AX PRO

Manuale d'uso

Informazioni legali

Informazioni su questo manuale

Il Manuale include le istruzioni per l'uso e la gestione del Prodotto. Le foto, i grafici, le immagini e tutte le altre informazioni che seguono sono solo per la descrizione e la spiegazione. Le informazioni contenute nel Manuale sono soggette a modifiche, senza preavviso, a causa di aggiornamenti del firmware o altri motivi. Si prega di trovare l'ultima versione di questo Manuale sul sito web di Hikvision (https://www.hikvision.com/).
Si prega di utilizzare questo manuale con la guida e l'assistenza di professionisti addestrati nel supporto del prodotto.

Marchi

HIKVISION e altri marchi e loghi di Hikvision sono proprietà di Hikvision in varie giurisdizioni.
Altri marchi e loghi menzionati sono di proprietà dei loro rispettivi proprietari.

Disclaimer

NELLA MISURA MASSIMA CONSENTITA DALLA LEGGE APPLICABILE, QUESTO MANUALE E IL PRODOTTO DESCRITTO, CON IL SUO HARDWARE, SOFTWARE E FIRMWARE, SONO FORNITI "COSÌ COME SONO" E "CON TUTTI I DIFETTI E GLI ERRORI". HIKVISION NON FORNISCE ALCUNA GARANZIA, ESPLICITA O IMPLICITA, INCLUSE, SENZA LIMITAZIONI, LA COMMERCIABILITÀ, LA QUALITÀ SODDISFACENTE O L'IDONEITÀ PER UNO SCOPO PARTICOLARE. L'USO DEL PRODOTTO DA PARTE VOSTRA E' A VOSTRO RISCHIO E PERICOLO. IN NESSUN CASO HIKVISION SARA' RESPONSABILE NEI CONFRONTI DELL'UTENTE PER QUALSIASI DANNO SPECIALE, CONSEQUENZIALE, INCIDENTALE O INDIRETTO, INCLUSI, TRA GLI ALTRI, I DANNI PER LA PERDITA DI PROFITTI, L'INTERRUZIONE DELL'ATTIVITA', LA PERDITA DI DATI, LA CORRUZIONE DI SISTEMI O LA PERDITA DI DOCUMENTAZIONE, ANCHE SE BASATI SU VIOLAZIONE DEL CONTRATTO, TORTO (INCLUSA LA NEGLIGENZA), RESPONSABILITA' DEL PRODOTTO O ALTRO, IN RELAZIONE ALL'USO DEL PRODOTTO, ANCHE SE HIKVISION E' STATA INFORMATA DELLA POSSIBILITA' DI TALI DANNI O PERDITE.
L'UTENTE RICONOSCE CHE LA NATURA DI INTERNET PREVEDE RISCHI INTRINSECI PER LA SICUREZZA, E HIKVISION NON SI ASSUME ALCUNA RESPONSABILITÀ PER OPERAZIONI ANOMALE, PERDITE DI PRIVACY O ALTRI DANNI DERIVANTI DA ATTACCHI INFORMATICI, ATTACCHI DI HACKER, ISPEZIONE DI VIRUS O ALTRI RISCHI PER LA SICUREZZA DI INTERNET; TUTTAVIA, HIKVISION FORNIRÀ ASSISTENZA TECNICA TEMPESTIVA, SE NECESSARIO.
LEI ACCETTA DI UTILIZZARE QUESTO PRODOTTO IN CONFORMITÀ CON TUTTE LE LEGGI APPLICABILI, E LEI È L'UNICO RESPONSABILE DI GARANTIRE CHE IL SUO UTILIZZO SIA CONFORME ALLA LEGGE APPLICABILE. IN PARTICOLARE, L'UTENTE È RESPONSABILE DELL'USO DI QUESTO PRODOTTO IN MODO DA NON VIOLARE I DIRITTI DI TERZI, INCLUSI, SENZA LIMITAZIONI, I DIRITTI DI PUBBLICITÀ, I DIRITTI DI PROPRIETÀ INTELLETTUALE, O LA PROTEZIONE DEI DATI E ALTRI DIRITTI DI PRIVACY. L'UTENTE NON DEVE UTILIZZARE QUESTO PRODOTTO PER USI FINALI PROIBITI, INCLUSO LO SVILUPPO O LA PRODUZIONE DI ARMI DI DISTRUZIONE DI MASSA, LO SVILUPPO O LA PRODUZIONE DI ARMI DI DISTRUZIONE DI MASSA.

PRODUZIONE DI ARMI CHIMICHE O BIOLOGICHE, QUALSIASI ATTIVITÀ NEL CONTESTO LEGATO A QUALSIASI ESPLOSIVO NUCLEARE O AL CICLO DEL COMBUSTIBILE NUCLEARE NON SICURO, O A SOSTEGNO DI ABUSI DEI DIRITTI UMANI.
IN CASO DI CONFLITTO TRA IL PRESENTE MANUALE E LA LEGGE APPLICABILE, PREVALE QUEST'ULTIMA.

Convenzioni sui simboli

I simboli che si possono trovare in questo documento sono definiti come segue.

Simbolo	Descrizione
Pericolo	Indica una situazione pericolosa che, se non evitata, provocherà o potrebbe provocare la morte o lesioni gravi.
Attenzione	Indica una situazione potenzialmente pericolosa che, se non evitata, potrebbe provocare danni alle apparecchiature, perdita di dati, degrado delle prestazioni o risultati inaspettati.
Nota	Fornisce informazioni aggiuntive per sottolineare o integrare punti importanti del testo principale.

Informazioni sulla regolamentazione

EN 50131-1:2006+A1:2009+A2:2017

EN 50131-3:2009

EN 50131-6:2017

EN 50131-5-3:2017

EN 50131-10: 2014

EN 50136-2: 2013

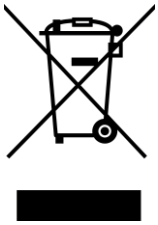
Grado di sicurezza (SG): 2

Classe ambientale (CE): II DP2

Certificato da Telefication

Nota L'etichettatura di conformità EN50131 dovrebbe essere rimossa se vengono utilizzate configurazioni non conformi.

Dichiarazione di conformità UE

CE	Questo prodotto e - se del caso - anche gli accessori forniti sono marcati "CE" e sono quindi conformi alle norme europee armonizzate applicabili elencate nella direttiva EMC 2014/30/UE, nella direttiva RE 2014/53/UE, nella direttiva RoHS 2011/65/UE
	2012/19/EU (direttiva WEEE): I prodotti contrassegnati con questo simbolo non possono essere smaltiti come rifiuti urbani non differenziati nell'Unione Europea. Per un corretto riciclaggio, restituire questo prodotto al fornitore locale al momento dell'acquisto di una nuova apparecchiatura equivalente, oppure smaltirlo presso i punti di raccolta designati. Per maggiori informazioni vedere: www.recyclethis.info
	2006/66/CE (direttiva sulle batterie): Questo prodotto contiene una batteria che non può essere smaltita come rifiuto urbano non differenziato nell'Unione Europea. Vedere la documentazione del prodotto per informazioni specifiche sulla batteria. La batteria è contrassegnata da questo simbolo, che può includere lettere per indicare cadmio (Cd), piombo (Pb) o mercurio (Hg). Per un corretto riciclaggio, restituire la batteria al proprio fornitore o a un punto di raccolta designato. Per ulteriori informazioni vedere:www.recyclethis.info

	Attenzione Questo è un prodotto di classe A. In un ambiente domestico questo prodotto può causare interferenze radio, nel qual caso all'utente può essere richiesto di prendere misure adeguate.
	Informazioni FCC Si prega di prestare attenzione al fatto che cambiamenti o modifiche non espressamente approvati dalla parte responsabile della conformità potrebbero annullare l'autorità dell'utente ad utilizzare l'attrezzatura. Conformità FCC: Questa apparecchiatura è stata testata e trovata conforme ai limiti per un dispositivo digitale di classe B, secondo la parte 15 delle norme FCC. Questi limiti sono progettati per fornire una protezione ragionevole contro le interferenze dannose in un'installazione residenziale. Questa apparecchiatura genera, utilizza e può irradiare energia in radiofrequenza e, se non installata e utilizzata secondo le istruzioni, può causare interferenze dannose alle comunicazioni radio. Tuttavia, non vi è alcuna garanzia che l'interferenza non si verifichi in una particolare installazione. Se questo apparecchio causa interferenze dannose alla ricezione radio o televisiva, che possono essere determinate spegnendo e accendendo l'apparecchio, l'utente è invitato a cercare di correggere l'interferenza adottando una o più delle seguenti misure: Riorientare o riposizionare l'antenna ricevente. Aumentare la separazione tra l'attrezzatura e il ricevitore. Collegare l'apparecchio a una presa di un circuito diverso da quello a cui è collegato il ricevitore. Consultare il rivenditore o un tecnico radiotelevisivo esperto per aiuto. Questo apparecchio deve essere installato e utilizzato con una distanza minima di 20 cm tra il radiatore e il vostro corpo. Condizioni FCC Questo dispositivo è conforme alla parte 15 delle norme FCC. Il funzionamento è soggetto alle seguenti due condizioni: 1. Questo dispositivo non deve causare interferenze dannose. 2. Questo dispositivo deve accettare qualsiasi interferenza ricevuta, comprese le interferenze che possono causare un

	funzionamento indesiderato.

Contenuto

Capitolo 1 Introduzione

1.1 Descrizione del sistema

AX Pro è un sistema di allarme senza fili progettato per proteggere i locali necessari per una corretta protezione dall'allarme intrusione. Supporta LAN/Wi-Fi come rete di trasmissione primaria e GPRS/3G/4G LTE come rete di trasmissione secondaria. Il sistema è applicabile agli scenari di mercato, negozio, casa, fabbrica, magazzino, ufficio, ecc.

- Innovativa tecnologia wireless a 2 vie Tri-X.
- Comunicazione bidirezionale con crittografia AES-128.
- Frequency-hopping spread spectrum (FHSS) è usato per evitare le interferenze, per prevenire le intercettazioni e per permettere le comunicazioni con accesso multiplo a divisione di codice (CDMA).
- Guida vocale per l'allarme, l'indicazione dello stato del sistema, la richiesta di funzionamento, ecc.
- Configurazione tramite client web, client mobile e Convergence Cloud.
- Spinge la notifica dell'allarme tramite messaggi o telefonate.
- Visualizza video di vita da Hik-Connect e video clip di allarme via e-mail, Hik-ProConnect e Hik- Connect.
- Carica i rapporti di allarme su ARC.
- Protocollo SIA-DC09, e supporta sia il Contact ID che il formato dati SIA.
- Batteria di riserva al litio da 4520 mAh con 12 ore di standby.

Ordinazione di

Model lo	Descrizione
DS-PWA64-L-WE	Supporta Ethernet/Wi-Fi e GPRS
DS-PWA96-M-WE	Supporta Ethernet/Wi-Fi, 3G/4G LTE e scheda IC

1.2 Specifiche

		AX PRO	
		64 Serie	**96 Serie**
Capacità	Aree	16	32
	Zone	Fino a 64	Fino a 96
	Uscite		
	Lettori di tag	Fino a 8	Fino a 8
	Tastiere		
	Sounders	4	6
	Ripetitori	2	4
	Portachiavi	32	48
	Tags	32	48
	Lettore di tag incorporato	×	√
Utente	Installatore	1	1
	Amministratore	1	1
	Utenti normali	30	46
Caratteristiche tecniche wireless	Frequenza RF	868 Mhz (865 Mhz per il rilevatore PIR-Camera) /433 Mhz	
	Tipo senza fili	2 vie senza fili	
	Sicurezza senza fili	Crittografia 128 AES	
Caratteristiche funzionali	Prompt vocali	√	√
	Lingua del prompt vocale	Inglese, italiano, spagnolo, francese, russo, portoghese, Germania, polacco	
	Cliente web	√	√
	Diagnostica	√	√
	Notifica SMS	√	√
	Notifica di chiamata vocale	√	√
	Registri del registro eventi	5000 di cui 1000 obbligatori	
	Supporto della telecamera PIR	√	√
	Stoccaggio IVaaS	×	4 clip x 7 sec
Interfacce di comunicazione	Ethernet	10/100 Mbps autoadattabile	
	Wi-Fi	802.11b/g/n (2.4GHz)	
	GPRS	√	×
	3G/4G LTE	×	√
	Slot SIM	Singolo	Doppio
Segnalazione ARC	Categoria ATS	DP2	
	Percorso di trasmissione primario	LAN / WiFi	
	Percorso di trasmissione secondario	GPRS o 3G/4G LTE	
	Operazione di riconoscimento	Pass-through	

	Protocolli	SIA-DC09b, ISUP 5.0	
Servizi cloud	Servizio Hik-ProConnect	√	√
	Servizio Hik-Connect	√	√
Automazione	Interruttore a muro	√	√
	Modulo relè	√	√
	Spina intelligente	√	√
Alimentazione	Tipo PS	Tipo A	
	Ingresso di rete	~ 100-240V 50/60Hz 0.3A (Max)	
	Capacità della batteria	4520 mAh	
	Batteria Standbye	Fino a 12 ore	
	Tipo di batteria	Built-in ricaricabile agli ioni di litio batteria ai polimeri Modello: 765965	
	Consumo di corrente	Con un allarme: 405mA Senza allarme: 340mA	
	Corrente a batteria	340 mA	
	Periodo di ricarica	4 ore all'80%	
	Messaggio di bassa tensione	3.55 V	
Servizio	Nessuna parte di servizio dell'utente all'interno		
Requisiti ambientali	Temperatura d'esercizio	Da -10°C a 50°C -10°Ca＋40°C(temperatura certificata)	
	Umidità relativa	10% ~ 90% senza condensa	
Dimensioni e peso	Dimensione (W×H×D)	170.0 mm (6.7") × 170.0 mm (6.7") ×38.6 mm (1.5")	
	Peso	557,5 g (19,7 once)	
Approvazioni	EN 50131	SG 2 CE II	
	CE	√	
	Rohs/Reach/WEEE	√	
a	Secondo i requisiti definiti in EN 50131-1:2006+A1:2009+A2:2017 Il pannello di controllo wireless AX Pro adotta la modalità pass-through dell'operazione di riconoscimento. Sia il riconoscimento positivo che quello negativo dal ricetrasmettitore del centro ricevente saranno registrati. Descrizione del registro eventi Positive acknowledgement ARC Uploaded acknowledgement Comunicazione ARC negativa fallita		

b	Il pannello di controllo wireless AX Pro è compatibile con il SIA IP Reporting (UDP/TCP-2013) come da ANSI/SIA DC-09-2013: Internet Protocol Event Reporting. Il pannello di controllo supporta i token (protocolli) di **ADM-CID** e **SIA-DCS** definiti in SIA DC-07-2001.04, che saranno modificati per inserire un "*" prima del nome del token come ***ADM-CID** e ***SIA-DCS** quando i dati e il timestamp del messaggio di trasmissione sono criptati AES. AES-128, AES-192 e AES- 256 sono tutti supportati.
c	Secondo EN 50131-1:2006+A1:2009+A2:2017, 9.1 Tipi di alimentazione
d	Valore nominale. La capacità effettiva può variare leggermente. La capacità effettiva della batteria per ogni singolo dispositivo può essere leggermente superiore o inferiore alla capacità nominale della batteria. La rimozione della batteria può causare danni al dispositivo. Per sostituire o riparare la batteria, contattate il vostro installatore.
e	Nella condizione di Wi-Fi connesso, GPRS/3G/4G LTE connesso, ARC connesso (intervallo di polling: 1800 s), 8 ingressi e 1 tastiera accessibili, e servizio cloud accessibile.

Nota

ISUP5.0: un protocollo internet di privacy che viene utilizzato per accedere alla piattaforma di terze parti, che supporta il caricamento dei rapporti di allarme, la gestione di AX PRO e il caricamento di brevi video.
La priorità del messaggio e le indicazioni sono le stesse. L'AXPRO carica i messaggi e dà le indicazioni in modo sincrono.

Nota

Protocollo standard DC-09:
ADM-CID: Il metodo di presentazione dei dati di DC-09 è CID, che non è criptato e solo per caricare il rapporto di allarme.
*ADC-CID: Il metodo di presentazione dei dati di DC-09 è CID, che è criptato e solo per caricare il rapporto di allarme.
SIA-DCS: Il metodo di presentazione dei dati del DC-09 è il DCS (chiamato anche protocollo SIA), che non è criptato e serve solo per caricare il rapporto di allarme.
*SIA-DCS: Il metodo di presentazione dei dati del DC-09 è il DCS (chiamato anche protocollo SIA), che è criptato e solo per caricare il rapporto di allarme.

Istruzione RSSI per le periferiche

Per quanto riguarda la norma EN 50131-5-3 4.2.2 Requisiti di immunità all'attenuazione.

Forza del segnale	Valore RSSI	Indicazione	Osservazione
Forte	>120	Verde	OK per l'installazione
Medio	81 a 120	Giallo	OK per l'installazione
Debole	60-80	Rosso	Non si consiglia di installare, ma può funzionare
Invalido	da 0 a 59	Rosso (flash)	Non va bene da installare, non può funzionare normalmente

Nota

Installate le periferiche solo se la potenza del segnale è superiore a 80. Per ottenere un sistema molto migliore, installare a 120 e oltre.

Opzioni di notifica AX PRO

L'AX PRO è adatto ai seguenti requisiti di notifica insieme ai segnalatori acustici richiesti

Attrezzatura di notifica	I&HAS Grado 2		
	Opzioni		
	C	E	F
WD acustico autoalimentato	2	1	Opzionale
ATS	DP1	Opzionale	DP2

1.3 Aspetto

Pannello frontale

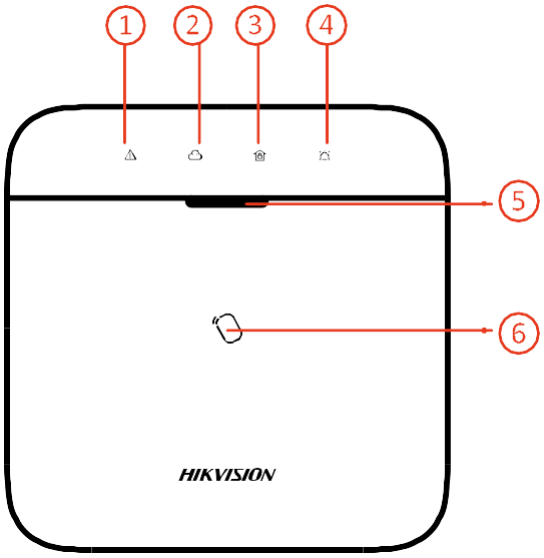


Tabella 1-2 Descrizione del pannello frontale

No.	Nome	Descrizione
1	Indicatore di allarme	Arancione fisso: Nello stato di disarmo, il LED indica l'allarme (come l'allarme panico, l'allarme di zona, l'allarme di manomissione, ecc.) e l'errore (come l'errore di funzionamento, l'errore di connessione, ecc.) **Nota** ● L'indicatore o le notifiche vocali non risponderanno a nessuna operazione effettuata dagli utenti di livello 1. Le notifiche risponderanno solo quando l'utente di livello 1 presenta o utilizza un tag o un portachiavi valido. ● Il dispositivo richiederà informazioni dettagliate sull'allarme o sul guasto mentre gli utenti autorizzati disarmano il sistema.
2	Indicatore di collegamento	Verde fisso: Il pannello è legato all'account Hik-connect Off: il pannello non è legato all'account Hik-connect
3	Indicatore del braccio/disarmo	Blu massiccio per 5 s: Armato Il verde lampeggia due volte: disarmato

No.	Nome	Descrizione
		Nota Se la funzione di **Arming Indicator Keeps Light** è abilitata, il LED rimane blu fisso quando è armato, e spento quando è disarmato. La funzione non è conforme allo standard EN.
4	Indicatore di allarme	Rosso lampeggiante: Allarme avvenuto Rosso fisso: Dispositivo manomesso Off: Nessun allarme
5	Indicatore di potenza	Verde fisso: Accensione Off: Spegnimento
6	Tag Area presente	**Nota** La funzione varia a seconda del modello di dispositivo.

Componente e interfaccia

Rimuovete il coperchio posteriore, e alcuni dei componenti e delle interfacce sono sul pannello posteriore.

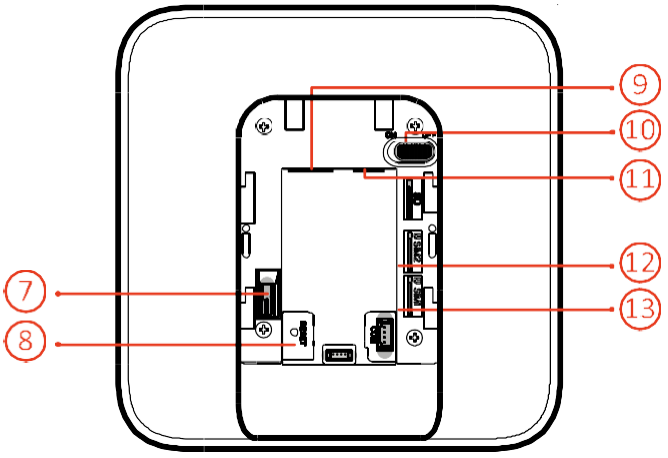


Tabella 1-3 Descrizione del pannello posteriore

Numero	Descrizione
7	Interruttore antimanomissione
8	Pulsante Reset

Numero	Descrizione
	Nota Riavviare il dispositivo, il LED di alimentazione lampeggia 3 volte, e tenere premuto il pulsante di reset per 5 s. Il messaggio vocale indica il risultato dell'operazione. Premere il pulsante per commutare la modalità STA e Hotspot.
9	Interfaccia di alimentazione
10	Interruttore di alimentazione
11	Interfaccia di rete
12	Slot per scheda SIM 1 **Nota** La funzione di GPRS o 3G/4G (implementata con slot per SIM card integrato) varia a seconda del modello del dispositivo.
13	Scheda SIM Slot 2 **Nota** La funzione di GPRS o 3G/4G (implementata con slot per SIM card integrato) varia a seconda del modello del dispositivo.

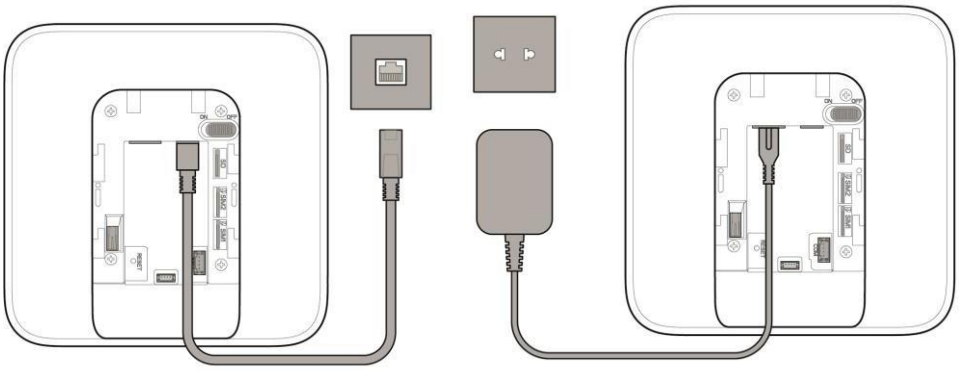
Capitolo 2 Avvio

2.1 Inizializza il dispositivo

Quando si inizia il dispositivo con Hik-ProConnector, l'AX Pro dovrebbe sempre essere aggiunto a un account installatore prima. L'account dell'installatore inviterà e trasferirà la proprietà all'account dell'amministratore più tardi dopo aver terminato tutte le impostazioni iniziali e test. Seguire i passaggi qui sotto per inizializzare il sistema di allarme wireless.

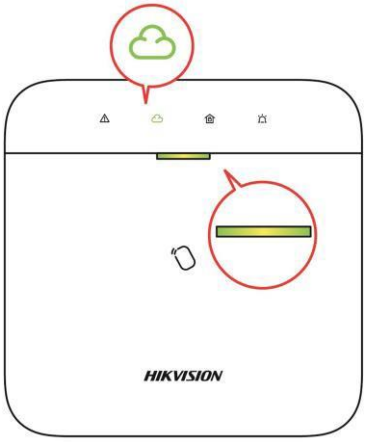
1. Connettiti alla rete.

Collegare il dispositivo alla rete Ethernet e accendere il dispositivo.



Nota

Mentre il dispositivo è acceso, il LED di alimentazione e il LED di collegamento diventano verdi.



2. Creare un sito

Aprite Hik-ProConnect ed effettuate il login con l'account dell'installatore.

Un sito è il luogo in cui il sistema di allarme è stato distribuito. Crea un sito dove il dispositivo può essere aggiunto con il suo nome e indirizzo. Il proprietario del sito sarebbe un utente finale, solitamente considerato come amministratore.

3. Aggiungi dispositivo

Aprire il sito. Tocca **Aggiungi dispositivo** e scansiona il codice QR sull'etichetta del pannello.

Il pannello di controllo sarà aggiunto al sito creato e gestito dall'account dell'installatore, il che significa anche che l'account dell'installatore è stato creato nel pannello.

L'installatore ora può eseguire la configurazione e i test del pannello prima di distribuirlo. Sia il servizio Hik-ProConnect che il client web locale possono essere collegati con l'account dell'installatore Hik-ProConnect.

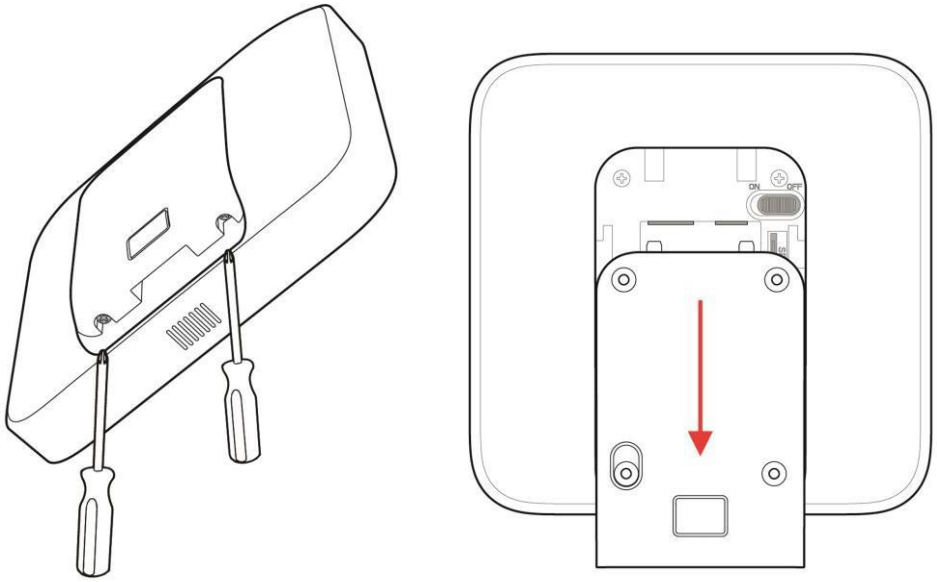
Nota

Mentre inizializza il dispositivo con Hik-connect, non è necessario costruire prima un sito. Scarica e accedi all'App, e aggiungi il dispositivo con la scansione del codice QR o inserisci il numero di serie del dispositivo.

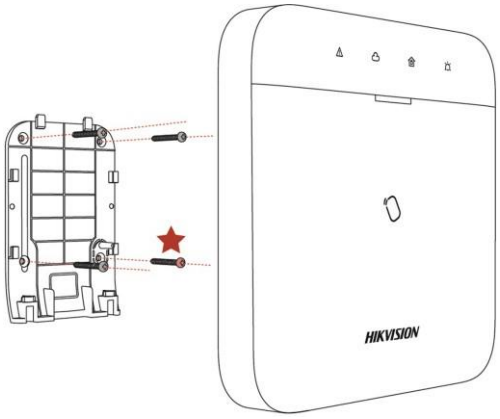
2.2 Installare il dispositivo

Passi

1. Allentare la vite del coperchio posteriore. Fate scorrere verso il basso il coperchio posteriore e rimuovetelo dall'AX PRO.



2. Fissare il coperchio posteriore alla posizione di installazione con le viti in dotazione. Attacca l'AX PRO sul coperchio posteriore e stringi la vite del coperchio posteriore per completare l'installazione.



Nota

- Stella Rossa: Vite TAMPER. È obbligatorio fissare la vite TAMPER.
- Non sono necessari aggiustamenti.
- Da usare solo all'interno dei locali sorvegliati.

Nota

Controllare la potenza del segnale RF prima del collegamento e dell'installazione della periferica. È possibile visualizzare l'indicazione dell'intensità del segnale RF sulla periferica.

Capitolo 3 Gestione degli utenti

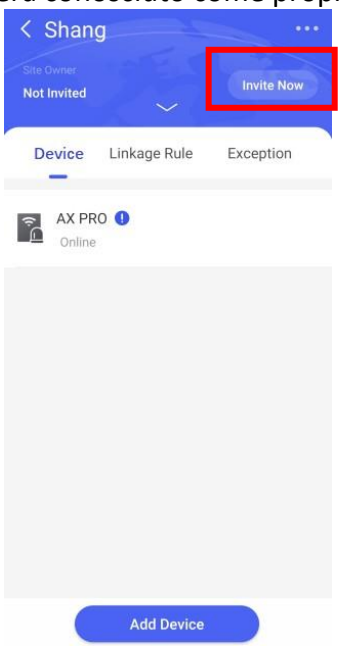
3.1 Gestione degli utenti

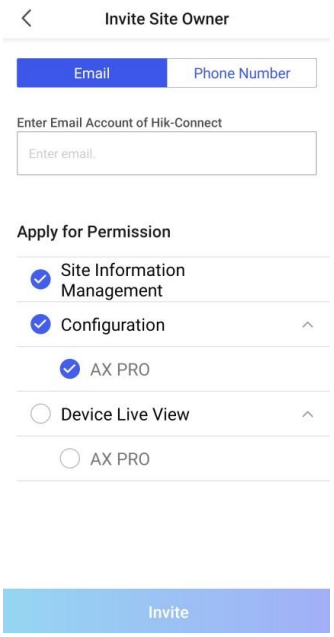
Nota

- Gli utenti possono essere creati nei client.
- Il nome e la password dell'utente di rete (client web e utente APP) possono essere da 1 a 32 caratteri e da 8 a 16 caratteri.

3.1.1 Invita l'amministratore

L'amministratore era conosciuto come proprietario del sito in Hik-ProConnect Service.





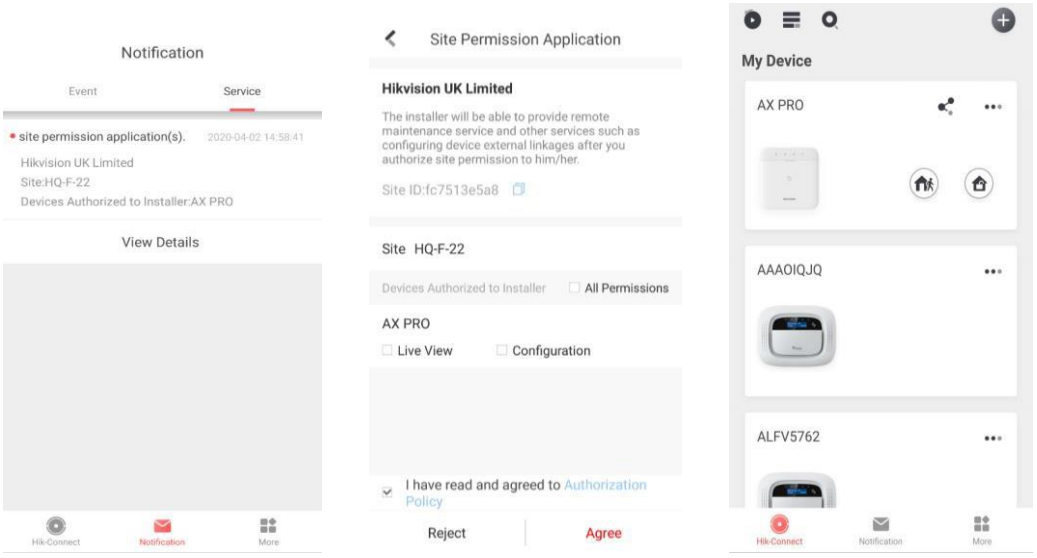
Dopo che la configurazione iniziale è terminata, l'installatore deve invitare il proprietario del sito e

applicare il permesso di gestione del sito e di configurazione del dispositivo dall'account dell'amministratore. L'account amministratore sarebbe un account utente finale nel servizio Hik-Connect.

