Controller di accesso serie DS-K2600

Manuale d'uso

Manuale d'uso

Questo manuale si applica al controller di accesso.

nome del prodotto	Seriali
Accesso Controllore	Controller di accesso seriale DS-K2601
	Controller di accesso seriale DS-K2602
	Controller di accesso seriale DS-K2604

Include istruzioni su come utilizzare il Prodotto. Il software incorporato nel Prodotto è regolato dal contratto di licenza con l'utente che copre quel 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, in tutto o in parte, con qualsiasi mezzo, senza previa autorizzazione scritta di Hikvision.

Marchi Trade

HIKVISION e altri marchi Hikvision sono di proprietà di Hikvision e sono registrati marchi o oggetto di applicazioni degli stessi da parte di Hikvision e/o delle sue affiliate. Gli altri marchi citati in questo manuale sono di proprietà dei rispettivi proprietari. Non viene concesso alcun diritto di licenza per l'utilizzo di tali marchi senza espressa autorizzazione.

Dichiarazione di non responsabilità

NELLA MISURA MASSIMA CONSENTITA DALLA LEGGE APPLICABILE, HIKVISION NON FORNISCE ALCUNA GARANZIA, ESPRESSA O IMPLICITA, INCLUSE SENZA LIMITAZIONI LE GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO PARTICOLARE, IN RELAZIONE AL PRESENTE MANUALE. HIKVISION NON GARANTISCE NÉ RILASCIA ALCUNA DICHIARAZIONE IN MERITO ALL'UTILIZZO DEL MANUALE O ALLA CORRETTEZZA, ACCURATEZZA O AFFIDABILITÀ DELLE INFORMAZIONI QUI CONTENUTE. L'UTILIZZO DI QUESTO MANUALE E QUALSIASI AFFIDAMENTO SU QUESTO MANUALE SARÀ INTERAMENTE A PROPRIO RISCHIO E RESPONSABILITÀ.

PER QUANTO RIGUARDA IL PRODOTTO CON ACCESSO A INTERNET, L'UTILIZZO DEL PRODOTTO SARÀ INTERAMENTE A PROPRIO RISCHIO. LA NOSTRA AZIENDA NON SI ASSUME ALCUNA RESPONSABILITÀ PER FUNZIONAMENTO ANORMALE, FUGHE DI PRIVACY O ALTRI DANNI DERIVANTI DA ATTACCHI INFORMATICI, ATTACCHI DI HACKER, ISPEZIONE DI VIRUS O ALTRI RISCHI PER LA SICUREZZA DI INTERNET; TUTTAVIA, LA NOSTRA AZIENDA FORNIRÀ TEMPESTIVA SUPPORTO TECNICO SE NECESSARIO.

LE LEGGI DI SORVEGLIANZA VARIANO A SECONDA DELLA GIURISDIZIONE. SI PREGA DI VERIFICARE TUTTE LE LEGGI RILEVANTI NELLA TUA GIURISDIZIONE PRIMA DI UTILIZZARE QUESTO PRODOTTO PER GARANTIRE CHE IL TUO UTILIZZO CONFORME ALLA LEGGE APPLICABILE. LA NOSTRA AZIENDA NON SARÀ RESPONSABILE NEL CASO IN CUI QUESTO PRODOTTO SIA UTILIZZATO CON SCOPI ILLECITI.

IN CASO DI EVENTUALI CONFLITTI TRA IL PRESENTE MANUALE E LA LEGGE APPLICABILE, PREVALGA QUESTA ULTIMA.

Supporto

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

Informazioni normative

Informazioni FCC

Si prega di prestare attenzione al fatto che cambiamenti o modifiche non espressamente approvati dalla parte responsabile della conformità potrebbero annullare l'autorità dell'utente 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 in radiofrequenza e, se non installata e utilizzata secondo le istruzioni, può causare interferenze dannose alle comunicazioni radio. Tuttavia, non vi è alcuna garanzia che non si verifichino interferenze 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 provare a 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 due seguenti condizioni:

1. Questo dispositivo non può causare interferenze dannose.

2. Questo dispositivo deve accettare qualsiasi interferenza ricevuta, comprese 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 sono quindi conformi alle norme europee armonizzate applicabili elencate 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 RAEE): i prodotti contrassegnati da 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 attrezzatura equivalente o smaltirlo presso i punti di raccolta designati. Per ulteriori informazioni, vedere: www.recyclethis.info.

2006/66/CE (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 di Industry 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 dispositivo, ricevere 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.
- Assicurarsi che le condizioni ambientali soddisfino le specifiche di fabbrica.
- Assicurarsi che l'unità sia adeguatamente fissata a un rack o a uno scaffale. Urti o scossoni gravi all'unità a seguito di una 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 dovrebbe essere utilizzato un HDD consigliato in fabbrica.

L'uso improprio o la sostituzione 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 correttamente il prodotto per evitare pericoli o perdite di proprietà.

La misura precauzionale si articola in **Avvertenze** e **Avvertenze: Avvertenze:**

Trascurare una qualsiasi delle avvertenze può causare lesioni gravi o morte.

Avvertenze: Trascurare una qualsiasi delle precauzioni può causare lesioni o danni all'apparecchiatura.

Avvertenze	**Avvertenze** Seguire Segui queste precauzioni per prevenire prevenire potenziali lesioni o lesioni gravi danni materiali. o morte.

Avvertenze

Tutte le operazioni elettroniche devono essere rigorosamente conformi alle normative sulla sicurezza elettrica, alle normative sulla prevenzione degli incendi e ad altre normative correlate nella propria regione.

Si prega di utilizzare l'adattatore di alimentazione, fornito dalla normale azienda. Il consumo di energia non può essere inferiore al valore richiesto.

Non collegare più dispositivi a un adattatore di alimentazione 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 oa soffitto, il dispositivo deve essere fissato saldamente.

Se dal dispositivo escono 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.)

Avvertenze

Non far cadere il dispositivo o sottoporlo a urti fisici e non esporlo a radiazioni elettromagnetiche elevate. Evitare l'installazione dell'apparecchiatura su superfici soggette a vibrazioni o in 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 operativa dettagliata), 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.

La copertura del dispositivo per uso interno deve essere protetta da pioggia e umidità.

È vietato esporre l'apparecchiatura alla luce solare diretta, a bassa ventilazione oa fonti di calore come caloriferi o radiatori (l'ignoranza può causare pericolo di incendio).

Non puntare il dispositivo verso il sole o luoghi molto luminosi. In caso contrario, potrebbe verificarsi una fioritura o una macchia (che tuttavia non è un malfunzionamento) e allo stesso tempo influire sulla resistenza del sensore.

Si prega di 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 può erodere il rivestimento superficiale del coperchio del dispositivo.

Si prega di 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 gli involucri dopo averli disimballati per un uso futuro. In caso di guasto, è necessario restituire il dispositivo alla fabbrica con l'involucro originale. Il trasporto senza l'involucro originale può provocare danni al dispositivo e comportare costi aggiuntivi.

L'uso improprio o la sostituzione 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 1Descrizione del prodotto

1.1 Panoramica

DS-K2600 è un controller di accesso potente e stabile, che utilizza il design dell'architettura logica. DS-K2600 è progettato con un'interfaccia di rete TCP/IP e il suo segnale è 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 e GPRS, l'accesso a Ehome. I dati di comunicazione sono appositamente crittografati per alleviare il problema della perdita di privacy

Supporta il riconoscimento e la memorizzazione del numero della carta con una lunghezza massima di 20

Il controllore di accesso può memorizzare 100mila tessere legali (97mila tessere normali e 3mila tessere visitatori) e 300mila tessere di passaggio

Supporta la funzione di interblocco multi-porta, la funzione anti-passback, la funzione multi-card, la funzione di apertura della prima carta, la funzione super card e super password, la crittografia della carta M1, la funzione di aggiornamento online e il controllo remoto delle porte

Supporta l'allarme antimanomissione per lettore di carte, allarme per porta non protetta, allarme per apertura forzata della porta, allarme per timeout apertura porta, allarme antiscasso e codice, allarme lista nera e allarme per tentativi illegali di strisciata carta che raggiungono il limite

L'ingresso di allarme del controller supporta la funzione di protezione da cortocircuito e la funzione antitaglio

Metodi di caricamento di più eventi: canale, gruppo centrale e ascolto

50 collegamenti tra eventi e carte

Rilevamento del conflitto di indirizzi IP

Funzione anti-pass-back cross-controller (per l'anti-pass-back cross-controller basato sulla scheda, collegare il lettore di schede con RS-485. Per l'anti-pass-back cross-controller basato sulla rete, collegare il server e il dispositivo correttamente. fino a 5000 record di scorrimento delle carte possono essere archiviati nel server selezionato.) e funzione anti-pass-back del dispositivo interno

Supporta l'interfaccia RS485 e l'interfaccia Wiegand per l'accesso al lettore di schede. L'interfaccia RS485 adotta un design a doppia interfaccia e supporta il rilevamento del punto di interruzione del loop e la funzione di ridondanza; 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/disabilitato/lista nera/pattuglia/ospite/coercizione/super carta, ecc.

Vari indicatori per mostrare diversi stati

Supporta la sincronizzazione dell'ora tramite NTP, metodo manuale o automatico

Supporta la funzione di archiviazione delle registrazioni quando è offline e la funzione di allarme di archiviazione dello spazio di archiviazione insufficiente

Il controller di accesso ha un design della batteria di backup, un design del watchdog e una funzione a prova di manomissione

I dati possono essere salvati in modo permanente dopo lo spegnimento del controller di accesso.

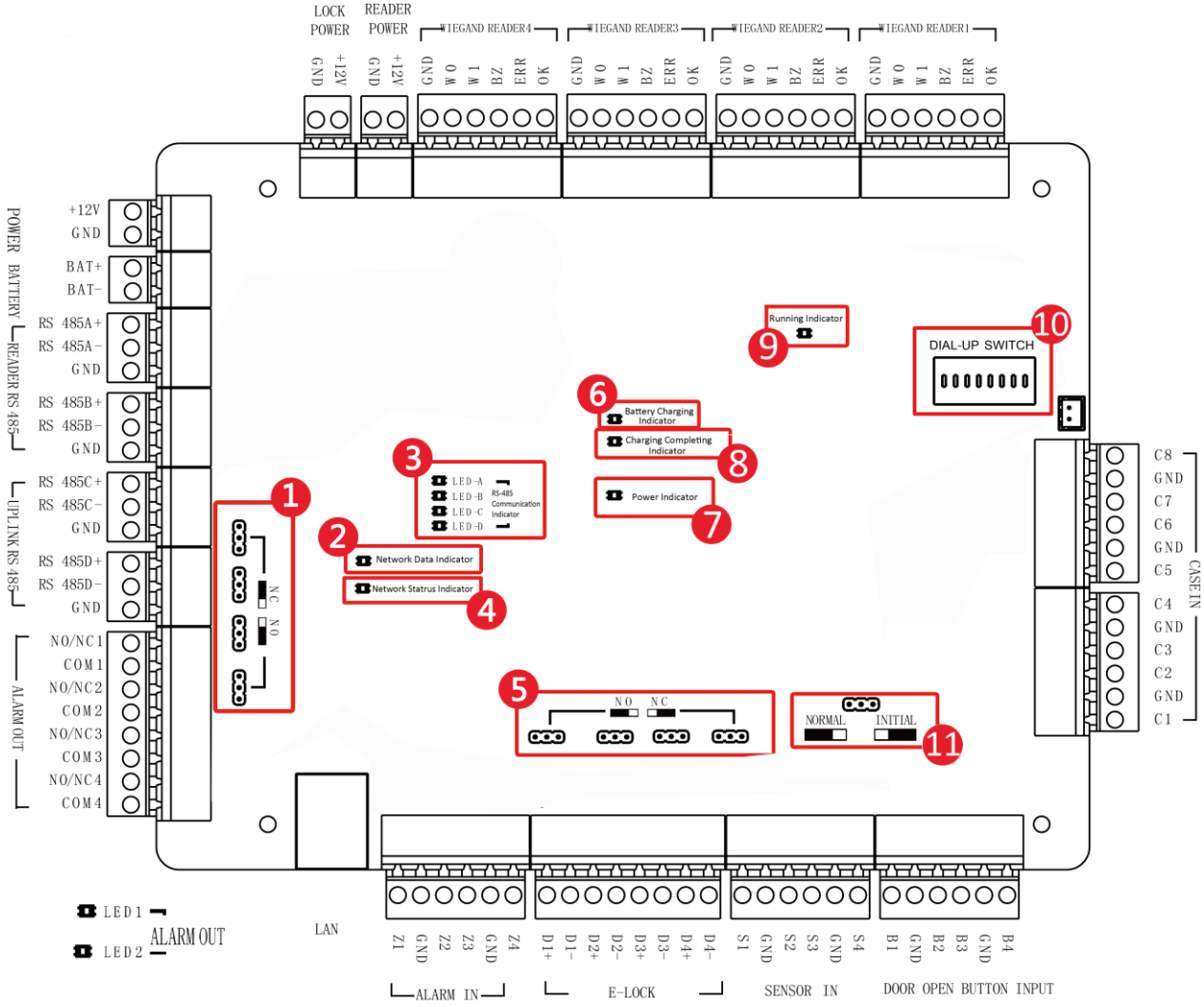
Supporta il collegamento I/O e il collegamento degli eventi

Supporta il protocollo Ehome e la comunicazione tra reti

500 gruppi di password in modalità di autenticazione di carta e password

Capitolo 2Descrizione dei componenti

Prendi DS-K2604 come esempio, il diagramma schematico del componente è mostrato di seguito.



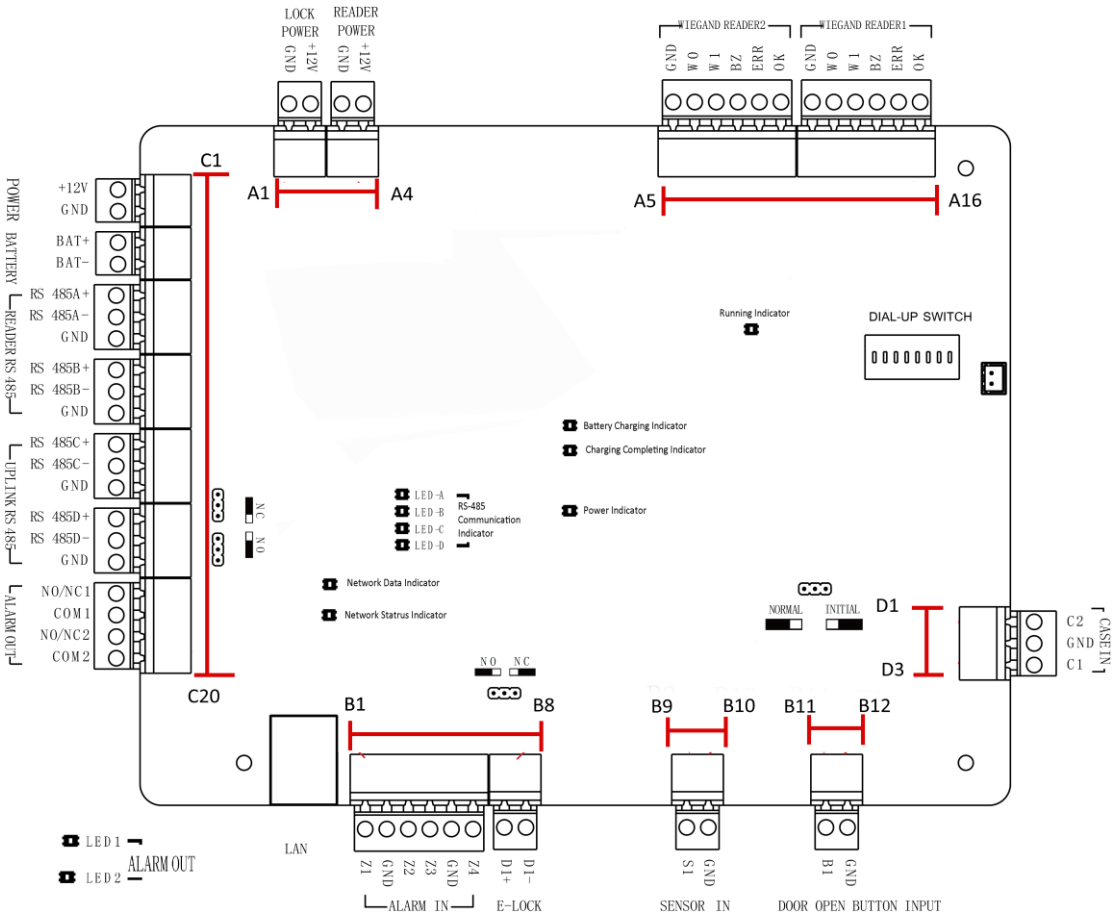
No.	Descrizione del componente		
	DS-K2601	**DS-K2602**	**DS-K2604**
1	Indicatore dei dati di rete dello stato		
2	dell'uscita del relè di allarme (NC/NO)		
3	Indicatore di comunicazione RS-485		
4	Indicatore di stato della rete		
5	Scelta dello stato dell'uscita del relè della porta (NC/NO)		
6	Indicatore di carica della batteria		

No.	**Descrizione del componente**
7	Indicatore di energia
8	Indicatore di carica completa
9	Indicatore di marcia
10	Inizializzazione hardware e scelta di funzionamento normale Interruttore di
11	accesso remoto della scheda principale Impostare l'indirizzo DIP per il controller di accesso. Intervallo disponibile: da 1 a 63. Esempio: Se l'indirizzo DIP è 24, impostare Bit 4 e Bit 5 su ON. ***Appunti:*** Le impostazioni saranno valide dopo il riavvio del dispositivo. Per i dettagli sulle impostazioni DIP, vedere *Appendice C Descrizione dell'interruttore DIP.*

Capitolo 3 Collegamento del terminale

3.1 Descrizione del terminale

3.1.1 Descrizione del terminale DS-K2601



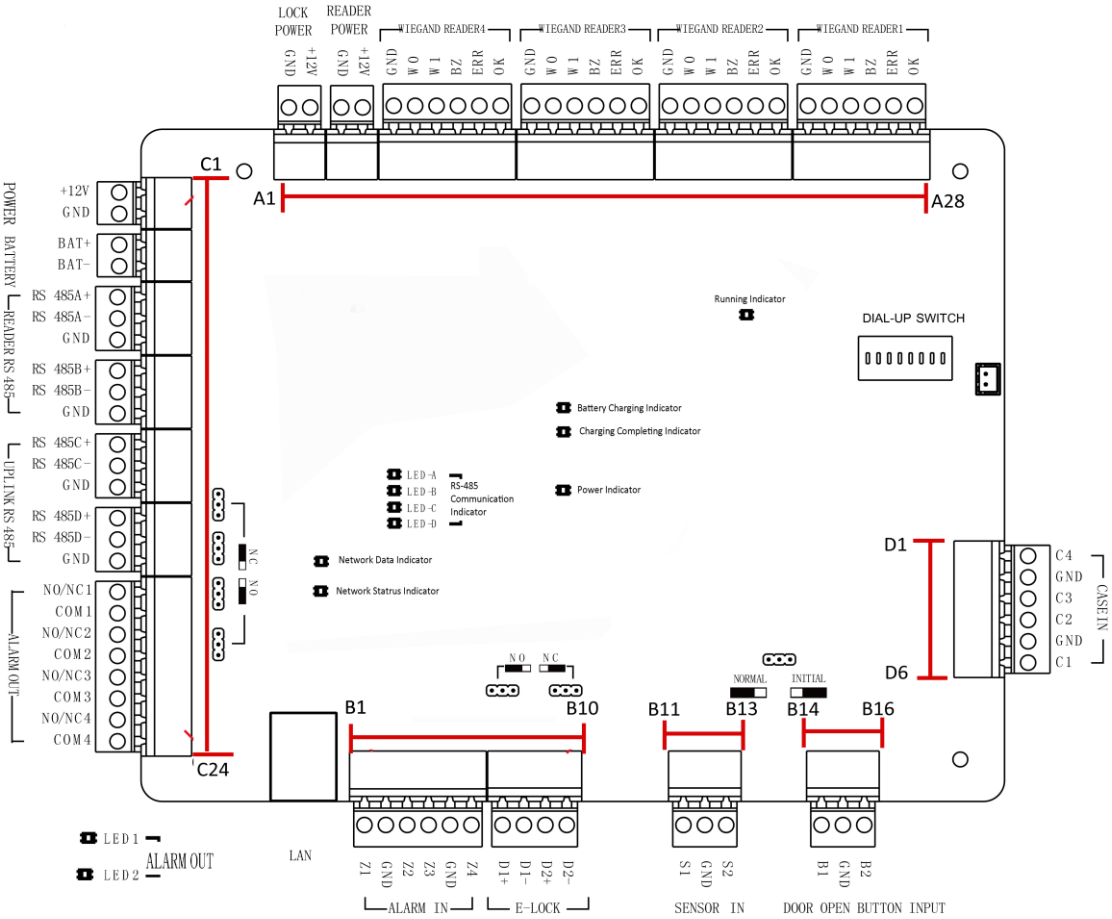
Le descrizioni dei terminali DS-K2601 sono le seguenti:

No.	DS-K2601		
A1	Potere di blocco	GND	messa a terra
la2		+ 12V	Potenza di uscita della serratura
LA3	Alimentazione del lettore di schede	GND	messa a terra
A4		+ 12V	Potenza di uscita della testina letta
A5	Lettore di schede Wiegand 2	GND	messa a terra
A6		W0	Testina Wiegand Lettura Dati Input Data0
LA7		W1	Testina Wiegand Lettura Dati Input Data1
A8		BZ	Cicalino Lettore di Schede Uscita di Controllo
A9		ERR	Indicatore di Uscita di Controllo Lettore di Schede (Uscita Scheda Non Valida)

No.	DS-K2601		
A10		ok	Indicatore di controllo del lettore di schede Uscita (uscita carta valida)
A11	Lettore di schede Wiegand 1	GND	messa a terra
A12		W0	Testina Wiegand Lettura Dati Input Data0
A13		W1	Testina Wiegand Lettura Dati Input Data1
A14		BZ	Cicalino Lettore di Schede Uscita di Controllo
A15		ERR	Indicatore di Uscita di Controllo Lettore di Schede (Uscita Scheda Non Valida)
A16		ok	Indicatore di controllo del lettore di schede Uscita (uscita scheda valida) Area di
B1	Ingresso regione di inserimento	Z1	inserimento Terminale di accesso 1
B2		GND	messa a terra
B3		Z2	Zona di inserimento Accesso al terminale 2
B4		Z3	Zona di inserimento Accesso al terminale 3
B5		GND	messa a terra
B6		Z4	Terminale di accesso alla regione di inserimento 4
B7	E-Lock	D1+	Ingresso relè porta 1 porta (contatto pulito)
B8		D1-	
B9	Ingresso contatto porta	S1	Ingresso rilevatore contatto porta porta 1
B10		GND	messa a terra
B11	Pulsante di apertura della porta	B1	Porta 1 Ingresso pulsante di apertura porta
B12		GND	messa a terra
do1	Energia	+ 12V	Catodo DC12V
do2		GND	Ingresso di messa a terra DC12V
C3	Batteria	BAT+	Catodo batteria DC12V
C4		BAT-	Anodo della batteria DC12V
C5	Lettore di schede 485	RS485A+	Lettore di schede Accesso RS485+
C6		RS485A-	Lettore di schede Accesso RS485
C7		GND	messa a terra
C8		RS485B+	Lettore di schede RS485+
C9		RS485B-	Lettore di schede RS485-
C10		GND	messa a terra
C11	Controllore di accesso RS485 Interfaccia	RS485C+	Uplink RS485+Comunicazione
C12		RS485C-	Uplink RS485-Comunicazione
C13		GND	messa a terra
C14		RS485D+	Riservato
C15		RS485D-	
C16		GND	
C17	Uscita allarme	NA/NC1	Uscita relè allarme 1 (contatto pulito)
C18		COM1	
C19		NA/NC2	Uscita relè allarme 2 (contatto pulito)
C20		COM2	
D1	Ingresso evento	do2	Evento Allarme Ingresso 2

No.	DS-K2601		
re2		GND	messa a terra
RE3		do1	Evento Ingresso allarme 1

3.1.2 Descrizione del terminale DS-K2602



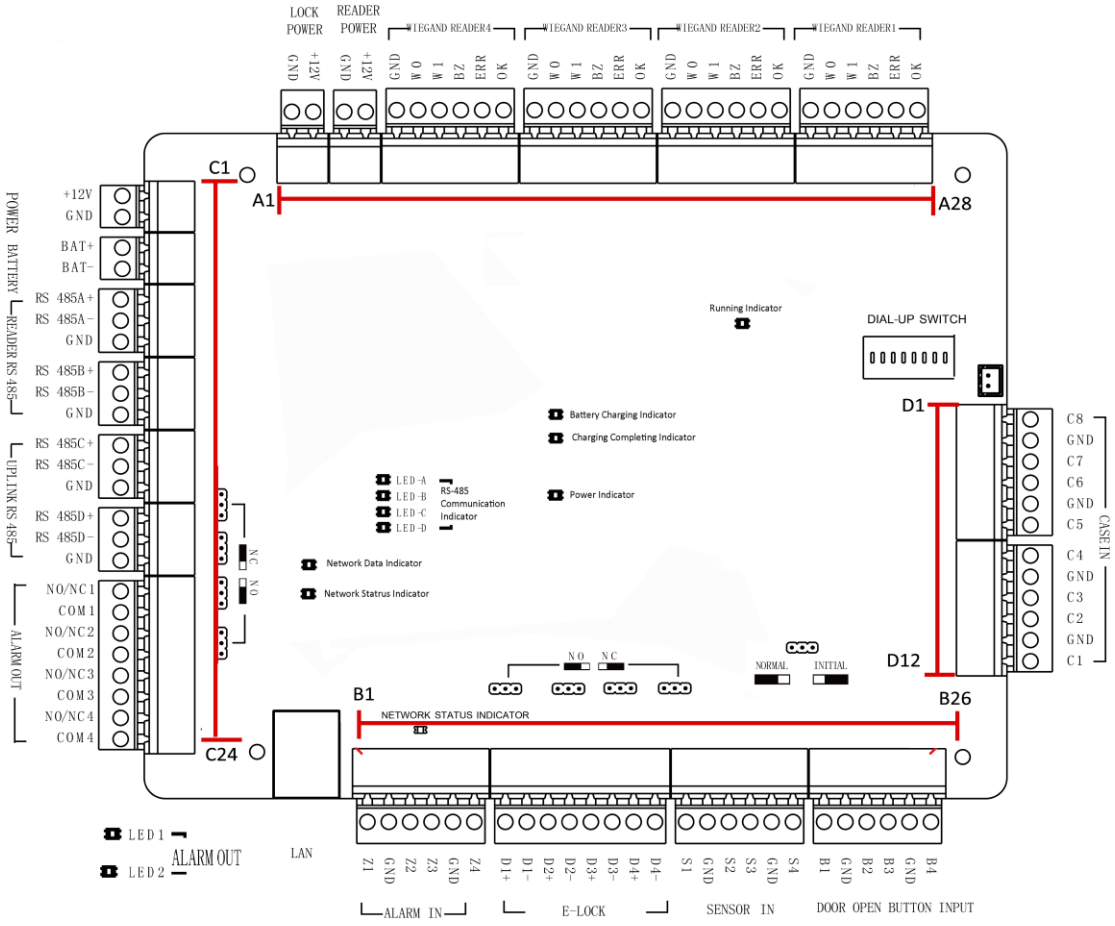
DS-K2602Le descrizioni dei terminali sono le seguenti:

No.	DS-K2602		
A1	Potenza per E-Lock	GND	messa a terra
la2		+ 12V	Potenza di uscita della serratura
LA3	Alimentazione per lettore di schede	GND	messa a terra
A4		+ 12V	Potenza di uscita della testina letta
A5	Lettore di schede Wiegand 4	GND	messa a terra
A6		W0	Testina Wiegand Lettura Dati Input Data0 Testina
LA7		W1	Wiegand Lettura Dati Input Data1 Cicalino Lettore di
A8		BZ	Schede Uscita di Controllo Indicatore di Uscita di
A9		ERR	Controllo Lettore di Schede (Non valido uscita scheda)
A10		ok	Indicatore dell'uscita di controllo del lettore di schede (valido)

No.	DS-K2602		
			uscita scheda)
A11	Lettore di schede Wiegand 3	GND	messa a terra
A12		W0	Testina Wiegand Lettura Dati Input Data0
A13		W1	Testina Wiegand Lettura Dati Input Data1
A14		BZ	Lettore Schede Uscita Controllo Buzzer
A15		ERR	Indicatore dell'uscita di controllo del lettore di schede (non valido uscita scheda)
A16		ok	Indicatore dell'uscita di controllo del lettore di schede (valido) uscita scheda)
A17	Lettore di schede Wiegand 2	GND	messa a terra
A18		W0	Testina Wiegand Lettura Dati Input Data0 Testina
A19		W1	Wiegand Lettura Dati Input Data1 Cicalino Lettore di
A20		BZ	Schede Uscita di Controllo Indicatore di Uscita di
A21		ERR	Controllo Lettore di Schede (Non valido uscita scheda)
A22		ok	Indicatore dell'uscita di controllo del lettore di schede (valido) uscita scheda)
A23	Lettore di schede Wiegand 1	GND	messa a terra
A24		W0	Testina Wiegand Lettura Dati Input Data0 Testina
A25		W1	Wiegand Lettura Dati Input Data1 Cicalino Lettore di
A26		BZ	Schede Uscita di Controllo Indicatore di Uscita di
A27		ERR	Controllo Lettore di Schede (Non valido uscita scheda)
A28		ok	Indicatore dell'uscita di controllo del lettore di schede (valido) uscita scheda)
B1	Regione di inserimento	Z1	Terminale di accesso alla regione di inserimento 1
B2		GND	messa a terra
B3		Z2	Zona di inserimento Accesso al terminale 2
B4		Z3	Zona di inserimento Accesso al terminale 3
B5		GND	messa a terra
B6		Z4	Terminale di accesso alla regione di inserimento 4
B7	E-Lock1	D1+	Ingresso relè porta 1 porta (contatto pulito)
B8		D1-	
B9	E-Lock2	D2+	Ingresso relè porta porta 2 (contatto pulito)
B10		D2-	
B11	Magnetica della porta Rivelatore	S1	Ingresso rilevatore magnetico porta 1
B12		GND	Messa a terra del segnale
B13		S2	Ingresso rilevatore magnetico porta 2
B14	Pulsante della porta	B1	Ingresso pulsante porta 1 porta
B15		GND	Messa a terra del segnale
B16		B2	Ingresso pulsante porta porta 2
do1	Energia	+ 12V	Catodo DC12V
do2		GND	messa a terra

No.	DS-K2602		
C3	Batteria	BAT+	Catodo batteria DC12V
C4		BAT-	Anodo della batteria DC12V
C5	Lettore di schede 485 Interfaccia	RS 485A+	Lettore di schede Accesso RS485+
C6		RS 485A-	Lettore di schede RS485- Accesso
C7		GND	messa a terra
C8		RS 485B+	Lettore di schede RS485+
C9		RS 485B-	Lettore di schede RS485-
C10		GND	messa a terra
C11	Interfaccia RS-485	RS 485C+	Uplink RS485+Comunicazione
C12		RS 485C-	Uplink Comunicazione RS485
C13		GND	messa a terra
C14		RS 485D+	Riservato
C15		RS 485D-	
C16		GND	
C17	Uscita allarme	NON do1	Uscita relè allarme 1 (contatto pulito)
C18		COM1	
C19		NON do2	Uscita relè allarme 2 (contatto pulito)
C20		COM2	
C21		NON C3	Uscita relè allarme 3 (contatto pulito)
C22		COM3	
C23		NON C4	Uscita relè allarme 4 (contatto pulito)
C24		COM4	
D1	Ingresso evento	C4	Ingresso allarme evento 4
re2		GND	messa a terra
RE3		C3	Ingresso allarme evento3
D4		do2	Evento Allarme Ingresso 2
D5		GND	messa a terra
D6		do1	Evento Ingresso allarme 1

3.1.3 Descrizione del terminale DS-K2604



DS-K2604Le descrizioni dei terminali sono le seguenti:

No.	DS-K2604		
A1	Alimentazione elettrica di E-Lock	GND	messa a terra
la2		+ 12V	Alimentazione dell'uscita E-Lock
LA3	Alimentazione elettrica del lettore di schede	GND	messa a terra
A4		+ 12V	Alimentazione dell'uscita del lettore di schede
A5	Carta Wiegand Lettore 4	GND	messa a terra
A6		W0	Wiegand Card Reader Data Input Data0
LA7		W1	Wiegand Card Reader Data Input Data1 Cicalino
A8		BZ	dell'uscita di controllo del lettore di carte
A9		ERR	Cresset dell'output di controllo del lettore di schede (non valido uscita scheda)
A10		ok	Cresset dell'uscita di controllo del lettore di schede (scheda valida Produzione)
A11	Carta Wiegand Lettore 3	GND	messa a terra
A12		W0	Dati di ingresso dati del lettore di schede Wiegand0
A13		W1	Dati di ingresso dati del lettore di schede Wiegand1

No.	DS-K2604		
A14		BZ	Cicalino dell'uscita di controllo del lettore di schede
A15		ERR	Cresset dell'output di controllo del lettore di schede (non valido uscita scheda)
A16		ok	Cresset dell'uscita di controllo del lettore di schede (scheda valida Produzione)
A17	Carta Wiegand Lettore 2	GND	messa a terra
A18		W0	Wiegand Card Reader Data Input Data0
A19		W1	Wiegand Card Reader Data Input Data1 Cicalino
A20		BZ	dell'uscita di controllo del lettore di carte
A21		ERR	Cresset dell'output di controllo del lettore di schede (non valido uscita scheda)
A22		ok	Cresset dell'uscita di controllo del lettore di schede (scheda valida Produzione)
A23	Carta Wiegand Lettore 1	GND	messa a terra
A24		W0	Wiegand Card Reader Data Input Data0
A25		W1	Wiegand Card Reader Data Input Data1 Cicalino
A26		BZ	dell'uscita di controllo del lettore di carte
A27		ERR	Cresset dell'uscita di controllo del lettore di schede (scheda non valida Produzione)
A28		ok	Cresset dell'uscita di controllo del lettore di schede (scheda valida Produzione)
B1	Regione di inserimento Ingresso	Z1	Terminale di accesso alla regione di inserimento 1
B2		GND	messa a terra
B3		Z2	Terminale di accesso alla regione di inserimento 2
B4		Z3	Terminale di accesso alla regione di inserimento 3
B5		GND	messa a terra
B6		Z4	Terminale di accesso alla regione di inserimento 4
B7	E-Lock 1	D1+	Ingresso relè porta 1 porta (contatto pulito)
B8		D1-	
B9	E-Lock 2	D2+	Ingresso relè porta porta 2 (contatto pulito)
B10		D2-	
B11	E-Lock 3	D3+	Ingresso relè porta 3 porta (contatto pulito)
B12		D3-	
B13	E-Lock 4	D4+	Porta 4 Ingresso relè porta (contatto pulito)
B14		D4-	
B15	Magnetica della porta Ingresso	S1	Ingresso rilevatore magnetico porta 1
B16		GND	Messa a terra del segnale
B17		S2	Ingresso rilevatore magnetico porta 2
B18		S3	Ingresso rilevatore magnetico porta 3

No.	DS-K2604		
B19		GND	Messa a terra del segnale
B20		S4	Ingresso rilevatore magnetico porta 4
B21	Pulsante della porta	B1	Ingresso pulsante porta 1 porta
B22		GND	Messa a terra del segnale
B23		B2	Ingresso pulsante porta porta 2
B24		B3	Ingresso pulsante porta porta 3
B25		GND	Messa a terra del segnale
B26		B4	Ingresso pulsante porta 4 porte
do1	Energia	+ 12V	Catodo DC12V
do2		GND	messa a terra
C3	Batteria	BAT+	Catodo batteria DC12V
C4		BAT-	Anodo della batteria DC12V
C5	Lettore di schede RS485	RS485A+	Lettore di schede RS485A+
C6		RS485A-	Lettore di schede RS485A-
C7		GND	messa a terra
C8		RS485B+	Lettore di schede RS485B+
C9		RS485B-	Lettore di schede RS485B-
C10		GND	messa a terra
C11	Accesso Controllore RS485	RS485C+	Uplink RS485+Comunicazione
C12		RS485C-	Uplink RS485-Comunicazione
C13		GND	messa a terra
C14		RS485D+	Riservato
C15		RS485D-	
C16		GND	
C17	Uscita allarme	NA/NC1	Uscita relè allarme 1 (contatto pulito)
C18		COM1	
C19		NA/NC2	Uscita relè allarme 2 (contatto pulito)
C20		COM2	
C21		NA/NC3	Uscita relè allarme 3 (contatto pulito)
C22		COM3	
C23		NA/NC4	Uscita relè allarme 4 (contatto pulito)
C24		COM4	
D1	Ingresso evento	C8	Ingresso allarme evento 8
re2		GND	messa a terra
RE3		C7	Ingresso allarme evento 7
D4		C6	Ingresso allarme evento 6
D5		GND	messa a terra
D6		C5	Ingresso allarme evento 5
RE7		C4	Ingresso allarme evento 4
D8		GND	messa a terra
D9		C3	Ingresso allarme evento3
D10		do2	Evento Allarme Ingresso 2
D11		GND	messa a terra

No.	DS-K2604		
D12		do1	Evento Ingresso allarme 1

Appunti:

L'interfaccia hardware di ingresso allarme è normalmente aperta per impostazione predefinita. Quindi è consentito solo il segnale normalmente aperto. Può essere collegato al cicalino del lettore di tessere e del controller di accesso, e l'uscita del relè di allarme e il relè della porta si aprono e si chiudono.

