Controller di accesso serie DS-K2800

Manuale d'uso

Manuale d'uso

© 2018 Hangzhou Hikvision Digital Technology Co., Ltd. Questo manuale si applica al controller di accesso.

nome del prodotto	Seriali
Accesso Controller	DS-K2801 Controller di accesso seriale
	DS-K2802 Controller di accesso seriale
	DS-K2804 Controller di accesso seriale

Include istruzioni su come utilizzare il prodotto. Il software incorporato nel Prodotto è regolato dal contratto di licenza dell'utente che copre tale Prodotto.

Di questo manuale

Questo manuale è soggetto alla protezione del copyright nazionale e internazionale. Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") si riserva tutti i diritti su questo manuale. Questo manuale non può essere riprodotto, modificato, tradotto o distribuito, parzialmente o totalmente, con alcun mezzo, senza previa autorizzazione scritta di Hikvision.

Marchi

HIKVISION e altri marchi Hikvision sono di proprietà di Hikvision e sono registrati marchi o oggetto di domande per gli stessi da parte di Hikvision e / o delle sue affiliate. Gli altri marchi citati in questo manuale appartengono ai rispettivi proprietari. Non viene concesso alcun diritto di licenza per utilizzare tali marchi senza espressa autorizzazione.

Disclaimer

NELLA MISURA MASSIMA CONSENTITA DALLA LEGGE VIGENTE, HIKVISION NON FORNISCE ALCUNA GARANZIA, ESPLICITA O IMPLICITA, INCLUSE SENZA LIMITAZIONI LE GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UN PARTICOLARE SCOPO, RIGUARDO A QUESTO MANUALE. HIKVISION NON GARANTISCE, GARANTISCE O FORNISCE ALCUNA DICHIARAZIONE RIGUARDANTE L'USO DEL MANUALE, O LA CORRETTEZZA, PRECISIONE O AFFIDABILITÀ DELLE INFORMAZIONI CONTENUTE IN QUESTO DOCUMENTO. L'UTILIZZO DI QUESTO MANUALE E QUALSIASI AFFIDAMENTO SU QUESTO MANUALE SARANNO COMPLETAMENTE A PROPRIO RISCHIO E RESPONSABILITÀ.

PER QUANTO RIGUARDA IL PRODOTTO CON ACCESSO A INTERNET, L'UTILIZZO DEL PRODOTTO DEVE ESSERE INTERAMENTE A PROPRIO RISCHIO. LA NOSTRA AZIENDA NON SI ASSUME ALCUNA RESPONSABILITÀ PER FUNZIONAMENTO ANOMALO, PERDITA DI PRIVACY O ALTRI DANNI RISULTANTI DA ATTACCO INFORMATICO, ATTACCO DI HACKER, ISPEZIONE DI VIRUS O ALTRI RISCHI PER LA SICUREZZA IN INTERNET; TUTTAVIA, LA NOSTRA AZIENDA FORNIRÀ PUNTUALMENTE SUPPORTO TECNICO SE NECESSARIO.

LE LEGGI SULLA SORVEGLIANZA VARIANO A SECONDA DELLA GIURISDIZIONE. SI PREGA DI CONTROLLARE TUTTE LE LEGGI RILEVANTI NELLA VOSTRA GIURISDIZIONE PRIMA DI UTILIZZARE QUESTO PRODOTTO PER ASSICURARVI CHE IL VOSTRO UTILIZZO SIA CONFORME ALLE LEGGI APPLICABILI. LA NOSTRA AZIENDA NON SARÀ RESPONSABILE NEL CASO IN CUI QUESTO PRODOTTO VENGA UTILIZZATO CON SCOPI ILLEGITTIMI.

IN CASO DI CONFLITTO TRA IL PRESENTE MANUALE E LA LEGGE VIGENTE, PREVEDE QUELLO SUCCESSIVO.

Supporto

In caso di domande, non esitare a contattare il rivenditore locale.

Informazioni sulla regolamentazione

Informazioni FCC

Fare attenzione che cambiamenti o modifiche non espressamente approvati dalla parte responsabile della conformità potrebbero annullare l'autorizzazione dell'utente a utilizzare l'apparecchiatura.

Conformità FCC: Questa apparecchiatura è stata testata ed è risultata conforme ai limiti per un dispositivo digitale di Classe B, ai sensi della 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 a 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 verificherà in una particolare installazione. Se questa apparecchiatura causa interferenze dannose alla ricezione radiofonica o televisiva, che possono essere determinate accendendo e spegnendo l'apparecchiatura, l'utente è incoraggiato a cercare di correggere l'interferenza adottando una o più delle seguenti misure:

- Riorientare o riposizionare l'antenna ricevente.
- Aumentare la distanza tra l'apparecchiatura e il ricevitore.
- Collegare l'apparecchiatura a una presa su un circuito diverso da quello a cui è collegato il ricevitore.
- Consultare il rivenditore o un tecnico radio / TV esperto per assistenza.

Condizioni FCC

Questo dispositivo è conforme alla parte 15 delle norme FCC. Il funzionamento è soggetto alle seguenti due condizioni:

1. Questo dispositivo non può causare interferenze dannose.
2. Questo dispositivo deve accettare qualsiasi interferenza ricevuta, incluse le interferenze che potrebbero causare un funzionamento indesiderato.

Dichiarazione di conformità UE

CE Questo prodotto e, se applicabile, anche gli accessori in dotazione sono contrassegnati con "CE" e pertanto sono conformi agli standard europei armonizzati applicabili elencati nella direttiva R & TTE 1999/5 / CE, nella direttiva EMC 2014/30 / UE, nella direttiva LVD 2014 / 35 / UE, la direttiva RoHS 2011/65 / UE.

2012/19 / UE (direttiva WEEE): i prodotti contrassegnati con questo simbolo non possono essere smaltiti come rifiuti urbani indifferenziati nell'Unione Europea. Per un corretto riciclaggio, restituire questo prodotto al fornitore locale al momento dell'acquisto di una nuova apparecchiatura equivalente o smaltirlo presso i punti di raccolta designati. Per ulteriori informazioni, vedere: www.recyclethis.info.

2006/66 / EC (direttiva sulle batterie): questo prodotto contiene una batteria che non può essere smaltita come rifiuto urbano indifferenziato nell'Unione Europea. Consultare 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 fornitore o a un punto di raccolta designato. Per ulteriori informazioni, vedere: www.recyclethis.info.

Conformità ICES-003 del Canada

Questo dispositivo soddisfa i requisiti degli standard CAN ICES-3 (A) / NMB-3 (A).

Suggerimenti preventivi e cautelativi

Prima di collegare e utilizzare il tuo dispositivo, tieni presente i seguenti suggerimenti:

- Assicurarsi che l'unità sia installata in un ambiente ben ventilato e privo di polvere.
- Tenere tutti i liquidi lontani dal dispositivo.
- Garantire che le condizioni ambientali soddisfino le specifiche di fabbrica.
- Assicurarsi che l'unità sia adeguatamente fissata a un rack o uno scaffale. Forti urti o scosse all'unità a seguito della sua caduta possono causare danni ai componenti elettronici sensibili all'interno dell'unità.
- Se possibile, utilizzare il dispositivo insieme a un UPS.
- Spegnere l'unità prima di collegare e scollegare accessori e periferiche.
- Per questo dispositivo deve essere utilizzato un HDD consigliato dalla fabbrica.

L'uso o la sostituzione impropria della batteria può comportare il rischio di esplosione. Sostituire solo con lo stesso tipo o equivalente. Smaltire le batterie usate secondo le istruzioni fornite dal produttore.

Istruzioni di sicurezza

Queste istruzioni hanno lo scopo di garantire che l'utente possa utilizzare il prodotto correttamente per evitare pericoli o perdite di proprietà.

La misura precauzionale è suddivisa in **Avvertenze** e **Precauzioni: Avvertenze:** La mancata osservanza di una qualsiasi delle avvertenze può causare lesioni gravi o morte.

Precauzioni: La mancata osservanza di una qualsiasi delle precauzioni può causare lesioni alle persone o danni alle apparecchiature.

	
Avvertenze Segui questi salvaguardie per prevenire lesioni gravi o morte.	**Precauzioni** Seguire questi precauzioni per prevenire potenziali lesioni o danni materiali.

 **Avvertenze**

- Tutte le operazioni elettroniche devono essere rigorosamente conformi alle norme sulla sicurezza elettrica, alle norme sulla prevenzione degli incendi e ad altre normative correlate nella regione locale.
- Si prega di utilizzare l'adattatore di alimentazione, fornito dalla normale azienda. Il consumo energetico non può essere inferiore al valore richiesto.
- Non collegare più dispositivi a un alimentatore poiché il sovraccarico dell'adattatore può causare surriscaldamento o rischio di incendio.
- Assicurarsi che l'alimentazione sia stata scollegata prima di cablare, installare o smontare il dispositivo.
- Quando il prodotto è installato a parete o soffitto, il dispositivo deve essere fissato saldamente.
- Se il dispositivo emette fumo, odori o rumore, spegnere immediatamente l'alimentazione e scollegare il cavo di alimentazione, quindi contattare il centro di assistenza.
- Se il prodotto non funziona correttamente, contattare il rivenditore o il centro di assistenza più vicino. Non tentare mai di smontare il dispositivo da soli. (Non ci assumiamo alcuna responsabilità per problemi causati da riparazioni o manutenzioni non autorizzate.)

 **Precauzioni**

- Non far cadere il dispositivo né sottoporlo a shock fisici e non esporlo a radiazioni elettromagnetiche elevate. Evitare l'installazione dell'apparecchiatura su superfici soggette a vibrazioni o luoghi soggetti a urti (l'ignoranza può causare danni all'apparecchiatura).
- Non posizionare il dispositivo in luoghi estremamente caldi (fare riferimento alle specifiche del dispositivo per la temperatura di funzionamento dettagliata), in luoghi freddi, polverosi o umidi e non esporlo a radiazioni elettromagnetiche elevate. La temperatura di funzionamento appropriata è 0 ℃ a +45 ℃, e la temperatura di conservazione dovrebbe essere -10 ℃ a +55 ℃.
- Il coperchio del dispositivo per uso interno deve essere protetto dalla pioggia e dall'umidità.
- È vietato esporre l'apparecchiatura alla luce solare diretta, a bassa ventilazione oa fonti di calore come stufe o radiatori (l'ignoranza può causare pericolo di incendio).
- Non puntare il dispositivo verso il sole o luoghi particolarmente luminosi. In caso contrario, potrebbe verificarsi una fioritura o una sbavatura (che non è un malfunzionamento) e allo stesso tempo compromettere la durata del sensore.
- Utilizzare il guanto fornito quando si apre il coperchio del dispositivo, evitare il contatto diretto con il coperchio del dispositivo, poiché il sudore acido delle dita potrebbe erodere il rivestimento superficiale del coperchio del dispositivo.
- Utilizzare un panno morbido e asciutto per pulire le superfici interne ed esterne del coperchio del dispositivo, non utilizzare detergenti alcalini.

- Si prega di conservare tutti i wrapper dopo averli decompressi per un utilizzo futuro. In caso di guasto occorso, è necessario restituire il dispositivo alla fabbrica con l'involucro originale. Il trasporto senza l'involucro originale può danneggiare il dispositivo e comportare costi aggiuntivi.
- L'uso o la sostituzione impropria della batteria può comportare il rischio di esplosione. Sostituire solo con lo stesso tipo o equivalente. Smaltire le batterie usate secondo le istruzioni fornite dal produttore della batteria.

Sommario

Capitolo 1 Descrizione del prodotto

1.1 Panoramica

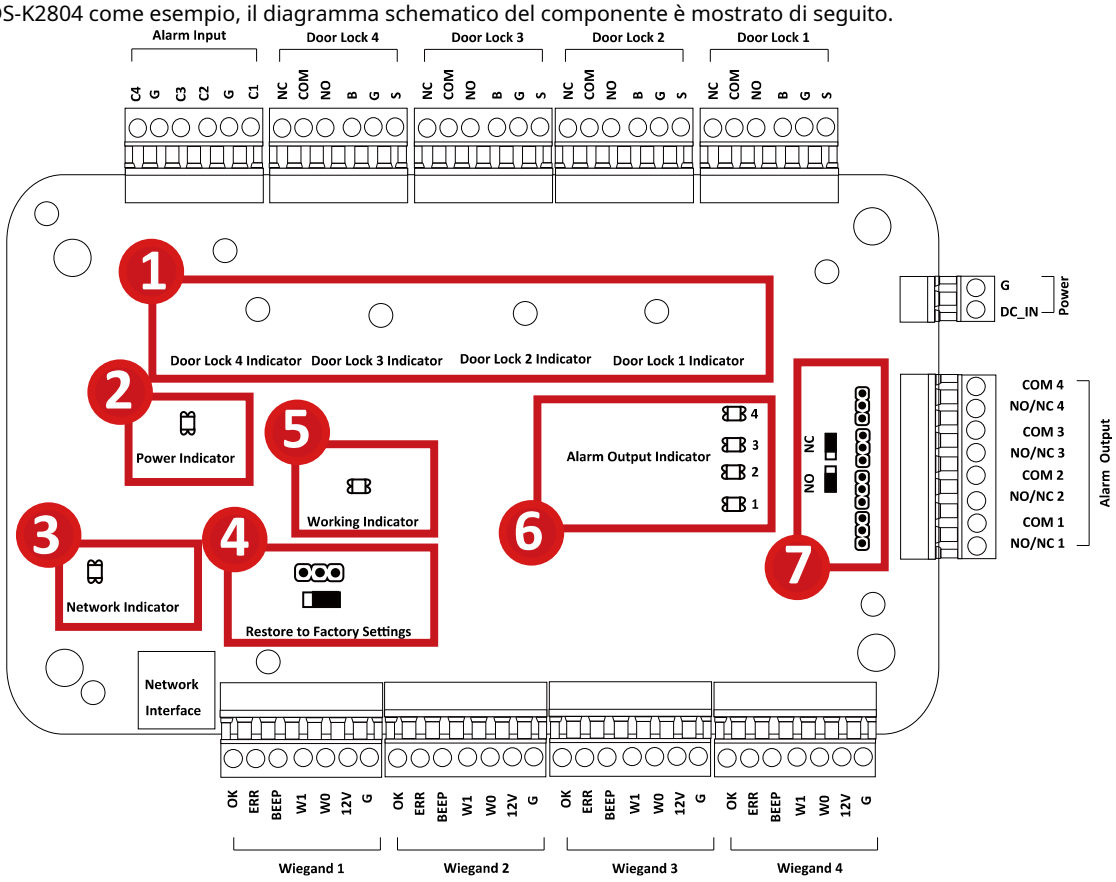
DS-K2800 è un controller di accesso potente e stabile, che utilizza il design dell'architettura logica. DS-K2800 è progettato con un'interfaccia di rete TCP / IP e il suo segnale viene elaborato con una crittografia speciale e può essere eseguito offline. È supportata anche la funzione anti-manomissione.

1.2 Caratteristiche principali

- Il controller di accesso è dotato di processore ad alta velocità a 32 bit
- Supporta la comunicazione di rete TCP / IP, con interfaccia di rete autoadattativa. I dati di comunicazione sono appositamente crittografati per alleviare la preoccupazione di perdita di privacy Supporta il
- riconoscimento e la memorizzazione del numero di carta con una lunghezza massima di 20
- Il controller di accesso può memorizzare 10mila carte legali e 50mila record di scorrimento delle carte Supporta la
- prima porta aperta della carta e la funzione di autorizzazione della prima carta, la funzione super card e super password, funzione di aggiornamento online e controllo remoto delle porte
- Supporta l'interfaccia Wiegand per l'accesso al lettore di carte. L'interfaccia Wiegand supporta W26 / W34 ed è perfettamente compatibile con lettori di schede di terze parti con interfaccia Wiegand
- Supporta vari tipi di carte come normale / blocklist / pattuglia / ospite / coercizione / super card, carta per l'apertura estesa della porta, ecc.
- Supporta la sincronizzazione dell'ora tramite NTP, metodo manuale o automatico
- Supporta la funzione di archiviazione dei record quando è offline e la funzione di allarme di archiviazione dello spazio di archiviazione insufficiente
- Il controller di accesso ha un design watchdog
- I dati possono essere salvati in modo permanente dopo lo spegnimento del controller di accesso. Supporta il
- collegamento I / O e il collegamento degli eventi
- Supporta l'allarme di eventi offline superiori al 90%
- Metodi di caricamento di più eventi: canale, gruppo centrale e ascolto di 500
- gruppi di codici di autenticazione
- Funzione anti-pass-back.

Capitolo 2 Descrizione dei componenti

Prendi DS-K2804 come esempio, il diagramma schematico del componente è mostrato di seguito.

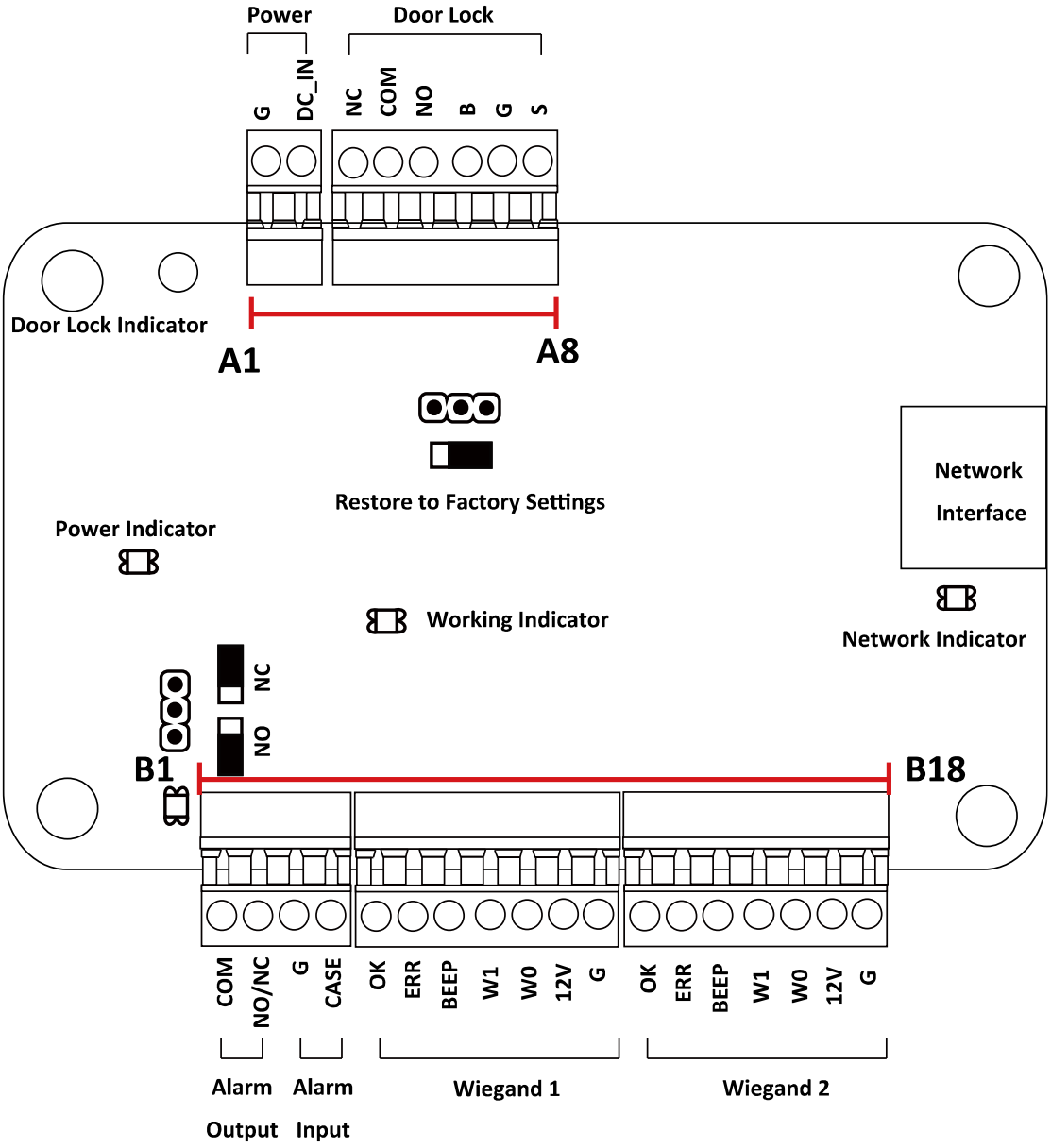


Le descrizioni dei componenti DS-K2800 sono le seguenti:

No.	Descrizione dei componenti		
	DS-K2801	**DS-K2802**	**DS-K2804**
1	Blocco porta 1 Indicatore	Serratura porta 1/2 Indicatore	Serratura porta 1/2/3/4 Indicatore
2	Indicatore di energia		
3	Indicatore di rete		
4	Tappo del ponticello per il ripristino delle impostazioni di		
5	fabbrica Indicatore di funzionamento		
6	Indicatore di uscita allarme		
7	Cap ponticello uscita allarme (NO / NC)		

Capitolo 3 Collegamento terminale

3.1 Descrizione del terminale DS-K2801

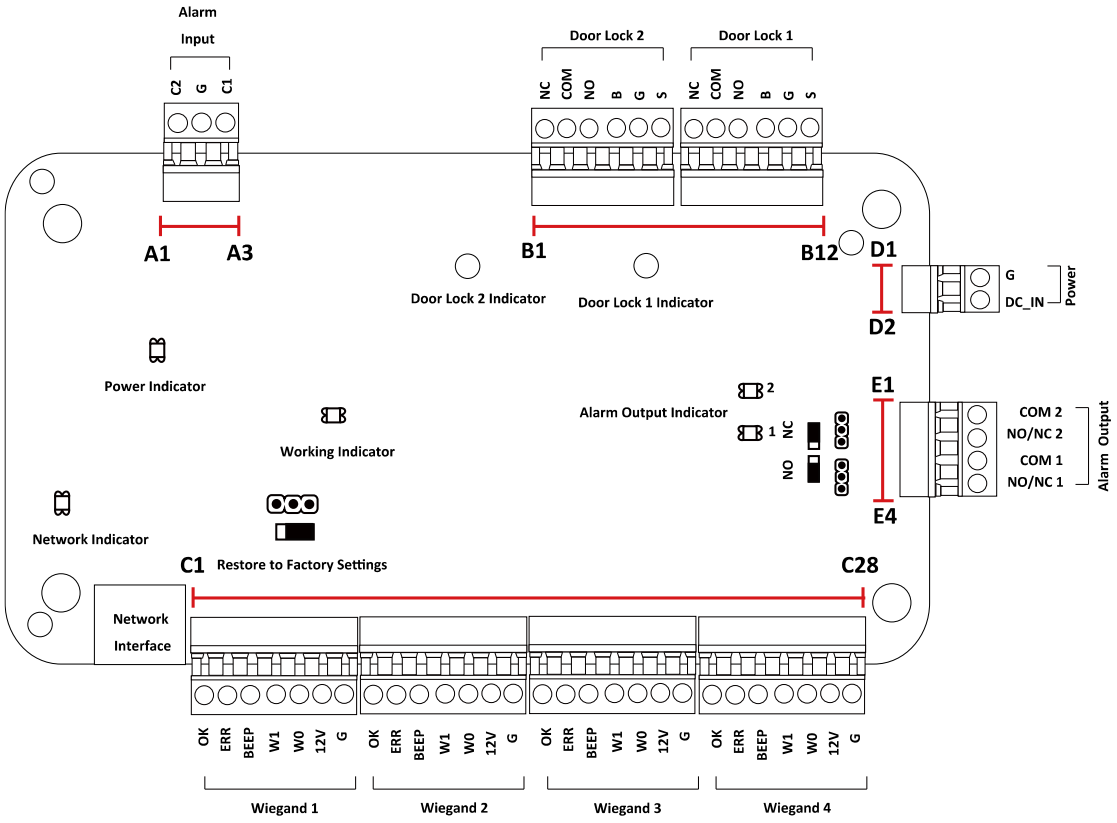


Le descrizioni del terminale DS-K2801 sono le seguenti:

No.	DS-K2801		
A1	Energia	GND	Messa a terra DC12V
A2		+ 12V	Ingresso DC12V
A3	Porta	NC	Uscita relè blocco porta
A4		COM	
A5		NO	
A6		PULSANTE	Ingresso pulsante porta
A7		GND	Messa a terra

No.	DS-K2801		
A8		SENSORE	Rilevatore magnetico per porte
B1	Uscita allarme	COM	Uscita relè allarme (contatto pulito)
B2		NO / NC	
B3	Ingresso allarme	GND	Messa a terra
B4		NEL	Ingresso evento
B5	Wiegand Card Lettore 1	ok	Indicatore dell'uscita di controllo del lettore di schede (uscita scheda valida)
B6		ERR	Indicatore dell'uscita di controllo del lettore di schede (uscita scheda non valida)
B7		BZ	Lettore di schede Buzzer Uscita di controllo
B8		W1	Testina Wiegand Lettura dei dati di input 1
B9		W0	Wiegand Head Read Data Input Data0
B10		PWR	Uscita di alimentazione del lettore di schede
B11		GND	
B12	Wiegand Card Lettore 2	ok	Indicatore dell'uscita di controllo del lettore di schede (uscita scheda valida)
B13		ERR	Indicatore dell'uscita di controllo del lettore di schede (uscita scheda non valida)
B14		BZ	Lettore di schede Buzzer Uscita di controllo
B15		W1	Testina Wiegand Lettura dei dati di input 1
B16		W0	Wiegand Head Read Data Input Data0
B17		PWR	Uscita di alimentazione del lettore di schede
B18		GND	

3.2 Descrizione terminale DS-K2802

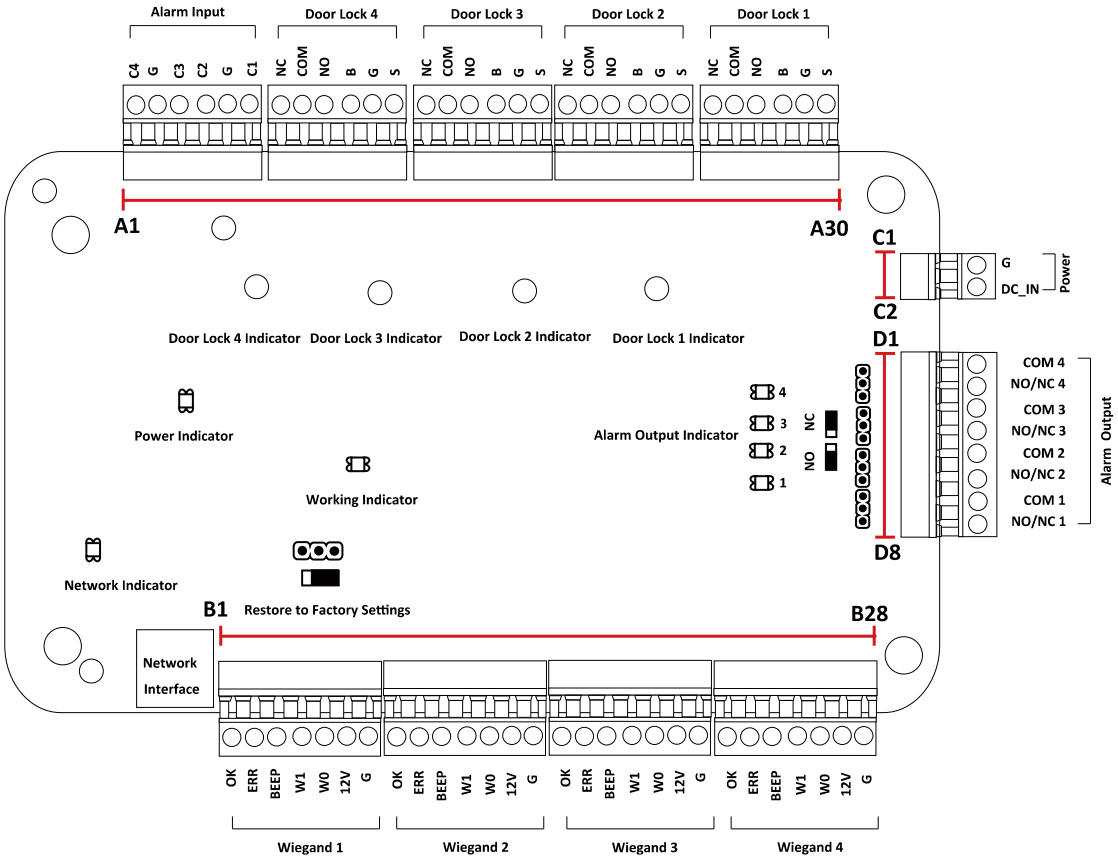


DS -K280 2 Le descrizioni dei terminali sono le seguenti:

No.	DS-K2802		
A1	Ingresso allarme	IN 2	Ingresso evento 2
A2		GND	Messa a terra
A3		IN 1	Ingresso evento 1
B1	Porta 2	NC	Uscita relè blocco porta (contatto pulito)
B2		COM	
B3		NO	
B4		PULSANTE	Ingresso pulsante porta
B5		GND	Messa a terra
B6		SENSORE	Rilevatore magnetico per porte
B7	Porta 1	NC	Uscita relè blocco porta (contatto pulito)
B8		COM	
B9		NO	
B10		PULSANTE	Ingresso pulsante porta
B11		GND	Messa a terra
B12		SENSORE	Rilevatore magnetico per porte
D1	Energia	GND	Messa a terra DC12V
D2		+ 12V	Ingresso DC12V
E1	Uscita allarme 2	COM2	Uscita relè allarme 2 (contatto pulito)
E2		NO / NC2	

No.	DS-K2802		
E3	Uscita allarme 1	COM1	Uscita relè allarme 1 (contatto pulito)
E4		NO / NC1	
C1	Wiegand Card Lettore 1	ok	Indicatore dell'uscita di controllo del lettore di schede (uscita scheda valida)
C2		ERR	Indicatore dell'uscita di controllo del lettore di schede (uscita scheda non valida)
C3		BZ	Lettore di schede Buzzer Uscita di controllo
C4		W1	Testina Wiegand Lettura dati in ingresso Dati1
C5		W0	Testina Wiegand Lettura dati Input Data0
C6		PWR	Uscita di alimentazione del lettore di schede
C7		GND	
C8	Wiegand Card Lettore 2	ok	Indicatore dell'uscita di controllo del lettore di schede (uscita scheda valida)
C9		ERR	Indicatore dell'uscita di controllo del lettore di schede (uscita scheda non valida)
C10		BZ	Lettore di schede Buzzer Uscita di controllo
C11		W1	Testina Wiegand Lettura dati in ingresso Dati1
C12		W0	Testina Wiegand Lettura dati Input Data0
C13		PWR	Uscita di alimentazione del lettore di schede
C14		GND	
C15	Wiegand Card Lettore 3	ok	Indicatore dell'uscita di controllo del lettore di schede (uscita scheda valida)
C16		ERR	Indicatore dell'uscita di controllo del lettore di schede (uscita scheda non valida)
C17		BZ	Lettore di schede Buzzer Uscita di controllo
C18		W1	Testina Wiegand Lettura dati in ingresso Dati1
C19		W0	Testina Wiegand Lettura dati Input Data0
C20		PWR	Uscita di alimentazione del lettore di schede
C21		GND	
C22	Wiegand Card Lettore 4	ok	Indicatore dell'uscita di controllo del lettore di schede (uscita scheda valida)
C23		ERR	Indicatore dell'uscita di controllo del lettore di schede (uscita scheda non valida)
C24		BZ	Lettore di schede Buzzer Uscita di controllo
C25		W1	Testina Wiegand Lettura dati in ingresso Dati1
C26		W0	Testina Wiegand Lettura dati Input Data0
C27		PWR	Uscita di alimentazione del lettore di schede
C28		GND	

3.3 Descrizione terminale DS-K2804



Le descrizioni del terminale DS-K2804 sono le seguenti:

No.	DS-K2804		
A1	Ingresso allarme	IN4	Ingresso evento 4
A2		GND	Messa a terra
A3		IN3	Ingresso evento 3
A4		IN 2	Ingresso evento 2
A5		GND	Messa a terra
A6		IN 1	Ingresso evento 1
A7	Porta 4	NC	Uscita relè blocco porta (contatto pulito)
A8		COM	
A9		NO	
A10		PULSANTE	Ingresso pulsante porta
A11		GND	Messa a terra
A12		SENSORE	Rilevatore magnetico per porte
A13	Porta 3	NC	Uscita relè blocco porta (contatto pulito)
A14		COM	
A15		NO	
A16		PULSANTE	Ingresso pulsante porta
A17		GND	Messa a terra
A18		SENSORE	Rilevatore magnetico per porte