Premi il pulsante "Invita ora" e inserisci l'account email o il numero di telefono per trasferire la proprietà del sito all'amministratore. Allo stesso tempo, l'installatore applicherà i permessi del proprietario del sito, come la configurazione e la gestione.

Aprite l'applicazione Hik-Connect ed effettuate il login con l'account di amministratore. La richiesta del servizio di installazione sarà ricevuta nella pagina di notifica. Aprire il dettaglio della notifica per accettare il servizio di installazione e impostare le autorizzazioni. Il pannello di controllo e gli altri dispositivi del sito saranno visualizzati nell'elenco dei dispositivi.

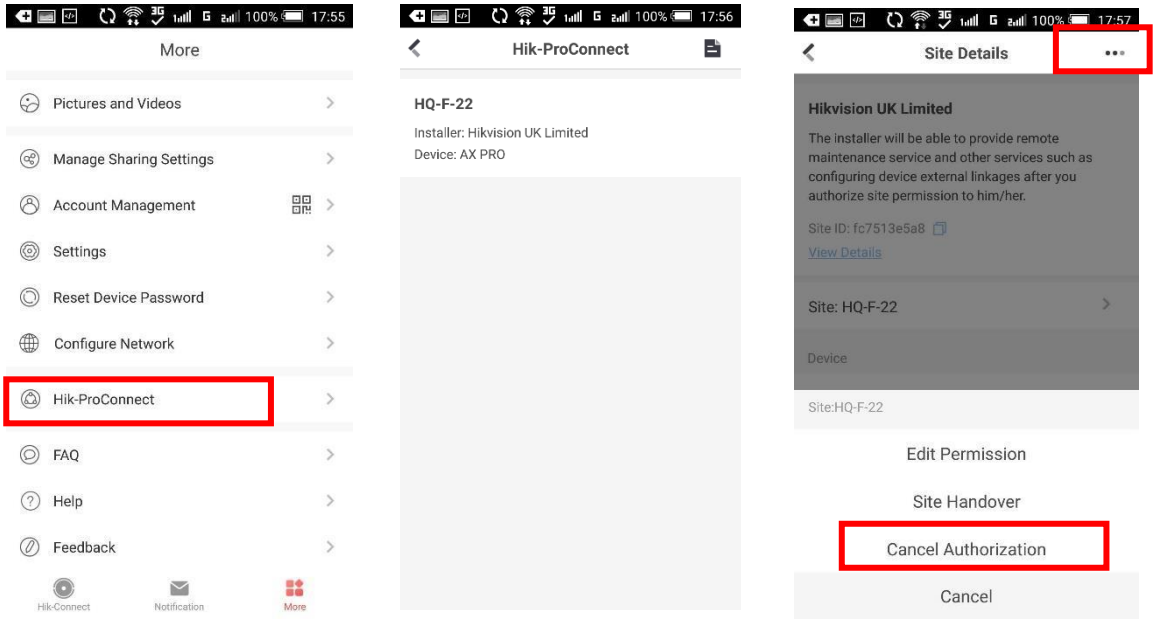
L'account di amministratore sarà aggiunto al pannello di controllo, che potrebbe essere usato per accedere all'app Hik- Connect e al client web locale.



3.1.2 Annullamento dell'accesso dell'installatore

L'amministratore può annullare l'autorizzazione di accesso dell'installatore.

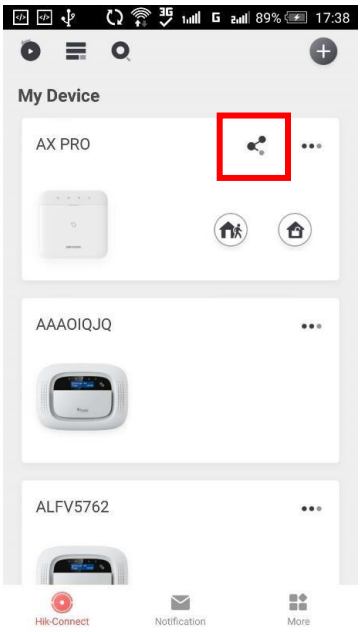
1. Entrare nella pagina **Altro** e toccare **Hik-ProConnect**. Tutti i siti gestiti dal servizio Hik-ProConnect sono elencati nella pagina.
2. Tocca il pulsante di opzione nell'angolo in alto a destra della pagina dei dettagli del sito e tocca **Annulla autorizzazione** nel menu di richiesta.
3. Confermate l'operazione e l'autorizzazione dell'installatore sarà annullata. Una volta che l'autorizzazione è annullata, l'installatore deve applicarla di nuovo se c'è qualche

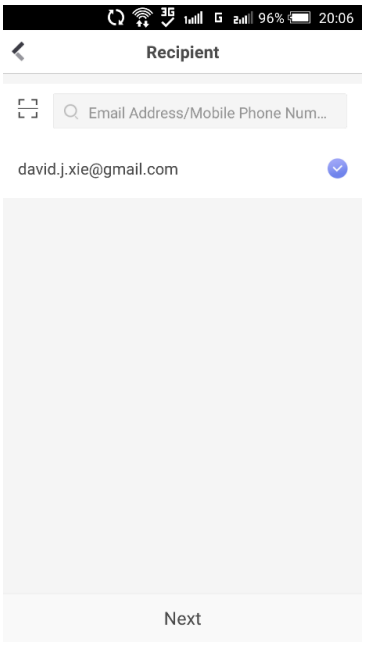


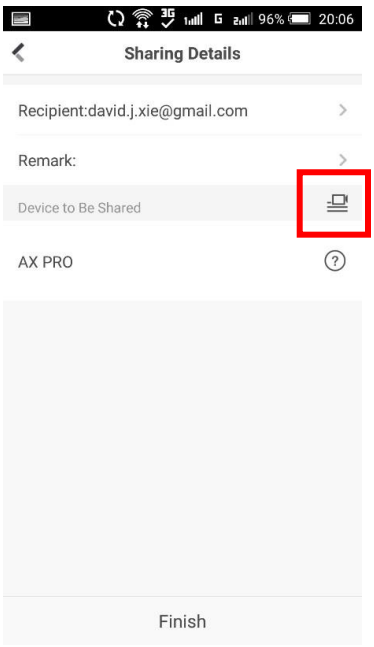
requisito di accesso.

3.1.3 Aggiungere un operatore

L'amministratore può condividere il dispositivo con altri operatori.

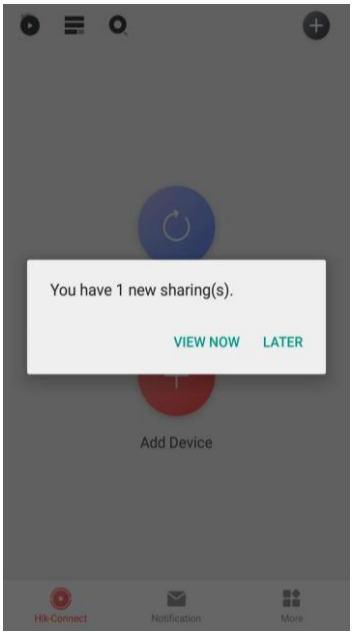


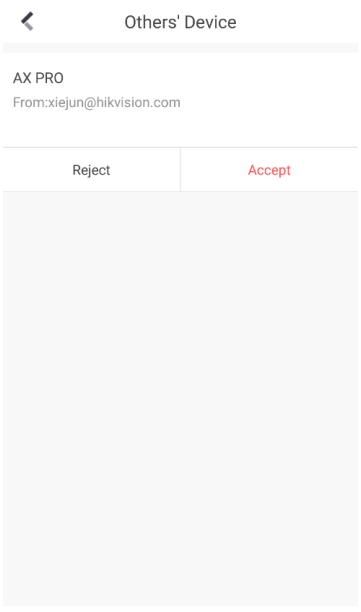


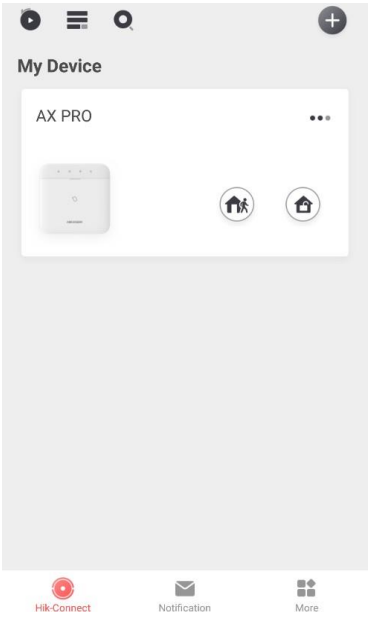


1. Tocca the (pulsante di condivisione) nell'elenco dei the dispositivi.
2. Inserire l'account Hik-Connect dell'operatore.

   L'amministratore può anche selezionare il dispositivo da condividere.







Un messaggio di condivisione sarà inviato all'account dell'operatore, e l'operatore può leggere il messaggio nell'app Hik-Connect.

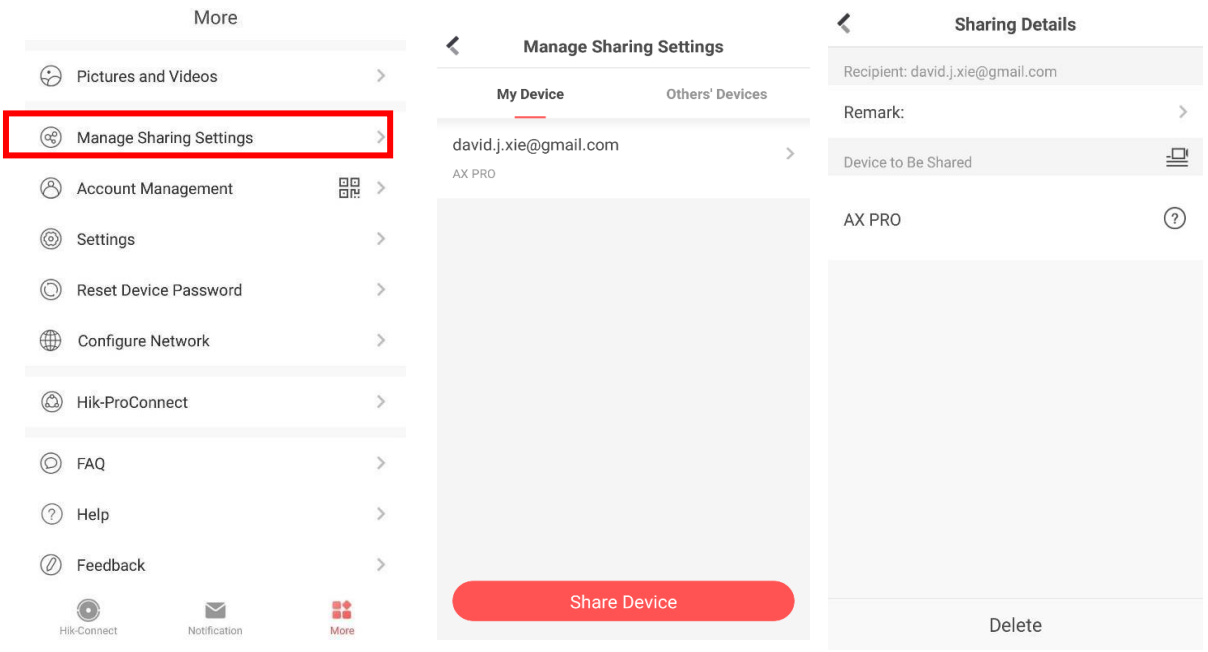
3. Accetta l'invito e il dispositivo sarà elencato nell'elenco dei dispositivi.

L'account dell'operatore sarà aggiunto al pannello di controllo, che potrebbe essere utilizzato per accedere all'app Hik- Connect e al client web locale.

3.1.4 Cancellare un operatore

L'utente amministratore può cancellare un operatore.

1. Entrare nella pagina **More** e toccare **Manage Sharing Settings**.
2. Elimina l'operatore selezionato o lo rimuove dal dispositivo.



3.2 Voci di accesso

All'installatore e agli operatori di AXPRO sono stati assegnati diversi livelli di accesso che definiscono le funzioni del sistema che un singolo utente può eseguire. Diverse voci utente sono previste per diversi ruoli utente con un particolare livello di accesso.

Voci di accesso per installatori (livello di accesso 3)

- **Servizio Hik-ProConnect**
  Hik-ProConnect è un servizio per gli installatori che serve a gestire a distanza i sistemi di allarme dei clienti situati in vari siti. Le centrali possono essere aggiunte a un account installatore sul servizio Hik-ProConnect ed essere gestite nei siti.

- **Client web locale**
  Visitate l'indirizzo IP del dispositivo che può essere scoperto con lo strumento SADP. L'installatore può accedere con l'account di servizio Hik-ProConnect dopo che il pannello è stato aggiunto.
- **Voci dell'eredità**
  I PIN della tastiera e i tag possono essere assegnati anche con l'utente installatore a un particolare livello di accesso per

eseguire operazioni essenziali.

Voci di accesso per l'amministratore e gli operatori (livello di accesso 2)

- **Servizio Hik-Connect**
  Il servizio Hik-Connect può essere utilizzato dagli utenti finali per accedere e gestire i dispositivi.
- **Web Client locale (per l'amministratore)**
  Non appena il pannello è stato aggiunto all'account dell'utente finale su Hik-Connect Service, l'account Hik- Connect può essere utilizzato per accedere al web client build in.

  Gli operatori non possono accedere al client web.
- **Voci dell'eredità**
  I PIN della tastiera e i tag possono essere assegnati anche all'utente finale a un particolare livello di accesso per eseguire operazioni essenziali.

Capitolo 4 Configurazione

4.1. Configurazione con Hik-Proconnect

4.1.1 Utilizzare l'APP Hik-Proconnect

L'installatore può usare Hik-Proconnect per configurare l'AX PRO, come l'attivazione, l'iscrizione del dispositivo ecc.

Scaricare e accedere a Hik-ProConnect

Scaricare il client mobile Hik-ProConnect e fare il login nel client prima di mettere in funzione l'AX PRO.

Passi

1. Scarica il client mobile di Hik-ProConnect.
2. Opzionale: Registra un nuovo account se è la prima volta che usi il client mobile Hik-ProConnect.

Nota

- Per i dettagli, vedere il *manuale utente di Hik-ProConnect Mobile Client*.
- Hai bisogno di un codice d'invito per la registrazione. Si prega di chiedere al supporto tecnico.

3. Esegui e accedi al client.

Aggiungere AX PRO al client mobile

Aggiungere AX PRO al client mobile prima di altre operazioni.

Passi

1. Accendere l'AX PRO.
2. Crea o cerca un sito.
   – Tocca **+**, imposta il nome del sito, il fuso orario, l'indirizzo, la città, lo stato/provincia/regione e tocca **OK** per creare un sito.
   – Inserisci il nome del sito nell'area di ricerca e tocca l'**icona Cerca** per cercare un sito.
3. Toccare **Aggiungi dispositivo**.
   – Toccare **Scan QR Code** per accedere alla pagina Scan QR code. Scansiona il codice QR sull'AX PRO.

   Nota

   Normalmente, il codice QR è stampato sull'etichetta incollata sul coperchio posteriore dell'AX PRO.

Toccare **Aggiunta manuale** per accedere alla pagina Aggiungi dispositivo. Inserisci il numero di serie del dispositivo e il codice di verifica per aggiungere il dispositivo.

4. Attivare il **dispositivo**.

Aggiungere una **periferica all'AX**

PRO Aggiungere una periferica

all'AX PRO. **Passi**

1. Seleziona un sito.
2. Selezionare un dispositivo di controllo (AX PRO).
3. Tocca l'icona **+.**
   - Tocca **Scan QR Code** per entrare nella pagina Scan QR code. Scansiona il codice QR sulla periferica.
   - Toccare **Aggiunta manuale** per accedere alla pagina Aggiungi dispositivo. Inserisci il numero di serie del dispositivo e il codice di verifica per aggiungere il dispositivo.

Gestione degli utenti

Gli installatori (utente di Hik-ProConnect) possono gestire gli utenti. Se sei l'amministratore, puoi aggiungere, modificare e cancellare gli utenti, e assegnare diversi permessi ai nuovi utenti aggiunti.

Passi

Nota

Ci sono quattro tipi di utenti per AX PRO, tra cui amministratore (o proprietario), operatore e installatore (o setter). I diversi tipi di utenti hanno diversi permessi per accedere alle funzionalità dell'AX PRO.

1. Entrare nel sito, toccare l'AX PRO e quindi accedere al dispositivo (se richiesto) per entrare nella pagina AX PRO.
2. Tocca **Avanti** per invitare l'utente.

Nota

Il destinatario deve accettare l'invito.

3. Toccare → **Gestione utenti** → **Utente**.
4. Tocca un utente per entrare nella pagina di gestione degli utenti.
5. Opzionale: Eseguire le seguenti operazioni, se necessario.

Autorizzazione dell'utente	Si può toccare l'utente di destinazione nell'elenco degli utenti e poi toccare **Edit Icon** per impostare i permessi autorizzati all'utente di destinazione. **Nota** Solo l'amministratore può fare una tale operazione.
Impostare le aree collegate	Se l'utente di destinazione è un operatore, toccare l'utente di destinazione nell'elenco utenti e poi toccare **Aree collegate** per impostare l'area collegata all'utente di destinazione.

Nota

Solo l'amministratore può fare una tale operazione.

Modifica della password della tastiera Se l'utente di destinazione è un amministratore, un installatore o un operatore, si può toccare l'utente di destinazione nell'elenco utenti e poi toccare **Modifica password tastiera** per impostare la password della tastiera all'utente di destinazione.

Modifica della password di coercizione Se l'utente di destinazione è un amministratore o un operatore, si può toccare l'utente di destinazione nell'elenco utenti e poi toccare **Modifica password di coercizione** per impostare la

Nota

password di coercizione all'utente di destinazione.

In caso di costrizione, è possibile inserire il codice di costrizione sulla tastiera per armare e disarmare la/e zona/e e caricare un allarme di costrizione.

Controllo dell'automazione Un amministratore, un installatore o un operatore può controllare il modulo relè, l'interruttore a muro e la spina intelligente.

Nota

- Gli elementi di configurazione e i permessi degli utenti variano a seconda del tipo di utente.
- Puoi visualizzare le carte/etichette e i portachiavi collegati dell'utente, ma non hai il permesso di configurarli.

Gestione delle carte/dei tag

Dopo aver aggiunto carte/etichette all'AX PRO wireless, è possibile passare la carta/etichetta per armare o disarmare tutti i rivelatori aggiunti a specifiche aree dell'AX PRO, e silenziare gli allarmi.

Nota

L'ID/PIN del tag è un intero di 32 bit, e la variante potrebbe essere 42949672956.

Passi

1. Entra nel sito, tocca l'AX PRO e poi accedi al dispositivo (se richiesto) per entrare nella pagina.
2. Tocca → **Gestione utente** → **Scheda/Tag** per entrare nella pagina di gestione dei tag.
3. Tocca **+** per aggiungere un tag.
4. Quando si sente la richiesta vocale "Swipe Tag", si deve presentare il tag sull'area di presentazione del tag AX PRO.
   - Quando si sente un bip, il Tag viene riconosciuto.

- Il tag verrà visualizzato nella pagina dei tag.

5. Opzionale: Tocca un tag per entrare nella pagina delle impostazioni.
6. Tocca l'**icona Edit** per modificare il nome del tag.

Nota

- Se accedi come installatore, salta questo passaggio. La modifica del nome del tag è disponibile solo per l'amministratore.
- Il nome deve contenere da 1 a 32 caratteri.

7. **Abilitare il Tag...**
8. Seleziona un utente collegato.
9. Selezionare il tipo di Tag

Nota

Diversi utenti collegati hanno diversi permessi di Tag.

Operazione Tag

Puoi far scorrere il Tag per armare o disarmare.

Etichetta di pattuglia

Quando si striscia il Tag, il sistema caricherà un record.

10. Opzionale: Tocca **Elimina** per cancellare il tag.

Impostazioni di

sistema

Configurazione del

sistema

È possibile impostare il fuso orario del dispositivo e impostare l'ora legale.

Nel sito, toccare l'AX PRO e poi accedere al dispositivo (se richiesto).

Toccare → **Sistema** → **Configurazione** per entrare nella pagina di

configurazione. Si può toccare per selezionare un fuso orario.

È possibile abilitare il DST e impostare la distorsione DST, l'ora di inizio DST e l'ora di fine DST.

Opzioni del sistema

Impostare le opzioni di sistema.

Gestione delle opzioni

Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se richiesto). Tocca → **Sistema** → **Sistema**

Opzioni → **Gestione sistema** per entrare nella pagina.

Braccio automatico forzato

Se l'opzione è abilitata e ci sono guasti attivi in una zona, la zona sarà bypassata automaticamente.

Rapporto sullo stato del sistema

Interruttore per il caricamento dei rapporti di sistema.

Prompt vocale

Se l'opzione è attivata, l'AX PRO abiliterà la richiesta vocale di testo.

Allarme anti-manomissione udibile

Se l'opzione è abilitata, il sistema avviserà con un buzzer l'allarme di manomissione.
Se l'opzione è disabilitata, le periferiche riporteranno il coperchio aperto, ma non si collegheranno agli allarmi.

Volume del sistema

L'intervallo di volume del sistema disponibile va da 0 a 10.

Pulsante di blocco del pannello

Se l'opzione è attivata, l'installatore può utilizzare la funzione del pulsante di blocco per bloccare AX PRO. Dopo il blocco, gli utenti non possono utilizzare il dispositivo e ricevere messaggi.

Durata dell'allarme del pannello

Impostare la durata temporale degli allarmi del pannello.

Tempi di perdita dei sondaggi

Impostare la durata massima della perdita di polling. Il sistema segnalerà un errore se la durata è superiore al limite.

Bypass su Re-Arm

La zona bypassata tornerà ad armare se il guasto viene ripristinato.

Controllo dei guasti

Nel sito, toccare l'AX PRO. Toccare → **Sistema** → **Opzioni di sistema** → **Controllo guasti pannello** per entrare nella pagina.

Rileva la disconnessione della telecamera di rete

Se l'opzione è attivata, quando la telecamera di rete collegata viene scollegata, viene attivato un allarme.

Controllo del guasto della batteria

Se l'opzione è attivata, quando la batteria è scollegata o scarica, il dispositivo non caricherà gli eventi.

Controllo guasti LAN

Se l'opzione è abilitata, quando la rete cablata è scollegata o con altri guasti, l'allarme scatta.

Controllo del guasto Wi-Fi

Se l'opzione è abilitata, quando il Wi-Fi è scollegato o con altri guasti, l'allarme verrà attivato.

Controllo dei guasti della rete cellulare

Se l'opzione è attivata, quando la rete dati cellulare è scollegata o con altri guasti, l'allarme verrà attivato.

Tempo di controllo di spegnimento AC

Il sistema controlla il guasto dopo la durata di tempo configurata dopo lo spegnimento della corrente. Per soddisfare la norma EN 50131-3, la durata del tempo di controllo dovrebbe essere di 10 s.

Istruzioni di sistema

Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se richiesto). Toccare → **Sistema** → **Opzioni di sistema** → **Istruzioni di sistema** per entrare nella pagina.

Braccio con errore

Se l'opzione è abilitata, quando c'è un errore durante la procedura di armamento, è possibile interrompere l'armamento manualmente.

Lista di controllo

Il sistema controllerà se il dispositivo ha i difetti nella lista di controllo durante la procedura di armamento.

Braccio con lista di controllo dei guasti

Controllare i guasti nell'elenco Fault Check, e il dispositivo non interromperà la procedura di armamento quando si verificano dei guasti.

Il LED del braccio rimane acceso

Se il dispositivo applica lo standard EN, per impostazione predefinita, la funzione è disabilitata. In questo caso, se il dispositivo è armato, il LED sarà blu fisso per 5 s. E se il dispositivo è disarmato, il LED lampeggerà 5 volte. Quando la funzione è abilitata, se il dispositivo è armato, il LED sarà sempre acceso. E se il dispositivo è disarmato, il LED sarà spento.

Prompt di guasto all'armamento

Se il dispositivo applica lo standard EN, per default la funzione è disabilitata. In questo caso, il dispositivo non richiederà guasti durante la procedura di armamento.

Prompt di guasto al disarmo

Se il dispositivo applica lo standard EN, per impostazione predefinita, la funzione è disabilitata. In questo caso, l'apparecchio non segnalerà i guasti durante la procedura di disinserimento.

Allarme precoce

Se abilitate la funzione, quando la zona è armata e la zona è attivata, l'allarme scatterà dopo il tempo di ritardo.

Ora della sveglia presto

Quando la funzione di allarme anticipato è abilitata, è necessario impostare l'ora dell'allarme anticipato. L'allarme sarà

attivato dopo il tempo di allarme anticipato configurato.

Metodo di iscrizione

1. Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se necessario).
2. Toccare → **Sistema** → **Opzioni di sistema** → **Metodo di iscrizione** per entrare nella pagina.
3. Toccare **Enter the Enrollment Mode**.
4. Segui le istruzioni nella pagina per aggiungere un dispositivo.
5. Toccare **Esci dalla modalità di iscrizione**.

Telecamera di rete

Aggiungere telecamere all'AX PRO

Passi

1. Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se necessario).
2. Toccare → **IPC** → **Gestione IPC** per entrare nella pagina.
3. Tocca **Aggiungi**.
4. Inserisci l'indirizzo IP, la porta, il nome utente e la password della telecamera.
5. Tocca l'**icona Salva**.
6. Opzionale: tocca **Modifica** o **Elimina** per modificare o eliminare la telecamera selezionata.

Impostare i parametri video

Passi

1. Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se necessario).
2. Toccare → **IPC** → **Impostazioni video evento** per entrare nella pagina.
3. Seleziona una telecamera e imposta i parametri video.

Tipo di flusso

Flusso principale: Essendo usato nella registrazione e nell'anteprima HD, ha un'alta risoluzione, velocità di codifica e qualità dell'immagine.
Sub-Stream: È usato per trasmettere immagini di rete e in anteprima come uno streaming video con caratteristiche di risoluzione, bit rate e qualità dell'immagine inferiori.

Tipo di bitrate

Seleziona il tipo di bitrate come costante o variabile.

Risoluzione

Seleziona la risoluzione dell'uscita video.

Bitrate video

Il valore più alto corrisponde alla maggiore qualità video, ma è richiesta una migliore larghezza di banda.

Impostare il programma di attivazione/disattivazione

1. Impostare il programma di attivazione/disattivazione per armare/disarmare automaticamente una particolare zona.
2. Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se necessario).
3. Toccare → Area per entrare nella pagina.
4. Tocca un'area nell'elenco, abilita l'area e seleziona le aree collegate.
5. Abilita la funzione auto arm/disarm e imposta il tempo di auto arm/ auto disarm. Puoi anche impostare il tempo di ritardo al disarmo, il tempo di ritardo all'entrata, il tempo di ritardo all'uscita, il tempo di ritardo del segnalatore acustico, l'eccezione per il fine settimana e il giorno festivo escluso.

Braccio automatico

Abilita l'area ad armarsi automaticamente in un punto temporale specifico.

Tempo del braccio automatico

Impostare il programma per l'armamento automatico dell'area.

Disarmo automatico

Abilita l'area a disarmarsi automaticamente in un determinato momento.

Tempo di disarmo automatico

Impostare l'orario in cui l'area si disarma automaticamente.

Tardivo al disarmo

Abilita il dispositivo a inviare una notifica al telefono o al tablet per ricordare all'utente di disarmare l'area quando questa è ancora armata dopo un determinato periodo di tempo.

Nota

È necessario abilitare la funzione di notifica della gestione del pannello sul Web Client di **Parametri di comunicazione** → **Comunicazione degli eventi** prima di abilitare la funzione di ritardo nel disinserimento.

Tempo di ritardo al disarmo

Impostare il punto di tempo menzionato in **Late to Disarm**.

Eccezione di fine settimana

Se abilitato, **Auto Arm**, **Auto Disarm**, e **Late to Disarm** sono disabilitati nel weekend.

Ferie escluse

Abilitare la funzione e la zona non sarà armata/disarmata durante le vacanze. Si dovrebbe impostare il programma delle vacanze dopo l'abilitazione.

Nota

Si possono impostare fino a 6 gruppi di vacanze.

Comunicazione

Rete dati cellulare

Inserisci qui una breve descrizione del tuo compito (opzionale).

Passi

1. Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se necessario).
2. Toccare → **Parametri di comunicazione→ Impostazioni rete dati cellulare** per entrare nella pagina.
3. Abilita la **rete mobile**.
4. Toccare **Parameter Configuration** → **Edit Icon** e impostare i parametri tra cui il nome utente, la password di accesso, APN, MTU e PIN conde.
5. Tocca l'**icona Salva**.
6. Abilita **il limite di utilizzo dei dati**.
7. Modifica i **dati utilizzati questo mese** e i **dati limitati al mese**.

Notifiche push

Quando scatta un allarme, se si desidera inviare la notifica di allarme al telefono cellulare, è possibile impostare i parametri di push della notifica.

Passi

1. Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se necessario).
2. Toccare → **Parametri di comunicazione→ Notifica(e) push** per entrare nella pagina.
3. Tocca **Phone Call** e **SMS**.
4. Tocca **+** o **+ Aggiungi numero di telefono** per inserire il numero di telefono.
5. Tocca il numero di telefono aggiunto per attivare **Phone Call** e **SMS** secondo le tue esigenze.
6. (Per la telefonata) Impostare i **numeri di chiamata**.
7. (Per SMS) Impostare il **permesso di armare**, il **permesso di disarmare** e il **permesso di cancellare l'allarme** per le aree.
8. Controllare le notifiche.

Allarme di zona/segnalazione del coperchio

Il dispositivo invierà delle notifiche quando l'allarme della zona viene attivato o il coperchio della zona aperta viene attivato o ripristinato.

Nota

È necessario impostare l'intervallo di tempo di filtraggio degli eventi per le chiamate telefoniche.

Periferiche Coperchio aperto

Il dispositivo spingerà le notifiche quando il coperchio aperto di qualsiasi periferica viene attivato o ripristinato.

Coperchio del pannello aperto

Il dispositivo spingerà le notifiche quando il coperchio aperto del pannello di controllo viene attivato o ripristinato.

Allarme antipanico

Il dispositivo invierà notifiche quando l'allarme antipanico viene attivato o ripristinato da zone, tastiere o portachiavi.

Allarme medico

Il dispositivo spinge le notifiche quando scatta l'allarme medico.

Allarme gas

Il dispositivo invierà delle notifiche quando scatta l'allarme gas.

Stato del pannello

Il dispositivo invierà delle notifiche quando lo stato del sistema del pannello di controllo viene modificato

Stato della zona

Il dispositivo invierà delle notifiche quando lo stato della zona viene cambiato.

Stato delle periferiche

Il dispositivo invierà delle notifiche quando qualsiasi stato della periferica viene cambiato.

Funzionamento del pannello

Il dispositivo spinge le notifiche quando l'utente aziona l'AX PRO.

Notifica di allarme intelligente

Il dispositivo spingerà le notifiche quando l'allarme viene attivato nelle telecamere termiche.

Centro di ricezione allarmi (ARC)

È possibile impostare i parametri del centro di ricezione allarmi e tutti gli allarmi saranno inviati al centro allarmi configurato.

Passi

1. Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se necessario).
2. Toccare → **Parametri di comunicazione→ Centro di ricezione allarmi (ARC)** per entrare nella pagina.
3. Selezionate un ARC e abilitatelo.
4. Selezionare il **tipo di protocollo** come **ADM-CID**, **ISUP**, **SIA-DCS**, ***SIA-DCS**, o ***ADM-CID** per impostare la modalità di caricamento.

   ADM-CID o **SIA-DCS**

   Dovreste selezionare il **tipo di indirizzo** come **IP** o **nome di dominio**, e inserire l'IP/nome di dominio, il numero di porta, il codice dell'account, la modalità di trasmissione, il periodo di timeout dei tentativi, i tentativi, l'opzione di polling e il periodo di test.

   Nota

   Impostare l'intervallo di test del periodo con la gamma da 10 secondi a 24 ore.

   ISUP

   Non è necessario impostare i parametri del protocollo ISUP.

   ***SIA-DCS** o ***ADM-CID**

   Dovresti selezionare il **tipo di indirizzo** come **IP** o **nome di dominio**, e inserire l'IP/nome di dominio,

numero di porta, codice account, modalità di trasmissione, periodo di timeout per i tentativi, opzione di polling, aritmetica di crittografia, lunghezza della password, chiave segreta e test di

Nota

periodo.

Impostare l'intervallo di test del periodo con la gamma da 10 secondi a 24 ore.