Il collegamento dell'ingresso allarme della regione di attivazione è solo per il collegamento dell'uscita del relè di allarme.

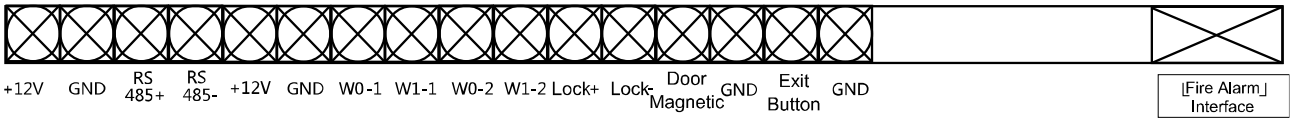
L'ID della scheda RS485 deve essere impostato da 1 a 8. Ad esempio, l'ID della porta 1 è 1 e 2 stanno rispettivamente per entrata e uscita.

Per il controller di accesso a porta singola, 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, i lettori di carte Wiegand 1 e 2 corrispondono rispettivamente ai lettori di carte in entrata e in uscita della porta 1 e il lettore di tessere Wiegand 3 e 4 corrispondono rispettivamente ai lettori di tessere in entrata e in uscita dalla porta 2. Per il controller di accesso a quattro porte, il lettore di tessere Wiegand 1, 2, 3 e 4 corrispondono rispettivamente ai lettori di tessere in entrata della porta 1, 2, 3 e 4.

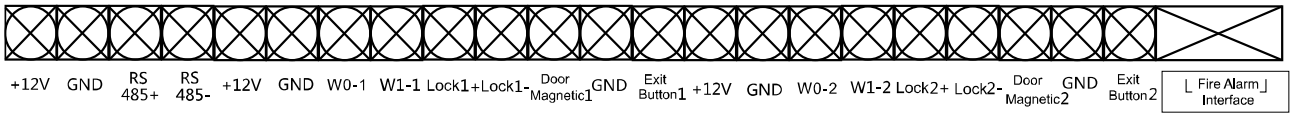
Capitolo 4Installazione del lettore di schede

4.1 Terminale esterno

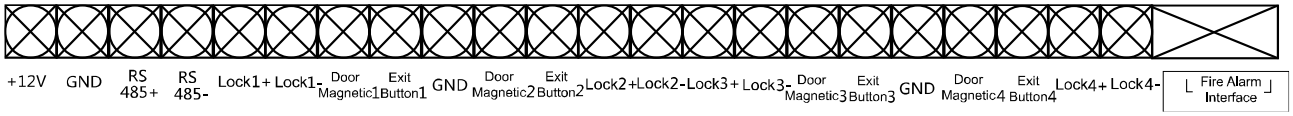
4.1.1 Terminali esterni DS-K2601



4.1.2 Terminali esterni DS-K2602

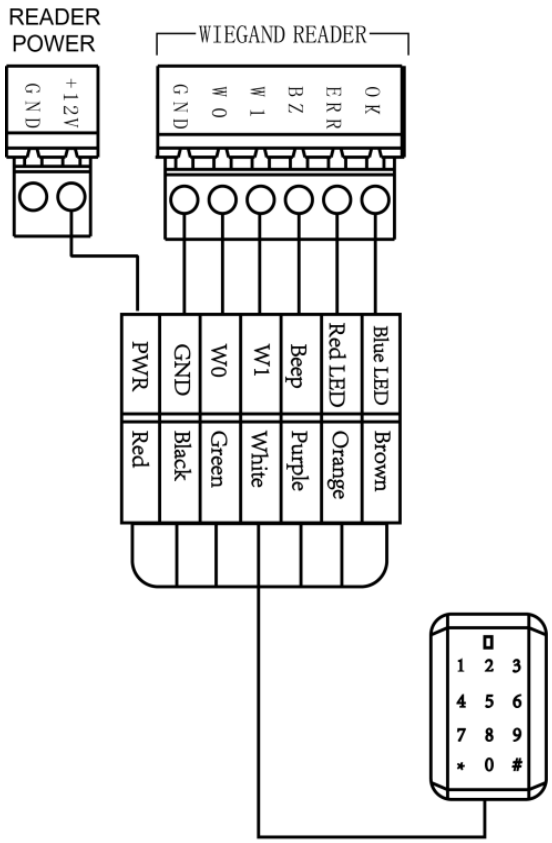


4.1.3 Terminali esterni DS-K2604



4.2 Installazione del lettore di schede

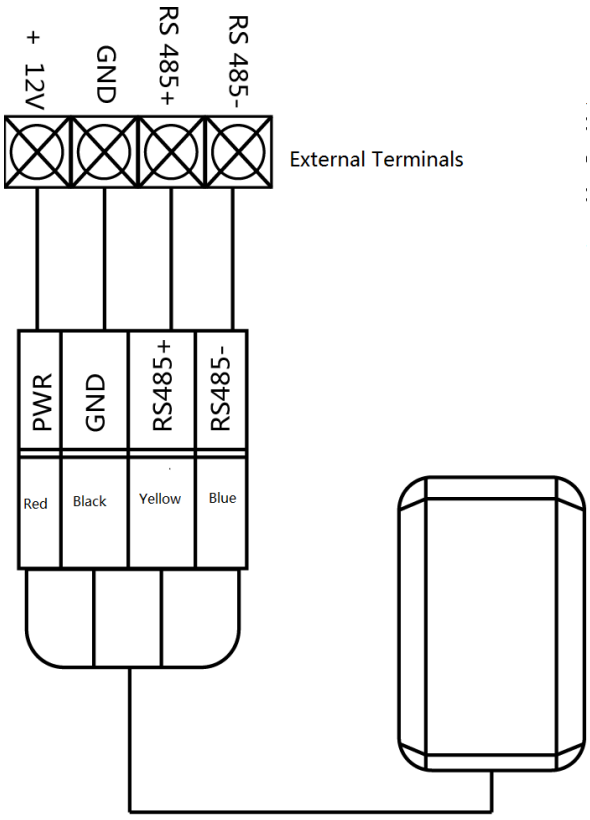
4.2.1 La connessione del lettore di schede Wiegand



Wiegand Communication Wiring

Nota: È necessario collegare l'OK/ERR/BZ, se si utilizza il controller di accesso per controllare il LED e il cicalino del lettore di schede Wiegand.

4.2.2 Collegamento lettore di schede RS485

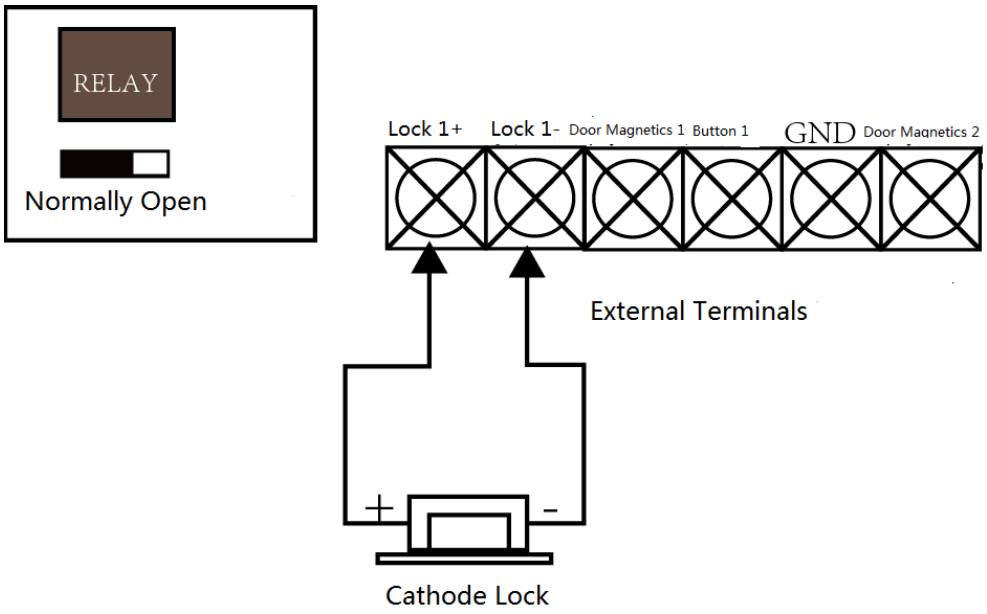


RS485 Communication Wiring

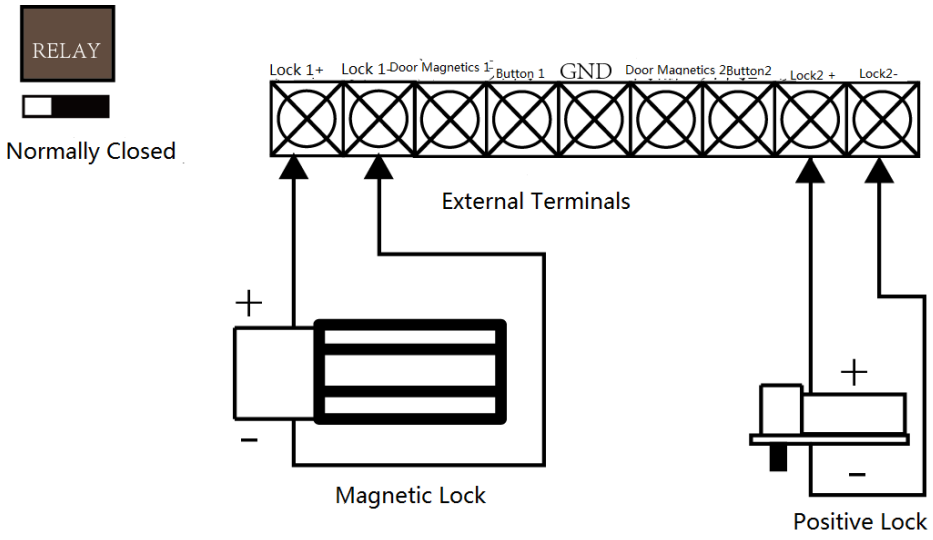
Nota: Se il lettore di schede è installato troppo lontano dal controller di accesso, è possibile utilizzare un alimentatore esterno.

4.3 Installazione di E-Lock

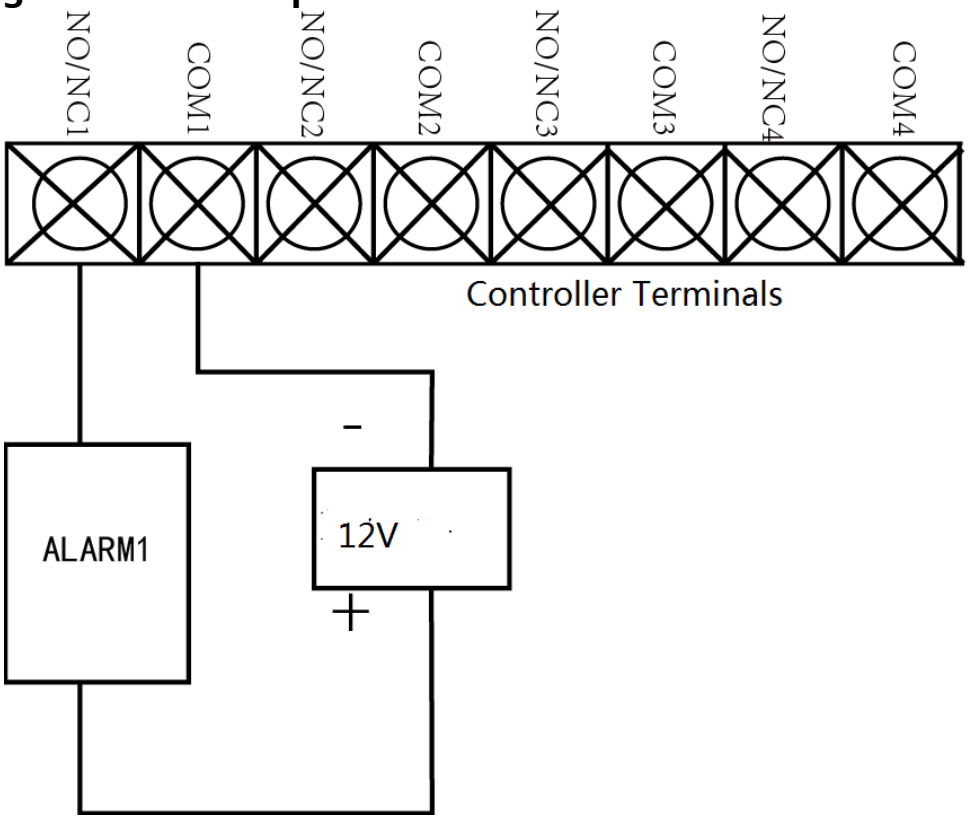
4.3.1 Installazione del blocco catodico



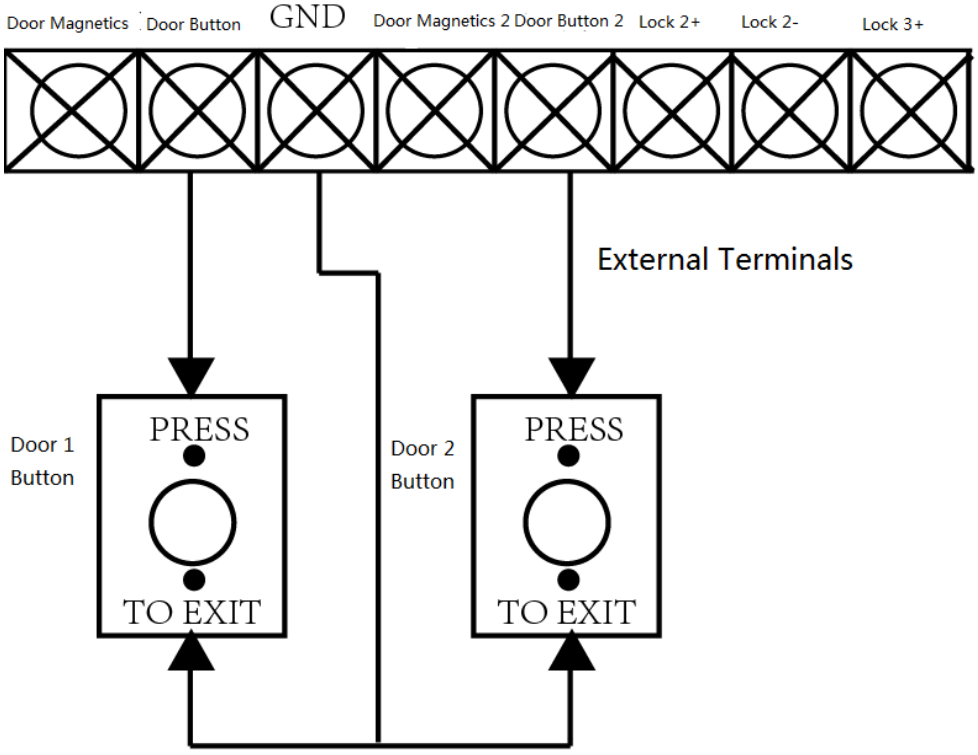
4.3.2 Installazione del blocco dell'anodo



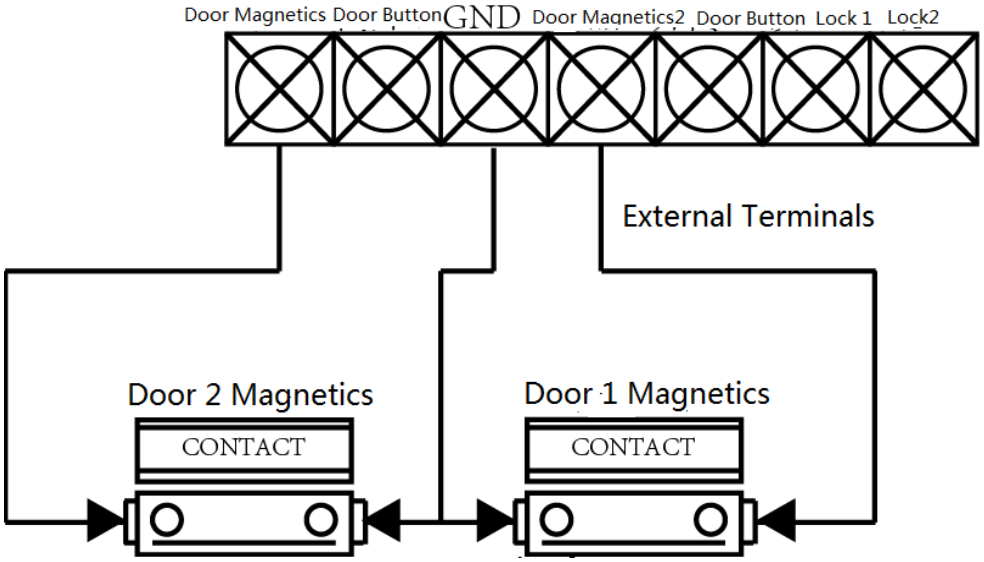
4.4 Collegamento del dispositivo di allarme esterno



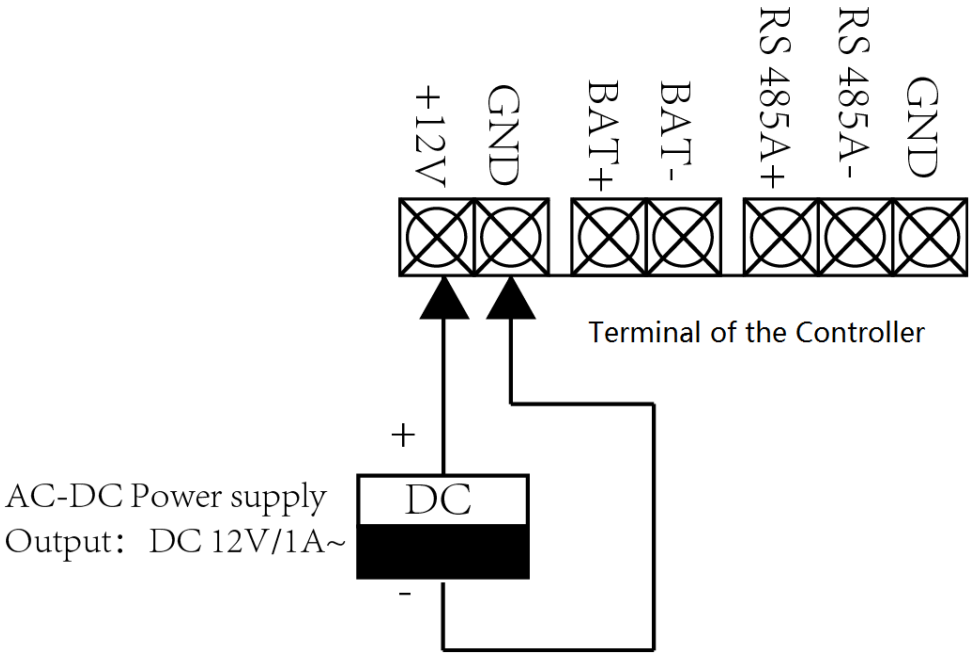
4.5 Schema elettrico del pulsante della porta



4.6 La connessione del rilevamento magnetico

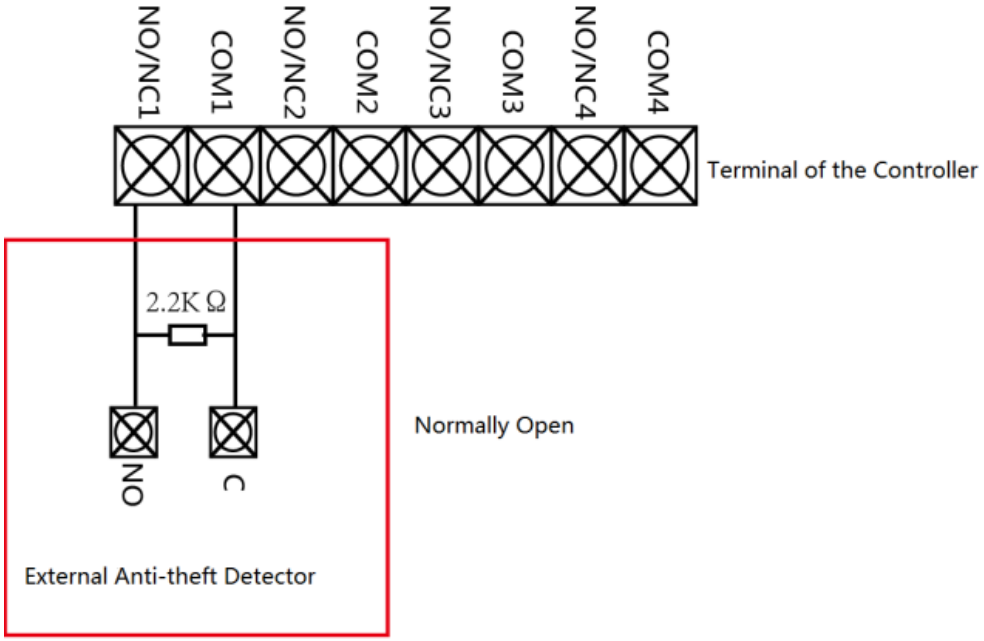


4.7 Collegamento dell'alimentazione

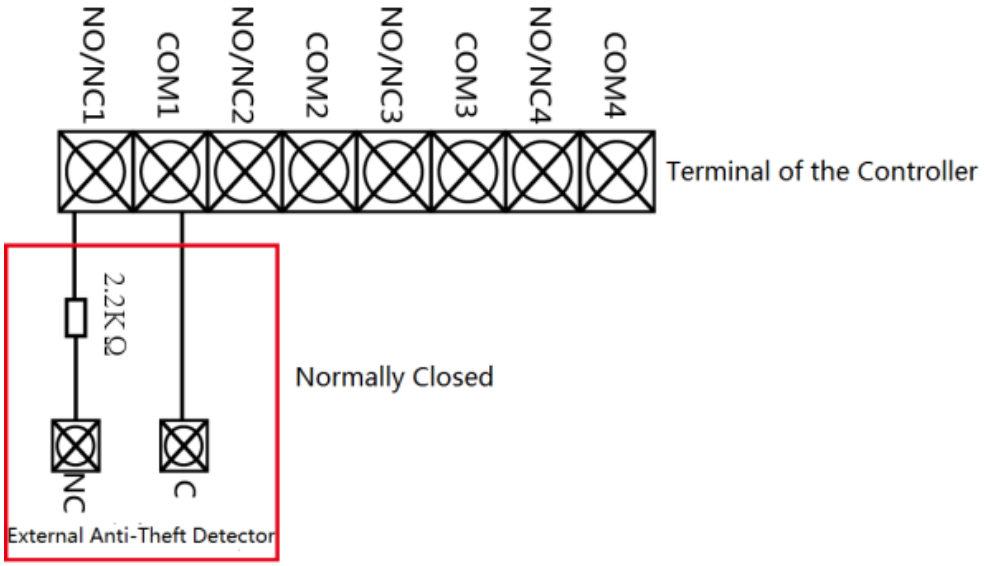


4.8 Terminale di ingresso della regione di inserimento

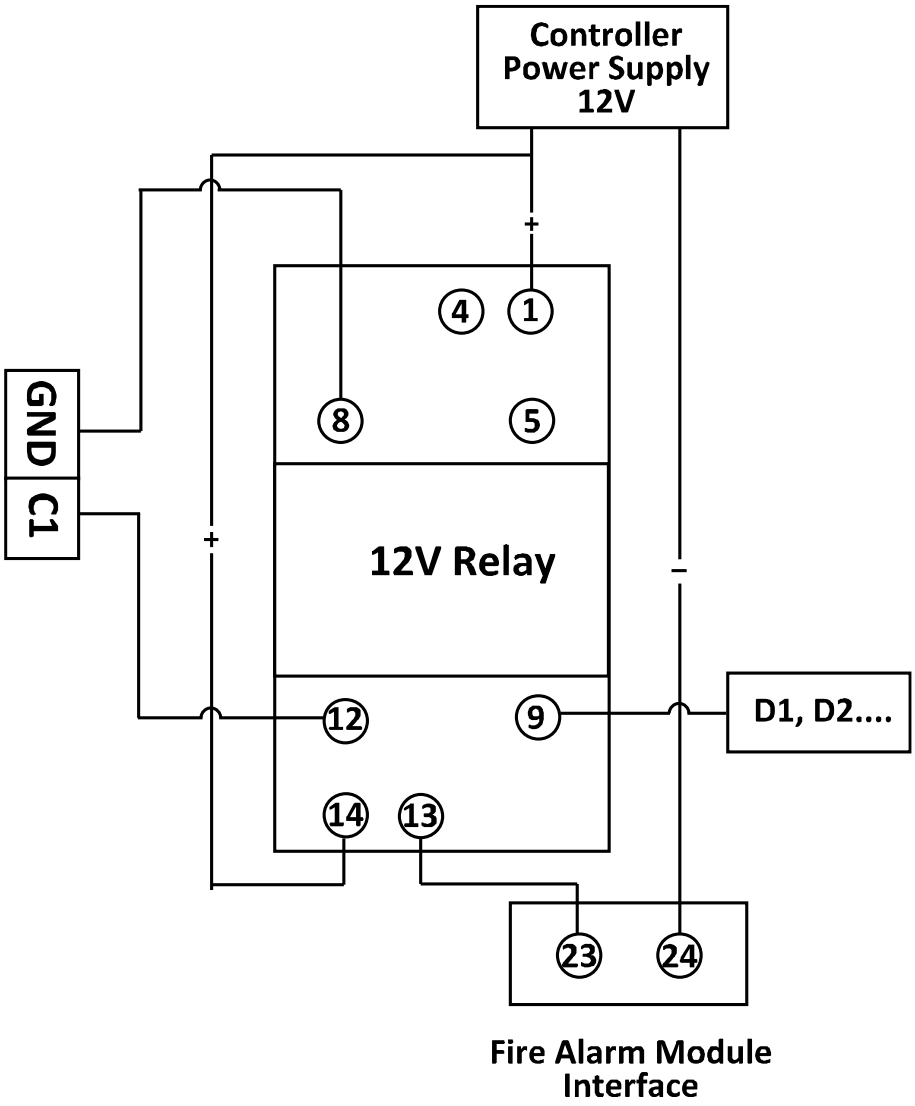
4.8.1 Collegamento del rivelatore normalmente aperto



4.8.2 Collegamento del rivelatore normalmente chiuso



4.9 Cablaggio del modulo di allarme antincendio



Capitolo 5Impostazioni

5.1 Inizializzazione dell'hardware

Opzione 1:

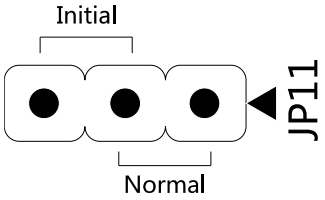
Passaggi:

1. Rimuovere il cappuccio del ponticello dal terminale Normal.
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 è interrotto, 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 è interrotto, riportare il cappuccio del ponticello su Normale.
4. Scollegare l'alimentazione e riavviare il controller di accesso.

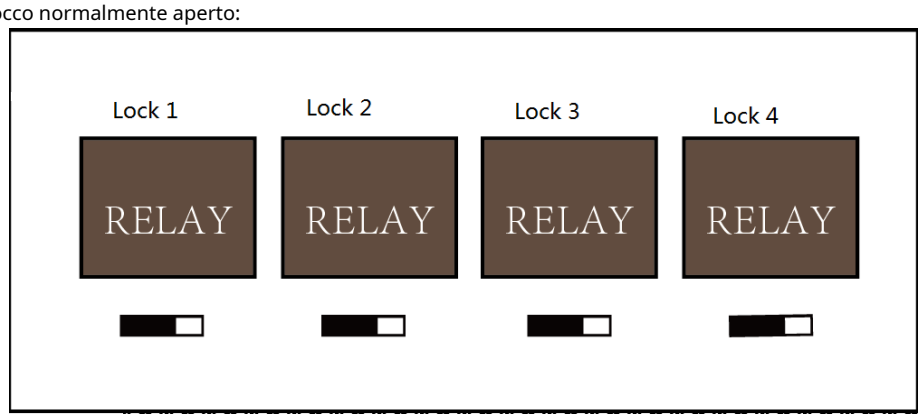


Nota: L'inizializzazione dell'hardware ripristinerà tutti i parametri all'impostazione predefinita e tutti gli eventi del dispositivo verranno cancellati.

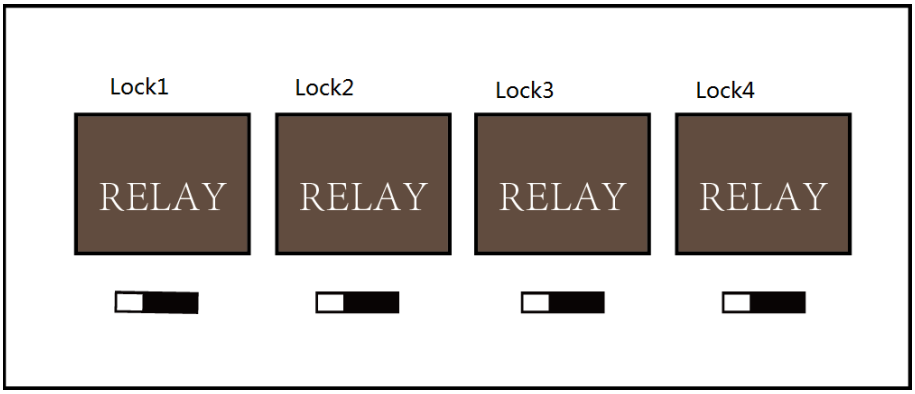
5.2 Ingresso relè NO/NC

5.2.1 Uscita relè di blocco

Stato del relè di blocco normalmente aperto:

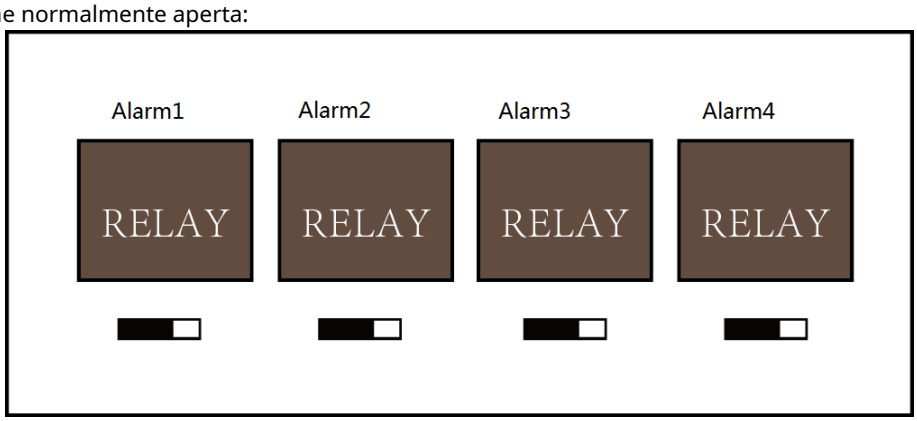


Stato del relè di blocco normalmente chiuso:

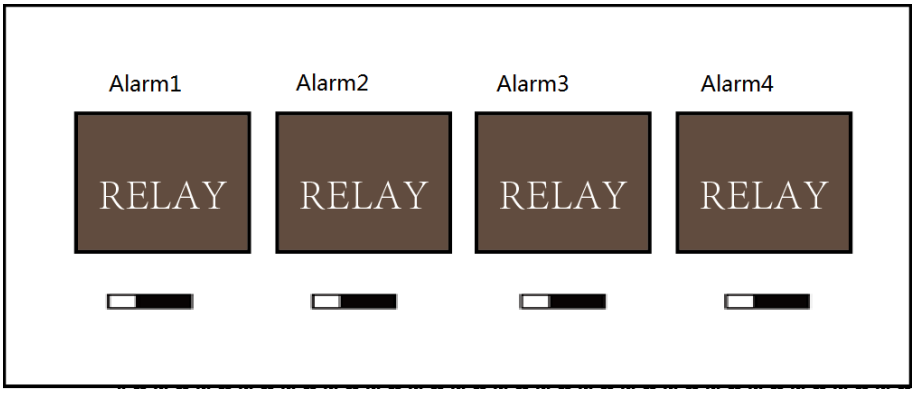


5.2.2 Stato uscita relè di allarme

Uscita relè allarme normalmente aperta:

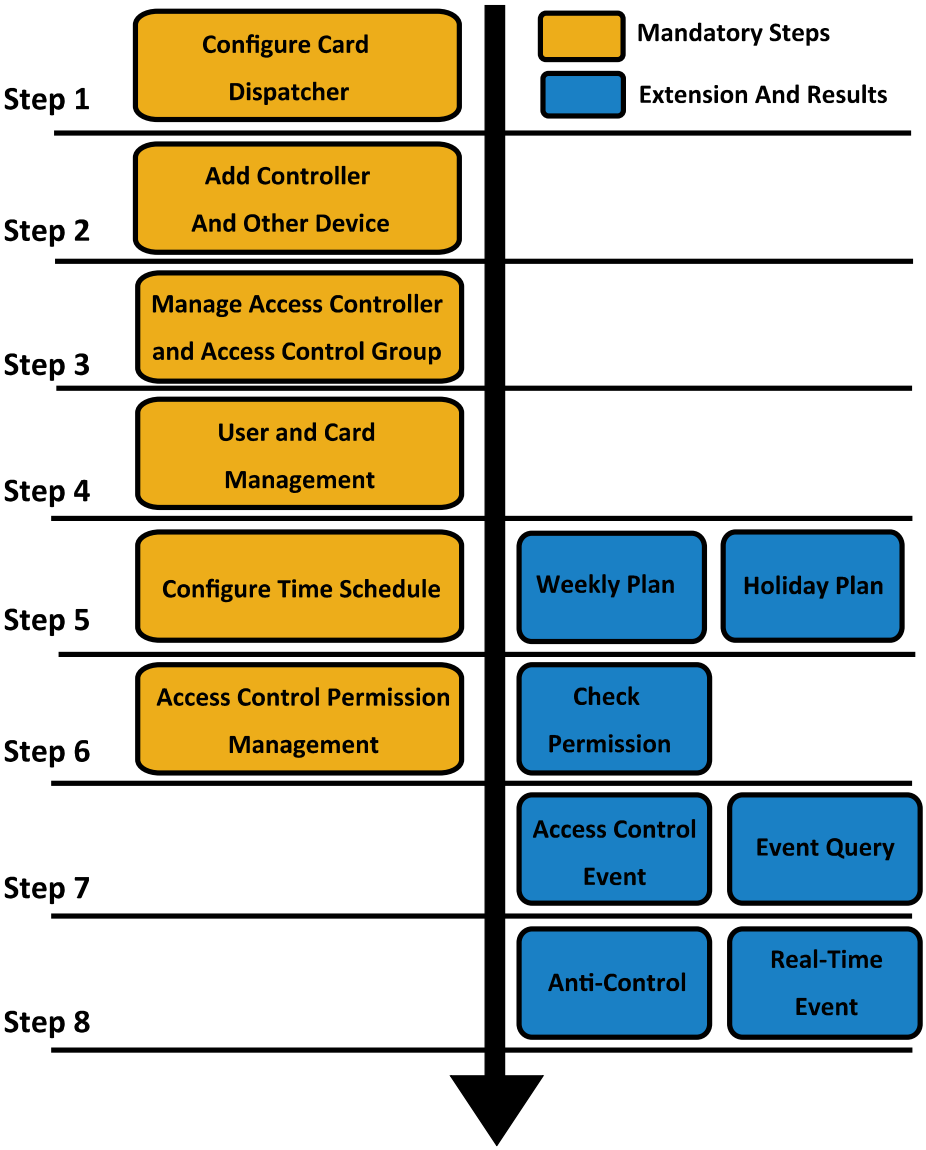


Uscita relè allarme normalmente chiusa:



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 6Attivazione del controllo di accesso 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.