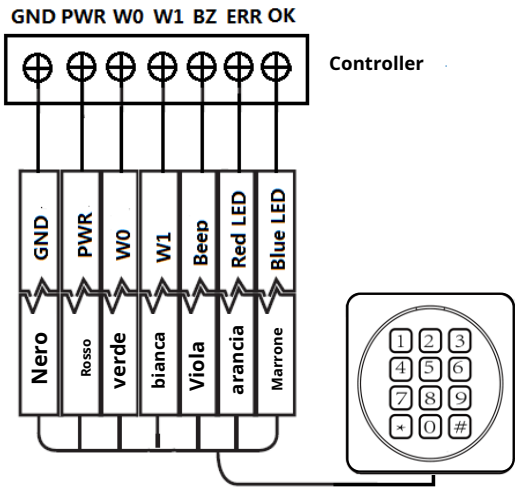
No.	DS-K2804		
A19	Porta 2	NC	Uscita relè blocco porta (contatto pulito)
A20		COM	
A21		NO	
A22		PULSANTE	Ingresso pulsante porta
A23		GND	Messa a terra
A24		SENSORE	Rilevatore magnetico per porte
A25	Porta 1	NC	Uscita relè blocco porta (contatto pulito)
A26		COM	
A27		NO	
A28		PULSANTE	Ingresso pulsante porta
A29		GND	Messa a terra
A30		SENSORE	Rilevatore magnetico per porte
B1	Wiegand Card Lettore 1	ok	Indicatore dell'uscita di controllo del lettore di schede (uscita della scheda valida) Indicatore
B2		ERR	dell'uscita di controllo del lettore di schede (uscita della scheda non valida)
B3		BZ	Lettore di schede Buzzer Uscita di controllo
B4		W1	Testina Wiegand Lettura dati in ingresso Dati1
B5		W0	Testina Wiegand Lettura dati Input Data0
B6		PWR	Uscita di alimentazione del lettore di schede
B7		GND	
B8	Wiegand Card Lettore 2	ok	Indicatore dell'uscita di controllo del lettore di schede (uscita della scheda valida) Indicatore
B9		ERR	dell'uscita di controllo del lettore di schede (uscita della scheda non valida)
B10		BZ	Lettore di schede Buzzer Uscita di controllo
B11		W1	Testina Wiegand Lettura dati in ingresso Dati1
B12		W0	Testina Wiegand Lettura dati Input Data0
B13		PWR	Uscita di alimentazione del lettore di schede
B14		GND	
B15	Wiegand Card Lettore 3	ok	Indicatore dell'uscita di controllo del lettore di schede (uscita della scheda valida) Indicatore
B16		ERR	dell'uscita di controllo del lettore di schede (uscita della scheda non valida)
B17		BZ	Lettore di schede Buzzer Uscita di controllo
B18		W1	Testina Wiegand Lettura dati in ingresso Dati1
B19		W0	Testina Wiegand Lettura dati Input Data0
B20		PWR	Uscita di alimentazione del lettore di schede
B21		GND	
B22	Wiegand Card Lettore 4	ok	Indicatore dell'uscita di controllo del lettore di schede (uscita della scheda valida) Indicatore
B23		ERR	dell'uscita di controllo del lettore di schede (uscita della scheda non valida)

No.	DS-K2804		
B24		BZ	Lettore di schede Buzzer Uscita di controllo
B25		W1	Testina Wiegand Lettura dati in ingresso Dati1
B26		W0	Testina Wiegand Lettura dati Input Data0
B27		PWR	Uscita di alimentazione del lettore di schede
B28		GND	
C1	Energia	GND	Messa a terra DC12V
C2		+ 12V	Ingresso DC12V
D1	Uscita allarme 4	COM4	Uscita relè allarme 4 (contatto pulito)
D2		NO / NC4	
D3	Uscita allarme 3	COM3	Uscita relè allarme 3 (contatto pulito)
D4		NO / NC3	
D5	Uscita allarme 2	COM2	Uscita relè allarme 2 (contatto pulito)
D6		NO / NC2	
D7	Uscita allarme 1	COM1	Uscita relè allarme 1 (contatto pulito)
D8		NO / NC1	

Appunti:

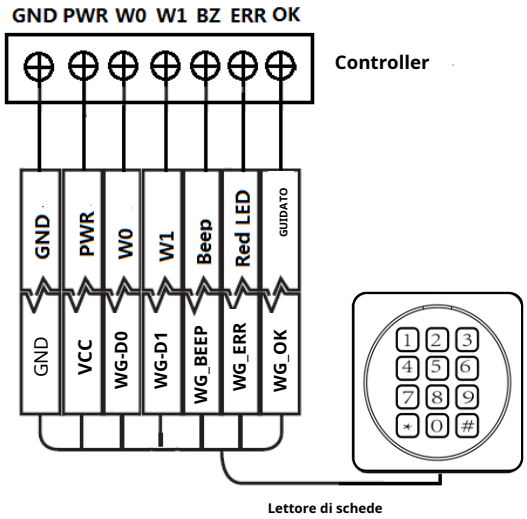
- L'interfaccia hardware dell'ingresso allarme è normalmente aperta per impostazione predefinita. Quindi è consentito solo il segnale normalmente aperto. Può essere collegato al buzzer del lettore di schede e del controller di accesso, all'uscita del relè di allarme e all'uscita relativa alla porta aperta.
- Per il controller di accesso a una porta, il lettore di carte Wiegand 1 e 2 corrispondono rispettivamente ai lettori di carte in entrata e in uscita della porta 1. Per il controller di accesso a due porte, il lettore di carte Wiegand 1 e 2 corrispondono rispettivamente ai lettori di carte in entrata e in uscita della porta 1 e il lettore di carte Wiegand 3 e 4 corrispondono rispettivamente ai lettori di carte in entrata e in uscita della porta 2. Per il controller di accesso a quattro porte, il lettore di carte Wiegand 1, 2, 3 e 4 corrispondono rispettivamente ai lettori di carte in entrata della porta 1, 2, 3 e 4.

e Cablaggio



Giallo
Blu
Nero
Rosso

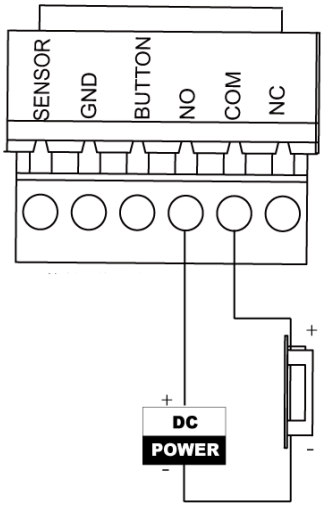
ontrol il LED e il buzzer di



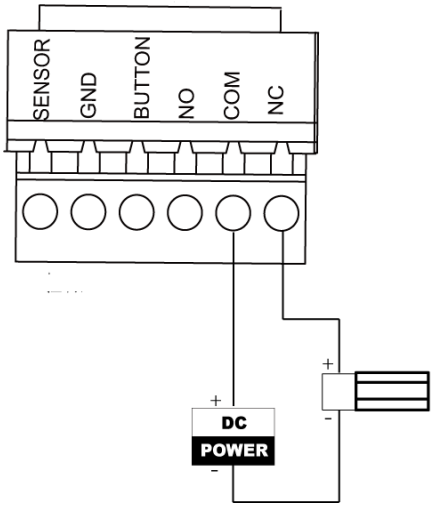
Giallo
Blu
Nero
Rosso

4.2 Terminali esterni DS-K2801

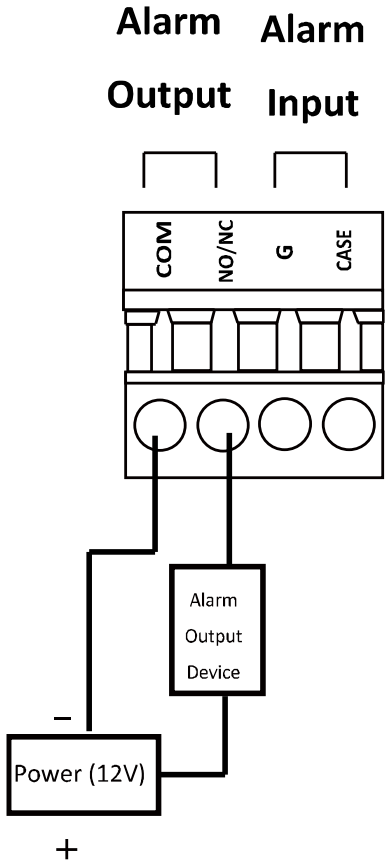
4.2.1 Installazione del blocco del catodo



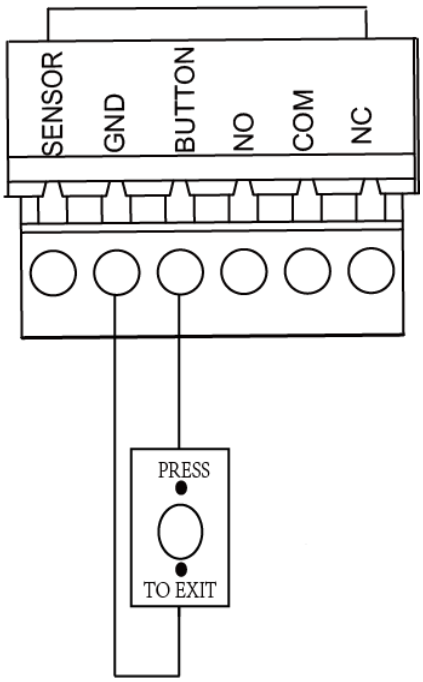
4.2.2 Installazione dell'Anode Lock



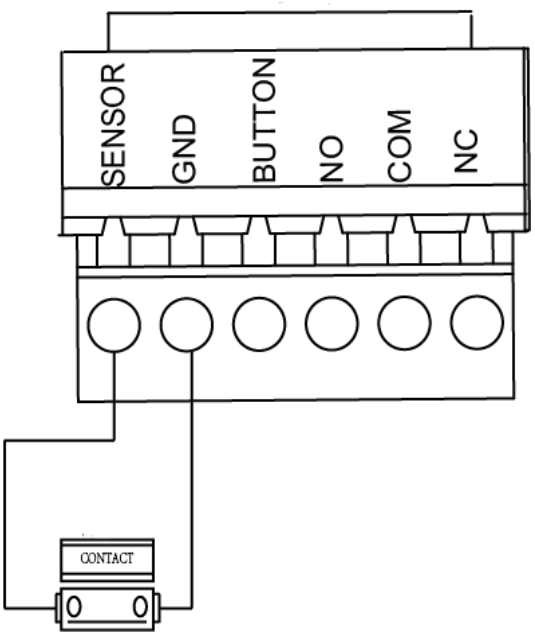
4.3 Collegamento del dispositivo di allarme esterno



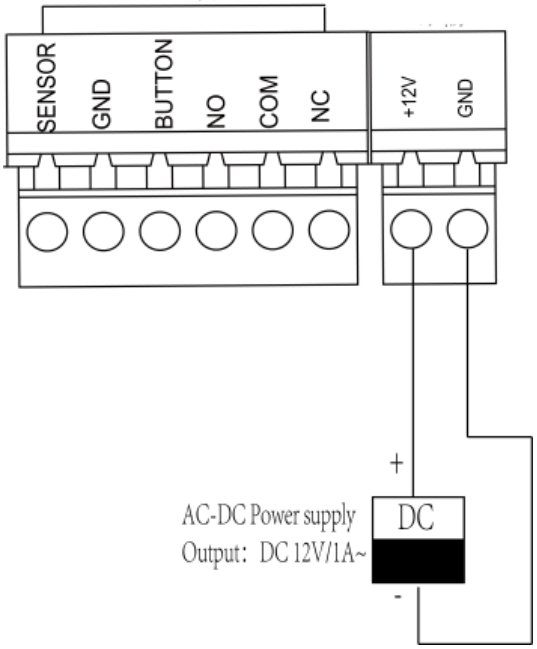
4.4 Schema elettrico pulsante porta



4.5 Il collegamento del rilevamento magnetico



4.6 Collegamento dell'alimentazione



Capitolo 5 Impostazioni

5.1 Inizializzazione dell'hardware

Opzione 1:

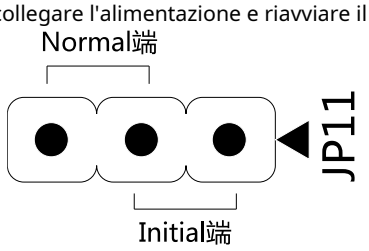
Passaggi:

1. Rimuovere il cappuccio del ponticello dal terminale normale.
2. Scollegare l'alimentazione e riavviare il controller di accesso. Il cicalino del controller emette un lungo segnale acustico.
3. Quando il segnale acustico si interrompe, ricollegare il cappuccio del ponticello a Normale.
4. Scollegare l'alimentazione e riavviare il controller di accesso.

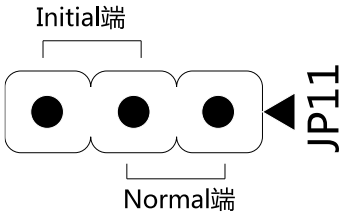
Opzione 2:

Passaggi:

1. Salta il cappuccio del ponticello da Normale a Iniziale.
2. Scollegare l'alimentazione e riavviare il controller di accesso. Il cicalino del controller emette un lungo segnale acustico.
3. Quando il segnale acustico si interrompe, riporta il cappuccio del ponticello su
4. Normale. Scollegare l'alimentazione e riavviare il controller di accesso.



Accesso remoto di inizializzazione DS-K2801



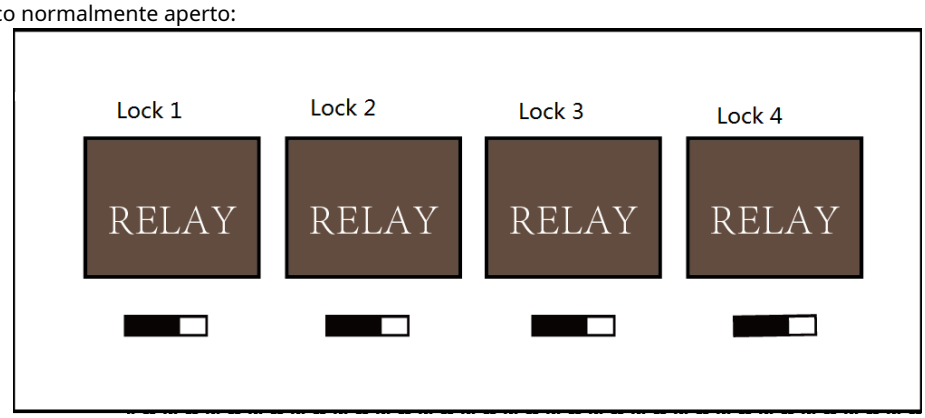
Accesso remoto di inizializzazione DS-K2802 / DS-K2804

Nota: L'inizializzazione dell'hardware ripristinerà tutti i parametri all'impostazione predefinita e tutti gli eventi del dispositivo verranno cancellati.

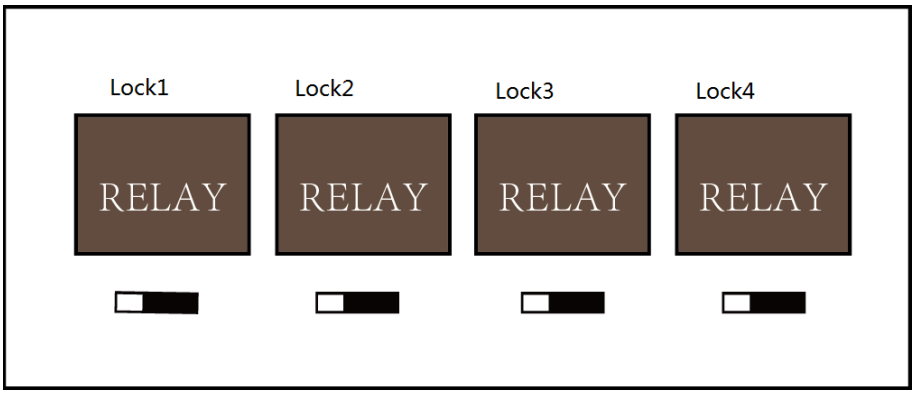
5.2 Ingresso relè NO / NC

5.2.1 Uscita relè di blocco

Stato relè di blocco normalmente aperto:

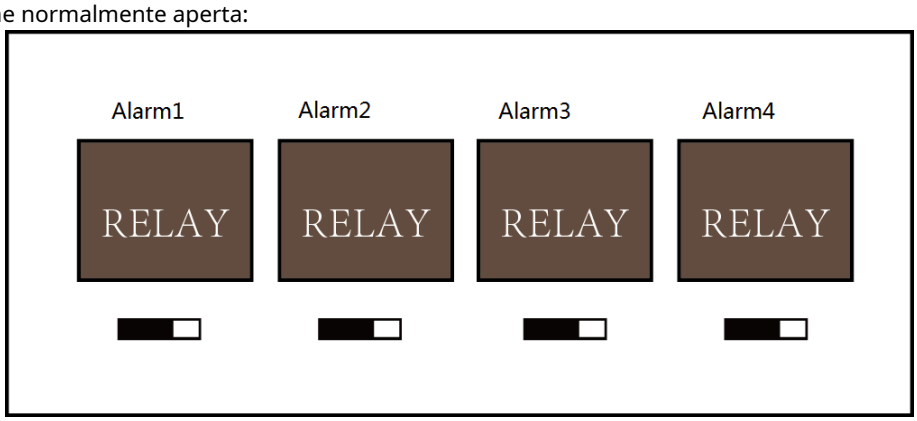


Stato del relè di blocco normalmente chiuso:

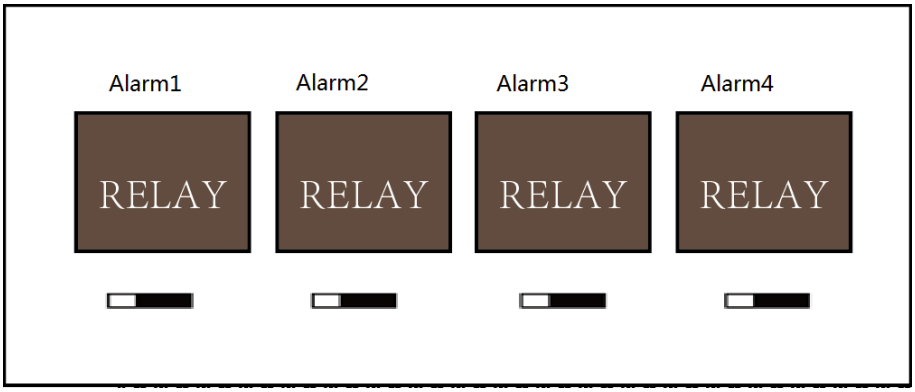


5.2.2 Stato dell'uscita del relè di allarme

Uscita relè allarme normalmente aperta:

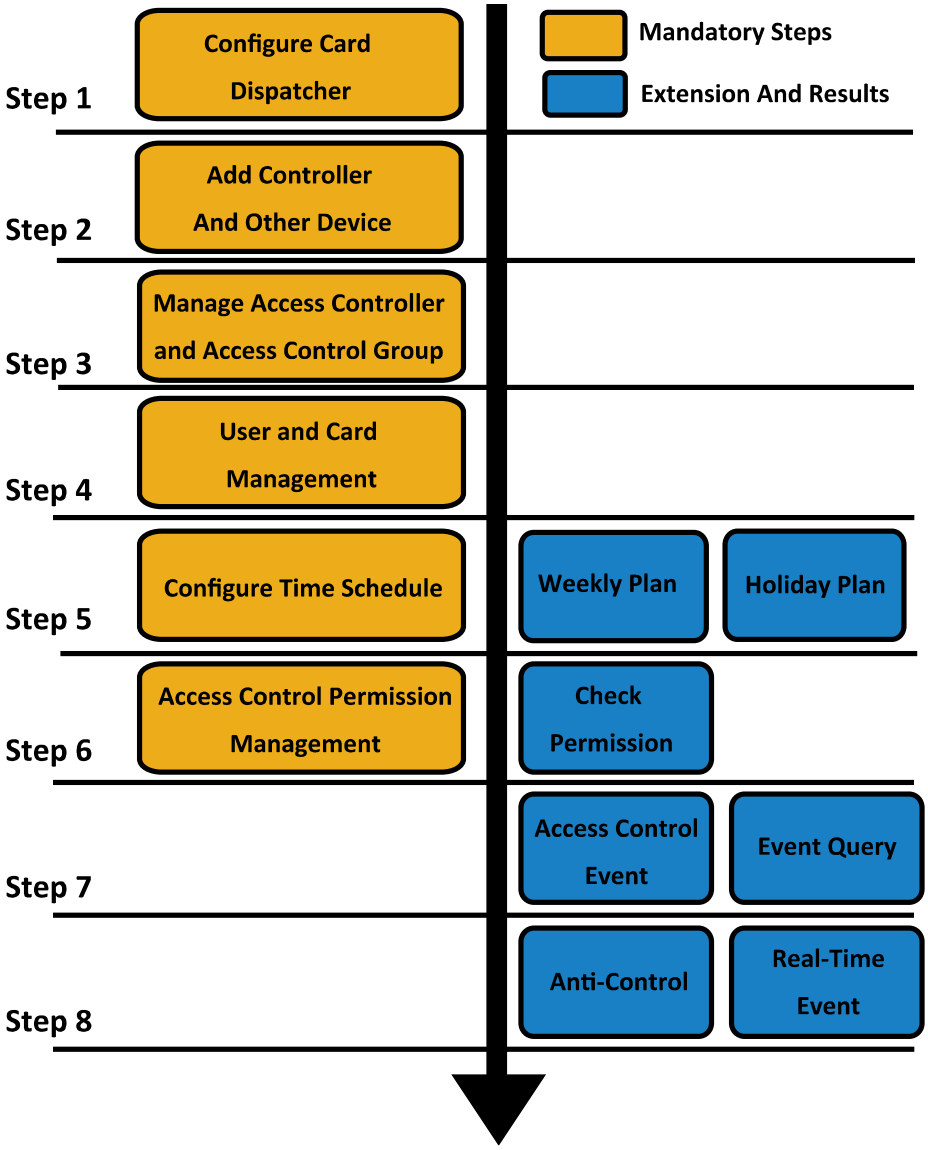


Uscita relè allarme normalmente chiusa:



Flusso di lavoro del software

Per informazioni dettagliate, consultare il manuale utente del software client. Fare riferimento al seguente flusso di lavoro:


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

Capitolo 6 Attivazione del controllo degli accessi terminale

Scopo:

È necessario attivare il terminale prima di utilizzarlo. Sono supportate l'attivazione tramite SADP e l'attivazione tramite software client. I valori predefiniti del terminale di controllo sono i seguenti.

- L'indirizzo IP predefinito: 192.0.0.64.
- Il numero di porta predefinito: 8000.
- Il nome utente predefinito: admin.

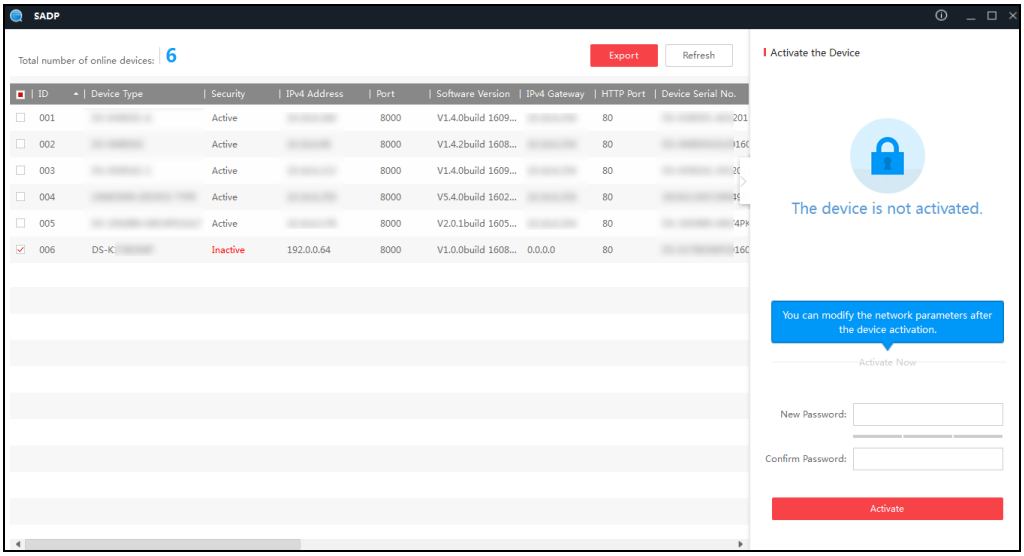
6.1 Attivazione tramite software SADP

Il software SADP viene utilizzato per rilevare il dispositivo online, attivare il dispositivo e reimpostare la password.

Ottieni il software SADP dal disco in dotazione e installa SADP in base alle istruzioni. Segui i passaggi per attivare il pannello di controllo.

Passaggi:

1. Eseguire il software SADP per cercare i dispositivi in linea.
2. Verificare lo stato del dispositivo dall'elenco dei dispositivi e selezionare un dispositivo inattivo.

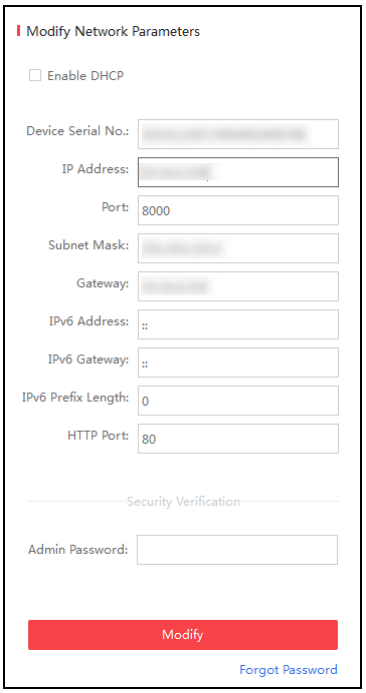


3. Crea una password e inserisci la password nel campo della password, quindi conferma la password.

RACCOMANDATA UNA PASSWORD FORTE - *Ti consigliamo vivamente di creare una password complessa di tua scelta (utilizzando un minimo di 8 caratteri, comprese lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per aumentare la sicurezza del tuo prodotto. E ti consigliamo di reimpostare la password regolarmente, soprattutto nel sistema di alta sicurezza, reimpostare la password mensilmente o settimanalmente può proteggere meglio il tuo prodotto.*

4. Clic **Attivare** per attivare il dispositivo.
5. Verificare il dispositivo attivato. È possibile modificare l'indirizzo IP del dispositivo sulla stessa rete

segmentare con il computer modificando manualmente l'indirizzo IP o selezionando la casella di controllo Abilita DHCP.



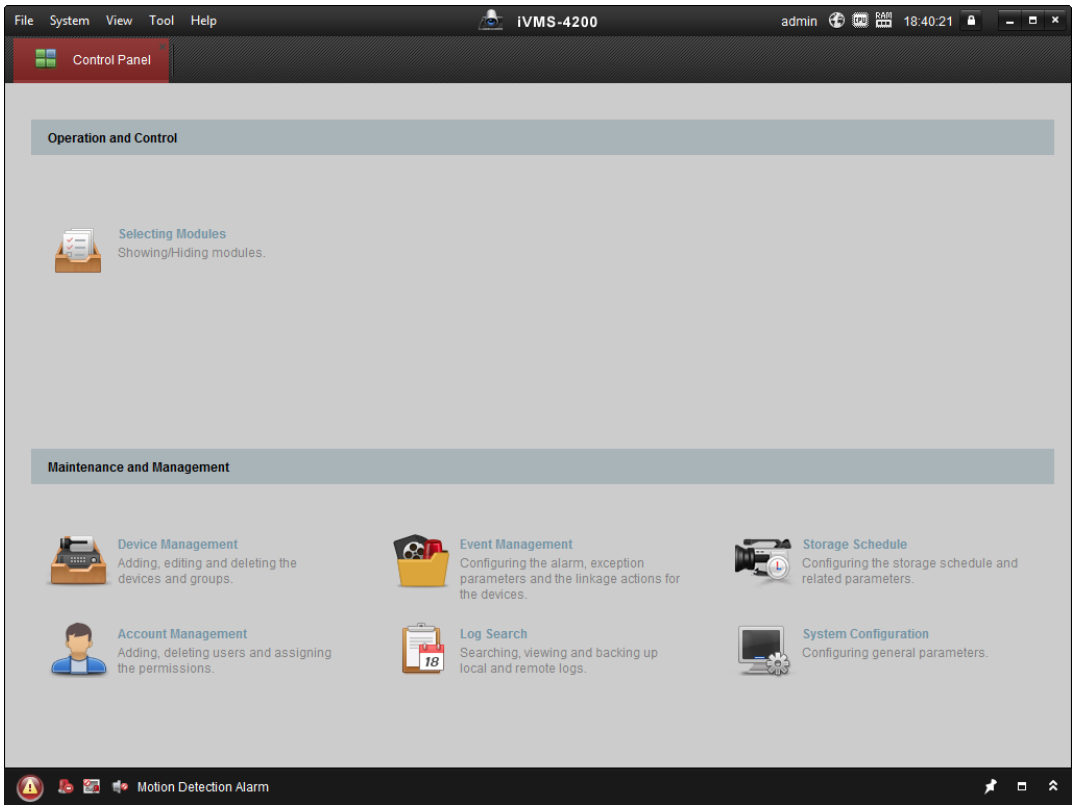
6. Immettere la password e fare clic su **Modificare** pulsante per attivare la modifica dell'indirizzo IP.

6.2 Attivazione tramite software client

Il software client è un software di gestione video versatile per diversi tipi di dispositivi.
Ottieni il software client dal disco in dotazione e installa il software in base alle istruzioni. Segui i passaggi per attivare il pannello di controllo.

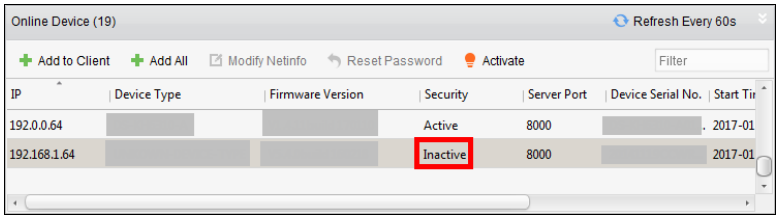
Passaggi:

1. Eseguire il software client e verrà visualizzato il pannello di controllo del software, come mostrato nella figura seguente.



2. Fare clic su **Gestione dei dispositivi** per accedere all'interfaccia di gestione dei dispositivi.

3. Controllare lo stato del dispositivo dall'elenco dei dispositivi e selezionare un dispositivo inattivo.



4. Clicca il **Attivare** per visualizzare l'interfaccia di attivazione.

5. Nella finestra a comparsa, creare una password nel campo della password e confermare la password.

RACCOMANDATA UNA PASSWORD FORTE - *Ti consigliamo vivamente di creare una password complessa di tua scelta (utilizzando un minimo di 8 caratteri, comprese lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per aumentare la sicurezza del tuo prodotto. E ti consigliamo di reimpostare la password regolarmente, soprattutto nel sistema di alta sicurezza, reimpostare la password mensilmente o settimanalmente può proteggere meglio il tuo prodotto.*

6. Clic **ok** pulsante per avviare l'attivazione. Clicca il **Modifica Netinfor** per visualizzare l'interfaccia di
7. modifica dei parametri di rete. Modificare l'indirizzo IP del dispositivo sullo stesso segmento di
8. rete del computer modificando manualmente l'indirizzo IP.