Per la crittografia aritmetica: Il formato di crittografia di sostegno del pannello per la sicurezza delle informazioni secondo DC-09, AES-128, AES-192 e AES-256 sono supportati quando si configura il centro di allarme.

Per la chiave segreta: Quando si usa un formato criptato di DC-09, una chiave dovrebbe essere impostata quando si configura l'ARC. La chiave verrebbe emessa offline dall'ARC, che verrebbe usata per criptare il messaggio per la sicurezza della sostituzione.

Manutenzione del

dispositivo È possibile

riavviare il dispositivo.

Passi

1. Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se necessario).
2. Toccare →Manutenzione→ **Manutenzione del dispositivo** per entrare nella pagina.
3. Tocca **Test** e tocca **Start Walk Test** per verificare se il dispositivo funziona correttamente o meno.
3. Toccare **Manutenzione** → **Riavvia dispositivo** . L'AX PRO si riavvierà.

Gestione dei dispositivi

Inserisci qui una breve descrizione del tuo concetto

(opzionale). Questo è l'inizio del tuo concetto.

Zona

Puoi impostare i parametri della zona nella pagina della zona.

Passi

1. Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se necessario).
2. Tocca una zona nella scheda **Dispositivo.**
3. Rubinetto .
4. Tocca **Modifica Icona** il nome della zona.
5. Seleziona un tipo di zona.

Zona istantanea

Questo tipo di zona attiverà immediatamente un evento di allarme quando viene armata.

Zona ritardata

Ritardo di uscita: Exit Delay fornisce il tempo per lasciare attraverso l'area di difesa senza allarme. Ritardo di entrata: Entry Delay ti dà il tempo di entrare nell'area di difesa per disarmare il sistema

senza allarme.
Il sistema dà il tempo di ritardo di entrata/uscita quando è armato o rientrato. Di solito è usato nel percorso di entrata/uscita (per esempio porta principale/ingresso principale), che è un percorso chiave per armare/disarmare tramite tastiera operativa per gli utenti.

Nota

È possibile impostare 2 diverse durate di tempo in **Opzioni sistema → Programma e timer.** Assicurarsi che il timer non sia più lungo di 45 secondi per rispettare la norma EN50131-1. Se la zona è una zona ritardata, è possibile impostare i parametri di ritardo di entrata/ritardo di uscita.

Seguire la zona

La zona agisce come zona ritardata quando rileva l'evento di attivazione durante il ritardo di entrata del sistema, mentre altrimenti agisce come zona istantanea.

Zona di panico silenzioso 24h

Questo tipo di zona è attivo 24 ore, è usato per Panic o HUD (Hold Up Devices) non per sensori di fumo o rivelatori di rottura vetro.

Zona di panico

La zona si attiva tutto il tempo. Di solito viene utilizzata nei siti dotati di pulsante antipanico, rilevatore di fumo e rilevatore di rottura vetri.

Zona del fuoco

La zona si attiva tutto il tempo con uscita sonora/sonora quando si verifica l'allarme. Di solito viene utilizzata in aree a rischio d'incendio dotate di rilevatori di fumo e sensori di temperatura.

Zona gas

La zona si attiva tutto il tempo con l'uscita del suono/suono quando si verifica l'allarme. Si usa di solito in zone dotate di rilevatori di gas (per esempio, la cucina).

Zona medica

La zona si attiva tutto il tempo con conferma di bip quando si verifica l'allarme. Di solito viene utilizzata in luoghi dotati di pulsanti di emergenza medica.

Zona di timeout

La zona è sempre attiva. Il tipo di zona è usato per monitorare e segnalare lo stato "ATTIVO" di una zona, ma segnalerà e allarmerà questo stato solo dopo la scadenza del tempo programmato. (da 1 a 599) secondi. Può essere utilizzato in luoghi dotati di contatti magnetici che richiedono l'accesso ma solo per un breve periodo (ad esempio, la porta della cassetta dell'idrante o un'altra porta della cassetta di sicurezza esterna)

Zona chiave

L'area collegata si attiverà dopo essere stata attivata e si disattiverà dopo essere stata ripristinata. Nel caso dell'allarme di manomissione, l'operazione di inserimento e disinserimento non verrà attivata.

Zona disabili

Zona disattivata ignorando qualsiasi evento di allarme. Di solito è usato per disabilitare i rivelatori difettosi.

6. Abilita **Stay Arm Bypass**, **Chime**, **Double Knock**, **Silent Alarm** e altre funzioni secondo le tue reali necessità.

Nota

- Alcune zone non supportano la funzione. Fare riferimento alla zona attuale per impostare la funzione.
- I diversi tipi di zona hanno parametri diversi.

7. Impostare il tasso di polling.
8. Opzionale: Tocca **Elimina** per cancellare il dispositivo.

Tastiera

È possibile impostare i parametri della tastiera iscritta all'AX PRO.

Passi

1. Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se necessario).
2. Tocca una tastiera nella scheda **Dispositivo.**
3. Rubinetto .
4. Tocca **Modifica Icona** il nome della tastiera.
5. Abilita **il Keyfob**.
6. Seleziona gli utenti collegati.
7. Tocca **Impostazioni tasti funzione** per impostare le funzioni per i tasti singoli e combinati.
8. Opzionale: Tocca **Elimina** per cancellare il dispositivo.

Sounder

La sirena è iscritta all'AX PRO tramite il modulo ricevitore wireless, e la sirena wireless 868 Mhz può essere iscritta all'ibrido AX PRO tramite il ricevitore wireless che si trova all'indirizzo 9.

Passi

1. Nel sito, tocca l'AX PRO e poi accedi al dispositivo (se necessario).
2. Tocca una sirena nella scheda **Dispositivo.**
3. Rubinetto .
4. Tocca **Modifica Icona** il nome dell'ecoscandaglio.
5. Seleziona le aree collegate.
6. Impostare il tempo di durata dell'allarme e il volume dell'allarme.
7. Abilitare il LED di attivazione/disattivazione, il cicalino di attivazione/disattivazione, l'indicatore di allarme secondo le esigenze reali.
8. Imposta il ciclo del battito cardiaco.
9. Opzionale: Tocca **Elimina** per cancellare il dispositivo.

4.1.2 Utente del portale Hik-ProConnect

Per il pannello di controllo di sicurezza AX Pro, è possibile eseguire operazioni tra cui armare/disarmare l'area, silenziare l'allarme, bypassare la zona ecc, e configurare a distanza il pannello di controllo sul portale. È anche possibile richiedere il PIN (necessario per l'aggiornamento del firmware di AX Pro) e cambiare la lingua di AX

Pro.

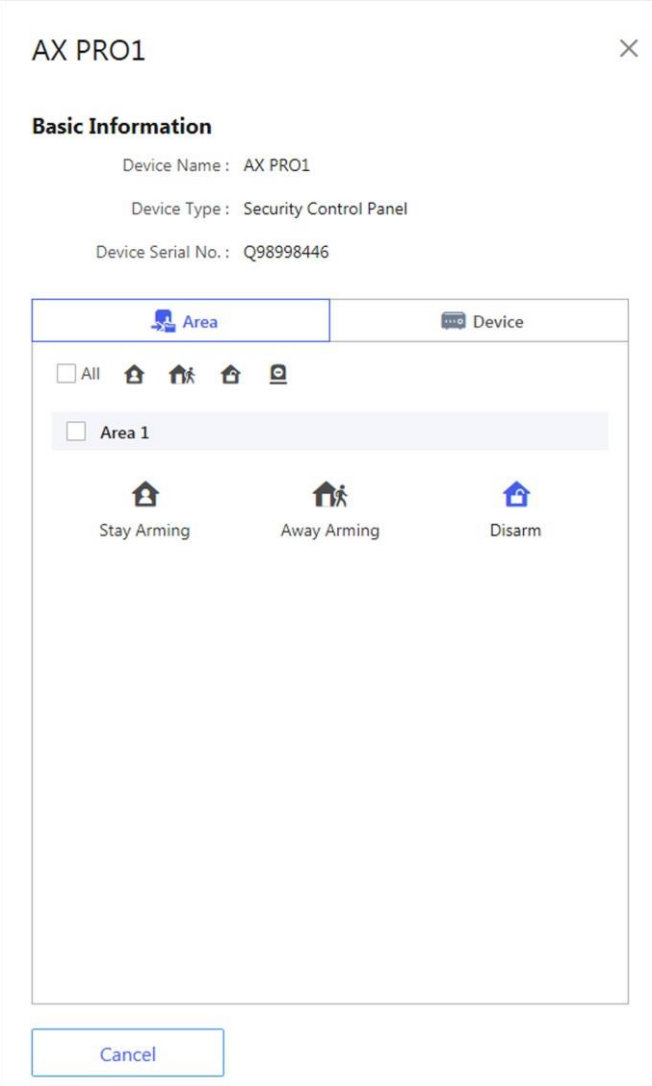
Clicca su **Sito** per entrare nella pagina dell'elenco dei siti, e poi clicca sul nome di un sito per entrare nella pagina dei dettagli del sito.

Comandare a distanza AX Pro

Cliccate su AX Pro per aprire il pannello delle operazioni. Ed è possibile eseguire le seguenti operazioni.

Tabella 4-3 Descrizione delle operazioni

Operazione	Descrizione
Rimanere in un'area specifica	Seleziona la scheda **Area** e poi clicca su **Stay Arming** per armare l'area.
Lontano armare un'area specifica	Selezionate la scheda **Area** e poi cliccate su **Away Arming**.
Disarmare un'area specifica	Seleziona la scheda **Area** e poi clicca su **Disarma**.
Soggiorno braccio multiplo	Selezionare la scheda **Area**, quindi selezionare le aree e fare clic su .
Braccio di allontanamento Aree multiple	Selezionare la scheda **Area**, quindi selezionare le aree e fare clic su
Disattivare aree multiple	Selezionare la scheda **Area**, quindi selezionare le aree e fare clic su .
Silenziare gli allarmi di più aree	Selezionare la scheda **Area,** quindi selezionare le aree e fare clic su
Filtrare il dispositivo periferico per area	Seleziona la scheda **Dispositivo e** then clickseleziona un'area per visualizzare solo le periferiche collegate all'area selezionata, oppure seleziona **Tutto** per visualizzare tutte le periferiche collegate a tutte le aree.
Relè di controllo	Seleziona la scheda **Dispositivo**, quindi seleziona un espansore di uscita wireless per visualizzare le sirene ad esso collegate, quindi seleziona la sirena o le sirene per attivarle/disattivarle.
Zona di bypass	Selezionare la scheda **Device (Dispositivo)**, quindi selezionare una zona (cioè un rilevatore) e attivare l'interruttore **Bypass** per bypassare la zona.



Configurare a distanza AX Pro

Puoi cliccare per entrare nella pagina web del pannello di controllo della sicurezza per configurare il dispositivo.

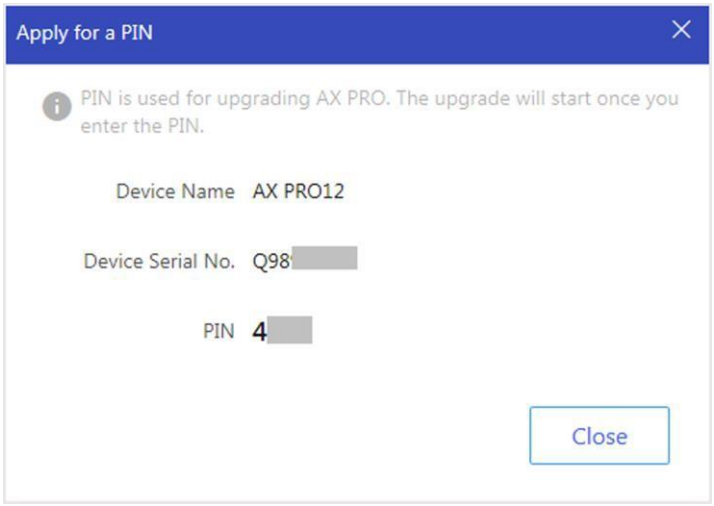
Nota

Per i dettagli sulla configurazione del pannello di controllo di sicurezza, vedere il manuale utente del dispositivo.

Richiedere un PIN

È possibile click → aprire la finestra Richiedi un PIN, e poi il codice PIN sarà

visualizzato.

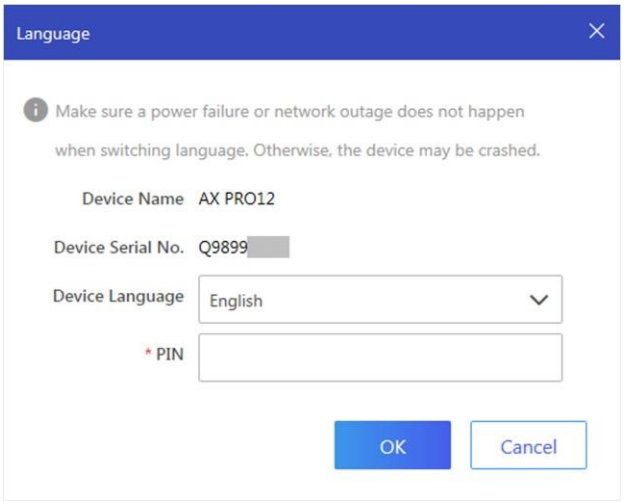


Cambia lingua

Nota

Avrebbe dovuto richiedere un PIN.

È possibile click • • → ⇆ aprire la finestra Lingua, quindi impostare la lingua del dispositivo e inserire il PIN.

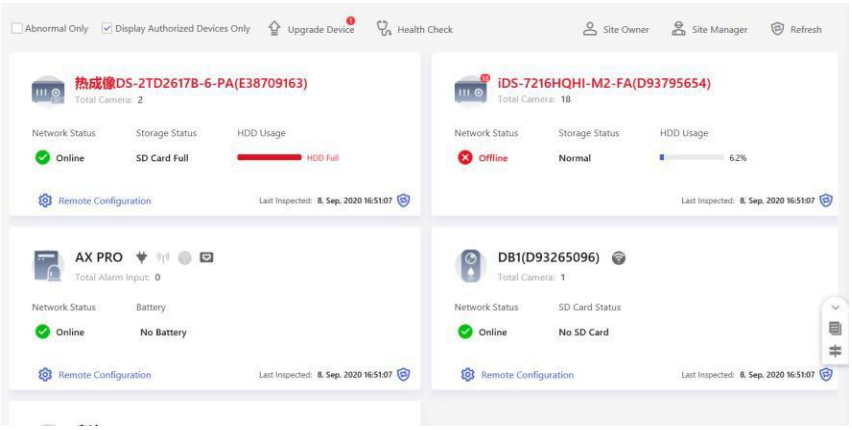


Monitoraggio della salute

1. Entrate nel sito web del portale Hik-ProConnect e cliccate su **Health Monitoring** → **Health Status** per entrare

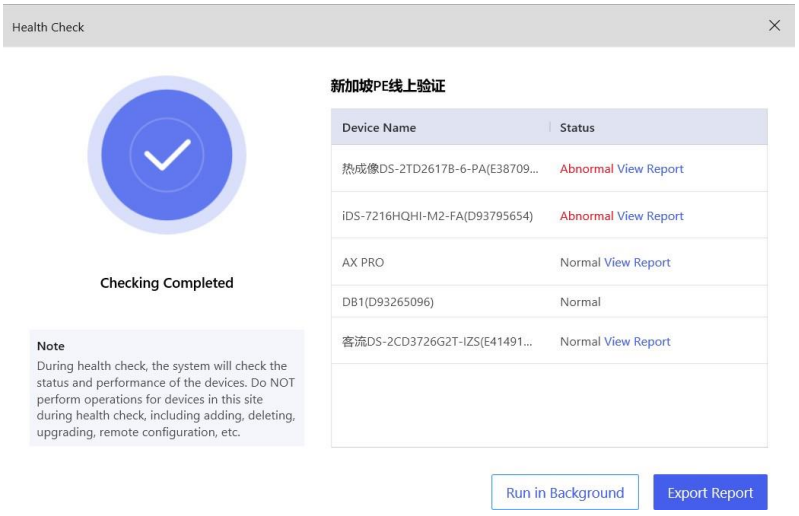
la pagina.

2. Seleziona un sito.



3. Clicca su **Health Check** e clicca su **Check Now**.

Quando il controllo è completato, è possibile visualizzare lo stato e i rapporti dei dispositivi. Puoi anche esportare il rapporto.



4. Clicca per ottenere lo stato più recente del dispositivo.

4.2 Configurazione con Hik-Connect

L'operatore può usare l'Hik-Connect per controllare il dispositivo, come il funzionamento generale di attivazione/disattivazione, la gestione degli utenti, ecc.

Scaricare e accedere al client mobile

Scaricate l'Hik-Connect mobile client e fate il login nel client prima di far funzionare l'AX PRO.

Passi

1. Scarica il client mobile di Hik-Connect.
2. Opzionale: Registra un nuovo account se è la prima volta che usi il client mobile Hik-Connect.

Nota

Per i dettagli, vedi il *Manuale utente di Hik-Connect Mobile Client*.

3. Esegui e accedi al client.

Aggiungere AX PRO al client mobile

Aggiungere un AX PRO al client mobile prima di altre operazioni.

Passi

1. Accendere l'AX PRO.
2. Selezionare il tipo di aggiunta.
   - Toccare **+** → **Scan QR Code** per accedere alla pagina Scan QR code. Scansiona il codice QR sull'AX PRO.

Nota

Normalmente, il codice QR è stampato sull'etichetta incollata sul coperchio posteriore dell'AX PRO.

Toccare **+** → **Manual Adding** per entrare nella pagina Add Device. Inserisci il numero di serie del dispositivo con il tipo di aggiunta di Hik- Connect Domain.

3. Tocca per cercare il dispositivo.
4. Tocca **Aggiungi** nella pagina dei risultati.
5. Inserisci il codice di verifica e tocca **OK**.
6. Dopo l'aggiunta completata, inserisci l'alias del dispositivo e tocca **Salva**.
7. Opzionale: Tap → **Elimina** per cancellare il dispositivo.
8. Opzionale: Tap → per modificare il nome del dispositivo.

Aggiungere una periferica all'AX PRO

Aggiungere una periferica all'AX PRO. **Passi**

1. Selezionare un dispositivo di controllo (AX PRO).
2. Toccare **+** .
   - Tocca **Scan QR Code** per entrare nella pagina Scan QR code. Scansiona il codice QR sulla periferica.
   - Toccare **Aggiunta manuale** per accedere alla pagina Aggiungi dispositivo. Inserisci il numero di serie del dispositivo e il codice di verifica per aggiungere il dispositivo.

Gestione delle carte/dei tag

Dopo aver aggiunto carte/etichette all'AX PRO wireless, è possibile passare la carta/etichetta per armare o disarmare tutti i rivelatori aggiunti a specifiche aree dell'AX PRO, e silenziare gli allarmi.

Passi

1. Nella pagina dell'elenco dei dispositivi, tocca l'AX PRO e poi accedi al dispositivo (se richiesto) per entrare nella pagina.
2. Toccare → **Gestione utente** → **Scheda/Tag** per entrare nella pagina.
3. Tocca **+** per aggiungere una carta/etichetta.
4. Quando si sente la richiesta vocale "Swipe Tag", si deve presentare la carta/tag sull'area di presentazione della carta/tag di AX PRO.
   - Quando si sente un bip, la carta/etichetta viene riconosciuta.
   - Il tag verrà visualizzato nella pagina della scheda/tag.
5. Opzionale: Tocca una carta/etichetta per entrare nella pagina delle impostazioni.
6. Tocca per modificare il nome del tag.

Nota

- Se accedi come installatore, salta questo passaggio. La modifica del nome del tag è disponibile solo per l'amministratore.
- Il nome deve contenere da 1 a 32 caratteri.

7. Far scorrere la **scheda/etichetta di abilitazione**.
8. Seleziona un utente collegato.
9. Seleziona il tipo di tag

Nota

Diversi utenti collegati hanno diversi permessi per i tag.

Operazione Tag

Puoi far scorrere il tag per armare o disarmare.

Etichetta di pattuglia

Quando si striscia il tag, il sistema caricherà un record.

10. Opzionale: Tocca **Elimina** per cancellare il tag.

Gestione degli utenti

L'amministratore e gli installatori possono gestire gli utenti. Se sei l'amministratore, puoi aggiungere,

modificare ed eliminare gli utenti, e assegnare diversi permessi ai nuovi utenti aggiunti.

Passi

Nota

Ci sono quattro tipi di utenti per AX PRO, tra cui amministratore (o proprietario), operatore e installatore (o setter). I diversi tipi di utenti hanno diversi permessi per accedere alle funzionalità dell'AX PRO.

1. Nella pagina dell'elenco dei dispositivi, tocca l'AX PRO e poi accedi al dispositivo (se richiesto) per entrare nella pagina AX PRO.
2. Toccare per entrare nella pagina del destinatario.
3. Seleziona un utente da invitare.
   – Scansione del codice QR per invitare un utente.
   – Inserisci l'indirizzo e-mail/numero di telefono cellulare per invitare un utente.
   – Seleziona un utente nell'elenco.
4. Tocca **Avanti** per invitare l'utente.

Nota

Il destinatario deve accettare l'invito.

5. Toccare → **Gestione utenti** → **Utente**.
6. Tocca un utente per entrare nella pagina di gestione degli utenti.
7. Opzionale: Eseguire le seguenti operazioni, se necessario.

Autorizzazione dell'utente	Si può toccare l'utente di destinazione nell'elenco degli utenti e poi toccare **Edit Icon** per impostare i permessi autorizzati all'utente di destinazione.
	Nota Solo l'amministratore può fare una tale operazione.
Impostare le aree collegate	Se l'utente di destinazione è un operatore, toccare l'utente di destinazione nell'elenco utenti e poi toccare **Aree collegate** per impostare l'area collegata all'utente di destinazione.
	Nota Solo l'amministratore può fare una tale operazione.
Modifica della password della tastiera	Se l'utente di destinazione è un amministratore, un installatore o un operatore, puoi toccare l'utente di destinazione nell'elenco degli utenti e poi toccare **Modifica tastiera Password** per impostare la password della tastiera per l'utente di destinazione.

Nota

La password (codice PIN) può essere da 4 a 6 cifre. Nessun numero è vietato, con 10.000 a 100.000 differenze, e nessun limite di combinazione di cifre.
Dopo aver aggiunto una tastiera, è possibile aggiungere il codice PIN (Keypad Password) nel menu utente. Quando si fa clic nella casella di input, ci sarà l'indicazione mostra che 4 a 6 numeri consentiti. Questo è lo stesso per ogni utente

Modifica della password di coercizione Se l'utente di destinazione è un amministratore o un operatore, si può toccare l'utente di destinazione nell'elenco utenti e poi toccare **Modifica password di coercizione** per impostare la

Nota

password di coercizione all'utente di destinazione.
In caso di costrizione, è possibile inserire il codice di costrizione sulla tastiera per armare e disarmare la/e zona/e e caricare un allarme di costrizione.

Controllo dell'automazione Un amministratore, un installatore o un operatore può controllare il modulo relè, l'interruttore a muro e la spina intelligente.

Nota

- Gli elementi di configurazione e i permessi degli utenti variano a seconda del tipo di utente.
- Puoi visualizzare i tag collegati e i portachiavi dell'utente ma non hai il permesso di configurarli.

8. Opzionale: (Solo per l'amministratore) Clicca su **+** per aggiungere un utente.

Zona di bypass

Quando l'area è armata, è possibile bypassare una zona particolare come desiderato.

Prima di iniziare

Collegare un rilevatore alla zona.

Passi

1. Nella pagina dell'elenco dei dispositivi, tocca l'AX PRO e poi accedi al dispositivo (se richiesto) per entrare nella pagina Area.
2. **Dispositivo** Tap.
3. Tocca una zona nella scheda Dispositivo.
4. Toccare per entrare nella pagina delle impostazioni.
5. Abilita il **bypass** e la zona sarà nello stato di bypass.

Il rilevatore della zona non rileva nulla e non si riceve alcun allarme dalla zona.

Armare/Disarmare l'area

Armare o disarmare l'area manualmente come si desidera.
Nella pagina dell'elenco dei dispositivi, tocca l'AX PRO e poi accedi al dispositivo (se richiesto) per entrare nella pagina Area.

Operazioni per una singola area

- **Armare a distanza**: Tocca qualsiasi zona per armare a distanza una singola area. Quando tutte le persone nell'area di rilevamento se ne vanno, attiva la modalità Away per armare tutte le zone dell'area dopo il tempo di permanenza definito.
- **Disarmare**: Tocca l'**icona Away Arming** in qualsiasi area per disarmare una singola zona. In modalità Disarmare, tutte le zone nell'area non attiveranno l'allarme, indipendentemente dal fatto che si verifichino o meno eventi di allarme.

Operazioni per tutte le aree

- **Via**: Tocca per armare via tutte le zone. Quando tutte le persone nell'area di rilevamento se ne vanno, attiva la modalità Away per armare tutte le zone in tutte le aree dopo il tempo di permanenza definito.
- **Resta**: Toccare per armare tutte le zone. Quando le persone rimangono all'interno dell'area di rilevamento, attivare la modalità Stay per armare tutti i rilevatori di effrazione perimetrali (come il rilevatore perimetrale, i contatti magnetici, il rilevatore a tenda nel balcone) impostati in tutte le zone di tutte le aree. Nel frattempo, i rivelatori all'interno dell'area di rilevamento sono bypassati (come i rivelatori PIR). Le persone possono muoversi all'interno dell'area e l'allarme non verrà attivato.
- **Disattivare**: Toccare per disarmare tutte le zone. In modalità Disarmare, tutte le zone di tutte le aree non attiveranno l'allarme, non importa se si verificano eventi di allarme o meno.
- **Silenzio allarme**: Tocca per silenziare gli allarmi di tutte le zone. Cancella tutti gli allarmi attivati da tutte le zone di tutte le aree.

Controllare la notifica dell'allarme

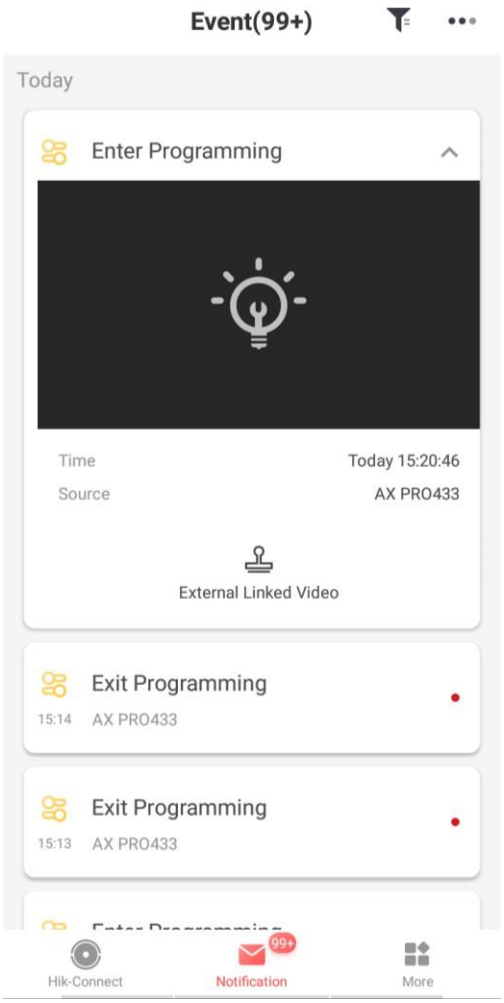
Quando scatta un allarme, riceverai una notifica di allarme. Puoi controllare le informazioni dell'allarme dal client mobile.

Prima di iniziare

- Assicuratevi di aver collegato una zona con un rilevatore.
- Assicuratevi che la zona non sia bypassata.
- Assicuratevi di non aver abilitato la funzione zona silenziosa.

Passi

1. Tocca **Notifica** nel client mobile per entrare nella pagina. Tutte le notifiche di allarme sono elencate nella pagina delle notifiche.
2. Seleziona un allarme e puoi visualizzare i dettagli dell'allarme.



3. Opzionale: se la zona ha collegato una telecamera, è possibile visualizzare la riproduzione quando l'allarme viene attivato.
4. Opzionale: Tocca per cercare eventi per date o dispositivi.

Connessione Wi-Fi

È possibile far connettere l'AX PRO al Wi-Fi tramite APP.

Passi

1. Nella pagina dell'elenco dei dispositivi, tocca l'AX PRO e poi accedi al dispositivo (se richiesto) per entrare nella pagina.
2. Tocca → **Configura rete Wi-Fi**.
3. Segui le istruzioni sulla pagina e cambia l'AX PRO in modalità AP. Tocca **Avanti**.
4. Seleziona un Wi-Fi stabile per la connessione del dispositivo.
5. Torna alla pagina di configurazione per inserire la password Wi-Fi e tocca **Next**.
6. Tocca **Connetti a una rete** e aspetta la connessione.

Al termine della connessione, l'AX PRO chiederà di uscire dalla modalità AP e passerà automaticamente alla modalità STA.

Manutenzione del dispositivo

È possibile riavviare il dispositivo.

Passi

1. Nella pagina dell'elenco dei dispositivi, tocca l'AX PRO e poi accedi al dispositivo (se richiesto) per inserire il pagina.
2. Toccare → **Manutenzione** → **Riavviare il dispositivo**. L'AX PRO si riavvierà.

4.3 Configurazione con il Web Client

Passi

1. Collegare il dispositivo all'Ethernet.
2. Cerca l'indirizzo IP del dispositivo tramite il software client e il software SADP.
3. Inserisci l'indirizzo IP cercato nella barra degli indirizzi.

Nota

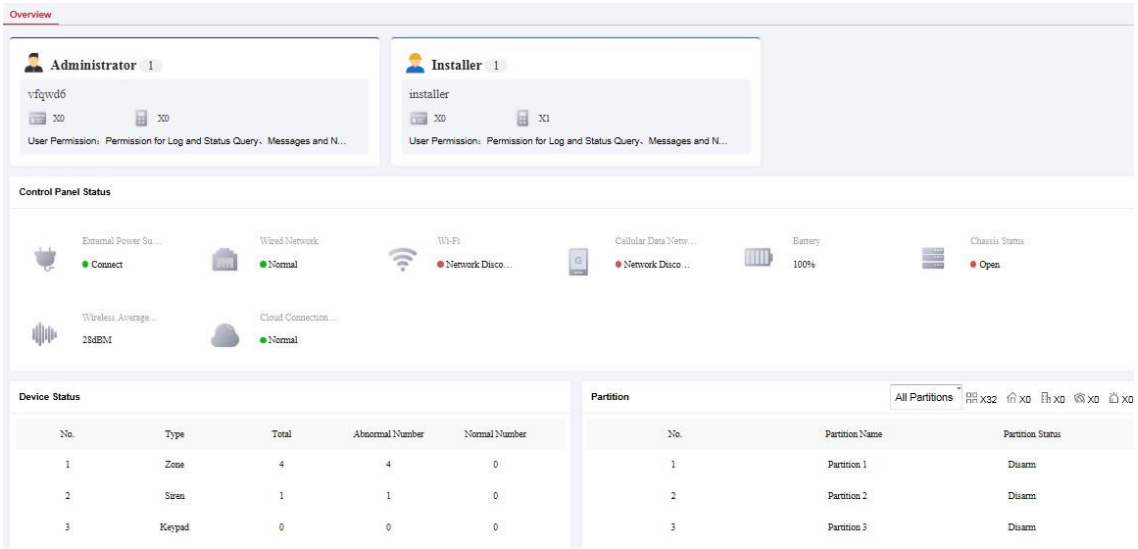
- Quando si usa il browser mobile, l'indirizzo IP di default è 192.168.8.1.
- Quando si collega il cavo di rete con il computer direttamente, l'indirizzo IP predefinito è 192.0.0.64.

4. Usa il nome utente e la password di attivazione per accedere.

Nota

- Fate riferimento al capitolo *Attivazione* per i dettagli.
- Solo l'amministratore e l'installatore possono accedere al client web.

È possibile visualizzare lo stato dell'utente, del dispositivo e dell'area nella pagina di panoramica.