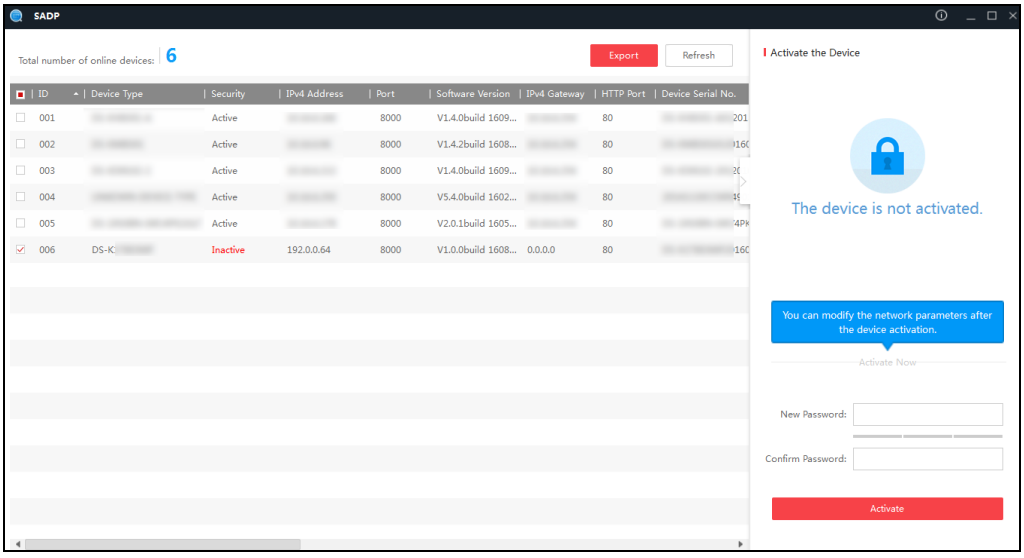
6.1 Attivazione tramite software SADP

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

Prendi il software SADP dal disco in dotazione e installa SADP secondo le istruzioni. Seguire i passaggi per attivare il pannello di controllo.

Passaggi:

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

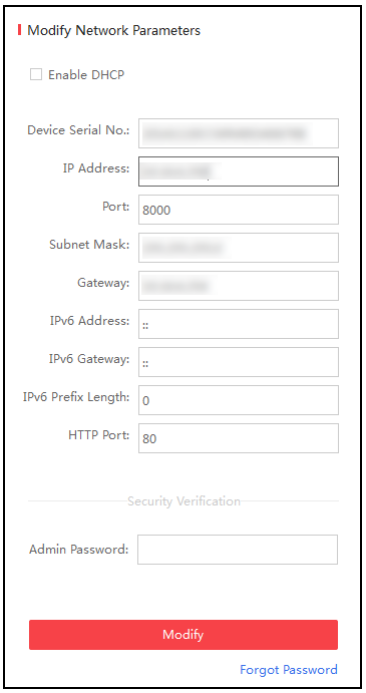


3. Creare una password e inserire la password nel campo della password, quindi confermare la password.

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

4. Fare clic su **Attivare** per attivare il dispositivo.
5. Controllare 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.

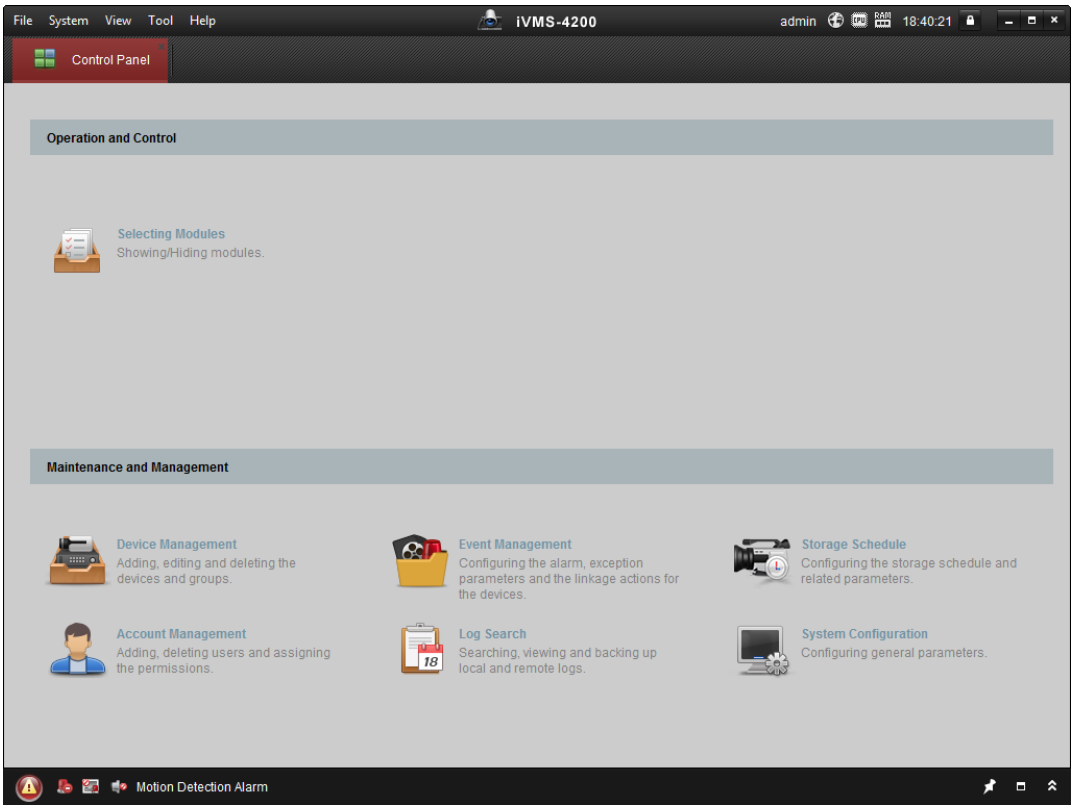
6.2 Attivazione tramite software client

Il software client è un versatile software di gestione video per più tipi di dispositivi.

Ottenere il software client dal disco in dotazione e installare il software in base alle istruzioni. Seguire i passaggi per attivare il pannello di controllo.

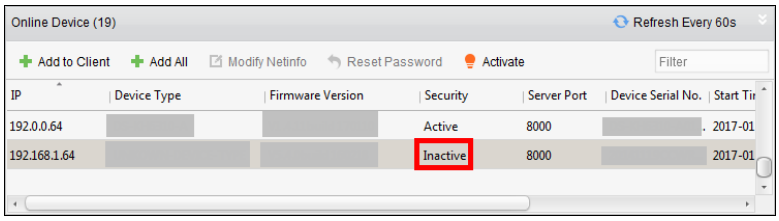
Passaggi:

1. Eseguire il software client e si apre 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. Fare clic su **Attivare** pulsante per visualizzare l'interfaccia di attivazione.

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

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

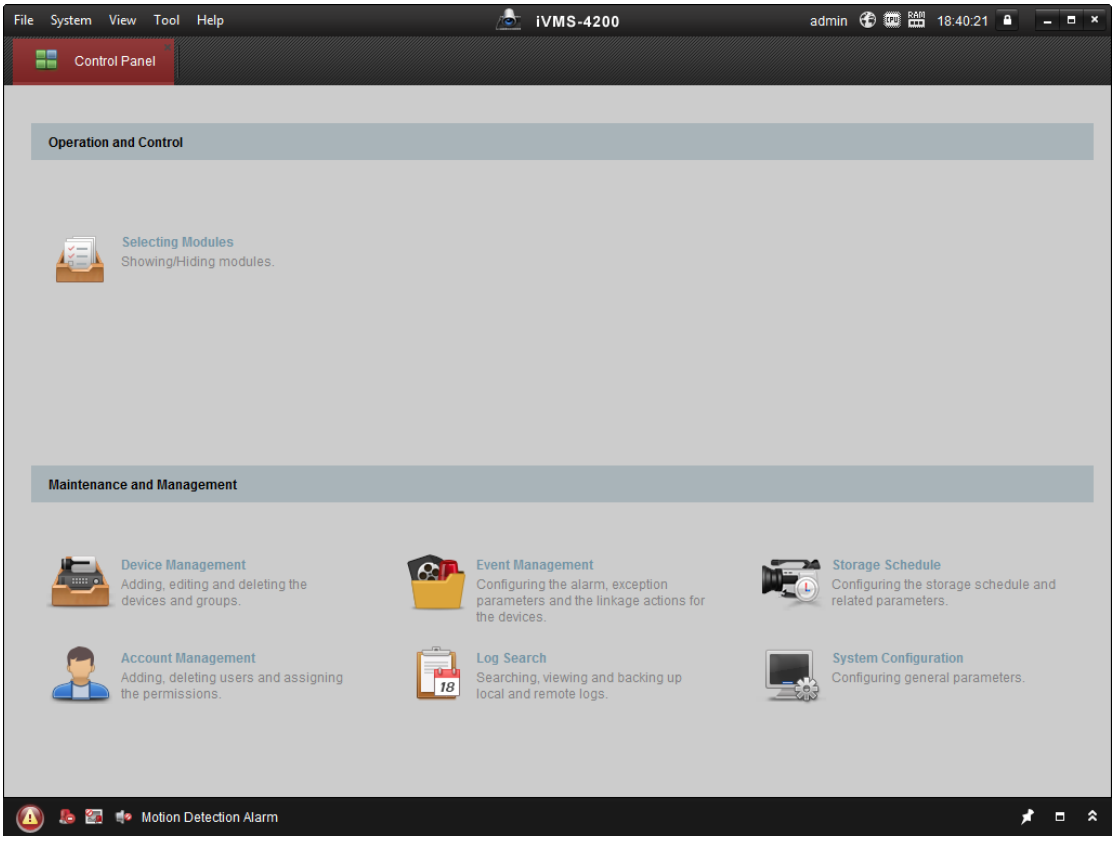
6. Fare clic su **ok** pulsante per avviare l'attivazione.
7. Fare clic su **Modifica Netinfor** per visualizzare l'interfaccia di modifica dei parametri di rete.
8. Modificare l'indirizzo IP del dispositivo sullo stesso segmento di rete del computer modificando manualmente l'indirizzo IP.
9. Immettere la password e fare clic su **ok** pulsante per salvare le impostazioni.

Capitolo 7 Funzionamento del 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:

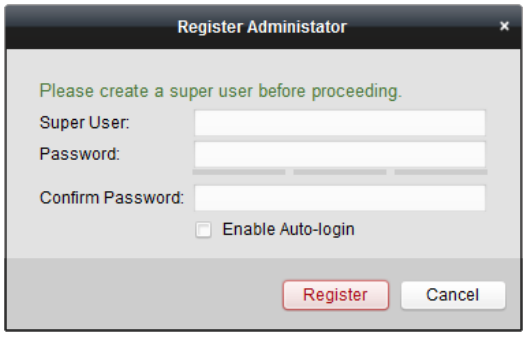


7.2 Registrazione utente e login

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

Passaggi:

1. Immettere il nome utente e la password del superutente. Il software giudicherà la sicurezza della password automaticamente e ti consigliamo vivamente di utilizzare una password complessa per garantire la sicurezza dei tuoi dati.
2. Confermare la password.
3. Facoltativamente, seleziona 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 una 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.

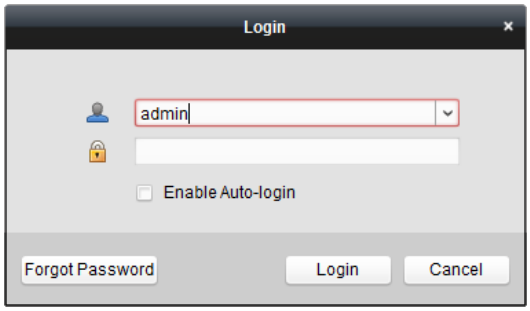
Passaggi:

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 pop-up. Contatta il tuo rivenditore e inviagli la stringa crittografata per reimpostare la password.

2. Facoltativamente, seleziona 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 (tra cui procedura guidata video, procedura guidata video wall, procedura guidata pannello di controllo di sicurezza, procedura guidata controllo accessi e videocitofono e procedura guidata presenze), per guidare l'utente ad aggiungere il dispositivo ed eseguire altre impostazioni e operazioni . Per una configurazione dettagliata delle procedure guidate, fare riferimento a *Guida rapida di iVMS-4200.*

7.3 Configurazione del sistema

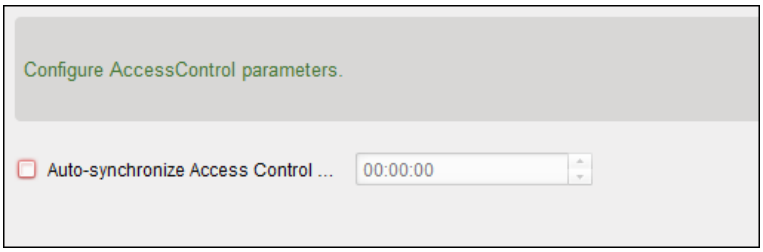
Scopo:

È possibile sincronizzare gli eventi di controllo degli accessi mancati al client.

Passaggi:

1. Fare clic su **Attrezzo** – **Configurazione di sistema.**
2. Nella finestra Configurazione del sistema, selezionare il **Sincronizzazione automatica dell'evento di controllo degli accessi** casella di controllo.
3. Impostare l'ora di sincronizzazione.

   Il client sincronizzerà automaticamente l'evento di controllo dell'accesso mancato al client all'ora impostata.



7.4 Gestione del controllo degli accessi

Scopo:

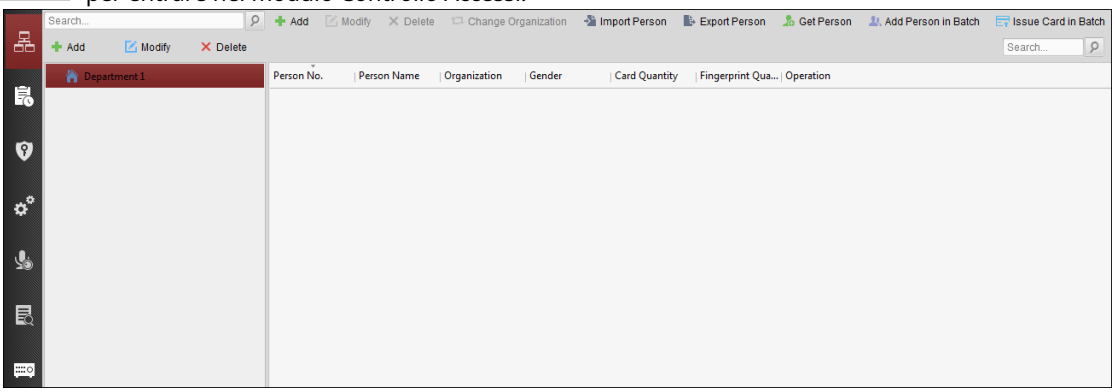
Il modulo Controllo Accessi è applicabile a dispositivi di controllo accessi e videocitofoni. Fornisce molteplici funzionalità, tra cui la gestione di persone e tessere, la configurazione dei permessi, la gestione dello stato del controllo degli accessi, il videocitofono e altre funzioni avanzate.

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

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

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

Clic  per entrare nel modulo Controllo Accessi.



Prima che inizi:

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

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.

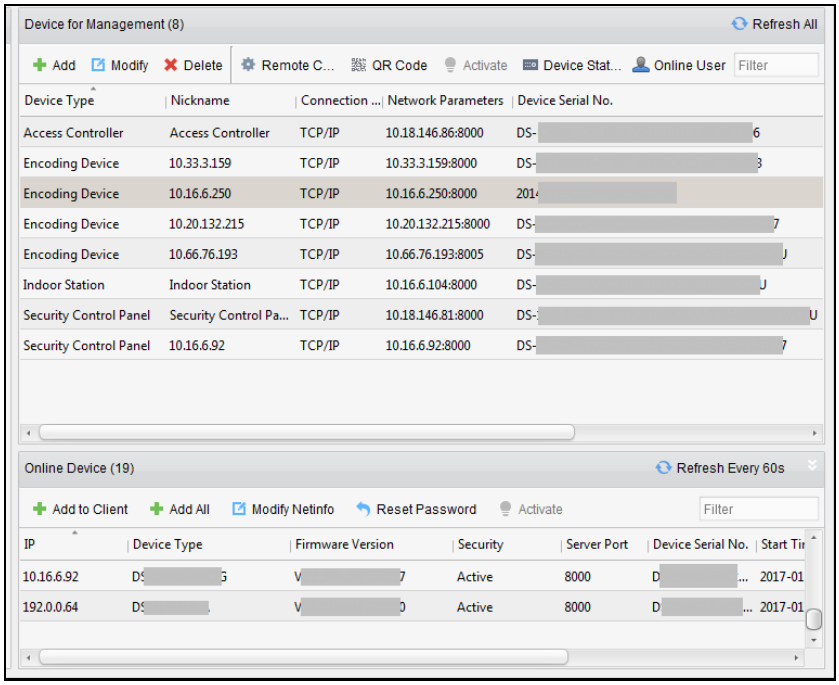
Il modulo Controllo Accessi è composto dai seguenti sottomoduli.

	Persona e carta	Gestire le organizzazioni, le persone e assegnare le carte alle persone.
	Programma e Modello	Configurazione della programmazione settimanale, del gruppo ferie e dell'impostazione del modello.
	Autorizzazione	Assegnazione dei permessi di controllo accessi alle persone e applicazione ai dispositivi.
	Funzione avanzata	Fornire funzioni avanzate tra cui le impostazioni dei parametri di controllo degli accessi, l'autenticazione del lettore di schede, porta apribile con prima tessera, antipassante, multi-porta incastro, e autenticazione parola d'ordine.
	Videocitofono	Videocitofono tra cliente e residente, ricerca nel registro delle chiamate e rilascio dell'avviso. Ricerca
	Ricerca	eventi storici di controllo accessi; Ricerca nei registri delle chiamate, sblocco dei registri e avvisi rilasciati. Gestione dei
	Dispositivo Gestione	dispositivi di controllo accessi e dei dispositivi videocitofonici.

Nota: In questo capitolo introduciamo solo le operazioni relative al 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 attivazione del dispositivo in **Attrezzo** – **Controllo dell'inserimento del dispositivo.** Se il dispositivo non è inserito, è necessario inserirlo, altrimenti non si riceveranno gli eventi tramite il software client. Per i dettagli sul controllo dell'attivazione del dispositivo, fare riferimento a *7.12 Controllo Inserimento.*

Creazione della password

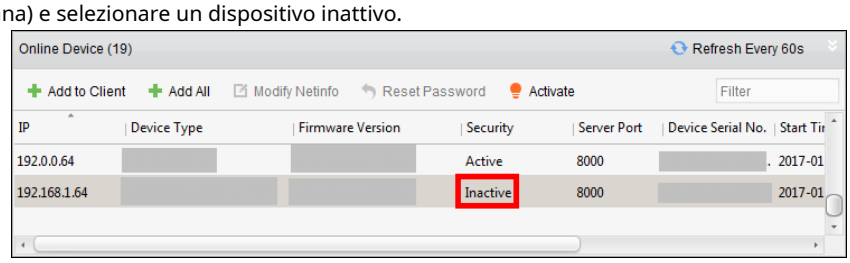
Scopo:

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

Nota: Questa funzione dovrebbe essere supportata dal dispositivo.

Passaggi:

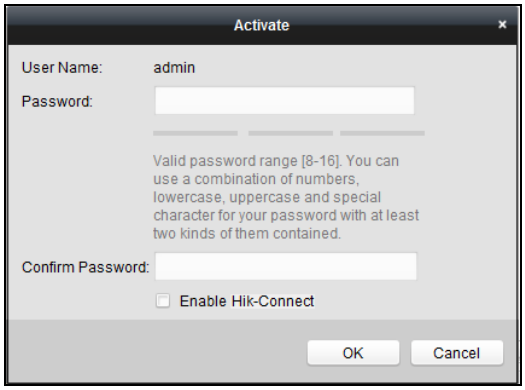
1. Accedere alla pagina Gestione dispositivi.
2. Sul **Dispositivo per la gestione** o **Dispositivo in linea** zona, controllare lo stato del dispositivo (mostrato su **Sicurezza** colonna) e selezionare un dispositivo inattivo.



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

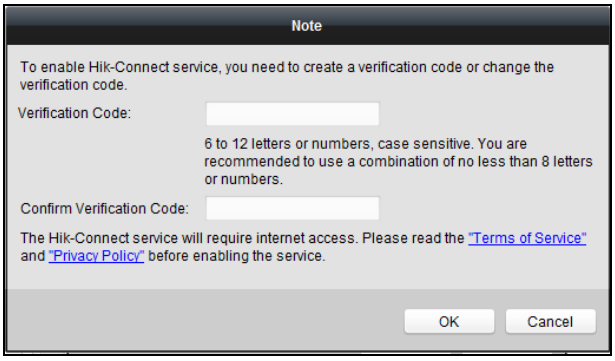
CONSIGLIATA UNA PASSWORD FORTE– *Ti consigliamo vivamente di creare una password sicura di tua scelta (utilizzando un minimo di 8 caratteri, comprese lettere maiuscole, minuscole, numeri e caratteri speciali) per aumentare la sicurezza del prodotto. E ti consigliamo di reimpostare la password regolarmente,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

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



5. (Facoltativo) Abilita il servizio Hik-Connect durante l'attivazione del dispositivo se il dispositivo supporta.

1) Controllare **Abilita Hik-Connect** casella di controllo per far apparire 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. Fare clic su **ok** per attivare il dispositivo.

A "Il dispositivo è attivato". finestra si apre quando la password è impostata con successo.

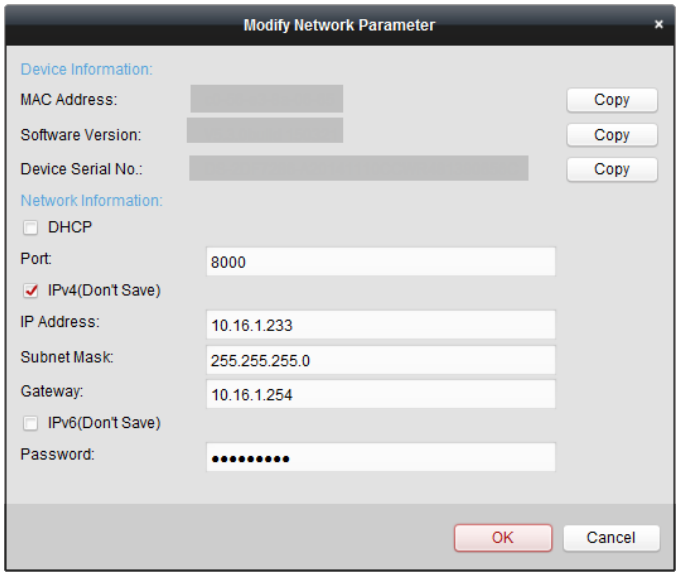
7. Fare clic su **Modifica informazioni di rete** per visualizzare l'interfaccia Modifica parametri di rete.

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

8. Modificare l'indirizzo IP del dispositivo sulla stessa sottorete con il computer modificando il

Indirizzo IP manualmente o selezionando la casella di controllo di DHCP.

9. Immettere la password impostata al passaggio 4 e fare clic su **ok** per completare le impostazioni di rete.

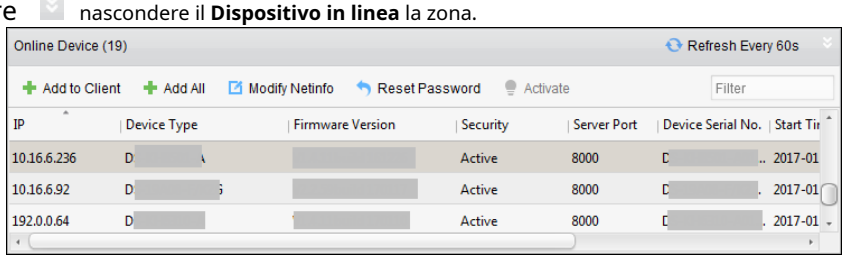


Aggiunta di un dispositivo online

Scopo:

I dispositivi online attivi nella stessa sottorete locale con il software client verranno visualizzati sul **Dispositivo in linea** la zona. Puoi fare clic su**Aggiorna ogni 60s** pulsante per aggiornare le informazioni del dispositivi in linea.

Nota: Puoi cliccare nascondere il **Dispositivo in linea** 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. Fare clic su **Aggiungi al cliente** per aprire la finestra di dialogo per l'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*amministratore.*

Parola d'ordine: Immettere la password del dispositivo.

La sicurezza della password del dispositivo può essere verificata dal software. Per la tua privacy, ti consigliamo vivamente di cambiare la password con qualcosa di tua scelta (usando a

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

4. Facoltativamente, controllare il **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.

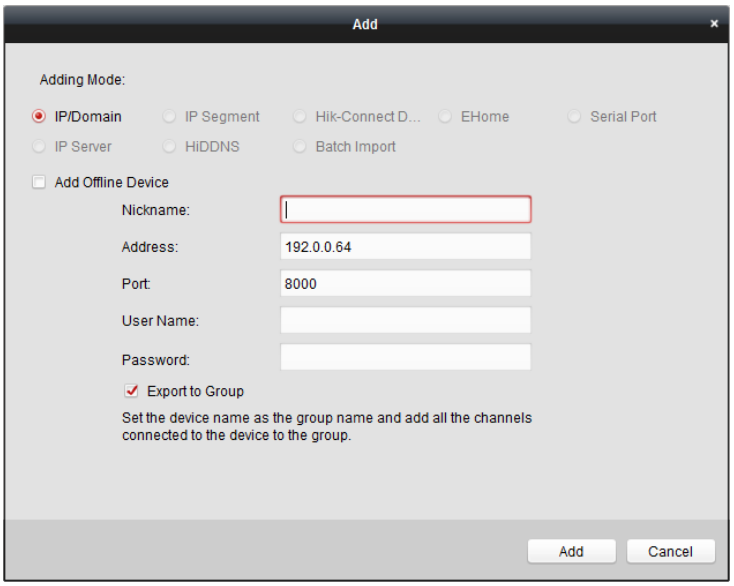
   1) Controllare il **Aggiungi dispositivo offline** casella di controllo.

   2) **io**ninserire le informazioni richieste, compreso il numero del canale del dispositivo e il numero dell'ingresso dell'allarme.

   3) Fare clic su **Inserisci.**

   Quando il dispositivo offline torna online, il software lo collegherà automaticamente.

5. Fare clic su **Inserisci** per aggiungere il dispositivo.

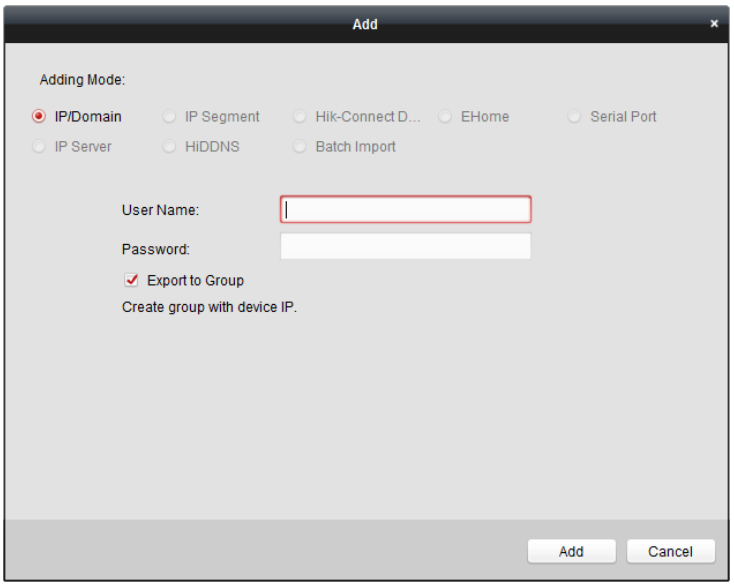


Aggiunta di più dispositivi online

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 per l'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 desideri aggiungere tutti i dispositivi online al software client, fai clic su **Aggiungi tutto** e clicca **ok** nella finestra di messaggio pop-up. Quindi inserire 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 per l'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*amministratore.*

   Parola d'ordine: Immettere la password del dispositivo.

   La sicurezza della password del dispositivo può essere verificata dal software. Per la tua privacy, ti consigliamo vivamente di cambiare la password con una 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 ad alta sicurezza, reimpostare la password mensilmente o settimanalmente può proteggere meglio il tuo prodotto.

4. Facoltativamente, controllare il **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.

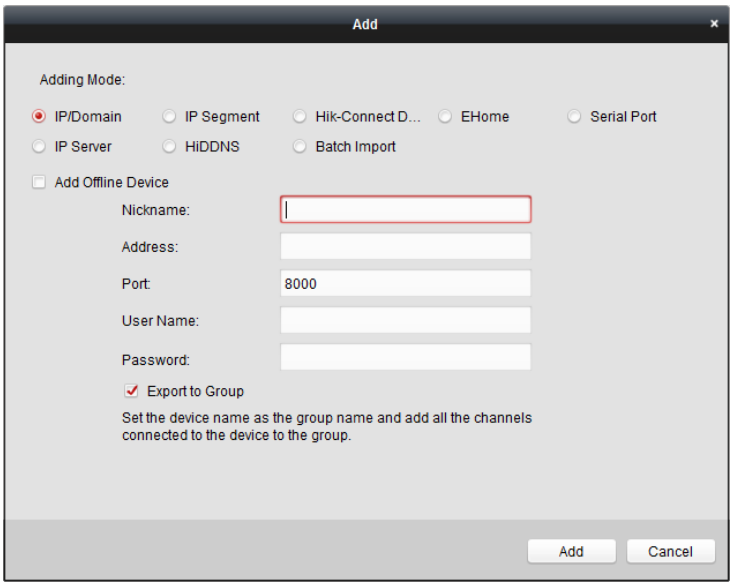
   1) Controllare il **Aggiungi dispositivo offline** casella di controllo.

   2) **io**ninserire le informazioni richieste, compreso il numero del canale del dispositivo e il numero dell'ingresso dell'allarme.

   3) Fare clic su **Inserisci.**

   Quando il dispositivo offline torna online, il software lo collegherà automaticamente.

5. Fare clic su **Inserisci** per aggiungere il dispositivo.



Aggiunta di dispositivi per segmento IP

Passaggi:

1. Fare clic su **Inserisci** per aprire la finestra di dialogo per l'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*amministratore.*

   Parola d'ordine: Immettere la password del dispositivo.

   La sicurezza della password del dispositivo può essere verificata dal software. Per la tua privacy, ti consigliamo vivamente di cambiare la password con una 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 ad alta sicurezza, reimpostare la password mensilmente o settimanalmente può proteggere meglio il tuo prodotto.

4. Facoltativamente, controllare il **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) Controllare il **Aggiungi dispositivo offline** casella di controllo.

   2) **io**ninserire le informazioni richieste, compreso il numero del canale del dispositivo e il numero dell'ingresso dell'allarme.

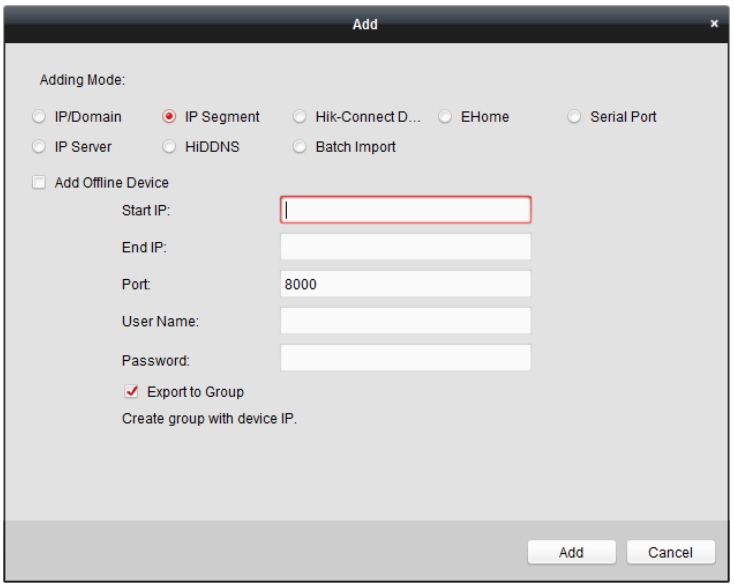
   3) Fare clic su **Inserisci.**

   Quando il dispositivo offline torna online, il software lo collegherà automaticamente.

5. Fare clic su **Inserisci.**

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

elenco.