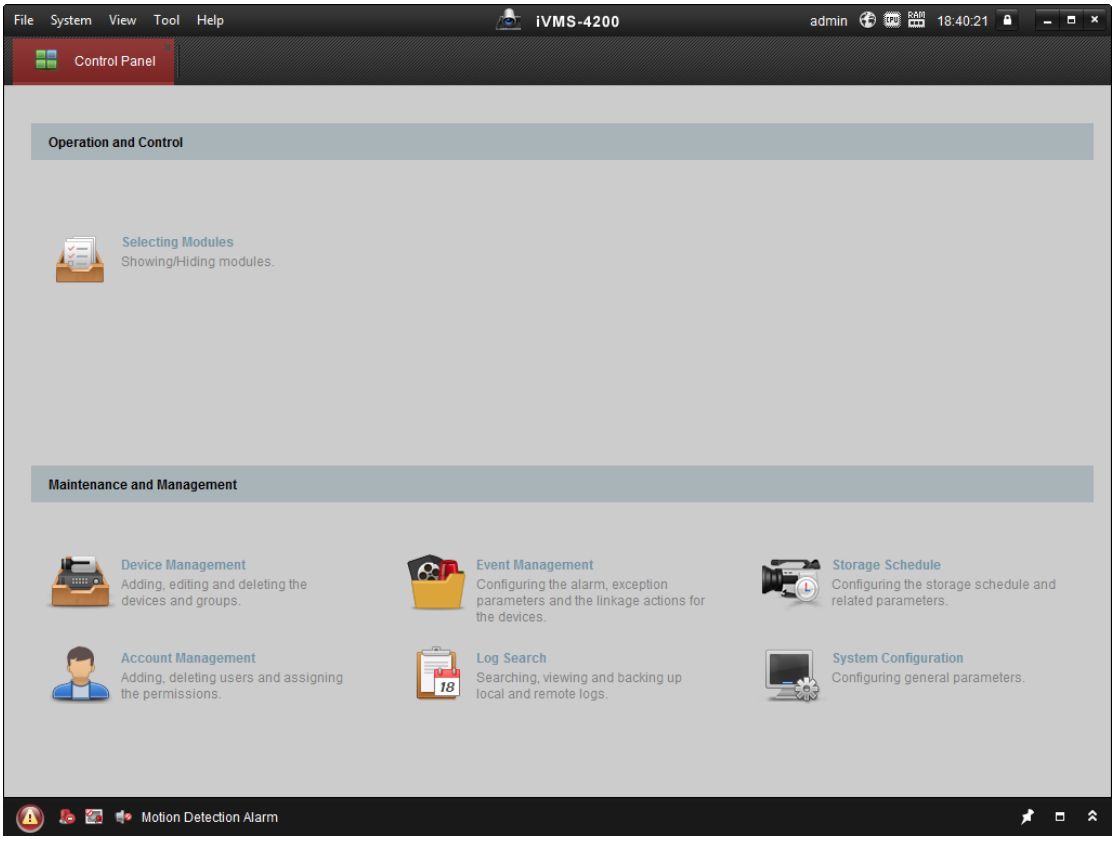
9. Immettere la password e fare clic su **ok** pulsante per salvare le impostazioni.

Capitolo 7 Operazione client

È possibile impostare e utilizzare i dispositivi di controllo degli accessi tramite il software client. Questo capitolo introdurrà le operazioni relative al dispositivo di controllo dell'accesso nel software client. Per le operazioni integrate, fare riferimento a *Manuale utente del software client iVMS-4200.*

7.1 Modulo funzione

Pannello di controllo di iVMS-4200:

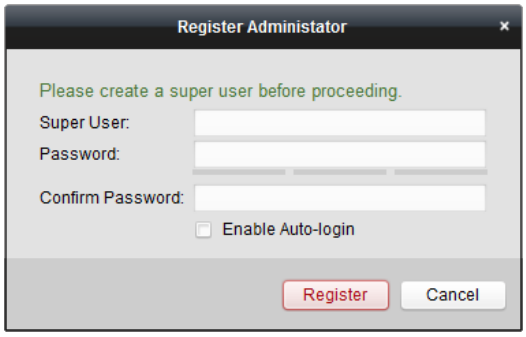


7.2 Registrazione e accesso dell'utente

Per la prima volta per utilizzare il software client iVMS-4200, è necessario registrare un super utente per il login.

Passaggi:

1. Immettere il nome utente e la password del super utente. Il software valuterà la forza della password automaticamente e ti consigliamo vivamente di utilizzare una password complessa per garantire la sicurezza dei tuoi dati.
2. Conferma la password.
3. Facoltativamente, selezionare la casella di controllo **Abilita accesso automatico** per accedere automaticamente al software.
4. Fare clic su **Registrati.** Quindi, puoi accedere al software come super utente.



- *Un nome utente non può contenere nessuno dei seguenti caratteri: / \: *? "<> |. E la lunghezza della password non può essere inferiore a 6 caratteri.*
- *Per la tua privacy, ti consigliamo vivamente di cambiare la password con qualcosa di tua scelta (utilizzando un minimo di 8 caratteri, comprese lettere maiuscole, lettere minuscole, numeri e caratteri speciali) al fine di aumentare la sicurezza del tuo prodotto.*
- *La corretta configurazione di tutte le password e altre impostazioni di sicurezza è responsabilità dell'installatore e / o dell'utente finale.*

Quando si apre iVMS-4200 dopo la registrazione, è possibile accedere al software client con il nome utente e la password registrati.

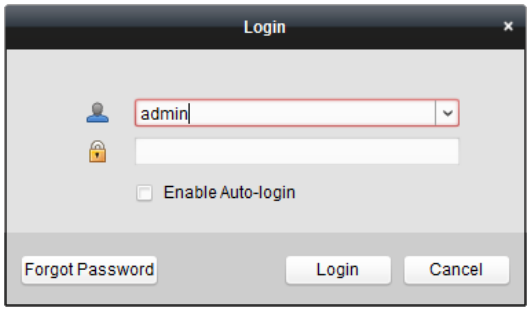
Passaggi:

1. Immettere il nome utente e la password registrati.

   Nota: Se dimentichi la password, fai clic su **Ha dimenticato la password** e ricorda la stringa crittografata nella finestra a comparsa. Contatta il tuo rivenditore e inviagli la stringa crittografata per reimpostare la password.

2. Facoltativamente, selezionare la casella di controllo **Abilita accesso automatico** per accedere automaticamente al software.

3. Fare clic su **Login.**



Dopo aver eseguito il software client, è possibile aprire le procedure guidate (inclusa la procedura guidata per il video, la procedura guidata per il video wall, la procedura guidata del pannello di controllo di sicurezza, la procedura guidata per il controllo degli accessi e il videocitofono e la procedura guidata per la presenza), per guidare l'utente ad aggiungere il dispositivo ed eseguire altre impostazioni e operazioni . Per la configurazione dettagliata delle procedure guidate, fare riferimento a *Guida rapida di iVMS-4200.*

7.3 Configurazione del sistema

Scopo:

È possibile sincronizzare gli eventi di controllo degli accessi persi con il client.

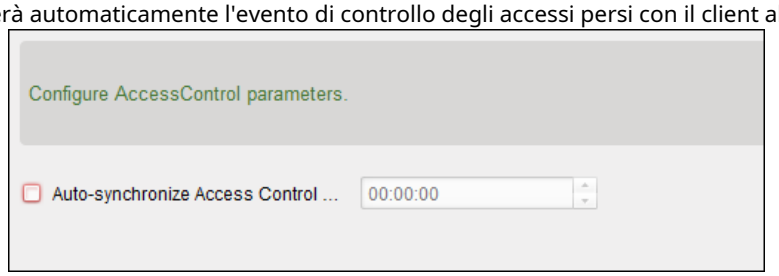
Passaggi:

1. Fare clic su **Attrezzo** - **Configurazione di sistema.**

2. Nella finestra Configurazione di sistema, selezionare il file **Sincronizza automaticamente l'evento di controllo degli accessi** casella di controllo.

3. Imposta l'ora di sincronizzazione.

   Il client sincronizzerà automaticamente l'evento di controllo degli accessi persi con il client all'ora impostata.



7.4 Gestione del controllo degli accessi

Scopo:

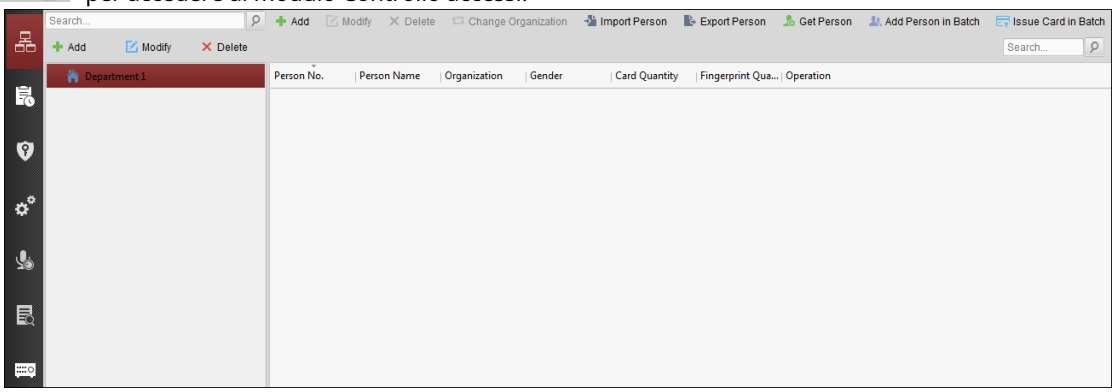
Il modulo Controllo accessi è applicabile ai dispositivi di controllo accessi e al videocitofono. Fornisce molteplici funzionalità, inclusa la gestione delle persone e delle carte, la configurazione delle autorizzazioni, la gestione dello stato del controllo degli accessi, il videocitofono e altre funzioni avanzate.

È inoltre possibile impostare la configurazione degli eventi per il controllo degli accessi e visualizzare i punti e le zone di controllo degli accessi su E-map.

Nota: Per l'utente con le autorizzazioni del modulo di controllo dell'accesso, l'utente può accedere al modulo di controllo dell'accesso e configurare le impostazioni di controllo dell'accesso.

Clic  nel pannello di controllo e controllare **Controllo di accesso** per aggiungere il modulo di controllo degli accessi a il pannello di controllo.

Clic  per accedere al modulo Controllo accessi.



Prima che inizi:

Per la prima volta aprendo il modulo Controllo Accessi, apparirà la seguente finestra di dialogo e verrà richiesto di selezionare la scena in base alle effettive necessità.

È possibile selezionare la scena come **Non residenza** e **Residenza.**

Appunti:

- Una volta configurata la scena, non è possibile modificarla in seguito.
- Quando selezioni **Non residenza** modalità, non è possibile configurare la regola di presenza quando si aggiunge una persona.

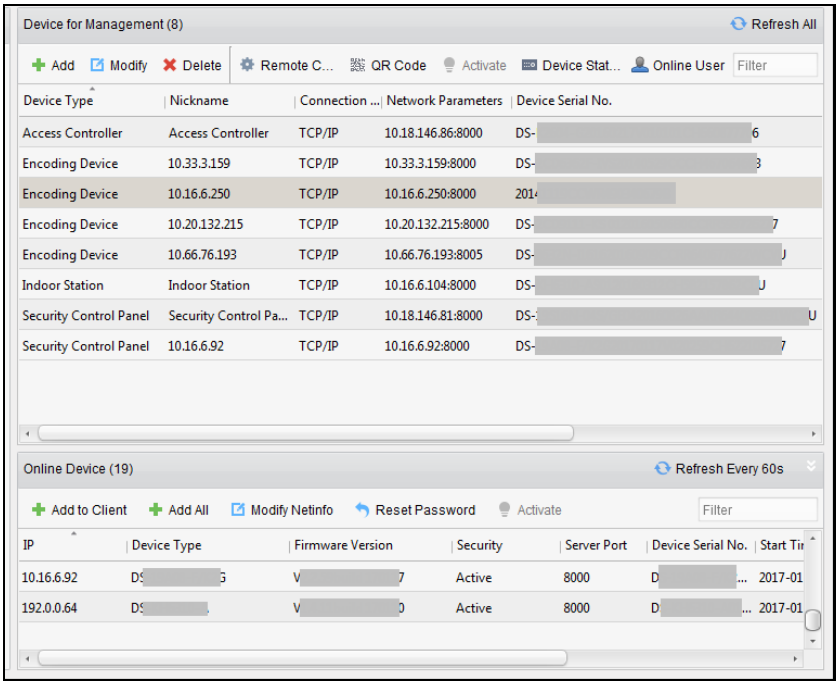
Il modulo Controllo accessi è composto dai seguenti sottomoduli.

	Persona e card	Gestire le organizzazioni, le persone e l'assegnazione carte alle persone.
	Programma e Modello	Configurazione della pianificazione settimanale, del gruppo di festività e impostazione del modello.
	Autorizzazione	Assegnazione delle autorizzazioni di controllo dell'accesso a persone e applicando ai dispositivi.
	Funzione avanzata	Fornire funzioni avanzate tra cui impostazioni dei parametri di controllo degli accessi, autenticazione del lettore di schede, porta apribile con prima tessera, retro anti-passante, multiporta ad incastro, e autenticazione parola d'ordine.
	Videocitofono	Videocitofono tra cliente e residente, ricerca nel registro chiamate e rilascio avviso. Ricerca eventi storici di controllo
	Ricerca	accessi; Ricerca nei registri delle chiamate, sblocco dei registri e avvisi rilasciati. Gestione dei dispositivi di
	Dispositivo Gestione	controllo accessi e dei dispositivi videocitofonici.

Nota: In questo capitolo vengono introdotte solo le operazioni sul controllo degli accessi.

7.4.1 Aggiunta di un dispositivo di controllo degli accessi

Clic nel modulo Controllo accessi per accedere alla seguente interfaccia.



Nota: Dopo aver aggiunto il dispositivo, è necessario controllare lo stato di inserimento del dispositivo in **Attrezzo** - **Controllo inserimento dispositivo.** Se il dispositivo non è attivato, è necessario attivarlo o non riceverai gli eventi tramite il software client. Per i dettagli sul controllo dell'inserimento del dispositivo, fare riferimento *7.12 Controllo inserimento.*

Creazione della password

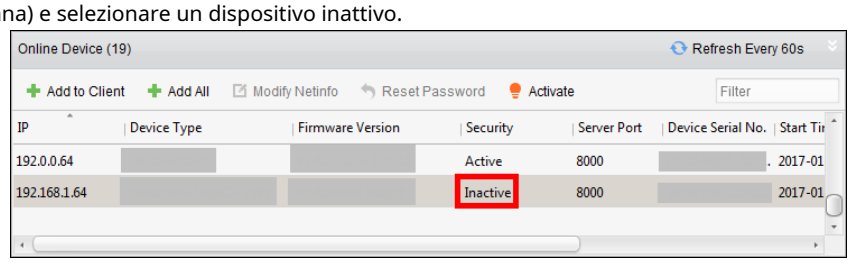
Scopo:

Per alcuni dispositivi, è necessario creare la password per attivarli prima che possano essere aggiunti al software e funzionare correttamente.

Nota: Questa funzione dovrebbe essere supportata dal dispositivo.

Passaggi:

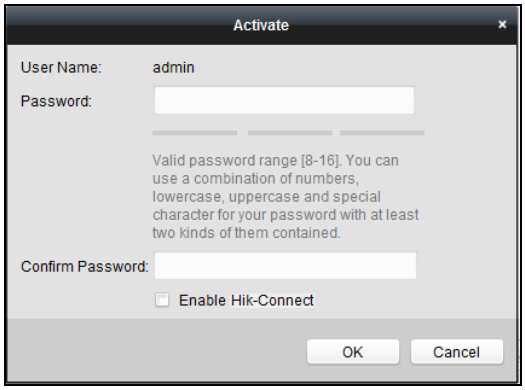
1. Accedere alla pagina Gestione dispositivi.
2. Sul **Dispositivo per la gestione** o **Dispositivo online** area, controllare lo stato del dispositivo (mostrato su **Sicurezza** colonna) e selezionare un dispositivo inattivo.



3. Fare clic su **Attivare** per visualizzare l'interfaccia di attivazione.
4. Creare una password nel campo della password e confermare la password.

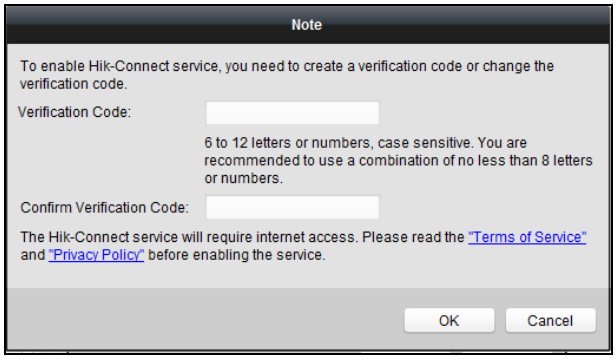
RACCOMANDATA UNA PASSWORD FORTE - *Ti consigliamo vivamente di creare una password complessa di tua scelta (utilizzando un minimo di 8 caratteri, comprese lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per aumentare la sicurezza del tuo prodotto. E ti consigliamo di reimpostare la password regolarmente, soprattutto nel sistema di alta sicurezza,*

reimpostare la password mensilmente o settimanalmente può proteggere meglio il tuo prodotto.



5. (Facoltativo) Abilitare il servizio Hik-Connect quando si attiva il dispositivo se il dispositivo lo supporta.

1) Verifica **Abilita Hik-Connect** casella di controllo per visualizzare la finestra di dialogo Nota.



2) Crea un codice di verifica.

3) Conferma il codice di verifica.

4) Fare clic su **Termini di servizio** e **politica sulla riservatezza** per leggere i requisiti.

5) Fare clic su **ok** per abilitare il servizio Hik-Connect.

6. Clic **ok** per attivare il dispositivo.

A "Il dispositivo è attivato." viene visualizzata la finestra quando la password è stata impostata

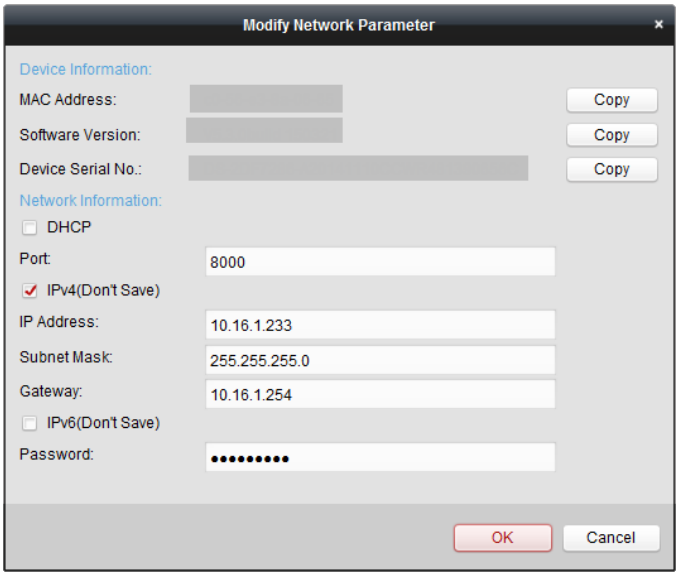
7. correttamente. Clic **Modifica Netinfo** per visualizzare l'interfaccia Modifica parametri di rete.

Nota: Questa funzione è disponibile solo su **Dispositivo online** la zona. È possibile modificare l'indirizzo IP del dispositivo nella stessa sottorete del computer se è necessario aggiungere il dispositivo al software.

8. Modificare l'indirizzo IP del dispositivo nella stessa sottorete del computer modificando il file

Indirizzo IP manualmente o selezionando la casella di controllo di DHCP. Immettere la password impostata al

9. passaggio 4 e fare clic su **ok** per completare le impostazioni di rete.

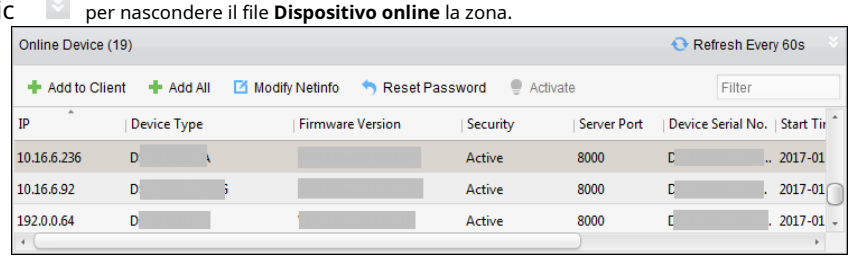


Aggiunta di un dispositivo online

Scopo:

I dispositivi online attivi nella stessa sottorete locale con il software client verranno visualizzati nel file **Dispositivo online** la zona. Puoi fare clic su **Aggiorna ogni 60 secondi** pulsante per aggiornare le informazioni dei dispositivi online.

Nota: Puoi fare clic per nascondere il file **Dispositivo online** la zona.



Passaggi:

1. Selezionare i dispositivi da aggiungere dall'elenco.

   Nota: Per il dispositivo inattivo, è necessario creare la relativa password prima di poter aggiungere correttamente il dispositivo. Per i passaggi dettagliati, fare riferimento a *Capitolo 6 Attivazione del terminale di controllo accessi.*

2. Clic **Aggiungi al cliente** per aprire la finestra di dialogo di aggiunta del dispositivo.
3. Immettere le informazioni richieste.

   Soprannome: Modifica un nome per il dispositivo come desideri.

   Indirizzo: Immettere l'indirizzo IP del dispositivo. L'indirizzo IP del dispositivo viene ottenuto automaticamente in questa modalità di aggiunta.

   Porta: Immettere il numero di porta del dispositivo. Il valore predefinito è *8000.*

   Nome utente: Immettere il nome utente del dispositivo. Per impostazione predefinita, il nome utente è *admin.*

   Parola d'ordine: Immettere la password del dispositivo.

   La sicurezza della password del dispositivo può essere controllata dal software. Per la tua privacy, ti consigliamo vivamente di cambiare la password con qualcosa di tua scelta (utilizzando un file

minimo 8 caratteri, comprese lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per aumentare la sicurezza del prodotto. E ti consigliamo di reimpostare la password regolarmente, soprattutto nel sistema di alta sicurezza, reimpostare la password mensilmente o settimanalmente può proteggere meglio il tuo prodotto.

4. Facoltativamente, controlla il file **Esporta in gruppo** casella di controllo per creare un gruppo in base al nome del dispositivo. È possibile importare tutti i canali del dispositivo nel gruppo corrispondente per impostazione predefinita.

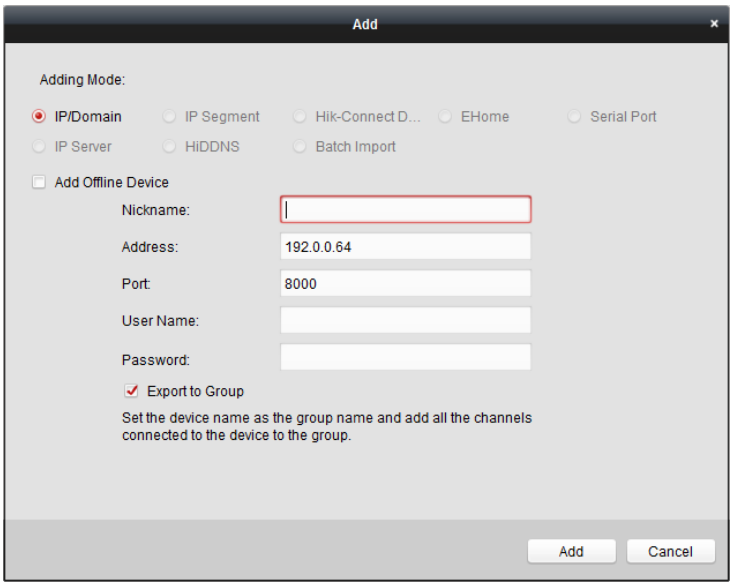
   Nota: iVMS-4200 fornisce anche un metodo per aggiungere i dispositivi offline.

   1) Controlla il file **Aggiungi dispositivo offline** casella di controllo.

   2) **io** Immettere le informazioni richieste, compreso il numero di canale del dispositivo e l'ingresso di allarme numero.

   3) Fare clic su **Inserisci.**

5. Quando il dispositivo offline torna online, il software lo connetterà automaticamente. Clic **Inserisci** per aggiungere il dispositivo.

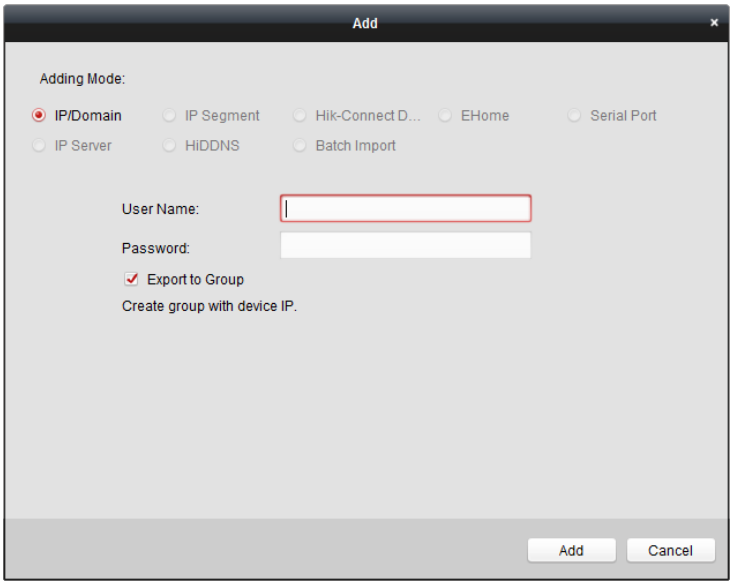


- **Aggiunta di più dispositivi online**

  Se desideri aggiungere più dispositivi online al software client, fai clic e tieni premuto *Ctrl* per selezionare più dispositivi e fare clic su **Aggiungi al cliente** per aprire la finestra di dialogo di aggiunta del dispositivo. Nella finestra del messaggio a comparsa, immettere il nome utente e la password per i dispositivi da aggiungere.

- **Aggiunta di tutti i dispositivi online**

  Se si desidera aggiungere tutti i dispositivi in linea al software client, fare clic su **Aggiungi tutto** e fare clic **ok** nella finestra di messaggio pop-up. Quindi immettere il nome utente e la password per i dispositivi da aggiungere.



Aggiunta di dispositivi tramite IP o nome di dominio

Passaggi:

1. Fare clic su **Inserisci** per aprire la finestra di dialogo di aggiunta del dispositivo.

2. Seleziona **IP / dominio** come modalità di aggiunta.

3. Immettere le informazioni richieste.

   Soprannome: Modifica un nome per il dispositivo come desideri.

   Indirizzo: Immettere l'indirizzo IP o il nome di dominio del dispositivo.

   Porta: Immettere il numero di porta del dispositivo. Il valore predefinito è *8000.*

   Nome utente: Immettere il nome utente del dispositivo. Per impostazione predefinita, il nome utente è *admin.*

   Parola d'ordine: Immettere la password del dispositivo.

   La sicurezza della password del dispositivo può essere controllata dal software. Per la tua privacy, ti consigliamo vivamente di cambiare la password con qualcosa di tua scelta (utilizzando un minimo di 8 caratteri, comprese lettere maiuscole, lettere minuscole, numeri e caratteri speciali) al fine di aumentare la sicurezza del tuo prodotto. E ti consigliamo di reimpostare la password regolarmente, soprattutto nel sistema di alta sicurezza, reimpostare la password mensilmente o settimanalmente può proteggere meglio il tuo prodotto.

4. Facoltativamente, controlla il file **Esporta in gruppo** casella di controllo per creare un gruppo in base al nome del dispositivo. È possibile importare tutti i canali del dispositivo nel gruppo corrispondente per impostazione predefinita.

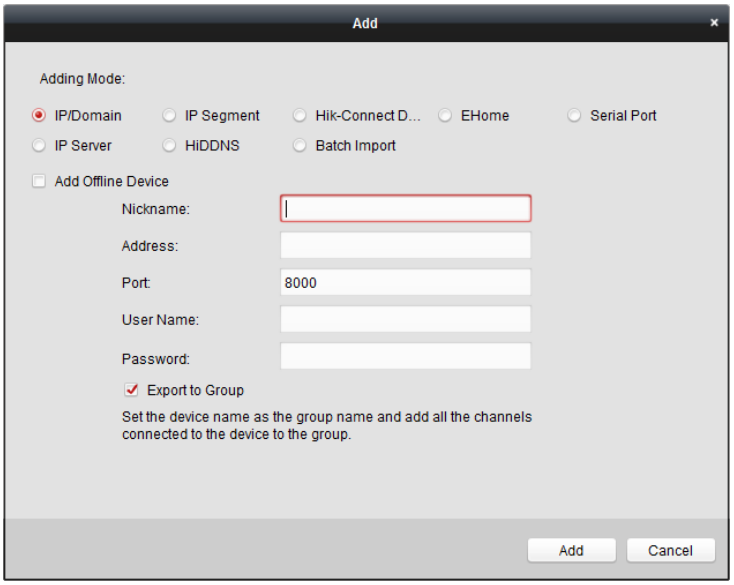
   Nota: iVMS-4200 fornisce anche un metodo per aggiungere i dispositivi offline.

   1) Controlla il file **Aggiungi dispositivo offline** casella di controllo.

   2) **io** Immettere le informazioni richieste, compreso il numero di canale del dispositivo e l'ingresso di allarme numero.

   3) Fare clic su **Inserisci.**

5. Quando il dispositivo offline torna online, il software lo connetterà automaticamente. Clic **Inserisci** per aggiungere il dispositivo.



Aggiunta di dispositivi per segmento IP

Passaggi:

1. Fare clic su **Inserisci** per aprire la finestra di dialogo di aggiunta del dispositivo.

2. Seleziona **Segmento IP** come modalità di aggiunta.

3. Immettere le informazioni richieste.

   IP iniziale: Immettere un indirizzo IP iniziale.

   IP finale: Immettere un indirizzo IP finale nello stesso segmento di rete con l'IP iniziale.

   Porta: Immettere il numero di porta del dispositivo. Il valore predefinito è *8000.*

   Nome utente: Immettere il nome utente del dispositivo. Per impostazione predefinita, il nome utente è *admin.*

   Parola d'ordine: Immettere la password del dispositivo.

   La sicurezza della password del dispositivo può essere controllata dal software. Per la tua privacy, ti consigliamo vivamente di cambiare la password con qualcosa di tua scelta (utilizzando un minimo di 8 caratteri, comprese lettere maiuscole, lettere minuscole, numeri e caratteri speciali) al fine di aumentare la sicurezza del tuo prodotto. E ti consigliamo di reimpostare la password regolarmente, soprattutto nel sistema di alta sicurezza, reimpostare la password mensilmente o settimanalmente può proteggere meglio il tuo prodotto.

4. Facoltativamente, controlla il file **Esporta in gruppo** casella di controllo per creare un gruppo in base al nome del dispositivo. È possibile importare tutti i canali del dispositivo nel gruppo corrispondente per impostazione predefinita.

   Nota: iVMS-4200 fornisce anche un metodo per aggiungere i dispositivi offline.

   1) Controlla il file **Aggiungi dispositivo offline** casella di controllo.

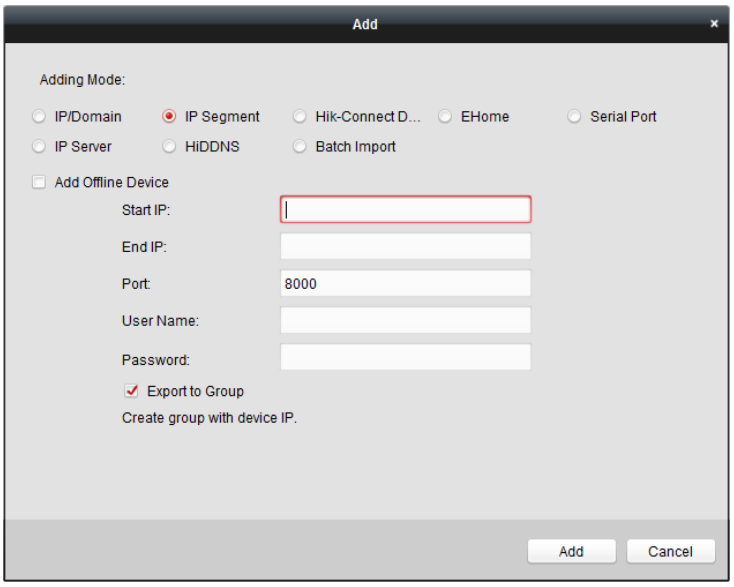
   2) **io** Immettere le informazioni richieste, compreso il numero di canale del dispositivo e l'ingresso di allarme numero.

   3) Fare clic su **Inserisci.**

   Quando il dispositivo offline torna online, il software lo connetterà automaticamente. Clic **Inserisci.**

5. È possibile aggiungere il dispositivo il cui indirizzo IP si trova tra l'IP iniziale e l'IP finale al dispositivo

elenco.