4.3.1 Impostazioni di comunicazione

Rete cablata

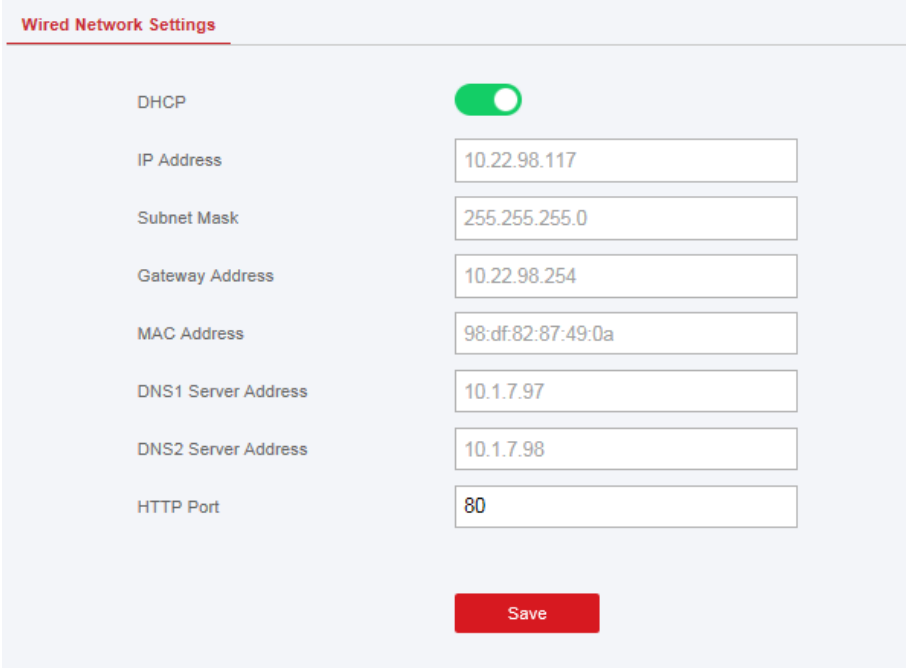
È possibile impostare l'indirizzo IP del dispositivo e altri parametri di rete.

Passi

Nota

Le funzioni variano a seconda del modello del dispositivo.

1. Nel software client, selezionare il dispositivo nella pagina **Device Management** e fare clic su , o inserire l'indirizzo IP del radar nella barra degli indirizzi del browser web e accedere.



2. Cliccare su **Communication Parameters** → **Ethernet** per entrare nella pagina.
3. Impostare i parametri.

Impostazioni automatiche: Abilita **DHCP** e imposta la porta HTTP.Impostazioni manuali: Disabilita **DHCP** e imposta **indirizzo IP**, **Subnet Mask**, **indirizzo Gateway**, **indirizzo del server DNS**.

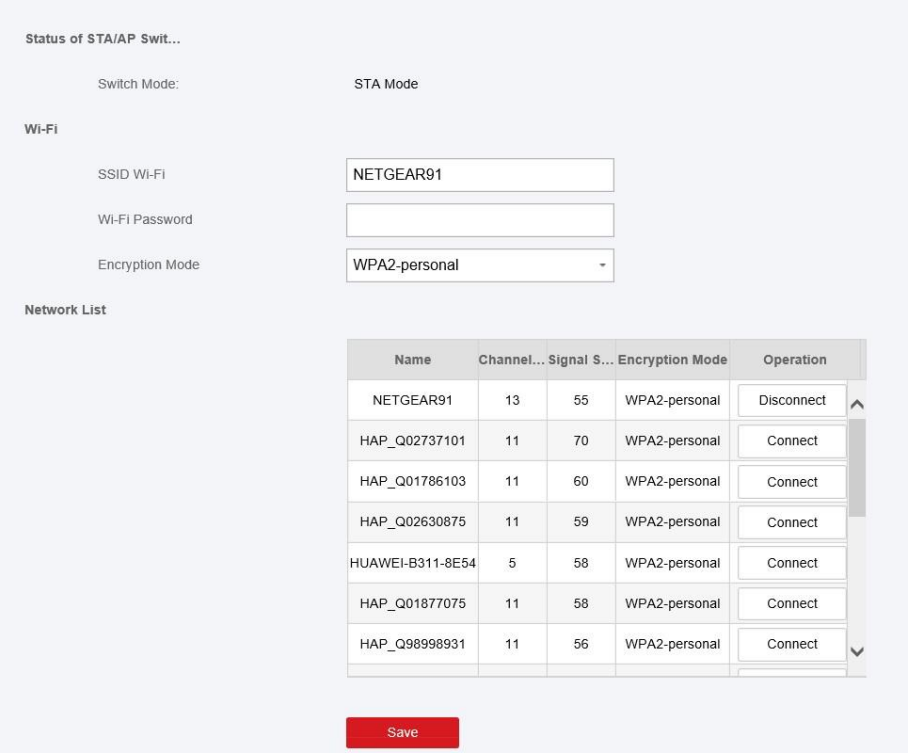
4. Opzionale: Impostare l'indirizzo corretto del server DNS se il dispositivo deve visitare il server Hik-Connect tramite un nome di dominio.
5. Fare clic su **Salva**.

Wi-Fi

È possibile impostare i parametri Wi-Fi se ci sono reti Wi-Fi sicure e credibili nelle vicinanze.

Passi

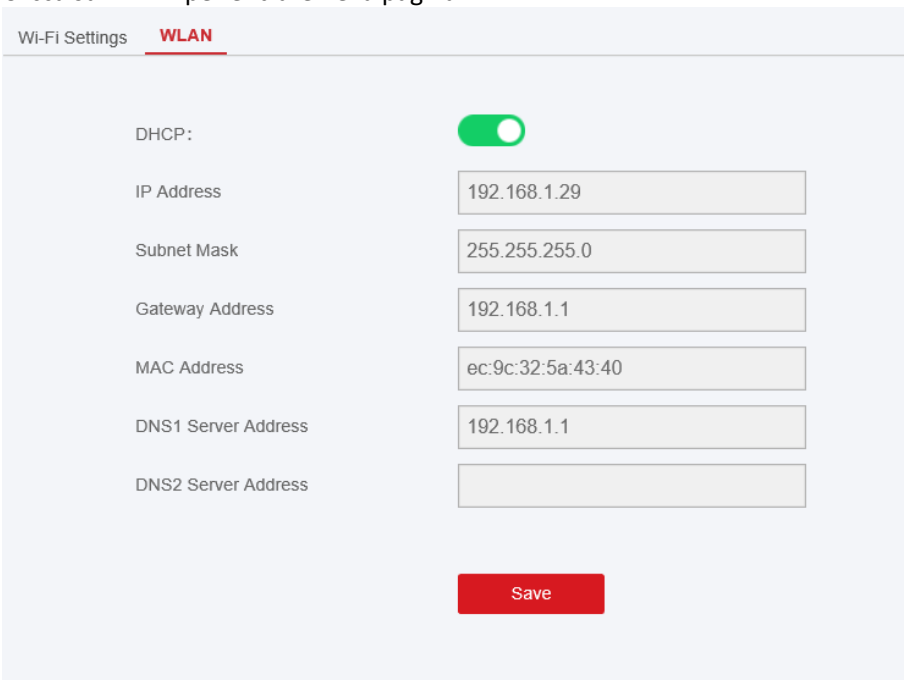
1. Clicca su **Parametri di comunicazione** → **Wi-Fi** per entrare nella pagina Wi-Fi.



2. Connettiti a un Wi-Fi.

Connettersi manualmente: Inserisci l'**SSID Wi-Fi** e la **password Wi-Fi**, seleziona la **modalità di crittografia** e clicca su **Save**.Select from Network List: Seleziona un Wi-Fi di destinazione dall'elenco delle reti. Fare clic su **Connect** e inserire la password Wi-Fi e fare clic su **Connect**.

2. Clicca su **WLAN** per entrare nella pagina WLAN.



4. Imposta l'**indirizzo IP**, la **maschera di sottorete**, l'**indirizzo del gateway** e l'**indirizzo del server DNS**.

Nota

Se abiliti il DHCP, il dispositivo otterrà i parametri Wi-Fi automaticamente.

5. Fare clic su **Salva**.

Rete cellulare

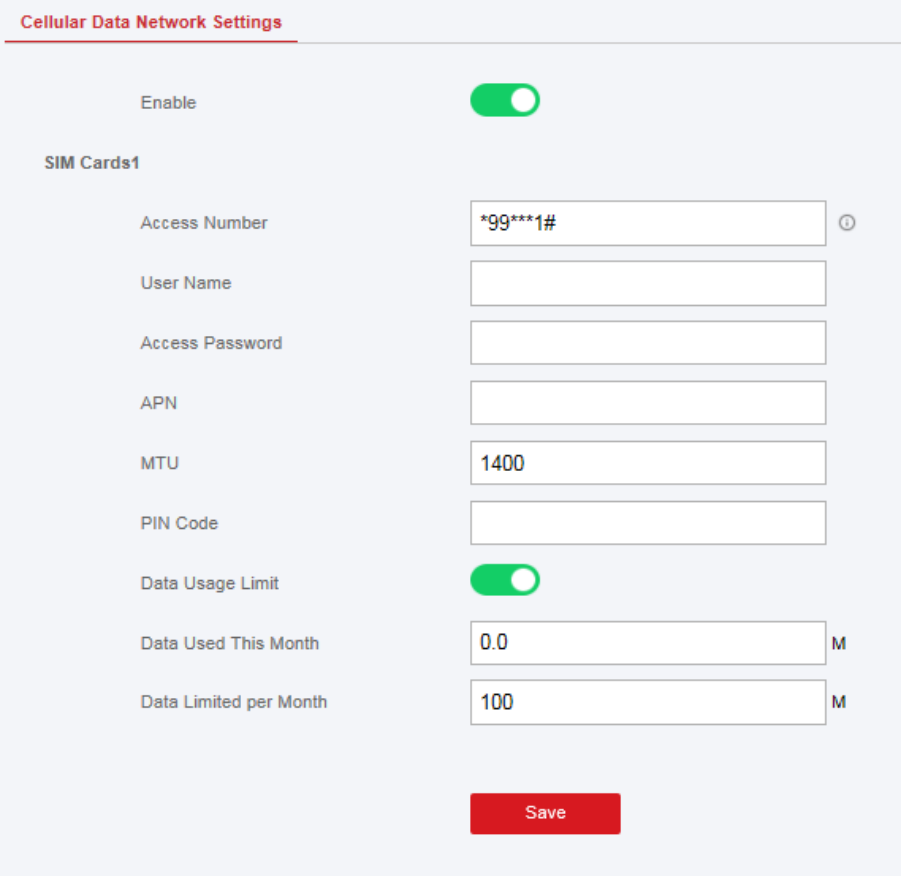
Imposta i parametri della rete cellulare se inserisci una scheda SIM all'interno del dispositivo. Utilizzando la rete cellulare, il dispositivo può caricare le notifiche di allarme alla centrale di allarme.

Prima di iniziare

Inserire una scheda SIM nello slot della scheda SIM del dispositivo.

Passi

1. Cliccate su **Parametri di comunicazione** → **Rete dati cellulare per** entrare nella pagina Impostazioni rete dati cellulare.



2. Abilita la composizione senza fili.
3. Imposta i parametri della rete dati cellulare.

Numero di accesso

Inserire il numero di composizione dell'operatore.

Nota

Solo l'utente della carta SIM della rete privata deve inserire il numero di accesso.

Nome utente

Chiedete all'operatore di rete e inserite il nome dell'utente.

Password di accesso

Chiedete all'operatore di rete e inserite la password.

APN

Chiedi all'operatore di rete di ottenere le informazioni APN e inserisci le informazioni APN.

Limite di utilizzo dei dati

È possibile attivare la funzione e impostare la soglia di dati ogni mese. Se l'utilizzo dei dati è superiore alla soglia configurata, scatterà un allarme che verrà caricato sulla centrale di allarme e sul client mobile.

Dati utilizzati questo mese

I dati utilizzati saranno accumulati e visualizzati in questa casella di testo.

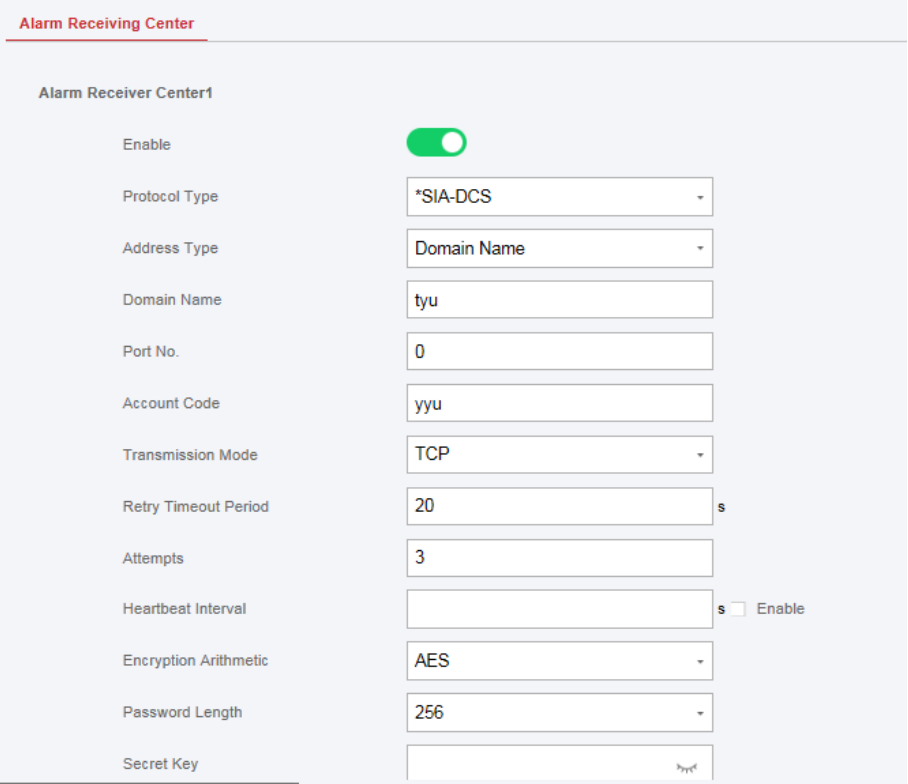
4. Fare clic su **Salva**.

Centro di allarme

È possibile impostare i parametri del centro di allarme e tutti gli allarmi saranno inviati al centro di allarme configurato.

Passi

1. Clicca su **Communication Parameters** → **Alarm Receiving Center** per entrare nella pagina Alarm Receiving Center.



2. Selezionare il **centro di ricezione dell'allarme** come **1** o **2** per la configurazione, e far scorrere il cursore per abilitare il centro di ricezione dell'allarme selezionato.

Nota

Solo se la centrale di ricezione dell'allarme 1 è abilitata, è possibile impostare la centrale di ricezione dell'allarme 2 come
canale di backup e modificare i parametri del canale.

---

3. Selezionare il **tipo di protocollo** come **ADM-CID**, **ISUP**, **SIA-DCS**, ***SIA-DCS**, o ***ADM-CID** per impostare la modalità di caricamento.

Nota

Protocollo standard DC-09
ADM-CID: Il metodo di presentazione dei dati di DC-09 è CID, che non è criptato e solo per caricare il rapporto di allarme.
*ADC-CID: Il metodo di presentazione dei dati di DC-09 è CID, che è criptato e solo per caricare il rapporto di allarme.
SIA-DCS: Il metodo di presentazione dei dati del DC-09 è il DCS (chiamato anche protocollo SIA), che non è criptato e serve solo per caricare il rapporto di allarme.
*SIA-DCS: Il metodo di presentazione dei dati del DC-09 è il DCS (chiamato anche protocollo SIA), che è criptato e solo per caricare il rapporto di allarme.

ADM-CID o **SIA-DCS** Si deve selezionare il **tipo di ricevitore d'allarme** come **IP** o **nome di dominio**, e inserire il nome IP/dominio, il numero di porta, il codice dell'account, il timeout, i tempi di ricarica e

intervallo di battito cardiaco.

Nota

Impostare l'intervallo di heartbeat con l'intervallo da 10 a 3888000 secondi.

ISUPY Non è necessario impostare i parametri del protocollo ISUP.
***SIA-DCS** o ***ADM-CID** Si dovrebbe selezionare il **tipo di ricevitore d'allarme** come **IP** o **nome di dominio**, e inserire il nome IP/dominio, il numero di porta, il codice dell'account, il periodo di timeout di ripetizione, i tentativi, l'intervallo di heartbeat, l'aritmetica di crittografia, la

Nota

lunghezza della password e la chiave segreta.

Impostare l'intervallo di heartbeat con l'intervallo da 10 a 3888000 secondi.
Per la crittografia aritmetica: Il formato di crittografia di sostegno del pannello per la sicurezza delle informazioni secondo DC-09, AES-128, AES-192 e AES-256 sono supportati quando si configura il centro di allarme.
Per la chiave segreta: Quando si usa un formato criptato di DC-09, una chiave dovrebbe essere impostata quando si configura l'ARC. La chiave verrebbe emessa offline dall'ARC, che verrebbe utilizzata per criptare il messaggio per la sicurezza della sostituzione.

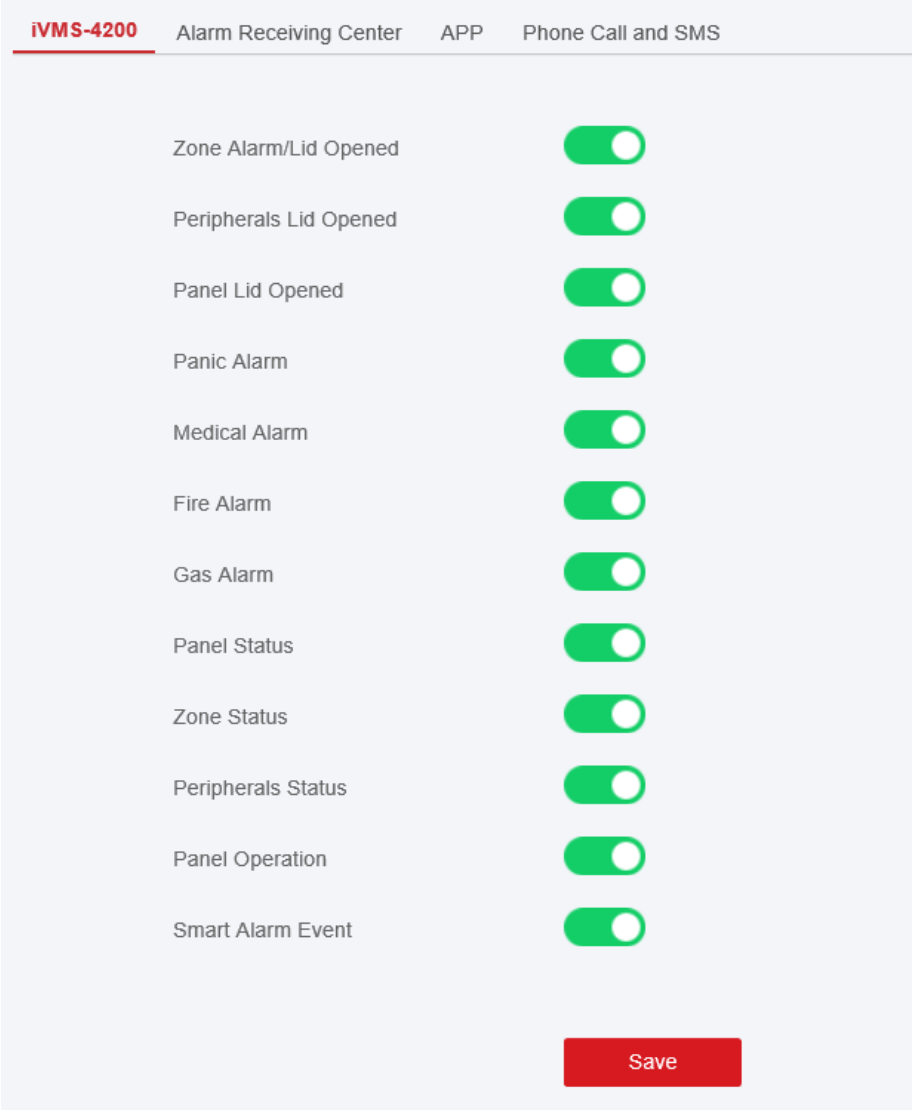
4. Fare clic su **Salva**.

Notifica Push

Quando scatta un allarme, se vuoi inviare la notifica dell'allarme al cliente, alla centrale d'allarme, al cloud o al telefono cellulare, puoi impostare i parametri di push della notifica.

Passi

1. Fare clic su **Parametri di comunicazione** → **Notifica dei tipi di evento** .



2. Abilita la notifica di destinazione.

Nota

Se vuoi inviare le notifiche di allarme al client mobile, devi anche impostare l'**indice del telefono cellulare**, il **numero di telefono cellulare** e controllare il **tipo di notifica**.

Nota

Per la notifica dei messaggi nel centro di ricezione degli allarmi, seleziona l'indice del centro prima delle impostazioni.

3. Fare clic su **Salva**.

Risultato

Tabella 4-1 Opzioni delle notifiche

Opzione	Notifica
iVMS-4200	Allarme di zona e coperchio aperto Dispositivo senza fili Coperchio aperto Notifica di manomissione Notifica di allarme antipanico Notifica di allarme medico Notifica di allarme gas Notifica di allarme incendio Notifica di gestione del pannello Notifica di stato del sistema Notifica di stato del rilevatore Notifica dello stato dei dispositivi wireless
Centro di ricezione degli allarmi	Centrale di ricezione dell'allarme 1&2 Allarme di zona & Coperchio aperto Dispositivo senza fili Coperchio aperto Notifica di manomissione Notifica di allarme antipanico Notifica di allarme medico Notifica di allarme gas Notifica di allarme incendio Notifica di gestione del pannello Notifica di stato del sistema Notifica di stato del rilevatore Notifica dello stato dei dispositivi wireless

Cloud	Allarme di zona e coperchio aperto Dispositivo senza fili Coperchio aperto Notifica di manomissione Notifica di allarme antipanico Notifica di allarme medico

Opzione	Notifica
	Notifica di allarme gas Notifica di allarme incendio Notifica di gestione del pannello Notifica di stato del sistema Notifica di stato del rilevatore Notifica dello stato dei dispositivi wireless
Telefono cellulare	Indice del telefono cellulare da 1 a 8 Numero di telefono cellulare Tipo di notifica SMS & Voice Call Check Box Zone alarm & Lid Opened (Set Filter Time) Numero di chiamate Coperchio del dispositivo wireless aperto Notifica di manomissione Notifica di allarme antipanico Notifica di allarme medico Notifica di allarme gas Notifica di allarme incendio Notifica di gestione del pannello Notifica di stato del sistema Notifica di stato del rilevatore Notifica dello stato dei dispositivi wireless

Nota

Per la notifica del telefono cellulare:

- È necessario premere * per terminare la chiamata.
- È necessario aggiungere il codice di controllo quando si inserisce il numero di cellulare.

Servizio cloud

Se volete registrare il dispositivo al client mobile per la configurazione remota, dovreste impostare il parametro

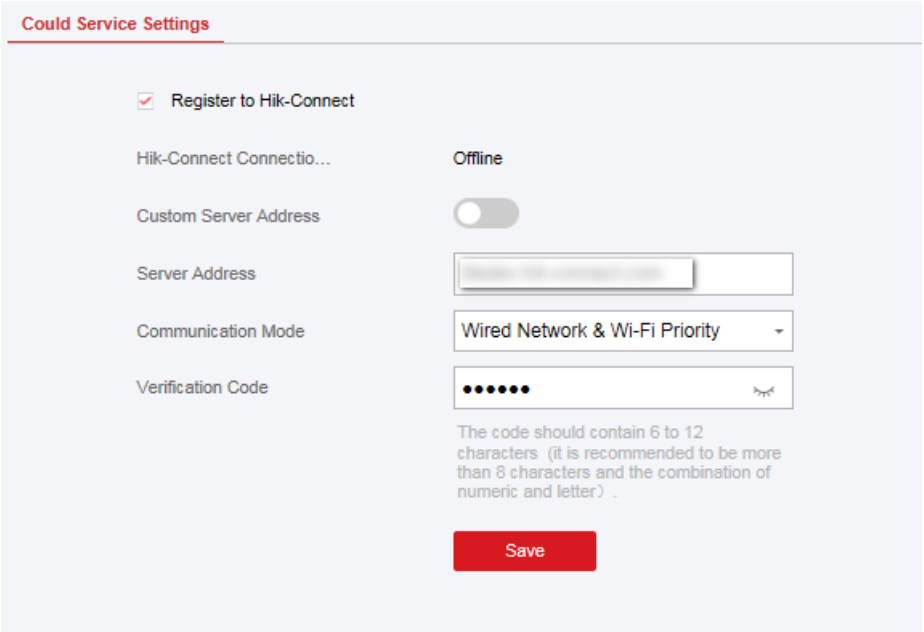
parametri di registrazione del client mobile.

Prima di iniziare

- Collegare il dispositivo alla rete tramite connessione cablata, connessione dial-up o connessione Wi-Fi.
- Impostare l'indirizzo IP del dispositivo, la subnet mask, il gateway e il server DNS nella LAN.

Passi

1. Fare clic su **Parametri di comunicazione** → **Impostazioni del servizio** cloud per entrare nella pagina delle impostazioni di registrazione di Hik-Connect.



2. Fare clic su **Parametri di comunicazione** → **Registrazione Guarding Vision** per accedere alla pagina delle impostazioni di registrazione Guarding Vision.
3. Controlla **il registro di Hik-Connect**.

Nota

Per impostazione predefinita, il servizio Hik-Connect del dispositivo è abilitato.

È possibile visualizzare lo stato del dispositivo nel server Hik-Connect (www.hik-connect.com).

4. Controllare **il registro a Guarding Vision**.

Nota

Per impostazione predefinita, il servizio Guarding Vision del dispositivo è abilitato.

È possibile visualizzare lo stato del dispositivo nel server Guarding Vision (www.guardingvision.com).

5. Abilita l'**indirizzo del server personalizzato**.

L'indirizzo del server è già visualizzato nella casella di testo Server Address.

6. Selezionare una modalità di comunicazione dall'elenco a discesa in base al metodo di comunicazione attuale del dispositivo.

   Auto

   Il sistema selezionerà automaticamente la modalità di comunicazione secondo la sequenza di, rete cablata, rete Wi-Fi e rete dati cellulare. Solo quando la rete corrente è scollegata, il dispositivo si collegherà ad un'altra rete.

   Rete cablata e priorità Wi-Fi

   L'ordine di priorità della connessione dall'alto al basso è: rete cablata, Wi-Fi, rete dati cellulare.

   Wired &Wi-Fi

   Il sistema selezionerà prima la rete cablata. Se non viene rilevata alcuna rete cablata, selezionerà la rete Wi-Fi.

   Rete dati cellulare

   Il sistema selezionerà solo la rete dati cellulare.
7. Opzionale: Cambia la password di autenticazione.

Nota

- Per impostazione predefinita, la password di autenticazione viene visualizzata nella casella di testo.
- La password di autenticazione dovrebbe contenere da 6 a 12 lettere o cifre. Per ragioni di sicurezza, si suggerisce una password di 8 caratteri, che contenga due o più dei seguenti tipi di caratteri: maiuscole, minuscole e cifre.

8. Fare clic su **Salva**.

Notifica via e-mail

È possibile inviare il video dell'allarme o l'evento all'e-mail configurata.

Passi

1. Clicca su **Comunicazione** →Notifica **via e-mail** per entrare nella pagina.
2. Fare clic sul blocco per abilitare la funzione di invio dell'evento di verifica video.
3. Inserisci le informazioni del mittente.

Nota

Si raccomanda di usare Gmail e Hotmail per inviare le mail.

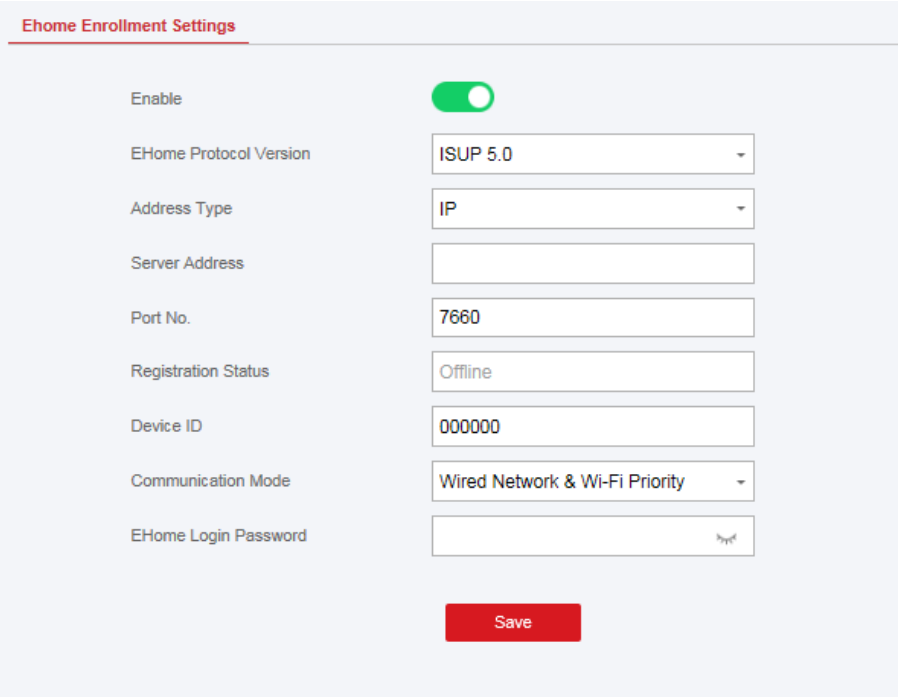
4. Inserire le informazioni del ricevitore.
5. Clicca su **Receiver Address Test** e assicurati che l'indirizzo sia corretto.
6. Fare clic su **Salva**.

ISUP

In questa sezione, potete creare un account ISUP, e modificare l'indirizzo IP/nome di dominio, il numero di porta.

Passi

1. Fare clic su **Parametri di comunicazione** → **Registrazione ISUP** per entrare nella pagina delle impostazioni di registrazione ISUP.



2. Far scorrere il cursore per abilitare il protocollo ISUP.
3. Selezionate il **tipo di indirizzo** come **IP** o **nome di dominio**.
4. Inserisci l'indirizzo IP o il nome di dominio secondo il tipo di indirizzo.
5. Inserire il numero di porta per il protocollo.

Nota

Per impostazione predefinita, il numero di porta per ISUP è 7660.

6. Impostare un account, compreso l'**ID** dispositivo e la **password di accesso ISUP**.
7. Selezionare la **modalità di**

comunicazione. **Auto**

Il sistema selezionerà automaticamente la modalità di comunicazione in base alla sequenza di, rete cablata, rete Wi-Fi e rete dati cellulare. Solo quando la rete corrente è scollegata, il dispositivo si connetterà ad altre reti.

Rete cablata e priorità Wi-Fi

L'ordine di priorità della connessione dall'alto al basso è: rete cablata, Wi-Fi, rete dati cellulare.

Wired &Wi-Fi

Il sistema selezionerà prima la rete cablata. Se non viene rilevata alcuna rete cablata, selezionerà la rete Wi-Fi.

Rete dati cellulare

Il sistema selezionerà solo la rete dati cellulare.

8. Fare clic su **Salva**.

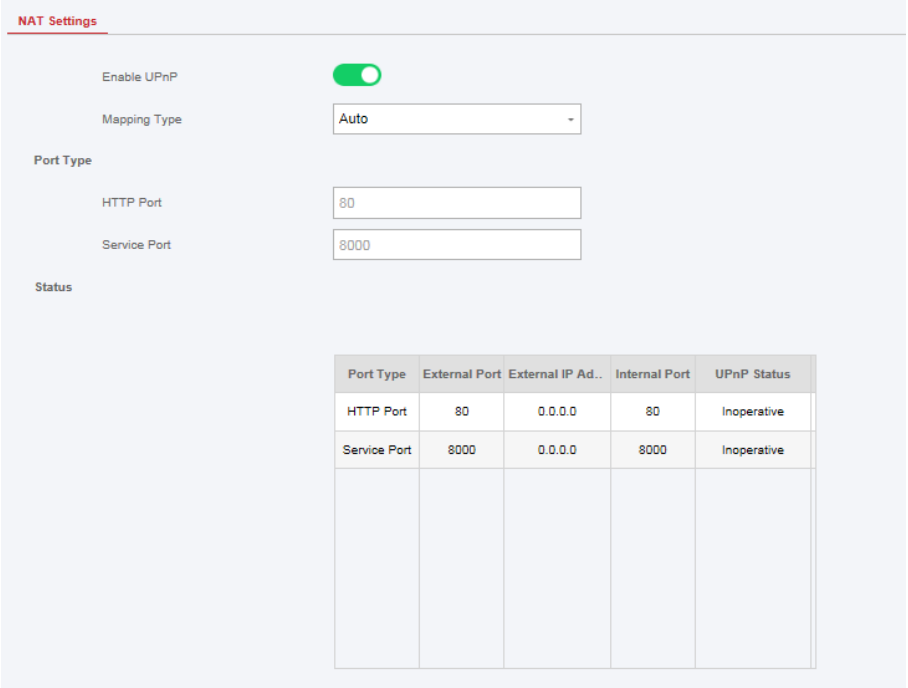
NAT

Universal Plug and Play (UPnP™) è un'architettura di rete che fornisce compatibilità tra apparecchiature di rete, software e altri dispositivi hardware. Il protocollo UPnP permette ai dispositivi di connettersi senza soluzione di continuità e di semplificare l'implementazione delle reti negli ambienti domestici e aziendali.