Aggiunta di dispositivi tramite account EHome

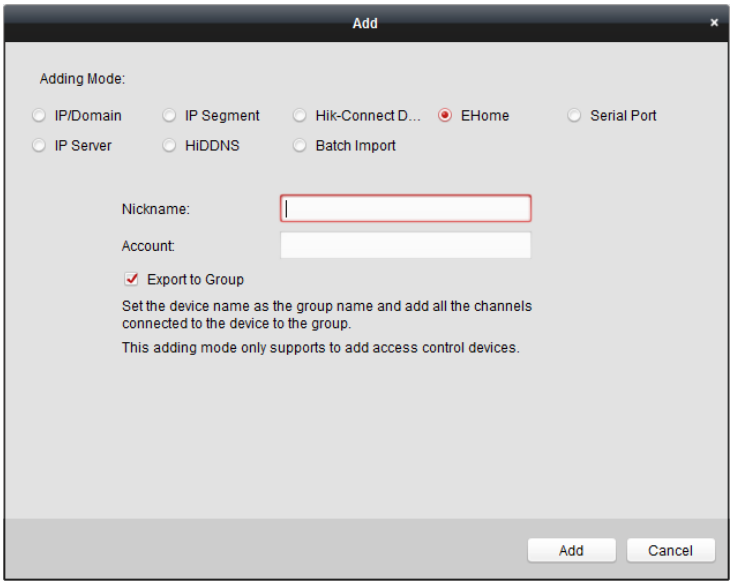
Scopo:

È possibile aggiungere un dispositivo di controllo accessi connesso tramite protocollo EHome inserendo l'account EHome.

Prima che inizi: Impostare prima il parametro del centro di rete. Per i dettagli, fare riferimento a *Capitolo 7.4.4 Impostazioni di rete.*

Passaggi:

1. Fare clic su **Inserisci** per aprire la finestra di dialogo per l'aggiunta del dispositivo.
2. Seleziona **EHome** come modalità di aggiunta.



3. Immettere le informazioni richieste.

   Soprannome: Modifica un nome per il dispositivo come desideri.

   Account: Immettere il nome dell'account registrato sul protocollo EHome.

4. Facoltativamente, controllare il **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) Controllare il **Aggiungi dispositivo offline** casella di controllo.

2) **io**ninserire le informazioni richieste, compreso il numero del canale del dispositivo e il numero dell'ingresso dell'allarme.

3) Fare clic su **Inserisci.**

Quando il dispositivo offline torna online, il software lo collegherà automaticamente.

5. Fare clic su **Inserisci** per aggiungere il dispositivo.

Aggiunta di dispositivi tramite porta seriale

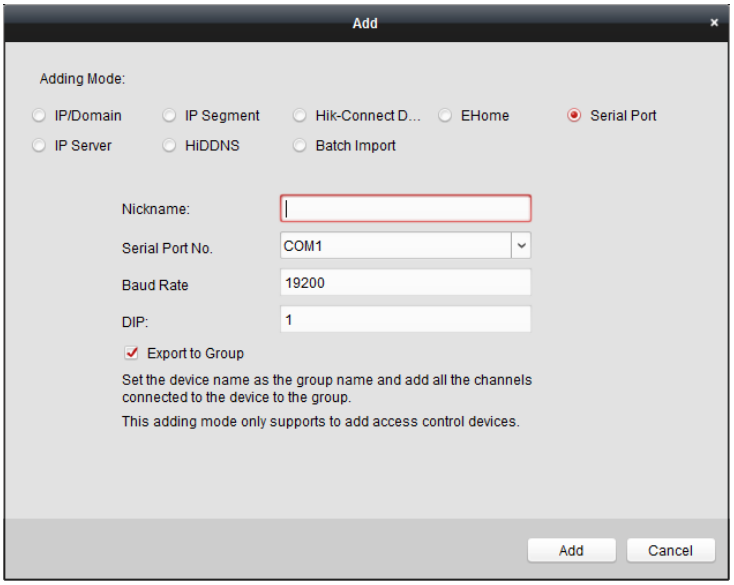
Scopo:

È possibile aggiungere un dispositivo di controllo accessi collegato tramite porta seriale.

Passaggi:

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

2. Seleziona **Porta seriale** come modalità di aggiunta.



3. Immettere le informazioni richieste.

Soprannome: Modifica un nome per il dispositivo come desideri.

Numero porta seriale: Selezionare la porta seriale connessa del dispositivo n.

Velocità di trasmissione: Immettere la velocità di trasmissione del dispositivo di controllo accessi.

TUFFO: Immettere l'indirizzo DIP del dispositivo.

4. Facoltativamente, controllare il **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) Controllare il **Aggiungi dispositivo offline** casella di controllo.

2) **io**ninserire le informazioni richieste, compreso il numero del canale del dispositivo e il numero dell'ingresso dell'allarme.

3) Fare clic su **Inserisci.**

Quando il dispositivo offline torna online, il software lo collegherà automaticamente.

5. Fare clic su **Inserisci** per aggiungere il dispositivo.

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** pulsante per visualizzarne lo stato.

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

Stato della porta: Lo stato della porta collegata.

Stato dell'ospite: Lo stato dell'host, tra cui la tensione di alimentazione della batteria di archiviazione, lo stato dell'alimentazione del dispositivo, lo stato di interblocco multi-porta, lo stato di anti-rientro e lo stato di antimanomissione 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 carte con connessione Wiegand, puoi visualizzare lo stato di offline.

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

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

Stato del sensore di evento: Lo stato del sensore 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 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 Impostazioni di rete

Scopo:

Dopo aver aggiunto il dispositivo di controllo dell'accesso, è possibile impostare la modalità di caricamento e impostare la rete

centrale e centro di comunicazione wireless. Selezionare il dispositivo nell'elenco dei dispositivi e fare clic su**Modificare** per visualizzare la finestra di modifica delle informazioni sul dispositivo.

Clic **Impostazioni di rete** scheda per accedere all'interfaccia delle impostazioni di rete.

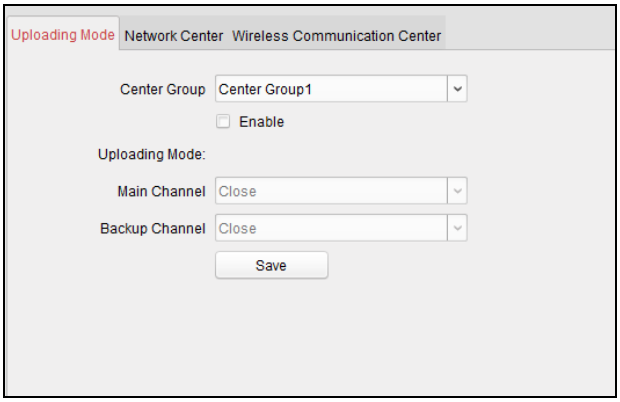
Impostazioni della modalità di caricamento

Scopo:

È possibile impostare il gruppo centrale per il caricamento del registro tramite il protocollo EHome.

Passaggi:

1. Fare clic su **Modalità di caricamento** scheda.



2. Selezionare il gruppo centrale nell'elenco a discesa.
3. Controlla il **Abilitare** casella di controllo per abilitare il gruppo centrale selezionato.
4. Selezionare la modalità di caricamento nell'elenco a discesa. Puoi abilitare**N1/G1** per il canale principale e il canale di backup, oppure selezionare **Vicino** per disabilitare il canale principale o il canale di backup.

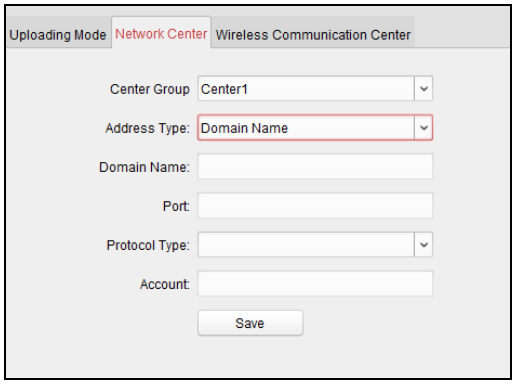
   Nota: Il canale principale e il canale di backup non possono abilitare contemporaneamente N1 o G1.
5. Fare clic su **Salva** pulsante per salvare i parametri.

Impostazioni del centro di rete

È possibile impostare l'account per il protocollo EHome nella pagina Impostazioni di rete. Quindi puoi aggiungere dispositivi tramite il protocollo EHome.

Passaggi:

1. Fare clic su **Centro di rete** scheda.



2. Selezionare il gruppo centrale nell'elenco a discesa.
3. Selezionare il tipo di indirizzo.

4. Impostare l'indirizzo IP/nome di dominio.

5. Impostare il numero di porta per il protocollo EHome. Per impostazione predefinita, il numero di porta è 7660.

6. Selezionare il tipo di protocollo come EHome.

7. Impostare un nome account per il centro di rete.

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

Appunti:

L'account deve contenere da 1 a 32 caratteri e sono consentiti solo lettere e numeri.

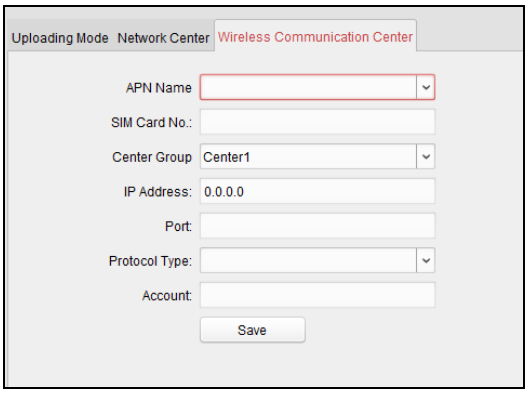
Il numero di porta della rete wireless e della rete cablata deve essere coerente con il numero di porta di EHome.

Puoi impostare il nome di dominio nell'area Abilita NTP *Tempo* sezione in Configurazione remota. Per i dettagli, fare riferimento a *Tempo* nel *7.4.7 Configurazione remota.*

Impostazioni del centro di comunicazione wireless

Passaggi:

1. Fare clic su **Centro di comunicazione wireless** scheda.



2. Selezionare il nome APN come CMNET o UNINET.

3. Immettere il numero della carta SIM.

4. Selezionare il gruppo centrale nell'elenco a discesa.

5. Immettere l'indirizzo IP e il numero di porta.

6. Selezionare il tipo di protocollo come EHome. Per impostazione predefinita, il numero di porta per EHome è 7660.

7. Impostare un nome account per il centro di rete. Un account coerente dovrebbe essere utilizzato in un'unica piattaforma.

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

Nota: Il numero di porta della rete wireless e della rete cablata deve essere coerente con il numero di porta di EHome.

7.4.5 Impostazioni RS-485

Scopo:

È possibile impostare i parametri RS-485 tra cui la porta seriale, il baud rate, il bit di dati, il bit di stop, il tipo di parità, la modalità di comunicazione e la modalità di lavoro.

Selezionare il dispositivo nell'elenco dei dispositivi e fare clic su **Modificare** per visualizzare le informazioni sul dispositivo di modifica

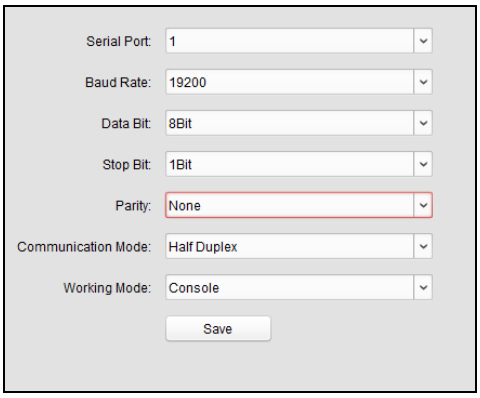
finestra.

Clic **Impostazioni RS-485** scheda per accedere all'interfaccia delle impostazioni RS-485.

Nota: Le impostazioni RS-485 dovrebbero essere supportate dal dispositivo.

Passaggi:

1. Fare clic su **Impostazioni RS-485** scheda per accedere all'interfaccia delle impostazioni RS-485.



2. Selezionare il numero di serie della porta dall'elenco a discesa per impostare i parametri RS-485.
3. Impostare la velocità di trasmissione, il bit di dati, il bit di stop, il tipo di parità, la modalità di comunicazione e la modalità di lavoro nell'elenco a discesa.
4. Clic **Salva** per salvare le impostazioni e i parametri configurati verranno applicati automaticamente al dispositivo.

Nota: Dopo aver modificato la modalità di lavoro, il dispositivo verrà riavviato. Dopo aver cambiato la modalità di lavoro, verrà visualizzato un messaggio.

7.4.6 Crittografia della scheda M1

La funzione M1 Card Encryption aumenta il livello di sicurezza dell'autenticazione, che dovrebbe essere applicato insieme alla stazione di registrazione delle carte della nostra azienda tramite il software client o il client web. Dopo aver emesso la carta, è possibile impostare la funzione di crittografia della carta M1 sul controller.

Appunti:

La funzione dovrebbe essere supportata dal dispositivo.

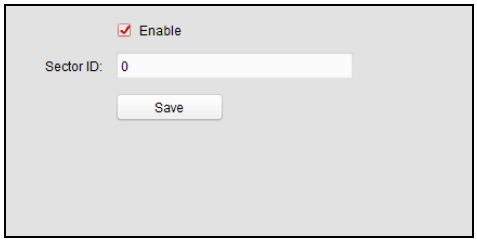
Per i dettagli sull'emissione della carta, fare riferimento a *Aggiunta di persone (carta)* nel *7.5.2 Gestione delle persone.*

Selezionare il dispositivo nell'elenco dei dispositivi e fare clic su **Modificare** per visualizzare la finestra di modifica delle informazioni sul dispositivo.

Clic **Crittografia della scheda M1** scheda per accedere all'interfaccia M1 Card Encryption.

Passaggi:

1. Nell'interfaccia M1 Card Encryption, selezionare **Abilitare** casella di controllo per abilitare la crittografia della scheda M1 funzione.



2. Impostare l'ID del settore.

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

Nota: L'ID del settore va da 1 a 100. Selezionare i settori appropriati in base al tipo di carta.

7.4.7 Configurazione remota

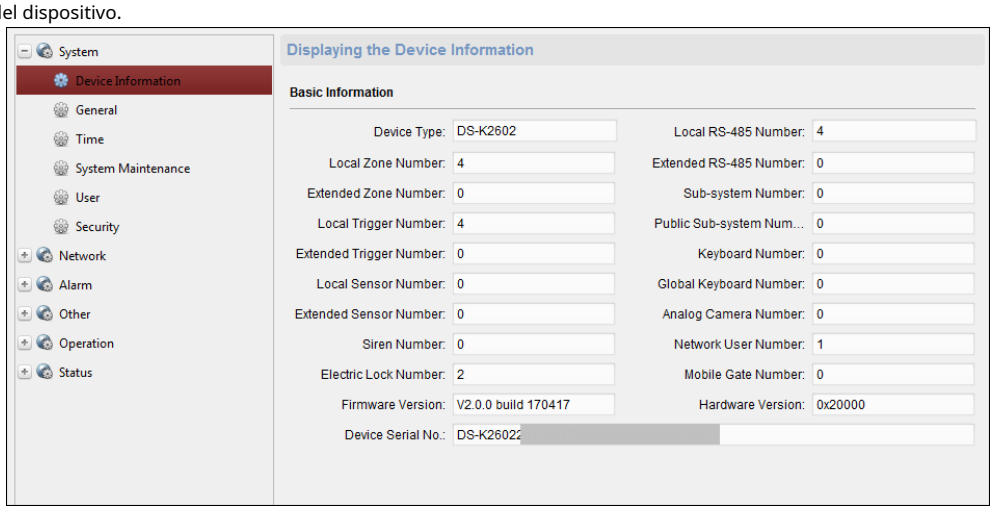
Scopo:

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

Controllo delle informazioni sul dispositivo

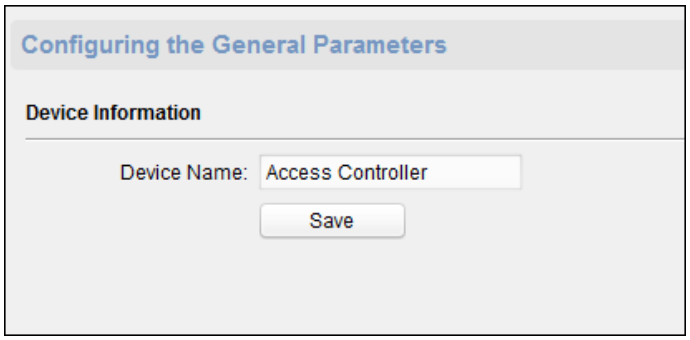
Passaggi:

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



Modifica del nome del dispositivo

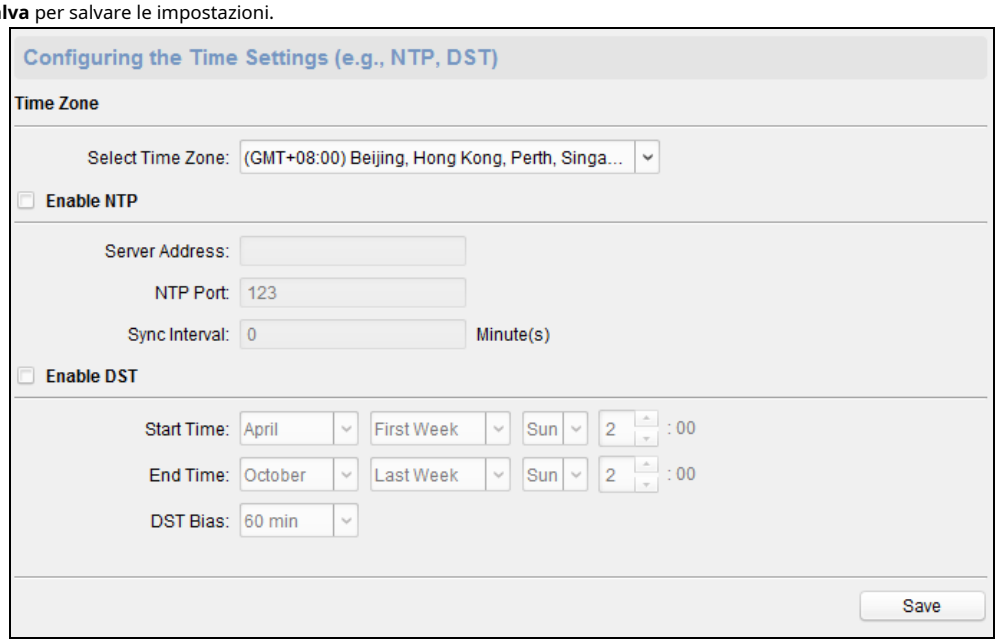
Nell'interfaccia di Configurazione remota, fare clic su **Sistema -> Generale** per configurare il nome del dispositivo. Clic **Salva** per salvare le impostazioni.



Tempo di modifica

Passaggi:

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



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 clicca**Ripristina le impostazioni di default** per ripristinare le impostazioni del dispositivo a quelle di default, escluso l'indirizzo IP.

   Oppure clicca **Ripristinare tutto** per ripristinare i parametri del dispositivo a quelli di default. Il dispositivo dovrebbe essere attivato dopo il ripristino.

   Nota: Il file di configurazione contiene i parametri del dispositivo.
3. Puoi anche aggiornare il dispositivo in remoto.

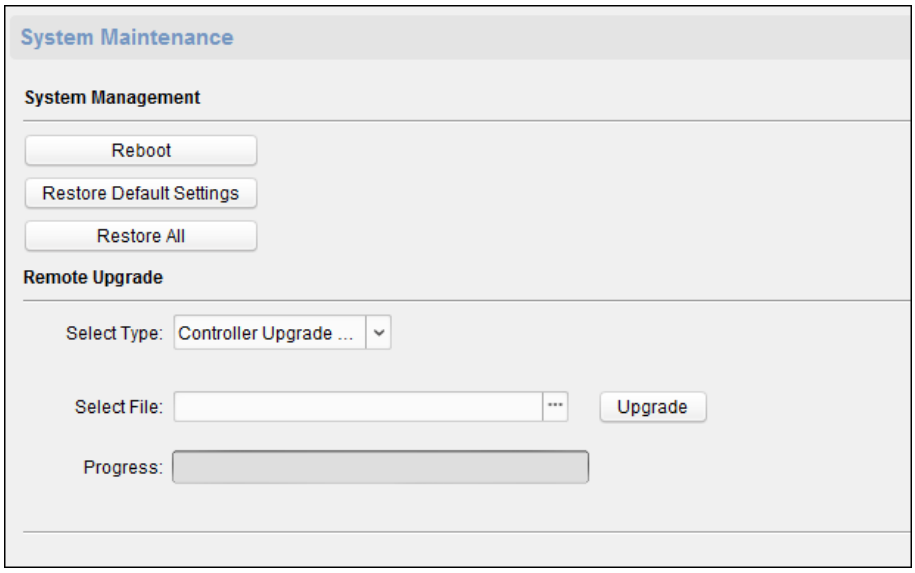
   1) Nella parte Aggiornamento remoto, selezionare un tipo di file di aggiornamento nell'elenco a discesa.

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

   2) Fare clic per selezionare il file di aggiornamento.

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

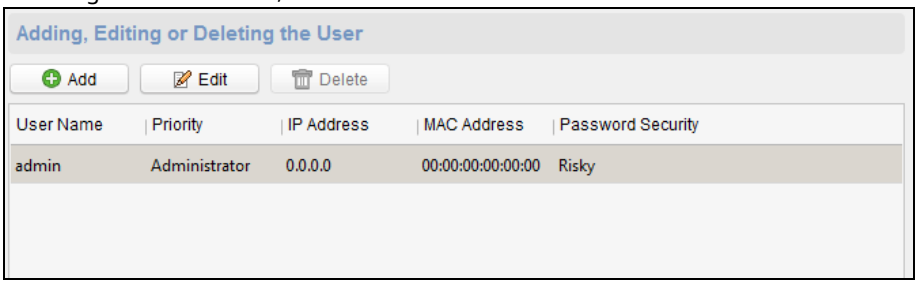
      Nota: È possibile aggiornare solo i lettori di schede collegati tramite RS-485.



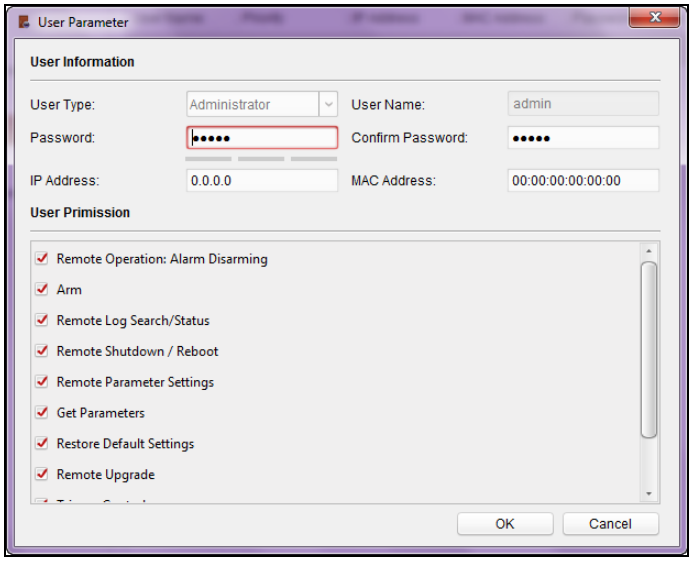
Gestione dell'utente

Passaggi:

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



2. Fare clic su **Inserisci** per aggiungere l'utente (non supportato dal controller dell'ascensore). Oppure seleziona un utente nell'elenco degli utenti e fai 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. clic**ok** per confermare la modifica.



Impostazione della sicurezza

Passaggi:

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

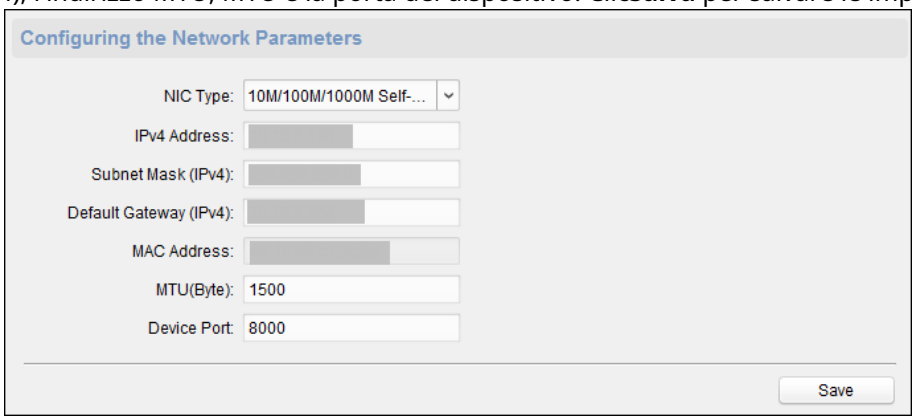
2. Selezionare la modalità di crittografia nell'elenco a discesa.

   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.



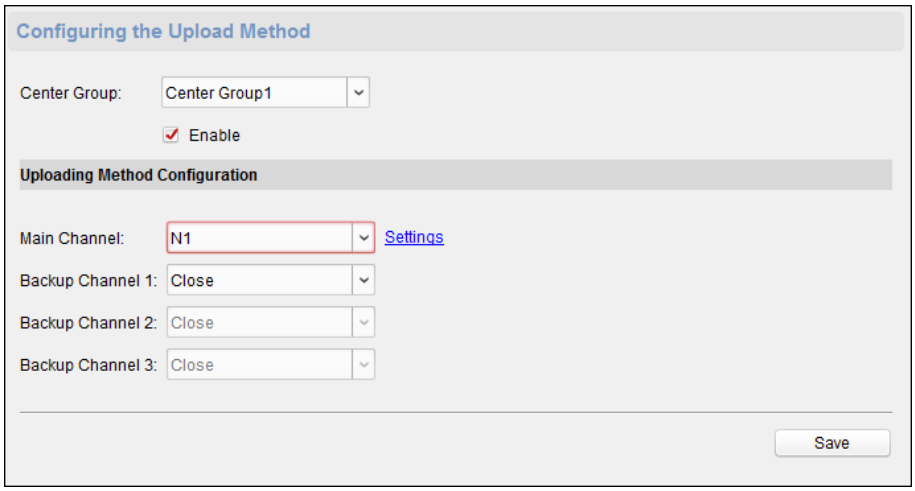
Configurazione del metodo di caricamento

Scopo:

È possibile impostare il gruppo centrale per il caricamento del registro tramite il protocollo EHome.

Passaggi:

1. Fare clic su **Rete -> Strategia di report.**



2. Selezionare un gruppo di centri dall'elenco a discesa.

3. Controlla il **Abilitare** casella di controllo.

4. Imposta il metodo di caricamento.

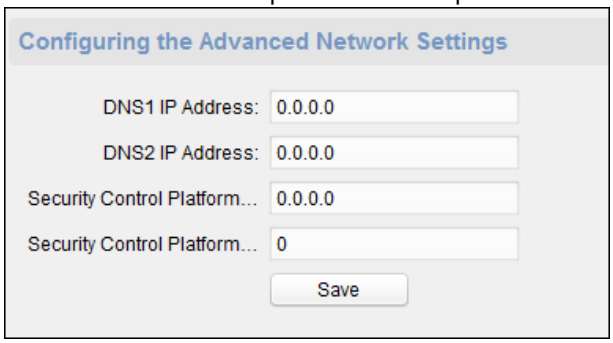
   È possibile impostare il canale principale e il canale di backup.

5. Fare clic su **impostazioni** a destra del campo del canale per impostare le informazioni dettagliate.

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

Configurazione della rete avanzata

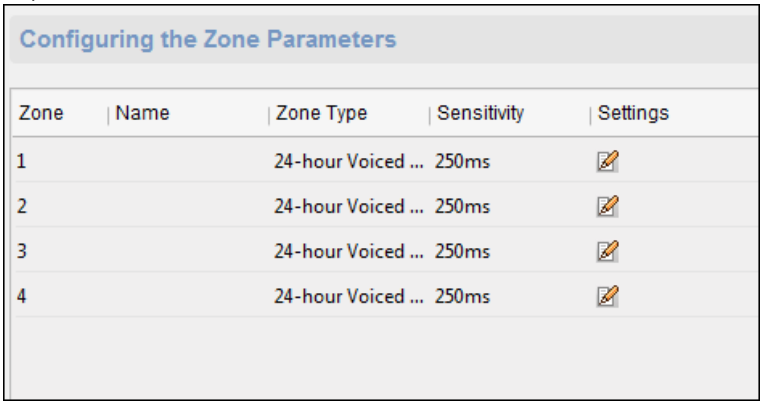
Clic **Rete -> Impostazioni avanzate.** È possibile configurare l'indirizzo DNS 1, l'indirizzo DNS 2, l'IP dell'host dell'allarme e la porta dell'host dell'allarme. Clic**Salva** per salvare le impostazioni.



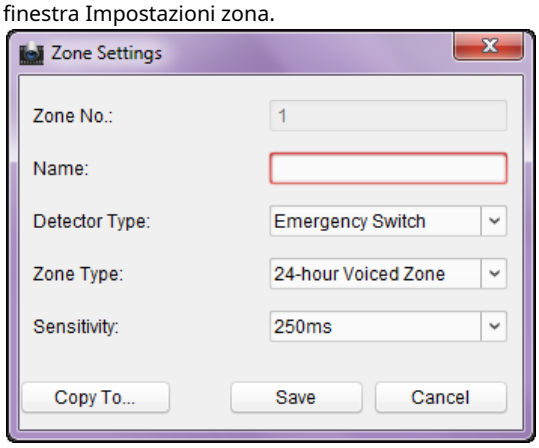
Configurazione dei parametri di zona

Passo:

1. Fare clic su **Allarme -> Zona** per accedere all'interfaccia di zona.



2. Fare clic su per far apparire la finestra Impostazioni zona.



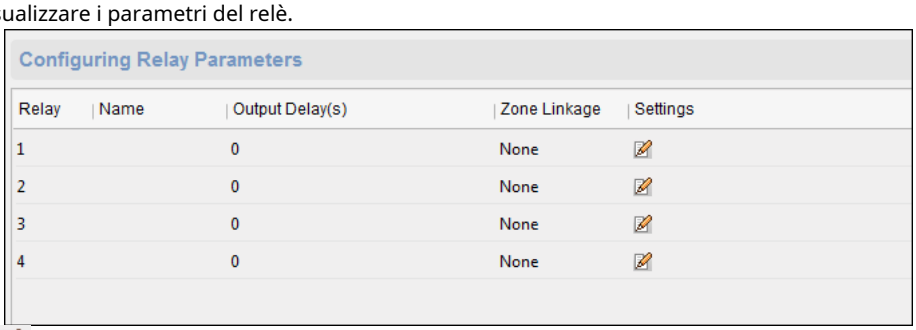
3. Impostare il nome della zona, il tipo di rilevatore, il tipo di zona e la sensibilità.
4. Fare clic su **Salva** per salvare le impostazioni. Oppure clicca**Copia a...** per copiare i parametri in altre zone.

Configurazione dei parametri del relè

Passaggi:

1. Fare clic su **Allarme -> Relè.**

   È possibile visualizzare i parametri del relè.



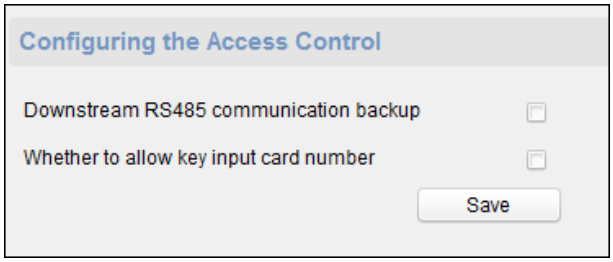
2. Fare clic su per far apparire la finestra Impostazioni parametri relè.
3. Impostare il nome del relè e il ritardo dell'uscita.
4. Fare clic su **Salva** per salvare i parametri. Oppure clicca**Copia a...** per copiare le informazioni del relè su altri relè.

Configurazione dei parametri di controllo degli accessi

Passaggi:

1. Nell'interfaccia di Configurazione remota, fare clic su **Altro -> Parametri di controllo dell'accesso.**
2. Selezionare e controllare il **Backup della comunicazione RS-485 downstream** casella di controllo o il **Premere il tasto per inserire la scheda n.** casella di controllo.

   Nota: Se si utilizza l'interfaccia RS-485B, è necessario controllare il backup della comunicazione RS-485 downstream. Per i dettagli sul cablaggio dei cavi, vedere*4.1 Terminale esterno.*
3. Fare clic su **Salva** per salvare le impostazioni.

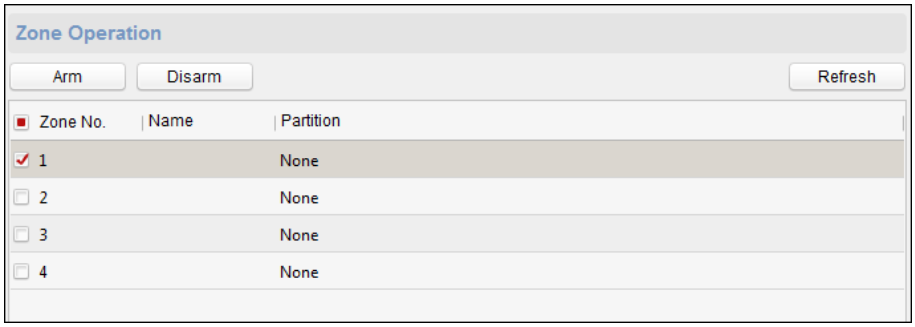


Zona operativa

Passaggi:

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

   È possibile visualizzare le informazioni sulla zona.



2. Selezionare la casella di controllo della zona.

3. Fare clic su **Braccio** o **Disarmare** per inserire o disinserire la zona.

4. (Facoltativo) fare clic su **ricaricare** per aggiornare lo stato della zona.

Relè di funzionamento

Passaggi:

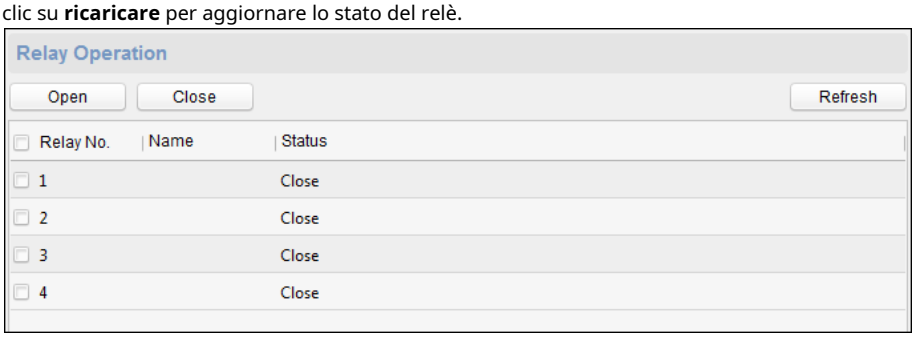
1. Fare clic su **Operazione -> Relè.**

   È possibile visualizzare lo stato del relè.

2. Seleziona la casella di controllo del relè

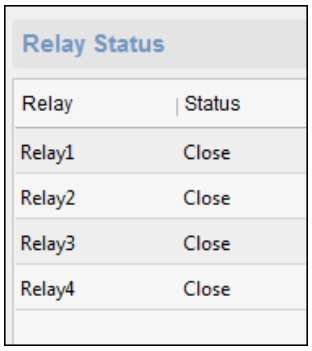
3. Fare clic su **Aperto** o **Vicino** per aprire/chiudere il relè.