Importazione di dispositivi in batch

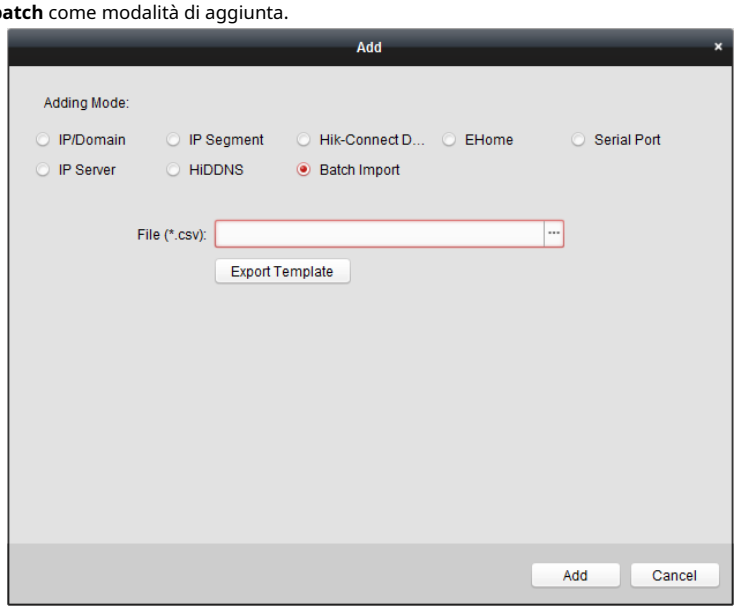
Scopo:

I dispositivi possono essere aggiunti al software in batch inserendo le informazioni sul dispositivo nel file CSV predefinito.

Passaggi:

1. Fare clic su **Inserisci** per aprire la finestra di dialogo di aggiunta del dispositivo.

2. Seleziona **Importazione in batch** come modalità di aggiunta.



3. Clic **Esporta modello** e salva il modello predefinito (file CSV) sul tuo PC.
4. Aprire il file modello esportato e inserire le informazioni richieste dei dispositivi da aggiungere nella colonna corrispondente.

   Soprannome: Modifica un nome per il dispositivo come desideri.

   Modalità di aggiunta: È possibile immettere 0, 2, 3, 4, 5 o 6 che indica diverse modalità di aggiunta. 0 indica che il dispositivo viene aggiunto tramite indirizzo IP o nome di dominio; 2 indica che il dispositivo è

aggiunto tramite server IP; 3 indica che il dispositivo è stato aggiunto tramite HiDDNS; 4 indica che il dispositivo è stato aggiunto tramite protocollo EHome; 5 indica che il dispositivo viene aggiunto dalla porta seriale; 6 indica che il dispositivo è stato aggiunto tramite Hik-Connect Domain.

Indirizzo: Modifica l'indirizzo del dispositivo. Se si imposta 0 come modalità di aggiunta, è necessario inserire l'indirizzo IP o il nome di dominio del dispositivo; se si imposta 2 come modalità di aggiunta, è necessario inserire l'indirizzo IP del PC che installa IP Server; se si imposta 3 come modalità di aggiunta, è necessario immettere *www.hik-online.com.*

Porta: Immettere il numero di porta del dispositivo. Il valore predefinito è *8000.*

Informazioni sul dispositivo: Se si imposta 0 come modalità di aggiunta, questo campo non è obbligatorio; se si imposta 2 come modalità di aggiunta, immettere l'ID del dispositivo registrato sul server IP; se si imposta 3 come modalità di aggiunta, immettere il nome di dominio del dispositivo registrato sul server HiDDNS; se imposti 4 come modalità di aggiunta, inserisci l'account EHome; se si imposta 6 come modalità di aggiunta, immettere il numero di serie del dispositivo

Nome utente: Immettere il nome utente del dispositivo. Per impostazione predefinita, il nome utente è *admin.*

Parola d'ordine: Immettere la password del dispositivo.

La sicurezza della password del dispositivo può essere controllata dal software. Per la tua privacy, ti consigliamo vivamente di cambiare la password con qualcosa di tua scelta (utilizzando un minimo di 8 caratteri, comprese lettere maiuscole, lettere minuscole, numeri e caratteri speciali) al fine di aumentare la sicurezza del tuo prodotto. E ti consigliamo di reimpostare la password regolarmente, soprattutto nel sistema di alta sicurezza, reimpostare la password mensilmente o settimanalmente può proteggere meglio il tuo prodotto.

Aggiungi dispositivo offline: È possibile immettere 1 per abilitare l'aggiunta del dispositivo offline, quindi il software lo connetterà automaticamente quando il dispositivo offline sarà online. 0 indica la disabilitazione di questa funzione.

Esporta in gruppo: È possibile immettere 1 per creare un gruppo in base al nome del dispositivo (nickname). Per impostazione predefinita, tutti i canali del dispositivo verranno importati nel gruppo corrispondente. 0 indica la disabilitazione di questa funzione.

Numero canale: Se si imposta 1 per Aggiungi dispositivo offline, immettere il numero di canale del dispositivo. Se imposti 0 per Aggiungi dispositivo offline, questo campo non è obbligatorio.

Numero ingresso allarme: Se si imposta 1 per Aggiungi dispositivo offline, immettere il numero di ingresso allarme del dispositivo. Se imposti 0 per Aggiungi dispositivo offline, questo campo non è obbligatorio.

Porta seriale n .: Se si imposta 5 come modalità di aggiunta, immettere il numero della porta seriale per il dispositivo di controllo accessi.

Velocità in baud: Se si imposta 5 come modalità di aggiunta, immettere la velocità di trasmissione del dispositivo di controllo accessi.

TUFFO: Se si imposta 5 come modalità di aggiunta, immettere l'indirizzo DIP del dispositivo di controllo accessi.

Account Hik-Connect: Se imposti 6 come modalità di aggiunta, inserisci l'account Hik-Connect.

Password Hik-Connect: Se imposti 6 come modalità di aggiunta, inserisci la password di Hik-Connect.

5. Fare clic su  e seleziona il file modello.

6. Fare clic su **Inserisci** per importare i dispositivi.

I dispositivi verranno visualizzati nell'elenco dei dispositivi per la gestione dopo averli aggiunti con successo. È possibile controllare l'utilizzo delle risorse, lo stato dell'HDD, lo stato della registrazione e altre informazioni sui dispositivi aggiunti nell'elenco.

Clic **Aggiorna tutto** per aggiornare le informazioni di tutti i dispositivi aggiunti. È inoltre possibile inserire il nome del dispositivo nel campo del filtro per la ricerca.

7.4.2 Visualizzazione dello stato del dispositivo

Nell'elenco dei dispositivi, è possibile selezionare il dispositivo e quindi fare clic su **Stato del dispositivo** per visualizzarne lo stato.

Nota: L'interfaccia potrebbe essere diversa dall'immagine mostrata sopra. Fare riferimento all'interfaccia effettiva quando si adotta questa funzione.

Stato della porta: Lo stato della porta connessa.

Stato host: Lo stato dell'host, inclusi la tensione di alimentazione della batteria di archiviazione, lo stato di alimentazione del dispositivo, lo stato di interblocco multi-porta, lo stato anti-pass-back e lo stato anti-manomissione dell'host.

Stato del lettore di schede: Lo stato del lettore di schede.

Nota: Se si utilizza il lettore di schede con connessione RS-485, è possibile visualizzare lo stato di online o offline. Se utilizzi il lettore di schede con connessione Wiegand, puoi visualizzare lo stato offline.

Stato uscita allarme: Lo stato dell'uscita allarme di ciascuna porta.

Stato del sensore di eventi: Lo stato del sensore di eventi di ciascuna porta.

Stato di inserimento: Lo stato del dispositivo.

7.4.3 Modifica delle informazioni di base

Scopo:

Dopo aver aggiunto il dispositivo di controllo dell'accesso, è possibile modificare le informazioni di base del dispositivo.

Passaggi:

1. Selezionare il dispositivo nell'elenco dei dispositivi.
2. Fare clic su **Modificare** per visualizzare la finestra di modifica delle informazioni sul dispositivo.
3. Fare clic su **Informazioni di base** scheda per accedere all'interfaccia delle informazioni di base.

4. Modificare le informazioni sul dispositivo, inclusa la modalità di aggiunta, il nome del dispositivo, l'indirizzo IP del dispositivo, il numero di porta, il nome utente e la password.

7.4.4 Configurazione remota

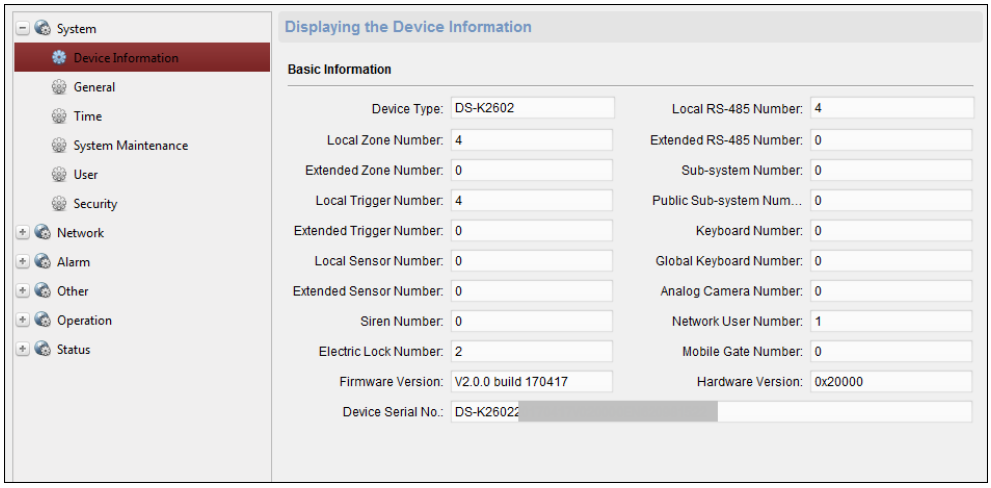
Scopo:

Nell'elenco dei dispositivi, seleziona il dispositivo e fai clic su **Configurazione remota** per accedere all'interfaccia di configurazione remota. È possibile impostare i parametri dettagliati del dispositivo selezionato.

Controllo delle informazioni sul dispositivo

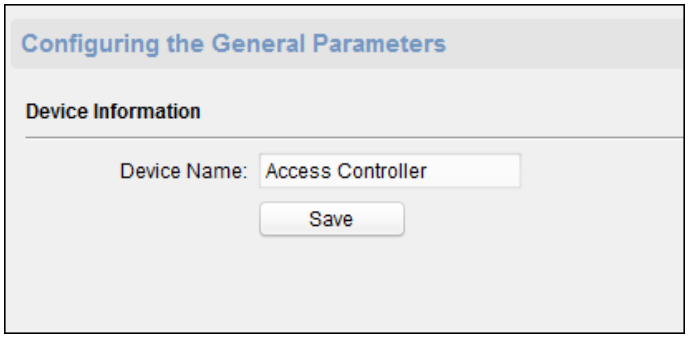
Passaggi:

1. Nell'elenco dei dispositivi, è possibile fare clic su **Configurazione remota** per entrare nella configurazione remota interfaccia.
2. Fare clic su **Sistema -> Informazioni sul dispositivo** per controllare le informazioni di base del dispositivo e il dispositivo informazioni sulla versione.



Modifica del nome del dispositivo

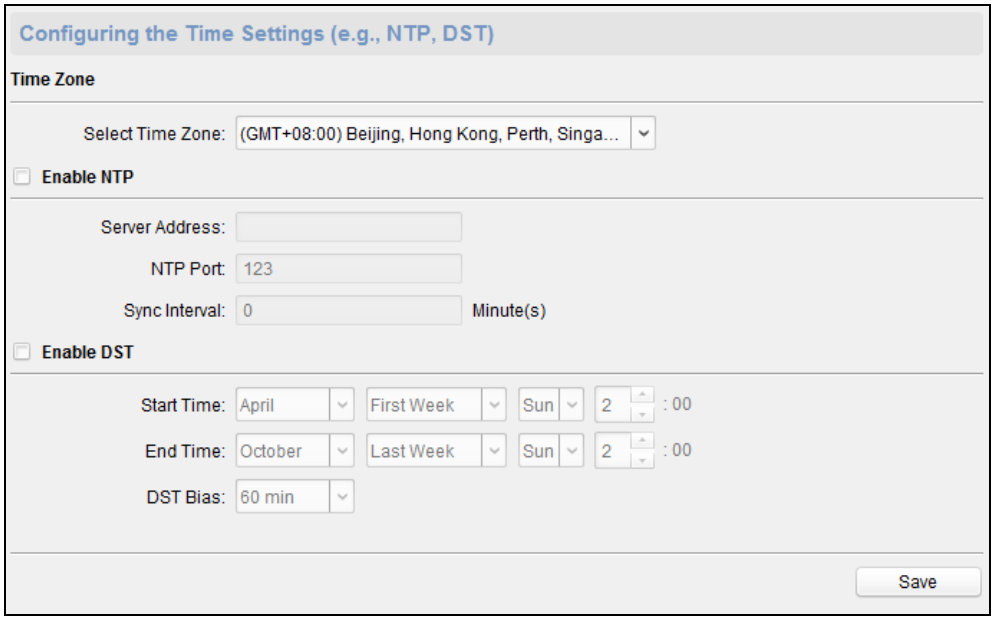
Nell'interfaccia di configurazione remota, fare clic su **Sistema -> Generale** per configurare il nome del dispositivo. Clic **Salva** per salvare le impostazioni.



Tempo di modifica

Passaggi:

1. Nell'interfaccia di configurazione remota, fare clic su **Sistema -> Ora** per configurare il fuso orario.
2. (Facoltativo) Controllare **Abilita NTP** e configurare l'indirizzo del server NTP (o dominio del server), il file Porta NTP e intervallo di sincronizzazione. (Facoltativo) Verifica **Abilita ora legale** e configurare
3. l'ora dell'ora legale, l'ora di fine e il bias. Clic **Salva** per salvare le impostazioni.
4.



Impostazione della manutenzione del sistema

Passaggi:

1. Nell'interfaccia di configurazione remota, fare clic su **Sistema -> Manutenzione del sistema.**
2. Fare clic su **Riavvia** per riavviare il dispositivo.

   Oppure fai clic su **Ripristina le impostazioni di default** per ripristinare le impostazioni del dispositivo a quelle predefinite, escluso l'indirizzo IP.

   Oppure fai clic su **Ripristinare tutto** ripristinare i parametri del dispositivo a quelli di default. Il dispositivo deve essere attivato dopo il ripristino.

   Nota: Il file di configurazione contiene i parametri del dispositivo. È inoltre
3. possibile eseguire l'aggiornamento remoto del dispositivo.

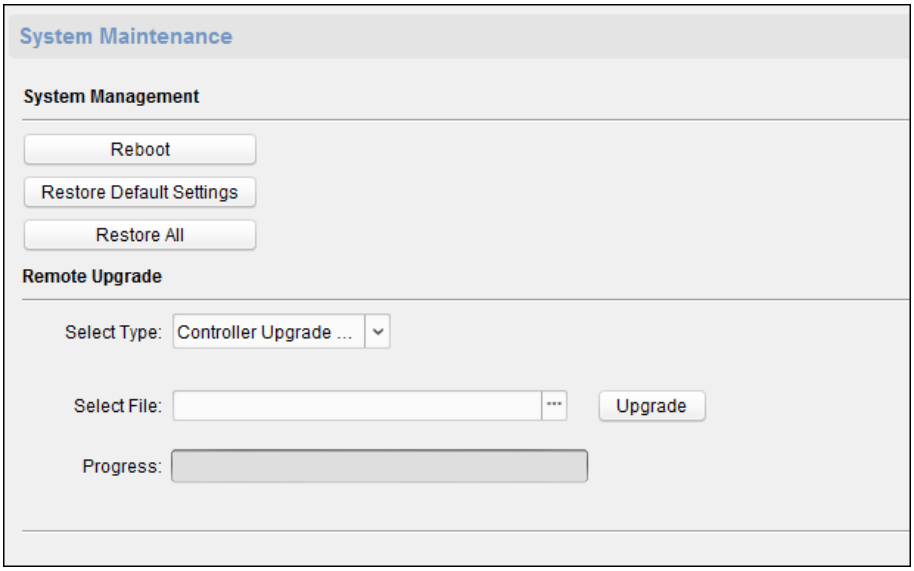
   1) Nella parte Aggiornamento remoto, selezionare un tipo di file di aggiornamento nell'elenco a discesa.

      È possibile selezionare File di aggiornamento del controller o Aggiornamento del lettore di schede nell'elenco a discesa.

   2) Fare clic su per selezionare il file di aggiornamento.

   3) Fare clic su **Upgrade** per avviare l'aggiornamento.

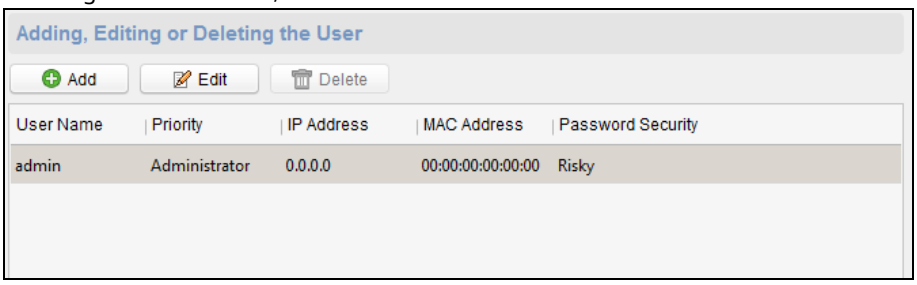
      Nota: È possibile aggiornare solo i lettori di schede collegati tramite RS-485. Il controller di accesso della serie DS-K2800 supporta solo il lettore di schede Wiegand.



Gestione dell'utente

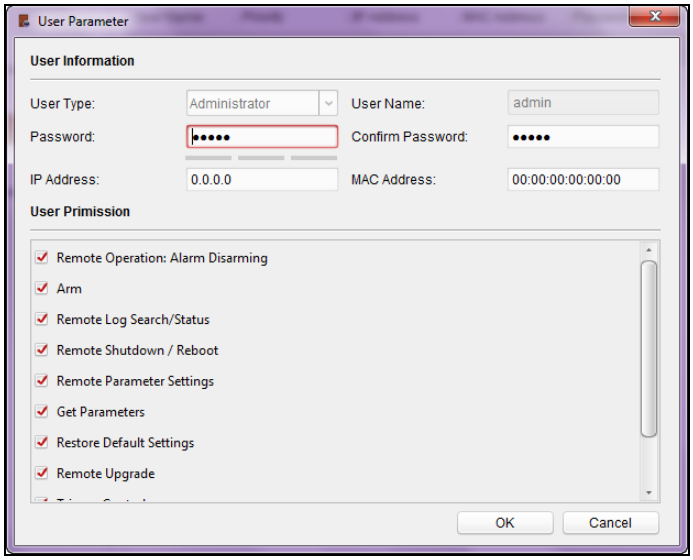
Passaggi:

1. Nell'interfaccia di configurazione remota, fare clic su **Sistema -> Utente.**



2. Fare clic su **Inserisci** per aggiungere l'utente.

   Oppure selezionare un utente nell'elenco degli utenti e fare clic su **modificare** per modificare l'utente. È possibile modificare la password dell'utente, l'indirizzo IP, l'indirizzo MAC e l'autorizzazione dell'utente. Cilck **ok** per confermare la modifica.



Impostazione della sicurezza

Passaggi:

1. Fare clic su **Sistema -> Sicurezza.**

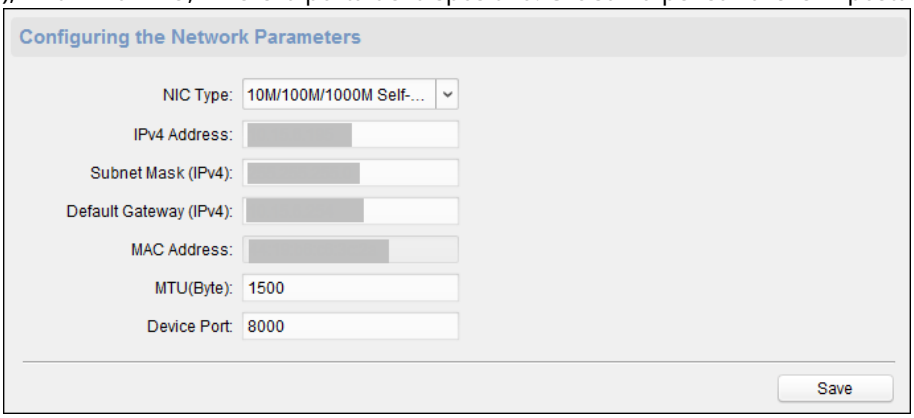
2. Selezionare la modalità di crittografia nell'elenco a discesa.

   È possibile selezionare Modalità compatibile o Modalità crittografia.

3. Fare clic su **Salva** per salvare le impostazioni.

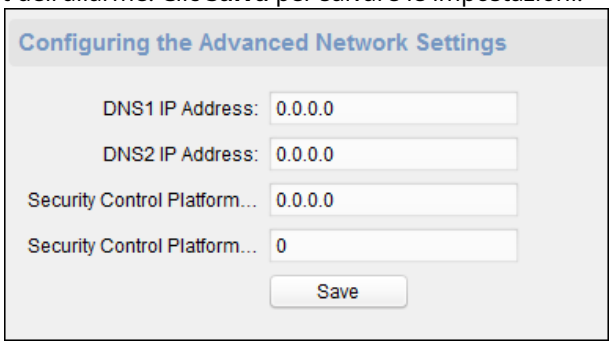
Configurazione dei parametri di rete

Clic **Rete -> Generale.** È possibile configurare il tipo di NIC, l'indirizzo IPv4, la subnet mask (IPv4), il gateway predefinito (IPv4), l'indirizzo MTU, MTU e la porta del dispositivo. Clic **Salva** per salvare le impostazioni.



Configurazione della rete avanzata

Clic **Rete -> Impostazioni avanzate.** È possibile configurare l'indirizzo DNS 1, l'indirizzo DNS 2, l'IP host dell'allarme e la porta dell'host dell'allarme. Clic **Salva** per salvare le impostazioni.

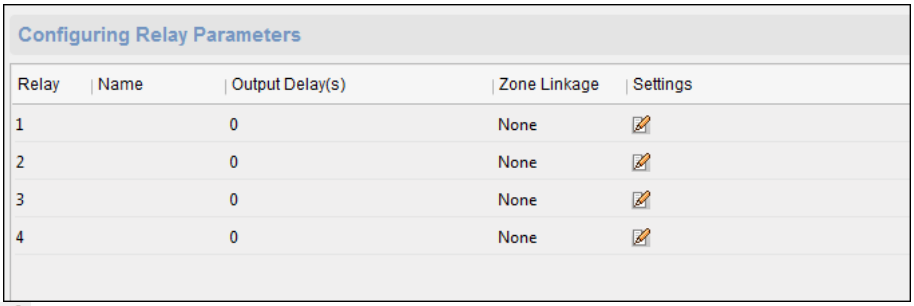


Configurazione dei parametri del relè

Passaggi:

1. Fare clic su **Allarme -> Relè.**

   È possibile visualizzare i parametri del relè.



2. Fare clic su per visualizzare la finestra Impostazioni parametri relè.
3. Impostare il nome del relè e il ritardo di uscita.
4. Fare clic su **Salva** per salvare i parametri.

   Oppure fai clic su **Copia a...** per copiare le informazioni del relè su altri relè.

Configurazione dei parametri di controllo dell'accesso

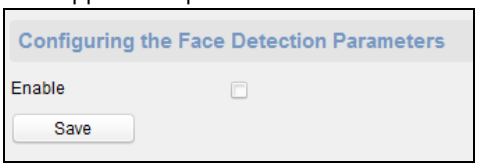
Passaggi:

1. Nell'interfaccia di configurazione remota, fare clic su **Altro -> Parametri di controllo dell'accesso.**
2. Selezionare e controllare il file **Premere il tasto per inserire la scheda n.** casella di controllo.
3. Fare clic su **Salva** per salvare le impostazioni.

Configurazione dei parametri di rilevamento dei volti

Clic **Altro -> Rilevamento volti.** Puoi controllare il file **Abilitare** casella di controllo per abilitare la funzione di rilevamento del volto del dispositivo.

Nota: Solo i dispositivi con funzione video supportano questa funzione.

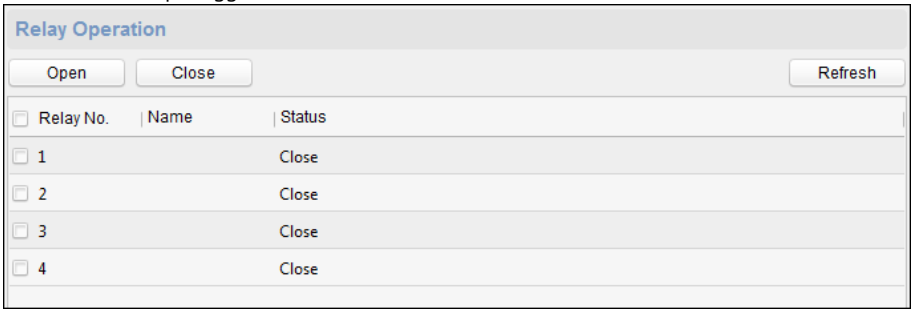


Relè di funzionamento

Passaggi:

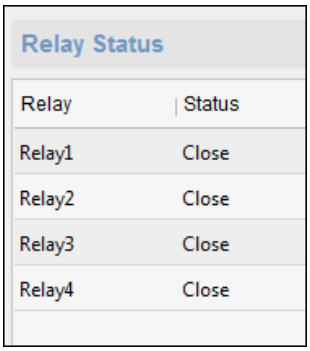
1. Fare clic su **Operazione -> Relè.**

   È possibile visualizzare lo stato del relè.
2. Selezionare la casella di controllo del relè
3. Fare clic su **Aperto** o **Vicino** per aprire / chiudere il relè.
4. (Facoltativo) Fare clic su **ricaricare** per aggiornare lo stato del relè.



Visualizzazione dello stato del relè

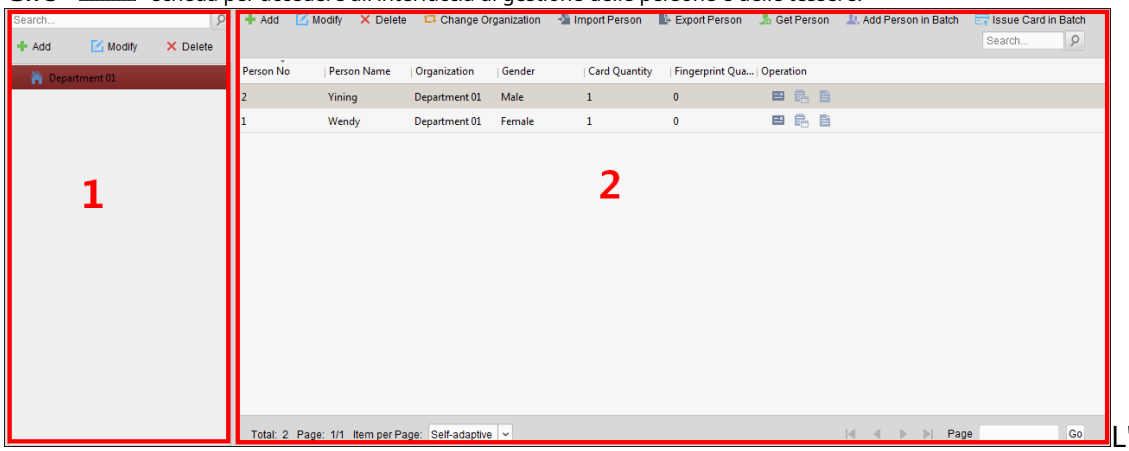
Clic **Stato -> Relè** per visualizzare lo stato del relè.



7.5 Gestione delle persone e delle carte

È possibile aggiungere, modificare ed eliminare l'organizzazione e la persona nel modulo Gestione persone e tessere.

Clic  scheda per accedere all'interfaccia di gestione delle persone e delle tessere.



L'interfaccia è diviso in due parti: Gestione organizzazione e Gestione delle persone.

1	**Organizzazione** **Gestione**	Puoi aggiungere, modificare o eliminare l'organizzazione come desiderato.
2	**Gestione delle persone**	Dopo aver aggiunto l'organizzazione, è possibile aggiungere la persona all'organizzazione e rilasciare la carta alle persone per ulteriore gestione.

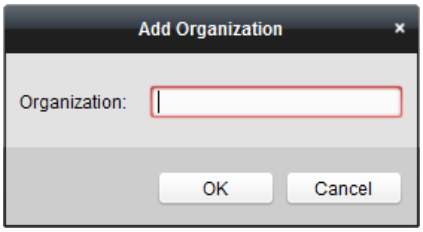
7.5.1 OrganizzazioneGestione

Aggiunta di organizzazione

Passaggi:

1. Nell'elenco delle organizzazioni a sinistra, è necessario aggiungere un'organizzazione principale come organizzazione principale di tutte le organizzazioni.

   Clic **Inserisci** pulsante per visualizzare l'interfaccia di aggiunta dell'organizzazione.



2. Immettere il nome dell'organizzazione come
3. desiderato. Clic **ok** per salvare l'aggiunta.
4. È possibile aggiungere più livelli di organizzazioni in base alle effettive esigenze.

   Per aggiungere organizzazioni secondarie, seleziona l'organizzazione principale e fai clic su **Inserisci.**

   Ripetere *Passo 2* e *3* per aggiungere la sottoorganizzazione.

   Quindi l'organizzazione aggiunta sarà la sotto-organizzazione dell'organizzazione di livello superiore.

Nota: È possibile creare fino a 10 livelli di organizzazioni.

Modifica ed eliminazione dell'organizzazione

È possibile selezionare l'organizzazione aggiunta e fare clic su **Modificare** per modificarne il nome. È possibile selezionare un'organizzazione e fare clic su **Elimina** pulsante per eliminarlo.

Appunti:

- Anche le organizzazioni di livello inferiore verranno eliminate se elimini un'organizzazione.
- Assicurati che non ci siano persone aggiunte nell'organizzazione, altrimenti l'organizzazione non può essere eliminata.

7.5.2 Gestione delle persone

Dopo aver aggiunto l'organizzazione, è possibile aggiungere una persona all'organizzazione e gestire la persona aggiunta come l'emissione di carte in batch, l'importazione e l'esportazione di informazioni sulle persone in batch, ecc.

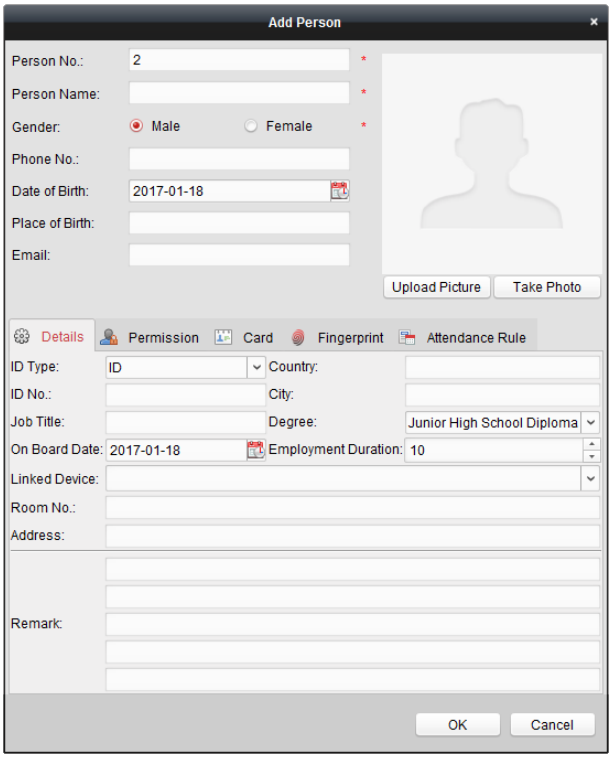
Nota: È possibile aggiungere fino a 10.000 persone o carte.

Aggiunta di una persona

Aggiunta di una persona (informazioni di base)

Passaggi:

1. Selezionare un'organizzazione nell'elenco delle organizzazioni e fare clic su **Inserisci** pulsante sul pannello Persona per far apparire nella finestra di dialogo per l'aggiunta di una persona.



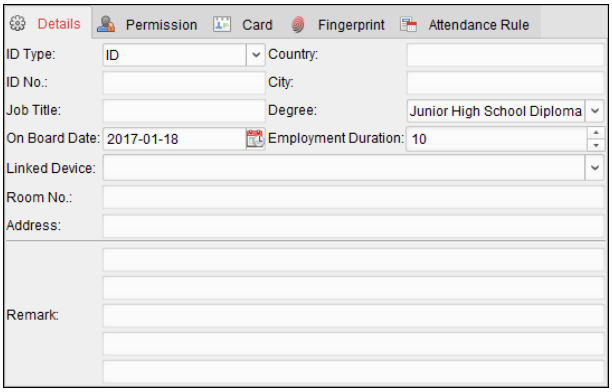
2. Il numero della persona verrà generato automaticamente e non è modificabile.
3. Immettere le informazioni di base tra cui nome della persona, sesso, numero di telefono, dettagli sulla data di nascita e indirizzo e-mail.
4. Clic **Carica l'immagine** per selezionare l'immagine della persona dal PC locale per caricarla sul client.

