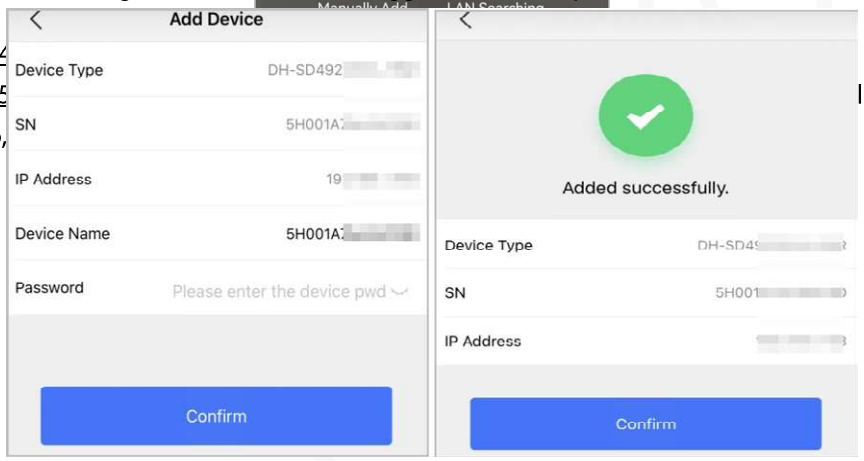
Passaggio 1: Nella schermata **Home**, toccare per accedere all'interfaccia **Siti** (Sites).

Passaggio 2: Toccare nell'angolo in alto a sinistra per passare alla **Modalità dispositivo** (Device mode).

Passaggio 3: Toccare per aggiungere un dispositivo.

Figura 4-7 Aggiunta di un dispositivo

Figura 4-8 Conferma dell'aggiunta di un dispositivo



Passaggio 4

Passaggio 5

dispositivo,

4.2.2 Aggiunta di Accessori

È possibile aggiungere vari accessori alla centralina. Per l'esempio illustrato in questa sezione, viene utilizzato un rilevatore per porte. Per ulteriori dettagli sull'aggiunta di accessori, consultare i relativi manuali d'uso.

È possibile aggiungere fino a 6 sirene, 64 radiocomandi, 4 ripetitori e 8 tastierini a una centralina.

Passaggio 1: Sulla schermata della centralina, toccare nell'angolo in alto a destra, quindi scansionare il codice QR sul fondo del rilevatore per porte.

Passaggio 2: Toccare **Avanti** (Next).

Passaggio 3: Seguire le istruzioni sullo schermo e attivare il rilevatore per porte, quindi toccare **Avanti** (Next) per aggiungerlo alla centralina.

Passaggio 4: Attendere il completamento dell'abbinamento.

Passaggio 5: Personalizzare il nome del rilevatore per porte e selezionare la zona, quindi toccare **Fine** (Completed).

- Per eliminare un accessorio, accedere alla schermata della centralina, selezionare l'accessorio dall'elenco e scorrere verso sinistra.
- In una centralina è possibile creare un massimo di 32 zone.

4.3 Gestione degli utenti

4.3.1 Aggiunta di amministratori DMSS

Gli installatori possono aggiungere amministratori DMSS condividendo con loro i dispositivi affidati o accettando le loro richieste di affidamento.

Gli amministratori DMSS non possiedono le autorizzazioni per configurare il dispositivo quando affidano la centralina all'installatore o quando gli installatori prestano loro la centralina.

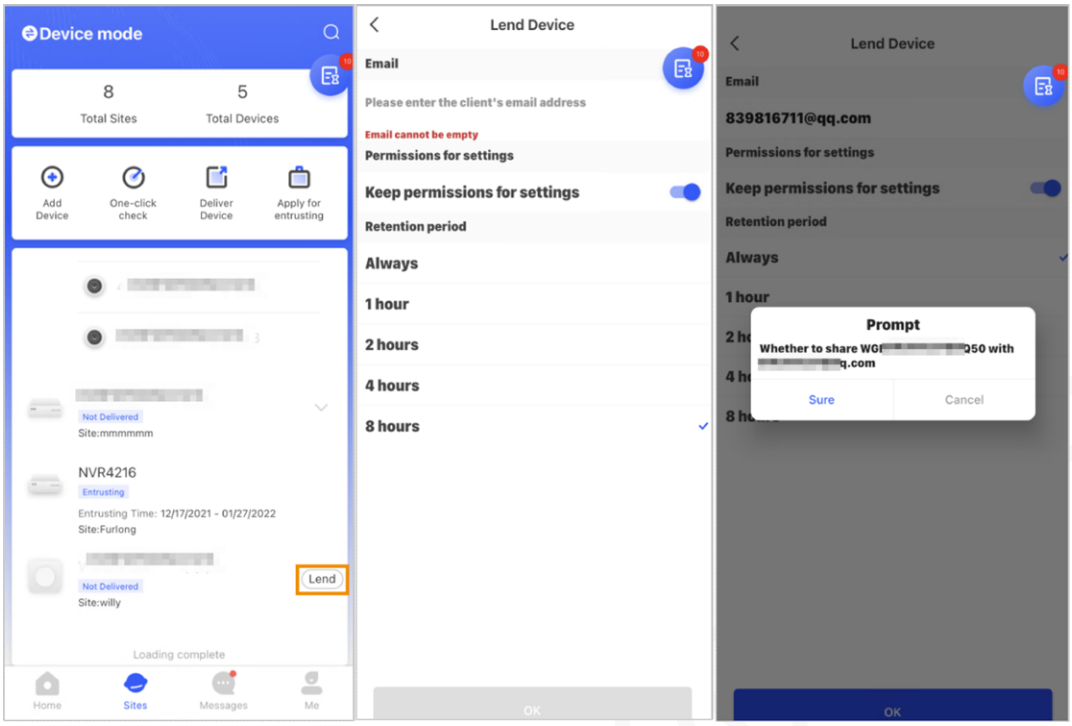
4.3.1.1 Prestito dei dispositivi agli amministratori DMSS

Gli installatori possono prestare la centralina agli amministratori DMSS. Dopo averlo fatto, devono richiedere all'amministratore DMSS le autorizzazioni per operazioni come la configurazione del dispositivo, l'inserimento e il disinserimento degli allarmi e la gestione degli utenti.

Accertarsi che la centralina non sia stata aggiunta da altri account.

Passaggio 1: Nella schermata **Home**, toccare per accedere all'interfaccia **Siti** (Sites).

Figura 4-9 Prestito della centralina a un amministratore DMSS



Passaggio 2: Toccare nell'angolo in alto a sinistra per passare alla **Modalità dispositivo** (Device mode).

Passaggio 3: Selezionare una centralina dall'elenco dei dispositivi, quindi toccare la voce **Presta** (Lend) sulla destra della centralina.

Passaggio 4: Inserire l'indirizzo e-mail dell'amministratore DMSS.

Passaggio 5: Attivare **Riserva autorizzazioni di configurazione** (Reserve Configuration Permissions) e selezionare un periodo di tempo.

Passaggio 6: Toccare **Conferma** (Confirm).

Passaggio 7: Nella schermata , toccare **Messaggi personali** (Personal Message) per visualizzare i messaggi e controllare se l'amministratore DMSS ha accettato la richiesta di condivisione.

Un messaggio con la richiesta di condivisione viene inviato all'account dell'amministratore DMSS e quest'ultimo può leggerlo nell'app DMSS.

4.3.1.2 Accettazione delle richieste di affidamento

L'installatore può accettare le richieste di affidamento inviate dall'amministratore DMSS.

Passaggio 1: Nella schermata **Home**, selezionare **Attività in sospeso > Valutazione affidamento** (Pending Task > Entrusting Review).

Passaggio 2: Nella schermata **Attività in sospeso** (Pending Task), selezionare un'attività per visualizzarne i dettagli e gestire le richieste di affidamento.

Figura 4-10 Gestione delle attivita di affidamento

- Per approvare una richiesta:

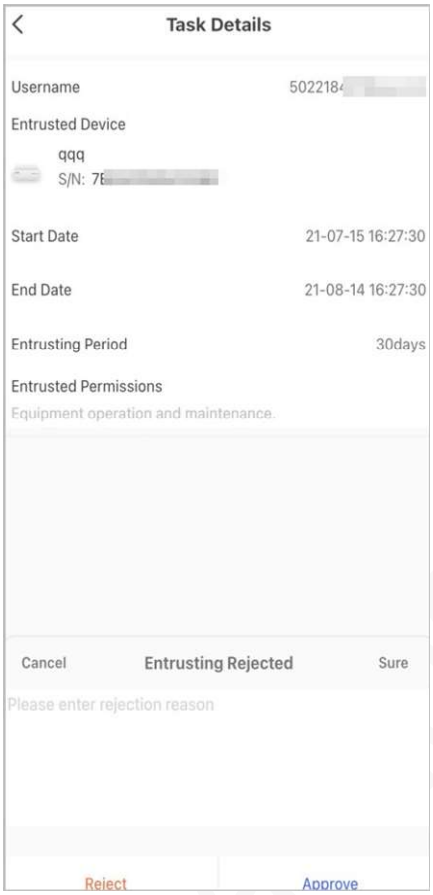
1) Toccare Approva (Approve) per accedere alla schermata Dispositivi non allocati (Unallocated Devices).
2) Selezionare i dispositivi da allocare o toccare Seleziona tutti (Select all), quindi toccare Aggiungi ai siti (Add to Sites).