Abilita la funzione UPnP, e non hai bisogno di configurare la mappatura delle porte per ogni porta, e il dispositivo è collegato alla Wide Area Network tramite il router.

Passi

1. Fare clic su **Parametri di comunicazione** → **NAT** per entrare nella pagina.



2. Trascinate il cursore per abilitare l'UPnP.
3. Opzionale: Selezionare il tipo di mappatura come **Manuale**
4. Impostare la porta HTTP e la porta di servizio.
5. Fare clic su **Salva** per completare le impostazioni

FTP

È possibile configurare il server FTP per salvare il video dell'allarme.

Passi

1. Fare clic su **Comunicazione→ FTP** per entrare nella pagina.
2. Configurare i parametri FTP

Tipo FTP

Impostare il tipo di FTP come preferito o alternato.

Protocollo FTP

FTP e SFTP sono selezionabili. Il caricamento dei file è criptato utilizzando il protocollo SFTP.

Indirizzo e porta del server

L'indirizzo del server FTP e la porta corrispondente.

Nome utente e password

L'utente FTP deve avere il permesso di caricare immagini. Se il server FTP supporta il caricamento di immagini da parte di utenti anonimi, puoi selezionare Anonymous per nascondere le informazioni del tuo dispositivo durante il caricamento.

Struttura dell'elenco

Il percorso di salvataggio delle istantanee nel server FTP.

4.3.2 Gestione dei dispositivi

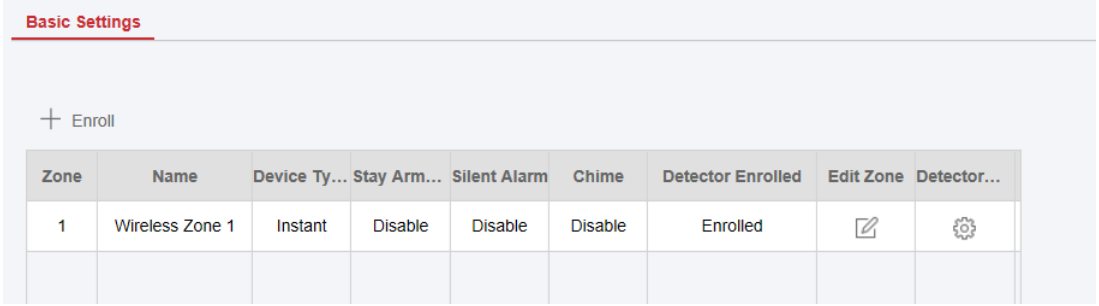
In questa sezione è possibile gestire le periferiche iscritte, tra cui rilevatore, sirena, tastiera, ecc.

Zona

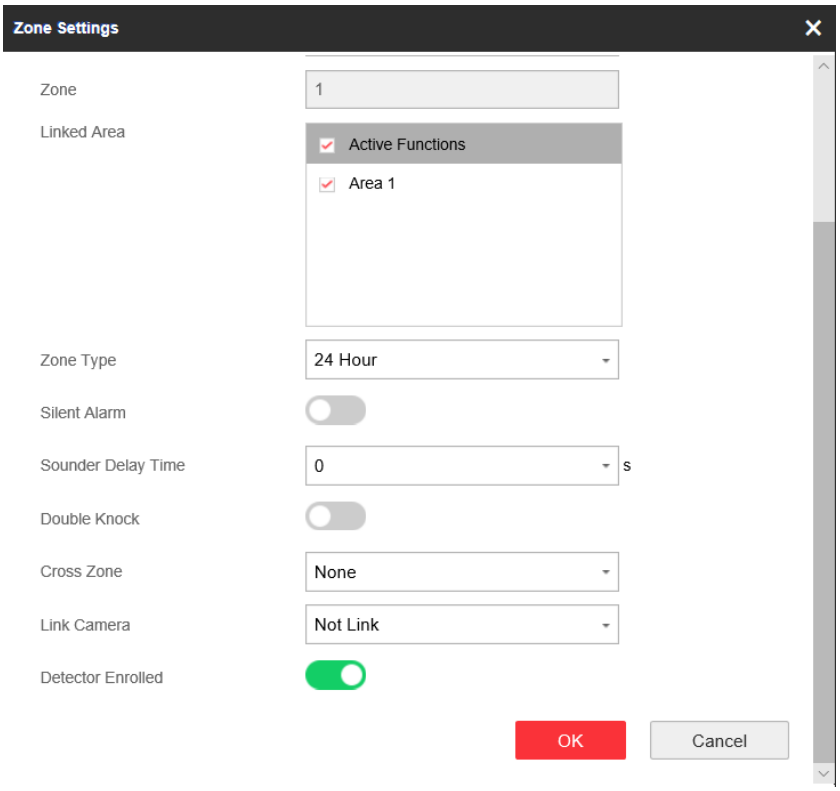
Puoi impostare i parametri della zona nella pagina della zona.

Passi

1. Clicca su **Dispositivo** → **Zona** per entrare nella pagina Zona.



2. Seleziona una zona e clicca su **Edit Zone** per entrare nella pagina Zone Settings.



3. Modifica il nome della zona.
4. Controllare le aree collegate.

Nota

- Solo le aree abilitate saranno elencate.
- La nuova periferica aggiunta è collegata all'area 1 per impostazione predefinita.

5. Seleziona un tipo di zona.

Zona istantanea

Questo tipo di zona attiverà immediatamente un evento di allarme quando viene armata.

Zona di ritardo

Ritardo di uscita: Exit Delay fornisce il tempo per lasciare attraverso l'area di difesa senza allarme. Ritardo di entrata: Entry Delay fornisce il tempo di entrare nell'area di difesa per disarmare il sistema senza allarme.
Il sistema dà il tempo di ritardo di entrata/uscita quando è armato o rientrato. Di solito è usato nel percorso di entrata/uscita (per esempio porta principale/ingresso principale), che è un percorso chiave per armare/disarmare tramite tastiera operativa per gli utenti.

Nota

- È possibile impostare 2 diverse durate di tempo in **Opzioni di sistema → Programmazione e timer.**
- Assicurarsi che il timer non sia più lungo di 45 secondi per essere conforme a EN50131-1.
  È possibile impostare il tempo di ritardo del braccio di permanenza per la zona di ritardo.

Zona di panico

La zona si attiva tutto il tempo. Di solito viene utilizzata nei siti dotati di pulsante antipanico, rilevatore di fumo e rilevatore di rottura vetri.

Zona dell'interruttore a chiave

L'area collegata si attiverà dopo essere stata attivata e si disattiverà dopo essere stata ripristinata. Nel caso dell'allarme di manomissione, l'operazione di inserimento e

Nota

disinserimento non verrà attivata.

Due tipi di attivazione (per tempi di attivazione e per stato della zona) possono essere selezionati per il zone. Se il tipo di stato della zona è selezionato, impostare l'operazione di attivazione (attivazione/disattivazione dell'zone.

attiv

azione).

Zona disabili

Zona disattivata ignorando qualsiasi evento di allarme. Di solito è usato per disabilitare i rivelatori difettosi.

Zona 24 ore

La zona si attiva tutto il tempo con l'uscita di suono/siren quando si verifica l'allarme. Di solito viene utilizzata nelle zone a rischio d'incendio dotate di rilevatori di fumo e sensori di temperatura.

6. Abilita **Cross zone**, **Allarme silenzioso, ecc.** in base alle tue esigenze reali.

Nota

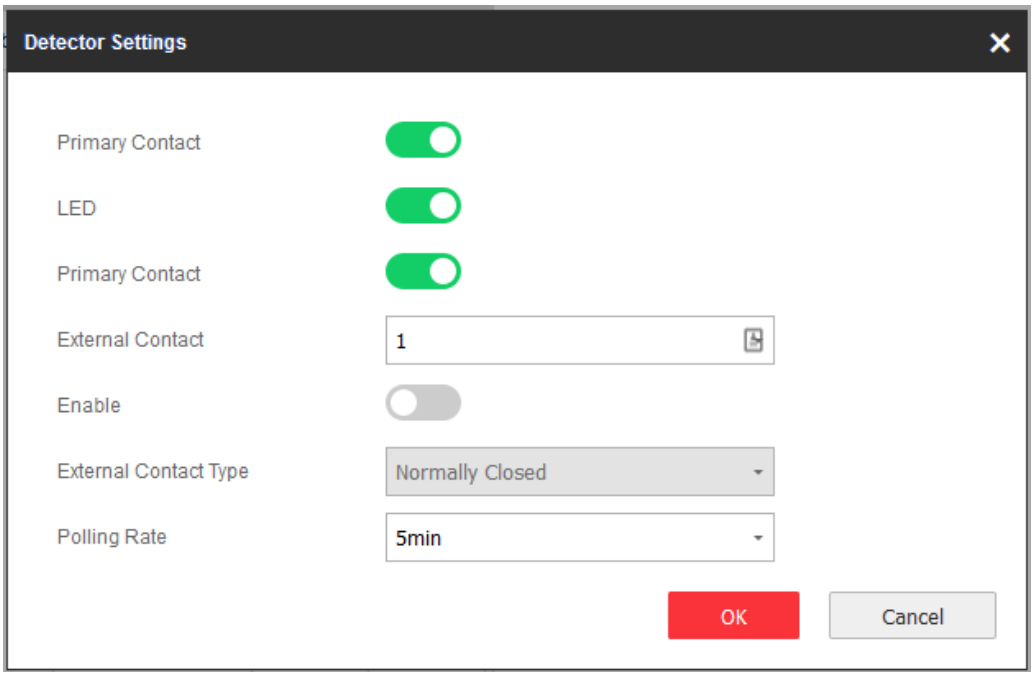
Alcune zone non supportano la funzione. Fare riferimento alla zona attuale per impostare la funzione.

7. Impostare il **tempo di ritardo della sirena. La** sirena sarà attivata immediatamente o dopo il tempo impostato.
8. Se necessario, collegare una telecamera per la zona.
9. Abilitare il **rilevatore iscritto**, inserire il numero di serie e impostare il numero di telecamera collegato.
10. Fare clic su **OK**.

Nota

Dopo aver impostato la zona, è possibile entrare in **Status** → **Zone** per visualizzare lo stato della zona.

11. Fai clic su **Detector Settings** per accedere alla pagina Detector Settings.



Nota

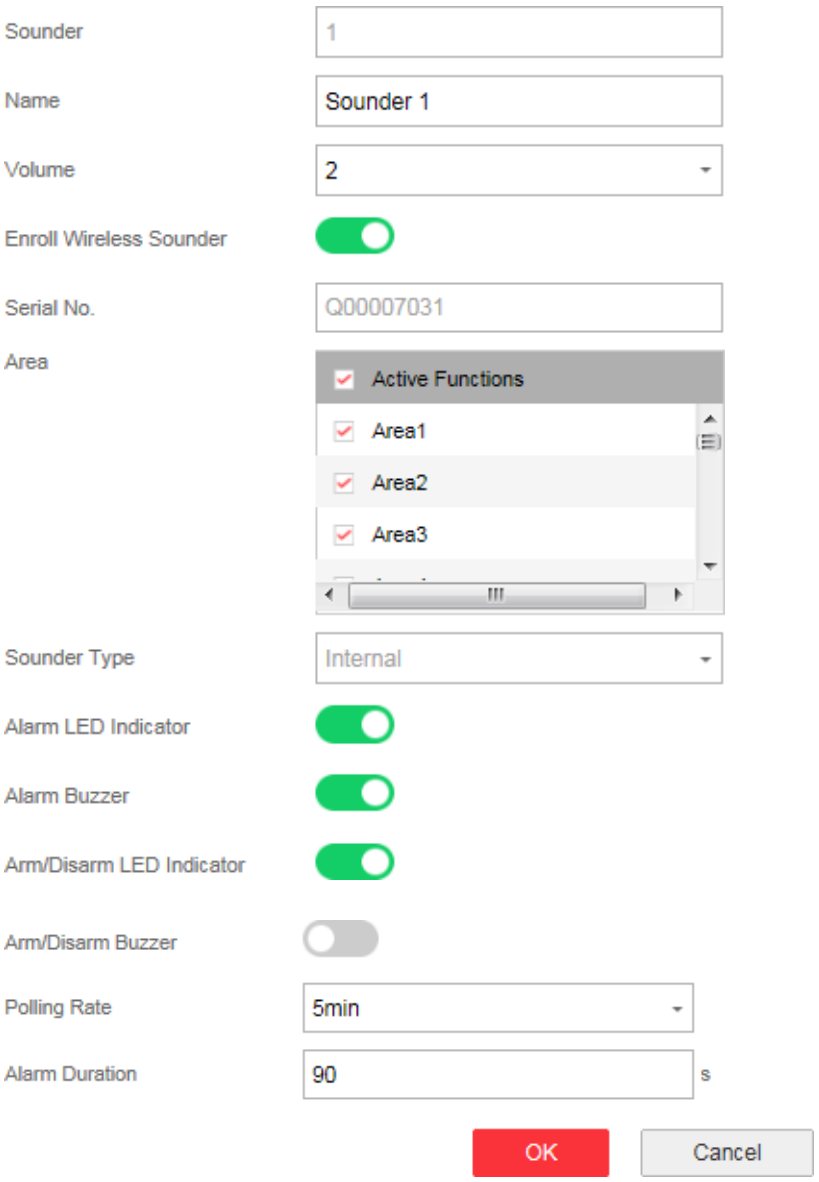
non è permesso spegnere il contatto per la conformità EN.

Sounder

La sirena è iscritta all'AX PRO tramite il modulo ricevitore wireless, e la sirena wireless 868 Mhz può essere iscritta all'ibrido AX PRO tramite il ricevitore wireless che si trova all'indirizzo 9.

Passi

1. Clicca su **Dispositivo** → **Sounder** per entrare nella pagina Sounder.
2. Clicchi per entrare nella pagina delle impostazioni del Sounder.



3. Impostare il nome della sirena e il volume.

Nota

La gamma di volume della sirena disponibile va da 0 a 3 (la funzione varia secondo il modello del dispositivo).

4. Abilitare **il Wireless Sounder** e impostare il numero di serie del sounder.
5. Seleziona l'area collegata.

Nota

- Solo le aree abilitate saranno elencate.
- La nuova periferica aggiunta è collegata all'area 1 per impostazione predefinita.

6. Selezionare per abilitare l'**indicatore LED di allarme**, il **cicalino di allarme**, l'**indicatore LED di attivazione/disattivazione** e **Arm/Disarm Buzzer**.
7. Impostare la **frequenza di polling** e la **durata dell'allarme**.
8. Fare clic su **OK**.

Nota

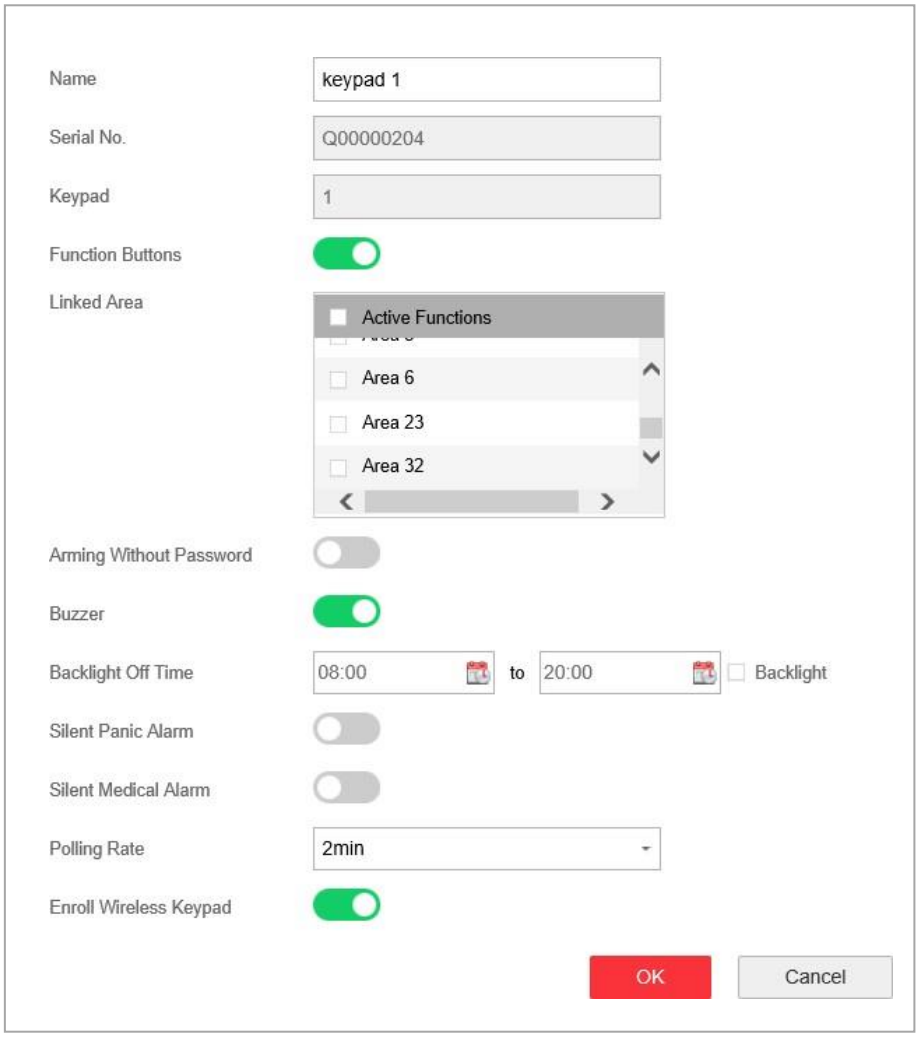
Dopo che la sirena è stata configurata, potete cliccare su **Status** → **Sounder** per visualizzare lo stato della sirena.

Tastiera

È possibile impostare i parametri della tastiera iscritta all'AX PRO.

Passi

1. Clicca su **Dispositivo** → **Tastiera** per entrare nella pagina.
2. Clicca per entrare nella pagina delle impostazioni della tastiera.



3. Imposta il nome della tastiera.
4. Selezionate la casella di controllo per abilitare la funzione di cicalino, allarme panico silenzioso, allarme medico silenzioso e pulsante della tastiera.
5. Selezionate la casella di controllo per abilitare la funzione di armare senza password.
6. Selezionate la casella di controllo **Enable** di Back-light Off Time, e impostate la durata di spegnimento della luce.
7. Impostare il tasso di rotolamento.
8. Selezionare l'area collegata alla tastiera.

Nota

- Solo le aree abilitate saranno elencate.
- La nuova periferica aggiunta è collegata all'area 1 per impostazione predefinita.

9. Impostare se annullare o meno l'iscrizione della tastiera. Se il collegamento è abilitato, il dispositivo sarà cancellato.
10. Fare clic su **OK**.

Nota

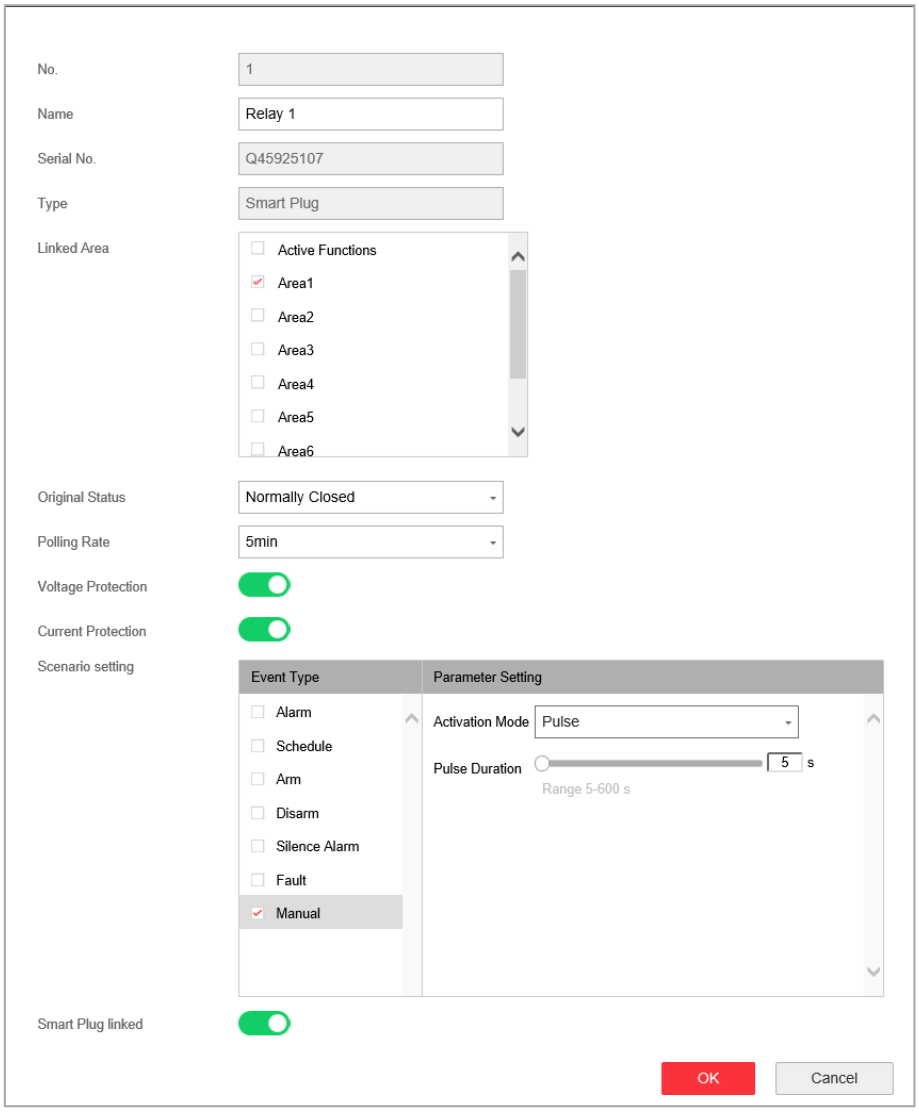
- Dopo che il tastierino è stato configurato, potete cliccare su **Stato** → **Tastierino** per visualizzare lo stato del tastierino.
- È possibile impostare la password della tastiera nella pagina di **Gestione utente** → **Utente** → **Funzionamento**.

Automazione

È possibile impostare i parametri delle uscite a relè che è iscritto all'AX PRO.

Passi

1. Fare clic su **Dispositivo** → **Automazione** per entrare nella pagina.
2. Fare clic su **Enroll**, inserire il numero di serie e selezionare il tipo di dispositivo per aggiungere un dispositivo di uscita a relè.
3. Clicca  per modificare le informazioni del relè.



- Imposta il nome del dispositivo di uscita a relè.

- Seleziona l'area collegata per l'uscita.

Nota

- Solo le aree abilitate saranno elencate.
- La nuova periferica aggiunta è collegata all'area 1 per impostazione predefinita.
- La funzione varia a seconda dei diversi tipi di relè

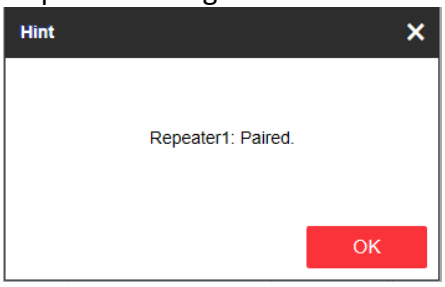
- Impostare lo stato originale come Normalmente Chiuso o Normalmente Aperto.
- Impostare il tasso di polling.
- Impostare se proteggere la tensione/corrente o no.
- Imposta l'evento per essere attivato.
- Imposta l'attivazione dopo essere stato attivato.
- Impostare se collegare o meno il dispositivo di uscita a relè. Se il collegamento è abilitato, il dispositivo sarà cancellato.

Ripetitore

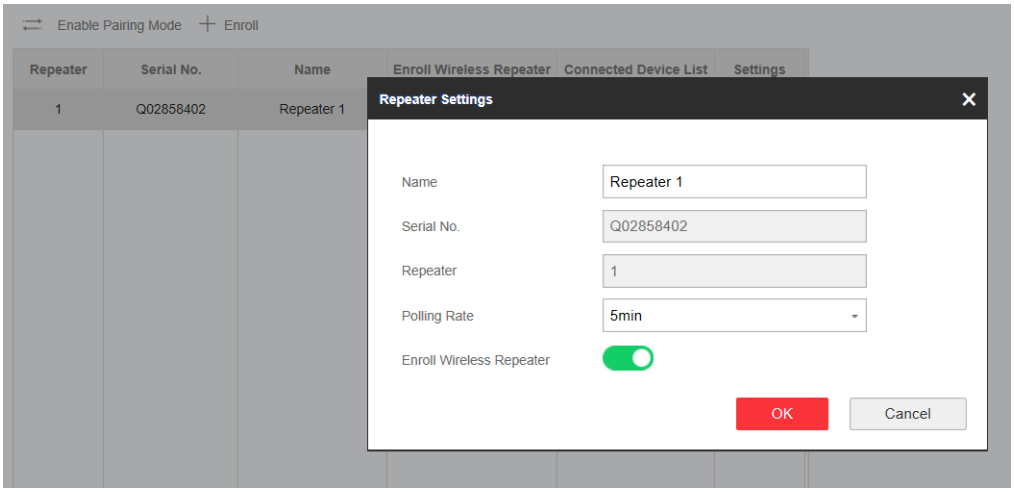
Il ripetitore può amplificare i segnali tra il pannello di controllo e le periferiche.

Passi

1. Fare clic su **Dispositivo** →Ripetitore per entrare nella pagina.
2. Fare clic su **Enroll**, inserire il numero di serie e selezionare il tipo di dispositivo per aggiungere un ripetitore
3. Fare clic su **Enter Paring Mode** per far entrare il ripetitore nella modalità di paring del dispositivo.
4. Quando la distanza tra la periferica e il pannello di controllo è lontana, il ripetitore può essere usato come stazione di trasferimento per l'accoppiamento. La modalità di accoppiamento dura 3 minuti e non può essere interrotta. Dopo che l'accoppiamento è avvenuto con successo, viene visualizzato un elenco di dispositivi collegati.



5. Click  per modificare le informazioni Click sul ripetitore.



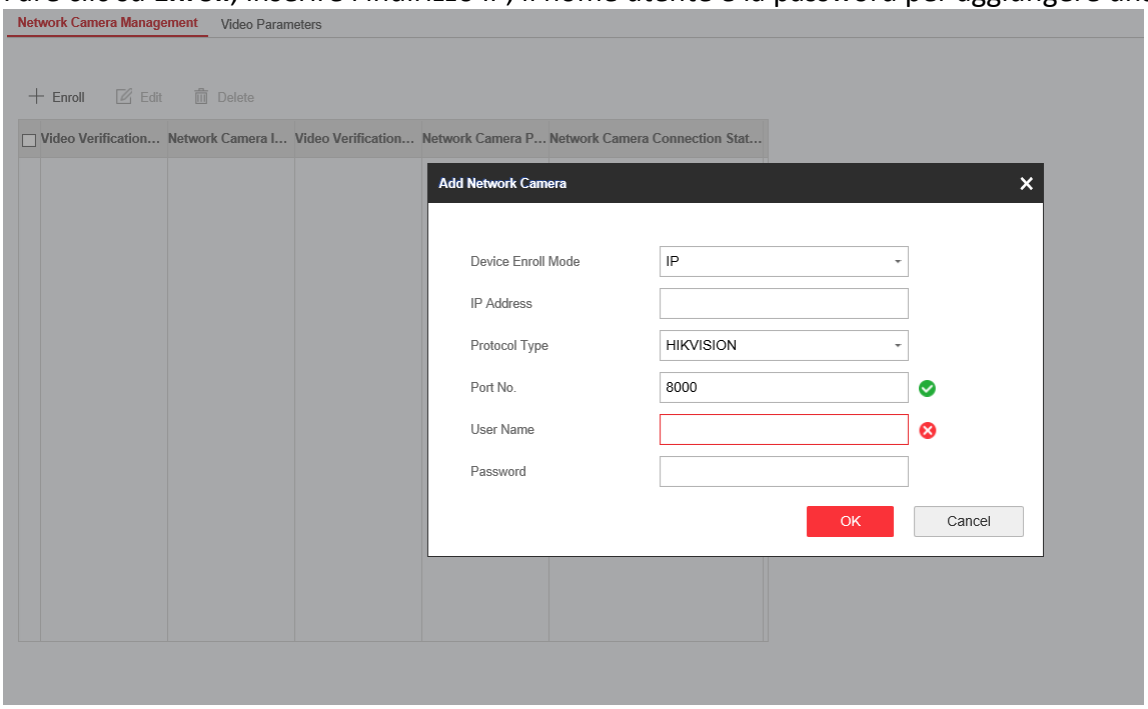
- Imposta il nome del ripetitore.
- Impostare la frequenza di polling del ripetitore.
- Imposta se cancellare o meno l'iscrizione del ripetitore. Se il collegamento è abilitato, il dispositivo sarà cancellato.

Telecamera di rete

È possibile aggiungere telecamere di rete nel sistema.

Passi

1. Clicca su **Dispositivo** → **Fotocamera** per entrare nella pagina.
2. Fare clic su **Enroll**, inserire l'indirizzo IP, il nome utente e la password per aggiungere una telecamera.



3. Fare per modificare le informazioni

also click Edit È possibile also click Delete modificare la telecamera, o clickeliminare la telecamera.

4.3.3 Impostazioni dell'area

Impostazioni di base

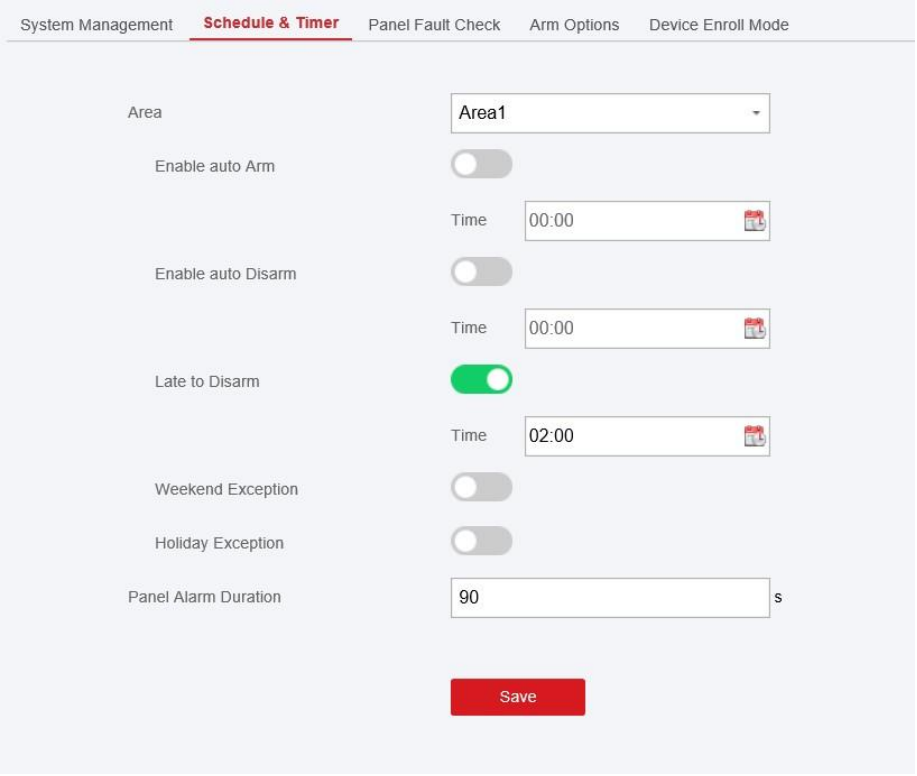
È possibile collegare le zone all'area selezionata.

Passi

1. Clicca su **Area** → **Impostazioni di base** per entrare nella pagina.
2. Seleziona un'area.
3. Controllare **Abilita**.
4. Spunta la casella di controllo davanti alla zona per selezionare le zone per l'area.
5. Clicca su **Salva** per completare le impostazioni.

Impostazioni del programma e del timer

È possibile impostare il programma di allarme. La zona sarà armata/disarmata secondo il programma orario configurato.