   Nota: L'immagine dovrebbe essere in formato * .jpg. (Facoltativo) Puoi anche fare clic su **Prendi il telefono** per scattare
5. la foto della persona con la fotocamera del PC. Clic **ok** per finire di aggiungere.
6.

Aggiunta di una persona (informazioni dettagliate)

Passaggi:

1. Nell'interfaccia Aggiungi persona, fare clic su **Dettagli** tab.



2. Immettere le informazioni dettagliate della persona, incluso il tipo di ID della persona, il numero di ID, il paese, ecc., In base alle effettive esigenze.
   - **Dispositivo collegato:** Puoi associare il posto interno alla persona.

     Nota: Se selezioni **Stazione interna analogica** nel dispositivo collegato, il file **Posto esterno** verrà visualizzato il campo e verrà richiesto di selezionare il posto esterno per comunicare con l'analogico

posto interno.

- **Stanza No.:** È possibile inserire il numero della stanza della persona.

3. Fare clic su **ok** per salvare le impostazioni.

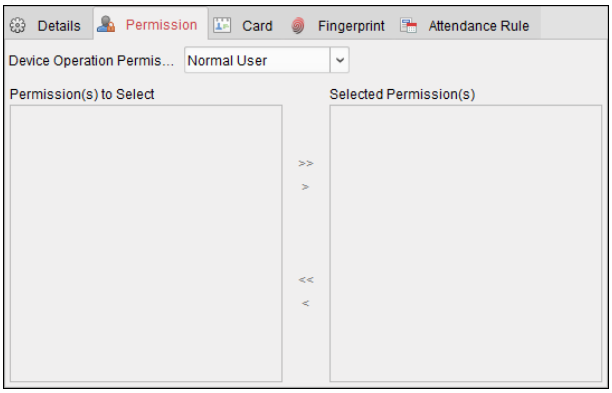
Aggiunta di una persona (autorizzazione)

È possibile assegnare le autorizzazioni (comprese le autorizzazioni di funzionamento del dispositivo di controllo dell'accesso e le autorizzazioni di controllo dell'accesso) alla persona quando si aggiunge una persona.

Nota: Per impostare l'autorizzazione al controllo dell'accesso, fare riferimento a *Capitolo 7.7 Configurazione delle autorizzazioni.*

Passaggi:

1. Nell'interfaccia Aggiungi persona, fare clic su **Autorizzazione** tab.



2. Nel campo Ruolo operazione dispositivo, selezionare il ruolo di funzionamento del dispositivo di controllo degli accessi.
   Utente normale: La persona ha il permesso di effettuare il check-in / out sul dispositivo, passare il punto di controllo accessi, ecc.
   Amministratore: La persona ha la normale autorizzazione dell'utente, nonché l'autorizzazione per configurare il dispositivo, inclusa l'aggiunta di un utente normale, ecc.
3. Nell'elenco Autorizzazioni da selezionare, vengono visualizzate tutte le autorizzazioni configurate.
   Seleziona le caselle di controllo delle autorizzazioni e fai clic su> per aggiungerle all'elenco delle autorizzazioni selezionate.
   (Facoltativo) È possibile fare clic su >> per aggiungere tutte le autorizzazioni visualizzate all'elenco delle autorizzazioni selezionate.

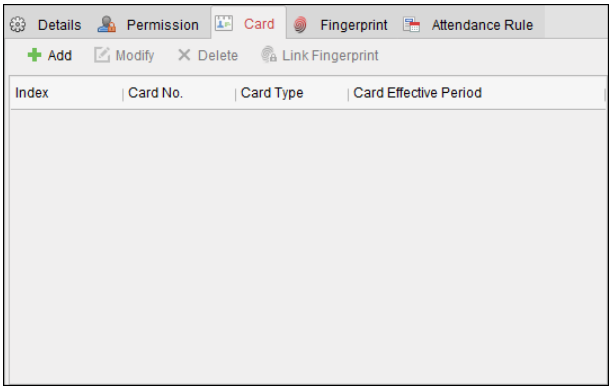
   (Facoltativo) Nell'elenco Autorizzazioni selezionate, selezionare l'autorizzazione selezionata e fare clic su <per rimuoverla. Puoi anche fare clic su << per rimuovere tutte le autorizzazioni selezionate.
4. Clic **ok** per salvare le impostazioni.

Aggiunta di una persona (carta)

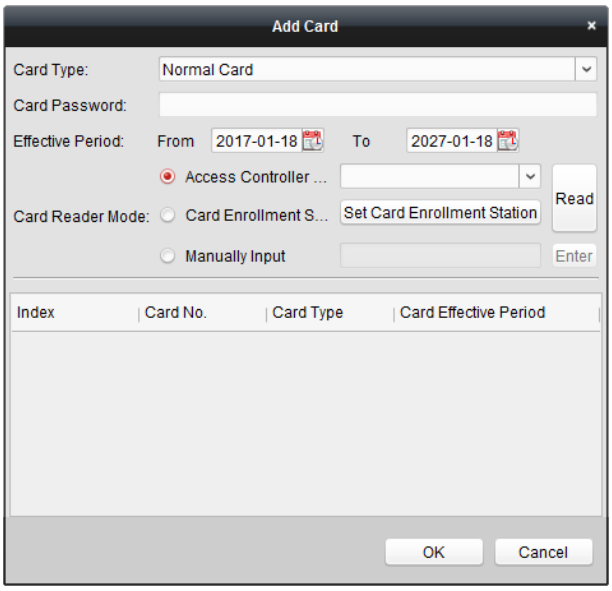
Puoi aggiungere la carta ed emettere la carta alla persona.

Passaggi:

1. Nell'interfaccia Aggiungi persona, fare clic su **Carta** tab.



2. Fare clic su **Inserisci** per visualizzare la finestra di dialogo Aggiungi scheda.



3. Selezionare il tipo di carta in base alle effettive esigenze.

- **Carta normale**
- **Scheda per apertura estesa della porta:** La porta rimarrà aperta per il periodo di tempo configurato per il titolare della carta.
- **Carta nella block list:** L'azione di scorrimento della carta verrà caricata e la porta non potrà essere aperta.
- **Carta pattuglia:** L'azione di scorrimento della carta può essere utilizzata per controllare lo stato di lavoro del personale di ispezione. Il permesso di accesso del personale di ispezione è configurabile.
- **Carta coercizione:** La porta può aprirsi facendo scorrere la carta coercizione quando c'è costrizione. Allo stesso tempo, il cliente può segnalare l'evento di coercizione.
- **Super Card:** La tessera è valida per tutte le porte del controllore durante l'orario configurato.
- **Carta dei visitatori:** La carta è assegnata ai visitatori. Per la Visitor Card è possibile impostare il file **Max. Tempi di scorrimento.**

  Appunti:

  - Il Max. I tempi di scorrimento devono essere compresi tra 0 e 255. Quando i tempi di scorrimento della carta sono superiori ai tempi configurati, lo scorrimento della carta non sarà valido.
  - Quando si impostano i tempi a 0, significa che lo scorrimento della carta è illimitato.

4. Immettere la password della scheda stessa nel campo Password scheda. La password della carta deve contenere da 4 a 8 cifre.

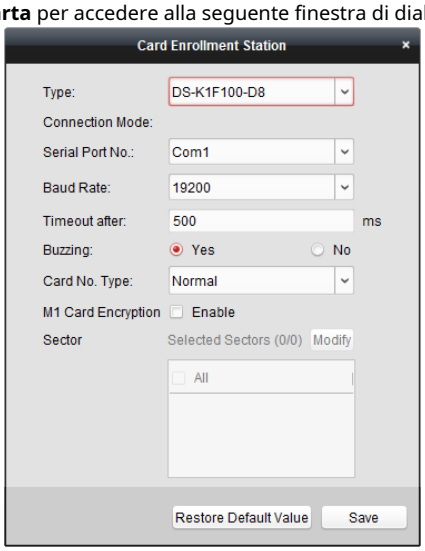
   Nota: La password sarà richiesta quando il titolare della carta strisciando la carta per entrare o uscire dalla porta se abiliti la modalità di autenticazione del lettore di carte **Carta e password, password e impronta digitale,** e **Carta, password e impronta digitale.** Per dettagli, *Capitolo 7.8.2 Autenticazione del lettore di schede.*

5. Clic per impostare l'ora effettiva e l'ora di scadenza della carta.
6. Selezionare la modalità lettore di schede per leggere la scheda n.

   - **Lettore controller di accesso:** Posizionare la carta sul lettore del controller di accesso e fare clic **Leggere** per ottenere la carta n.

- **Stazione di registrazione della carta:** Posizionare la carta sulla stazione di registrazione delle carte e fare clic **Leggere** per ottenere la carta n.

  Nota: La Card Enrollment Station dovrebbe connettersi al PC su cui è in esecuzione il client. Puoi fare clic **Impostare la stazione di registrazione della carta** per accedere alla seguente finestra di dialogo.



  2) Selezionare il tipo di stazione di registrazione tessere.

  Nota: Attualmente, i tipi di lettori di schede supportati includono DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E e DS-K1F180-D8E.

  3) Impostare il numero di porta seriale, la velocità di trasmissione, il valore di timeout, il ronzio o il tipo di numero di scheda.

  Nota: Il controller di accesso della serie DS-K2800 non supporta la funzione di crittografia della scheda M1.

  4) Clic **Salva** pulsante per salvare le impostazioni.

  Puoi fare clic **Ripristina valore predefinito** pulsante per ripristinare le impostazioni predefinite.

- **Inserimento manuale:** Immettere il numero di carta e fare clic **accedere** per inserire la carta No.

7. Fare clic su **ok** e la carta o le carte verranno rilasciate alla persona.

8. (Facoltativo) È possibile selezionare la carta aggiunta e fare clic su **modificare** o **Elimina** per modificare o eliminare la carta.

9. Fare clic su **ok** per salvare le impostazioni.

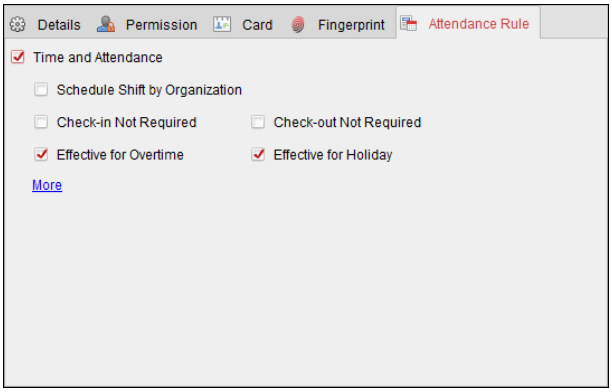
Aggiunta di persone (regola di presenza)

È possibile impostare la regola di presenza per la persona.

Nota: Questa pagina della scheda verrà visualizzata quando si seleziona **Non residenza** modalità nella scena dell'applicazione quando si esegue il software per la prima volta.

Passaggi:

1. Nell'interfaccia Aggiungi persona, fare clic su **Regola di partecipazione** tab.



2. Se la persona si unisce agli orari e alle presenze, controllare il file **Tempo e presenza** casella di controllo a abilitare questa funzione per la persona. Quindi i record di scorrimento della scheda della persona verranno registrati e analizzati per tempo e presenze.

   Per dettagli su tempo e presenza, fare clic su **Di più** per andare al modulo Time and Attendance.

3. Fare clic su **ok** per salvare le impostazioni.

Importazione ed esportazione di informazioni sulla persona

Le informazioni sulla persona possono essere importate ed esportate in batch.

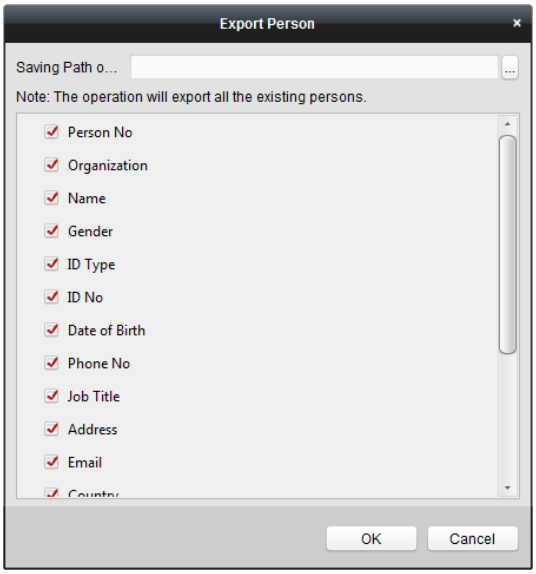
Passaggi:

1. **Persona esportatrice:** È possibile esportare le informazioni sulle persone aggiunte in formato Excel nel locale PC.

   1) Dopo aver aggiunto la persona, puoi fare clic su **Esporta persona** nella scheda Persona e scheda a compare la seguente finestra di dialogo.

   2) Fare clic su ... per selezionare il percorso di salvataggio del file Excel esportato.

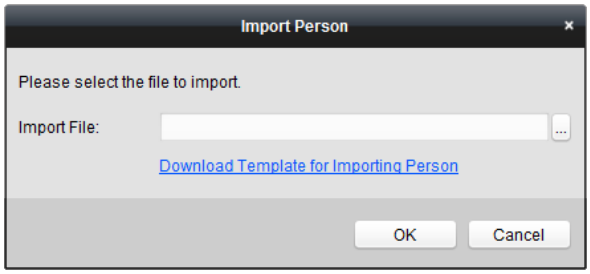
   3) Selezionare le caselle di controllo per selezionare le informazioni sulla persona da esportare.



   4) Fare clic su **ok** per avviare l'esportazione.

2. **Persona importatrice:** È possibile importare il file Excel con le informazioni sulle persone in batch dal file PC locale

   1) fare clic **Importa persona** pulsante nella scheda Persona e scheda.



2) Puoi fare clic **Scarica il modello per l'importazione della persona** per scaricare prima il modello.

3) Immettere le informazioni sulla persona nel modello scaricato.

4) Fare clic su ... per selezionare il file Excel con le informazioni sulla persona.

5) Fare clic su **ok** per avviare l'importazione.

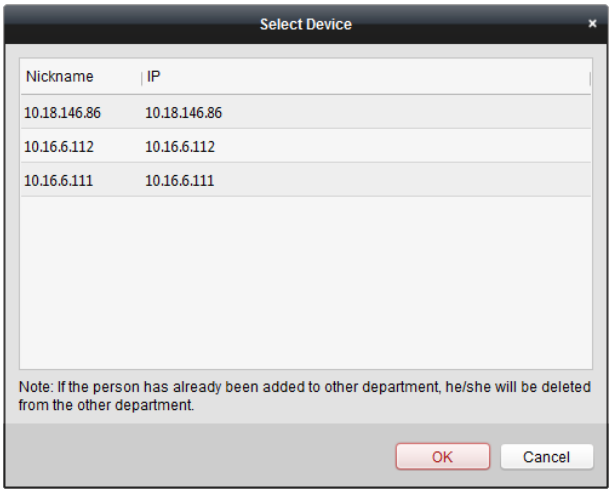
Recupero delle informazioni sulla persona dal dispositivo di controllo degli accessi

Se il dispositivo di controllo accessi aggiunto è stato configurato con le informazioni sulla persona (inclusi i dettagli della persona, l'impronta digitale, le informazioni sulla carta emessa), è possibile ottenere le informazioni sulla persona dal dispositivo e importarle nel client per ulteriori operazioni.

Nota: Questa funzione è supportata solo dal dispositivo la cui modalità di connessione è TCP / IP quando si aggiunge il dispositivo.

Passaggi:

1. Nell'elenco delle organizzazioni a sinistra, fare clic per selezionare un'organizzazione per importare le persone.
2. Fare clic su **Ottieni persona** per visualizzare la seguente finestra di dialogo.



3. Verrà visualizzato il dispositivo di controllo accessi aggiunto. Fare clic per selezionare il dispositivo, quindi fare clic su **ok**
4. per iniziare a ottenere le informazioni sulla persona dal dispositivo.

Puoi anche fare doppio clic sul nome del dispositivo per iniziare a ottenere le informazioni sulla persona.

Appunti:

- Le informazioni sulla persona, inclusi i dettagli della persona, le informazioni sull'impronta digitale della persona (se configurato) e la scheda collegata (se configurata) verrà importata nell'organizzazione selezionata.
- Se il nome della persona memorizzato nel dispositivo è vuoto, il nome della persona verrà riempito con il numero della carta emessa dopo l'importazione nel client.
- Il sesso delle persone sarà **Maschio** per impostazione predefinita.
- È possibile importare fino a 10000 persone con un massimo di 5 carte ciascuna.

Persona di gestione

Modifica ed eliminazione di una persona

Per modificare le informazioni sulla persona e la regola di presenza, fare clic su o selezionare la persona e O nella colonna Operazione, fare clic su **Modificare** per aprire la finestra di dialogo della persona di modifica. Puoi fare clic per visualizzare i record di scorrimento della scheda della persona.

Per eliminare la persona, seleziona una persona e fai clic su **Elimina** per eliminarlo.

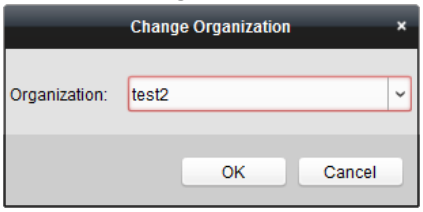
Nota: Se una carta viene rilasciata alla persona corrente, il collegamento non sarà valido dopo che la persona è stata eliminata.

Cambio di persona in un'altra organizzazione

Puoi spostare la persona in un'altra organizzazione, se necessario.

Passaggi:

1. Selezionare la persona nell'elenco e fare clic su **Cambia organizzazione** pulsante.



2. Selezionare l'organizzazione in cui spostare la persona.

3. Fare clic su **ok** per salvare le impostazioni.

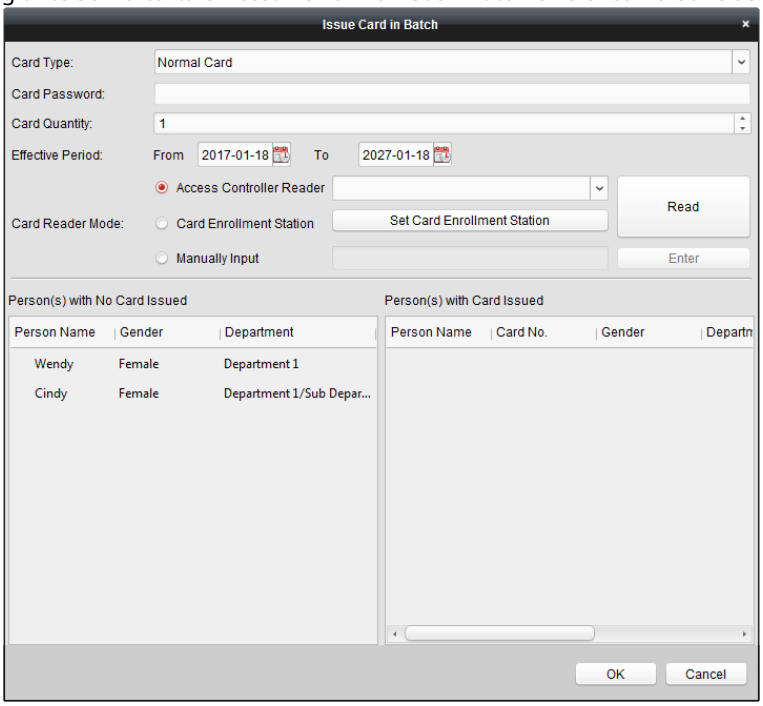
Emissione della carta in batch

Puoi emettere più carte per la persona senza carta emessa in batch.

Passaggi:

1. Fare clic su **Carta dei problemi in batch** per accedere alla seguente finestra di dialogo.

Tutte le persone aggiunte senza carta emessa verranno visualizzate nell'elenco Persone senza carta emessa.



2. Selezionare il tipo di carta in base alle effettive esigenze.

Nota: Per i dettagli sul tipo di carta, fare riferimento a *Aggiunta di una persona.*

3. Immettere la password della scheda stessa nel campo Password scheda. La password della carta deve contenere da 4 a 8 cifre.

   Nota: La password sarà richiesta quando il titolare della carta strisciando la carta per entrare o uscire dalla porta se abiliti la modalità di autenticazione del lettore di carte **Carta e password, password e impronta digitale,** e **Carta, password e impronta digitale.** Per i dettagli, fare riferimento a *Capitolo 7.8.2 Autenticazione del lettore di schede.*

4. Immettere la quantità di carte emesse per ogni persona.

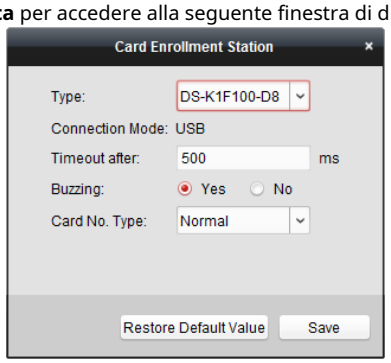
   Ad esempio, se la quantità della carta è 3, è possibile leggere o inserire tre numeri di carta per ogni persona.

5. Clic  per impostare l'ora effettiva e l'ora di scadenza della carta.

6. Selezionare la modalità lettore di schede per leggere la scheda n.

   - **Lettore controller di accesso:** Posizionare la carta sul lettore del controller di accesso e fare clic **Leggere** per ottenere la carta n.
   - **Stazione di registrazione della carta:** Posizionare la carta sulla stazione di registrazione delle carte e fare clic **Leggere** per ottenere la carta n.

     Nota: La Card Enrollment Station dovrebbe connettersi al PC su cui è in esecuzione il client. Puoi fare clic **Impostare la stazione di registrazione della carta** per accedere alla seguente finestra di dialogo.



     1) Selezionare il tipo di stazione di registrazione tessere.

        Nota: Attualmente, i tipi di lettori di schede supportati includono DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E e DS-K1F180-D8E.

     2) Impostare i parametri sulla stazione di registrazione della carta collegata. Clic **Salva** pulsante
     3) per salvare le impostazioni. Puoi fare clic **Ripristina valore predefinito** pulsante per ripristinare le impostazioni predefinite.

   - **Inserimento manuale:** Immettere il numero di carta e fare clic **accedere** per inserire la carta No.

7. Dopo aver rilasciato la carta alla persona, le informazioni sulla persona e sulla carta verranno visualizzate nell'elenco Persona / e con carta emessa.

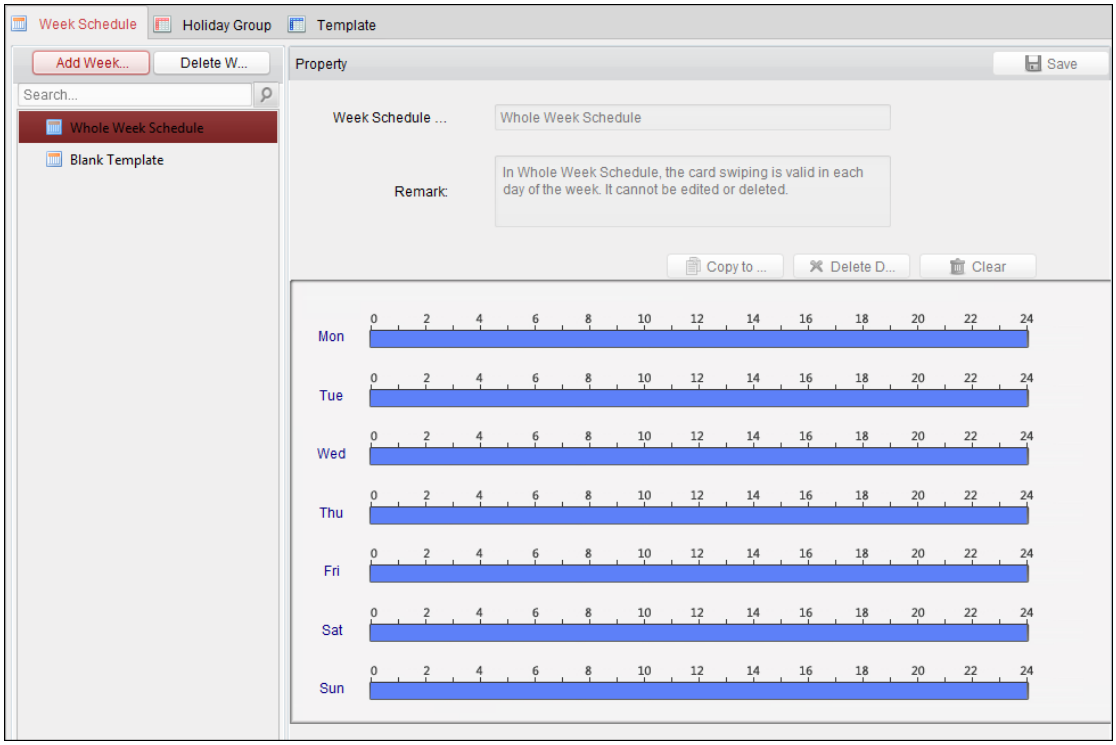
8. Fare clic su **ok** per salvare le impostazioni.

7.6 Programma e modello

Scopo:

È possibile configurare il modello includendo la pianificazione settimanale e la pianificazione delle vacanze. Dopo aver impostato i modelli, è possibile adottare i modelli configurati per le autorizzazioni di controllo dell'accesso quando si imposta l'autorizzazione, in modo che l'autorizzazione di controllo dell'accesso abbia effetto nelle durate del modello.

Clic  per accedere all'interfaccia del programma e del modello.



È possibile gestire la pianificazione dell'autorizzazione al controllo dell'accesso, inclusi pianificazione settimanale, pianificazione festività e modello. Per le impostazioni dei permessi, fare riferimento a *Capitolo 7.7 Configurazione delle autorizzazioni.*

7.6.1 Programma settimanale

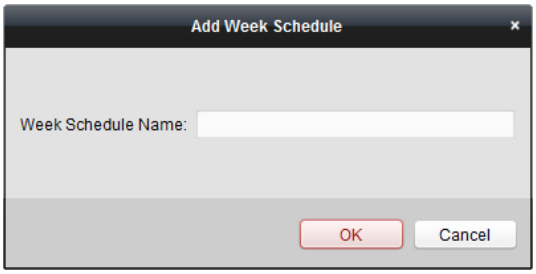
Clic **Programma settimanale** scheda per accedere all'interfaccia di gestione della pianificazione settimanale. Il cliente definisce di default due tipi di piano settimanale: **Programma dell'intera settimana** e **Programma vuoto,**
che non possono essere cancellati e modificati.

- **Programma dell'intera settimana:** Lo scorrimento della carta è valido ogni giorno della settimana.
- **Programma vuoto:** Lo scorrimento della carta non è valido ogni giorno della settimana.

È possibile eseguire i seguenti passaggi per definire pianificazioni personalizzate su richiesta.

Passaggi:

1. Fare clic su **Aggiungi programma settimanale** pulsante per visualizzare l'interfaccia di aggiunta della pianificazione.



2. Immettere il nome della pianificazione settimanale e fare clic su **ok** pulsante per aggiungere il programma settimanale.
3. Selezionare la pianificazione settimanale aggiunta nell'elenco di pianificazione e visualizzare le sue proprietà sulla destra. È possibile modificare il nome del programma settimanale e inserire le informazioni sul commento.
4. Nella pianificazione settimanale, fare clic e trascinare su un giorno per disegnare sulla pianificazione, il che significa in quello

periodo di tempo, l'autorizzazione configurata viene attivata.

Nota: È possibile impostare fino a 8 periodi di tempo per ogni giorno nel programma.

5. Quando il cursore si trasforma in , puoi spostare la barra temporale selezionata che hai appena modificato. Puoi anche modificare il punto temporale visualizzato per impostare il periodo di tempo preciso.

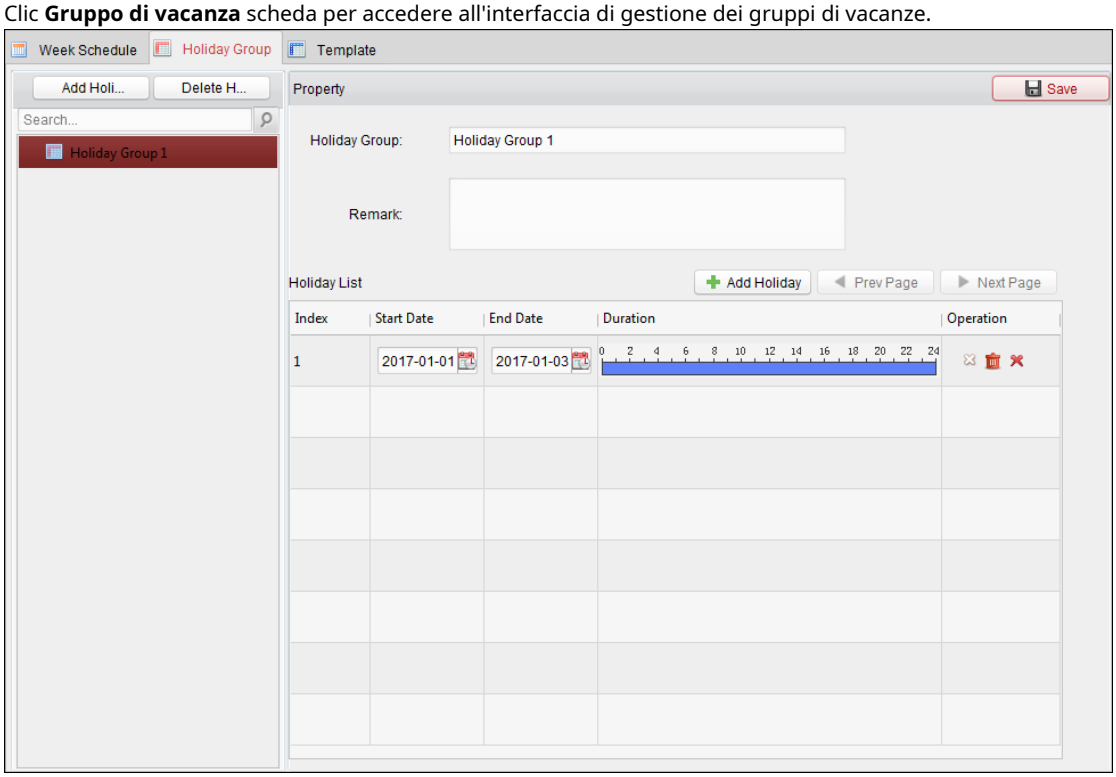
   Quando il cursore si trasforma in , puoi allungare o accorciare la barra temporale selezionata.

6. Facoltativamente, è possibile selezionare la barra dell'orario di pianificazione e quindi fare clic su **Elimina durata** per eliminare la barra temporale selezionata oppure fare clic su **Chiaro** per eliminare tutte le barre temporali oppure fare clic su **Copia in settimana** per copiare le impostazioni della barra temporale per l'intera settimana. Clic **Salva** per salvare le impostazioni.

7.

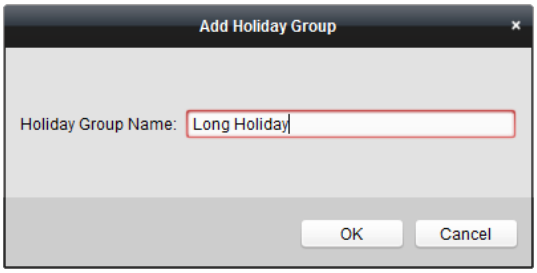
7.6.2 Gruppo di vacanze

Clic **Gruppo di vacanza** scheda per accedere all'interfaccia di gestione dei gruppi di vacanze.