Figura 4-11 Aggiunta di dispositivi ai siti

3) Nella schermata Siti (Sites), selezionare un sito o aggiungerne uno nuovo.
4) Toccare OK per confermare l'assegnazione del dispositivo al sito selezionato.

- Per rifiutare una richiesta: Toccare Rifiuta (Reject), inserire i motivi del rifiuto, quindi toccare Procedi (Sure).

Figura 4-12 Rifiuto di una richiesta



4.3.2 Eliminazione degli utenti

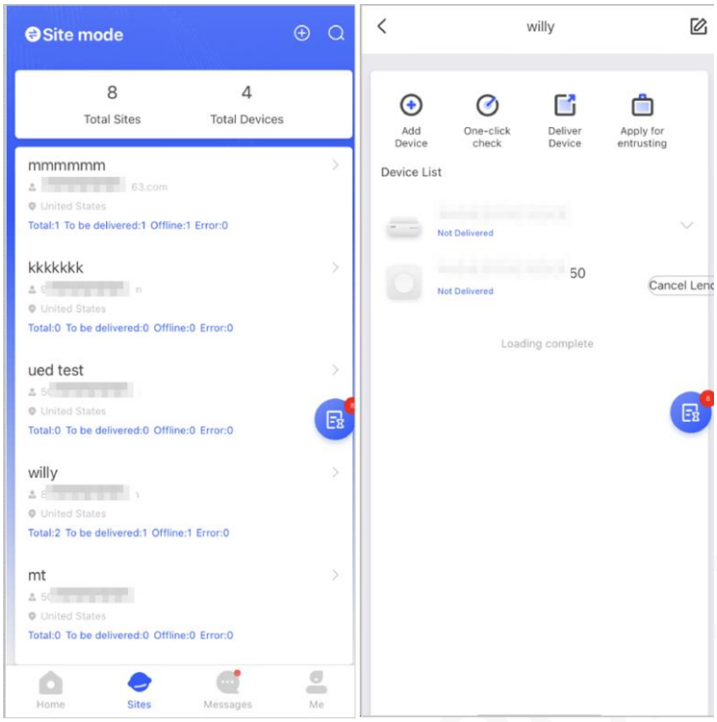
Gli installatori possono eliminare un utente annullando il prestito dei dispositivi agli amministratori DMSS o eliminando i dispositivi.

4.3.2.1 Annullamento del prestito dei dispositivi

Gli installatori possono eliminare gli amministratori DMSS annullando il prestito della centralina.

Passaggio 1: Nella schermata **Home**, toccare per accedere all'interfaccia **Siti** (Sites).

Figura 4-13 Prestito della centralina a un amministratore DMSS



Passaggio 2: Toccare nell'angolo in alto a sinistra per passare alla **Modalità sito** (Site mode).

Passaggio 3: Selezionare il sito contenente il dispositivo prestato all'amministratore DMSS dal relativo elenco, quindi selezionare la centralina e toccare **Annulla prestito** (Cancel Lend).

Un messaggio viene inviato all'account dell'amministratore DMSS e quest'ultimo può leggerlo nell'app DMSS.

4.3.2.2 Eliminazione dei dispositivi

Gli installatori possono eliminare gli amministratori DMSS eliminando i dispositivi.

-
-

dispositivi con gli utenti DMSS generici.

Passaggio 1: Nella schermata **Home**, toccare per accedere all'interfaccia **Siti** (Sites).

Passaggio 2: Toccare nell'angolo in alto a sinistra per passare alla **Modalità dispositivo** (Device mode).

Passaggio 3: Selezionare il dispositivo desiderato dal relativo elenco.

Passaggio 4: Nella schermata della centralina, toccare prima , quindi **Elimina** (Delete) per eliminare il dispositivo.

4.4 Richiesta delle autorizzazioni agli amministratori DMSS

Gli installatori possono aggiungere la centralina direttamente all'app DoLynk per offrire servizi di gestione e manutenzione dei dispositivi agli amministratori DMSS. Tutte ie autorizzazioni, comprese quelle per la configurazione dei dispositivi e la gestione degli utenti, sono temporanee e devono essere rinnovate alla scadenza.

Passaggio 1: Nella schermata Home, toccare per accedere all'interfaccia Siti (Sites).

Passaggio 2: Toccare ,_, nell'angolo in alto a sinistra per passare alia Modalitâ dispositivo (Device mode).

Passaggio 3: Selezionare il dispositivo desiderato dal relativo elenco.

Passaggio 4: Nella schermata Centralina (Hub), selezionare > Impostazioni centralina (Hub Setting) e toccare il parametro che si desidera configurare: comparira una finestra di dialogo per la richiesta delle autorizzazioni all'amministratore DMSS.

Passaggio 5: Toccare Procedi (Sure).

Passaggio 6: Selezionare ie ore di autorizzazione e toccare Conferma (Confirm).

Passaggio 7: Nella schermata @, toccare Messaggi personali (Personal Message) per visualizzare i messaggi e controllare se l'amministratore DMSS ha accettato di concedere le autorizzazioni.

Un messaggio con la richiesta viene inviato all'account dell'amministratore DMSS e quest'ultimo puo leggerlo nell'app DMSS.

4.5 Consegna dei dispositivi agli amministratori DMSS

Una volta eseguito il debug dei dispositivi, é possibile consegnarli agli amministratori DMSS. I dispositivi affidati e quelli offline non possono essere consegnati.

I requisiti delle certificazioni EN 50131 non vengono rispettati se l'installatore consegna la centralina a un amministratore DMSS.

Passaggio 1: Nella schermata Home, toccare '*' per accedere all'interfaccia Siti (Sites).

Passaggio 2: Toccare , , nell'angolo in alto a sinistra per passare alla Modalitâ sito (Site mode).

Passaggio 3: Dal relativo elenco, selezionare il sito con i dispositivi che devono essere consegnati agli amministratori DMSS.

Passaggio 4: Toccare Eu per accedere alia schermata Consegna dispositivi (Deliver devices).

Non é possibile consegnare pid di 5 dispositivi per volta.

Passaggio 5: Inserire l'indirizzo e-mail dell'amministratore DMSS, quindi toccare Procedi (Sure) per visualizzare i risultati della consegna. Se la consegna di alcuni dispositivi a un amministratore DMSS non riesce, accedere alla schermata Consegna non riuscita (Failed) per ripetere la procedura.

Se i clienti utilizzano un account Imou, i loro dispositivi non verranno consegnati. Inoltre, sulla schermata Home comparirà un messaggio che segnala che l'account non dispone delle autorizzazioni necessarie. Chiedere al cliente di aggiornare l'account sull'app DMSS. Per ulteriori dettagli, consultare il *Manuale d'uSo dell'app DMSS.*

4.9 Gestione del funzionamento e dello stato dei dispositivi

Gli installatori possono fornire servizi di gestione e manutenzione dei dispositivi, come la verifica dello stato, la configurazione remota e la correzione degli errori.

4.b.1 Verifica dello stato dei dispositivi

E possibile verificare se i dispositivi sono offline o online in tempo reale e controllarne lo stato di funzionamento singolarmente o in serie. L'esempio in questa sezione si basa sulla verifica in serie. La procedura puo essere effettuata in Modalitâ sito (Site mode) e in Modalitâ dispositivo (Device mode). La procedura é simile per entrambe ie modalita. L'esempio in questa sezione si basa sulla configurazione in Modalitâ dispositivo (Device mode).

Passaggio 1: Nella schermata Home, toccare per accedere all'interfaccia Siti (Sites).

Passaggio 2: Toccare , , nell'angolo in alto a sinistra per passare alla Modalitâ dispositivo (Device mode).

Passaggio 3: Toccare .

Passaggio 4: Selezionare i dispositivi che si desidera verificare, quindi toccare X dispositivi selezionati. Avvia la verifica dello stato (X devices selected. Start Health Check).

Per selezionare tutti i dispositivi, toccare Seleziona tutti (Select all).

Passaggio 5: Visualizzare i risultati della verifica, quindi toccare OK.

I dispositivi offline non possono essere verificati.

4.b.2 Configurazioni di base del dispositivo

Una volta aggiunti i dispositivi, compresi la centralina di allarme e gli accessori, é possibile visualizzarne e modificarne le informazioni generali.

Passaggio 1: Nella schermata Home, toccare per accedere all'interfaccia Siti (Sites).

Passaggio 2: Toccare , _, nell'angolo in alto a sinistra per passare alia Modalitâ dispositivo (Device mode).

Passaggio 3: Selezionare il dispositivo desiderato dal relativo elenco.

Passaggio 4: Nella schermata della centralina, toccare per visualizzare e modificare ie informazioni generali sul dispositivo.