Passi

1. Fare clic su **Sistema→ Opzioni di sistema** → **Programma e timer per** accedere alla pagina Programma e timer.
2. Seleziona un'area.
3. Impostare i seguenti parametri in base alle esigenze reali.

Abilitare il braccio automatico

Abilitare la funzione e impostare l'ora di inizio dell'attivazione. La zona sarà armata secondo l'ora configurata.

Nota

- Il tempo di armamento automatico e il tempo di disarmo automatico non possono essere gli stessi.
- Il cicalino suona lentamente 2 minuti prima che inizi l'armamento automatico e suona rapidamente 1 minuto prima che inizi l'armamento automatico.
- È possibile selezionare l'abilitazione dell'armatura forzata nella pagina System Options (Opzioni sistema). Quando la funzione è abilitata, il sistema sarà armato indipendentemente dal guasto.
- Se l'area pubblica è abilitata, l'area 1 non supporta l'armatura automatica.

Abilitare il disarmo automatico

Abilitare la funzione e impostare l'ora di inizio del disinserimento. La zona sarà disarmata secondo l'ora configurata.

Nota

- Il tempo di armamento automatico e il tempo di disarmo automatico non possono essere gli stessi.
- Se l'area pubblica è abilitata, l'area 1 non supporta il disarmo automatico.

Tardivo al disarmo

Attivare la funzione e impostare l'ora. Se l'allarme scatta dopo l'ora configurata, la persona sarà considerata in ritardo.

Nota

È necessario abilitare la funzione di notifica della gestione del pannello in **Parametri di comunicazione** → **Comunicazione degli eventi** prima di abilitare la funzione di disinserimento tardivo.

Eccezione di fine settimana

Abilita la funzione e la zona non sarà armata nel fine settimana.

Eccezione di vacanza

Abilitare la funzione e la zona non sarà armata/disarmata durante le vacanze. Si dovrebbe impostare il programma delle vacanze dopo l'abilitazione.

Nota

Si possono impostare fino a 6 gruppi di vacanze.

Durata dell'allarme del pannello

La durata temporale dell'allarme del pannello.

Nota

L'intervallo di tempo disponibile va da 10 s a 900 s.

5. Fare clic su **Salva**.

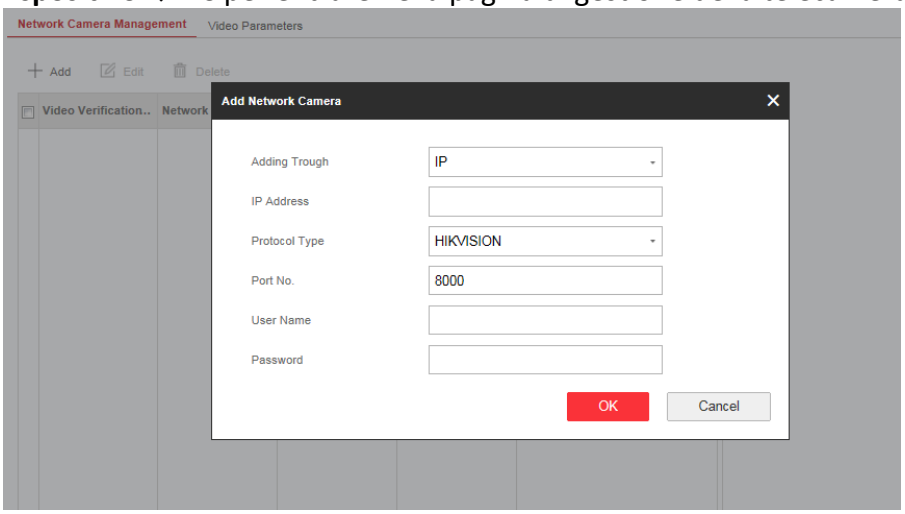
4.3.4 Gestione video

Puoi aggiungere due telecamere di rete all'AX PRO e collegare la telecamera alla zona selezionata per il monitoraggio video. Puoi anche ricevere e visualizzare il video dell'evento tramite client e Email.

Aggiungere telecamere all'AX PRO

Passi

1. Fare clic su **Dispositivo** →IPC per entrare nella pagina di gestione della telecamera di rete.



2. Fare clic su **Add** , e inserire le informazioni di base della telecamera, come l'indirizzo IP e il numero di porta, e selezionare il tipo di protocollo.
3. Inserisci il nome utente e la password della telecamera.
4. ClickOK .
5. Opzionale: Fai clic su **Modifica** o **Elimina** per modificare o eliminare la telecamera selezionata.

Collegare una telecamera con la zona

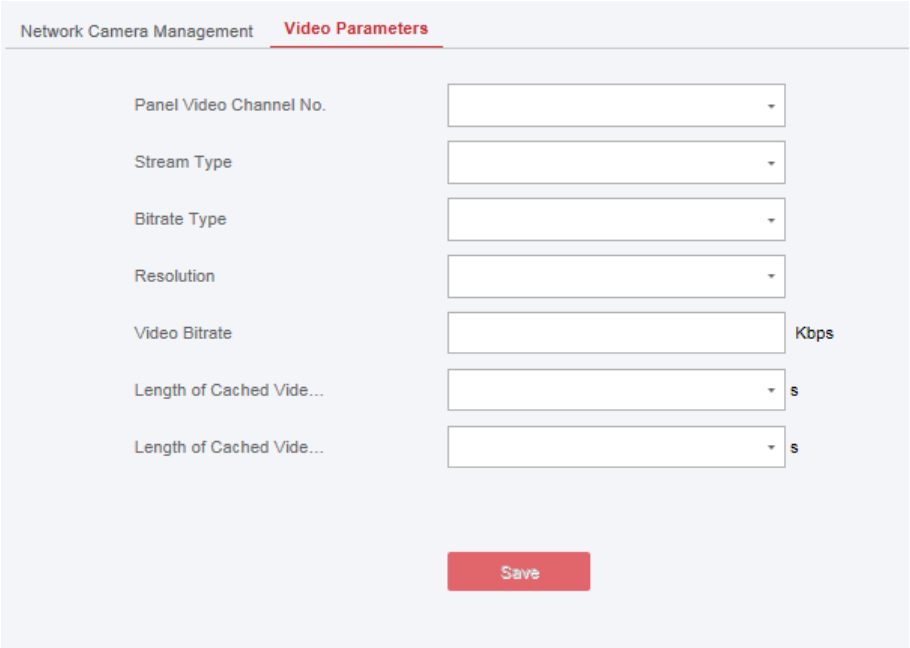
Passi

1. Fare clic su **Dispositivo** → **Zona** per entrare nella pagina di configurazione.
2. Selezionare una zona che si desidera includere il monitoraggio video e fare clic sul pulsante .
3. Selezionare il **numero di canale video del pannello**.
4. Fare clic su **OK**.

Impostare i parametri video

Passi

1. Fare clic su **Dispositivo** →IPC→Video per entrare nella pagina.



2. Seleziona una telecamera e imposta i parametri video.

Tipo di flusso

Flusso principale: Essendo usato nella registrazione e nell'anteprima HD, ha un'alta risoluzione, velocità di codifica e qualità dell'immagine.
Sub-Stream: È usato per trasmettere immagini di rete e in anteprima come uno streaming video con caratteristiche di risoluzione, bit rate e qualità dell'immagine inferiori.

Tipo di bitrate

Seleziona il tipo di bitrate come costante o variabile.

Risoluzione

Seleziona la risoluzione dell'uscita video.

Bitrate video

Il valore più alto corrisponde alla maggiore qualità video, ma è richiesta una migliore larghezza di banda.

4.3.5 Gestione dei permessi

Aggiungi/modifica/cancella il portachiavi

È possibile aggiungere un portachiavi all'AX PRO e controllare l'AX PRO tramite il portachiavi. Puoi anche

modificare le informazioni del portachiavi o cancellare il portachiavi dall'AX PRO.

Passi

1. Clicca su **Dispositivo** → **Portachiavi** per entrare nella pagina di gestione dei portachiavi.
2. Fare clic su **Aggiungi** e premere un tasto qualsiasi del portachiavi.
3. Impostare i parametri del portachiavi.

   Nome

   Personalizza un nome per il portachiavi.

   Impostazioni dei permessi

   Spunta diverse voci per assegnare i permessi.

   Impostazioni del tasto singolo

   Selezionare dall'elenco a discesa per impostare le funzioni dei tasti I e II

   Impostazioni dei tasti combinati

   Selezionare dall'elenco a discesa per impostare le funzioni dei tasti combinati.

4. Fare clic su **OK**.
5. Opzionale: Clicca per modificare le informazioni del portachiavi.
6. Opzionale: Elimina un singolo portachiavi o controlla più portachiavi e clicca su **Elimina** per eliminare i portachiavi in batch.

Nota

La comunicazione dei dispositivi wireless come il keyfob è stata identificata dal numero SN, che sarà criptato durante la trasmissione. Il numero SN era preceduto da un carattere dalla Q alla Z, e seguito da 8 cifre, come Q02235774. permettendo un numero massimo di 100.000.000 (10 alla potenza di 8 [cifre]).

Aggiungi/modifica/cancella tag

È possibile aggiungere tag all'AX PRO ed è possibile utilizzare il tag per armare/disarmare la zona. Puoi anche modificare le informazioni del tag o cancellare il tag dall'AX PRO.

Nota

La comunicazione del tag è stata identificata dal numero SN, che sarà criptato durante la trasmissione. Il numero SN era composto da 32 cifre, e ci sono al massimo 4.294.967.296 numeri SN che possono essere identificati.

Passi

1. Fare clic su **Dispositivo** → **Tag** per entrare nella pagina di gestione.
2. Clicca su **Add** e inserisci un Tag nell'area Tag di AX PRO.
3. Personalizza un nome per il Tag nella finestra pop-up.

4. Seleziona il tipo di tag e l'area collegata al tag.
5. Seleziona il permesso per il Tag.

Nota

Dovreste assegnare almeno un permesso per il Tag.

6. Clicca su **OK** e le informazioni del tag saranno visualizzate nell'elenco.

Nota

Il Tag supporta almeno 20.000 numeri di serie.

7. Opzionale: Clicca e puoi cambiare il nome del tag.
8. Opzionale: Elimina un singolo tag o seleziona più tag e clicca su **Elimina** per eliminare i tag in batch.

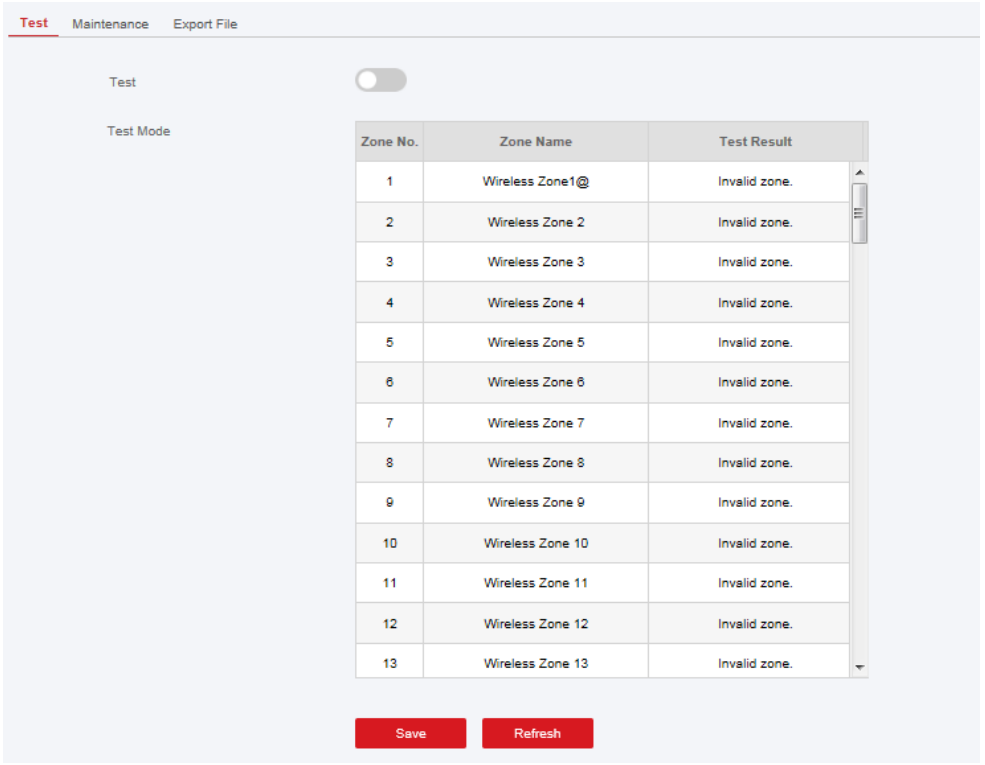
4.3.6 Manutenzione

Test

L'AX PRO supporta la funzione walk test.

Passi

1. Entrare in **Project Management** →Maintain →Test → per abilitare la funzione.



Nota
Solo quando tutti i rilevatori sono senza guasti, si può entrare nel modo TEST.

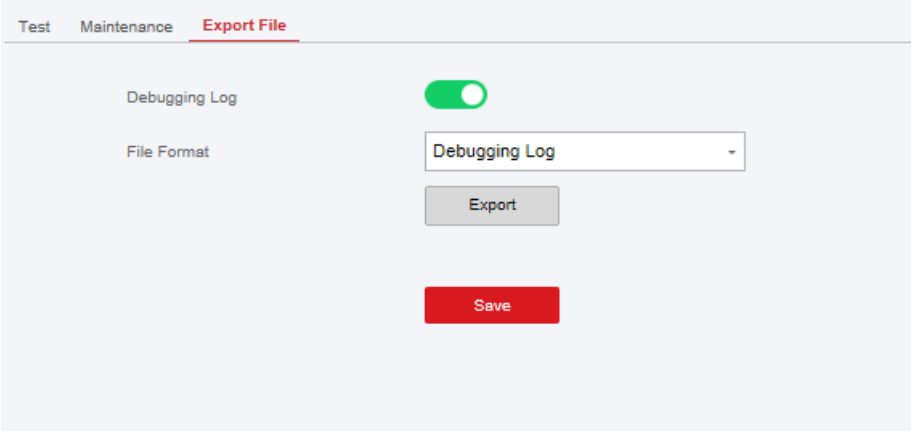
2. Seleziona la casella di controllo **Test** per avviare il walk test.
3. Clicca su **Salva** per completare le impostazioni.
4. Attivare il rilevatore in ogni zona.
5. Controllare il risultato del test.

Esportazione di file

È possibile esportare il file di debug sul PC.

Passi

1. Fare clic su **Manutenzione** → **Esporta file** per entrare nella pagina.

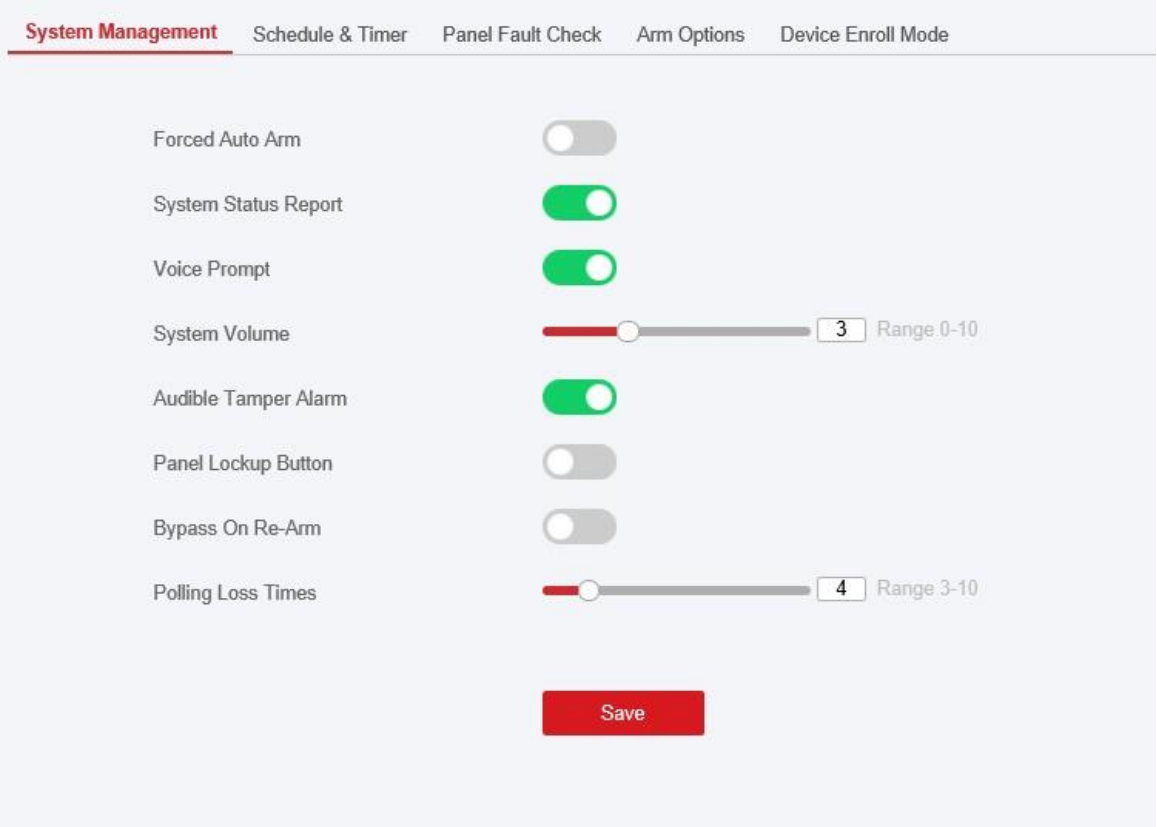


2. Selezionate la casella di controllo per abilitare la funzione.
3. Clicca su **Export** per salvare il file di debug nel PC.

4.3.7 Impostazioni di sistema

Gestione dell'autorità

Imposta le opzioni di autorità.
Fare clic su **Sistema** → **Opzioni di sistema** → **Gestione del sistema** per entrare nella pagina di gestione delle opzioni di sistema.



Braccio automatico forzato

Se l'opzione è abilitata e ci sono guasti attivi in una zona, la zona sarà bypassata automaticamente all'attivazione.

Nota

Si dovrebbe disabilitare la funzione di armatura nella pagina delle impostazioni avanzate. O l'armatura AX PRO con funzione di guasto non può essere valida.

Rapporto sullo stato del sistema

Se l'opzione è attivata, il dispositivo caricherà automaticamente il report quando lo stato di AX PRO viene modificato.

Prompt vocale

Se l'opzione è attivata, l'AX PRO abiliterà la richiesta vocale di testo.

Volume del sistema

L'intervallo di volume del sistema disponibile va da 0 a 10.

Allarme anti-manomissione udibile

Se abilitato, il sistema avviserà con un buzzer per l'allarme di manomissione.

Pulsante di blocco del pannello

Abilita/disabilita il pulsante di blocco del pannello di controllo.

Bypass al riarmo

Quando è abilitato, la zona con il guasto sarà bypassata automaticamente quando si riarma.

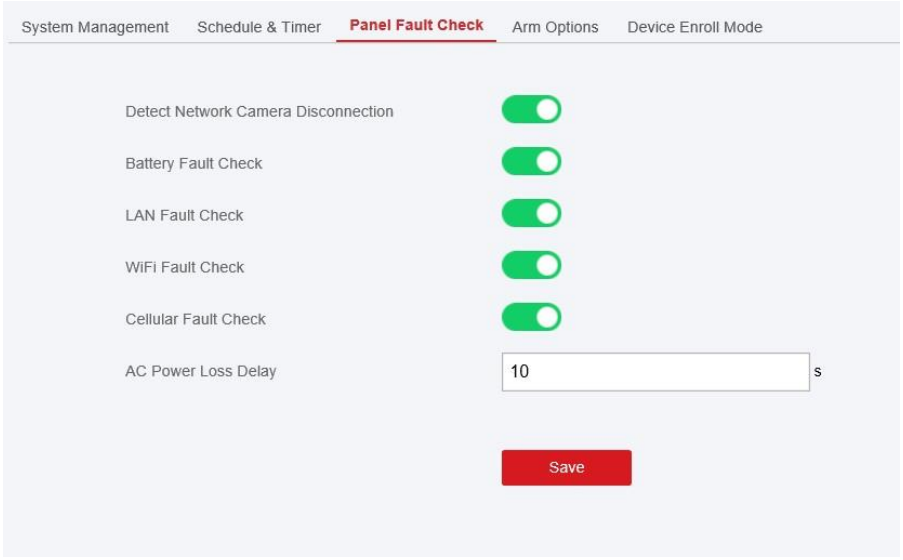
Tempi di perdita dei sondaggi

Impostare la durata massima della perdita di polling. Il sistema segnalerà un errore se la durata è superiore al limite.

Controllo dei guasti

Il sistema determina se controllare i guasti elencati nella pagina. Il sistema controllerà solo il guasto selezionato.

Fare clic su **Sistema** → **Opzioni di sistema** → **Controllo** dei guasti per entrare nella pagina.



Rileva la disconnessione della telecamera di rete

Se l'opzione è attivata, quando la telecamera di rete collegata viene scollegata, viene attivato un allarme.

Controllo del guasto della batteria

Se l'opzione è attivata, quando la batteria è scollegata o senza carica, il dispositivo caricherà gli eventi.

Controllo guasti LAN

Se l'opzione è abilitata, quando la rete cablata è scollegata o con altri guasti, l'allarme scatta.

Controllo del guasto Wi-Fi

Se l'opzione è abilitata, quando il Wi-Fi è scollegato o con altri guasti, l'allarme verrà attivato.

Controllo dei guasti della rete cellulare

Se l'opzione è attivata, quando la rete dati cellulare è scollegata o con altri guasti, il

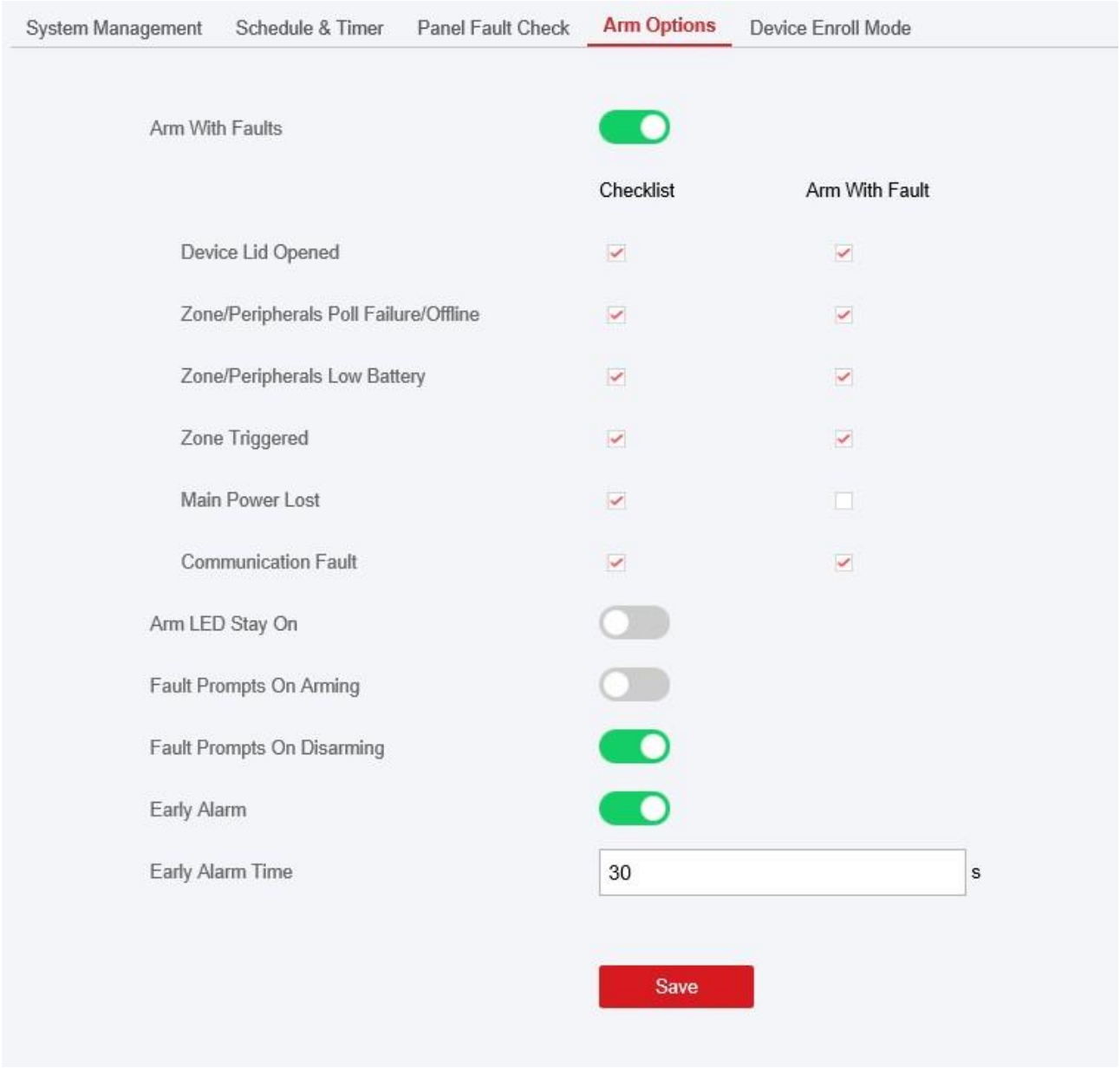
verrà attivato l'allarme.

Ritardo della perdita di potenza AC

Il sistema controlla il guasto dopo la durata di tempo configurata dopo lo spegnimento della corrente. Per soddisfare la norma EN 50131-3, la durata del tempo di controllo dovrebbe essere di 10 s.

Opzioni del braccio

Imposta i parametri avanzati dell'autorità.
Fare clic su **Sistema** → **Opzioni di sistema** → **Opzioni di sistema** per entrare nella pagina delle impostazioni avanzate.



Potete impostare i seguenti parametri:

Abilitare l'armamento con il guasto

Controllare i guasti nell'elenco Enable Arming with Fault, e il dispositivo non interromperà la procedura di armamento quando si verificano dei guasti.

Lista di controllo dei guasti

Il sistema controllerà se il dispositivo ha i difetti nella lista di controllo durante la procedura di armamento.

Il LED del braccio rimane acceso

Se il dispositivo applica lo standard EN, per default, la funzione è disabilitata. In questo caso, se il dispositivo è armato, l'indicatore sarà blu fisso per 5 s. E se il dispositivo è disarmato, l'indicatore lampeggerà 5 volte.
Quando la funzione è abilitata, se il dispositivo è armato, l'indicatore sarà sempre acceso. E se il dispositivo è disarmato, l'indicatore sarà spento.

Prompt di guasto all'attivazione/disattivazione

Se il dispositivo applica lo standard EN, per default, la funzione è disabilitata. In questo caso, l'apparecchio non segnalerà i guasti durante la procedura di inserimento/disinserimento.

Abilitare l'allarme precoce

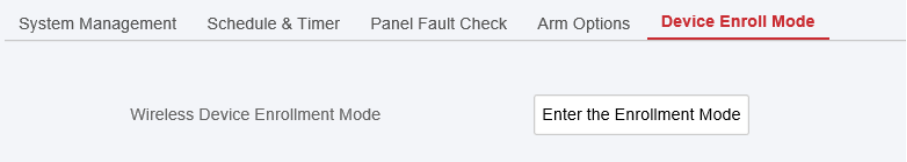
Se abilitate la funzione, quando la zona è armata e la zona è attivata, l'allarme scatterà dopo il tempo di ritardo impostato.

Nota

L'allarme anticipato avrà effetto solo dopo l'attivazione della zona ritardata.

Modalità di iscrizione del dispositivo

Clicca su Enter the Enrollment Mode per far entrare il pannello nella modalità di iscrizione.

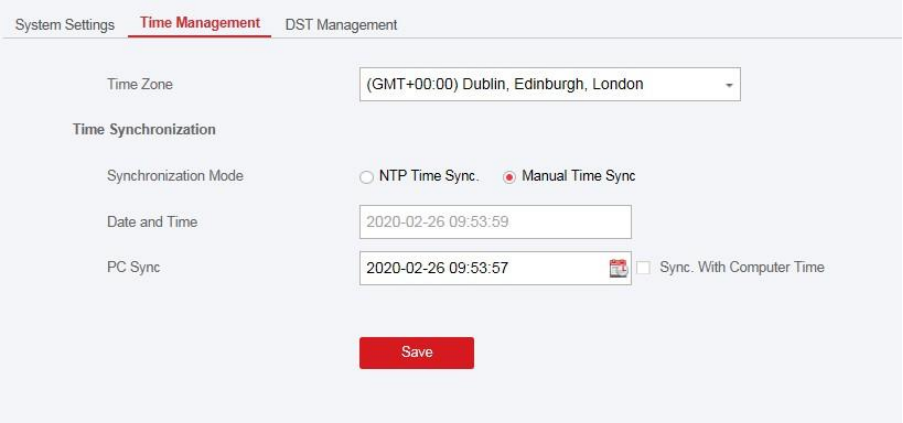


Impostazioni del tempo

È possibile impostare il fuso orario del dispositivo, sincronizzare l'ora del dispositivo e impostare l'ora legale. Il dispositivo supporta la sincronizzazione dell'ora tramite il server **Hik-Connect Guarding Vision.**

Gestione del tempo

Fare clic su **Sistema** → **Impostazioni di sistema** → **Ora** per entrare nella pagina di gestione dell'ora.



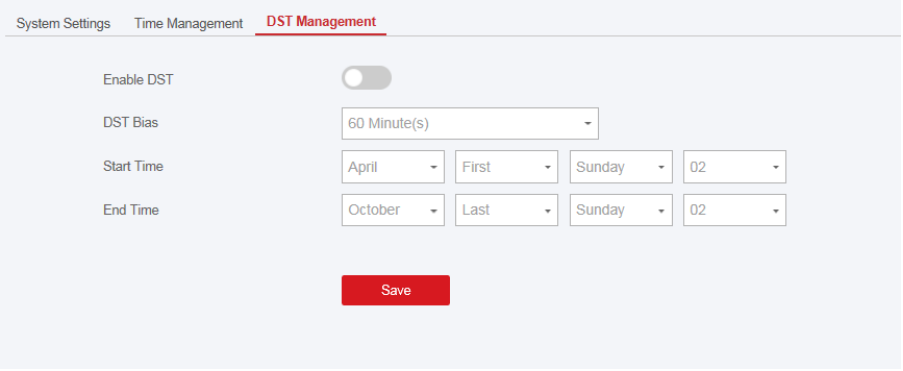
Puoi selezionare un fuso orario dall'elenco a discesa.
È possibile sincronizzare l'ora del dispositivo manualmente con NTP. Selezionare la casella di controllo diNTP **Time Sync.** inserire l'indirizzo del server e il numero di porta e impostare l'intervallo di sincronizzazione.
È possibile sincronizzare l'ora del dispositivo manualmente. Oppure selezionaSync**. with Computer Time** per sincronizzare l'ora del dispositivo con quella del computer.

Nota

Mentre si sincronizza l'ora manualmente o con quella del computer, il sistema registra il registro "SDK Synchronization".

Gestione DST

Fare clic su **Sistema** → **Impostazioni di sistema** → **Gestione DST** per entrare nella pagina di gestione dell'orario.

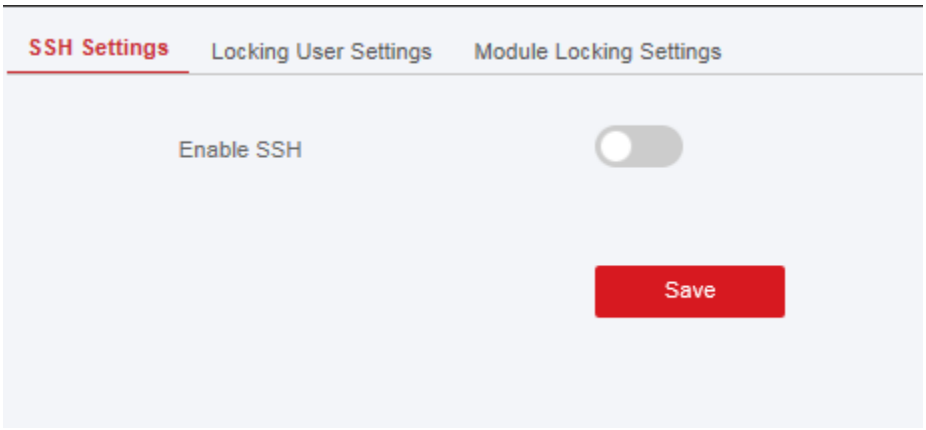


È possibile abilitare il DST e impostare la distorsione DST, l'ora di inizio DST e l'ora di fine DST.