Passaggi:

1. Fare clic su **Aggiungi gruppo vacanze** a sinistra per visualizzare l'interfaccia di aggiunta del gruppo di vacanze.

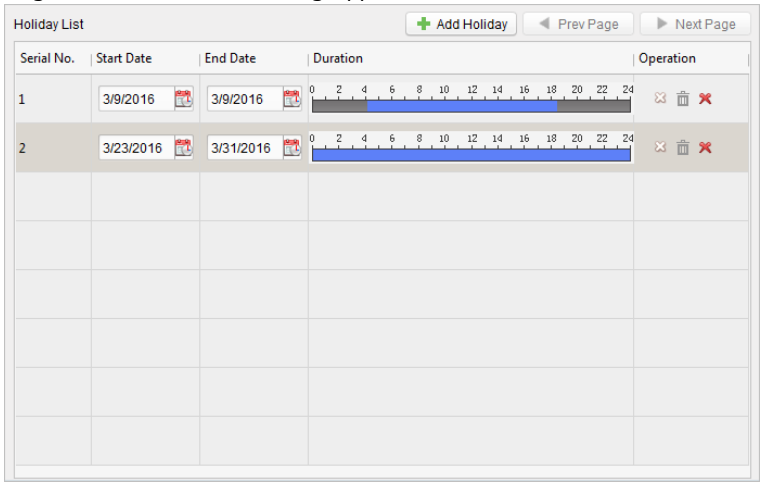


2. Immettere il nome del gruppo di vacanze nel campo di testo e fare clic su **ok** pulsante per aggiungere il gruppo di vacanze.
3. Selezionare il gruppo di vacanze aggiunto e modificare il nome del gruppo di vacanze e inserire il commento

informazione.

4. Fare clic su **Aggiungi vacanza** a destra per aggiungere un periodo di vacanza all'elenco delle festività e configurare il durata della vacanza.

Nota: È possibile aggiungere fino a 16 vacanze a un gruppo di vacanze.



1) Nella pianificazione del periodo, fare clic e trascinare per disegnare il periodo, il che significa che in quel periodo di tempo viene attivata l'autorizzazione configurata.

   Nota: È possibile impostare fino a 8 durate di tempo per ogni periodo del programma.

2) Quando il cursore si trasforma in  , puoi spostare la barra temporale selezionata che hai appena modificato. Puoi modificare anche il punto temporale visualizzato per impostare il periodo di tempo preciso.

3) Quando il cursore si trasforma in  , puoi allungare o accorciare la barra temporale selezionata.

4) Facoltativamente, è possibile selezionare la barra dell'orario di pianificazione, e quindi fare clic su  per eliminare la barra temporale selezionata, o fare clic su  per eliminare tutte le barre temporali delle festività oppure fare clic su  per eliminare direttamente la vacanza.

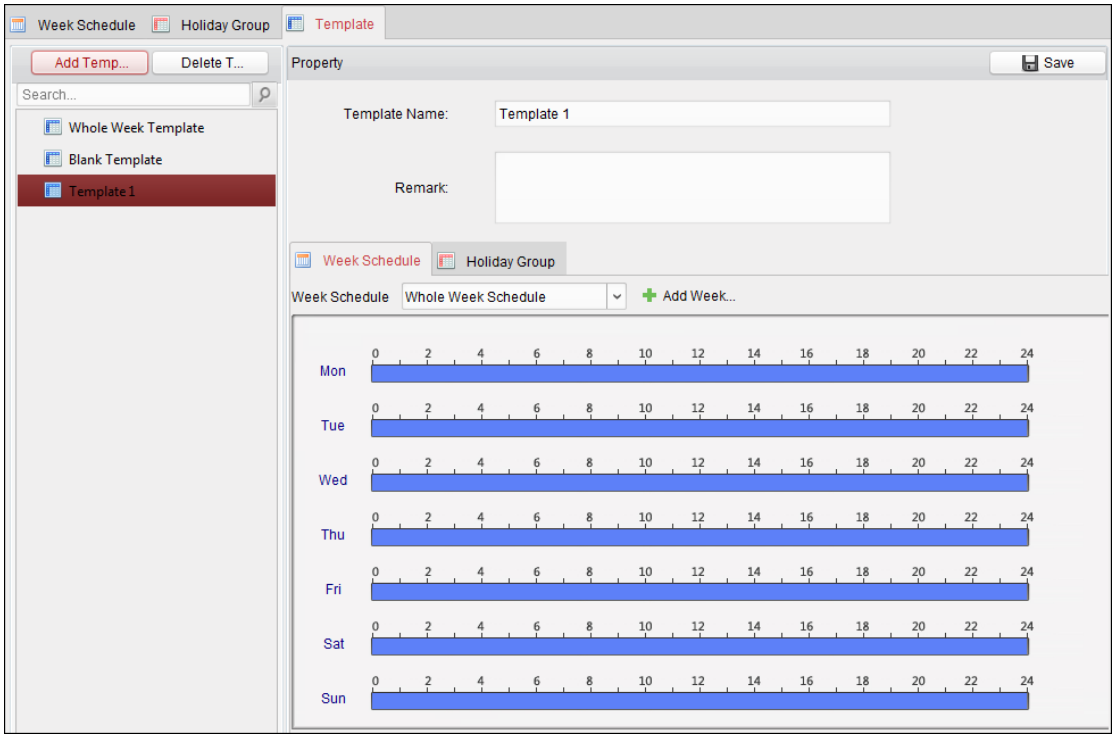
5. Fare clic su **Salva** per salvare le impostazioni.

Nota: Le festività non possono essere sovrapposte tra loro.

7.6.3 Modello

Dopo aver impostato la pianificazione settimanale e il gruppo di festività, è possibile configurare il modello che contiene la pianificazione settimanale e la pianificazione del gruppo di festività.

Nota: La priorità della pianificazione del gruppo di vacanze è superiore alla pianificazione settimanale. Clic **Modello** scheda per accedere all'interfaccia di gestione dei modelli.



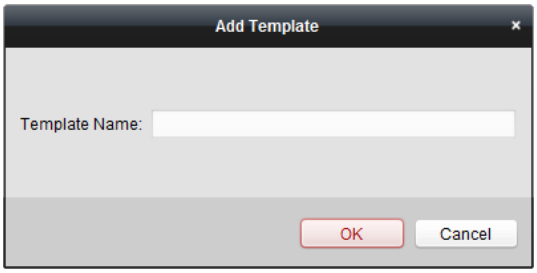
Esistono due modelli predefiniti per impostazione predefinita: **Modello di intera settimana** e **Modello vuoto,** che non possono essere cancellati e modificati.

- **Modello intera settimana:** Lo swipe della carta è valido tutti i giorni della settimana e non ha festività programma di gruppo.
- **Modello vuoto:** Lo scorrimento della carta non è valido ogni giorno della settimana e non ha un programma di gruppo festivo.

Puoi definire modelli personalizzati su tua richiesta.

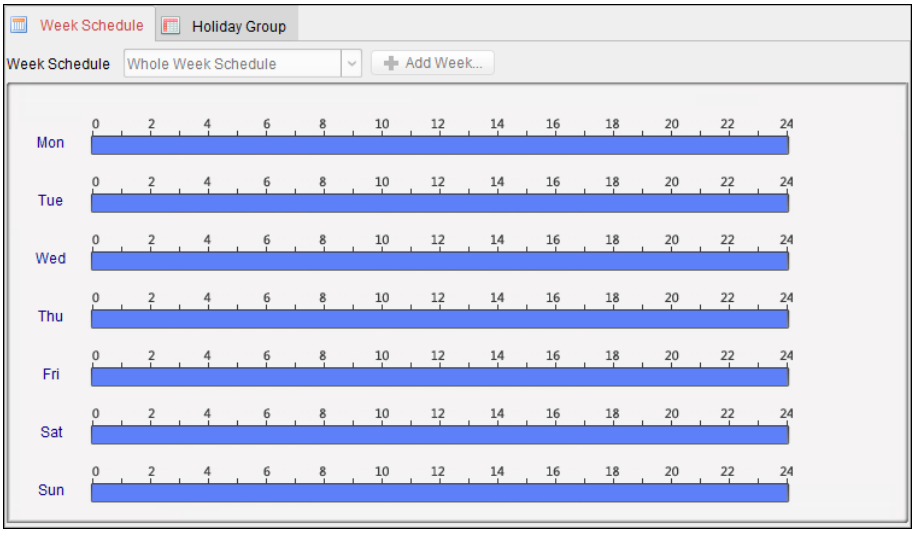
Passaggi:

1. Fare clic su **Aggiungi modello** per far apparire l'interfaccia di aggiunta del modello.



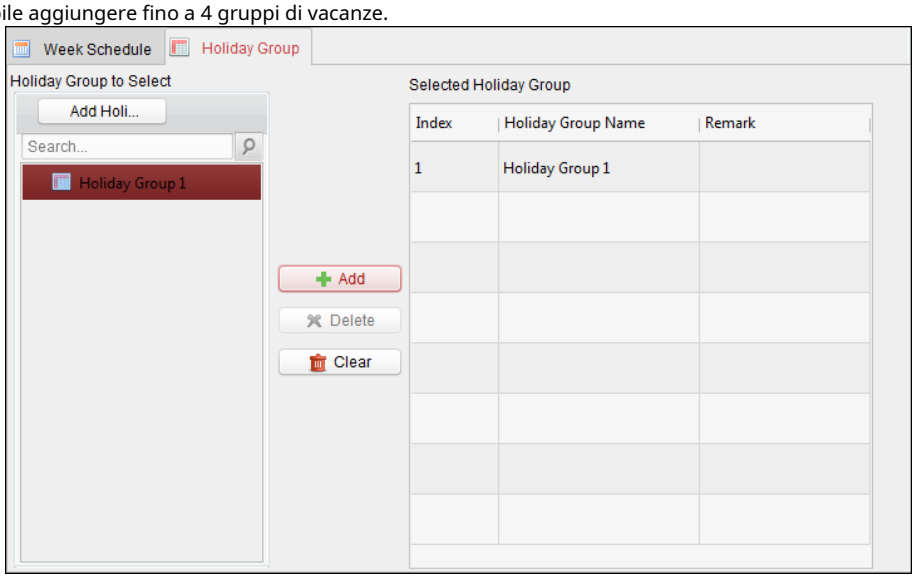
2. Immettere il nome del modello nel campo di testo e fare clic **ok** pulsante per aggiungere il modello.
3. Seleziona il modello aggiunto e puoi modificarne la proprietà sulla destra. È possibile modificare il nome del modello e inserire le informazioni sul commento.
4. Seleziona un programma settimanale da applicare al programma.

   Clic **Programma settimanale** scheda e selezionare una pianificazione nell'elenco a discesa. Puoi anche fare clic su **Aggiungi programma settimanale** per aggiungere un nuovo programma settimanale. Per i dettagli, fare riferimento a *Capitolo 7.6.1 Programma settimanale.*



5. Selezionare i gruppi di festività da applicare alla pianificazione.

Nota: È possibile aggiungere fino a 4 gruppi di vacanze.



Fare clic per selezionare un gruppo di vacanze nell'elenco e fare clic su **Inserisci** per aggiungerlo al modello. Puoi anche fare clic su **Aggiungi gruppo vacanze** per aggiungerne uno nuovo. Per i dettagli, fare riferimento a *Capitolo 7.6.2 Gruppo di vacanze.*

È possibile fare clic per selezionare un gruppo di vacanze aggiunto nell'elenco a destra e fare clic **Elimina** per eliminarlo.

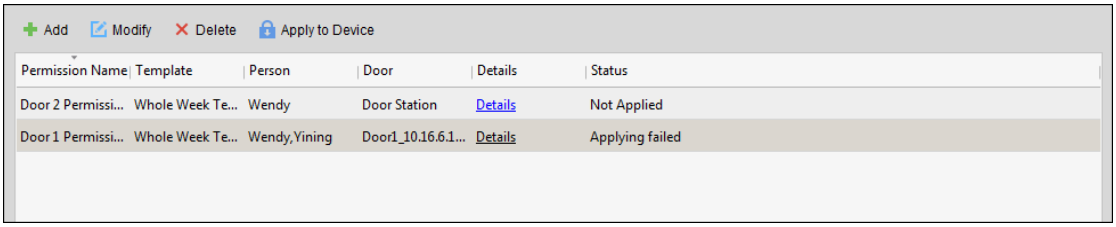
Puoi fare clic **Chiaro** per eliminare tutti i gruppi di vacanze aggiunti.

6. Fare clic su **Salva** pulsante per salvare le impostazioni.

7.7 Configurazione delle autorizzazioni

Nel modulo Configurazione autorizzazioni, è possibile aggiungere, modificare ed eliminare l'autorizzazione di controllo dell'accesso, quindi applicare le impostazioni di autorizzazione al dispositivo affinché abbiano effetto.

Clic  per accedere all'interfaccia di autorizzazione del controllo di accesso.



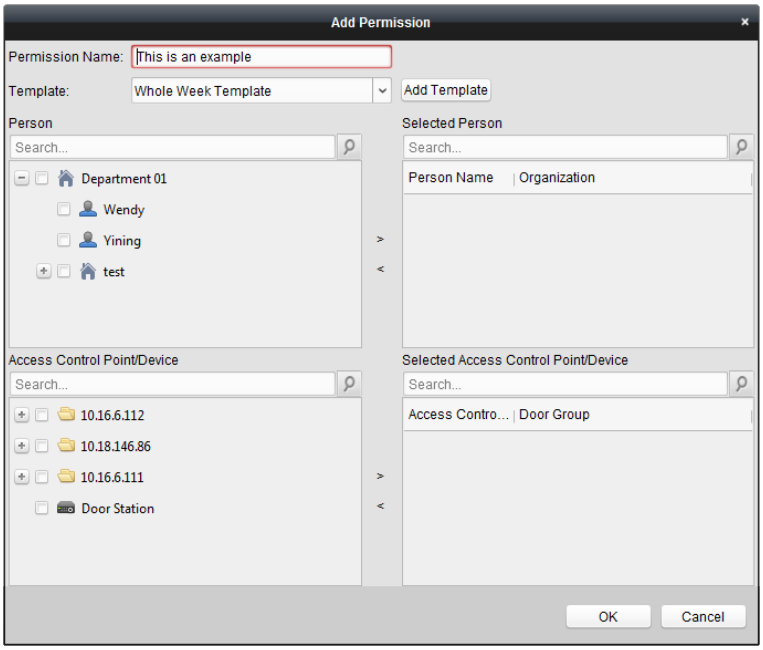
7.7.1 Aggiunta dell'autorizzazione

Scopo:

È possibile assegnare il permesso alle persone di entrare / esistere nei punti di controllo dell'accesso (porte) in questa sezione.

Passaggi:

1. Fare clic su **Inserisci** per accedere alla seguente interfaccia.



2. Nel campo Nome autorizzazione, immettere il nome dell'autorizzazione come desiderato.
3. Fare clic sul menu a discesa per selezionare un modello per l'autorizzazione.

   Nota: È necessario configurare il modello prima delle impostazioni delle autorizzazioni. Puoi fare clic **Aggiungi modello** pulsante per aggiungere il modello. Fare riferimento a *Capitolo 7.6 Programma e modello* per dettagli. Nell'elenco Persona, vengono
4. visualizzate tutte le persone aggiunte.

   Seleziona le caselle di controllo per selezionare le persone e fai clic su> per aggiungerle all'elenco delle persone selezionate.

   (Facoltativo) È possibile selezionare la persona nell'elenco Persona selezionata e fare clic su <per annullare la selezione.
5. Nell'elenco Access Control Point / Device, verranno visualizzati tutti i punti di controllo accessi (porte) e le stazioni porta aggiunti.

   Selezionare le caselle di controllo per selezionare le porte o i citofoni esterni e fare clic su> per aggiungere all'elenco selezionato.

   (Facoltativo) È possibile selezionare la porta o il posto esterno nell'elenco selezionato e fare clic su <per annullare la selezione.
6. Clic **ok** pulsante per completare l'aggiunta dell'autorizzazione. La persona selezionata avrà il

permesso di entrare / uscire dal posto esterno / posto esterno selezionato con le loro carte collegate o impronte digitali.

7. (Facoltativo) dopo aver aggiunto l'autorizzazione, è possibile fare clic su **Dettagli** per modificarlo. Oppure puoi selezionare il file permesso e fare clic **Modificare** modificare.

   È possibile selezionare l'autorizzazione aggiunta nell'elenco e fare clic su **Elimina** per eliminarlo.

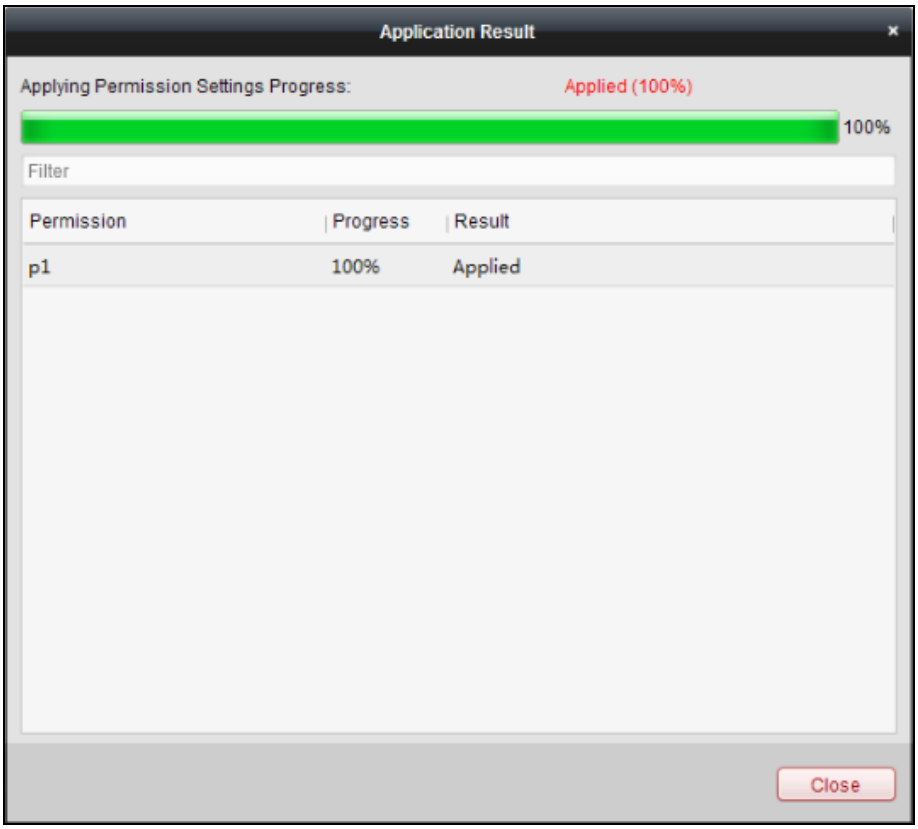
7.7.2 Applicazione dell'autorizzazione

Scopo:

Dopo aver configurato le autorizzazioni, è necessario applicare l'autorizzazione aggiunta al dispositivo di controllo degli accessi affinché abbia effetto.

Passaggi:

1. Selezionare le autorizzazioni da applicare al dispositivo di controllo accessi. Per selezionare più autorizzazioni, puoi tenere il *Ctrl* o *Cambio* chiave e selezionare le autorizzazioni.
2. Fare clic su **Applica al dispositivo** per iniziare ad applicare le autorizzazioni selezionate al dispositivo di controllo accessi o posto esterno.
3. Apparirà la seguente finestra, indicando il risultato dell'applicazione dell'autorizzazione.



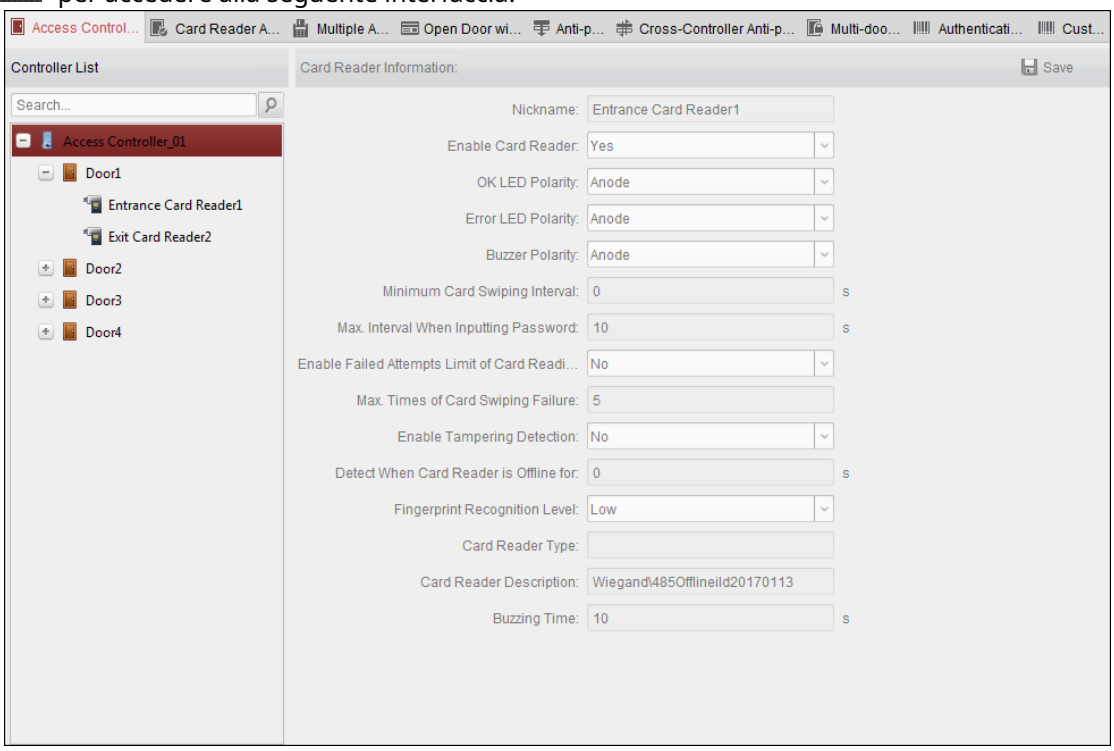
7.8 Funzioni avanzate

Scopo:

Dopo aver configurato la persona, il modello e l'autorizzazione al controllo degli accessi, è possibile configurare le funzioni avanzate dell'applicazione per il controllo degli accessi.

Nota: Le funzioni avanzate dovrebbero essere supportate dal dispositivo.

Clic  per accedere alla seguente interfaccia.



7.8.1 Parametri di controllo dell'accesso

Scopo:

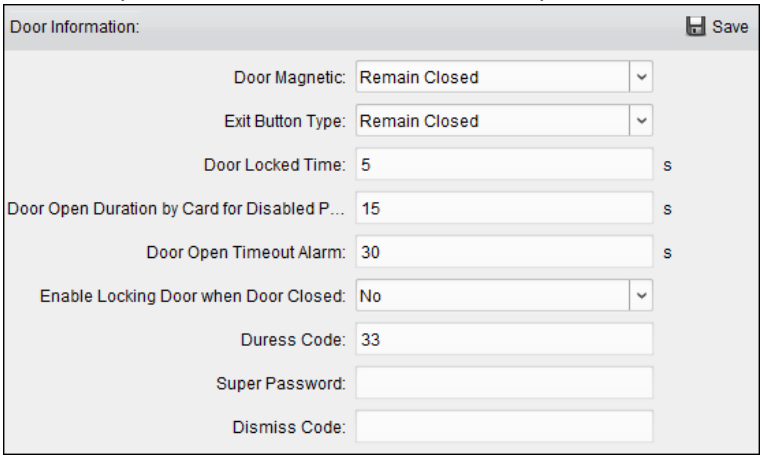
Dopo aver configurato la persona, il modello e l'autorizzazione al controllo degli accessi, è possibile configurare le funzioni avanzate dell'applicazione per il controllo degli accessi.

Clic **Parametri di controllo dell'accesso** scheda per accedere all'interfaccia delle impostazioni dei parametri.

Parametri della porta

Passaggi:

1. Nell'elenco dei controller a sinistra, fare clic su  per espandere il dispositivo di controllo accessi selezionare la porta (punto di controllo accessi) e puoi modificare le informazioni della porta selezionata sulla destra.



2. È possibile modificare i seguenti parametri:

Porta magnetica: La porta magnetica è nello stato di **Rimani chiuso (** escluse le condizioni speciali).

Tipo di pulsante di uscita: Il tipo di pulsante di uscita è nello stato di **Rimani aperto (** escluse le condizioni speciali).

Tempo di chiusura della porta: Dopo aver strisciato la carta normale e l'azione del relè, il timer per il blocco della porta inizia a funzionare.

Durata apertura porta per scheda per apertura estesa porta: Il magnete della porta può essere abilitato con un ritardo appropriato dopo che il titolare della carta ha strisciato la carta.

Allarme timeout porta aperta: L'allarme può essere attivato se la porta non è stata chiusa

Abilita il blocco della porta quando la porta è chiusa (riservato): La porta può essere bloccata una volta chiusa anche se non è stato raggiunto il tempo di chiusura della porta.

Codice coercizione: La porta può aprirsi inserendo il codice coercizione quando c'è coercizione. Allo stesso tempo, il cliente può segnalare l'evento di coercizione.

Super Password: La persona specifica può aprire la porta inserendo la super password.

Ignora codice: Immettere il codice di annullamento per interrompere il cicalino del lettore di schede.

Appunti:

- Il codice coercizione, la super password e il codice di eliminazione dovrebbero essere diversi.
- Il codice coercizione, la super password e il codice di eliminazione dovrebbero essere diversi dalla password di autenticazione.
- Il codice coercizione, la super password e il codice di eliminazione devono contenere da 4 a 8 valori numerici.

3. Fare clic su **Salva** pulsante per salvare i parametri.

Parametri del lettore di schede

Passaggi:

1. Nell'elenco dei dispositivi a sinistra, fare clic su per espandere la porta, seleziona il nome del lettore di schede e tu può modificare i parametri del lettore di schede a
2. destra. È possibile modificare i seguenti parametri:

Soprannome: Modificare il nome del lettore di schede come desiderato.

Abilita lettore di schede: Selezionare **sì** per abilitare il lettore di schede.

Polarità LED OK: Selezionare la polarità del LED OK della scheda madre del lettore di schede.

Polarità LED di errore: Selezionare la polarità del LED di errore della scheda madre del lettore di schede.

Polarità cicalino: Selezionare la polarità del LED del cicalino della scheda madre del lettore di schede.

Intervallo minimo di scorrimento della carta: Se l'intervallo tra lo scorrimento della carta della stessa carta è inferiore al valore impostato, lo scorrimento della carta non è valido. È possibile impostarlo da 0 a 255.

Max. Intervallo durante l'immissione della password: Quando si immette la password sul lettore di schede, se l'intervallo tra la pressione di due cifre è maggiore del valore impostato, le cifre che si sono premute prima verranno cancellate automaticamente.

Abilita limite tentativi falliti di lettura tessera: Abilita la segnalazione di allarme quando i tentativi di lettura della tessera raggiungono il valore impostato.

Max. Tempi di errore di scorrimento della carta: Imposta il max. tentativi falliti di lettura tessera.

Abilita rilevamento manomissione: Abilita il rilevamento antimanomissione per il lettore di carte.

Nota: Per il controller di accesso serie DS-K2800, la funzione non è ancora supportata.

Rileva quando il lettore di schede è offline per: Quando il dispositivo di controllo accessi non riesce a connettersi con

il lettore di carte per un tempo superiore al tempo impostato, il lettore di carte passerà automaticamente offline.

Nota: Per il controller di accesso serie DS-K2800, la funzione non è ancora supportata.

Tempo di ronzio: Imposta il tempo di ronzio del lettore di schede. Il tempo disponibile varia da 0 a 5999 s. 0 rappresenta un ronzio continuo.

Descrizione del lettore di schede: Leggi la descrizione del lettore di schede.

3. Fare clic su **Salva** pulsante per salvare i parametri.

7.8.2 Autenticazione del lettore di schede

Scopo:

È possibile impostare le regole di passaggio per il lettore di carte del dispositivo di controllo accessi.

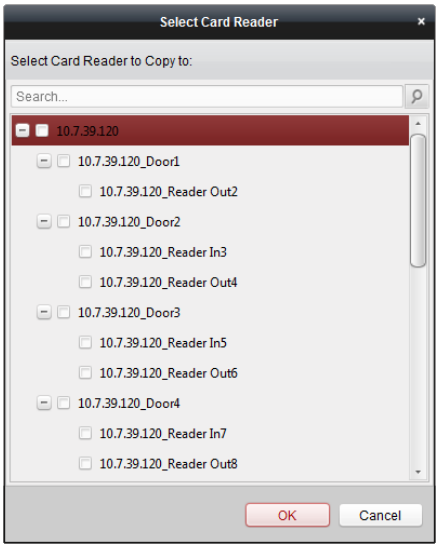
Passaggi:

1. Fare clic su **Autenticazione del lettore di schede** scheda e selezionare un lettore di schede a sinistra.
2. Selezionare una modalità di autenticazione del lettore di schede. Le modalità di autenticazione disponibili dipendono dal tipo di lettore di carte:
   - **Carta e password:** La porta può aprirsi immettendo la password della carta e facendo scorrere la carta.

     Nota: Qui la password si riferisce alla password impostata quando si rilascia la carta alla persona. *Capitolo 7.5.2 Gestione delle persone.*
   - **Carta o password di autenticazione:** La porta può aprirsi immettendo l'autenticazione password o strisciare la carta.

     Nota: Qui la password di autenticazione si riferisce alla password impostata per aprire la porta. Fare riferimento a *Capitolo 7.8.5 Password di autenticazione.*
   - **Carta:** La porta può aprirsi solo facendo scorrere la carta.
3. Fare clic e trascinare il mouse in un giorno per disegnare una barra colorata sulla pianificazione, il che significa che in quel periodo di tempo l'autenticazione del lettore di schede è valida.
4. Ripetere il passaggio precedente per impostare altri periodi di tempo. Oppure puoi selezionare un giorno configurato e fare clic su **Copia in settimana** pulsante per copiare le stesse impostazioni per l'intera settimana.

   (Facoltativo) Puoi fare clic su **Elimina** per eliminare il periodo di tempo selezionato o fare clic su **Chiaro** pulsante per eliminare tutti i periodi di tempo configurati.
5. (Facoltativo) Fare clic su **Copia a** pulsante per copiare le impostazioni su altri lettori di schede.



6. Fare clic su **Salva** pulsante per salvare i parametri.

7.8.3 Porta aperta con la prima carta

Scopo:

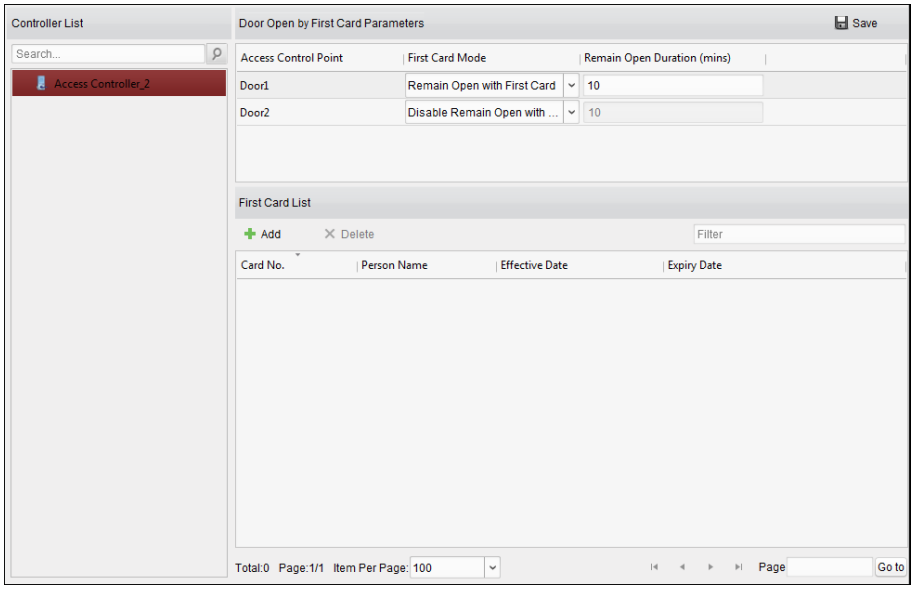
È possibile impostare più prime carte per un punto di controllo accessi. Dopo il primo passaggio della carta, consente a più persone di accedere alla porta o ad altre azioni di autenticazione. La modalità della prima carta contiene Resta aperto con la prima carta, Disabilita Resta aperto con la prima carta e Autorizzazione della prima carta.

Rimani aperto con la prima carta: La porta rimane aperta per la durata di tempo configurata dopo il primo passaggio della tessera fino al termine della durata di permanenza aperta.

Prima autorizzazione della carta: Tutte le autenticazioni, ad eccezione delle autenticazioni della super card, della carta coercizione e del codice coercizione, sono consentite solo dopo la prima autorizzazione della carta.