Tabella 4-1 Descrizione dei parametri

Parametro	Descrizione
Configurazione del dispositivo	• Visualizzare il nome, il tipo e il numero di serie del dispositivo. • Modificare il nome del dispositivo, quindi toccare Salva (Save) per salvare la configurazione.
Stato della centralina	Per ulteriori dettagli, consultare la sezione "4.6.2.2 Configurazione della centralina".
Impostazioni della centralina	Per ulteriori dettagli, consultare la sezione "4.6.2.1 Visualizzazione dello stato".
Fuso orario	Toccare Fuso orario (Time Zone) per selezionare il proprio fuso orario e attivare l'ora legale (se necessario). • Fuso **orario:** selezionare il fuso orario del luogo di utilizzo della centralina. • Ora legate: selezionare una data o una settimana, quindi selezionare l'ora di inizio e l'ora di fine.
Configurazione di rete	Toccare Configurazione di rete (Network Configuration) per visualizzare ie informazioni sulla rete in uso.
Condivisione del dispositivo	Toccare Condivisione dispositivo (Device Sharing) per condividere Io stato della centralina con altri utenti. Per ulteriori dettagli, consultare la sezione "4.3.1.1 Prestito dei dispositivi agli amministratori DMSS".
Aggiornamento via cloud	Aggiornamento online. Non é possibile effettuare aggiornamenti quando la centralina é in stato "inserito" o ha ie batterie scariche.
Log	I log dei dispositivi e dell'app. • Log dei dispositivi: selezionare Log > Log dispositivo (Log > Device log) per visualizzare i log di allarme dei dispositivi. E anche possibile toccare nella schermata Log dispositivo (Device log) per inviare i log di allarme all'e-mail collegata. • Log dell'app: selezionare Log > Log app (Log > App log) per visualizzare i log di allarme dell'app DoLynk. E anche possibile toccare nella schermata Log app (App log) per inviare i log di allarme all'e-mail collegata.

4.6.2.1 Visualizzazione dello stato

Nella schermata Centralina (Hub), selezionare > Stato centralina (Hub Status) per visualizzare Io stato della centralina.

Tabella 4-2 Stato

Parametro	Descrizione
Potenza del segnale GSM	La potenza del segnale della rete mobile della scheda SIM attiva. • ‹ : molto basso. • ‹i :basso. • «I :medio. • ‹ill: alto. • ‹v I: No.
Potenza del segnale Wi-Fi	Stato della connessione Wi-Fi a Internet della centralina. Per una maggiore affidabilita, consigliamo di installare la centralina in luoghi dove la potenza del segnale é di almeno due barre. • : molto basso. • - : basso. • :medio. • :alto. • : No.
Livello batteria	Mostra la carica rimanente della batteria. • - : completamente carica. • • : sufficiente. • :medio. • :insufficiente.
Antimanomissione	Modalita antimanomissione, che rileva quando il corpo dell'accessorio viene staccato.
Stato dell'alimentazione principale	Mostra lo stato dell'alimentazione principale.
Stato della connessione GSM	Lo stato della connessione della centralina via SIM, Wi-Fi e Ethernet. • :Connesso. • :Disconnesso.
Stato della connessione Wi-Fi	
Stato della connessione cablata	
Stato della scheda SIM	Lo stato della connessione della scheda SIM. • GB:La scheda SIM 1 é attiva. • M:La scheda SIM 2 é attiva. • :Non sono presenti schede SIM.
Versione del software	La versione del programma della centralina.

4.b.2.2 Configurazione della centralina

Nella schermata Centralina (Hub), selezionare > Impostazioni centralina (Hub Setting) per configurare i parametri della centralina.

Tabella 4-3 Descrizione dei parametri della centralina

Parametro	**Descrizione**
Inserimento/disinserimento globale	Inserimento o disinserimento rapido dei rilevatori in tutte ie zone.
Inserimento/disinserimento programmato	Inserimento o disinserimento programmato delle zone. • Zona: consente di selezionare la zona gestita dalla centralina. • **Modalitâ di inserimento:** selezionare una modalita di inserimento toccando **Inserimento in** presenza (Home), Inserimento in assenza (Away) o Disinserito (Disarm). • Ora: consente di selezionare i periodi di funzionamento della centralina. • **Ripeti:** consente di copiare la programmazione degli inserimenti e dei disinserimenti. • **Inserimento forzato:** consente l'inserimento del sistema di allarme anche quando si verificano degli errori in alcune zone.
Impostazioni suoneria	La suoneria che segnala l'attivazione o la disattivazione della modalita di inserimento.
Indicatore LED	L'opzione Indicatore LED (LED Indicator) é attiva per impostazione predefinita. Per ulteriori dettagli sullo stato dell'indicatore, consultare la sezione "2.1 Aspetto". • Se l'opzione Indicatore LED (LED Indicator) é disattiva, l'indicatore LED non si attivera a prescindere dal corretto funzionamento della centralina. • La funzione é disponibile solo con ie versioni dell'app DMSS successive alla 1.96 e con le versioni della centralina superiori alla V1.001.0000000.4.R.211014.
Modalita test	Toccare Avvia (Start) per testare lo stato degli accessori connessi alla centralina nelle varie zone, quindi toccare **Interrompi** (Stop) per completare la verifica.
Modalita a sensibilita ridotta	Attivare **Modalitâ a sensibilitâ ridotta** (Reduced Sensitivity Mode) per ridurre la potenza di trasmissione della centralina. La funzione é disponibile solo con ie versioni dell'app DMSS successive alla 1.97 e con le versioni della centralina superiori alla V1.001.0000000.6.R.211215.
Connessione al servizio cloud	Assegnare all'intervallo del ping tra server e centralina un valore compreso fra 150 e 900 secondi (l'opzione predefinita é 150 secondi). Se D-cloud rileva che la centralina é rimasta offline per pid di 150 secondi, segnala lo stato della centralina all'utente tramite l'app. La funzione é disponibile solo con ie versioni dell'app DMSS successive alia 1.96 e con ie versioni della centralina superiori alia V1.001.0000000.6.R.211215.

Parametro	Descrizione
	Configurazione dell'intervallo del ping tra centralina e rilevatore. L'impostazione determina con quale frequenza la centralina comunica con gli accessori e quanto rapidamente viene rilevata la perdita di connessione. • Intervallo del ping di rilevamento: la frequenza di comunicazione con gli accessori connessi alla centralina é configurabile in un intervallo compreso fra 12 e 300 secondi (il valore predefinito é 60 secondi). Pid breve é l'intervallo di ping, minore sara la durata della batteria.
Heartbeat	• Numero di pacchetti non consegnati che determinano un errore di connessione: il numero di pacchetti non consegnati si puo configurare in un intervallo compreso fra 3 e 60 (il valore predefinito é 15 pacchetti). □ Minore é il numero di pacchetti selezionato, pid frequentemente viene rilevato e segnalato lo stato offline degli accessori. □ Se la centralina perde spesso la connessione con gli accessori e non riesce a rilevare il valore del loro heartbeat, li segnalera come offline al sistema.
Altoparlante manomissione	Attiva una sirena di allarme se viene aperto il coperchio posteriore degli accessori o della centralina. Quando la funzione viene attivata, prima di inserire gli allarmi la centralina verifica lo stato di tutti i rilevatori, come quelli per il livello di carica della batteria, gli incidenti di manomissione e la connettivita. Se la centralina rileva degli errori, vengono mostrati i relativi avvisi.
Verifica dell'integrita del sistema	• Sul radiocomando, l'indicatore lampeggia di verde e poi diventa FOSSO. • Sull'app, viene visualizzato un messaggio di allarme. • Sul tastierino, viene prodotto un segnale acustico della durata di 1 secondo e l'indicatore di inserimento e disinserimento lampeggia di verde per 2 secondi per poi tornare allo stato normale.
CMS	Inserire l'indirizzo IP, il numero di porta e l'ID del dispositivo per registrare la centralina su D-cloud. La funzione é disponibile solo con le versioni dell'app DMSS successive alia 1.96 e con ie versioni della centralina superiori alia V1.001.0000000.6.R.211215.