4. (Facoltativo) Fare clic su **ricaricare** per aggiornare lo stato del relè.



Visualizzazione dello stato del relè

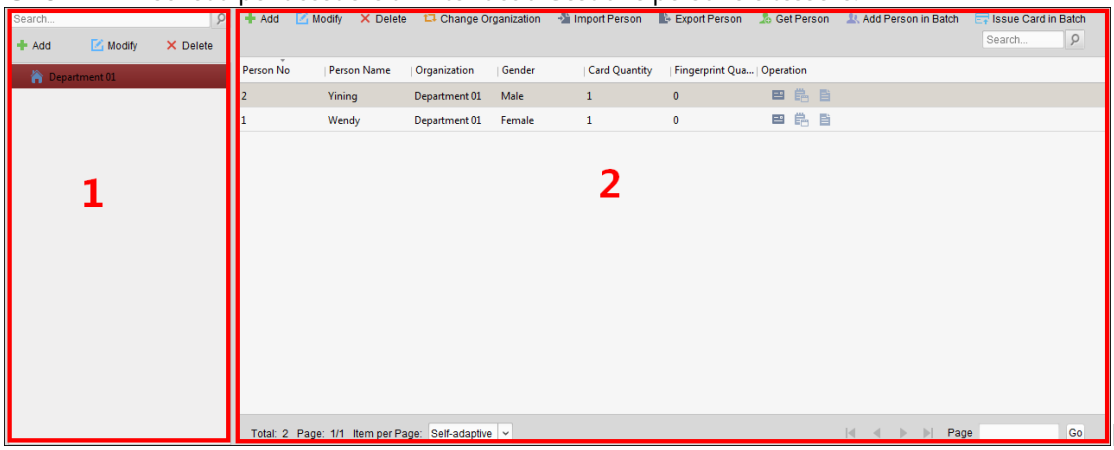
Clic **Stato -> Relè** per visualizzare lo stato del relè.



7.5 Gestione della persona e della carta

Puoi aggiungere, modificare ed eliminare l'organizzazione e la persona in Gestione persone e carte modulo.

Clic scheda per accedere all'interfaccia Gestione persone e tessere.



L'interfaccia è diviso in due parti: Gestione dell'Organizzazione e Gestione della Persona.

1	**Organizzazione Gestione**	Puoi aggiungere, modificare o eliminare l'organizzazione come desideri.
2	**Gestione della persona**	Dopo aver aggiunto l'organizzazione, è possibile aggiungere la persona all'organizzazione ed emettere la tessera alle persone per un'ulteriore gestione.

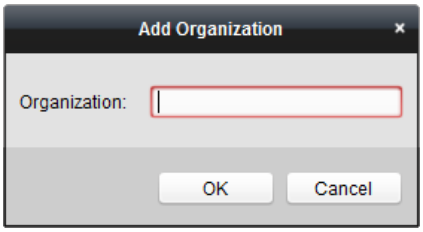
7.5.1 Gestione dell'organizzazione

Aggiunta di organizzazione

Passaggi:

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

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



2. Immettere il nome dell'organizzazione come desiderato.

3. Fare clic su **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 l'organizzazione secondaria.

Quindi l'organizzazione aggiunta sarà l'organizzazione secondaria 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. Puoi selezionare un'organizzazione e fare clic su**Elimina** pulsante per eliminarlo.

Appunti:

Se elimini un'organizzazione, verranno eliminate anche le organizzazioni di livello inferiore.

Assicurati che non sia stata aggiunta alcuna persona all'interno dell'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, ad esempio l'emissione di carte in batch, l'importazione e l'esportazione di informazioni sulle persone in batch, ecc.

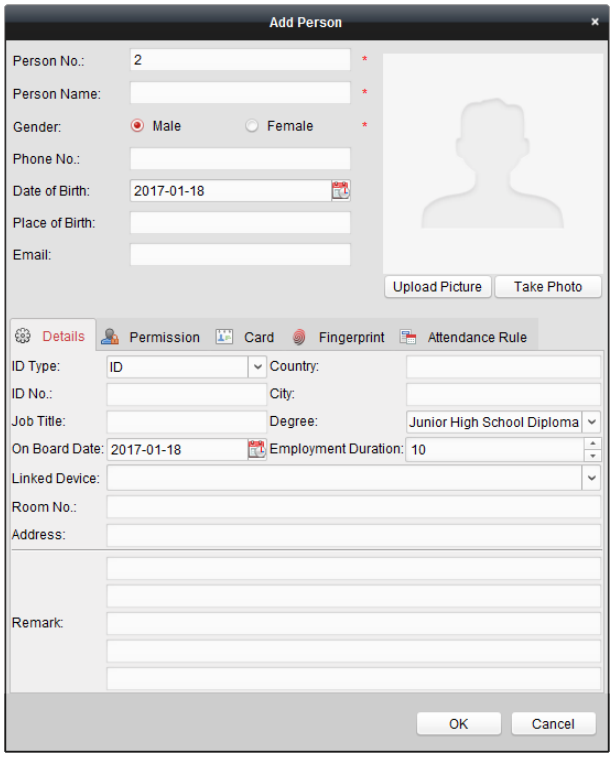
Nota: È possibile aggiungere fino a 10.000 persone o tessere.

Aggiunta di persona

Aggiunta di una persona (informazioni di base)

Passaggi:

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



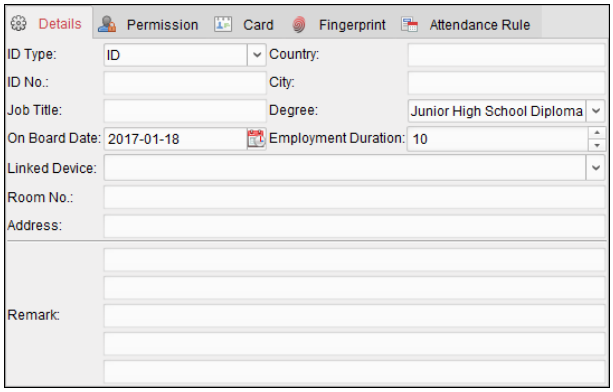
2. Il numero di persona verrà generato automaticamente e non è modificabile.
3. Immettere le informazioni di base tra cui nome della persona, sesso, numero di telefono, dettagli della data di nascita e indirizzo e-mail.
4. Fare clic su **Carica l'immagine** per selezionare l'immagine della persona dal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

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

Aggiunta di una persona (informazioni dettagliate)

Passaggi:

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



2. Immettere le informazioni dettagliate della persona, compreso il tipo di ID della persona, il numero di ID, il paese, ecc., in base alle effettive esigenze.

   Dispositivo collegato: È possibile associare il posto interno alla persona.

   Nota: Se selezioni **Postazione interna analogica** nel dispositivo collegato, il **Stazione della porta** 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 di camera della persona.

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

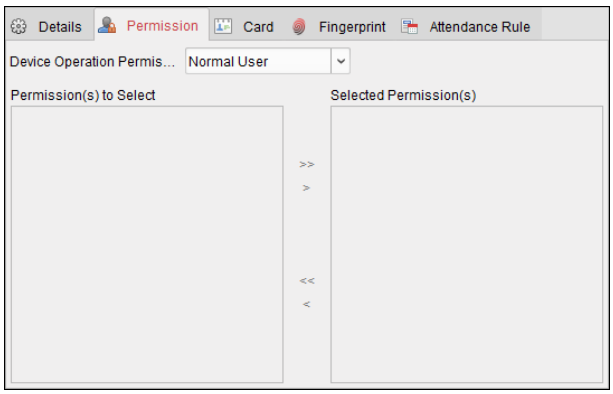
Aggiunta di una persona (autorizzazione)

È possibile assegnare le autorizzazioni (incluse le autorizzazioni operative 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 dei permessi.*

Passaggi:

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



2. Nel campo Ruolo operazione dispositivo, selezionare il ruolo di azionamento del dispositivo di controllo accessi.

Utente normale: La persona ha il permesso di effettuare il check-in/out sul dispositivo, superare il punto di controllo degli accessi, ecc.

Amministratore: La persona ha l'autorizzazione utente normale, nonché l'autorizzazione per configurare il dispositivo, inclusa l'aggiunta di 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 aggiungere all'elenco Autorizzazioni selezionate. (Facoltativo) È possibile fare clic su >> per aggiungere tutte le autorizzazioni visualizzate all'elenco 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.

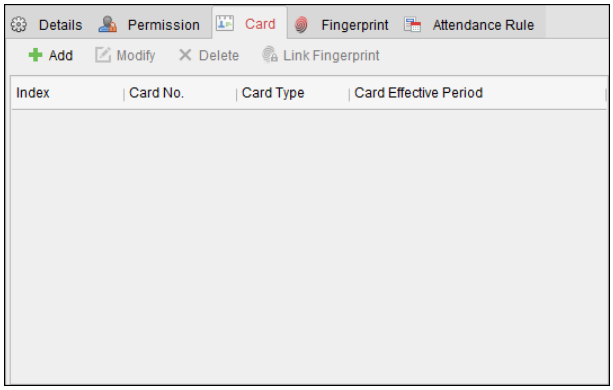
4. Fare clic su **ok** per salvare le impostazioni.

Aggiunta di persone (carta)

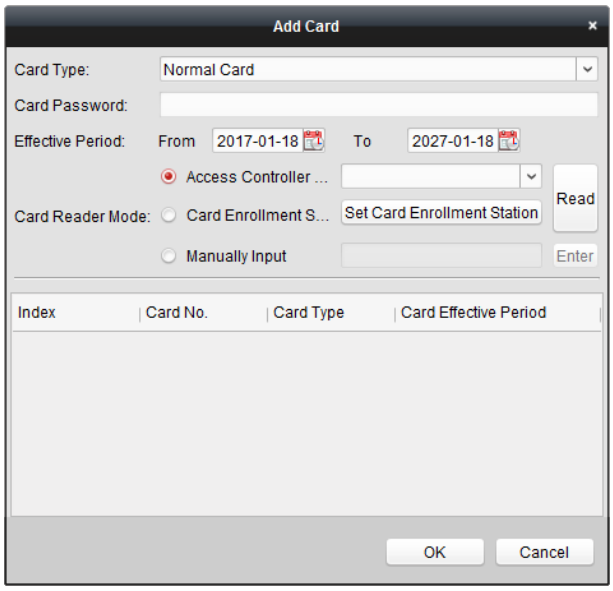
Puoi aggiungere la carta ed emettere la carta alla persona.

Passaggi:

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



2. Fare clic su **Inserisci** per far apparire la finestra di dialogo Aggiungi carta.



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

Carta normale

Tessera per Disabili: La porta rimarrà aperta per il periodo di tempo configurato per il titolare della carta.

Carta nella lista nera: L'azione di scorrimento della carta verrà caricata e la porta non potrà essere aperta.

Carta di pattuglia: L'azione di scorrimento della carta può essere utilizzata per verificare lo stato di lavoro del personale di controllo. Il permesso di accesso del personale ispettivo è configurabile.

Carta coercizione: La porta può essere aperta facendo scorrere la carta coercizione quando c'è coercizione. Allo stesso tempo, il cliente può segnalare l'evento di coercizione.

Supercarta: La tessera è valida per tutte le porte del controllore durante la programmazione configurata.

Biglietto da visita: La tessera è assegnata ai visitatori. Per la Visitor Card è possibile impostare il**massimo Tempi di scorrimento.**

Appunti:

Il massimo 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 su 0, significa che lo scorrimento della carta è illimitato.

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

Nota: La password sarà richiesta quando il titolare della carta scorrerà la carta per entrare o uscire dalla porta se si abilita la modalità di autenticazione del lettore di carte come **Carta e password, password e impronte digitali,** e **Carta, password e impronte digitali.** Per dettagli, *Capitolo 7.8.2 Autenticazione del lettore di schede.*

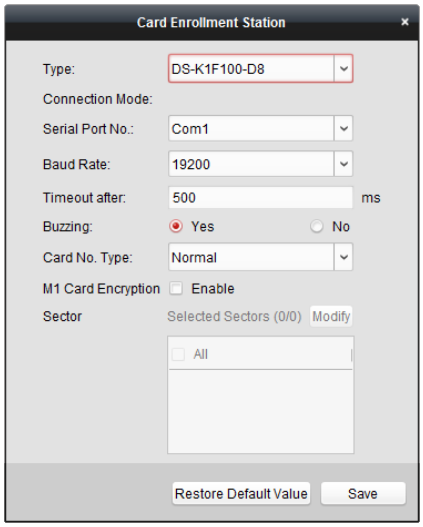
5. Fare clic per impostare l'ora effettiva e l'ora di scadenza della carta.

6. Selezionare la modalità Card Reader per leggere la carta n.

Lettore controller di accesso: Posizionare la tessera sul lettore del Controller di Accesso e cliccare **Leggere** per ricevere la tessera n.

Stazione di registrazione della carta: Posiziona la carta sulla stazione di registrazione della carta e fai clic su **Leggere** per ricevere la tessera n.

Nota: La Card Enrollment Station dovrebbe connettersi con il PC che esegue il client. Puoi cliccare**Imposta stazione di registrazione della carta** per accedere alla seguente finestra di dialogo.



2) Selezionare il tipo di stazione di registrazione della tessera.

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, il baud rate, il valore di timeout, il ronzio o il tipo di numero di scheda.

Se la scheda è una scheda M1 e se è necessario abilitare la funzione di crittografia della scheda M1, è necessario controllare **Abilitare** casella di controllo di M1 Card Encryption e fare clic su **Modificare** per selezionare il settore.

4) Fare clic su **Salva** pulsante per salvare le impostazioni. Puoi cliccare**Ripristina valore predefinito** pulsante per ripristinare le impostazioni predefinite.

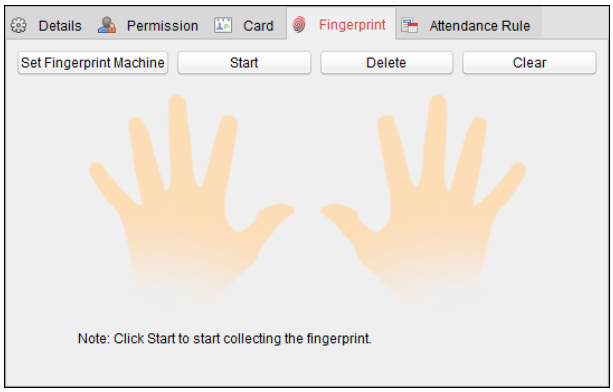
Inserimento manuale: Inserisci il numero della carta e clicca **accedere** per inserire la carta n.

7. Fare clic su **ok** e la/e carta/e saranno 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. (Facoltativo) Puoi fare clic su **Collega l'impronta digitale** per collegare la carta con l'impronta digitale della persona, in modo che la persona possa posizionare il dito sullo scanner invece di strisciare la carta quando passa la porta.
10. Fare clic su **ok** per salvare le impostazioni.

Aggiunta di una persona (impronta digitale)

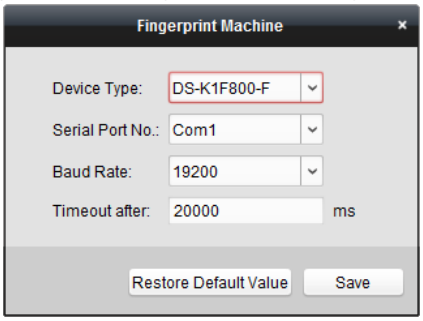
Passaggi:

1. Nell'interfaccia Aggiungi persona, fare clic su **impronta digitale** scheda.



2. Prima di inserire l'impronta digitale, è necessario collegare la macchina per impronte digitali al PC e impostare prima i suoi parametri.

   Clic **Imposta macchina per impronte digitali** per accedere alla seguente finestra di dialogo.



   1) Selezionare il tipo di dispositivo.

      Attualmente, i tipi di macchine per impronte digitali supportati includono DS-K1F800-F, DS-K1F300-F e DS-K1F810-F.

   2) Per il tipo di macchina per impronte digitali DS-K1F800-F, è possibile impostare il numero di porta seriale, velocità di trasmissione e parametri straordinari della macchina per impronte digitali.

   3) Fare clic su **Salva** pulsante per salvare le impostazioni. Puoi cliccare**Ripristina valore predefinito** pulsante per ripristinare le impostazioni predefinite.

   Appunti:

   Il numero della porta seriale deve corrispondere al numero della porta seriale del PC. Puoi controllare il numero della porta seriale in Gestione dispositivi nel tuo PC.

   La velocità di trasmissione dovrebbe essere impostata in base al lettore di schede di impronte digitali esterno. Il valore predefinito è 19200.

   Timeout dopo il campo si riferisce al tempo di rilevamento dell'impronta digitale valido. Se l'utente non inserisce un'impronta digitale o inserisce un'impronta digitale senza successo, il dispositivo indicherà che la raccolta delle impronte digitali è terminata.

3. Fare clic su **Inizio** pulsante, fare clic per selezionare l'impronta digitale per iniziare a raccogliere.
4. Sollevare e appoggiare due volte l'impronta digitale corrispondente sullo scanner di impronte digitali per raccogliere l'impronta digitale sul client.
5. Fare clic su **Fermare** il pulsante può interrompere la raccolta. Puoi anche fare clic su**Raccogli dal dispositivo** pulsante e selezionare il dispositivo per raccogliere l'impronta digitale. (La funzione dovrebbe essere supportata dal dispositivo.

6. Dopo aver raccolto l'impronta digitale, fare clic su Tessera nella finestra Aggiungi persona per accedere alla scheda Tessera.

7. Fare clic su **Collega l'impronta digitale** per collegare l'impronta digitale alla carta. È possibile selezionare l'impronta digitale registrata e fare clic su**Elimina** per eliminarlo. Puoi cliccare**Chiaro** per cancellare tutte le impronte digitali.
8. Fare clic su **ok** per salvare le impronte digitali.

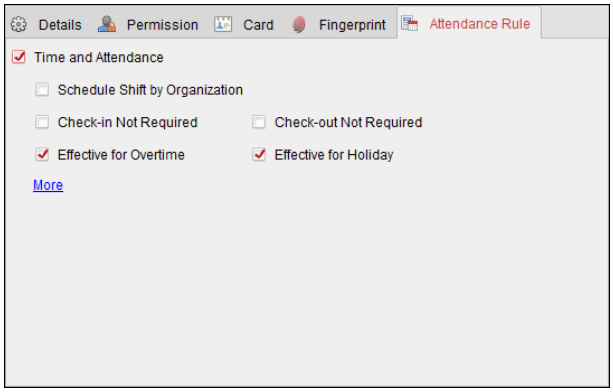
Aggiunta di persone (regola della presenza)

È possibile impostare la regola di presenza per la persona.

Nota: Questa scheda verrà visualizzata quando si seleziona you **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** scheda.



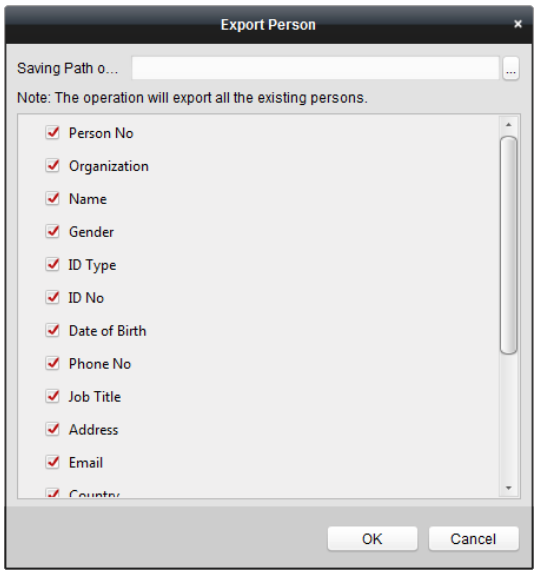
2. Se la persona si unisce nel tempo e presenze, controllare il **Orario e presenze** casella di controllo per abilitare questa funzione per la persona. Quindi i record di scorrimento della carta della persona verranno registrati e analizzati per tempo e presenze.
   Per i dettagli su Orario e Presenze, fare clic su **Di più** per andare al modulo Orario e Presenze.
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:

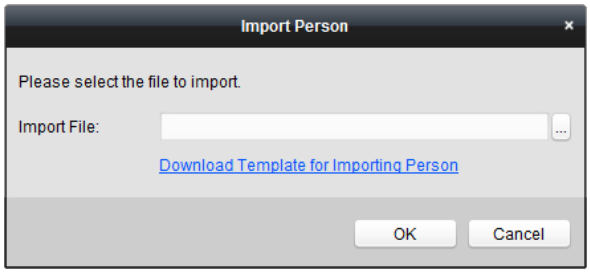
1. **Persona esportatrice:** Puoi esportare le informazioni delle persone aggiunte in formato Excel nel locale PC.
   1) Dopo aver aggiunto la persona, puoi fare clic su **Esporta persona** nella scheda Persona e tessera per far apparire la seguente finestra di dialogo.
   2) Fare clic per selezionare il percorso di salvataggio del file Excel esportato.
   3) Spuntare le caselle di controllo per selezionare le informazioni sulla persona da esportare.



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

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

1) clicca **Importa persona** pulsante nella scheda Persona e tessera.



2) Puoi cliccare **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 per selezionare il file Excel con le informazioni sulla persona.

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

Ottenere informazioni sulla persona dal dispositivo di controllo degli accessi

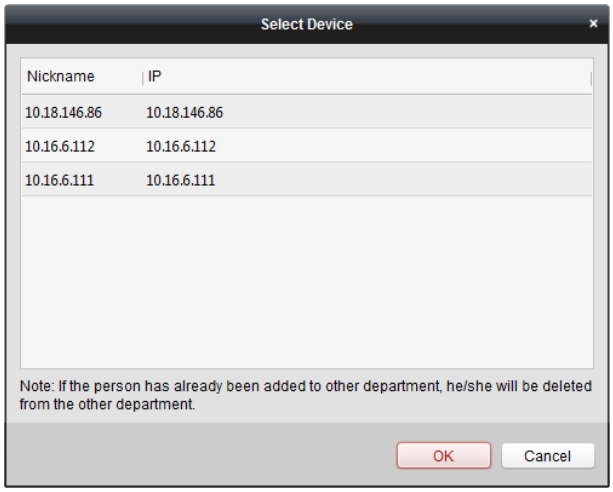
Se il dispositivo di controllo dell'accesso aggiunto è stato configurato con le informazioni sulla persona (inclusi i dettagli della persona, l'impronta digitale, le informazioni sulla carta emessa), è possibile ottenere le informazioni sulla persona dal dispositivo e importarle nel client per ulteriori 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** pulsante per far apparire la seguente finestra di dialogo.



3. Verrà visualizzato il dispositivo di controllo accessi aggiunto.

4. Fare clic per selezionare il dispositivo, quindi fare clic su **ok** 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 sulle impronte digitali 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 nome della persona emesso carta n. 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 dirigente

Modifica ed eliminazione di una persona

Per modificare le informazioni sulla persona e la regola di presenza, fare clic su o nella colonna Operazione, oppure seleziona la persona e clicca **Modificare** per aprire la finestra di modifica della persona.

Puoi fare clic per visualizzare i record di scorrimento della carta della persona.

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

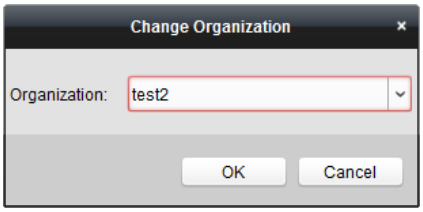
Nota: Se una carta viene emessa alla persona attuale, il collegamento non sarà valido dopo che la persona è stata cancellata.

Cambiare persona in un'altra organizzazione

Se necessario, puoi spostare la persona in un'altra organizzazione.

Passaggi:

1. Seleziona la persona nell'elenco e fai clic su **Cambia organizzazione** pulsante.



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

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

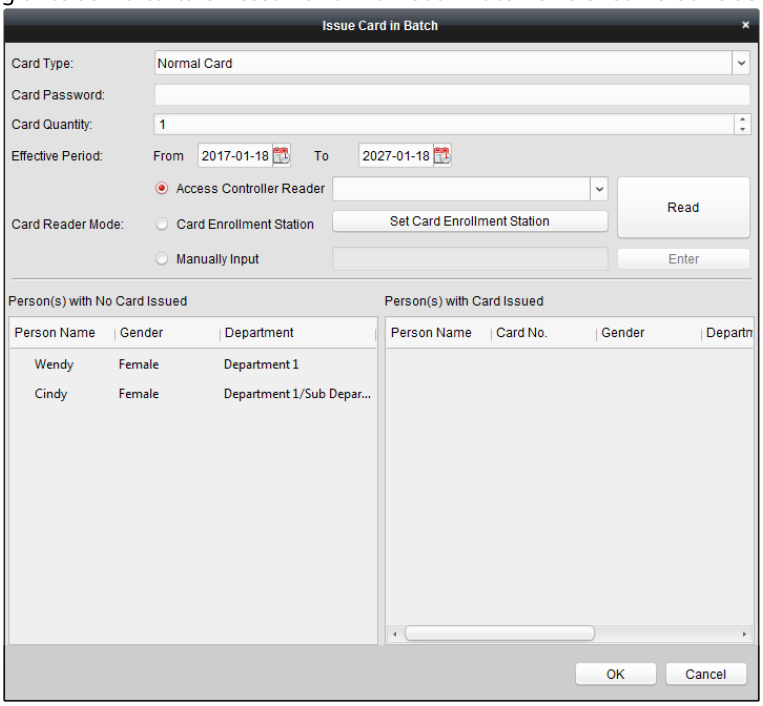
Carta di emissione in batch

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

Passaggi:

1. Fare clic su **Carta di emissione in batch** pulsante 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 scheda, fare riferimento a *Aggiunta di persona.*

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

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

4. Immettere la quantità di carta emessa per ogni persona.

Ad esempio, se il numero di carte è 3, puoi leggere o inserire tre numeri di carta per ogni persona.

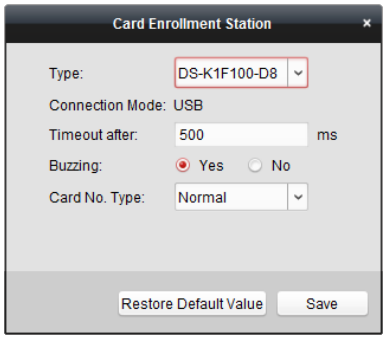
5. Fare clic per impostare l'ora effettiva e l'ora di scadenza della carta.

6. Selezionare la modalità Card Reader per leggere la carta n.

Lettore controller di accesso: Posizionare la tessera sul lettore del Controller di Accesso e cliccare **Leggere** per ricevere la tessera n.

Stazione di registrazione della carta: Posiziona la carta sulla stazione di registrazione della carta e fai clic su **Leggere** per ricevere la tessera n.

Nota: La Card Enrollment Station dovrebbe connettersi con il PC che esegue il client. Puoi cliccare**Imposta stazione di registrazione della carta** per accedere alla seguente finestra di dialogo.



1) Selezionare il tipo di stazione di registrazione della carta.

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 relativi alla postazione di registrazione delle tessere collegata.

Se la scheda è una scheda M1 e se è necessario abilitare la funzione di crittografia della scheda M1, è necessario controllare **Abilitare** casella di controllo di M1 Card Encryption e fare clic su **Modificare** per selezionare il settore.

3) Fare clic su **Salva** pulsante per salvare le impostazioni. Puoi cliccare**Ripristina valore predefinito** pulsante per ripristinare le impostazioni predefinite.

Inserimento manuale: Inserisci il numero della carta e clicca **accedere** per inserire la carta n.

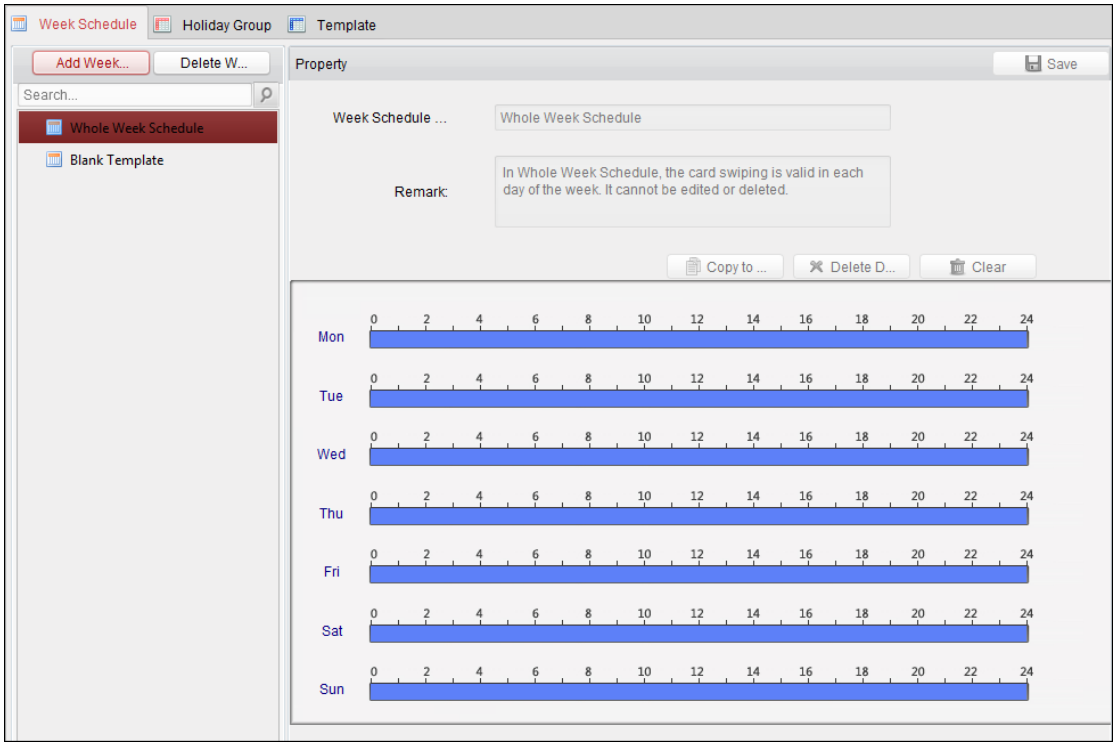
7. Dopo aver rilasciato la carta alla persona, le informazioni sulla persona e sulla carta verranno visualizzate nell'elenco delle persone con carta emessa.
8. Fare clic su **ok** per salvare le impostazioni.

7.6 Programma e modello

Scopo:

È possibile configurare il modello includendo il programma settimanale e il programma festivo. Dopo aver impostato i modelli, è possibile adottare i modelli configurati per accedere alle autorizzazioni di controllo durante l'impostazione dell'autorizzazione, in modo che l'autorizzazione al controllo di accesso abbia effetto nelle durate temporali del modello.

Clic  per accedere all'interfaccia di pianificazione e modello.



È possibile gestire la pianificazione dell'autorizzazione al controllo degli accessi, inclusi la pianificazione settimanale, la pianificazione festiva e il modello. Per le impostazioni dei permessi, fare riferimento a*Capitolo 7.7 Configurazione dei permessi.*

7.6.1Programma della settimana

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

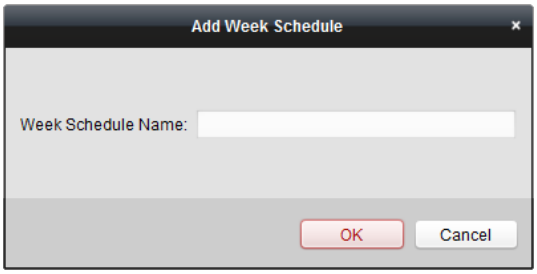
Programma intera settimana: Lo scorrimento della carta è valido tutti i giorni della settimana.

Programma vuoto: Lo scorrimento della carta non è valido in 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 pianificazione dell'aggiunta.



2. Immettere il nome del programma settimanale e fare clic su **ok** pulsante per aggiungere il programma settimanale.
3. Selezionare il programma settimanale aggiunto nell'elenco dei programmi e visualizzare le sue proprietà sulla destra. È possibile modificare il nome del programma settimanale e inserire le informazioni sull'osservazione.
4. Nella pianificazione della settimana, fai clic e trascina su un giorno per disegnare sulla pianificazione, il che significa che

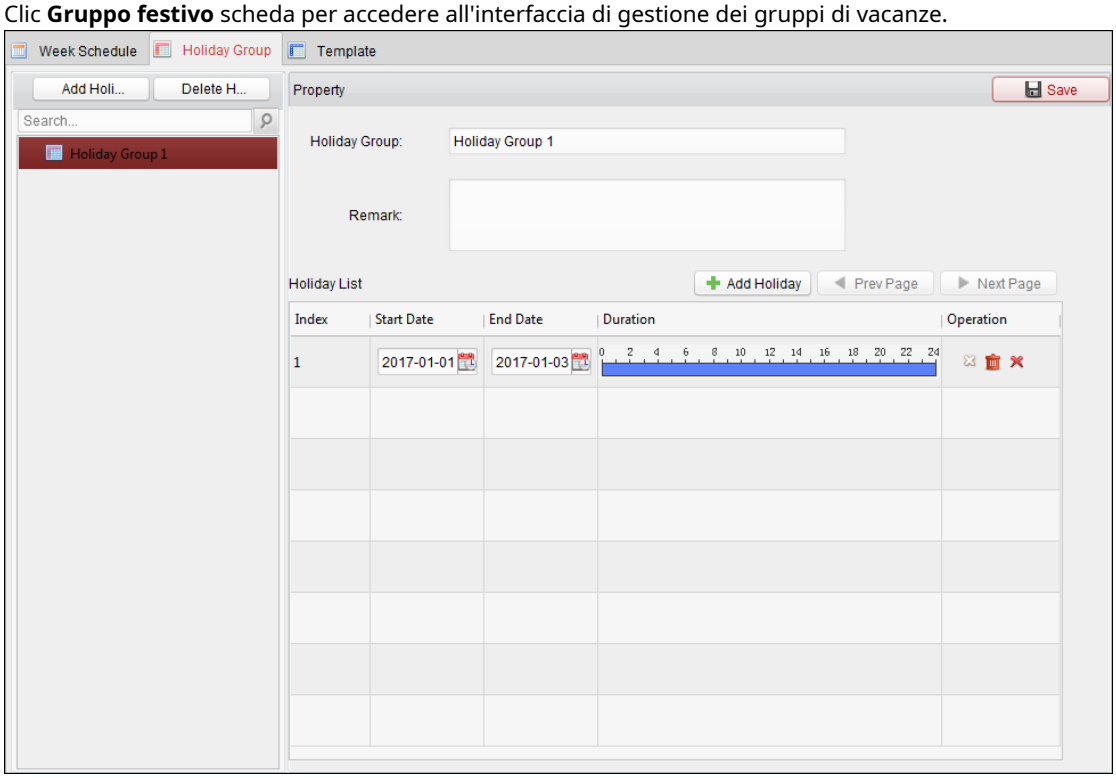
periodo di tempo, l'autorizzazione configurata viene attivata.

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

5. Quando il cursore si sposta su , è possibile spostare la barra temporale selezionata appena modificata. Puoi anche modificare il punto temporale visualizzato per impostare il periodo di tempo preciso. Quando il cursore si sposta su , è possibile allungare o accorciare la barra temporale selezionata.
6. Facoltativamente, è possibile selezionare la barra del tempo di pianificazione, quindi fare clic su **Elimina durata** per eliminare la barra temporale selezionata o fare clic su **Chiaro** per eliminare tutte le barre del tempo o fare clic su **Copia nella settimana** per copiare le impostazioni della barra del tempo sull'intera settimana.
7. Fare clic su **Salva** per salvare le impostazioni.