Passaggi:

1. Fare clic su **Porta aperta con la prima carta** scheda per accedere alla seguente interfaccia.

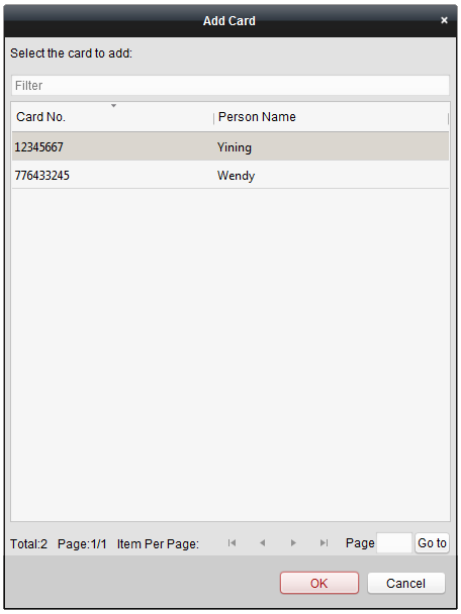


2. Selezionare un dispositivo di controllo dell'accesso dall'elenco a sinistra.

3. Selezionare la prima modalità scheda nell'elenco a discesa per il punto di controllo accessi.
4. (Facoltativo) Se selezioni Rimani aperto con la prima carta, devi impostare la durata di apertura.

   Appunti:

   - La durata residua aperta dovrebbe essere compresa tra 0 e 1440 minuti. Per impostazione predefinita, è di 10 minuti.
   - Nella modalità Autorizzazione prima carta, è possibile accedere alla porta quando si striscia la super card, la carta coercizione o si inserisce il codice coercizione senza strisciare la prima carta. È possibile scorrere
   - nuovamente la prima scheda per disabilitare la modalità della prima scheda.
   - La prima autorizzazione della carta ha effetto solo il giorno corrente. L'autorizzazione scadrà dopo le 24:00 del giorno corrente.
5. Nell'elenco Prima scheda, fare clic su **Inserisci** per visualizzare la seguente finestra di dialogo.



   1) Seleziona le carte da aggiungere come prima carta per la porta

      Nota: Impostare prima l'autorizzazione della scheda e applicare l'impostazione dell'autorizzazione al dispositivo di controllo dell'accesso. Per i dettagli, fare riferimento a *Capitolo 7.7 Configurazione delle autorizzazioni.*

   2) Fare clic su **ok** pulsante per salvare l'aggiunta della carta.

6. È possibile fare clic su **Elimina** pulsante per rimuovere la tessera dal primo elenco tessere.
7. Fare clic su **Salva** per salvare e rendere effettive le nuove impostazioni.

7.8.4 Anti-Passing Back

Scopo:

È possibile impostare l'anti-passaggio per i lettori di schede nello stesso controller di accesso. È necessario strisciare la carta in base al percorso della carta di scorrimento configurato. E solo una persona potrebbe passare il punto di controllo accessi dopo aver strisciato la carta.

Appunti:

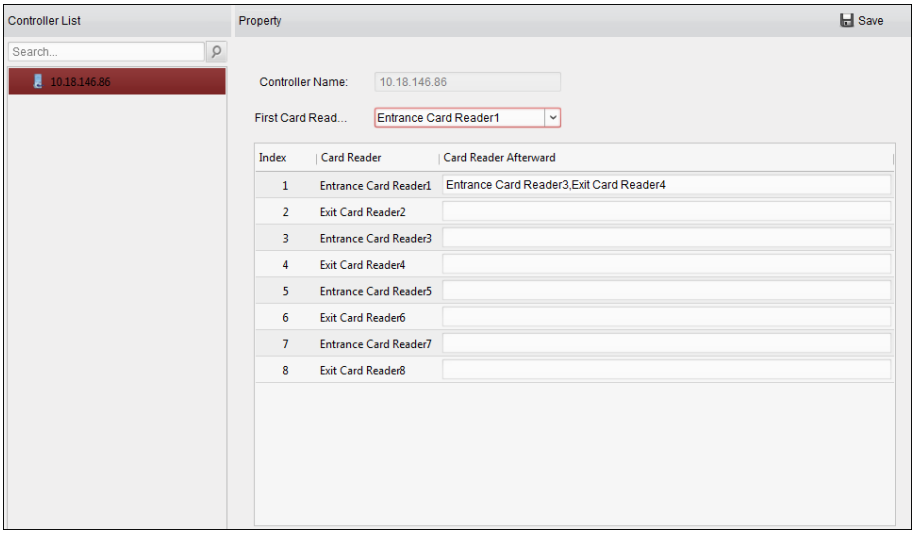
- Per un accesso è possibile configurare la funzione anti-pass back o interblocco multiporta dispositivo di controllo allo stesso tempo.

- È necessario abilitare prima la funzione anti-pass-back sul dispositivo di controllo accessi.

Impostazione del percorso di scorrimento della scheda (ordine del lettore di schede)

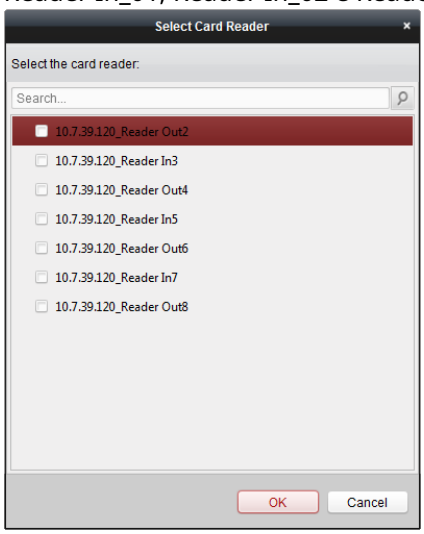
Passaggi:

1. Fare clic su **Anti-passaggio indietro** scheda per accedere alla seguente interfaccia.



2. Seleziona un dispositivo di controllo accessi dall'elenco dei dispositivi a sinistra.
3. Nel campo Primo lettore di schede selezionare il lettore di schede come inizio del percorso. Nell'elenco, fare
4. clic sul testo archiviato di **Lettore di schede in seguito** e seleziona i lettori di carte collegati.

   Esempio: Se si seleziona Reader In_01 come inizio e si seleziona Reader In_02, Reader Out_04 come lettori di schede collegati. Quindi è possibile accedere al punto di controllo accessi solo facendo scorrere la carta nell'ordine come Reader In_01, Reader In_02 e Reader Out_04.



   Nota: È possibile aggiungere fino a quattro lettori di schede successivi per un lettore di schede.

5. (Facoltativo) È possibile accedere nuovamente alla finestra di dialogo Seleziona lettore di schede per modificarne i successivi lettori di schede.
6. Fare clic su **Salva** per salvare e rendere effettive le nuove impostazioni.

7.8.5 Password di autenticazione

Scopo:

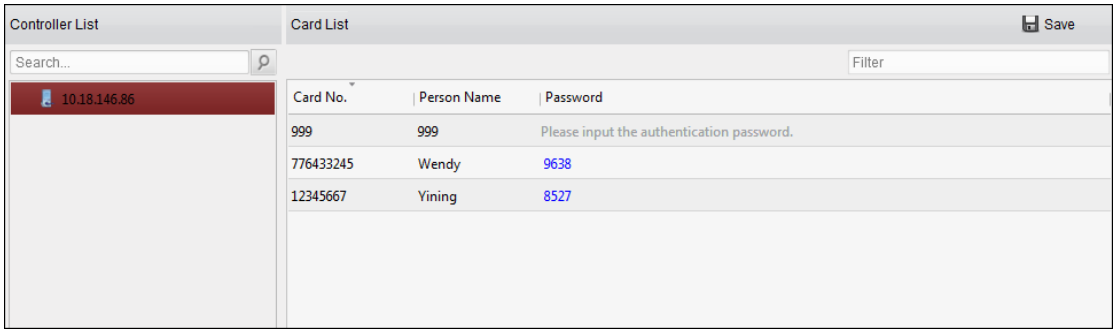
È possibile aprire la porta immettendo la password di autenticazione sulla tastiera del lettore di schede dopo aver terminato l'operazione di impostazione della password di autenticazione.

Appunti:

- Questa funzione di password di autenticazione è valida solo durante le pianificazioni quando il lettore di schede la modalità di autenticazione per il dispositivo di controllo accessi è impostata come **Carta o password di autenticazione.** Per i dettagli, fare riferimento a *Capitolo 7.8.2 Autenticazione del lettore di schede.*
- Questa funzione dovrebbe essere supportata dal dispositivo di controllo accessi.

Passaggi:

1. Fare clic su **Password di autenticazione** scheda e selezionare un dispositivo di controllo accessi dall'elenco.



Verranno visualizzate tutte le carte e le persone che sono state applicate al dispositivo.

Nota: Per impostare e applicare le autorizzazioni al dispositivo, fare riferimento a *Capitolo 7.7 Configurazione delle autorizzazioni.*

2. Clicca il **Parola d'ordine** campo della carta e inserire la password di autenticazione per la carta.

   Nota: La password di autenticazione deve contenere da 4 a 8 cifre.

3. Dopo aver impostato la password di autenticazione, la funzione della password di autenticazione della scheda sarà abilitato per impostazione predefinita.
4. (Facoltativo) È possibile inserire le parole chiave del numero della carta, del nome della persona o della password di autenticazione per la ricerca.

Appunti:

- È possibile aggiungere fino a 500 tessere con password di autenticazione a un dispositivo di controllo accessi.
- La password deve essere univoca e non può essere la stessa della super password, del codice di coercizione e del codice di eliminazione nei parametri di controllo dell'accesso.

7.8.6 CustomWiegand

Scopo:

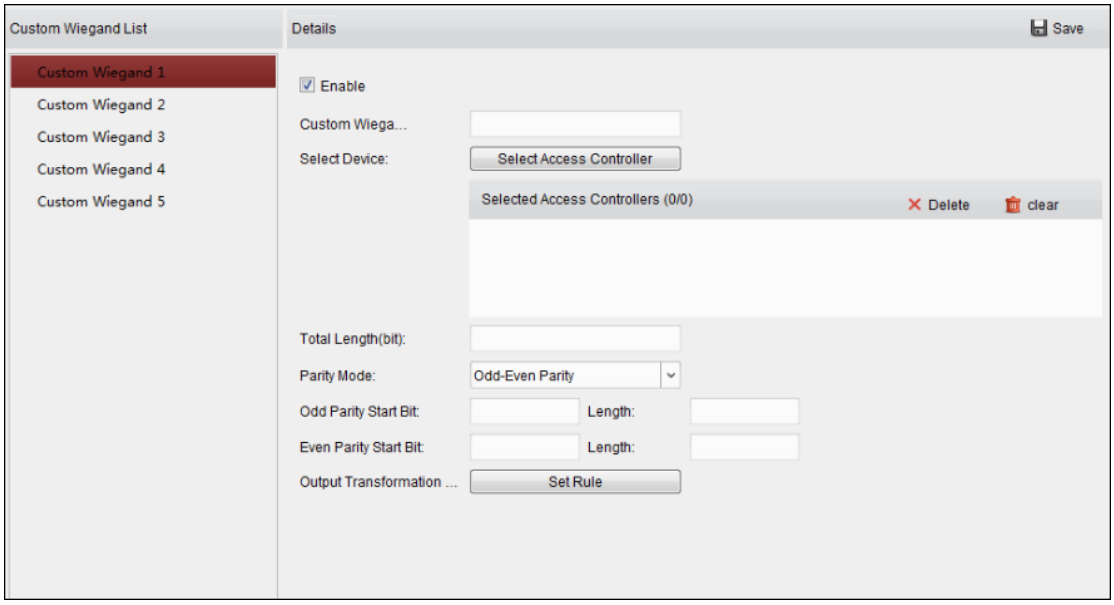
In base alla conoscenza della regola di caricamento per il wiegand di terze parti, è possibile impostare più protocolli wiegand personalizzati per comunicare tra il controller ei lettori di schede di terze parti.

Prima che inizi:

Collegare i lettori di schede di terze parti al controller.

Passaggi:

1. Fare clic su **CustomWiegand** per accedere alla scheda CustomWiegand.



2. Seleziona un customwiegand a sinistra dell'interfaccia. Dai un'occhiata **Abilitare**
3. casella di controllo per abilitare il customwiegand. Imposta il nome del
4. wiegand.
5. Seleziona dispositivo.

   1) Fare clic su **Seleziona dispositivo.**

   2) Selezionare il dispositivo necessario per utilizzare customwiegand.

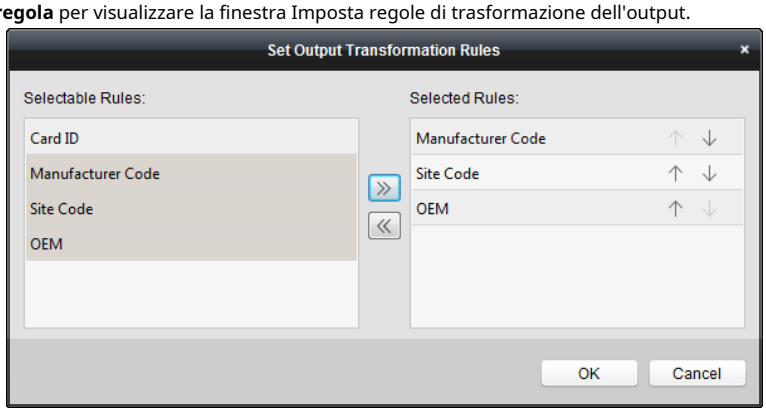
   3) Fare clic su **ok** per salvare le impostazioni.
6. Immettere la lunghezza totale e selezionare la modalità di parità nell'elenco a discesa.

   Se si seleziona Parità pari-dispari, è necessario impostare il bit di inizio parità dispari, la lunghezza parità dispari, il bit di inizio parità pari e la lunghezza parità pari.

   Se si seleziona Parità XOR, è necessario impostare il bit di inizio parità XOR, la lunghezza per gruppo e la lunghezza totale.

   Se si seleziona Nessuno, non è necessario impostare la modalità di parità.
7. Imposta la regola di trasformazione dell'output.

   1) Fare clic su **Imposta regola** per visualizzare la finestra Imposta regole di trasformazione dell'output.



   2) Seleziona le regole dall'elenco a sinistra.

   Nota: premi il *Cambio* tasto per selezionare più regole.

3) Clic  per spostare le regole selezionate nell'elenco di destra.
4) (Facoltativo) Fare clic su  o  per modificare l'ordine delle regole.
5) (Facoltativo) Selezionare le regole nell'elenco Regola selezionata e fare clic  per rimuovere la regola da sull'elenco a destra.
6) Clic **ok** per salvare le impostazioni.
7) Nella scheda CustomWiegand, impostare il bit di inizio della regola, la lunghezza e la cifra decimale.

8. Fare clic su **Salva** nell'angolo in alto a destra dell'interfaccia per salvare le impostazioni.

Appunti:

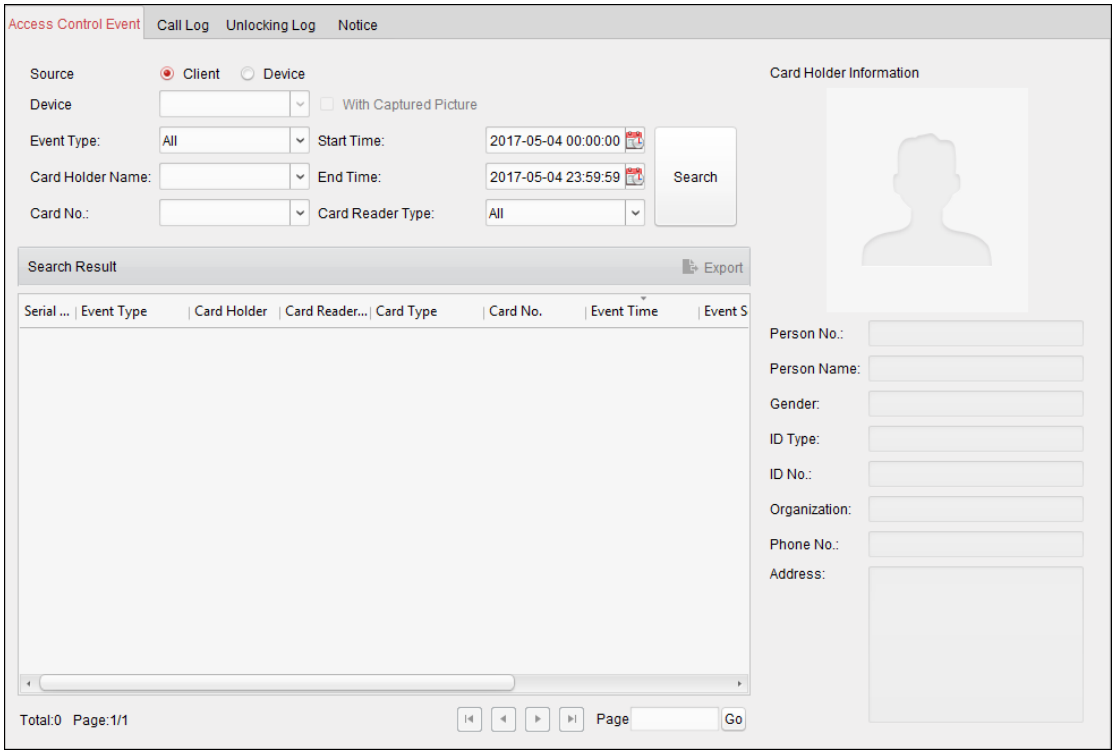
- Per impostazione predefinita, il dispositivo disabilita la funzione customwiegand.
- Se il dispositivo abilita la funzione wiegand personalizzato, tutte le interfacce wiegand nel dispositivo utilizzeranno il protocollo wiegand personalizzato.
- È possibile impostare fino a 5 wiegand personalizzati.
- Sono consentiti fino a 32 caratteri nel nome customwiegand. Sono
- disponibili fino a 80 bit nella lunghezza totale.
- Il bit di inizio parità dispari, la lunghezza di parità dispari, il bit di inizio parità pari e la lunghezza di parità pari sono compresi tra 1 e 80 bit.
- Il bit iniziale dell'ID della scheda, il codice del produttore, il codice del sito e l'OEM dovrebbero essere compresi tra 1 e 80 bit.
- Per i dettagli sul customwiegand, vedere l'Appendice.

7.9 Ricerca di eventi di controllo accessi

Scopo:

È possibile cercare gli eventi della cronologia del controllo di accesso, inclusi eventi di eccezione del dispositivo, eventi della porta, input di allarme e eventi del lettore di schede.

Clic  e fare clic sulla scheda Evento controllo accesso per accedere alla seguente interfaccia.



Passaggi:

1. Selezionare la sorgente.

   Puoi selezionare Client o Device.

2. Immettere la condizione di ricerca (origine, tipo di evento / nome del titolare della carta / numero della carta / acquisizione / ora di inizio e fine).
3. Clic **Ricerca** per ottenere i risultati della ricerca.
4. Visualizza le informazioni sull'evento nell'elenco degli eventi.
5. Fare clic su un evento per visualizzare le informazioni del titolare della carta sul **Informazioni sul titolare della carta** pannello sul lato sinistro della pagina.
6. Puoi fare clic **Esportare** pulsante per esportare i risultati della ricerca sul PC locale.

7.10 Configurazione degli eventi di controllo degli accessi

Scopo:

Per il dispositivo di controllo degli accessi aggiunto, è possibile configurare il collegamento del controllo degli accessi incluso il collegamento dell'evento di controllo dell'accesso, il collegamento dell'ingresso dell'allarme di controllo dell'accesso, il collegamento della scheda evento e il collegamento tra dispositivi.

Clicca il  icona sul pannello di controllo,
o fare clic su **Strumento-> Gestione eventi** per aprire la pagina Gestione eventi.

7.10.1 Collegamento eventi di controllo accessi

Scopo:

È possibile assegnare azioni di collegamento all'evento di controllo dell'accesso impostando una regola. Ad esempio, quando viene rilevato l'evento di controllo dell'accesso, viene visualizzato un avviso acustico o vengono eseguite altre azioni di collegamento.

Nota: Il collegamento qui si riferisce al collegamento delle azioni proprie del software client.

Passaggi:

1. Fare clic su **Evento di controllo degli accessi** tab.
2. I dispositivi di controllo accessi aggiunti verranno visualizzati nel pannello Dispositivo di controllo accessi a sinistra. Selezionare il dispositivo di controllo accessi, l'ingresso allarme, il punto di controllo accessi (porta) o il lettore di schede per configurare il collegamento degli eventi.
3. Seleziona il tipo di evento per impostare il collegamento.
4. Seleziona la telecamera attivata. L'immagine o il video della telecamera attivata apparirà quando si verifica l'evento selezionato.

   Per acquisire l'immagine della telecamera attivata quando si verifica l'evento selezionato, è anche possibile impostare la pianificazione dell'acquisizione e l'archiviazione in Pianificazione archiviazione.
5. Selezionare le caselle di controllo per attivare le azioni di collegamento. Per i dettagli, fare riferimento a *Tabella 14.1 Azioni di collegamento per l'evento di controllo dell'accesso.*
6. Clic **Salva** per salvare le impostazioni.
7. È possibile fare clic sul pulsante Copia in per copiare l'evento di controllo accessi su un altro dispositivo di controllo accessi, ingresso allarme, punto di controllo accessi o lettore di schede.

   Selezionare i parametri per la copia, selezionare la destinazione in cui copiare e fare clic **ok** per confermare.

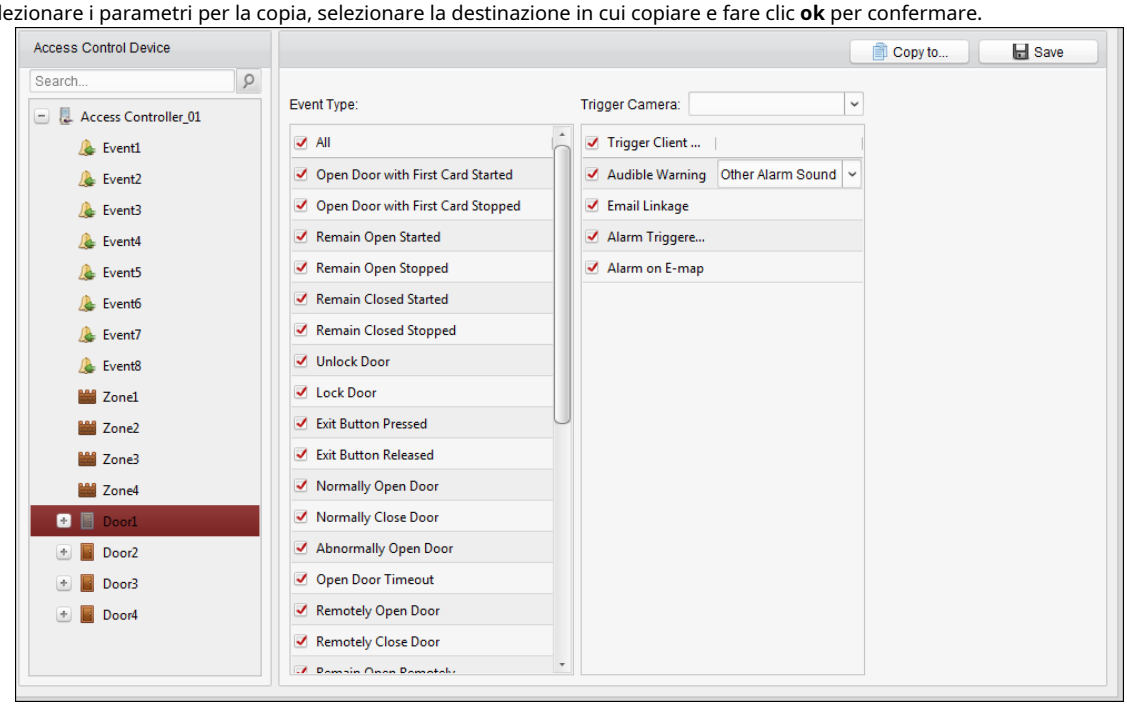


Tabella 1. 1 Azioni di collegamento per l'evento di controllo dell'accesso

Azioni di collegamento	Descrizioni
Avviso acustico	Il software client emette un avviso acustico quando viene attivato l'allarme. È possibile selezionare il suono dell'allarme per un avviso
Collegamento e-mail	acustico. Invia una notifica e-mail delle informazioni sull'allarme a uno o più destinatari.
Allarme su mappa elettronica	Visualizza le informazioni sugli allarmi sulla mappa elettronica. ***Nota:*** Questo collegamento è disponibile solo per accedere al punto di controllo e ingresso allarme.

Allarme attivato Immagine pop-up	L'immagine con le informazioni sull'allarme si apre quando l'allarme è innescato.

7.10.2 Collegamento ingresso allarme controllo accessi

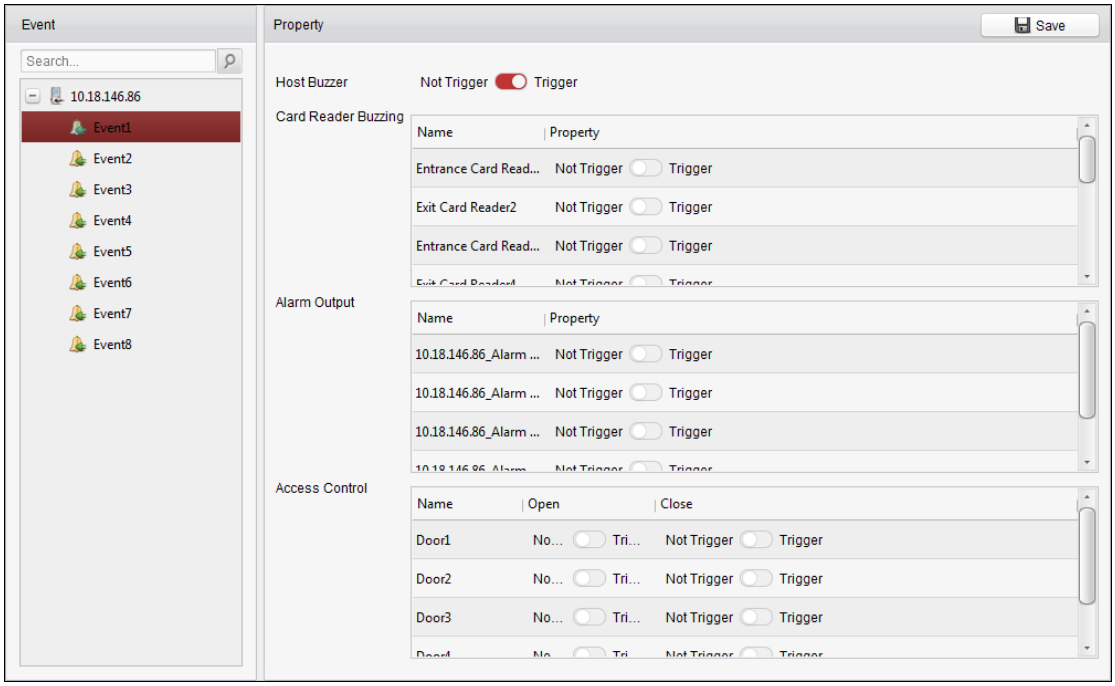
Scopo:

Gli ingressi allarme di controllo accessi possono essere collegati ad alcune azioni (es. Uscita allarme, cicalino host) quando viene attivato.

Nota: Il collegamento qui si riferisce al collegamento delle azioni proprie del software client.

Passaggi:

1. Fare clic su **Ingresso allarme controllo accessi** scheda per accedere alla seguente interfaccia.



2. Nell'elenco degli eventi a sinistra, selezionare un ingresso di
3. allarme. Cambia la proprietà da per per abilitare questa azione.

   Buzzer host: Verrà attivato l'allarme acustico del controller.

   Cicalino del lettore di schede: Verrà attivato l'allarme acustico del lettore di schede.

   Uscita allarme: L'uscita allarme verrà attivata per la notifica.

   Punto di controllo accessi (Apri / Chiudi): La porta sarà aperta o chiusa quando la custodia viene attivata.

   Nota: La Porta non può essere configurata come aperta o chiusa contemporaneamente.
4. Clic **Salva** pulsante per salvare le impostazioni.

7.10.3 Collegamento delle carte evento

Clic **Collegamento delle carte evento** scheda per accedere alla seguente interfaccia.

Appunti:

- L'Event Card Linkage dovrebbe essere supportato dal dispositivo.

- Il collegamento qui si riferisce al collegamento delle azioni proprie del software client.

Seleziona il dispositivo di controllo accessi dall'elenco a sinistra.

Clic **Inserisci** pulsante per aggiungere un nuovo collegamento. È possibile selezionare l'origine dell'evento come **Collegamento evento** o **Collegamento della carta.**

Collegamento eventi

Per il collegamento degli eventi, l'evento di allarme può essere suddiviso in quattro tipi: evento del dispositivo, ingresso di allarme, evento della porta e evento del lettore di schede.

Passaggi:

1. Fare clic per selezionare il tipo di collegamento come **Collegamento evento,** e seleziona il tipo di evento dal menu a discesa elenco.
   - Per Evento dispositivo, seleziona il tipo di evento dettagliato dall'elenco a discesa.
   - Per Ingresso allarme, selezionare il tipo come allarme o ripristino allarme e selezionare il nome dell'ingresso allarme dalla tabella.
   - Per Evento porta, seleziona il tipo di evento dettagliato e seleziona la porta di origine dalla tabella. Per Evento
   - lettore di schede, selezionare il tipo di evento dettagliato e selezionare il lettore di schede dalla tabella.

2. Impostare la destinazione del collegamento e cambiare la proprietà da per  per abilitare questa funzione.
   - **Buzzer host:** L'avviso acustico del controller verrà abilitato / disabilitato.
   - **Catturare:** L'acquisizione in tempo reale verrà abilitata.
   - **Cicalino del lettore di schede:** L'avviso acustico del lettore di schede verrà abilitato / disabilitato.
   - **Uscita allarme:** L'uscita allarme verrà abilitata / disabilitata per la notifica.
   - **Punto di controllo accessi:** Verrà abilitato lo stato della porta aperta, chiusa, rimasta aperta e rimasta chiusa.

     Appunti:

     - Lo stato della porta di aperto, chiuso, resta aperto e resta chiuso non può essere attivato contemporaneamente.
     - La porta di destinazione e la porta di origine non possono essere la stessa.
3. Fare clic su **Salva** pulsante per salvare e rendere effettivi i parametri.

Collegamento della carta

Passaggi:

1. Fare clic per selezionare il tipo di collegamento come **Collegamento della carta.**
2. Immettere il numero della scheda o selezionare la scheda dall'elenco a discesa.
3. Selezionare il lettore di schede dalla tabella per l'attivazione.
4. Impostare la destinazione del collegamento e cambiare la proprietà da per  per abilitare questa funzione.
   - **Buzzer host:** L'avviso acustico del controller verrà abilitato / disabilitato.
   - **Catturare:** L'acquisizione in tempo reale verrà abilitata.
   - **Cicalino del lettore di schede:** L'avviso acustico del lettore di schede verrà abilitato / disabilitato.
   - **Uscita allarme:** L'uscita allarme verrà abilitata / disabilitata per la notifica.
   - **Punto di controllo accessi:** Verrà abilitato lo stato della porta aperta, chiusa, rimasta aperta e rimasta chiusa.

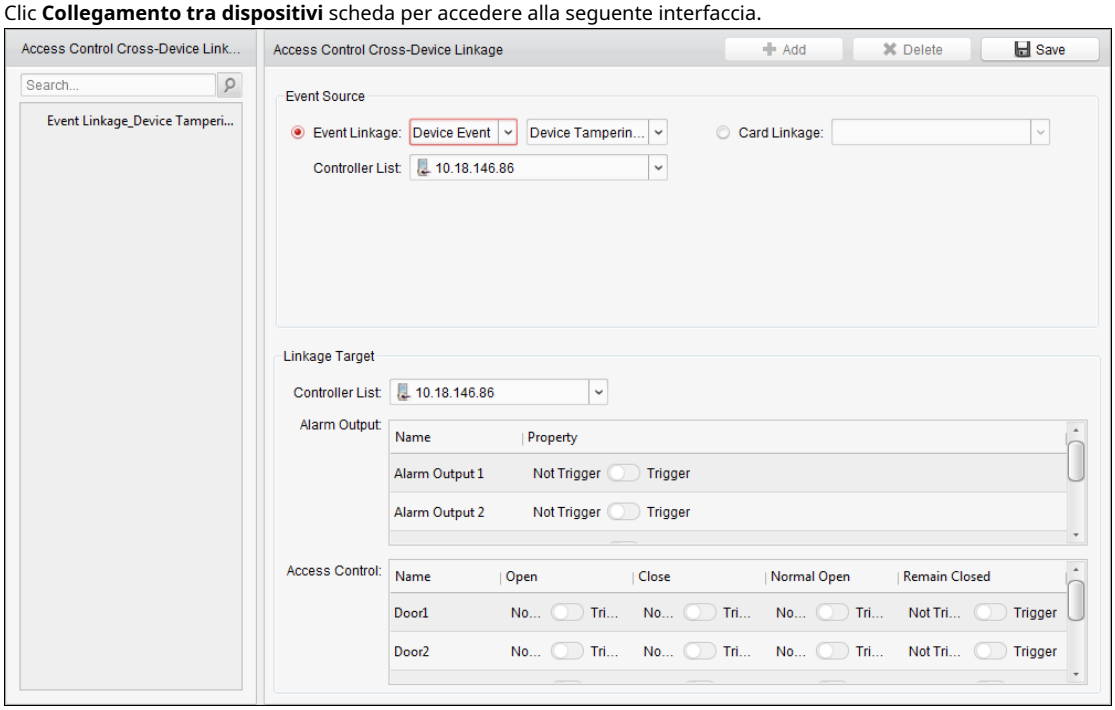
5. Fare clic su **Salva** pulsante per salvare e rendere effettivi i parametri.