Parametro	Descrizione
Postazione di monitoraggio	Attivare l'opzione Postazione di monitoraggio (Monitoring Station) e impostare i parametri del protocollo SIA per la centrale di ricezione degli allarmi (ARC). • **Indirizzo IP preferito:** inserire l'indirizzo IP e il numero di porta dell'ARC. • **Indirizzo IP alternativo:** inserire l'indirizzo IP alternativo e il numero di porta dell'ARC. □ I messaggi verranno inviati all'indirizzo IP alternativo solo in caso di errore di ricezione dell'indirizzo IP preferito. □ Se viene attivata l'opzione Intervallo heartbeat (Heartbeat interval), é il sistema a stabilire se inviare il messaggio all'indirizzo IP preferito o a quello alternativo. • Protocollo IP: l'opzione predefinita é TCP. • Intervallo heartbeat: impostare l'intervallo della funzione heartbeat su un valore compreso fra 0 secondi e 24 ore (l'opzione predefinita é 60 secondi). Il valore 0 secondi disattiva la funzione Intervallo heartbeat (Heartbeat interval). • Account centrale: inserire il numero dell'account creato dall'ARC, che deve essere utilizzato per identificare la centralina quando invia le informazioni all'ARC. • Crittografia: quando viene configurata l'ARC, la centralina utilizza un formato crittografato per garantire la sicurezza delle informazioni. AES128 é l'impostazione predefinita. • Evento di caricamento: Toccare accanto a un evento per caricarlo. □ Allarme: messaggio di allarme. □ Errore: interruzione dell'alimentazione, tensione della batteria insufficiente, manomissione e stato offline. □ Evento: impedisce l'uso delle periferiche, l'aggiunta o eliminazione delle periferiche e l'aggiunta o l'eliminazione degli utenti. □ Inserimento/Disinserimento: notifiche di inserimento e disinserimento del sistema di allarme.

4.b.3 Correzione degli errori

Se la verifica dei dispositivi evidenzia delle anomalie, queste possono essere corrette. E possibile trovare gli errori in due modi: tramite l'inclusione di rapporti automatici e attraverso la verifica manuale.

Passaggio 1: Nella schermata Home, selezionare Attivita in sospeso > Correzione degli errori (Pending Task > Error Fixing).

Passaggio 2: Nell'elenco degli errori, toccare prima un'attivita errore, quindi Avvia elaborazione (Start processing).

Passaggio 3: Correggere l'errore seguendo i suggerimenti forniti.

Passaggio 4: Toccare Errore corretto (Error Fixed) se l'errore é stato corretto, quindi attendere la conferma del cliente.

Quando gli errori vengono corretti, i clienti ricevono una notifica. Se i clienti confermano che l'errore é stato effettivamente corretto, sara chiesto loro di valutare il servizio.

4.6.4 Visualizzazione delle valutazioni

Dopo la configurazione remota dei dispositivi e la correzione degli errori, i clienti valuteranno la qualita del servizio offerto dall'operatore. Sull'account dell'amministratore é possibile visualizzare i dettagli relativi agli errori, come il tipo di errore, l'orario in cui si é verificato, l'operazione suggerita, il nome dell'operatore e le sue valutazioni.

Passaggio 1: Nella schermata @, toccare Notifiche di errore (Error Notification).

Passaggio 2: Toccare un messaggio nell'elenco per visualizzare informazioni come il nome utente del cliente, il nome utente dell'operatore, i dettagli relativi al dispositivo, i dettagli relativi all'errore e alia sua correzione nonché la valutazione.

5 Operazioni effettuabili dagli utenti finali sull'app DMSS

L'app DMSS offre servizi di sicurezza professionali agli utenti finali. Gli amministratori DMSS possono condividere la centralina con un massimo di 6 utenti DMSS generici e affidarla a un'azienda. Gli accessori della centralina possono essere contemporaneamente condivisi e affidati. Per condividere e affidare la centralina da soli, è necessario installare l'ultima versione dell'app DMSS.

Le figure servono unicamente a scopo illustrativo e potrebbero differire dall'interfaccia reale.

5.1 Accesso all'app DMSS

Il sistema di sicurezza si configura e si controlla tramite l'app DMSS. È possibile accedere all'app DMSS su iOS e Android. L'esempio illustrato in questa sezione si basa sul sistema operativo iOS.

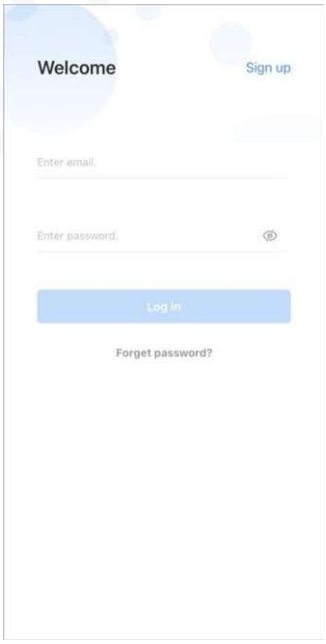
Verificare di avere installato la versione più recente dell'app.

Passaggio 1: Cercare l'app DMSS nell'App Store e scaricarla.

Gli utenti Android possono scaricare l'app DMSS da Google Play.

Passaggio 2: Sul telefono, toccare ⊕ per avviare l'app.

Figura 5-1 Accesso



Passaggio 3: Creare un account.

1) Nella schermata **Accesso** (Login), toccare **Registrazione** (Sign up).

2) Inserire l'indirizzo e-mail e la password.

Toccare per mostrare la password (l'icona diventerà).

3) Leggere il **Contratto con l'utente** (User Agreement) e la **Politica sulla privacy** (Privacy Policy), quindi selezionare la casella di spunta **Dichiaro di avere letto i documenti e di accettarli** (I have read and agree to).
4) Toccare **Ottieni codice di verifica** (Get verification code) e controllare di avere ricevuto il codice di verifica sulla propria casella di posta elettronica, quindi inserirlo.

Il codice di verifica deve essere utilizzato entro 60 secondi dalla ricezione. Passato questo tempo, non sarà più valido.

5) Toccare **OK**.

Passaggio 4: Nella schermata **Accesso** (Login), inserire il proprio indirizzo e-mail e la password, quindi toccare **Accedi** (Log in).

È possibile modificare la password dal menu **Profilo > Gestione account > Modifica password** (Me > Account Management > Modify Password).

5.2 Aggiunta di dispositivi

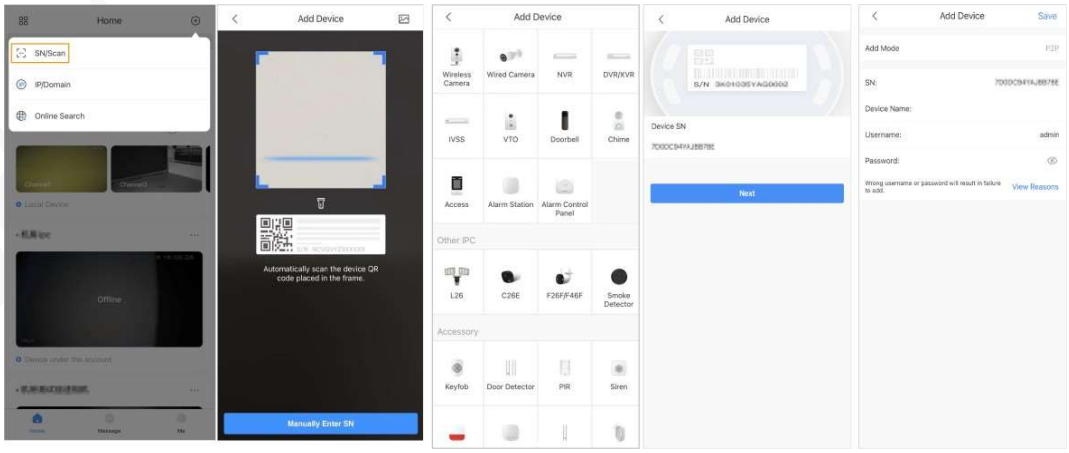
Gli utenti finali possono aggiungere dispositivi di allarme all'app DMSS.

5.2.1 Aggiunta della centralina

È possibile aggiungere la centralina aggiungendo manualmente il numero di serie del dispositivo o scansionandone il codice QR.

Passaggio 1: Nella schermata **Home**, toccare , quindi selezionare **Numero di serie/scansione** (SN/Scan).

Figura 5-2 Aggiunta tramite numero di serie/codice QR



Passaggio 2: Aggiunta di un dispositivo.

- Per aggiungere un dispositivo, scansionarne direttamente il codice QR o toccare e importare l'immagine del codice QR.
- Toccare **Inserisci il numero di serie manualmente** (Manually Enter SN), quindi inserire il numero di serie di un dispositivo per aggiungerlo manualmente.

Passaggio 3: Selezionare il tipo di dispositivo, quindi toccare **Avanti** (Next).

Toccare **Avanti** (Next) se il sistema identifica automaticamente il tipo di dispositivo.

Passaggio 4: Nella schermata **Aggiungi dispositivo** (Add Device), scegliere un nome per il dispositivo, inserire il nome utente e la password del dispositivo e toccare **Salva** (Save).

5.2.2 Aggiunta di accessori

Gli utenti finali possono aggiungere vari accessori alla centralina. La procedura per aggiungere accessori sull'app DMSS è la stessa utilizzata nell'app COS Pro. Per ulteriori dettagli, consultare la sezione "4.2.2 Aggiunta di accessori".

5.3 Impostazioni generali della centralina

5.3.1 Configurazione della centralina

Nella schermata **Dettagli dispositivo** (Device Details), toccare per visualizzare e modificare le informazioni generali sulla centralina. Le informazioni generali sul dispositivo mostrate sull'app DMSS sono le stesse visualizzate nell'app COS Pro. Per ulteriori dettagli, consultare la sezione "4.6.2 Configurazioni di base del dispositivo".