Impostazioni di sicurezza

Impostazioni SSH

Abilita o disabilita SSH (Secure Shell) in base alle tue esigenze reali.
Fare clic su **Sistema** → **Sicurezza del sistema→ Impostazioni SSH** per entrare nella pagina delle impostazioni SSH e si può abilitare o disabilitare la funzione SSH.



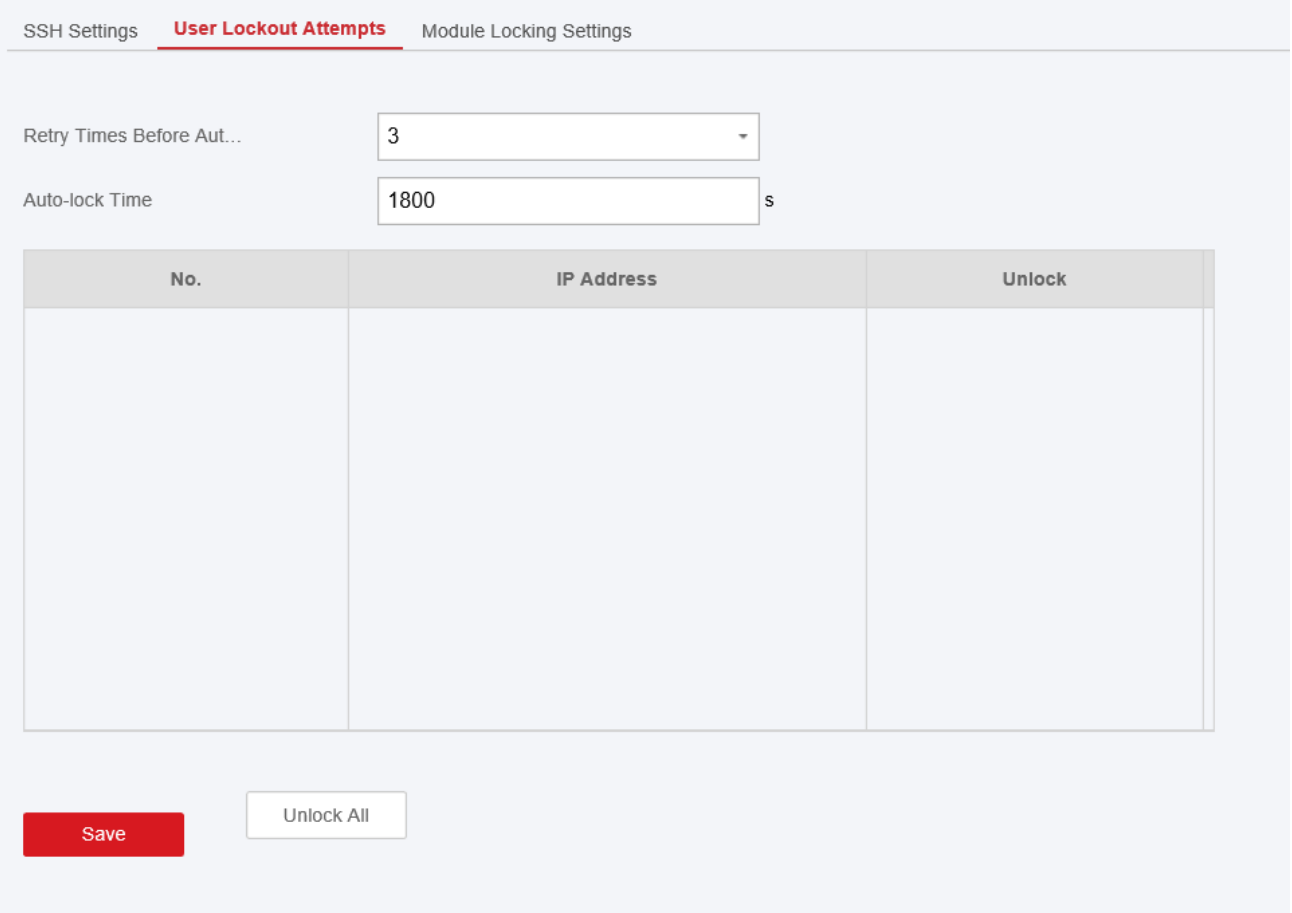
Bloccare le impostazioni dell'utente

Il dispositivo sarà bloccato 90 s dopo 3 tentativi di credenziali falliti (può essere impostato in Retry Time before Auto-Lock) in un minuto.
È possibile visualizzare l'utente bloccato o sbloccare un utente e impostare la durata del blocco dell'utente.

Nota
Per soddisfare il requisito EN, il sistema registrerà lo stesso registro solo 3 volte continuamente.

Passi

1. Fare clic su **Sistema** → **Sicurezza del sistema** → **Tentativi di blocco dell'utente** per accedere alla pagina delle impostazioni di blocco dell'utente.



2. Impostare i seguenti parametri.

Tempi di ripetizione prima del blocco automatico

Se l'utente inserisce continuamente la password errata per più delle volte configurate, l'account verrà bloccato.

Nota

L'amministratore ha due tentativi in più rispetto al valore configurato.

Durata bloccata

Imposta la durata del blocco quando l'account è bloccato.

Nota

La durata di bloccaggio disponibile va da 5s a 1800s.

3. Clicca per sbloccare l'account o clicca su **Sblocca tutto** per sbloccare tutti gli utenti bloccati nell'elenco.
4. Fare clic su **Salva**.

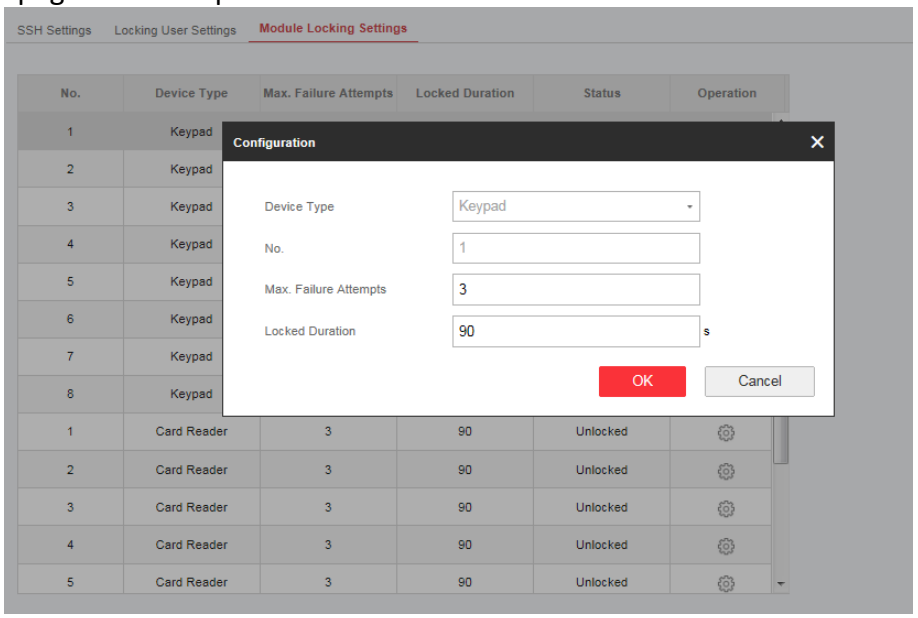
Impostazioni di blocco del modulo

Impostare i parametri di blocco del modulo, compresi i tentativi massimi di fallimento e la durata del blocco. Il

il modulo sarà bloccato per la durata di tempo programmata, una volta che l'autenticazione del modulo è fallita per il numero di volte configurato.

Passi

1. Fare clic su **Sistema** → **Sicurezza del sistema** → **Impostazioni di blocco del modulo** per accedere alla pagina delle impostazioni di blocco del modulo.



2. Selezionate un modulo dall'elenco e cliccate sull'the icona.
3. Impostare i seguenti parametri del modulo selezionato.

Max. Tentativi di fallimento

Se un utente cerca continuamente di autenticare una password per più dei tentativi configurati consentiti, la tastiera sarà bloccata per la durata programmata.

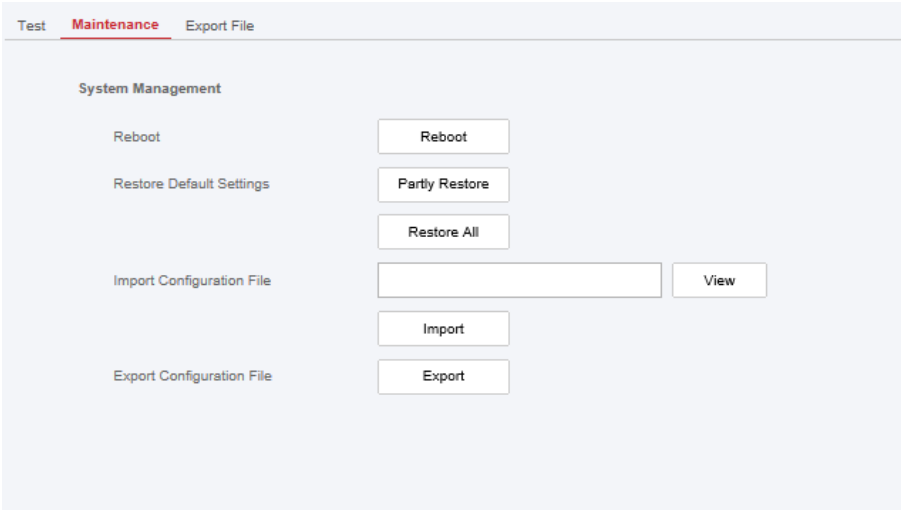
Durata bloccata

Impostare la durata del blocco quando la tastiera è bloccata. Dopo la durata configurata, la tastiera sarà sbloccata.

4. Fare clic su **OK**.
5. Opzionale: Fai clic sull'icona di **blocco** per sbloccare il modulo bloccato.

Manutenzione del sistema

È possibile riavviare il dispositivo, ripristinare le impostazioni predefinite, importare/esportare il file di configurazione o aggiornare il dispositivo da remoto.
Selezionare il dispositivo e cliccare barra degli indirizzi del browser web. Fare clic su **Project Management** →Manutenzione per entrare nella pagina di aggiornamento e manutenzione.



Riavvio

Clicca su **Reboot** per riavviare il dispositivo.

Ripristinare le impostazioni predefinite

Fare clic su **Partly Restore (Ripristina parzialmente)** per ripristinare tutti i parametri tranne le informazioni dell'utente amministratore, la rete cablata, la rete Wi-Fi, le informazioni del rilevatore e le informazioni della periferica a quelle predefinite. Clicca su **Restore All (Ripristina tutto)** per ripristinare tutti i parametri alle impostazioni di fabbrica.

Importazione del file di configurazione

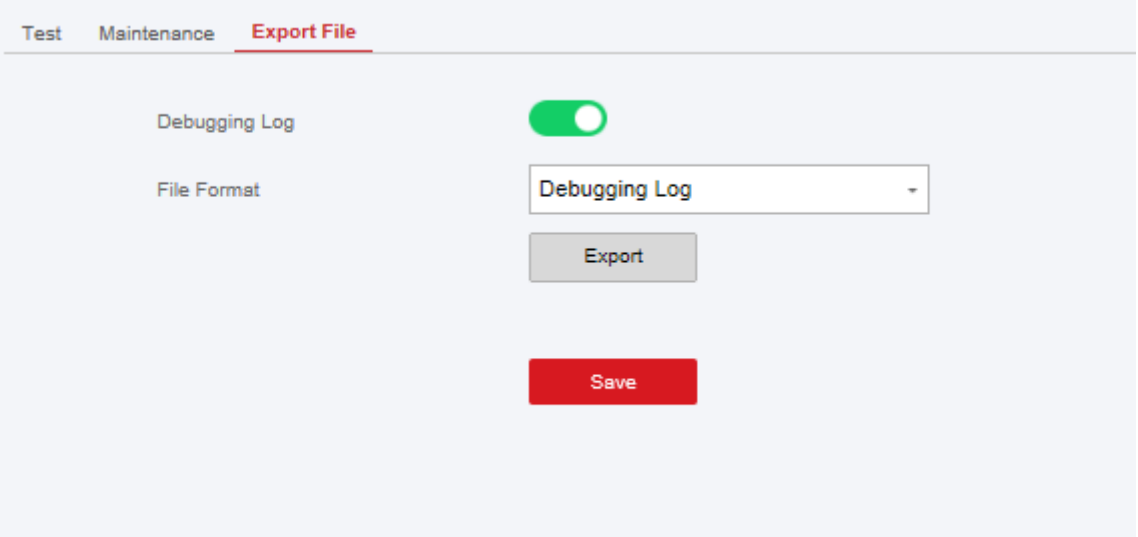
Fare clic su **View** per selezionare il file di configurazione dal PC e fare clic su **Import Configuration File** per importare i parametri di configurazione nel dispositivo. L'importazione del file di configurazione richiede l'inserimento della password impostata al momento dell'esportazione.

Esportazione del file di configurazione

Fare clic su **Export Configuration File** per esportare i parametri di configurazione del dispositivo sul PC. L'esportazione del file di configurazione richiede una password per la crittografia del file.

Esportazione di file

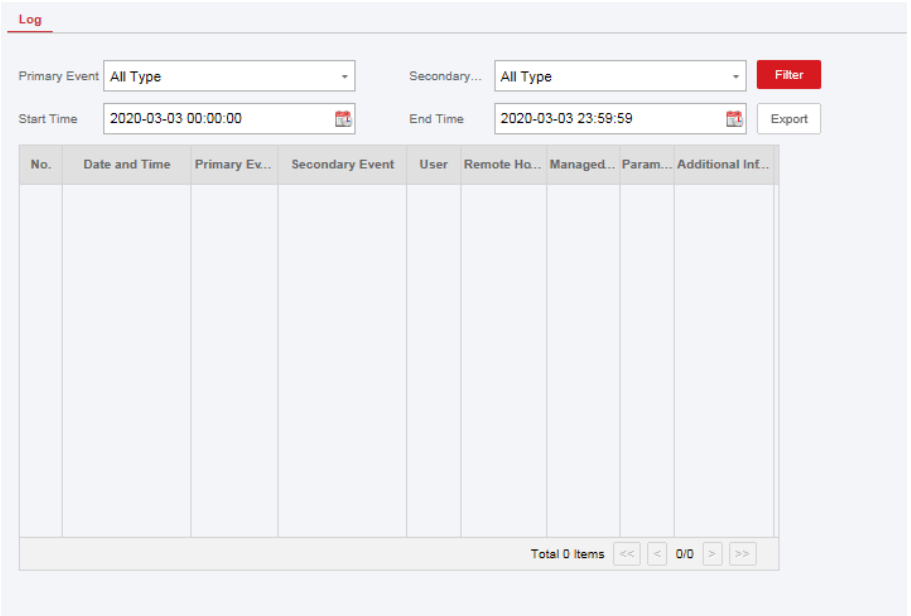
Fare clic su **Gestione progetto→ Mantenimento→ Esportazione file**
Enable **Debugging Log** per abilitare la funzione.



Seleziona il tipo di file da esportare.
Clicca su Export per esportare il file.

Ricerca del registro locale

È possibile cercare il registro sul dispositivo.
Fare clic su **Gestione progetto→ Registro** per accedere alla pagina di ricerca del registro locale.



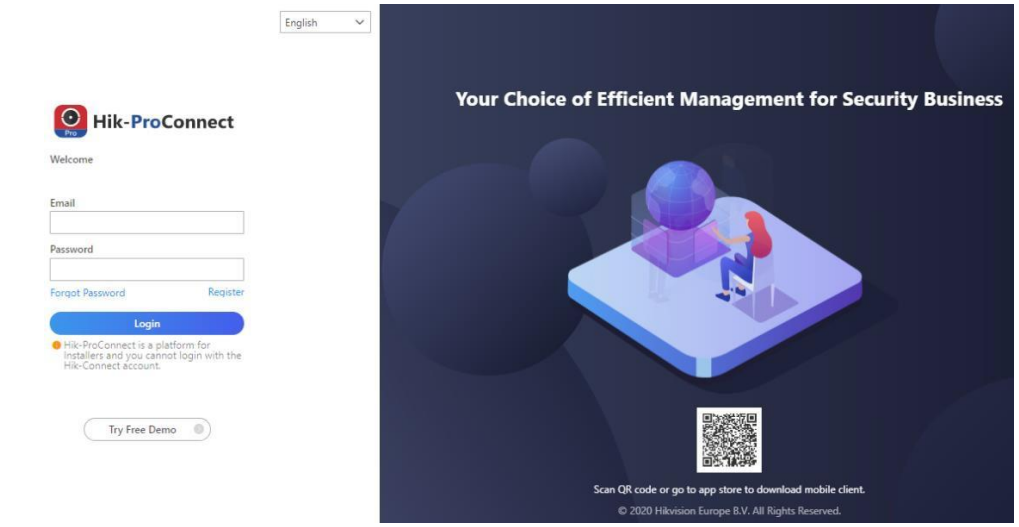
Seleziona un tipo principale e un tipo minore dall'elenco a discesa, imposta l'ora di inizio e di fine del registro e fai clic su **Filter**. Tutte le informazioni di registro filtrate verranno visualizzate nell'elenco.
Puoi anche cliccare su **Reset** per resettare tutte le condizioni di ricerca.

Aggiornamento del dispositivo

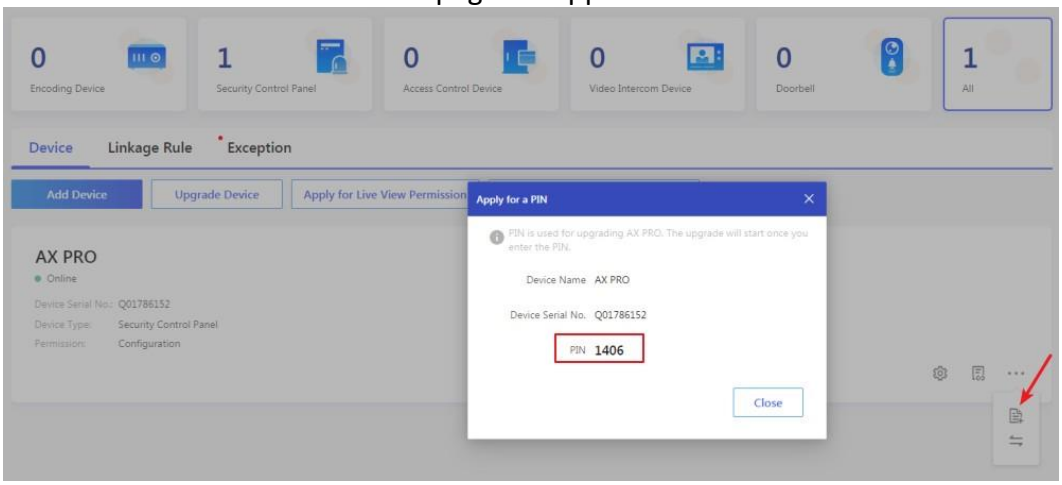
Ottieni il PIN di fabbricazione

Per aggiornare il dispositivo, è necessario un PIN di fabbricazione per l'autenticazione. Il PIN di fabbricazione può essere ottenuto solo dal servizio Hik-ProConnect, il che significa che l'installatore, autorizzato dall'amministratore al livello di accesso 2, ha autorizzato l'accesso al livello 4. Il PIN di fabbricazione può funzionare solo una volta.

- **Ottenere il PIN dal servizio Hik-ProConnect**



Accedi con l'account dell'installatore ed entra nella pagina del dispositivo da aggiornare. Clicca su **Altro menu** in basso a destra della pagina e applica un PIN.



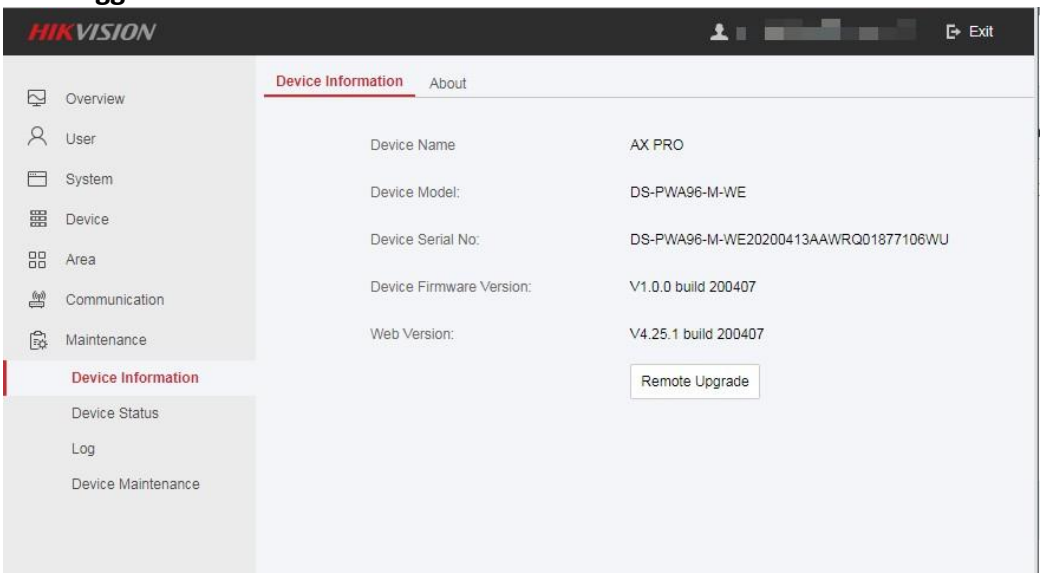
- **Ottieni il PIN dal supporto tecnico di HIKVISION**
  È meglio usare il desktop remoto per accedere al client web locale del pannello di controllo. Il PIN

sarà autorizzato secondo la procedura standard di supporto tecnico.

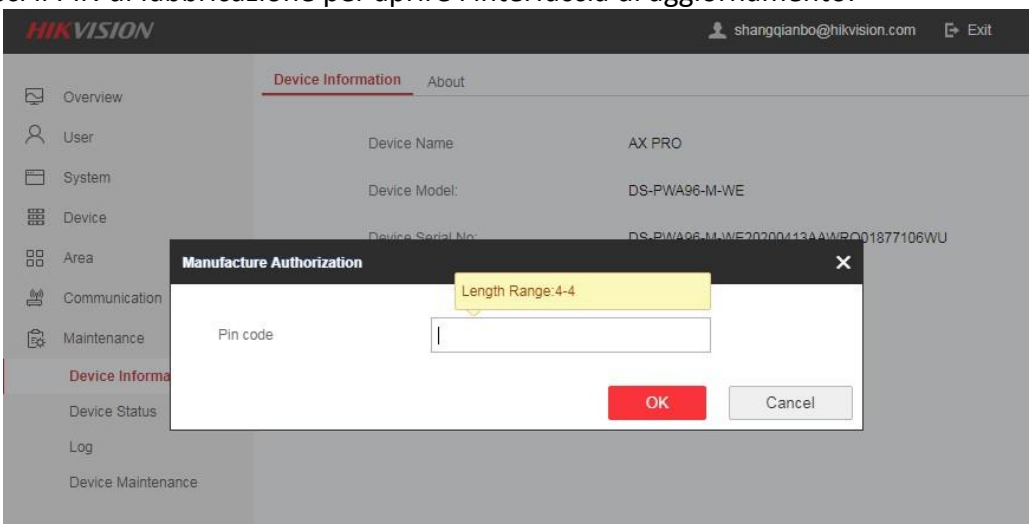
Aggiornamento del firmware

Passi:

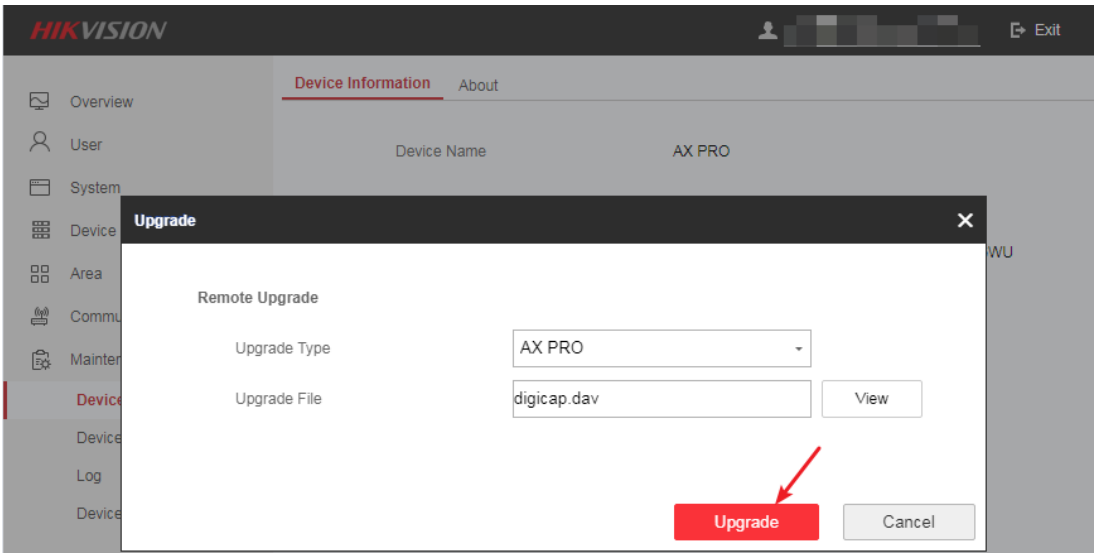
1. Fare clic su **Manutenzione→ Informazioni sul dispositivo** per entrare nella pagina.
2. Fate clic su **Aggiornamento remoto**.



3. Inserisci il PIN di fabbricazione per aprire l'interfaccia di aggiornamento.



4. Fare clic su **View** per trovare il file del firmware con il nome digicap.dav.
5. Clicca su **Upgrade** per completare.

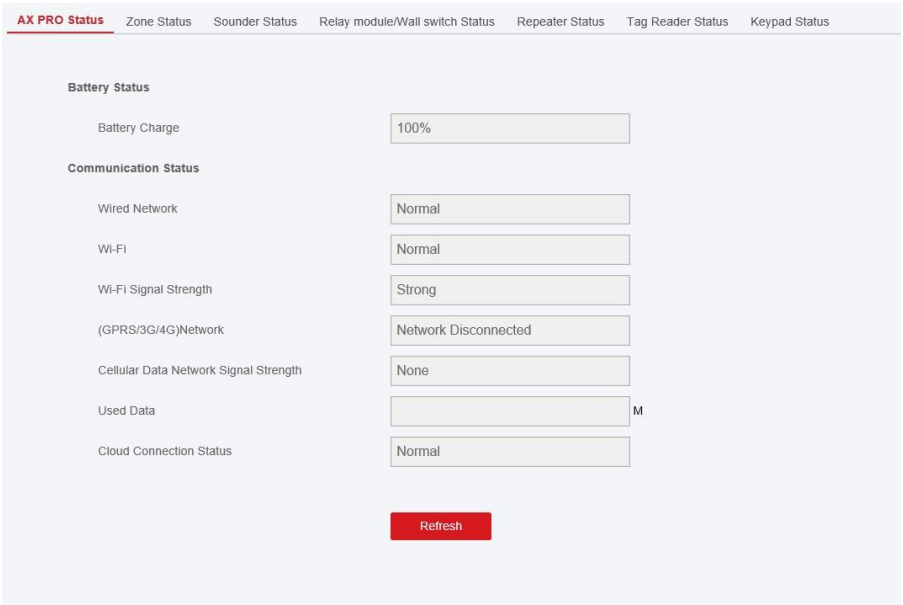


Nota

Entrambi gli utenti e le informazioni di configurazione saranno conservati dopo la fine dell'aggiornamento.

4.3.8 Controllare lo stato

Dopo aver impostato la zona, il ripetitore e altri parametri, è possibile visualizzare il loro stato. Fare clic su **Stato**. È possibile visualizzare lo stato di zona, relè, sirena, tastiera, lettore di tag, batteria e comunicazione.



- Zona: è possibile visualizzare lo stato della zona, lo stato dell'allarme, la capacità della batteria del rilevatore e la potenza del segnale.
- Sounder: È possibile visualizzare lo stato della sirena, lo stato della batteria e la potenza del segnale.
- Uscita: È possibile visualizzare lo stato del relè, lo stato della batteria e la potenza del segnale.
- Tastiera: È possibile visualizzare lo stato della tastiera, lo stato della batteria e la potenza del segnale.

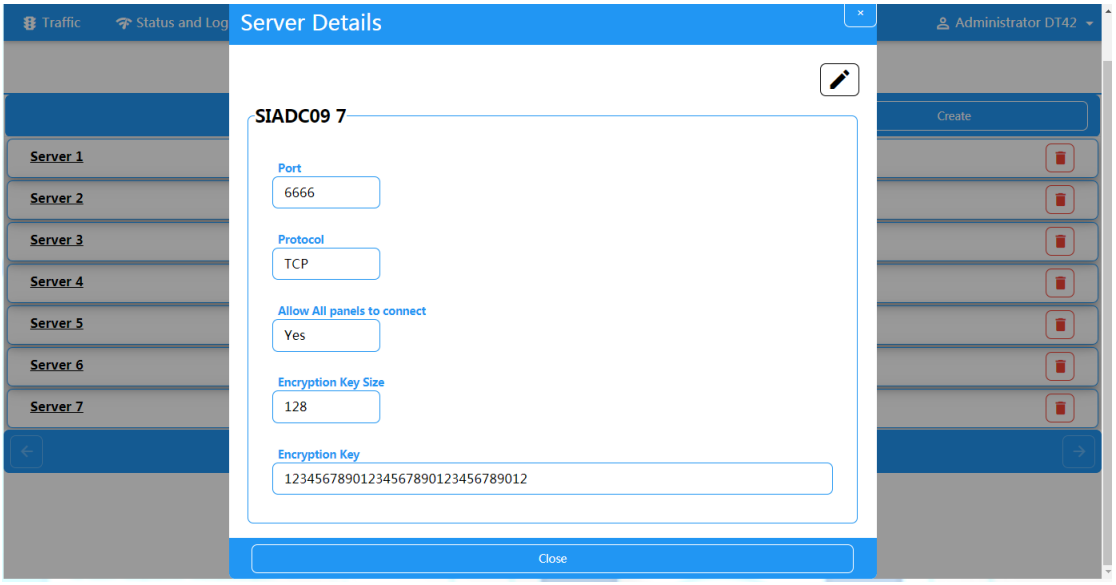
- Ripetitore: È possibile visualizzare lo stato di funzionamento del ripetitore.
- Lettore di tag: È possibile visualizzare lo stato del lettore di tag, lo stato della batteria e la potenza del segnale.

4.4 Rapporto all'ARC (Centro di Ricezione Allarmi)

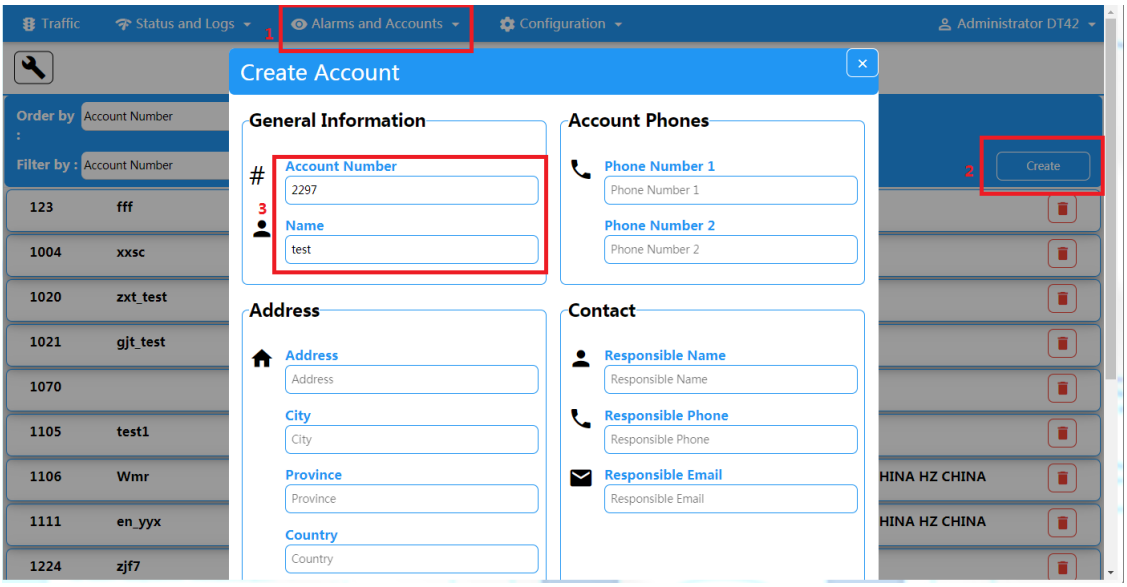
Il pannello di controllo wireless AX Pro è progettato con un ricetrasmettitore incorporato seguendo la guida della EN 50131-10 e della EN 50136-2. La categoria DP2 è dotata di un'interfaccia di rete primaria LAN/WiFi e di un'interfaccia di rete secondaria GPRS o 3G/4G LTE. ATS (Alarm Transmission system) è progettato per utilizzare sempre l'interfaccia di rete LAN/Wi-Fi quando disponibile per risparmiare l'utilizzo dei dati mobili. L'interfaccia di rete secondaria fornisce resilienza e affidabilità durante l'interruzione dell'alimentazione di rete.