7.10.4 Collegamento tra dispositivi

Scopo:

È possibile assegnare l'attivazione dell'azione di un altro dispositivo di controllo dell'accesso impostando una regola quando viene attivato l'evento di controllo dell'accesso.

Clic **Collegamento tra dispositivi** scheda per accedere alla seguente interfaccia.



Clic **Inserisci** pulsante per aggiungere un nuovo collegamento client. È possibile selezionare l'origine dell'evento come **Collegamento evento** o **Collegamento della carta.**

Collegamento eventi

Per il collegamento degli eventi, l'evento di allarme può essere suddiviso in quattro tipi: evento del dispositivo, ingresso di allarme, evento della porta e evento del lettore di schede.

Passaggi:

1. Fare clic per selezionare il tipo di collegamento come **Collegamento evento,** selezionare il dispositivo di controllo accessi come evento sorgente e selezionare il tipo di evento dall'elenco a discesa.
   - Per Evento dispositivo, seleziona il tipo di evento dettagliato dall'elenco a discesa.
   - Per Ingresso allarme, selezionare il tipo come allarme o ripristino allarme e selezionare il nome dell'ingresso allarme dalla tabella.
   - Per Evento porta, seleziona il tipo di evento dettagliato e seleziona la porta dalla tabella.
   - Per Evento lettore di schede, selezionare il tipo di evento dettagliato e selezionare il lettore di schede dalla tabella.
2. Impostare la destinazione del collegamento, selezionare il dispositivo di controllo dell'accesso dall'elenco a discesa come destinazione del collegamento e cambiare la proprietà da  per  per abilitare questa funzione.

- **Uscita allarme:** L'uscita allarme verrà attivata per la notifica.
- **Punto di controllo accessi:** Verrà attivato lo stato della porta aperta, chiusa, rimani aperta e rimasta chiusa. ***Nota:*** Lo stato della porta di aperto, chiuso, resta aperto e resta chiuso non può essere attivato contemporaneamente.

3. Fare clic su **Salva** pulsante per salvare i parametri.

Collegamento della carta

Passaggi:

1. Fare clic per selezionare il tipo di collegamento come **Collegamento della carta.**
2. Selezionare la scheda dall'elenco a discesa e selezionare il dispositivo di controllo dell'accesso come origine dell'evento.
3. Selezionare il lettore di schede dalla tabella per l'attivazione.
4. Impostare la destinazione del collegamento, selezionare il dispositivo di controllo dell'accesso dall'elenco a discesa come destinazione del collegamento e cambiare la proprietà da per  per abilitare questa funzione.
5. **Uscita allarme:** L'uscita allarme verrà attivata per la notifica. Clic **Salva** pulsante per salvare i parametri.

7.11 Gestione dello stato della porta

Scopo:

Lo stato della porta del dispositivo di controllo accessi aggiunto verrà visualizzato in tempo reale. È possibile controllare lo stato della porta e gli eventi collegati della porta selezionata. È possibile controllare lo stato della porta e impostare anche la durata dello stato delle porte.

7.11.1 Gestione del gruppo di controllo degli accessi

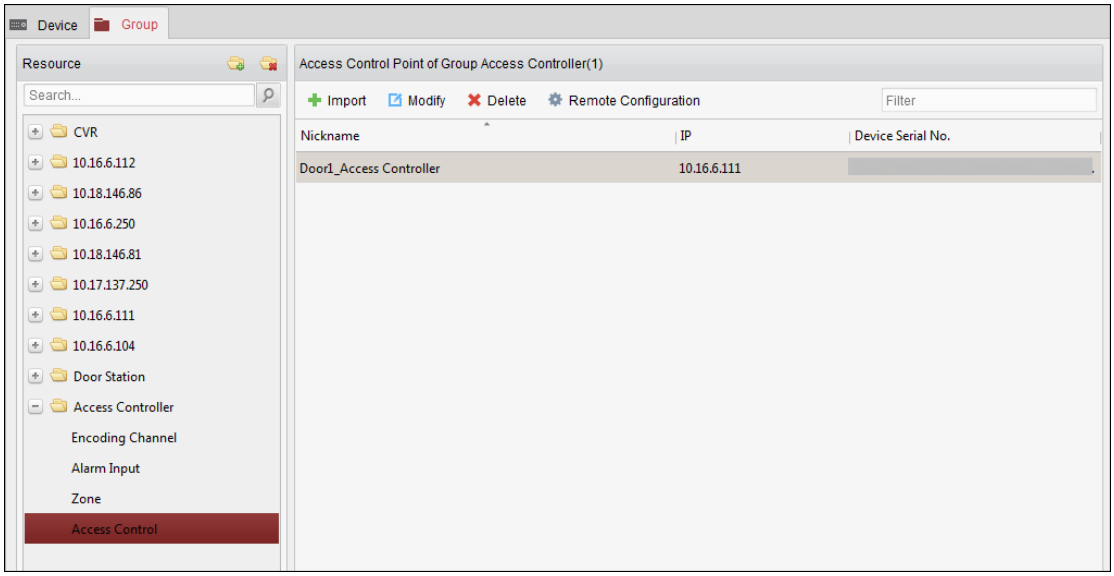
Scopo:

Prima di controllare lo stato della porta e impostare la durata dello stato, è necessario organizzarlo in gruppo per una comoda gestione.

Eseguire le seguenti operazioni per creare il gruppo per il dispositivo di controllo accessi:

Passaggi:

1. Fare clic su  sul pannello di controllo per aprire la pagina Gestione dispositivi.
2. Fare clic su **Gruppo** scheda per accedere all'interfaccia di gestione del gruppo.



3. Eseguire le seguenti operazioni per aggiungere il gruppo.

1) Fare clic su per aprire la finestra di dialogo Aggiungi gruppo.

2) Immettere un nome di gruppo come si desidera.

3) Fare clic su **ok** per aggiungere il nuovo gruppo all'elenco dei gruppi.

Puoi anche selezionare la casella di controllo **Crea gruppo per nome dispositivo** per creare il nuovo gruppo in base al nome del dispositivo selezionato.

4. Eseguire le seguenti operazioni per importare i punti di controllo dell'accesso nel gruppo:

1) Fare clic su **Importare** nell'interfaccia di gestione del gruppo, quindi fare clic su **Controllo di accesso** scheda a

apri la pagina Import Access Control.

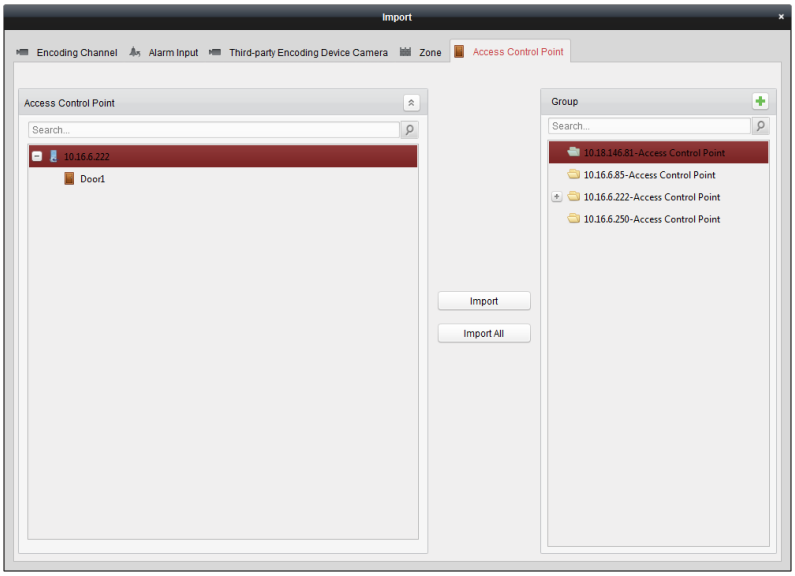
Appunti:

- Puoi anche selezionare **Ingresso allarme** scheda e importare gli ingressi di allarme nel gruppo.
- Per il terminale di controllo dell'accesso video, è possibile aggiungere le telecamere come canale di codifica al gruppo.

2) Selezionare i nomi dei punti di controllo dell'accesso nell'elenco.

3) Seleziona un gruppo dall'elenco dei gruppi.

4) Clic **Importare** per importare i punti di controllo dell'accesso selezionati nel gruppo. Puoi anche fare clic su **Importa tutto** per importare tutti i punti di controllo dell'accesso in un gruppo selezionato.



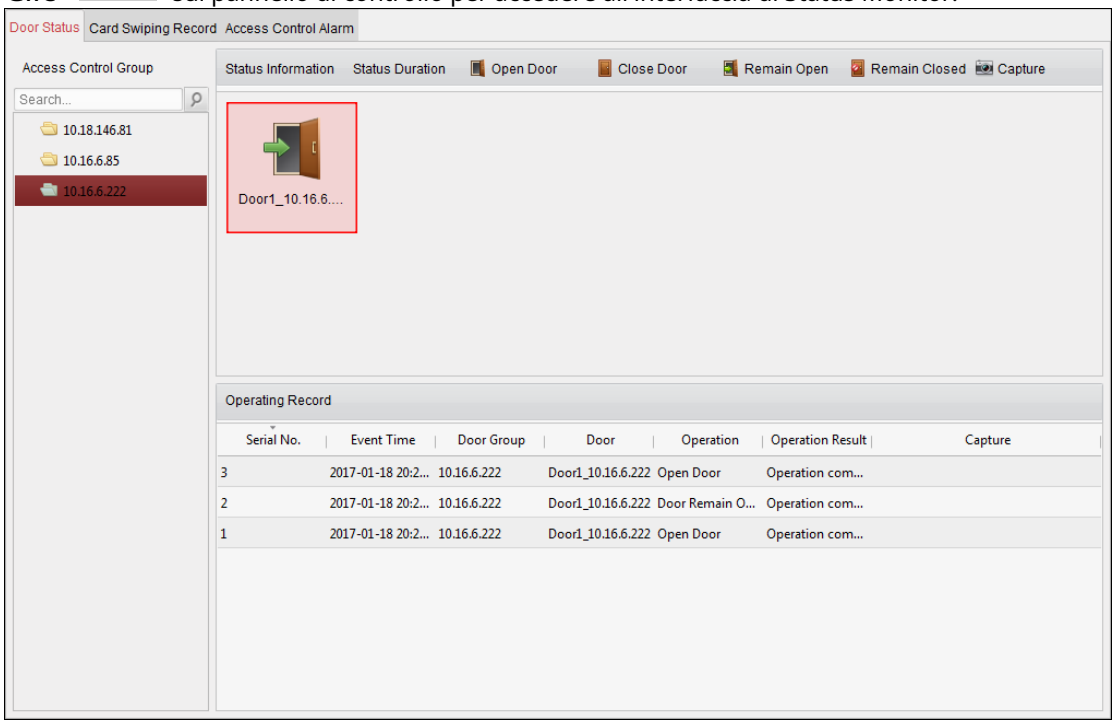
5. Dopo aver importato i punti di controllo dell'accesso nel gruppo, è possibile fare clic sul nome o fare doppio clic sul file del gruppo / punto di controllo dell'accesso per modificarlo.

7.11.2 Anti-controllo del punto di controllo accessi (porta)

Scopo:

È possibile controllare lo stato di un singolo punto di controllo dell'accesso (una porta), inclusa l'apertura della porta, la chiusura della porta, il rimanere aperto e il rimanere chiuso.

Clic sul pannello di controllo per accedere all'interfaccia di Status Monitor.

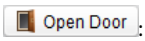


Passaggi:

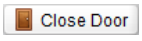
1. Selezionare un gruppo di controllo accessi a sinistra. Per la gestione del gruppo di controllo accessi, fare riferimento a *Capitolo 7.11.1 Gestione gruppo controllo accessi.*
2. I punti di controllo degli accessi del gruppo di controllo degli accessi selezionato verranno visualizzati sulla destra.

Fare clic sull'icona  sul pannello Informazioni di stato per selezionare una porta.

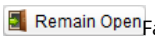
3. Fare clic sul pulsante seguente elencato in **Informazioni sullo stato** pannello per il controllo della porta.



: Fare clic per aprire la porta una volta. :



Fare clic per chiudere la porta una volta. :



Fare clic per tenere la porta aperta.

: Fare clic per tenere la porta chiusa.

: Fare clic per acquisire l'immagine manualmente.

4. È possibile visualizzare il risultato dell'operazione anti-controllo nel pannello Registro operazioni.

Appunti:

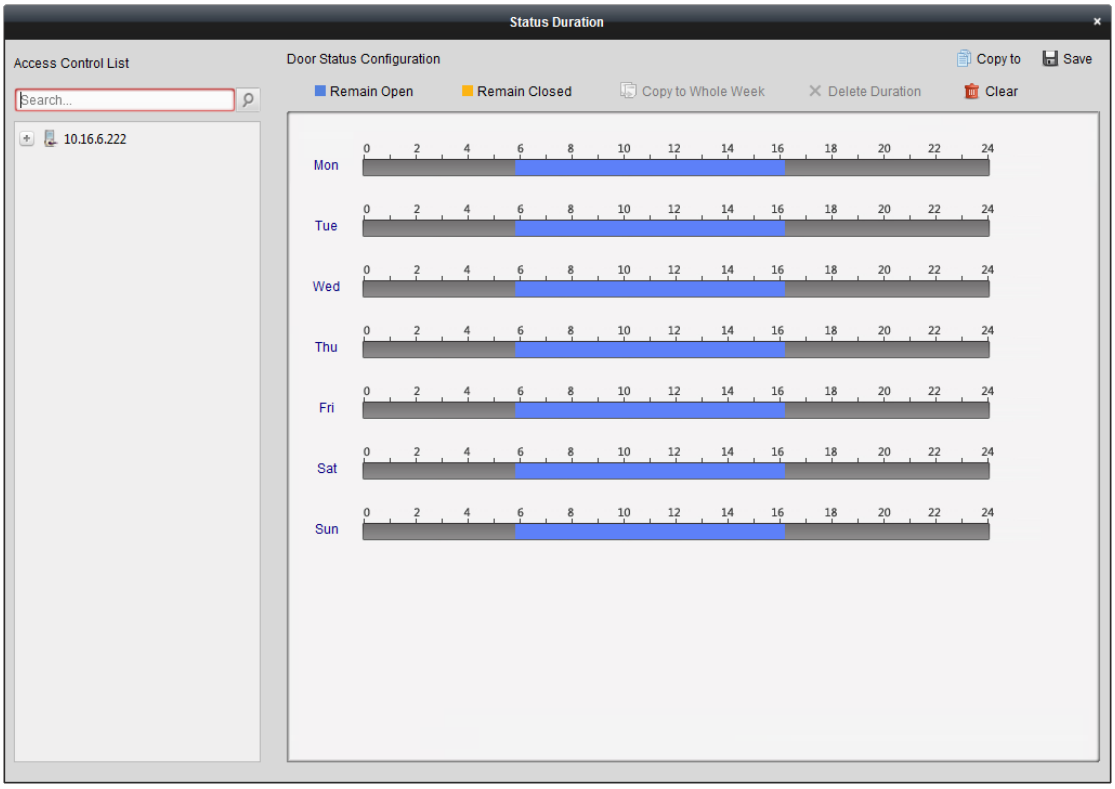
- Se selezioni lo stato come **Rimani aperto / Rimani chiuso,** la porta rimarrà aperta / chiusa fino a quando non verrà effettuato un nuovo comando anticontrollo.
- Il **Catturare** è disponibile quando il dispositivo supporta la funzione di acquisizione. E non può essere realizzato fino a quando il server di archiviazione non è configurato.
- Se la porta è nello stato di rimanere chiuso, solo la super card può aprire la porta o aprire la porta tramite il software client.

7.11.3 Configurazione della durata dello stato

Scopo:

È possibile programmare periodi di tempo settimanali in cui un punto di controllo accessi (porta) rimanga aperto o rimanga chiuso.

Nel modulo Stato porta, fare clic su **Durata dello stato** per accedere all'interfaccia della durata dello stato.



Passaggi:

1. Fare clic per selezionare una porta dall'elenco dei dispositivi di controllo accessi a sinistra.
2. Nel pannello Configurazione stato porta a destra, disegnare una pianificazione per la porta selezionata.
   1) Selezionare un pennello di stato della porta come Remain Open o Remain Closed.

      Rimani aperto: La porta rimarrà aperta durante il periodo di tempo configurato. Il pennello è contrassegnato come .

      Rimani chiuso: La porta rimarrà chiusa per tutta la durata configurata. Il pennello è contrassegnato come

   2) Fare clic e trascinare sulla timeline per disegnare una barra colorata sulla pianificazione per impostare la durata.

   3) Quando il cursore si trasforma in , puoi spostare la barra temporale selezionata che hai appena modificato. Puoi modificare anche il punto temporale visualizzato per impostare il periodo di tempo preciso.

      Quando il cursore si trasforma in , puoi allungare o accorciare la barra temporale selezionata.

3. Facoltativamente, è possibile selezionare la barra dell'orario di pianificazione e fare clic su **Copia in tutta la settimana** per copiare il file

impostazioni della barra temporale per gli altri giorni della settimana.

4. È possibile selezionare la barra temporale e fare clic su **Elimina durata** per eliminare il periodo di tempo.

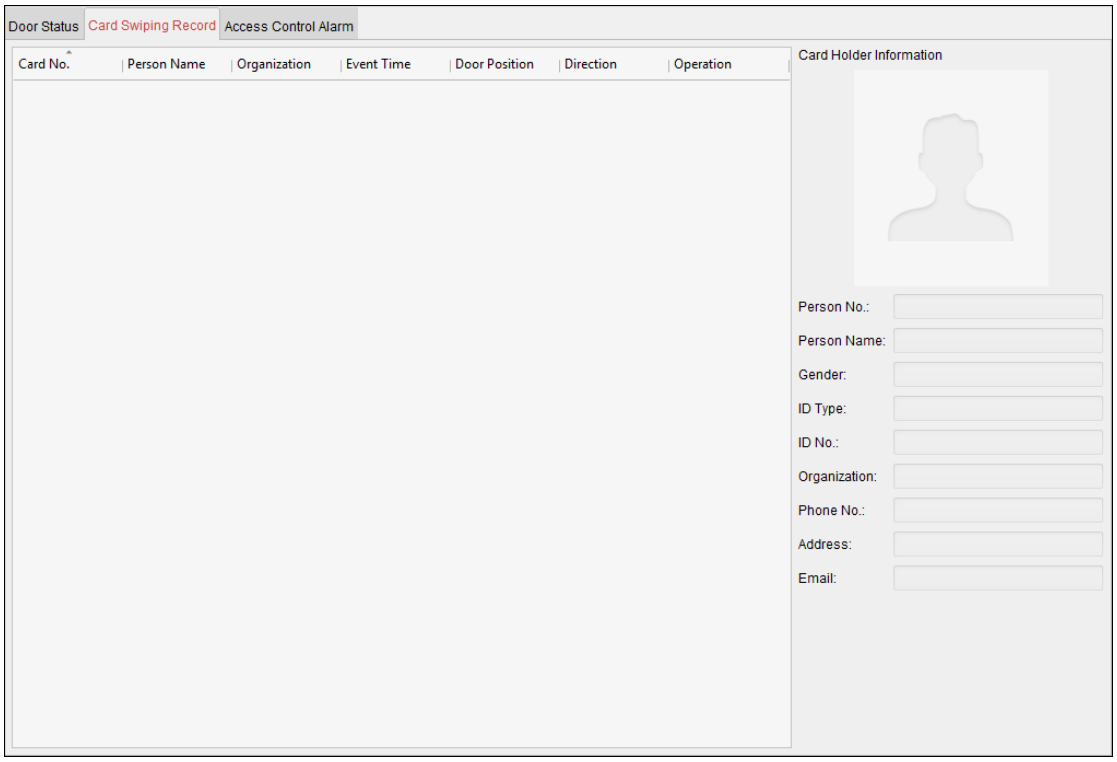
   Oppure puoi fare clic **Chiaro** per cancellare tutte le durate configurate nella pianificazione.

5. Fare clic su **Salva** per salvare le impostazioni.

6. È possibile fare clic su **Copia a** pulsante per copiare la pianificazione su altre porte.

7.11.4 Record di scorrimento della scheda in tempo reale

Clic **Record di scorrimento della scheda** scheda per accedere alla seguente interfaccia.



I registri delle registrazioni di scorrimento delle carte di tutti i dispositivi di controllo degli accessi verranno visualizzati in tempo reale. È possibile visualizzare i dettagli dell'evento di scorrimento della carta, inclusi il numero della carta, il nome della persona, l'organizzazione, l'ora dell'evento, ecc.

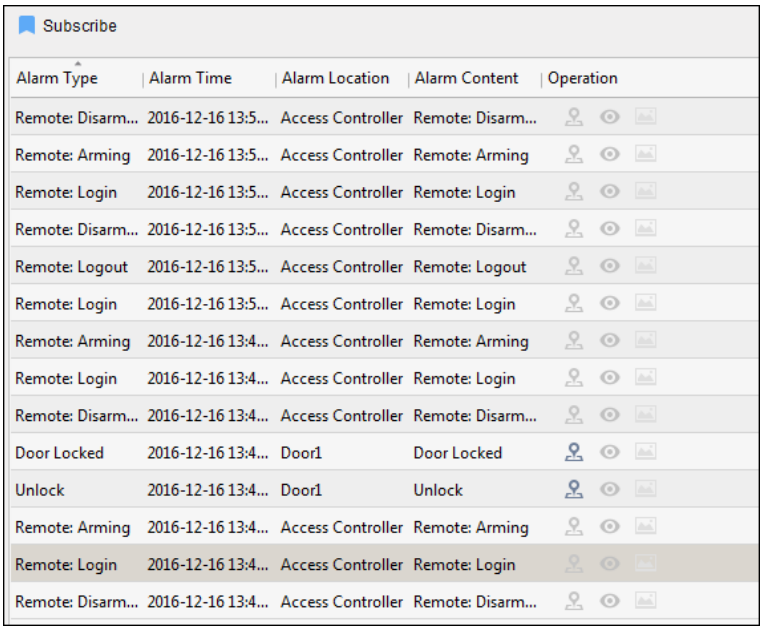
Puoi anche fare clic sull'evento per visualizzare i dettagli del titolare della carta, inclusi il numero della persona, il nome della persona, l'organizzazione, il telefono, l'indirizzo di contatto, ecc.

7.11.5 Allarme di controllo accessi in tempo reale

Scopo:

I registri degli eventi di controllo degli accessi verranno visualizzati in tempo reale, inclusi l'eccezione del dispositivo, l'evento della porta, l'evento del lettore di schede e l'ingresso di allarme.

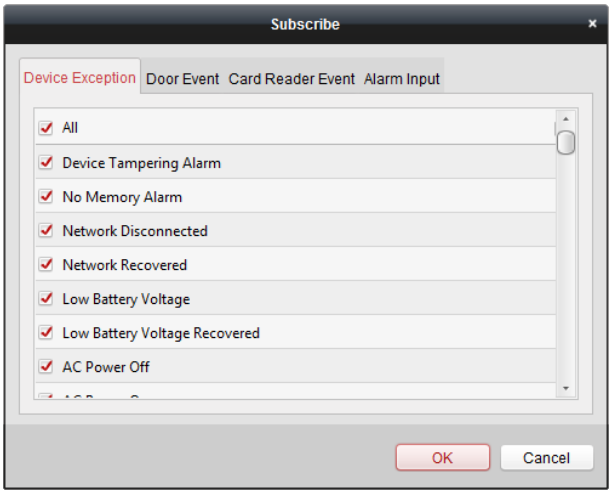
Clic **Allarme controllo accessi** scheda per accedere alla seguente interfaccia.



Passaggi:

1. Tutti gli allarmi di controllo accessi verranno visualizzati nell'elenco in tempo reale. È possibile visualizzare il tipo di allarme, l'ora, la posizione e così via. Fare clic su
2. per visualizzare l'allarme sulla mappa elettronica. Puoi fare clic o per visualizzare la visualizzazione live o l'immagine acquisita della telecamera attivata quando l'allarme è innescato.

   Nota: Per impostare la telecamera attivata, fare riferimento a *Capitolo 7.10.1 Collegamento eventi di controllo accessi.*
3. Clic **sottoscrivi** per selezionare l'allarme che il client può ricevere quando l'allarme viene attivato.



1) Selezionare le caselle di controllo per selezionare gli allarmi, inclusi allarme di eccezione del dispositivo, allarme di evento porta, allarme del lettore di schede e ingresso di allarme.

2) Fare clic su **ok** per salvare le impostazioni.

7.12 Controllo inserimento

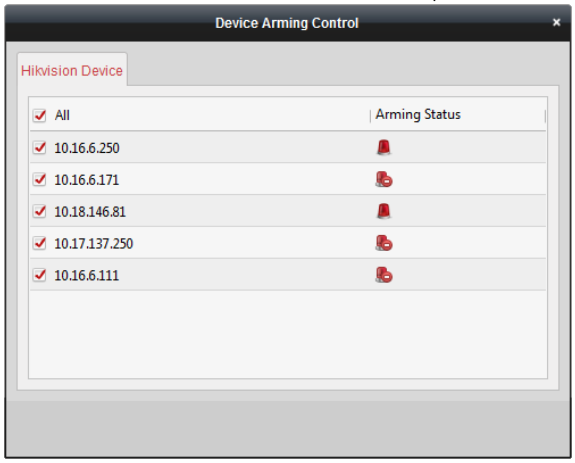
Scopo:

È possibile attivare o disattivare il dispositivo. Dopo aver inserito il dispositivo, il client può ricevere le informazioni di allarme dal dispositivo.

Passaggi:

1. Fare clic su **Strumento-> Controllo inserimento dispositivo** per visualizzare la finestra Controllo inserimento dispositivo.
2. Armare il dispositivo selezionando la casella di controllo corrispondente.

   Quindi le informazioni sull'allarme verranno caricate automaticamente nel software client quando si verifica l'allarme.



Appendice A Avviso sonoro e indicatore

Dopo che il lettore di schede è acceso, l'indicatore di stato LED diventerà blu e lampeggerà per 1 volta. Quindi diventerà rosso e lampeggerà per 3 volte. Alla fine il buzzer emetterà un segnale acustico che indica che il processo di avvio è completato.

Durante l'utilizzo del lettore di schede, invierà diversi suoni e l'indicatore LED su di esso avrà stati diversi. È possibile fare riferimento alle tabelle seguenti per informazioni dettagliate.

Tabella 7-1 Descrizione del suono di richiesta

Prompt audio	Descrizione
Un segnale acustico	Protocollo RS-485: premendo i tasti prompt; Richiesta di carta strisciata; Richiesta di timeout per premere i tasti o scorrere la scheda. Protocollo Wiegand: premendo i tasti prompt; Richiesta di carta magnetica.
Due bip rapidi	L'operazione di pressione dei tasti o strisciata della carta è valida.
Tre segnali acustici lenti	L'operazione di premere i tasti o strisciare la carta non è valida.
Rapidamente continuo bip	Allarme a prova di manomissione.
Lentamente continuo bip	Il lettore di schede non è crittografato.

Tabella 7-2 Descrizione dell'indicatore LED

Stato dell'indicatore LED	Descrizione
Verde e lampeggiante	Il lettore di schede funziona normalmente.
Verde fisso	L'operazione di pressione dei tasti o strisciata della carta è valida.
Rosso fisso	L'operazione di premere i tasti o strisciare la carta non è valida. Per il
Rosso e lampeggiante	protocollo RS-485: registrazione non riuscita o il lettore di schede non è in linea. Impossibile ottenere i file chiave della scheda PSAM; Impossibile rilevare la scheda PSAM.
Rosso e lampeggia rapidamente	Mantenere disponibile per la lettura della modalità file della scheda CPU: PSAM non lo è inserito o non rilevato.

Appendice B Regola CustomWiegand

Prendi Wiegand 44 come esempio, i valori di impostazione nella scheda CustomWiegand sono i seguenti:

Nome CustomWiegand:	Wiegand 44					
Lunghezza totale	44					
Trasformazione Regola (Decimale Cifra)	byFormatRule [4] = [1] [4] [0] [0]					
Modalità parità	Parità XOR					
Bit di inizio parità dispari		Lunghezza				
Bit di inizio parità pari		Lunghezza				
XOR Bit di inizio parità	0	Lunghezza per Gruppo 4		Lunghezza totale 40		
ID scheda Bit iniziale	0	Lunghezza	32	Cifra decimale	10	
Codice sito Bit iniziale		Lunghezza		Cifra decimale		
Bit iniziale OEM		Lunghezza		Cifra decimale		
Bit di inizio codice produttore	32	Lunghezza	8	Cifra decimale	3	

Dati Wiegand = Dati validi + Dati di parità

Lunghezza totale: Lunghezza dati Wiegand.

Regola di trasporto: 4 byte. Visualizza i tipi di combinazione di dati validi. L'esempio mostra la combinazione di ID tessera e codice produttore. I dati validi possono essere una singola regola o una combinazione di più regole.

Modalità parità: Parità valida per i dati wiegand. È possibile selezionare parità dispari o parità pari.

Bit di inizio parità dispari e lunghezza: Se selezioni Parità dispari, questi elementi sono disponibili. Se il bit di inizio parità dispari è 1 e la lunghezza è 12, il sistema inizierà il calcolo della parità dispari dal bit 1. Calcolerà 12 bit. Il risultato sarà nel bit 0. (Il bit 0 è il primo bit.)

Bit di inizio parità pari e lunghezza: Se selezioni Parità pari, questi elementi sono disponibili. Se il bit di inizio della parità pari è 12 e la lunghezza è 12, quindi il sistema inizierà il calcolo della parità pari dal bit 12. Calcolerà 12 bit. Il risultato sarà nell'ultimo bit.

Bit di inizio parità XOR, lunghezza per gruppo e lunghezza totale: Se si seleziona XOR Parity, questi elementi sono disponibili. A seconda della tabella visualizzata sopra, il bit di inizio è 0, la lunghezza per gruppo è 4 e la lunghezza totale è 40. Significa che il sistema calcolerà dal bit 0, calcolerà ogni 4 bit e calcolerà 40 bit in totale (10 gruppi in totale). Il risultato sarà negli ultimi 4 bit. (La lunghezza del risultato è la stessa della lunghezza per gruppo.)

Bit di inizio ID carta, lunghezza e cifra decimale: Se utilizzi la regola di trasformazione, questi elementi sono disponibili. A seconda della tabella visualizzata sopra, il bit di inizio dell'ID della scheda è 0, la lunghezza è 32 e la cifra decimale è 10. Rappresenta che dal bit 0 ci sono 32 bit che rappresentano l'ID della scheda. (La lunghezza qui è calcolata in bit.) E la lunghezza della cifra decimale è di 10 bit.

Bit di inizio del codice del sito, lunghezza e cifra decimale: Se utilizzi la regola di trasformazione, questi elementi sono disponibili. Per informazioni dettagliate, vedere la spiegazione dell'ID della carta.

Bit iniziale, lunghezza e cifra decimale OEM: Se utilizzi la regola di trasformazione, questi elementi sono disponibili. Per informazioni dettagliate, vedere la spiegazione dell'ID della carta.

Bit di inizio del codice del produttore, lunghezza e cifra decimale: Se utilizzi la regola di trasformazione, questi elementi sono disponibili. A seconda della tabella visualizzata sopra, il bit di inizio del codice del produttore è 32, la lunghezza è 8 e la cifra decimale è 3. Rappresenta che dal bit 32, ci sono 8 bit sono il codice del produttore. (La lunghezza qui è calcolata in bit.) E la lunghezza decimale è 3.

020000001080620


See Far, Go Further