5.3.2 Configurazione di rete

Nella sezione **Config. Generale** (Geneal Config) sulla schermata **Dettagli dispositivo** (Device Details), toccare **Configurazione di rete** (Network Configuration) e selezionare un tipo di connessione di rete per la centralina, scegliendo tra rete cablata, rete wireless o rete cellulare.

5.3.2.1 Configurazione della rete cablata

Passaggio 1: Selezionare **Impostazioni di rete > Config. rete cablata** (Network Settings > Wired Network Config.).

Passaggio 2: Configurare i parametri di connessione della rete cablata.

Tabella 5-1 Descrizione dei parametri della rete cablata

Parametro	Descrizione
DHCP	quando è presente un server DHCP sulla rete, abilitando l'opzione **DHCP**, la centralina ottiene automaticamente un indirizzo IP dinamico.

Parametro	Descrizione
Indirizzo IP	Configurazione manuale dell'indirizzo IP: impostare manualmente l'indirizzo IP, la subnet mask, il gateway predefinito e il DNS della centralina.
Subnet mask	
Centralina di allarme	
DNS	
DNS 2	

5.3.2.2 Configurazionedella rete Wi-Fi

Passaggio 1: Selezionare Impostazioni direte > Configurazione rete Wi-Fi (Network Settings > Wi-Fi Network Configuration).
Passaggio 2: Selezionare una rete Wi-Fi disponibile nell'area e inserire la password per connettersi.

5.3.2.3 Configurazionedella rete cellulare

Passaggio 1: Selezionare Impostazioni direte > Cellulare (Network Settings > Cellular).
Passaqqio 2: Configurare i parametri della rete cellulare.

Tabella 5-2 Descrizione dei parametri della rete cellulare

Parametro	Descrizione
Cellulare	Toccare accanto all'opzione Cellulare (Cellular) per abilitare la rete cellulare.
Priorita	Toccare accanto all'opzione Priorità (Priority) per impostare la rete cellulare come prioritaria.
SIM 1	• Sono supportate due schede SIM, di cui una in modalita standby. • Le schede SIM consentono alia centralina di usare il piano dati cellulare e inviare notifiche push di allarme.
SIM 2	
APN	Il nome del punto di accesso (APN) é il nome delle impostazioni lette dal dispositivo per configurare una connessione per il gateway tra la rete cellulare dell'operatore e la rete Internet pubblica.
Modalita di autenticazione	La modalita di autenticazione della rete cellulare.
Nome utente	Nome utente e password della rete cellulare.
Password	
Numero di accesso	Il numero che deve chiamare la centralina.
Utilizzo dati connessione mobile	Mostra l'utilizzo dei dati della connessione mobile.
Ripristina statistiche	Azzera il contegg io dei dati della connessione mobile utilizzati.

5.4 Gestione degli utenti

5.4.1 Aggiunta degli utenti

Gli amministratori DMSS possono aggiungere sia gli installatori che gli utenti DMSS generici.

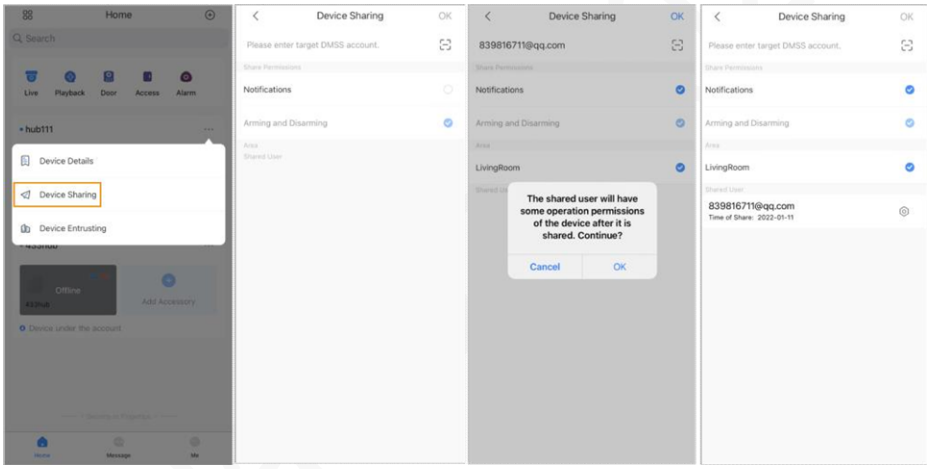
5.4.1.1 Aggiunta di utenti DMSS generici

È possibile condividere dispositivi con un massimo di 6 utenti DMSS generici.

Per condividere il dispositivo, accedere a ••• **> Dettagli dispositivo** (Device Details) > < o a ••• **> Dettagli dispositivo > Condivisione dispositivo** (Device Details > Device Sharing). I due metodi sono equivalenti. L'esempio in questa sezione si basa sulla condivisione dei dispositivi dal menu ••• > **Condivisione dispositivo** (Device Sharing).

Passaggio 1: Nella **schermata iniziale** (Home), toccare ••• accanto a un dispositivo, quindi toccare **Condivisione dispositivo** (Device Sharing).

Figura 5-3 Condivisione dei dispositivi



Passaggio 2: Nella schermata **Condivisione dispositivo** (Device Sharing), condividere il dispositivo con gli utenti inserendo il loro account DMSS o scansionando il loro codice QR.

Passaggio 3: Selezionare le autorizzazioni degli utenti in base alle proprie necessità.

Passaggio 4: Toccare **OK**.

L'account con cui si condivide il dispositivo comparirà nella sezione **Utenti in condivisione** (Shared User) della schermata **Condivisione dispositivo** (Device Sharing).

5.4.1.2 Aggiunta degli installatori

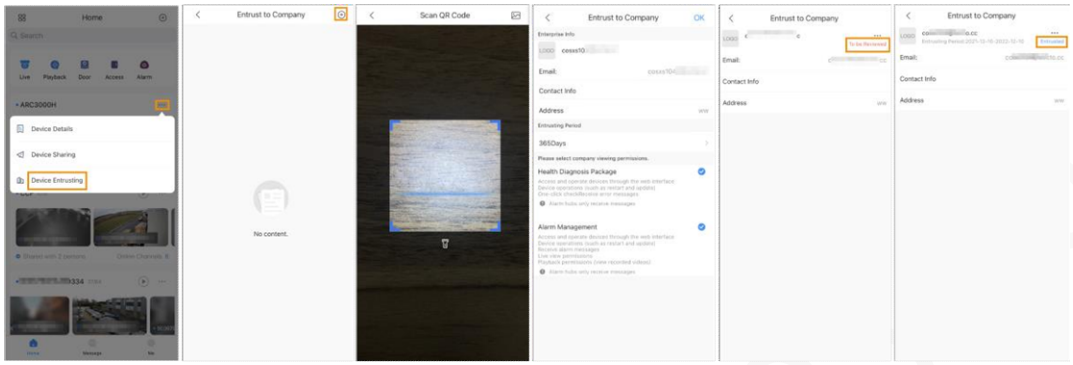
Gli amministratori DMSS possono aggiungere degli installatori affidando loro dei dispositivi. I dispositivi possono essere affidati agli installatori uno per volta o in serie.

5.4.1.2.1 Affidamento dei dispositivi uno per volta

Procedura

Passaggio 1: Nella schermata **Home**, toccare ••• accanto a un dispositivo, quindi toccare **Affidamento dispositivo** (Device Entrusting).

Figura 5-4 Affidamento di un dispositivo



Passaggio 2: Nella schermata **Affida a un'azienda** (Entrust to Company), toccare e scansionare il codice QR dell'installatore, o toccare e importare l'immagine del codice QR, per affidare il dispositivo all'installatore.

È possibile chiedere agli installatori i loro codici QR.

Passaggio 3: Nella schermata **Affida a un'azienda** (Entrust to Company), selezionare la durata dell'affidamento e le autorizzazioni di visualizzazione dell'azienda, quindi toccare **OK**.

- **Pacchetto diagnosi stato** (Health Diagnosis Package) e **Gestione allarme** (Alarm Management).
- scansionato il codice QR dell'installatore.

Passaggio 4: Visualizzare i dettagli relativi all'affidamento sulla schermata **Affida a un'azienda** (Entrust to Company).

Una volta completata la procedura di affidamento, la voce **Da verificare** (To be Reviewed) cambia in **Consegnato** (Delivered).

Quando viene inviata una richiesta di affidamento, nella schermata **Home** compare un messaggio. È necessario attendere la risposta dell'installatore, che comparirà nella schermata **Profilo > Casella di posta > Personali** (Me > Mailbox > Personal).

Operazioni correlate

- Per modificare le autorizzazioni, accedere alla schermata **Affida a un'azienda** (Entrust to Company) e toccare **Modifica autorizzazioni** (Change Permissions).
- Per revocare le autorizzazioni di affidamento, accedere alla schermata **Affida a un'azienda** (Entrust to Company) e toccare **Revoca** (Withdraw).