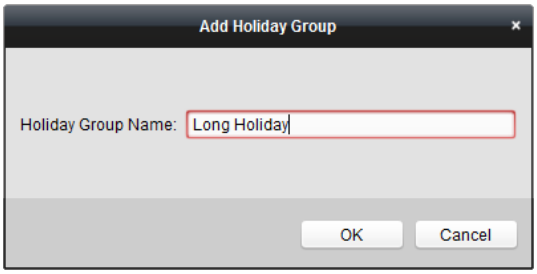
7.6.2 Gruppo Vacanze

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



Passaggi:

1. Fare clic su **Aggiungi gruppo vacanze Holiday** pulsante sulla sinistra per far apparire l'interfaccia di aggiunta del gruppo di festività.

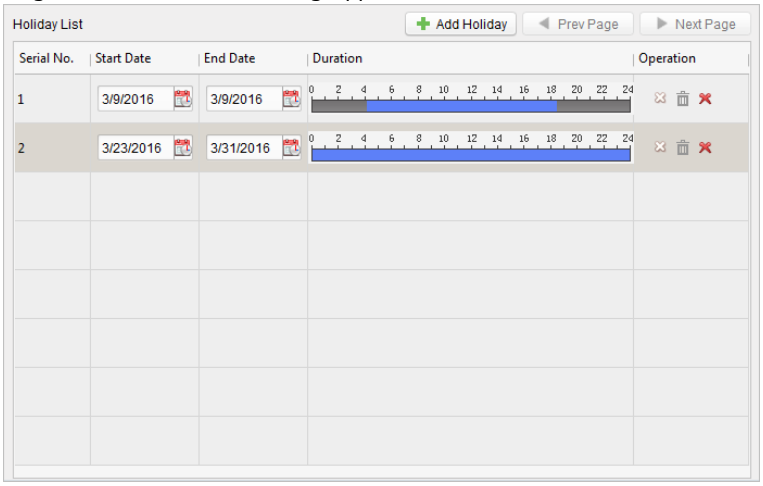


2. Inserisci il nome del gruppo di vacanze nel campo di testo e fai clic su **ok** pulsante per aggiungere il gruppo ferie.
3. Seleziona il gruppo di vacanze aggiunto e puoi modificare il nome del gruppo di vacanze e inserire il commento the

informazione.

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

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



   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 temporali per ciascun periodo nella pianificazione.

   2) Quando il cursore si sposta su , è possibile spostare la barra temporale selezionata appena modificata. Puoi modificare anche il punto temporale visualizzato per impostare il periodo di tempo preciso.

   3) Quando il cursore si sposta su , è possibile allungare o accorciare la barra temporale selezionata.

   4) Facoltativamente, è possibile selezionare la barra del tempo di pianificazione,

      e quindi fare clic per eliminare la barra del tempo selezionata,

      oppure fare clic per eliminare tutte le barre temporali della festività

      oppure fare clic per eliminare direttamente la festività.

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

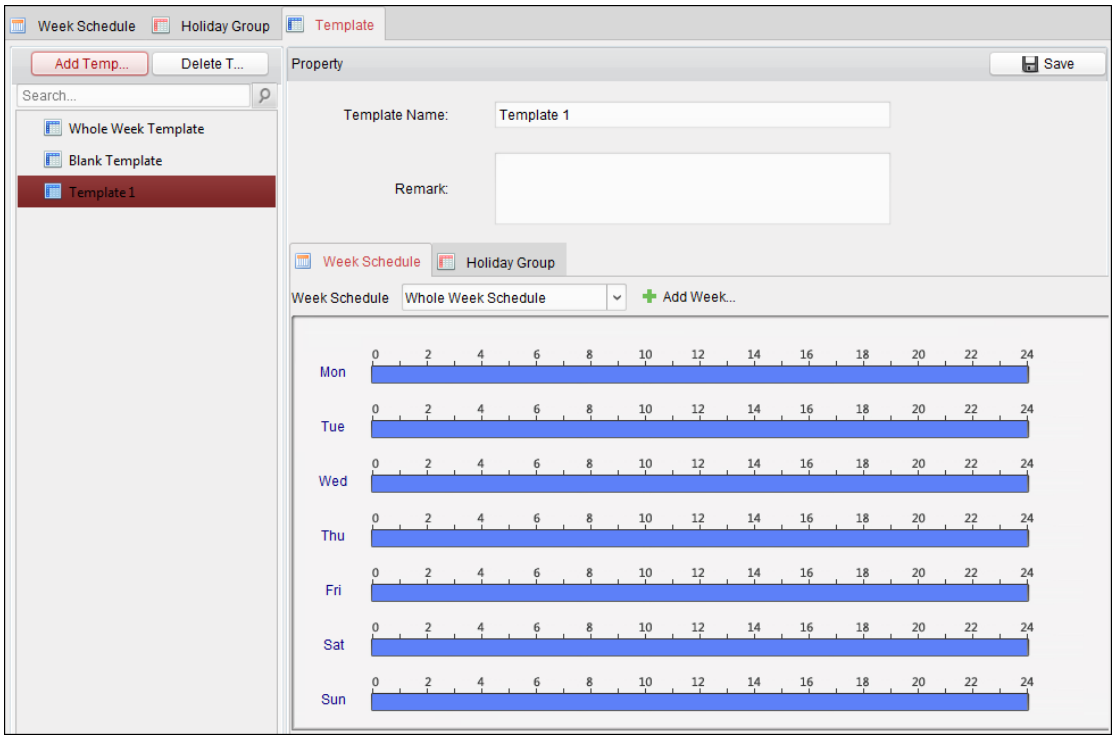
Nota: Le festività non possono essere sovrapposte tra loro.

7.6.3 Modello

Dopo aver impostato il programma settimanale e il gruppo festivo, è possibile configurare il modello che contiene il programma settimanale e il programma festivo.

Nota: La priorità della pianificazione del gruppo festivo è maggiore della pianificazione settimanale.

Clic**Modello** scheda per accedere all'interfaccia di gestione dei modelli.



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

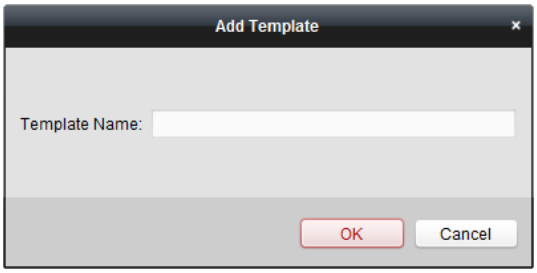
Modello intera settimana: La tessera magnetica è valida tutti i giorni della settimana e non è festiva orario di gruppo.

Modello vuoto: Lo scorrimento della carta non è valido in ogni giorno della settimana e non ha un programma di gruppo festivo.

Puoi definire modelli personalizzati su tua richiesta.

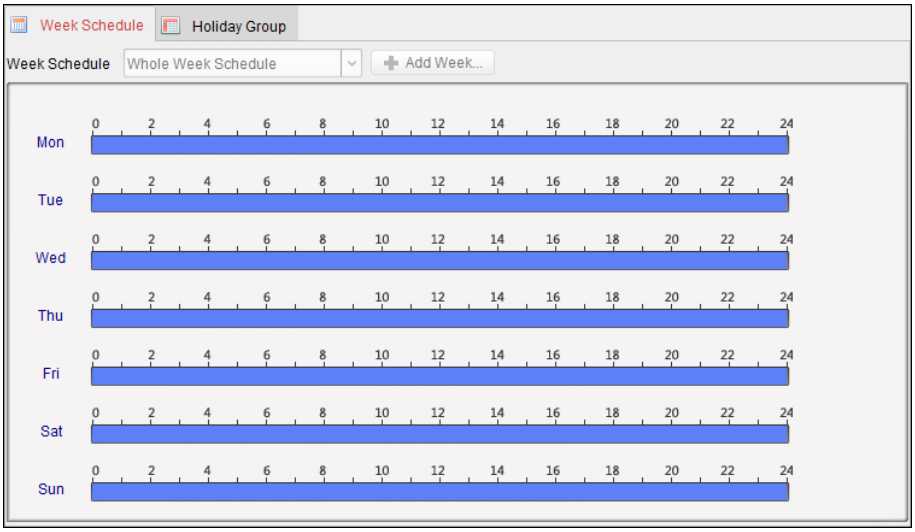
Passaggi:

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



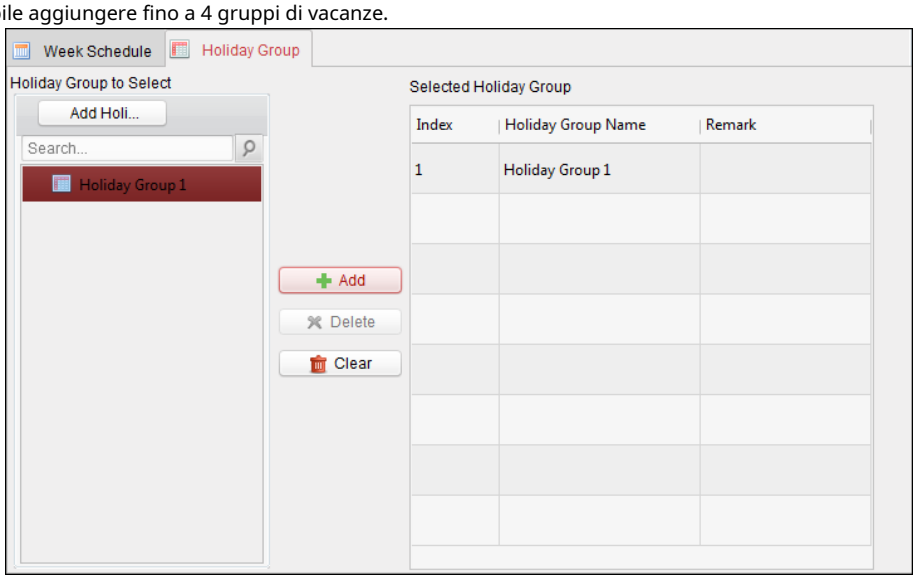
2. Inserisci il nome del modello nel campo di testo e fai clic su **ok** pulsante per aggiungere il modello.
3. Seleziona il modello aggiunto e puoi modificarne le proprietà sulla destra. È possibile modificare il nome del modello e inserire le informazioni sull'osservazione.
4. Selezionare un programma settimanale da applicare al programma.

   Clic **Programma della settimana** 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 al programma.

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 Holiday** per aggiungerne uno nuovo. Per i dettagli, fare riferimento a*Capitolo 7.6.2 Gruppo ferie.*

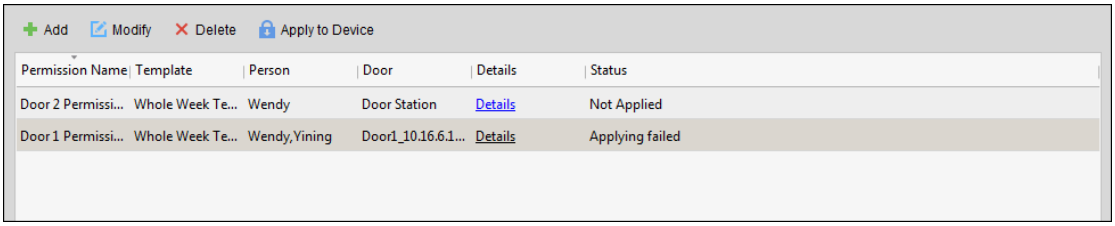
È possibile fare clic per selezionare un gruppo di festività aggiunto nell'elenco a destra e fare clic su **Elimina** per eliminarlo. Puoi cliccare**Chiaro** per eliminare tutti i gruppi di festività aggiunti.

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

7.7 Configurazione dei permessi

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

Fare clic sull'icona per accedere all'interfaccia di autorizzazione al controllo di accesso.



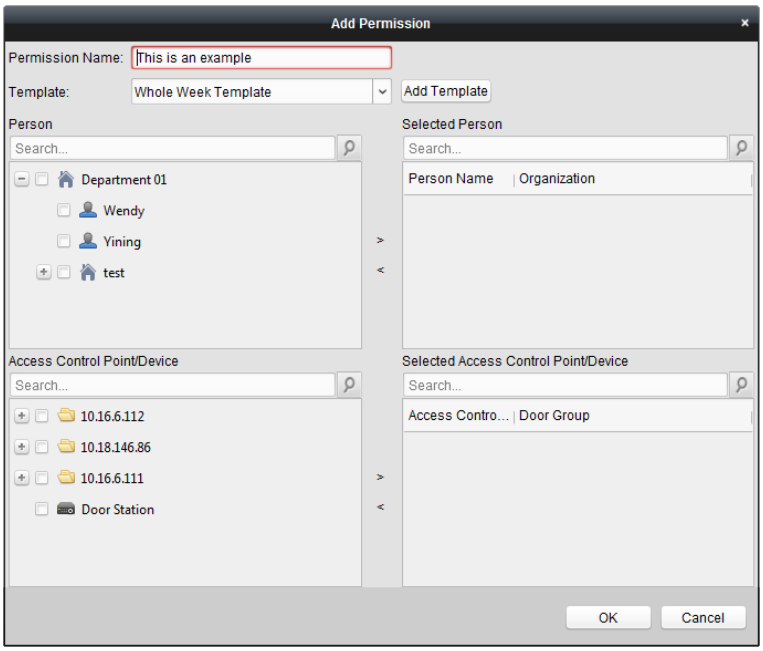
7.7.1 Aggiunta di autorizzazione

Scopo:

È possibile assegnare il permesso alle persone di entrare/esistere dai punti di controllo degli accessi (porte) in questa sezione.

Passaggi:

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



2. Nel campo Nome autorizzazione, inserire 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 di autorizzazione. Puoi cliccare**Aggiungi modello** pulsante per aggiungere il modello. Fare riferimento a*Capitolo 7.6 Programma e modello* per dettagli.

4. Nell'elenco Persone, vengono visualizzate tutte le persone aggiunte.

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

   (Facoltativo) È possibile selezionare la persona nell'elenco Persone selezionate e fare clic su < per annullare la selezione.

5. Nell'elenco Punti di controllo accessi/dispositivi, verranno visualizzati tutti i punti di controllo accessi (porte) e i videocitofoni aggiunti.

   Spuntare le caselle di controllo per selezionare la/e porta/e o il/i posto esterno/i e fare clic su > per aggiungere all'elenco selezionato.

   (Facoltativo) È possibile selezionare la porta o il videocitofono nell'elenco selezionato e fare clic su < per annullare la selezione.

6. Fare clic su **ok** pulsante per completare l'aggiunta dell'autorizzazione. La persona selezionata avrà il

permesso di entrare/uscire dal citofono/citofono selezionato con la/e tessera/e collegata/e o con le impronte digitali.

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

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

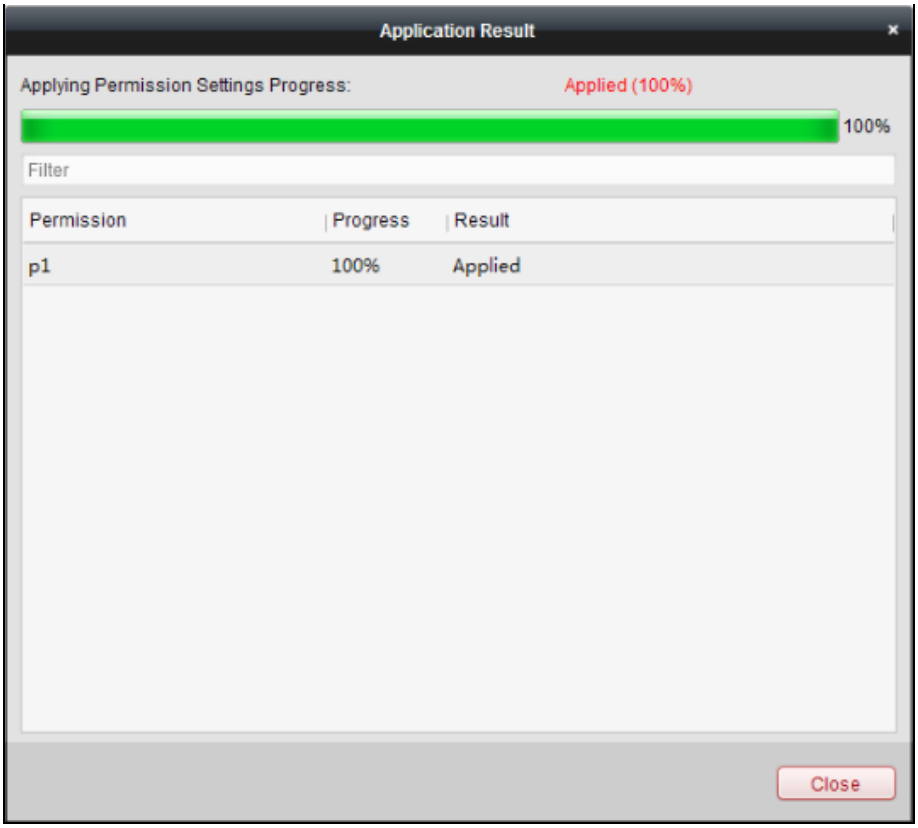
7.7.2 Richiesta di autorizzazione

Scopo:

Dopo aver configurato le autorizzazioni, è necessario applicare l'autorizzazione aggiunta al dispositivo di controllo dell'accesso per avere effetto.

Passaggi:

1. Selezionare le autorizzazioni da applicare al dispositivo di controllo dell'accesso. Per selezionare più autorizzazioni, puoi tenere il *Ctrl* o *Cambio* chiave e selezionare i permessi.
2. Fare clic su **Applica al dispositivo** per iniziare ad applicare le autorizzazioni selezionate al dispositivo di controllo accessi o al posto esterno.
3. Il seguitoiong apparirà una finestra, che indica il risultato dell'applicazione del permesso.

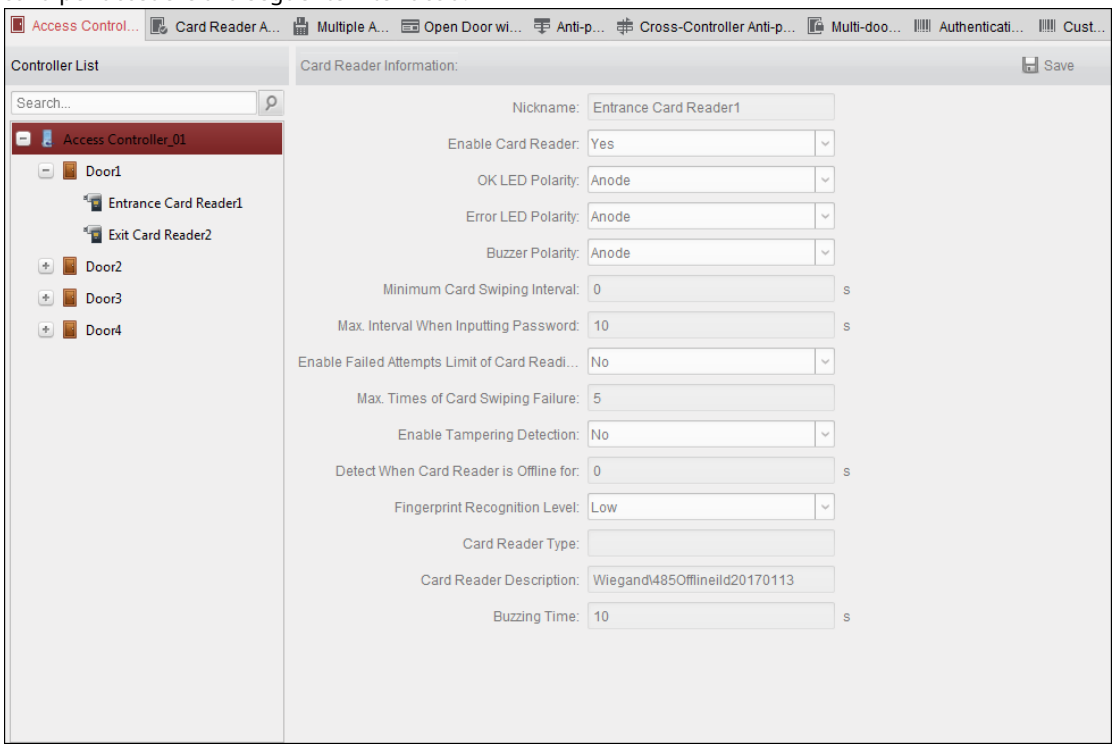


7.8 Funzioni avanzate

Scopo:

Dopo aver configurato la persona, il modello e l'autorizzazione al controllo degli accessi, è possibile configurare le funzioni avanzate dell'applicazione di controllo degli accessi, come i parametri di controllo degli accessi, la password di autenticazione e l'apertura della porta con la prima carta, l'anti-passback, ecc.

Nota: Le funzioni avanzate dovrebbero essere supportate dal dispositivo. Fare clic sull'icona per accedere alla seguente interfaccia.



7.8.1 Parametri di controllo dell'accesso

Scopo:

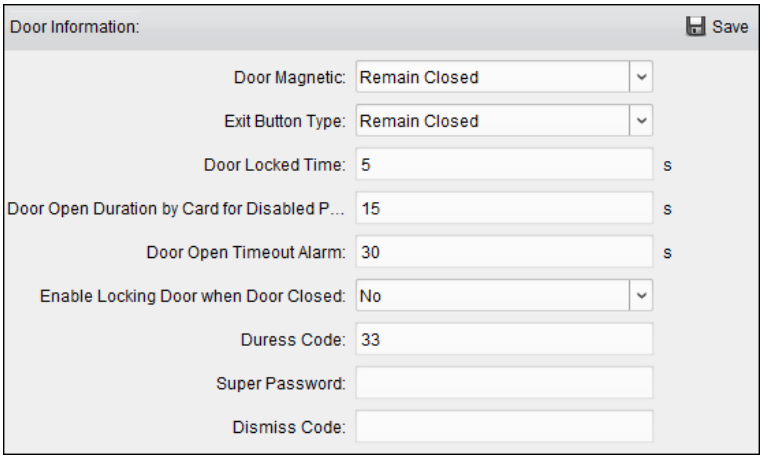
Dopo aver aggiunto il dispositivo di controllo accessi, è possibile configurare i parametri del suo punto di controllo accessi (porta) e dei suoi lettori di tessere.

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) ed è possibile 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 condizioni speciali).

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

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

Durata Apertura Porta con Tessera Disabili: La porta magnetica può essere abilitata con opportuno ritardo dopo che il disabile striscia la tessera.

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

Abilita chiusura porta a porta chiusa (riservato): La porta può essere bloccata una volta chiusa anche se non viene raggiunto il Tempo di porta chiusa.

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.

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

Ignora codice: Immettere il codice di espulsione per disattivare il cicalino del lettore di carte.

Appunti:

Il codice coercizione, la Super password e il codice di espulsione dovrebbero essere diversi.

Il codice coercizione, la super password e il codice di espulsione dovrebbero essere diversi dalla password di autenticazione.

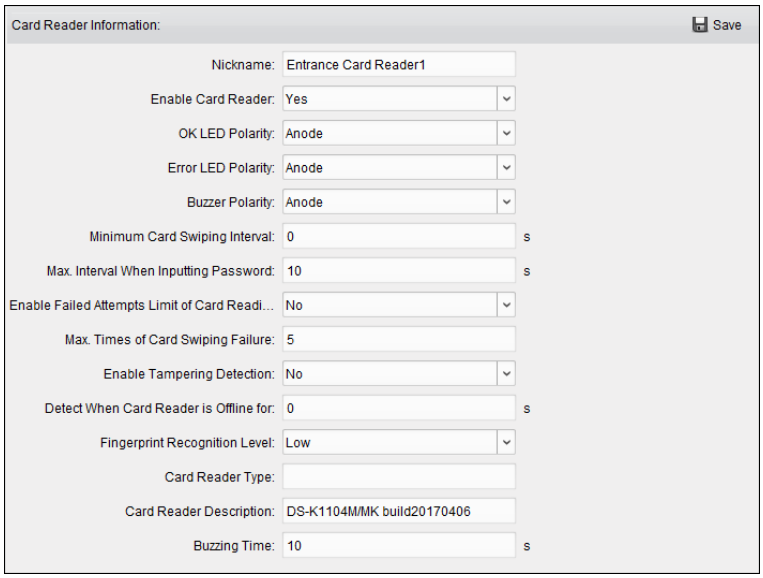
Il codice coercizione, la super password e il codice di espulsione dovrebbero contenere da 4 a 8 numeri.

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 carte e può modificare i parametri del lettore di schede sulla destra.



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

Intervallo minimo di passaggio 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. Puoi impostarlo da 0 a 255.

massimo 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 premute in precedenza verranno cancellate automaticamente.

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

massimo Tempi di mancato scorrimento della carta: Imposta il massimo tentativi falliti di lettura tessera.

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

Rileva quando il lettore di schede è offline per: Quando il dispositivo di controllo accessi non riesce a connettersi con il lettore di schede per un periodo più lungo del tempo impostato, il lettore di schede si disattiverà automaticamente.

Livello di riconoscimento delle impronte digitali: Selezionare il livello di riconoscimento dell'impronta digitale nell'elenco a discesa. Per impostazione predefinita, il livello è Basso.

Tipo di lettore di schede: Leggi il tipo di lettore di schede.

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

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

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 schede 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 schede:

   Carta e Password: La porta può essere aperta sia inserendo la password della carta che scorrendo la carta.

   Nota: Qui la password si riferisce alla password impostata al momento del rilascio della carta alla persona. *Capitolo 7.5.2 Gestione delle persone.*

   Carta o Password di Autenticazione: La porta può aprirsi inserendo l'autenticazione password o strisciando la carta.

   Nota: Qui la password di autenticazione si riferisce alla password impostata per aprire la porta. Fare riferimento a *Capitolo 7.8.8 Password di autenticazione.*

   Impronta digitale: La porta si apre inserendo solo l'impronta digitale.

   Carta: La porta può essere aperta solo scorrendo la carta.

   Carta o impronta digitale: La porta può essere aperta inserendo l'impronta digitale o scorrendo la carta.

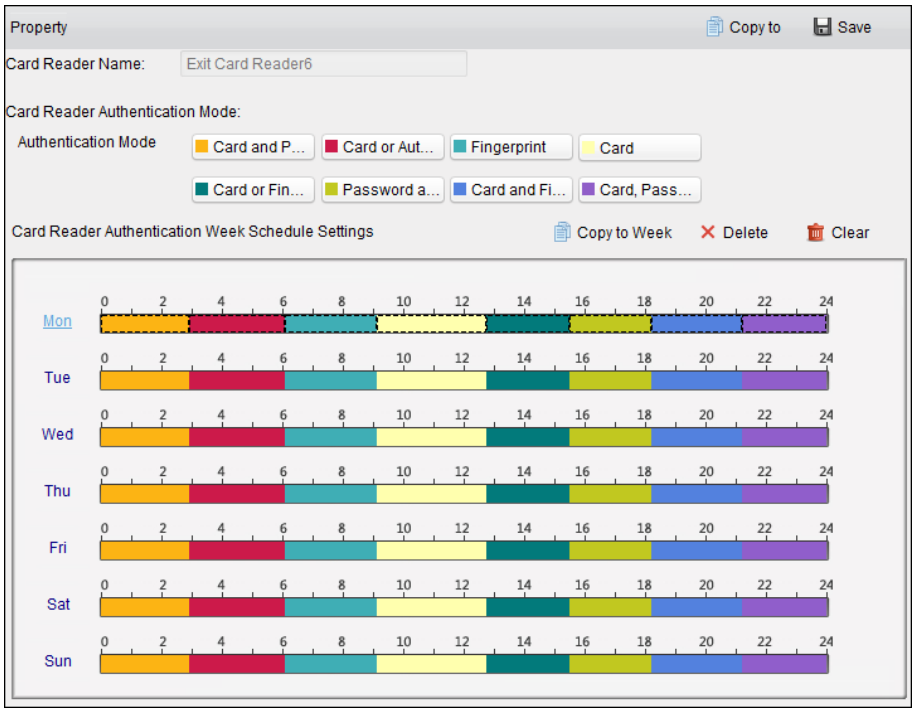
   Password e impronta digitale: La porta può essere aperta sia inserendo la password della carta che inserendo l'impronta digitale.

   Nota: Qui la password si riferisce alla password della carta impostata al momento del rilascio della carta alla persona. Fare riferimento a *Capitolo 7.5.2 Gestione delle persone.*

   Carta e impronte digitali: La porta può essere aperta sia inserendo l'impronta digitale che scorrendo la carta.

   Carta, password e impronta digitale: La porta può essere aperta sia inserendo l'impronta digitale, inserendo la password della carta, sia facendo scorrere la carta.

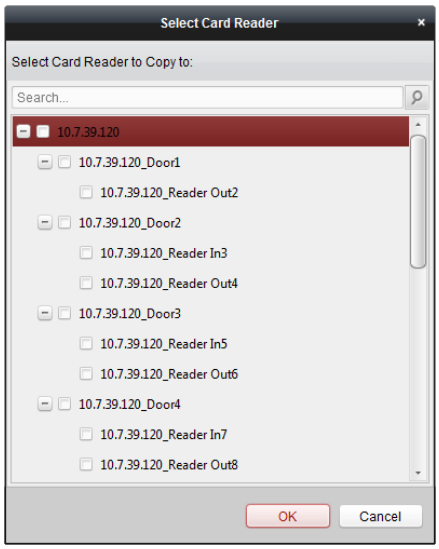
   Nota: Qui la password si riferisce alla password della carta impostata al momento del rilascio della carta alla persona. Fare riferimento a *Capitolo 7.5.2 Gestione delle persone.*
3. Fare clic e trascinare il mouse su un giorno per disegnare una barra colorata sulla pianificazione, il che significa 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 nella settimana** pulsante per copiare le stesse impostazioni su tutta la settimana.

   (Facoltativo) Puoi fare clic su **Elimina** pulsante 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 Autenticazione multipla

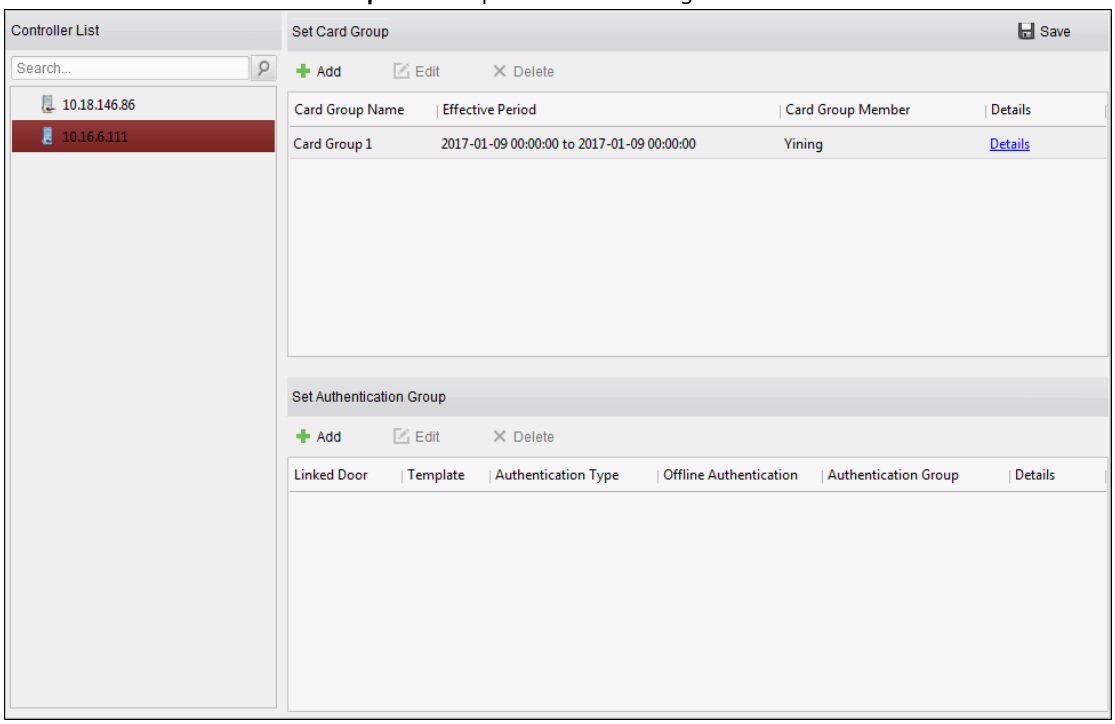
Scopo:

È possibile gestire le tessere per gruppo e impostare l'autenticazione per più tessere per un punto di controllo accessi (porta).

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

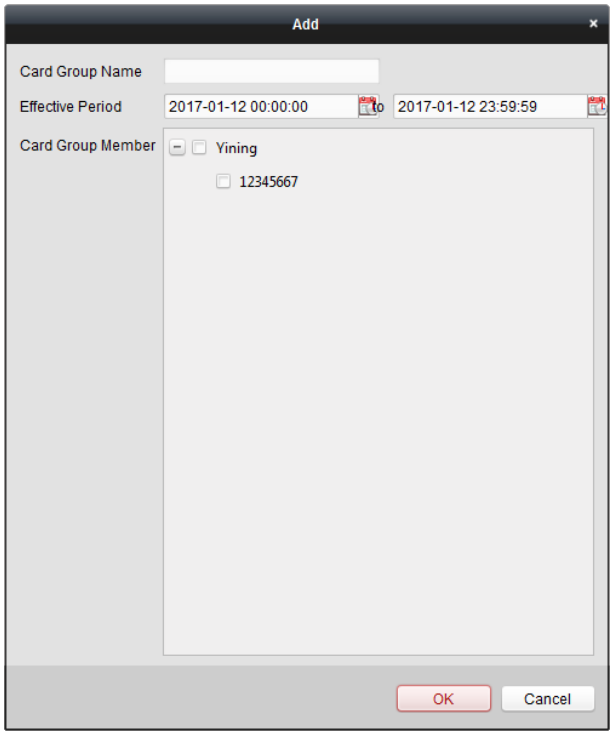
Passaggi:

1. Fare clic su **Autenticazione multipla** scheda per accedere alla seguente interfaccia.



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

3. Nel pannello Imposta gruppo di schede a destra, fare clic su **Inserisci** pulsante per far apparire la seguente finestra di dialogo:



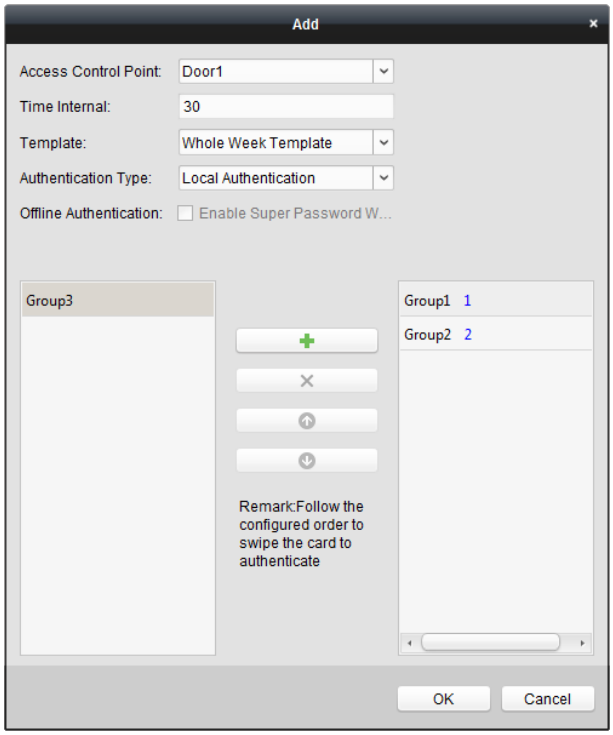
1) Nel campo Nome gruppo tessera, inserire il nome del gruppo come desiderato.