Setup ATS nel ricetrasmettitore del centro ricevente Passi:

1. Accedi al client web del ricevitore d'allarme.
2. Fare clic su **Configurazione→ Ricezione IP** e creare un server di ricezione come mostrato di seguito.

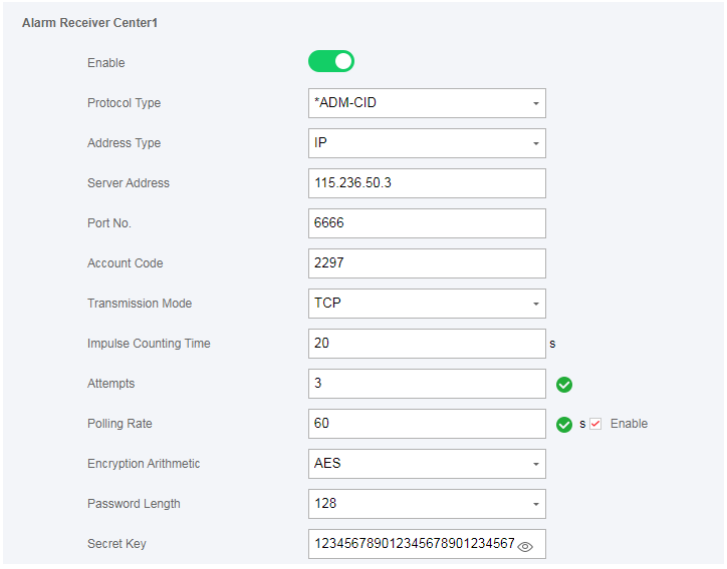


3. Fai clic su **Allarmi e account→ Gestione account** e assegna un account per il pannello come mostrato di seguito.



Setup ATS nel ricetrasmettitore dei passi del pannello:

1. Accedi usando l'account dell'installatore dal client web locale.
2. Cliccare su **Comunicazione→ Centro di Ricezione Allarmi (ARC)**, e abilitare il **Centro di Ricezione Allarmi 1**



= Impostazione del protocollo =

Tipo di protocollo

- ADM-CID
- SIA-DCS
- *ADM-CID
- *SIA-DCS

Selezionare il token supportato dal ricevitore nell'ARC. Scegli il token con il segno "*" per migliorare la sicurezza della comunicazione.

= Impostazione del server =

- ***Tipo di indirizzo***
  - IP
  - Nome di dominio
- ***Indirizzo del server / Nome di dominio***
- ***Porta No.***
  Inserire l'indirizzo IP o il nome del dominio con cui si può raggiungere il ricetrasmettitore del centro ricevente. Inserire il numero di porta del server fornito dall'ARC

= Impostazione dell'account =

- ***Codice del conto***
  Inserisci il conto assegnato fornito dall'ARC.

= Impostazione del protocollo SIA DC-09 =

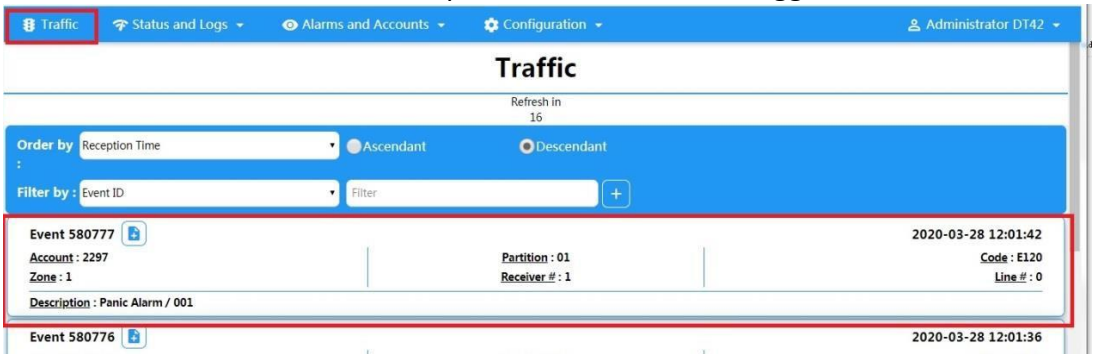
- ***Modalità di trasmissione***
  - TCP
  - UDP

  Sia TCP che UDP sono supportati per la trasmissione. UDP è raccomandato dallo standard SIA DC-09.
- ***Impostazione della connessione***
  - ***Tempo di conteggio degli impulsi / Periodo di timeout dei tentativi***
    Impostare il periodo di timeout in attesa della risposta del ricevitore. La ritrasmissione sarà organizzata se il ricetrasmettitore del centro ricevente è in timeout.
  - ***Tentativi***
    Impostare il numero massimo di tentativi di ritrasmissione.
  - ***Tasso di scrutinio***
    Impostare l'intervallo tra 2 polling live se l'abilitazione è selezionata.
- ***Impostazione della crittografia***
  - ***Crittografia aritmetica***
    -AES
  - ***Lunghezza della password***
    —128
    —192
    —256
  - ***Chiave segreta***
    Impostare la lunghezza della chiave di crittografia e inserire la chiave fornita dall'ARC.

Test di segnalazione

Attivare un allarme di panico dal pannello di controllo.

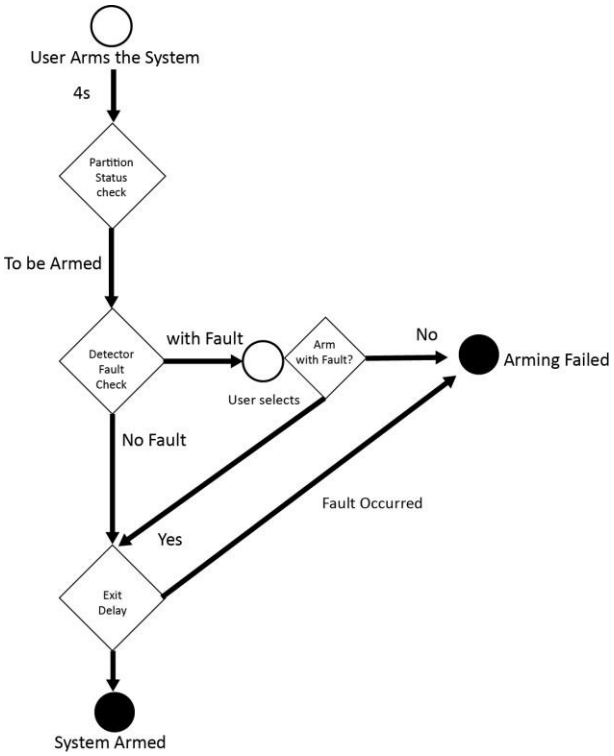
Accedere al Ricevitore. Clicca su **Traffico** per rivedere tutti i messaggi ricevuti.



Capitolo 5 Operazioni generali

5.1 Armare

Puoi usare la tastiera, il portachiavi, il Tag, il software client, il client mobile per armare il tuo sistema.
Dopo l'invio del comando di armamento ad AX PRO, il sistema controllerà lo stato del rilevatore.
Se il rivelatore è in guasto, dovrai scegliere se armare il sistema con guasto.
Mentre il sistema è armato, l'AX PRO chiederà il risultato in 5s, e caricherà il rapporto di armatura.



Livello di accesso di Arming

L'utente nel livello 2 o 3 ha il permesso di armare o armare parzialmente il sistema.

Indicazione di armamento

L'indicatore di attivazione/disattivazione rimane blu fisso per 5 secondi.

Motivo del fallimento dell'armamento

- Rilevatore di intrusione attivato (eccetto il rilevatore sul percorso di uscita).
- Dispositivo di allarme antipanico attivato.
- Si è verificato un allarme di manomissione.
- Eccezione di comunicazione
- Eccezione all'alimentazione principale

- Eccezione per la batteria di riserva
- Guasto di ricezione dell'allarme
- Guasto del sonar
- Batteria scarica del portachiavi
- Altri

Armare con il guasto

Mentre l'armatura è interrotta per guasto, l'utente nel livello 2 ha il permesso di armare il sistema per guasto (armatura forzata).
L'attivazione forzata ha effetto solo sull'operazione di attivazione in corso. L'operazione di armamento forzato sarà registrata nel registro eventi.

5.2 Disarmare

È possibile disarmare il sistema con la tastiera, il portachiavi, il Tag, il software client o il client mobile.

Indicazione di disarmo

L'indicatore di attivazione/disattivazione lampeggia per 30s mentre l'utente disarma con successo il sistema attraverso il percorso di entrata/uscita.
Il sistema riporterà il risultato del disarmo al termine dell'operazione.

Durata del ritardo di entrata

Assicurarsi che il timer non sia più lungo di 45 secondi per essere conforme a EN50131-1.

Allarme precoce

Se l'allarme intrusione o manomissione si verifica sul percorso di entrata/uscita quando AX PRO si trova nello stato di ritardo di entrata, AX PRO entra nella modalità di allarme anticipato.
La durata dell'allarme anticipato può essere impostata (> 30s).
L'AX PRO segnalerà l'allarme solo se l'evento di allarme dura oltre la durata dell'allarme anticipato con l'aggiunta del ritardo di entrata.

5.3 Controllo SMS

È possibile controllare il sistema di sicurezza con SMS, e il comando è mostrato di seguito. Formato SMS per armare/disarmare/silenziare l'allarme:

{Comando} + {Tipo di operazione} + {Target}

Comando: 2 cifre, 00- disarmare, 01- armare lontano, 02- restare armato, 03- silenziare l'allarme Tipo di operazione: 1- Operazione di area
Obiettivo: Non più di 3 cifre, 0-Operazione per tutte le zone, 1-Operazione per la zona 1 (zona1), e il resto può essere dedotto dall'analogia.

A. Risoluzione dei problemi

A.1 Errore di comunicazione

A.1.1 Conflitto IP

Descrizione del guasto:
L'IP che il pannello ha acquisito o impostato automaticamente è lo stesso di altri dispositivi,
con conseguenti conflitti IP. Soluzione:
Cerca l'attuale IP disponibile tramite ping. Cambia l'indirizzo IP e accedi di nuovo.

A.1.2 La pagina web non è accessibile

Descrizione del guasto:
Utilizzare il browser per accedere alle pagine web e
visualizzare Inaccessibile. Soluzioni:
1. Controllare se il cavo di rete è allentato e se la rete del pannello è anormale.
2. La porta del pannello è stata modificata. Si prega di aggiungere una porta all'indirizzo web per un ulteriore accesso.

A.1.3 Hik-Connect è offline

Descrizione del guasto:
La pagina web mostra che l'Hik-Connect è offline.
Soluzione:
La configurazione di rete del pannello è un errore, incapace di accedere a extranet.

A.1.4 La telecamera di rete cade frequentemente

Descrizione del guasto:
Il sistema riporta più registri di eventi di disconnessione e connessione IPC.
Soluzione:
Controllare se la comunicazione di rete o la visualizzazione dal vivo della telecamera è corretta.

A.1.5 Impossibile aggiungere un dispositivo su APP

Descrizione del guasto:
Quando si usa APP per aggiungere dispositivi, viene richiesto che il dispositivo non riesce ad essere aggiunto, il dispositivo non può essere trovato, ecc.
Soluzione:

Controllare la pagina web: se l'Hik-Connect è offline.

A.1.6 Le informazioni sull'allarme non sono riportate su APP/4200/Alarm Center

Descrizione del guasto:
Dopo l'attivazione dell'allarme, l'app/4200/la centrale d'allarme non riceve il messaggio d'allarme.
Soluzione:
"Messaggio push" - "allarme e avviso antimanomissione" non è abilitato. Dovresti abilitare "allarme e avviso antimanomissione".

A.2 Esclusione reciproca di funzioni

A.2.1 Impossibile entrare in modalità di registrazione

Descrizione del guasto:
Fare clic sul tasto funzione del pannello e richiedere un
tasto non valido. Soluzione:
Il pannello è in modalità "Hotspot". Passa il pannello alla modalità "stazione", e poi prova di nuovo a entrare nella modalità di registrazione.

A.3 Guasto di zona

A.3.1 La zona è offline

Descrizione del guasto:
Visualizza lo stato delle zone che viene
visualizzato offline. Soluzione:
Controllare se il rilevatore segnala una sottotensione. Sostituire la batteria del rilevatore

A.3.2 Zona a prova di manomissione

Descrizione del guasto:
Visualizzare lo stato delle zone che visualizzano a
prova di manomissione. Soluzione:
Rendere il pulsante antimanomissione del rivelatore holden.

A.3.3 Zona innescata/errore

Descrizione del guasto:

Visualizzare lo stato delle zone che visualizzano
l'attivazione/il guasto. Soluzione:
Resettare il rilevatore.

A.4 Problemi durante l'armamento

A.4.1 Errore nell'armamento (quando il processo di armamento non viene avviato)

Descrizione del guasto:
Quando il pannello si sta armando, il prompt
arming non riesce. Soluzione:
Il pannello non abilita l'"inserimento forzato", e quando c'è un guasto nella zona, l'inserimento non riesce. Si prega di attivare l'abilitazione dell'armatura forzata o di ripristinare lo stato normale della zona.

A.5 Guasto operativo

A.5.1 Impossibile entrare nella modalità test

Descrizione del guasto:
Non è riuscito ad attivare la modalità test, con il messaggio
"Un errore nella zona". Soluzione:
Lo stato della zona, lo stato dell'allarme o l'alimentazione della zona sono anormali.

A.5.2 L'operazione di cancellazione dell'allarme sul pannello non produce il rapporto di cancellazione dell'allarme

Descrizione del guasto:
L'operazione di cancellazione dell'allarme sul pannello non produce il rapporto di cancellazione dell'allarme. Soluzione:
In assenza di allarme, non verrà caricato alcun rapporto per la cancellazione del braccio.

A.6 Mancata consegna della posta

A.6.1 Impossibile inviare la posta di prova

Descrizione del guasto:
quando si configurano le informazioni sulla posta, si clicca su "test inbox" e il prompt test fallisce.

Soluzione:
Configurazione errata dei parametri della mailbox. Si prega di modificare le informazioni di configurazione della mailbox, come mostrato nella tabella 1/1.

A.6.2 Impossibile inviare la posta durante l'uso

Descrizione del guasto:
Controlla il log delle eccezioni del pannello. C'è un "fallimento
nell'invio della posta". Soluzione:
Il server della casella di posta ha un accesso limitato. Accedi alla casella di posta per vedere se la casella è bloccata.

A.6.3 Impossibile inviare messaggi a Gmail

Descrizione del guasto:
La casella di posta del destinatario è Gmail. Fai clic su "Test Inbox" e il test di richiesta fallisce.
1. Google impedisce agli utenti di accedere a Gmail utilizzando applicazioni/dispositivi che non soddisfano i loro standard di sicurezza.
Soluzione:
Accedere al sito web (https://www.google.com/settings/security/lesssecureapps), e "avviare l'accesso all'applicazione non abbastanza sicura". Il dispositivo può inviare mail normalmente.
2. Gmail non rimuove l'autenticazione CAPTCHA.
Soluzione: Clicca sul link qui sotto, e poi clicca su
"continua"
(https://accounts.google.com/b/0/displayunlockcaptcha).

A.6.4 Impossibile inviare e-mail a QQ o Foxmail

Descrizione del guasto:
La casella di posta del destinatario è QQ o Foxmail. Clicca su "Test Inbox" e il test del prompt fallisce.
1. Account o password QQ errati.
Soluzione:
la password richiesta per il login dell'account QQ non è la password utilizzata per il login normale. Il percorso specifico è: Inserire l'account e-mail → dispositivo → account → per generare il codice di autorizzazione, e utilizzare il codice di autorizzazione come password di accesso.
2. Il permesso di accesso SMTP è necessario per aprire.

A.6.5 Impossibile inviare e-mail a Yahoo

Descrizione del guasto:
La casella di posta del destinatario è yahoo. Clicca su "test inbox" e il test di prompt fallisce.
1. Il livello di sicurezza della cassetta
postale è troppo alto. Soluzione:
Vai al tuo account di posta e attiva "l'accesso meno sicuro".

A.6.6 Configurazione della posta

Tabella A-1 Configurazione della posta

Tipo di posta	Server di posta	Porta SMTP	Protocolli supportati
Gmail	smtp.gmail.com	587	TLS/STARTTLS (TLS)
Outlook	smtp.office365.com	587	STARTTLS (TLS)
Hotmail	smtp.office365.com	587	STARTTLS (TLS)
QQ	smtp.qq.com	587	STARTTLS (TLSv1.2)
Yahoo	smtp.mail.yahoo.com	587	STARTTLS (TLSv1.2)
126	smtp.126.com	465	SSL/TLS
Sina	smtp.sina.com	25/465/587	SSL/TLS/STARTTLS (SSL/TLS)

Nota

Sulla configurazione della posta:

- Porta SMTPDi default usa la porta 25 senza crittografia, o usa la porta 465 se viene usato SSL/TLS. La porta 587 è usata principalmente per la modalità di protocollo STARTTLS.
  La modalità di protocollo STARTTLS che di solito è usata di default quando si seleziona TLS.
- Nome utentell nome utente di Outlook e Hotmail richiedono nomi completi, mentre altre e-mail richiedono un prefisso prima di @.

B. Tipi di ingresso

Tabella B-1 Tipi di ingresso

Tipi di ingresso	Operazioni
Zona istantanea	Il sistema si allarma immediatamente quando rileva un evento scatenante dopo che il sistema si è armato. Risposta udibile: attiva il suono del sistema e il segnale acustico. Prompt vocale: Allarme zona X.
Zona perimetrale	Il sistema si allarma immediatamente quando rileva un evento scatenante dopo che il sistema si è armato. Risposta acustica: Attiva il suono del sistema e la sirena. C'è un intervallo configurabile tra l'allarme e l'uscita della sirena, che permette di controllare l'allarme e annullare l'uscita della sirena durante l'intervallo. Prompt vocale: Allarme perimetrale della zona X.
Zona ritardata	Il sistema vi dà il tempo di uscire o entrare nell'area di difesa senza allarme. Risposta acustica: Attiva il suono del sistema e il sounder. Prompt vocale: Allarme zona X.
Seguire la zona	La zona agisce come zona ritardata quando rileva l'evento di attivazione durante il ritardo di entrata del sistema, mentre altrimenti agisce come zona istantanea. Risposta acustica: Attiva il suono del sistema e il sounder. Prompt vocale: La zona X segue l'allarme.
Zona di silenzio 24H	La zona si attiva tutto il tempo senza alcun suono/uscita sonora quando si verifica l'allarme. Risposta udibile: Nessun suono di sistema (prompt vocale o sounder).
Zona di panico	La zona si attiva sempre. Risposta acustica: Attiva il suono del sistema e il sounder. Prompt vocale: Allarme panico zona X.
Zona del fuoco	La zona si attiva sempre con l'uscita del suono/suono quando si verifica l'allarme.

Tipi di ingresso	Operazioni
	Risposta acustica: Attiva il suono del sistema e il sounder. Prompt vocale: Allarme antincendio zona X.
Zona gas	La zona si attiva sempre con l'uscita del suono/suono quando si verifica l'allarme. Risposta acustica: Attiva il suono del sistema e il sounder. Prompt vocale: Allarme gas zona X.
Zona medica	La zona si attiva tutto il tempo con una conferma acustica quando si verifica l'allarme. Risposta acustica: Attiva il suono del sistema e il sounder. Prompt vocale: Allarme medico della zona X.
Zona di timeout	La zona è sempre attiva. Il tipo di zona è usato per monitorare e segnalare lo stato "ATTIVO" di una zona, ma segnalerà e allarmerà questo stato solo dopo che il tempo programmato è scaduto (da 1 a 599) secondi.
Zona disabili	Gli allarmi non saranno attivati quando la zona viene attivata o manomessa. Risposta udibile: Nessun suono di sistema (prompt vocale o sounder).
Zona virtuale (Tastiera/Telecomando)	Il sistema si allarma immediatamente quando rileva un evento scatenante dopo che il sistema si è armato. Risposta acustica: Attiva il suono del sistema e il sounder. Prompt vocale: Il cicalino emette un segnale acustico.
Allarme antimanomissione	Il sistema si allarma immediatamente quando rileva un evento scatenante dopo che il sistema si è armato. Risposta acustica: Attiva il suono del sistema e il sounder. Prompt vocale: Zona X manomessa.
Link	Attiva il dispositivo collegato quando si verifica un evento. Ad esempio, i relè collegati all'espansione delle uscite saranno abilitati quando AX PRO è armato.
Braccio	Quando è armato: Messaggio vocale per il guasto. È possibile gestire il guasto in base al messaggio vocale. ● Suono di sistema per armare con Tag o portachiavi. ● Messaggio vocale per il guasto. Potete gestire il guasto secondo la richiesta vocale.

L'evento di guasto viene visualizzato sul client. È possibile gestire il guasto tramite il software client o il client mobile.

Prompt vocale: Armed/Arming failed.

C. Tipi di uscita

Tabella C-1 Tipi di uscita

Tipi di uscita	Attivo	Ripristinare
Armare	Armare l'AX PRO	Dopo il ritardo di uscita configurato
Disarmare	Disattivare l'AX PRO	Dopo il ritardo di uscita configurato
Allarme	Quando si verifica un evento di allarme. L'uscita di allarme sarà attivata dopo il ritardo di uscita/entrata configurato.	Dopo il ritardo di uscita configurato, disarmare l'AX PRO o silenziare l'allarme
Collegamento di zona	Quando si verifica un evento di allarme, il relè collegato emette un segnale di allarme.	Dopo la durata di uscita configurata
Funzionamento manuale	Abilitare i relè manualmente	Sopra il tempo di attivazione o disabilitare i relè manualmente

D. Tipi di eventi

Tabella D-1 Tipi di eventi

Tipi di eventi	Personalizzato	Predefinito 1 (notifica del software client)	Default 2 (centro di ricezione allarmi 1/2)	Default 3 (client mobile)	Default 4 (telefono)
Allarme e manomissione	×/√	√	√	√	√
Evento per la sicurezza della vita	×/√	√	√	√	√
Stato del sistema	×/√	√	×	×	×
Gestione del pannello	×/√	√	×	×	×

E. Livelli di accesso

Livello	Descrizione
1	Accesso da parte di qualsiasi persona; per esempio il pubblico in generale.
2	User access by an operator and administrator; for example customers (systems users).
3	User access by an installer; for example an alarm company professional.

Table E-1 Permission of the Access Level

Function	Permission		
	1	2	3
Armare	No	Yes	Yes
Disarmare	No	Yes	Yes
Restoring/Clearing Alarm	No	Yes	Yes
Entering Walk Test Mode	No	Yes	Yes
Bypass(zone)/Disabling/Force Arming	No	Yes	Yes
Adding/Changing Verification Code	No	Yes[d]	Yes[d]
Adding/Editing Level 2 User and Verification Code	No	Yes	Yes
Adding/Editing Configuration Data	No	No	Yes
Replacing software and firmware	No	No	No

Nota

[a] By the condition of being accredited by user in level 2.

[b] By the condition of being accredited by user in level 2 and level 3.

[d] Users can only edit their own user code.

- The user level 2 can assign the login permission of the controller to the user level 3 in the settings page.
- The user level 2 should assign permissions to the user level 3 if the user level 3 wants to login the controller remotely.
- When the controller is bypassed, the user level 3 can login the controller without the permission assignment of the user level 2.

- When the controller is bypassed, the user level 3 can login the controller without the permission assignment of the user level 2.
- The user level 4 can login the controller only when the user level 2 or level 3 has assigned permissions to the user level 4.

F. Signalling

Detection of ATP/ATS Faults

ATP (Alarm Transmission Path) faults will be detected when network interface of the control panel disconnected or the transmission path to the transceiver of receiving center located in ARC blocked somewhere in between. An ATS (Alarm Transmission System) fault will be reported when ATP faults are detected on both transmission paths.
ATP restore will be detected as soon as network interface connected and the transmission path to the transceiver of receiving center restored. ATS restore will be reported when ATP restore of any transmission path is detected.

The timing performance of detecting ATP faults and restores shows in the table below.

	TN	Maximum timing of detection
Primary ATP failure/restore	LAN/WiFi	10 min
Secondary ATP failure/restore	GPRS	60 min
	3G/4G LTE	20 min (when primary ATP failed)

Signalling will be always transmitted from primary ATP when it is operational. Otherwise it will be automatically switched to secondary transmission path that is operational at the moment. Both primary and secondary ATP fault and restore events will be reported to ARC when there is an ATP left to work. They will also be recorded to mandatory log memory with capacity of 1000 records allocated in non-volatile flash memory storage, as well as the ATS fault record. The detail of reports and log records are listed in the table below.

	Event code when signalling	Event log description
Primary ATP failure/restore	E351/R351	LAN Path Failed/LAN Path Recovery
Secondary ATP failure/restore	E352/R352	Mobile Net Path Failed/Mobile Net Path Recovery
ATS failure/restore	N/A	ATS Failed
Primary network interface failure/restore	E351/R351	LAN Path Failed/LAN Path Recovery
Secondary network interface failure/restore	E352/R352	Mobile Net Path Failed/Mobile Net Path Recovery

ATS Category

The ATS category of AXPRO is DP2. While the alarm receiving center is enabled. The control panel will upload alarm report to the receiver center via the main path (LAN or Wi-Fi) or the back-up path (3G/4G). If the control panel is properly connected to the LAN or Wi-Fi, the main path is selected as the transmission path. If the main path connection is failed, the path will be switched to 3G/4G. And if the main path connection is restored, the path will be switched back to LAN or Wi-Fi. The control panel checks the connection status continuously, and generates logs transmission fault for any of the path. While both of the paths are invalid, the control panel determines ATS fault.

G. SIA and CID Code

Table F-1 SIA and CID Code

SIA Code	CID Code	Descrizione
MA	1100	Allarme medico
MH	3100	Medical Alarm Restored
BA	1130	Burglary Alarm
BH	3130	Burglary Alarm Restored
FA	1110	Fire Alarm
FH	3110	Fire Alarm Restored
HA	1121	Duress
HA	1122	Silent Panic Alarm
HH	3122	Silent Panic Alarm Restored
NA	1780	Timeout Alarm
BH	3780	Timeout Alarm Restored
PA	1120	Allarme antipanico
PH	3120	Panic Alarm Restored
BA	1133	24H Alarm
BH	3133	24H Alarm Restored
BA	1134	Entry/Exit Alarm
BH	3134	Entry/Exit Alarm Restored
TA	1137	Device Tampered
TR	3137	Device Tamper Restored
GA	1151	Gas Leakage Alarm
GH	3151	Gas Leakage Alarm Restored
AT	1301	AC Power Loss
AR	3301	AC Power Restored
YT	1302	Low System Battery
YR	3302	Low System Battery Restored
RN	1305	Control Panel Reset

SIA Code	CID Code	Descrizione
YM	1311	Battery Fault
YR	3311	Battery Fault Restored
YI	1312	Overcurrent Protection Triggered
YJ	3312	Overcurrent Protection Restored
YP	1319	Overvoltage Protection Triggered
YQ	3319	Overvoltage Protection Restored
XT	1338	Repeater Battery Low
XR	3338	Repeater Battery Voltage Restored
AT	1342	Repeater Mains Power Lost
AR	3342	Repeater Mains Power Restored
YM	1311	Repeater Battery Disconnected
YR	3311	Repeater Battery Reconnected
ES (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	1341 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Expander Tampered
EJ (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	3341 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Expander Tamper Restored
TA	1334	Wireless Repeater Tampered
TR	3334	Wireless Repeater Tamper Restored
TA	1321	Wireless Siren Tampered
TR	3321	Wireless Siren Tamper Restored
UY	1321	Wireless Siren Disconnected

SIA Code	CID Code	Descrizione
UJ	3321	Wireless Siren Connected
ES (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	1341 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Wireless Device Tampered
EJ (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	3341 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Wireless Device Tamper Restored
XT	1338	Low Wireless Device Battery
XR	3338	Low Wireless Device Battery Restored
ET (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	1333 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Wireless Device Disconnected
ER (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	3333 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Wireless Device Connected
LT	1351	Main Channel ATP Fault
LR	3351	Main Channel ATP Restored
LT	1352	Backup Channel ATP Fault
LR	3352	Backup Channel ATP Restored
TA	1383	Detector Tampered
TR	3383	Detector Tamper Restored
OP	1401	Disarmare
CL	3401	Away Arming
OA	1403	Auto Disarming
CA	3403	Auto Arming
BC	1406	Alarm Clearing
1409	CS	Keyswitch Zone Disarming
3409	OS	Keyswitch Zone Arming

SIA Code	CID Code	Descrizione
CL	3441	Stay Arming
CT	1452	Tardivo al disarmo
CD	1455	Auto Arming Failed
BB	1570	Zone Bypassed
BU	3570	Zone Bypass Restored
RP	1602	Periodic Report Test
TS	1607	Test Mode Entered
TE	3607	Test Mode Exited
LB	1627	Enter Programming
LX	1628	Exit Programming
BA	1131	Intrusion Alarm
BH	3131	Intrusion Alarm Restored
BA	1131	Cross-Zone Alarm
BH	3131	Cross-Zone Alarm Restored
BA	1134	Region Entrance Detection
FA	1112	Fire Source Alarm
FH	3112	Fire Source Alarm Restored
KS	1158	High Temperature Pre-Alarm
KR	3158	High Temperature Pre-Alarm Restored
1159	ZS	Low Temperature Pre-Alarm
ZR	3159	Low Temperature Pre-Alarm Restored
KA	1158	High Temperature Alarm
KH	3158	High Temperature Alarm Restored
ZA	1159	Low Temperature Alarm
ZH	3159	Low Temperature Alarm Restored
EA	1134	Region Exiting Detection

SIA Code	CID Code	Descrizione
PA (For distinguishing the keypad, the user number of the keyfob starts from 901)	1120 (For distinguishing the keypad, the user number of the keyfob starts from 901)	Keypad/Keyfob Panic Alarm
FA	1110	Keypad/Keyfob Fire Alarm
CI	1454	Arming Failed
MA	1100	Keypad/Keyfob Medical Alarm
DK	1501	Keypad Locked
DO	3501	Keypad Unlocked
/	/	Tag Reader Locked
/	/	Tag Reader Unlocked
UY	1381	Wireless Detector Disconnected
UJ	3381	Wireless Detector Connected
XT	1384	Wireless Detector Low Battery
XR	3384	Normal Wireless Detector Battery
ET (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	1333 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Expander Disconnected
ER (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	3333 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Expander Connected
UY	1334	Wireless Repeater Disconnected
UJ	3334	Wireless Repeater Connected
XT	1384	Wireless Siren Low Battery
XR	3384	Normal Wireless Siren Battery
NT	1350	Cellular Data Network Disconnected
NR	3350	Cellular Data Network Connected

SIA Code	CID Code	Descrizione
NT	1350	Wi-Fi Communication Fault
NR	3350	Wi-Fi Connected
XQ	1344	RF Signal Exception
XH	3344	Normal RF Signal
NT	1350	Network Flow Exceeded
XT	1384	Low Keyfob Battery
XR	3384	Low Keyfob Battery Restored
NT	1350	IP Address Conflicted
NR	3350	Normal IP address
NT	1350	Wired Network Exception
NR	3350	Normal Wired Network
/	/	Sending Email Failed
/	/	Network Camera Disconnected
/	/	Network Camera Connected
/	3250	Patrol
/	1306	Detector Deleted
/	3306	Detector Added
/	1306	Expander Deleted
/	3306	Expander Added
/	1306	Wireless Repeater Deleted
/	3306	Wireless Repeater Added
/	1306	Wireless Siren Deleted
/	3306	Wireless Siren Added
/	1306	Wireless Device Deleted
/	3306	Wireless Device Added