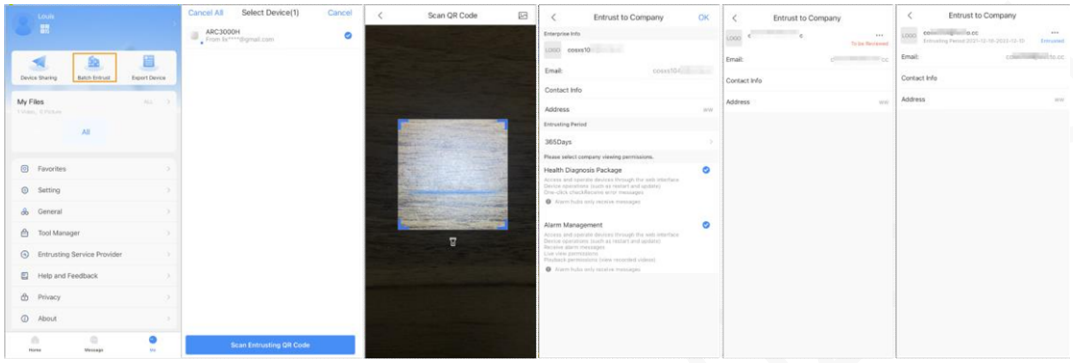
- Per rinnovare le autorizzazioni di affidamento, accedere alla schermata **Affida a un'azienda** (Entrust to Company) e toccare **Rinnova** (Renew).

5.4.1.2.2 Affidamento in serie dei dispositivi

I dispositivi possono essere affidati in serie a un'azienda.

Passaggio 1: Nella schermata **Home**, selezionare **Profilo > Affidamento in serie** (Me > Batch Entrust).

Figura 5-5 Affidamento in serie dei dispositivi



Passaggio 2: Nella schermata **Seleziona dispositivo** (Select Device), selezionare i dispositivi e affidarli all'azienda. La procedura per l'affidamento di uno o più dispositivi è la stessa. Per ulteriori dettagli, consultare la sezione "5.4.1.2.1 Affidamento dei dispositivi uno per volta".

5.4.2 Eliminazione degli utenti

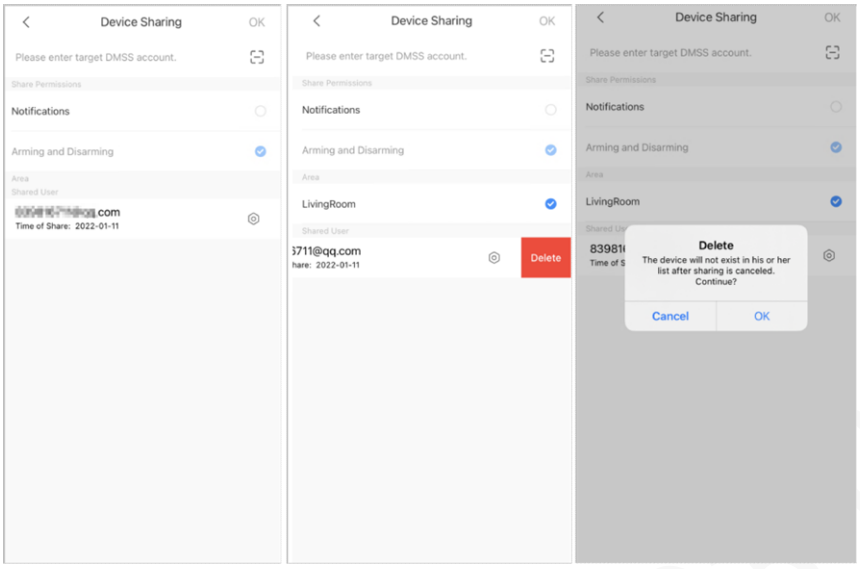
Gli amministratori DMSS possono eliminare sia gli installatori che gli utenti DMSS generici.

5.4.2.1 Annullamento della condivisione dei dispositivi

Gli amministratori DMSS possono eliminare gli utenti DMSS generici annullando le relative condivisioni dei dispositivi dalla schermata **Condivisione dispositivo** (Device Sharing). Per ulteriori dettagli su come accedere alla schermata **Condivisione dispositivo** (Device Sharing), consultare la sezione "5.4.1.1 Aggiunta di utenti DMSS generici". L'esempio in questa sezione si basa sui metodi del menu ••• > **Condivisione dispositivo** (Device Sharing).

Passaggio 1: Nella **schermata iniziale** (Home), toccare ••• accanto a un dispositivo, quindi toccare **Condivisione dispositivo** (Device Sharing).

Figura 5-6 Condivisione dei dispositivi



Passaggio 2: Selezionare un account dal relativo elenco nella schermata **Condivisione dispositivo** (Device Sharing), quindi scorrere il blocco verso sinistra e toccare **Elimina** (Delete).

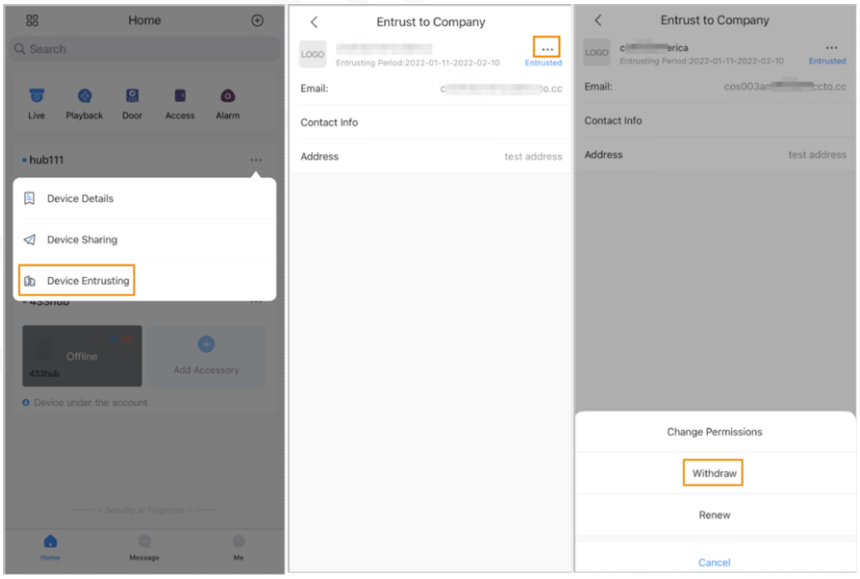
Passaggio 3: Toccare **OK** per annullare la condivisione.

5.4.2.2 Annullamento delle richieste di affidamento

Gli amministratori DMSS possono eliminare gli installatori annullando le relative richieste di affidamento.

Passaggio 1: Nella schermata **Home**, toccare ... accanto a un dispositivo, quindi toccare **Affidamento dispositivo** (Device Entrusting).

Figura 5-7 Revoca di una richiesta di affidamento



Passaggio 2: Nella schermata **Affidamento dispositivo** (Device Entrusting), selezionare ... > **Revoca** (Withdraw) e toccare **OK**.

Verrà inviato un messaggio all'account dell'installatore. L'affidamento viene annullato quando l'installatore legge il messaggio e approva la richiesta di revoca dell'affidamento nell'app COS Pro.

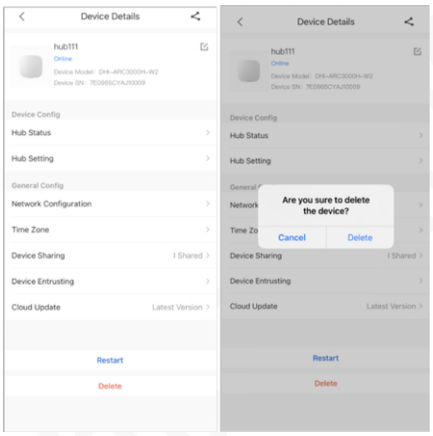
5.4.2.3 Eliminazione dei dispositivi

Gli amministratori DMSS possono eliminare sia gli installatori che gli utenti DMSS generici eliminando i dispositivi.

Gli amministratori DMSS non possono eliminare un installatore se i dispositivi sono stati condivisi da quest'ultimo.

Passaggio 1: Nella schermata **Home**, selezionare [illegible] > **Dettagli dispositivo** (Device Details).

Figura 5-8 Eliminazione di un dispositivo



Passaggio 2: Nella schermata **Dettagli dispositivo** (Device Details), toccare **Elimina** (Delete).

Passaggio 3: Toccare **Elimina** (Delete) per eliminare i dispositivi.

6 Operazioni generali

Gli utenti di livello 2 e 3 possiedono le autorizzazioni per inserire e disinserire il sistema di allarme. L'esempio illustrato in questa sezione si basa sull'utilizzo dell'app DMSS da parte dell'utente finale.

Prerequisiti

- Verificare di avere aggiunto una centralina prima di procedere con le configurazioni.
- Verificare che la connessione internet della centralina sia stabile.
- Verificare che la centralina sia disinserita.

Informazioni preliminari

È possibile gestire le centraline di allarme e gli accessori, eseguendo operazioni come l'inserimento e il disinserimento del sistema di allarme e la configurazione dei dispositivi di allarme.