2) Fare clic per impostare l'ora effettiva e l'ora di scadenza del gruppo di tessere.

3) Spuntare le caselle di controllo per selezionare le carte a cui aggiungere il gruppo di carte.

4) Fare clic su **ok** per salvare il gruppo di carte.

4. Nel pannello Imposta gruppo di autenticazione a sinistra, fare clic su **Inserisci** per far apparire la seguente finestra di dialogo.



1) Selezionare il punto di controllo accessi (porta) del dispositivo per l'autenticazione multipla.

2) Immettere l'intervallo di tempo per lo scorrimento della carta.

3) Selezionare il modello del gruppo di autenticazione dall'elenco a discesa. Per i dettagli sull'impostazione del modello, fare riferimento a*Capitolo 7.6 Programma e modello.*

4) Selezionare il tipo di autenticazione del gruppo di autenticazione dall'elenco a discesa.

Autenticazione locale: Autenticazione da parte del dispositivo di controllo accessi.

Autenticazione locale e porta aperta da remoto: Autenticazione da parte del dispositivo di controllo accessi e da parte del client.

Per il tipo Autenticazione locale e Porta aperta in remoto, è possibile selezionare la casella di controllo per abilitare l'autenticazione con super password quando il dispositivo di controllo dell'accesso è disconnesso dal client.

Autenticazione locale e Super Password: Autenticazione da parte del dispositivo di controllo accessi e dalla super password.

5) Nell'elenco a sinistra verrà visualizzato il gruppo di carte aggiunto. È possibile fare clic sul gruppo di schede e fare clic per aggiungere il gruppo al gruppo di autenticazione.

Puoi fare clic sul gruppo di carte aggiunto e fare clic per rimuoverlo dall'autenticazione gruppo.

Puoi anche fare clic su o per impostare l'ordine di scorrimento della carta.

5) Immettere il **Tempi di passaggio delle carte** per il gruppo di carte selezionato.

Appunti:

I tempi di scorrimento della carta devono essere maggiori di 0 e minori della quantità di carte aggiunta nel gruppo di carte.

Il limite massimo dei tempi di scorrimento della carta è 16.

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

5. Fare clic su **Salva** per salvare e rendere effettive le nuove impostazioni.

Appunti:

Per ogni punto di controllo accessi (porta), è possibile aggiungere fino a quattro gruppi di autenticazione.

Per il gruppo di autenticazione quale tipo di certificato è **Autenticazione locale,** è possibile aggiungere fino a 8 gruppi di tessere al gruppo di autenticazione.

Per il gruppo di autenticazione quale tipo di certificato è **Autenticazione locale e Super Password** o **Autenticazione locale e porta aperta da remoto,** è possibile aggiungere fino a 7 gruppi di tessere al gruppo di autenticazione.

7.8.4 Porta aperta con la prima carta

Scopo:

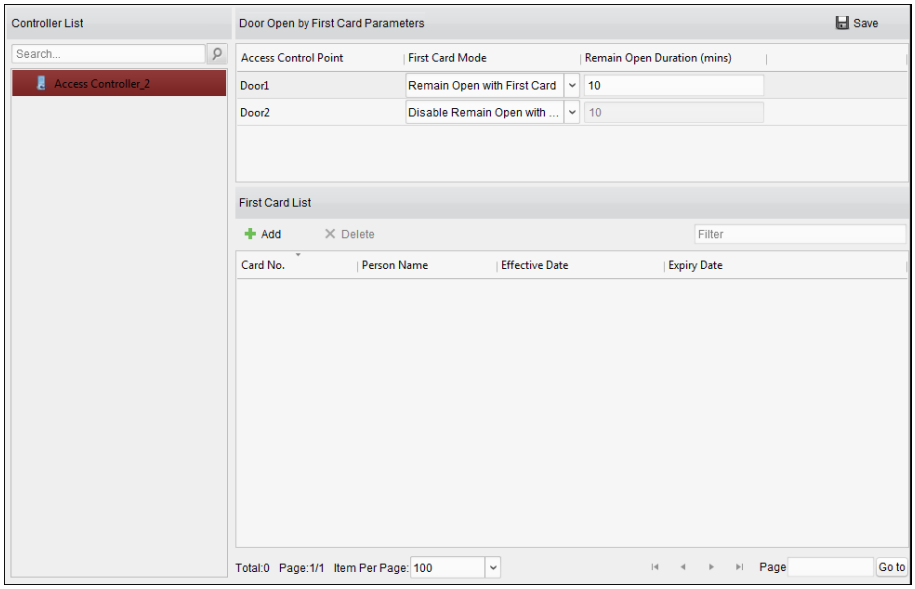
È possibile impostare più prime carte per un punto di controllo accessi. Dopo il primo passaggio della carta, consente a più persone di accedere alla porta o ad altre azioni di autenticazione. La modalità della prima carta contiene Rimani aperto con la prima carta, Disattiva Rimani aperto con la prima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

Rimani aperto con la prima carta: La porta rimane aperta per il periodo di tempo configurato dopo il primo passaggio della tessera fino al termine del periodo di apertura.

Autorizzazione prima carta: Tutte le autenticazioni, ad eccezione delle autenticazioni di super card, coercizione e coercizione codice, 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 accessi dall'elenco a sinistra.
3. Selezionare la prima modalità della scheda nell'elenco a discesa per il punto di controllo accessi.
4. (Facoltativo) Se si seleziona Rimani aperto con la prima carta, è necessario impostare la durata dell'apertura.

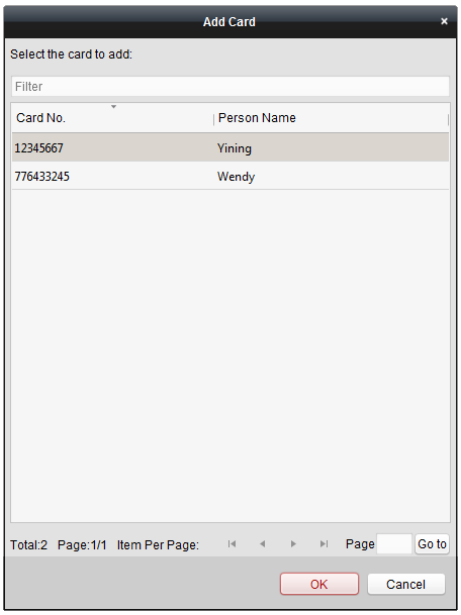
Appunti:

La durata rimane aperta dovrebbe essere compresa tra 0 e 1440 minuti. Per impostazione predefinita, sono 10 minuti.

Nella modalità di autorizzazione prima carta, è possibile accedere alla porta quando si striscia la carta super, la carta coercizione o inserire il codice coercizione senza strisciare la prima carta. Puoi scorrere nuovamente la prima carta per disabilitare la modalità prima carta.

La prima autorizzazione della carta è effettiva solo il giorno corrente. L'autorizzazione scadrà dopo le 24:00 del giorno corrente.

5. Nell'elenco Prima carta, fare clic su **Inserisci** pulsante per far apparire la seguente finestra di dialogo.



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

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

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

6. Puoi fare clic su **Elimina** pulsante per rimuovere la carta dalla prima lista di carte.

7. Fare clic su **Salva** per salvare e rendere effettive le nuove impostazioni.

7.8.5 Anti-passaggio indietro

Scopo:

È possibile impostare l'anti-passback per i lettori di schede nello stesso controller di accesso. Dovresti far scorrere la carta in base al percorso della carta di scorrimento configurato. E solo una persona poteva passare il punto di controllo degli accessi dopo aver strisciato la carta.

Appunti:

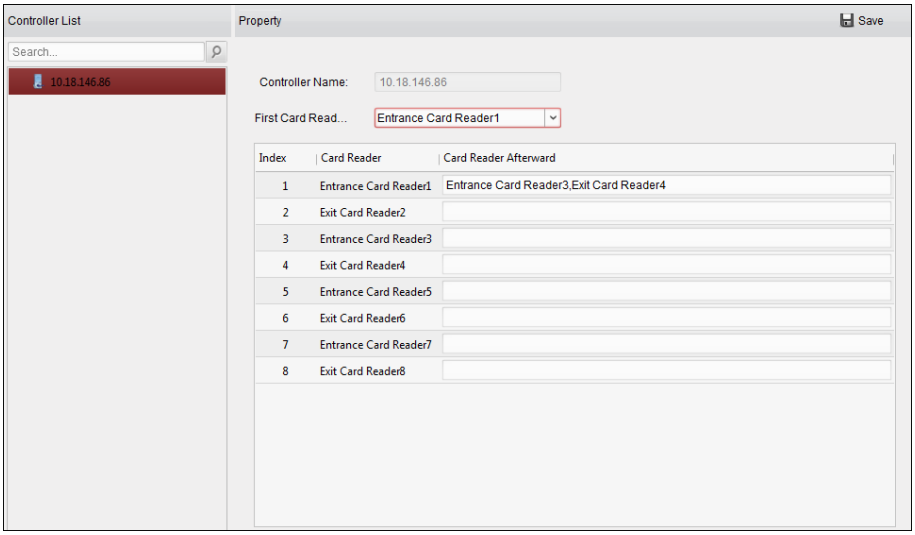
Per un accesso è possibile configurare sia la funzione anti-passante che l'interblocco multiporta dispositivo di controllo allo stesso tempo.

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

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

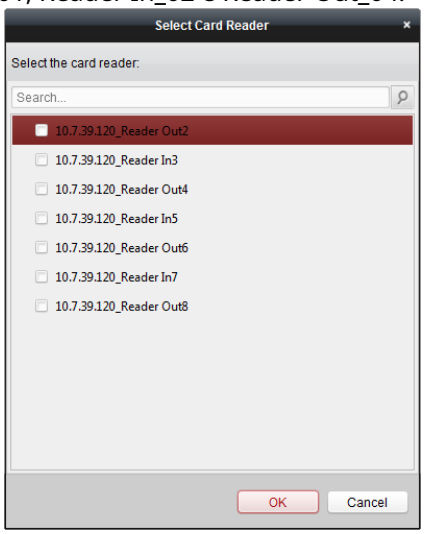
Passaggi:

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



2. Selezionare un dispositivo di controllo degli accessi dall'elenco dei dispositivi a sinistra.
3. Nel campo Primo lettore di schede, selezionare il lettore di schede come inizio del percorso.
4. Nell'elenco, fare clic sul testo archiviato di **Lettore di schede in seguito** e selezionare i lettori di schede 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 puoi solo passare attraverso il punto di controllo accessi scorrendo la carta nell'ordine come Reader In_01, Reader In_02 e Reader Out_04.



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

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

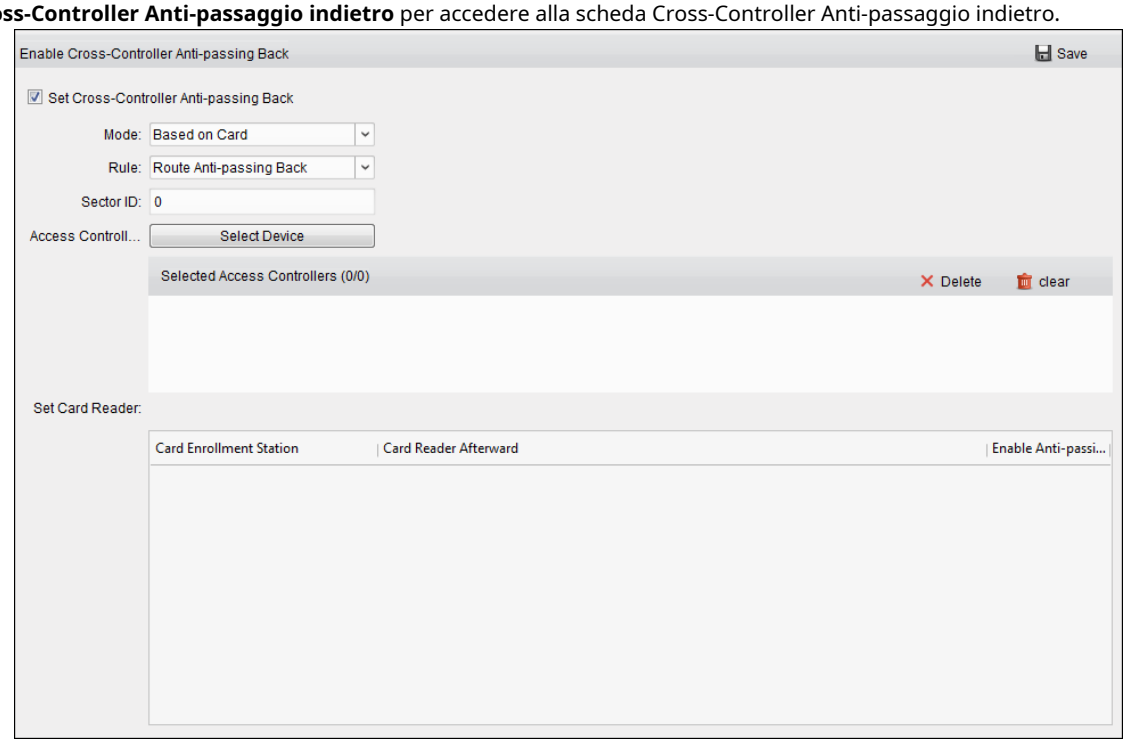
7.8.6 Cross-Controller Anti-passaggio indietro

Scopo:

È possibile impostare l'anti-passback per i lettori di schede in più controller di accesso. Dovresti scorrere il

carta in base al percorso della carta a scorrimento configurato. E solo una persona poteva passare il punto di controllo degli accessi dopo aver strisciato la carta.

Clic **Cross-Controller Anti-passaggio indietro** per accedere alla scheda Cross-Controller Anti-passaggio indietro.



Impostazione del percorso Anti-passaggio indietro

Scopo:

Il percorso anti-passback dipende dal percorso di scorrimento della carta. È necessario impostare il primo lettore di schede e successivamente i lettori di schede.

Passaggi:

1. Controlla il **Abilita Cross-Controller Anti-passing indietro** casella di controllo per abilitare la funzione.
2. Impostare i parametri anti-passback.

Basato su carta

Nota: Il sistema valuterà l'anti-passaggio in base alle registrazioni di ingresso e uscita sulla carta.

1) Seleziona **Basato su carta** come modalità anti-ripasso nell'elenco a discesa.

2) Selezionare Rotta Anti-passaggio indietro come regola.

3) Impostare l'ID del settore.

4) Fare clic su **Seleziona dispositivo** per selezionare un dispositivo nella finestra pop-up per l'autenticazione anti-passback.

5) Nell'area Imposta lettore di tessere, fare clic sull'icona a sinistra della stazione di registrazione delle tessere colonna per selezionare il primo lettore di schede. L'icona si trasformerà in .

6) Fare clic sul campo di immissione successivo del lettore di schede per selezionare successivamente i lettori di schede nella finestra a comparsa.

7) Spuntare la casella di controllo nella colonna Enable Anti-passing Back per abilitare la funzione anti-passaggio.

Appunti:

I lettori di schede visualizzati nel campo di immissione successivo del lettore di schede dovrebbero essere nell'ordine di autenticazione.

È possibile aggiungere fino a 64 controller con funzione anti-passback.

È possibile aggiungere successivamente fino a 16 lettori di schede per ogni lettore di schede.

Attualmente supporta la scheda M1 e il settore non può essere crittografato. Per i dettagli sulla crittografia dei settori, fare riferimento a *7.4.6 Crittografia della scheda M1.*

Basato su rete

Nota: Autenticare l'anti-rientro in base alle informazioni di ingresso e uscita sul lettore di carte.

1) Seleziona **Basato su rete** come modalità anti-ripasso nell'elenco a discesa.

2) Selezionare Rotta Anti-passaggio indietro come regola.

3) Selezionare un server nell'elenco a discesa per giudicare l'anti-passaggio.

4) (Facoltativo) Puoi fare clic su **Elimina record anti-passaggio indietro** e seleziona la carta nella finestra pop-up per eliminare le informazioni sullo scorrimento della carta in tutti i dispositivi.

L'utente dovrebbe ricominciare a scorrere la carta dal primo lettore di carte.

5) Nell'area Imposta lettore di tessere, fare clic sull'icona a sinistra della stazione di registrazione delle tessere colonna per selezionare il primo lettore di schede. L'icona si trasformerà in  .

6) Fare clic sul campo di immissione successivo del lettore di schede per selezionare successivamente i lettori di schede nella finestra a comparsa.

7) Spuntare la casella di controllo nella colonna Enable Anti-passing Back per abilitare la funzione anti-passaggio.

Appunti:

I lettori di schede visualizzati nel campo di immissione successivo del lettore di schede dovrebbero essere nell'ordine di autenticazione.

È possibile aggiungere fino a 64 controller con funzione anti-passback.

È possibile aggiungere successivamente fino a 16 lettori di schede per ogni lettore di schede.

Nel server selezionato è possibile memorizzare fino a 5000 record di scorrimento delle carte.

Impostazione Ingresso/Uscita Anti-passaggio Indietro

Scopo:

È possibile impostare il lettore di tessere di ingresso e il lettore di tessere di uscita solo in entrata e in uscita, senza impostare il primo lettore di tessere e successivamente i lettori di tessere.

Passaggi:

1. Nella scheda Cross-Controller Anti-passing Back, seleziona il **Abilita Cross-Controller Anti-passing Indietro** casella di controllo per abilitare la funzione.

2. Impostare i parametri anti-passback.

Basato su carta

Nota: Il sistema valuterà l'anti-passaggio in base alle registrazioni di ingresso e uscita sulla carta.

1) Seleziona **Basato su carta** come modalità anti-ripasso nell'elenco a discesa.

2) Selezionare Ingresso/Uscita Anti-passaggio indietro come regola.

3) Impostare l'ID del settore.

4) Fare clic su **Seleziona dispositivo** per selezionare un dispositivo nella finestra pop-up per l'autenticazione anti-passback.

5) Nell'area Imposta Lettore Tessera, spuntare le caselle di controllo nella colonna Abilita Anti-rientro per selezionare il lettore di tessera di ingresso e il lettore di tessera di uscita.

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

Appunti:

Devono essere controllati fino a un lettore di tessere di ingresso e un lettore di tessere di uscita.

È possibile aggiungere fino a 64 controller con funzione anti-passback.

Attualmente supporta la scheda M1 e il settore non può essere crittografato. Per i dettagli sulla crittografia dei settori, fare riferimento a *7.4.6 Crittografia della scheda M1.*

Basato su rete

Nota: Autenticare l'anti-rientro in base alle informazioni di ingresso e uscita sul lettore di carte.

1) Seleziona **Basato su rete** come modalità anti-ripasso nell'elenco a discesa.

2) Selezionare Ingresso/Uscita Anti-passaggio indietro come regola.

3) Selezionare il server nell'elenco a discesa per giudicare l'anti-passaggio indietro.

4) (Facoltativo) Puoi fare clic su **Elimina registrazione** e seleziona la carta nella finestra pop-up per eliminare le informazioni sullo scorrimento della carta in tutti i dispositivi.

5) Fare clic su **Seleziona dispositivo** per selezionare un dispositivo nella finestra pop-up per l'autenticazione anti-passback.

6) Nell'area Imposta Lettore Tessera, spuntare le caselle di controllo nella colonna Abilita Anti-rientro per selezionare il lettore di tessera di ingresso e il lettore di tessera di uscita.

7) Fare clic su **Salva** per salvare le impostazioni.

Appunti:

Devono essere controllati fino a un lettore di tessere di ingresso e un lettore di tessere di uscita.

È possibile aggiungere fino a 64 controller con funzione anti-passback.

Nel server selezionato è possibile memorizzare fino a 5000 record di scorrimento delle carte.

7.8.7 Interblocco multiporta

Scopo:

È possibile impostare l'interblocco multiporta tra più porte dello stesso dispositivo di controllo accessi. Per aprire una delle porte, le altre porte devono rimanere chiuse. Ciò significa che nel gruppo di porte combinato interbloccato è possibile aprire fino a una porta contemporaneamente.

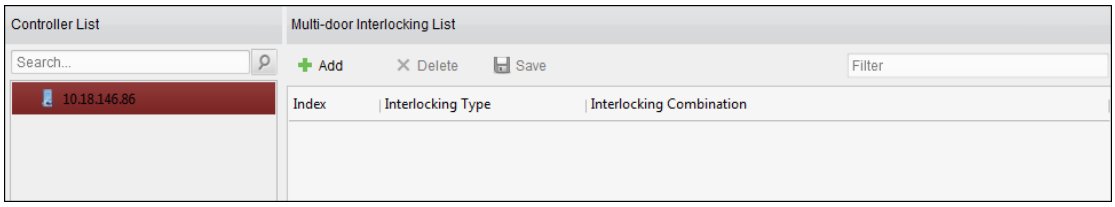
Appunti:

La funzione Interblocco multiporta è supportata solo dal dispositivo di controllo accessi che ha più punti di controllo accessi (porte).

Per un dispositivo di controllo accessi è possibile configurare contemporaneamente sia la funzione anti-passante che l'interblocco multiporta.

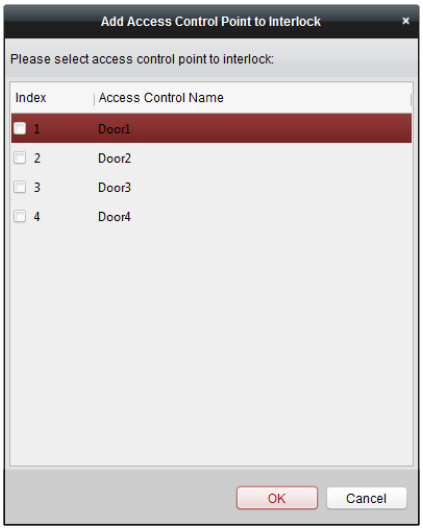
Passaggi:

1. Fare clic su **Interblocco multi-porta** scheda per accedere alla pagina delle impostazioni dell'interblocco multiporta.



2. Selezionare un controller di accesso dall'elenco dei controller.

3. Fare clic su **Inserisci** per visualizzare l'interfaccia Aggiungi punto di controllo di accesso all'interblocco.



4. Selezionare il punto di controllo accessi (porta) dall'elenco.

   Nota: È possibile aggiungere fino a quattro porte in una combinazione di interblocco a più porte.

5. Fare clic su **ok** per salvare l'aggiunta.

6. (Facoltativo) Dopo aver aggiunto la combinazione di interblocco multiporta, è possibile selezionarla dall'elenco e fare clic su **Elimina** per eliminare la combinazione.

7. Fare clic su **Salva** pulsante per salvare ed avere effetto.

7.8.8 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:

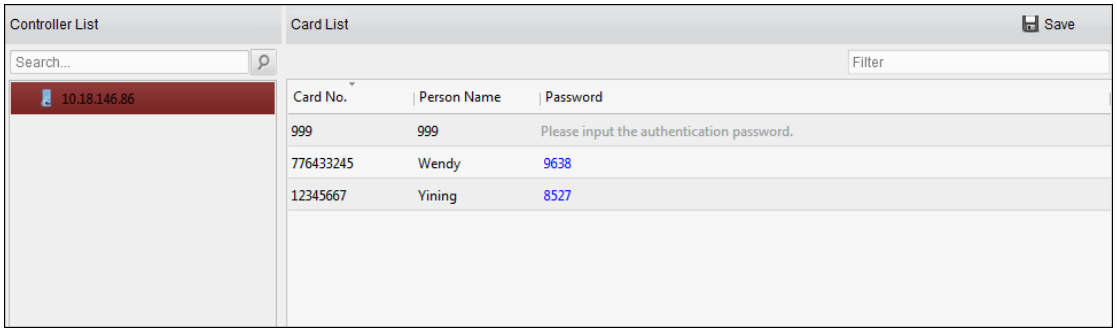
Questa funzione di password di autenticazione è valida solo durante gli orari in cui il lettore di tessere la modalità di autenticazione per il dispositivo di controllo accessi è impostata su **Carta o password di autenticazione.**

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 dei permessi.*

2. Fare clic su **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 di 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 con la super password, il codice coercizione e il codice di esclusione nei parametri di controllo dell'accesso.

7.8.9 CustomWiegand

Scopo:

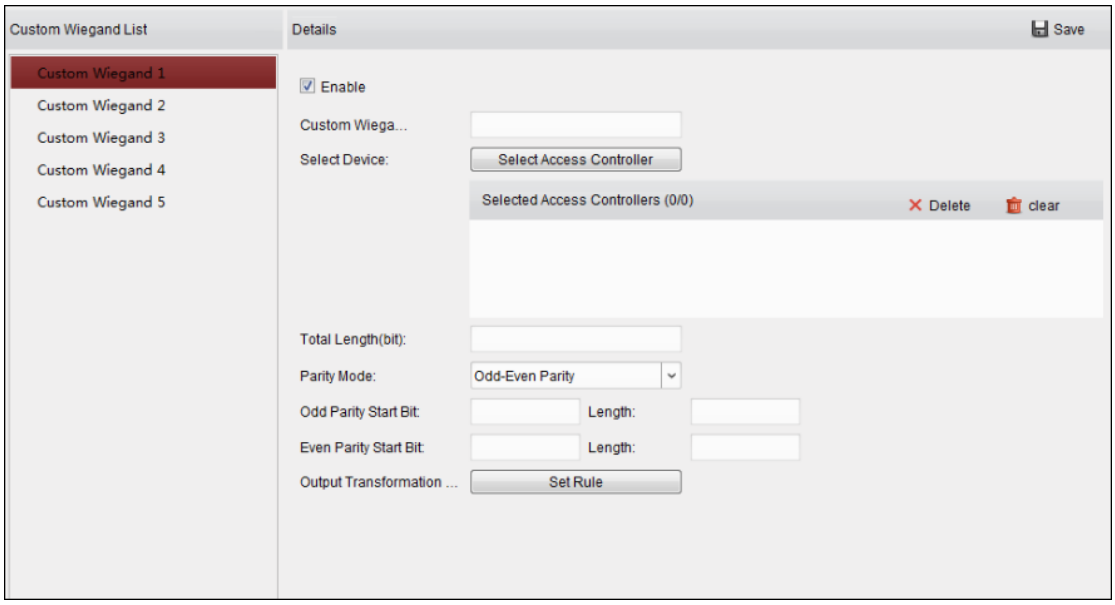
In base alla conoscenza della regola di caricamento per il wiegand di terze parti, è possibile impostare più protocolli wiegand personalizzati per comunicare tra il controller e i lettori di schede di terze parti.

Prima che inizi:

Collega i lettori di schede di terze parti al controller.

Passaggi:

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



2. Seleziona un wiegand personalizzato a sinistra dell'interfaccia.

3. Controlla **Abilitare** casella di controllo per abilitare il customwiegand.

4. Impostare il nome wiegand.

5. Selezionare il 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.

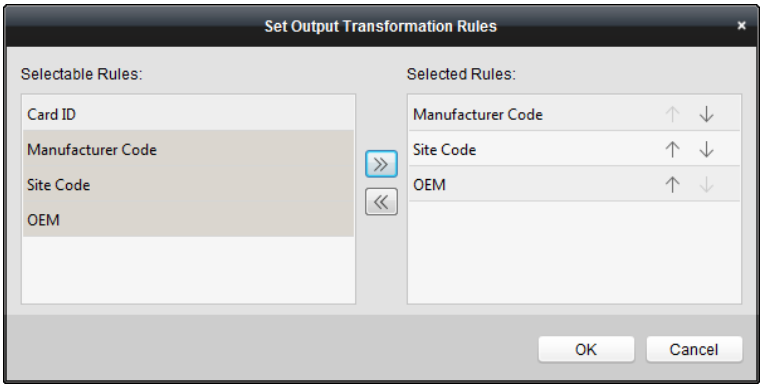
Se si seleziona Parità pari-dispari, è necessario impostare il bit di inizio della parità dispari, la lunghezza della parità dispari, il bit di inizio della parità pari e la lunghezza della parità pari.

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

Se si seleziona Nessuno, non è necessario impostare la modalità di parità.

7. Impostare la regola di trasformazione dell'output.

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



2) Selezionare le regole nell'elenco a sinistra.

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

3) Fare clic per spostare le regole selezionate nell'elenco a 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) Fare clic su **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 wiegand personalizzata.

Se il dispositivo abilita la funzione wiegand personalizzata, 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 della parità dispari, la lunghezza della parità dispari, il bit di inizio della parità pari e la lunghezza della parità pari vanno da 1 a 80 bit.

Il bit iniziale dell'ID della carta, il codice del produttore, il codice del sito e l'OEM dovrebbero essere compresi tra 1 e 80 bit.

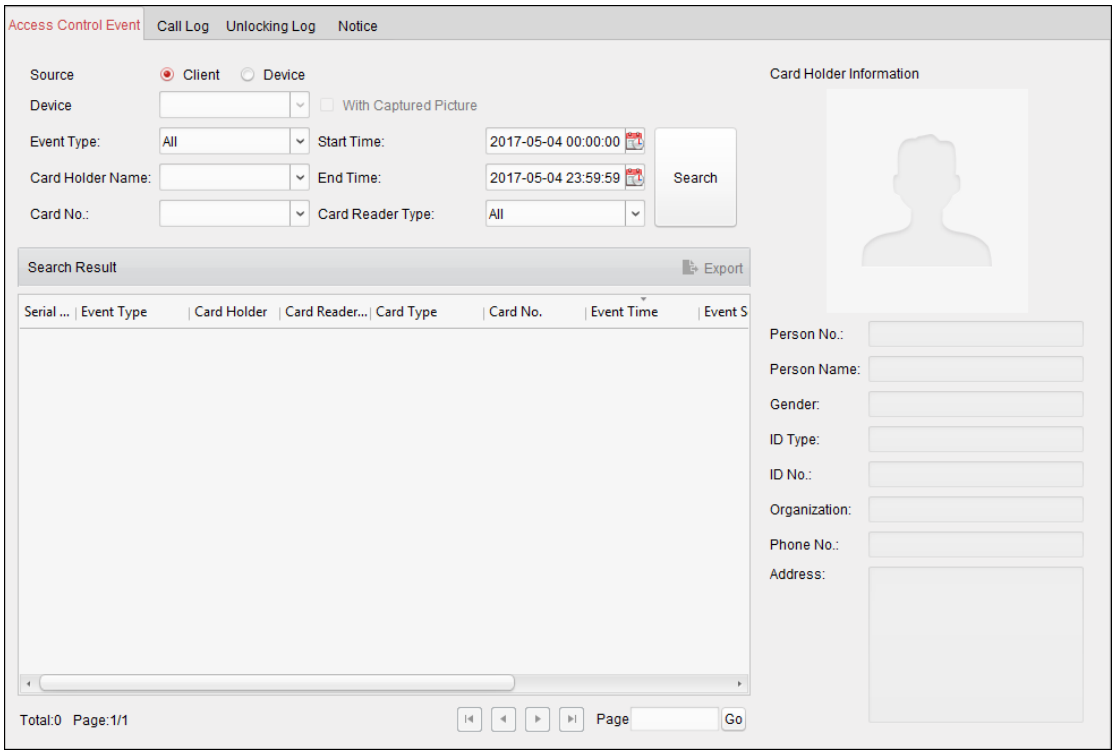
Per i dettagli sul wiegand personalizzato, vedere l'Appendice.

7.9 Ricerca di eventi di controllo degli accessi

Scopo:

È possibile cercare gli eventi della cronologia del controllo accessi, inclusi l'evento di eccezione del dispositivo, l'evento della porta, l'ingresso di allarme e l'evento del lettore di schede.

Fare clic  ona e fare clic sulla scheda Evento di controllo dell'accesso per accedere alla seguente interfaccia.



Passaggi:

1. Selezionare la fonte.

   Puoi selezionare Client o Dispositivo.

2. Immettere la condizione di ricerca (fonte, tipo di evento/nome del titolare della carta/n. carta/acquisizione/ora di inizio e fine).

3. Fare clic su **Ricerca** per ottenere i risultati della ricerca.

4. Visualizzare 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 su **Esportare** pulsante per esportare i risultati della ricerca sul PC locale.

7.10 Configurazione evento controllo accessi

Scopo:

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

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

7.10.1 Collegamento degli eventi di controllo degli accessi

Scopo:

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

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

Passaggi:

1. Fare clic su **Evento di controllo degli accessi** scheda.
2. I dispositivi di controllo dell'accesso aggiunti verranno visualizzati nel pannello Dispositivo di controllo dell'accesso a sinistra.
   Selezionare il dispositivo di controllo accessi, l'ingresso allarme o il punto di controllo accessi (porta) o il lettore di schede per configurare il collegamento dell'evento.
3. Selezionare il tipo di evento per impostare il collegamento.
4. Selezionare 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 degli accessi.*
6. Fare clic su **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 su cui copiare e fare clic su **ok** per confermare.

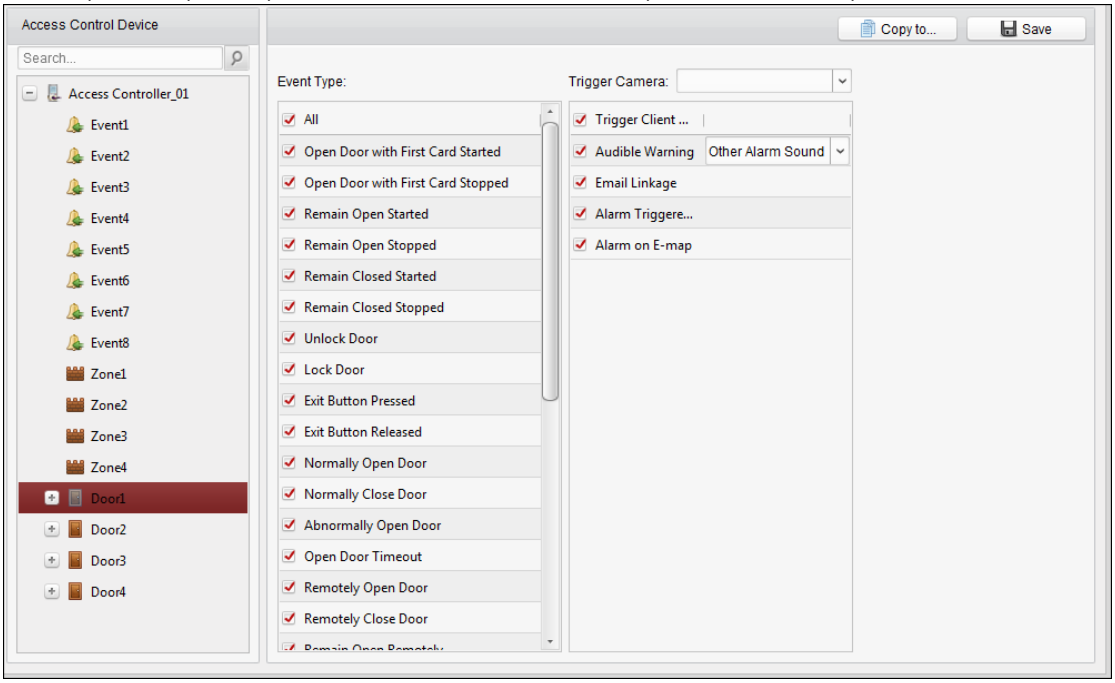


Tabella 1. 1 Azioni di collegamento per l'evento di controllo degli accessi

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 l'avviso
Collegamento e-mail	acustico. Invia una e-mail di notifica delle informazioni di allarme a uno o più destinatari.
Allarme su E-map	Visualizza le informazioni sull'allarme sulla mappa elettronica. ***Nota:*** Questo collegamento è disponibile solo per accedere al punto di controllo e all'ingresso allarme.