Procedura

Passaggio 1: Sulla schermata della centralina, toccare **Accessori** (Accessory) per aggiungere gli accessori. Per ulteriori dettagli sull'aggiunta degli accessori, consultare i manuali d'uso dei dispositivi interessati.

Passaggio 2: Inserire e disinserire i rilevatori, in una solo zona o in tutte le zone, manualmente o tramite programmazione.

- Inserimento e disinserimento in una sola zona: i rilevatori vengono inseriti e disinseriti in una zona specifica. Per ulteriori dettagli, consultare la sezione "6.1 Inserimento e disinserimento in una sola zona".
- Inserimento e disinserimento globale: i rilevatori vengono inseriti e disinseriti in tutte le zone. Per ulteriori dettagli, consultare la sezione "6.2 Inserimento e disinserimento globale".
- Inserimento e disinserimento manuale: il sistema di sicurezza viene inserito tramite l'app DMSS, il tastierino o il radiocomando.
- Inserimento e disinserimento programmato: i rilevatori vengono inseriti e disinseriti tramite programmazione. Per ulteriori dettagli, consultare la sezione "6.4 Inserimento e disinserimento programmati".

6.1 Inserimento e disinserimento singolo

È possibile inserire e disinserire i rilevatori in una sola zona.

Passaggio 1: Nella schermata della centralina, toccare **Zona** (Zona).

Passaggio 2: Toccare una zona e selezionare un'opzione tra **In presenza** (Home), **In assenza** (Away), **Disinserito** (Disarm) o **Esci** (Disable).

- **In presenza:** modalità che consente di inserire il sistema di allarme quando ci si trova all'interno della zona coperta.
- **In assenza:** il sistema di allarme viene inserito quando ci si trova fuori dalla zona coperta.

- **Disinserisci:** il sistema di allarme viene disinserito. È l'operazione opposta rispetto a quella di inserimento.
- **Esci:** consente di uscire dalla schermata.

6.2 Inserimento e disinserimento globale

Prerequisiti

Verificare di avere attivato la funzione **Inserimento/disinserimento globale** (Global Arming/Disarming). Nella schermata della centralina, selezionare > **Impostazioni centralina** (Hub Setting) e attivare la funzione **Inserimento/disinserimento globale** (Global Arming/Disarming).

Informazioni preliminari

È possibile inserire e disinserire i rilevatori in tutte le zone.

Procedura

Passaggio 1: Passare alla schermata della centralina.
Passaggio 2: Nella schermata in alto, selezionare un'opzione tra **In presenza** (Home), **In assenza** (Away) e **Disinserisci** (Disarm).

6.3 Inserimento e disinserimento manuale

È possibile inserire il sistema di sicurezza tramite l'app DMSS, il tastierino o il radiocomando.

- Per inserire e disinserire i rilevatori in una sola zona o in tutte le zone, consultare le sezioni "6.1 Inserimento e disinserimento in una sola zona", e "6.2 Inserimento e disinserimento globale".
- Per utilizzare il radiocomando e il tastierino, è necessario prima assegnare a questi ultimi le autorizzazioni di controllo delle zone. Per ulteriori dettagli, consultare i manuali d'uso del radiocomando e del tastierino.

6.4 Inserimento e disinserimento programmati

È possibile programmare l'inserimento e il disinserimento dei rilevatori. È possibile configurare piani che comprendono zone, modalità e periodi di inserimento.
Passaggio 1: Nella schermata della centralina, selezionare > **Impostazioni centralina > Inserimento/disinserimento programmato** (Hub Setting > Scheduled Arming/Disarming).
Passaggio 2: Nella schermata **Inserimento/disinserimento programmato** (Scheduled Arming/Disarming), toccare **Aggiungi** (Add), quindi configurare i piani di inserimento.

- **Nome:** scegliere un nome per i piani di inserimento.
- **Zona:** selezionare una o più zone da attivare.
- **Modalità di inserimento:** selezionare un'opzione fra **In presenza** (Home), **In assenza** (Away) e **Disattiva** (Disarm).
- **Ora:** impostare l'ora di inserimento.

Per applicare ad altri giorni l'ora di inserimento, toccare **Ripeti** (Repeat) e selezionare i giorni.

- **Inserimento forzato:** selezionare se necessario.

Appendice 1 Descrizione degli errori di inserimento

Appendice Tabella 1-1 Descrizione degli errori di inserimento (accessori)

N.	Causa	Descrizione
1	ModuleLoss	L'accessorio é offline.
2	HeartError	Non sono stati inviati pacchetti heartbeat per pid di 18 minuti.
3	Alarm	Allarme (24 ore).
4	Open	Il coperchio sul retro del dispositivo é stato aperto.
5	exopen	Il coperchio sul retro del dispositivo esterno é stato aperto.
6	Tamper	L'allarme antimanomissione dell'accessorio é stato attivato.
7	LowBattery	La batteria del dispositivo é scarica.
8	PriPowerLoss	Rilevato guasto all'alimentazione principale dell'accessorio.
9	BatteryLoss	Rilevato guasto alla batteria.
10	OverVoltage	Rilevata sovratensione.
11	OverCurrent	Rilevata sovracorrente.
12	OverHeat	Rilevato surriscaldamento.
13	FireAlarm	E stato attivato l'allarme antincendio.
14	MedicalAlarm	E stato attivato l'allarme emergenza medica.
15	SOSAlarm	E stato attivato l'allarme SOS.
16	PanicAlarm	E stato attivato l'allarme antipanico.
17	GasAlarm	E stato attivato l'allarme per ie fughe di gas.
18	IntrusionAlarm	E stato attivato l'allarme contro le intrusioni.
19	HoldUpAlarm	E stato attivato l'allarme antipanico.

Appendice Tabella 1-2 Descrizione degli errori di inserimento (centralina)

N.	Causa	Descrizione
1	SOSAlert	L'allarme antipanico puo essere attivato dall'app DMSS.
2	Tamper	L'allarme antimanomissione della centralina é stato attivato.
3	Server Connect Error	La centralina é offline.
4	SIAServer Connect Error	Si é verificato un errore di connessione tra la centralina e il centro di ricezione degli allarmi SIA.

N.	Causa	Descrizione
5	LowBattery	Batteria scarica.
6	MainLoss	E stato rilevato un guasto all'alimentazione principale.
7	BatteryLoss	Rilevato guasto alia batteria.
8	NoGSM	Sono stati rilevati errori nel modulo 2G/4G.
9	ATS Fault	E stato rilevato un guasto al sistema di trasmissione dell'allarme.
10	Cellular Network ATP Fault	E stato rilevato un guasto al percorso di trasmissione dell'allarme (errore della rete cellulare).
11	Wired Network/Wi-Fi ATP Fault	E stato rilevato un guasto al percorso di trasmissione dell'allarme (problema al cavo di connessione o errore Wi-Fi).

Appendice 2 Descrizione dei codici evento SIA

Appendice — Tabella 2-1 Descrizione dei codici evento SIA

N.	Evento	Codice CID	Descrizione
1	Allarme movimento	130 133 134	130: allarme antifurto. 133: allarme zone 24 ore (rilevatori). 134: allarme ingresso/uscita.
2	Ripristino allarme rilevatore per porte	130 133 134	130: allarme antifurto. 133: allarme zone 24 ore (rilevatori). 134: allarme ingresso/uscita.
3	Ripristino allarme ingresso esterno	130 133 134	130: allarme antifurto. 133: allarme zone 24 ore (rilevatori). 134: allarme ingresso/uscita.
4	Allarme coercizione	121	Allarme coercizione.
5	Allarme SOS	120	Allarme antipanico.
6	Allarme intrusione	130 133 134	130: allarme antifurto. 133: allarme zone 24 ore (rilevatori). 134: allarme ingresso/uscita.
7	Allarme incendio	110	Allarme incendio.
8	Allarme fuga di gas	151	Allarme rilevamento gas.
9	Allarme emergenza medica	100	Allarme emergenza medica.
10	Allarme rapina a mano armata	120	Allarme antipanico.
11	Manomissione controller risolta	137	Manomissione.
12	Manomissione periferica risolta	383	Manomissione sensore.
13	Manomissione dispositivo esterno risolta	383	Manomissione sensore.
14	Tensione batteria ripristinata	302	Batteria di sistema scarica.
15	Guasto batteria risolto	3J 1	Batteria mancante/guasta.
16	Corrente ripristinata	301	Interruzione CA.
17	Interferenza RF	344	Interferenza ricevitore RF rilevata.

N.	Evento	Codice CID	Descrizione
18	Guasto sistema di trasmissione allarme ripristinato	350	Problema di comunicazione.
19	Guasto percorso di trasmissione allarme ripristinato/errori Wi-Fi risolti	350	Problema di comunicazione.
20	Guasto percorso di trasmissione allarme ripristinato/errori Wi-Fi risolti	350	Problema di comunicazione.
21	Errore periferica non connessa risolto	381	Mancanza di supervisione — RF.
22	Allarme batteria scarica periferica ripristinato	302	Batteria di sistema scarica.
23	Guasto batteria periferica risolto	3 J 1	Batteria mancante/guasta.
24	Guasto alimentazione principale periferica risolto	301	Interruzione CA.
25	Guasto RF-HD risolto	354	Comunicazione evento non riuscita.
26	Dispositivo bloccato e sbloccato	501	Lettore di accesso disabilitato.
27	Protezione dalle sovratensioni ripristinata	3 J 9	Sovratensione dell'alimentatore.
28	Protezione dalle sovracorrenti ripristinata	3 â 2	Sovracorrente dell'alimentatore.
29	Protezione dal surriscaldamento ripristinata	318	Surriscaldamento dell'alimentatore.
30	Allarme alta temperatura ripristinato	158	Alta temp.
31	Allarme bassa temperatura ripristinato	159	Bassa temp.

N.	Evento	Codice CID	Descrizione
32	Inserimento	400 (app) 401 (tastierino) 403 (inserimento programmato) 407 (radiocomando) 408 (inserimento globale)	400: apertura/chiusura. 401: apertura/chiusura utente. 403: apertura/chiusura automatica. 407: inserimento/disinserimento remoto. 408: inserimento rapido.
33	Disinserimento	400 (app) 401 (tastierino) 403 (inserimento programmato) 407 (radiocomando) 408 (inserimento senza password)	400 Apertura/chiusura. 401 Apertura/chiusura utente. 403 Apertura/chiusura automatica. 407 Inserimento/disinserimento remoto. 408 Inserimento rapido.
34	Inserimento in presenza	441	Inserimento IN PRESENZA.
35	Errore inserimento	454 (errore inserimento) 455 (errore inserimento programmato) 457 (errore inserimento ritardato uscita)	454 Errore chiusura. 455 Errore inserimento automatico. 457 Errore uscita (utente).
36	Inserimento forzato	450	Errore apertura/chiusura.
37	Disattivazione periferica risolta	502	Disattivazione temporanea.
38	Disattivazione solo allarme manomissione ripristinata	503	Disabilitazione temporanea.
39	Rapporto test manuale	601	Rapporto test attivazione manuale.

Appendice 3 Raccomandazioni sulla sicurezza informatica

La sicurezza informatica non é solamente una parola di moda: é qualcosa che ha a che fare con tutti i dispositivi collegati a Internet. La sorveglianza video IP non é immune ai rischi informatici, ma adottare semplici misure di protezione e rafforzamento delle reti e dei dispositivi di rete rende questi ultimi meno suscettibili agli attacchi. Di seguito sono riportati alcuni consigli e raccomandazioni di Dahua su come creare un sistema di sorveglianza pid sicuro.

Azioni obbligatorie da intraprendere per la sicurezza di rete di base dei dispositivi:

1. Utilizzare password sicure

   Seguire queste raccomandazioni quando si impostano le password:

   - La lunghezza non deve essere inferiore a 8 caratteri.
   - Utilizzare almeno due tipi di caratteri diversi scelti fra lettere maiuscole e minuscole, numeri e simboli.
   - Le password non devono contenere il nome dell'account o il nome dell'account al contrario.
   - Non utilizzare caratteri in sequenza, come 123, abc ecc.
   - Non utilizzare caratteri ripetuti, come 111, aaa ecc.

2. Aggiornare il firmware e il software del client con regolaritâ

   - Per assicurare che il sistema sia sempre protetto dalle patch e dagli aggiornamenti di sicurezza pid recenti, é consigliabile mantenere aggiornati i firmware dei propri dispositivi (NVR, DVR, telecamere IP ecc.), come previsto dagli standard del settore tecnologico. Quando i dispositivi sono collegati a una rete pubblica, é consigliabile attivare la funzione "Verifica automaticamente la presenza di aggiornamenti" per ottenere informazioni regolari sugli aggiornamenti del firmware rilasciati dai produttori.
   - E consigliabile scaricare e utilizzare l'ultima versione del software del client.

Raccomandazioni facoltative ma consigliate per migliorare la sicurezza di rete dei dispositivi:

1. Protezione fisica

   E consigliabile proteggere fisicamente i dispositivi, specialmente quelli di archiviazione. Ad esempio, posizionare i dispositivi all'interno di un armadio in una stanza dei computer e implementare misure per il controllo degli accessi e la gestione delle chiavi adatte a evitare che il personale non autorizzato possa danneggiare l'hardware, collegare senza permesso dispositivi rimovibili (come chiavette USB e porte seriali) ecc.

2. Modificare le password con regolaritâ

   E consigliabile modificare ie password regolarmente per ridurre il rischio che vengano scoperte o violate.

3. Impostare e aggiornare tempestivamente le informazioni per il ripristino delle password

   Il dispositivo supporta la funzione di ripristino della password. Configurare per tempo ie informazioni relative al ripristino della password, compreso l'indirizzo e-mail dell'utente finale e le domande di sicurezza. Se le informazioni cambiano, modificarle tempestivamente. Quando si impostano le domande di sicurezza per il ripristino della password, é consigliabile non utilizzare domande ie cui risposte possono essere facilmente indovinate.

4. **Attivare il blocco dell'account**
   La funzione di blocco dell'account è attiva per impostazione predefinita ed è consigliabile non disattivarla per garantire la sicurezza dell'account. Se un malintenzionato cerca di accedere ripetutamente con una password errata, l'account corrispondente e l'indirizzo IP utilizzato verranno bloccati.
5. **Modificare i valori predefiniti delle porte HTTP e relative agli altri servizi**
   Per ridurre il rischio che venga scoperto il numero di porta utilizzato, è consigliabile modificare i valori predefiniti delle porte HTTP e relative agli altri servizi scegliendo una qualsiasi combinazione di numeri compresa fra 1024 e 65535.
6. **Attivare il protocollo HTTPS**
   È consigliabile attivare il protocollo HTTPS, così da poter accedere al servizio web tramite un canale di comunicazione sicuro.
7. **Associare l'indirizzo MAC**
   È consigliabile associare gli indirizzi IP e MAC del gateway ai dispositivi per ridurre il rischio di spoofing ARP.
8. **Assegnare account e autorizzazioni in modo ragionevole**
   Aggiungere gli utenti con ragionevolezza e assegnare loro il minimo set di permessi in base alle esigenze lavorative e di gestione.
9. **Disattivare i servizi non necessari e scegliere modalità sicure**
   Per ridurre i rischi, è consigliabile disattivare servizi come SNMP, SMTP, UPnP ecc quando non sono necessari.
   Se sono necessari, è vivamente consigliato utilizzare le modalità sicure per i servizi che seguono (l'elenco non è esaustivo):
   - SNMP: scegliere SNMP v3 e impostare password crittografiche e di autenticazione sicure.
   - SMTP: scegliere TLS per accedere al server e-mail.
   - FTP: scegliere SFTP e impostare password sicure.
   - Hotspot AP: scegliere la crittografia WPA2-PSK e impostare password sicure.
10. **Utilizzare la trasmissione crittografata di audio e video**
    Se i contenuti audio e video sono molto importanti o sensibili, è consigliabile utilizzare la funzione di trasmissione crittografata per ridurre il rischio che i dati vengano rubati.
    Nota: la trasmissione crittografata rende la trasmissione meno efficiente.
11. **Verifiche di sicurezza**
    - Verifica degli utenti online: è consigliabile verificare regolarmente gli utenti online per controllare se qualcuno ha eseguito l'accesso al dispositivo senza autorizzazione.
    - Verifica dei registri dei dispositivi: controllando i registri, è possibile conoscere gli indirizzi IP utilizzati per accedere ai propri dispositivi e alle operazioni chiave.
12. **Registro di rete**
    A causa della limitata capacità di archiviazione dei dispositivi, il registro salvato è limitato. Se è necessario archiviare il registro per un tempo maggiore, è consigliabile attivare il registro di rete per assicurarsi che i registri critici siano sincronizzati con il server del registro di rete, garantendo una tracciatura efficiente.
13. **Costruire un ambiente di rete sicuro**
    Per garantire la sicurezza dei dispositivi e ridurre i potenziali rischi informatici, è consigliabile:
    - Disattivare la funzione di mappatura delle porte del router per evitare l'accesso diretto ai dispositivi intranet da una rete esterna.

- La rete deve essere suddivisa e isolata in base alle effettive esigenze di rete. In assenza di requisiti di comunicazione fra due sottoreti, é consigliabile utilizzare tecnologie come VLAN, GAP e altre per suddividere la rete e isolarla.
- Utilizzare il sistema di autenticazione degli accessi 802.1x per ridurre il rischio di accessi non autorizzati alle reti private.
- Attivare la funzione di filtraggio degli indirizzi IP/MAC per limitare il numero di host che possono accedere al dispositivo.

Ulteriori informazioni

Visitare il centro per le risposte alle emergenze di sicurezza sul sito ufficiale Dahua per consultare gli avvisi e i consigli sulla sicurezza pid recenti.

E N ABLING A SAF ER SOC IETY A ND S MARTER LIVIN G

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: | Fax: +86-571-87688815 | Tel: +86-571-87688883