Allarme attivato **Immagine pop-up**	L'immagine con le informazioni sull'allarme viene visualizzata quando viene attivato l'allarme.

7.10.2 Collegamento ingresso allarme controllo accessi

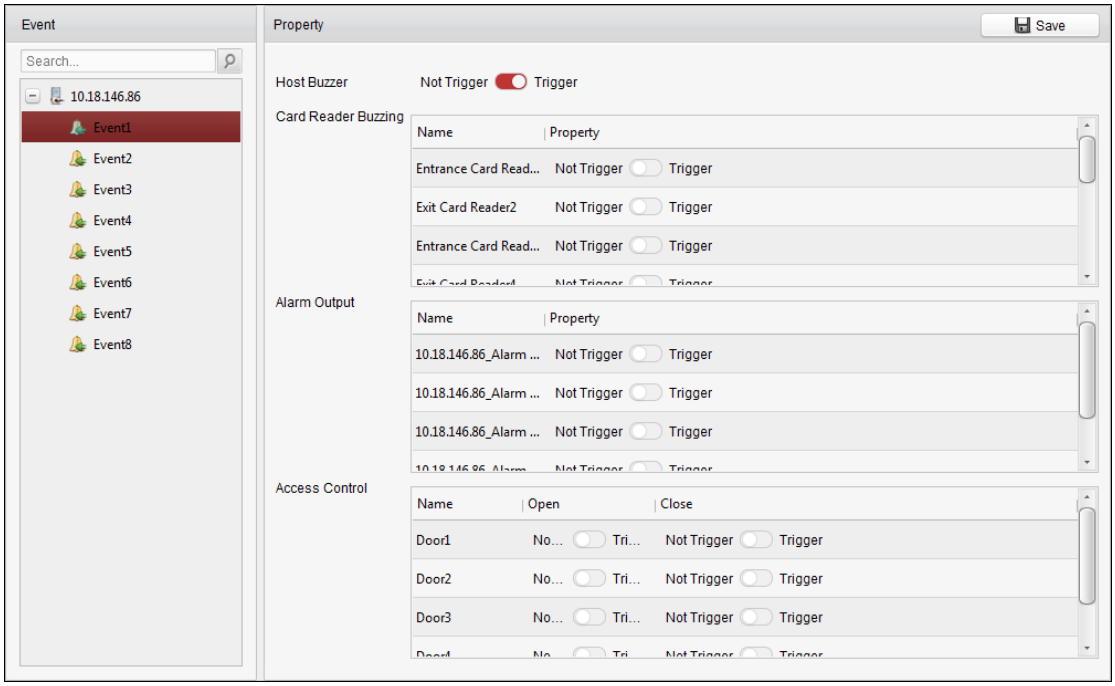
Scopo:

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

Nota: Il collegamento qui si riferisce al collegamento delle azioni 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 allarme.

3. Passare la proprietà da a per abilitare questa azione.

Cicalino ospite: Verrà attivato l'avviso acustico del controller.

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

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

Punto di controllo accessi (Apri/Chiudi): La porta sarà aperta o chiusa quando il caso viene attivato.

Nota: La Porta non può essere configurata come aperta o chiusa contemporaneamente.

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

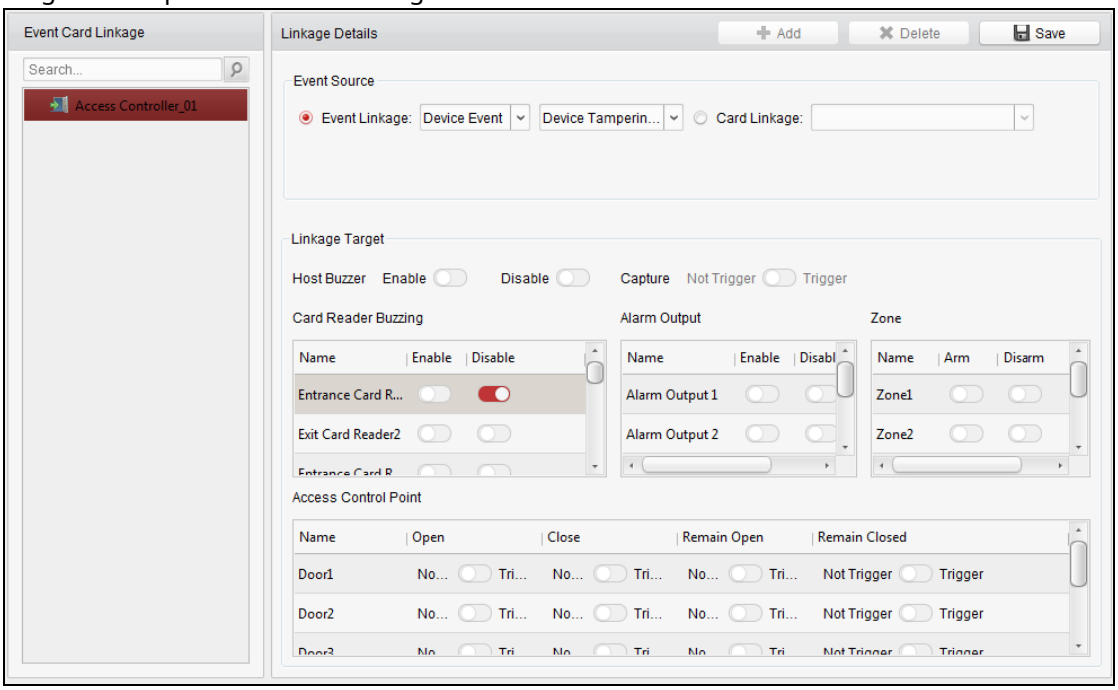
7.10.3 Collegamento della carta dell'evento

Clic **Collegamento della carta dell'evento** scheda per accedere alla seguente interfaccia.

Appunti:

Il collegamento della scheda evento dovrebbe essere supportato dal dispositivo.

Il collegamento qui si riferisce al collegamento delle azioni 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 eventi** o **Collegamento della carta.**

Collegamento eventi

Per il collegamento dell'evento, l'evento di allarme può essere suddiviso in quattro tipi: evento dispositivo, ingresso allarme, evento porta ed evento lettore di schede.

Passaggi:

1. Fare clic per selezionare il tipo di collegamento come **Collegamento di eventi,** e seleziona il tipo di evento dal menu a discesa elenco.

   Per Evento dispositivo, selezionare 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 carte, seleziona il tipo di evento dettagliato e seleziona il lettore di carte dalla tabella.

2. Imposta la destinazione del collegamento e cambia la proprietà da per  per abilitare questa funzione.

   Cicalino ospite: L'avviso acustico del controller sarà abilitato/disabilitato.

   Catturare: L'acquisizione in tempo reale sarà abilitata.

   Cicalino del lettore di schede: L'avviso acustico del lettore di carte sarà abilitato/disabilitato.

   Uscita allarme: L'uscita allarme sarà abilitata/disabilitata per la notifica.

   Zona: Inserire o disinserire la zona.

   Punto di controllo accessi: Verrà abilitato lo stato della porta aperta, chiusa, resta aperta e resta chiusa.

   Appunti:

Gli stati porta aperta, chiusa, resta aperta e resta chiusa non possono essere attivati 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 carta o selezionare la carta dall'elenco a discesa.
3. Selezionare il lettore di carte dalla tabella per l'attivazione.
4. Imposta la destinazione del collegamento e cambia la proprietà da per  per abilitare questa funzione.

   Cicalino ospite: L'avviso acustico del controller sarà abilitato/disabilitato.

   Catturare: L'acquisizione in tempo reale sarà abilitata.

   Cicalino del lettore di schede: L'avviso acustico del lettore di carte sarà abilitato/disabilitato.

   Uscita allarme: L'uscita allarme sarà abilitata/disabilitata per la notifica.

   Zona: Inserire o disinserire la zona.

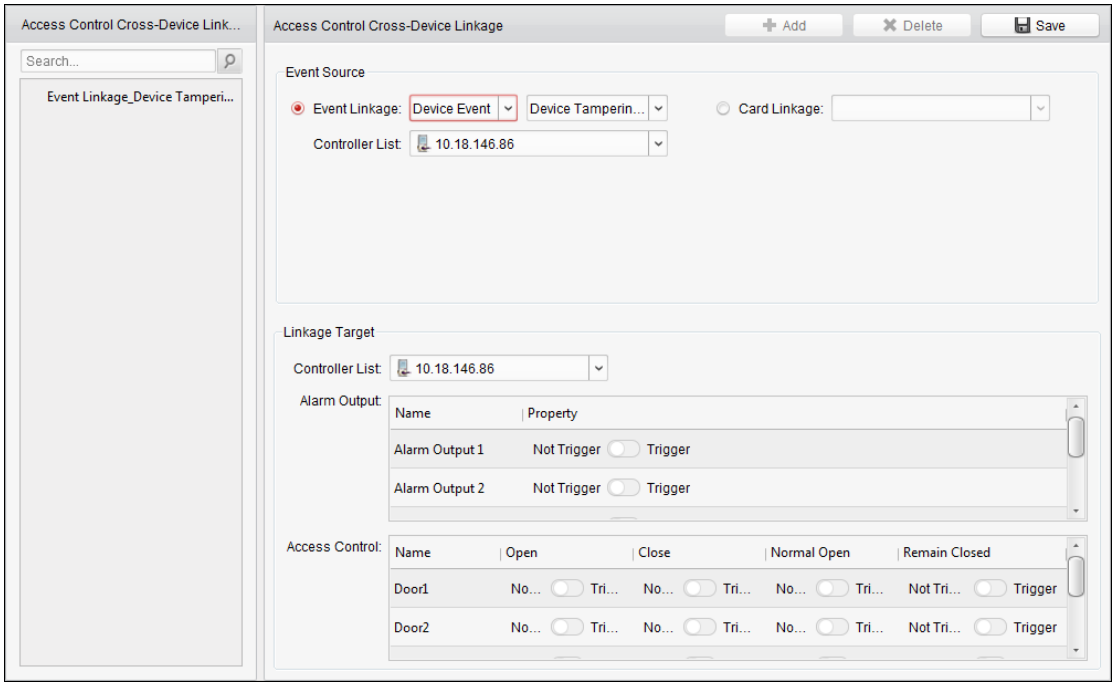
   Punto di controllo accessi: Verrà abilitato lo stato della porta aperta, chiusa, resta aperta e resta chiusa.
5. Fare clic su **Salva** pulsante per salvare e rendere effettivi i parametri.

7.10.4 Collegamento tra dispositivi

Scopo:

È possibile assegnare l'attivazione dell'azione di altri dispositivi di controllo accessi impostando una regola quando viene attivato l'evento di controllo accessi.

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 eventi** o **Collegamento della carta.**

Collegamento eventi

Per il collegamento dell'evento, l'evento di allarme può essere suddiviso in quattro tipi: evento dispositivo, ingresso allarme, evento porta ed evento lettore di schede.

Passaggi:

1. Fare clic per selezionare il tipo di collegamento come **Collegamento di eventi,** seleziona il dispositivo di controllo accessi come evento sorgente e selezionare il tipo di evento dall'elenco a discesa.

   Per Evento dispositivo, selezionare 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 carte, seleziona il tipo di evento dettagliato e seleziona il lettore di carte dalla tabella.

2. Impostare la destinazione del collegamento, selezionare il dispositivo di controllo dell'accesso dall'elenco a discesa come destinazione del collegamento e passare la proprietà da a per abilitare questa funzione.

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

   Punto di controllo accessi: Verrà attivato lo stato della porta aperta, chiusa, resta aperta e resta chiusa. ***Nota:*** Gli stati porta aperta, chiusa, resta aperta e resta chiusa non possono essere attivati 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 tessera dall'elenco a discesa e selezionare il dispositivo di controllo accessi come origine dell'evento.

3. Selezionare il lettore di carte 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 passare la proprietà da a per abilitare questa funzione.

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

5. Fare clic su **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:

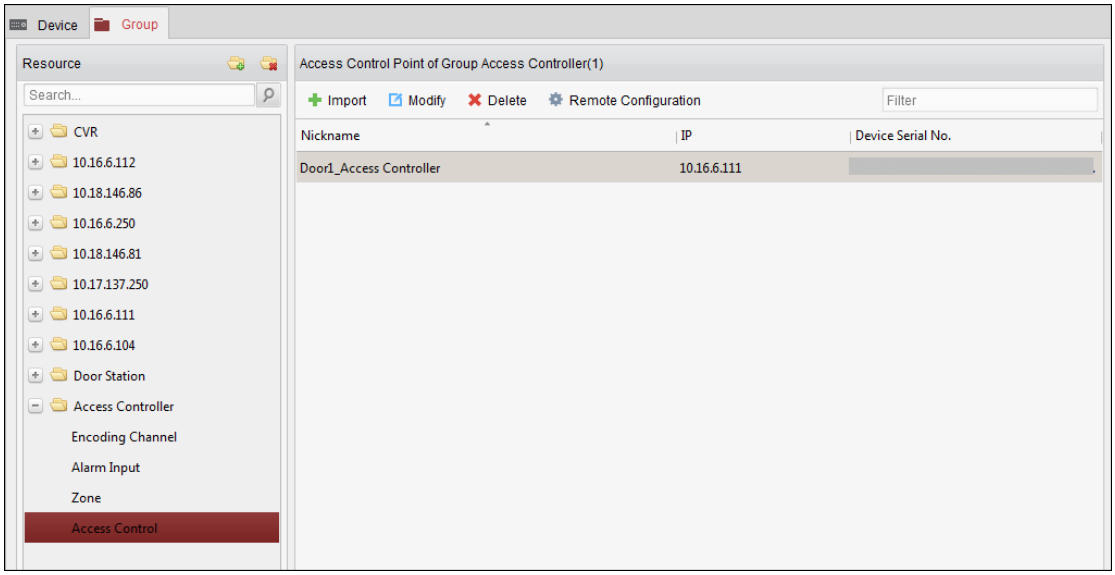
Prima di controllare lo stato della porta e impostare la durata dello stato, è necessario organizzarla in gruppi per una comoda gestione.

Eseguire i seguenti passaggi 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 i seguenti passaggi per aggiungere il gruppo.

   1) Fare clic 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 di

il nome del dispositivo selezionato.

4. Eseguire i seguenti passaggi per importare i punti di controllo accessi nel gruppo:

1) Fare clic su **Importare** nell'interfaccia di gestione del gruppo, quindi fare clic su **Controllo di accesso** scheda per aprire la pagina Import Access Control.

Appunti:

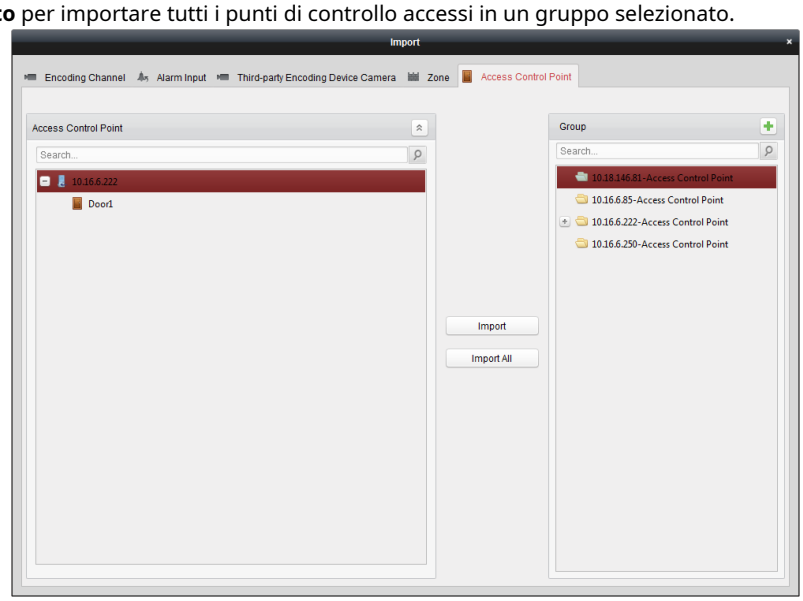
Puoi anche selezionare **Ingresso allarme** scheda e importare gli ingressi di allarme nel gruppo.

Per il terminale di controllo accessi video, è possibile aggiungere le telecamere come canale di codifica al gruppo.

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

3) Selezionare un gruppo dall'elenco dei gruppi.

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



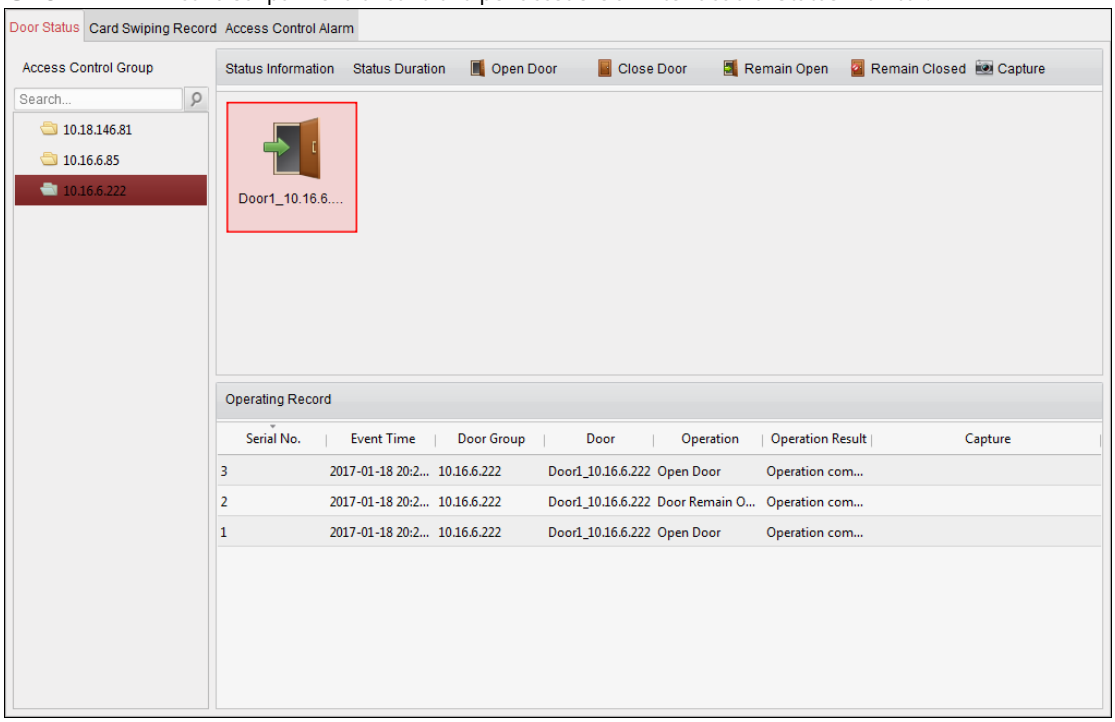
5. Dopo aver importato i punti di controllo accessi nel gruppo, è possibile fare clic sul nome o fai doppio clic su del gruppo/punto di controllo accessi per modificarlo.

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

Scopo:

È possibile controllare lo stato di un singolo punto di controllo degli accessi (una porta), inclusi apertura porta, chiusura porta, apertura e chiusura.

Clic  icona 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 del gruppo di controllo degli accessi.*
2. I punti di controllo accessi del gruppo di controllo accessi selezionato verranno visualizzati sulla destra.

   Fare clic sull'icona  nel pannello Informazioni sullo stato per selezionare una porta.
3. Fare clic sul seguente pulsante elencato sul **Informazioni sullo stato** pannello per il controllo della porta.

   Open Door: fare clic per aprire la porta una volta. :

   Close Door fare clic per chiudere la porta una volta. :

   Remain Open fare clic per tenere aperta la porta.

   Remain Closed: fare clic per tenere chiusa la porta.

   Capture: fare clic per acquisire manualmente l'immagine.
4. È possibile visualizzare il risultato dell'operazione anti-controllo nel pannello Registro operazioni.

Appunti:

Se selezioni lo stato come **Rimanere aperto/rimanere chiuso,** la porta resterà aperta/chiusa fino a quando non verrà effettuato un nuovo comando di anticontrollo.

Il **Catturare** è disponibile quando il dispositivo supporta la funzione di acquisizione. E non può essere realizzato finché il server di archiviazione non è configurato.

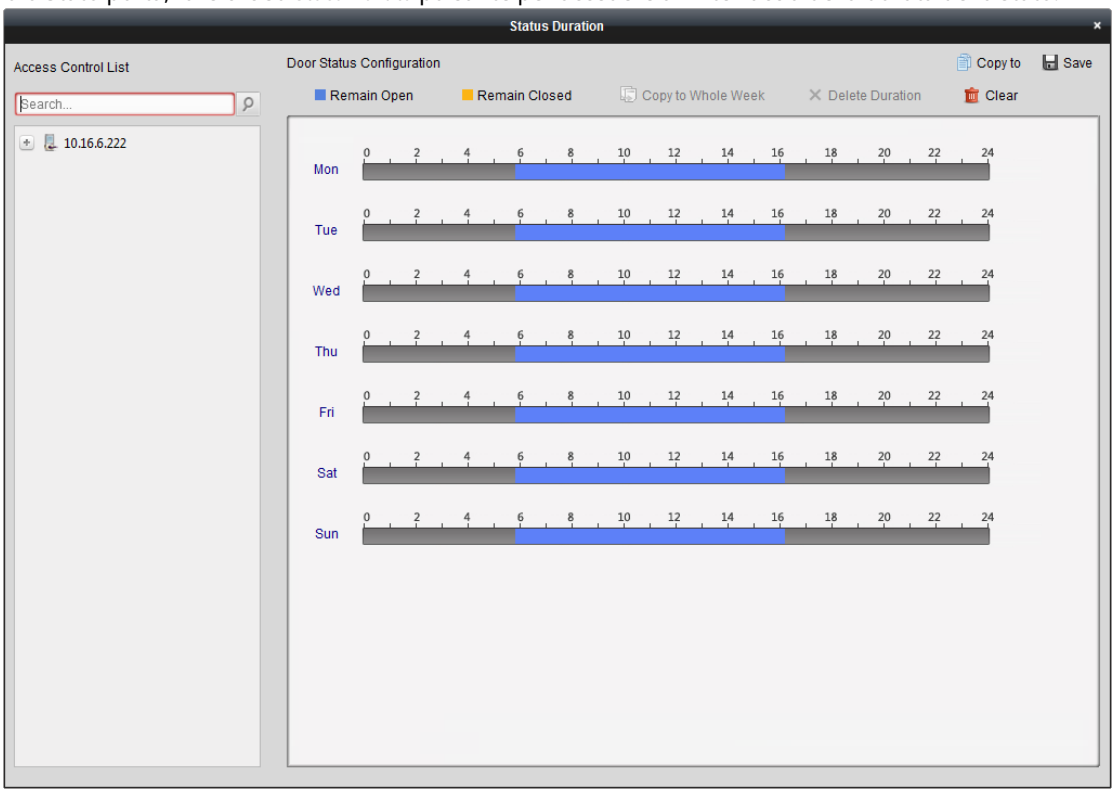
Se la porta è in stato di rimanere chiusa, solo la super card può aprire la porta o aprire la porta tramite il software client.

7.11.3 Stato Durata Configurazione

Scopo:

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

Nel modulo Stato porta, fare clic su **Stato Durata** pulsante 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 un programma per la porta selezionata.
   1) Selezionare un pennello stato porta come o .

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

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

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

3) Quando il cursore si sposta su , puoi spostare la barra del tempo selezionata che hai appena modificato. Puoi modificare anche il punto temporale visualizzato per impostare il periodo di tempo preciso. Quando il cursore si sposta su , è possibile 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 le impostazioni della barra temporale negli altri giorni della settimana.

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

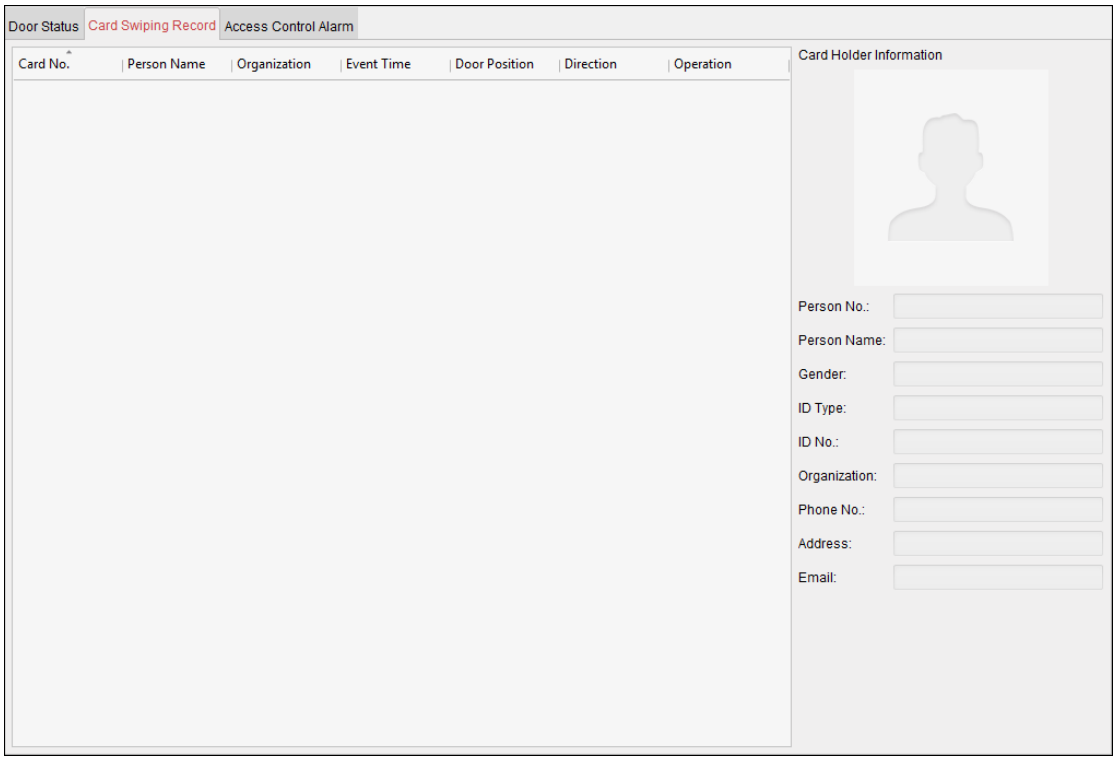
   Oppure puoi cliccare**Chiaro** per cancellare tutte le durate configurate nella pianificazione.

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

6. Puoi fare clic su **Copia a** pulsante per copiare il programma su altre porte.

7.11.4 Registrazione dello scorrimento delle carte in tempo reale

Clic **Registrazione dello scorrimento della carta** scheda per accedere alla seguente interfaccia.



I registri dei record 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, incluso il numero della carta, il nome della persona, l'organizzazione, l'ora dell'evento, ecc.

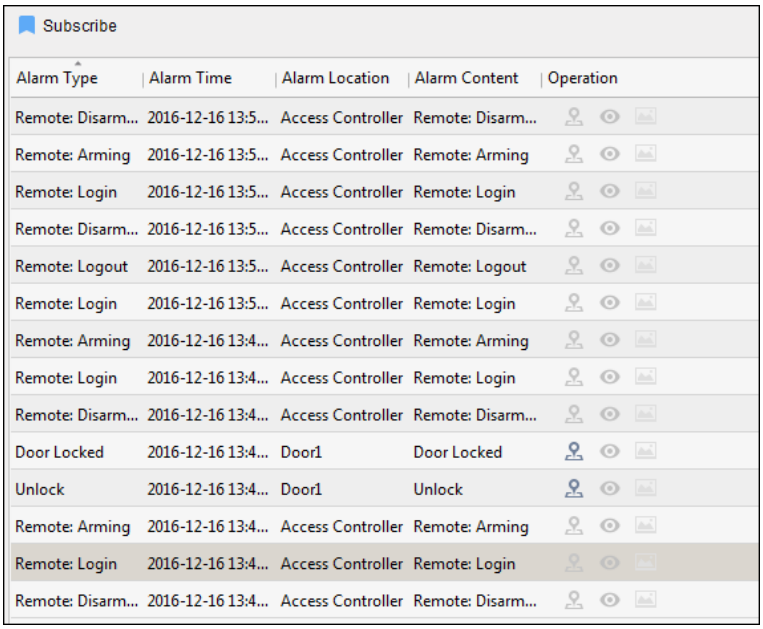
Puoi anche fare clic sull'evento per visualizzare i dettagli del titolare della carta, incluso il numero della persona, il nome della persona, l'organizzazione, il telefono, l'indirizzo di contatto, ecc.

7.11.5 Allarme controllo accessi in tempo reale

Scopo:

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

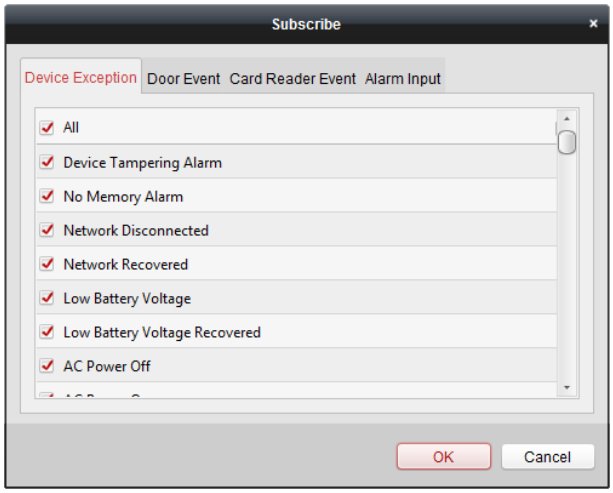
Clic **Allarme controllo accessi** scheda per accedere alla seguente interfaccia.



Passaggi:

1. Tutti gli allarmi di controllo accessi verranno visualizzati nell'elenco in tempo reale. È possibile visualizzare il tipo di sveglia, l'ora della sveglia, la posizione, ecc.
2. Fare clic per visualizzare l'allarme su E-map.
3. È possibile fare clic su o per visualizzare la vista dal vivo 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 degli eventi di controllo degli accessi.*
4. Fare clic su **sottoscrivi** per selezionare l'allarme che il client può ricevere quando viene attivato l'allarme.



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

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

7.12 Controllo inserimento

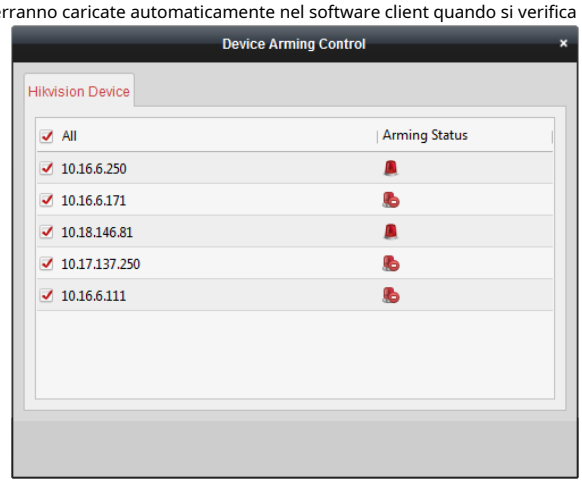
Scopo:

Puoi armare o disarmare il dispositivo. Dopo aver armato il dispositivo, il client può ricevere le informazioni di allarme dal dispositivo.

Passaggi:

1. Fare clic su **Strumento->Controllo inserimento dispositivo** per far apparire 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 Prompt sonoro e indicatore

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

Durante l'utilizzo del lettore di schede, invierà diversi suoni di richiesta 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

Avviso sonoro	Descrizione
Un bip	Protocollo RS-485: premendo i tasti viene richiesto; Richiesta di scorrimento della carta; Richiesta di timeout per la pressione dei tasti o lo scorrimento della carta. Protocollo Wiegand: premendo i tasti viene richiesto; Richiesta di scorrimento della
Due segnali acustici rapidi	carta. L'operazione di pressione dei tasti o scorrimento della tessera è valida.
Tre beep lenti	L'operazione di pressione dei tasti o scorrimento della carta non è valida.
Rapidamente continuo beep	Allarme antimanomissione.
Lentamente continuo beep	Il lettore di schede non è crittografato.

Tabella 7-2 Descrizione dell'indicatore LED

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

Appendice B Regola CustomWiegand Descrizioni

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

Nome Wiegand personalizzato:	Wiegand 44					
Lunghezza totale	44					
Trasformazione Regola (Decimale cifra)	perFormatRule[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 carta Bit di inizio	0	Lunghezza	32	Cifra decimale	10	
Codice sito Bit di inizio		Lunghezza		Cifra decimale		
OEM Bit di inizio		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 Carta e Codice Produttore. I dati validi possono essere una regola singola 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 della 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, il sistema avvierà 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 Parità XOR, 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. Ciò 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 tessera, lunghezza e cifra decimale: Se utilizzi la regola di trasformazione, questi elementi sono disponibili. A seconda della tabella visualizzata sopra, il bit iniziale dell'ID della carta 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 carta. (La lunghezza qui è calcolata in bit.) E la lunghezza della cifra decimale è di 10 bit.

Bit di inizio del codice 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.

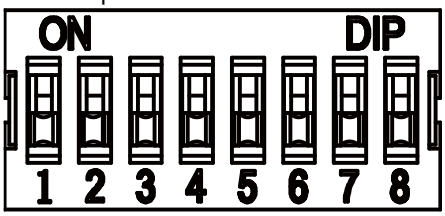
Bit di inizio OEM, lunghezza e cifra decimale: Se utilizzi la regola di trasformazione, questi elementi sono disponibili. Per informazioni dettagliate, vedere la spiegazione dell'ID della carta.

Bit di inizio del codice del produttore, lunghezza e cifra decimale: Se usi la regola di trasformazione, questi elementi sono

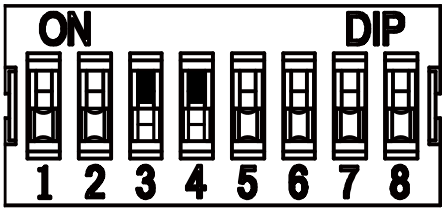
a disposizione. A seconda della tabella visualizzata sopra, il bit di inizio del codice del produttore è 32, la lunghezza è 8 e la cifra decimale è 3. Rappresenta che dal bit 32, ci sono 8 bit per il codice del produttore. (La lunghezza qui è calcolata in bit.) E la lunghezza decimale è 3.

Appendice C Descrizione del DIP Switch

Ci sono due gruppi di DIP switch sulla scheda di controllo della corsia principale. Prendiamo come esempio il DIP switch a 8 bit; Dal n.1 al n.8 va dal bit basso a quello alto.



Quando l'interruttore è verso ON, significa che l'interruttore è abilitato, altrimenti l'interruttore è spento.
Se si imposta l'interruttore DIP come nella figura mostrata di seguito, il suo valore binario è 00001100 e il suo valore decimale è 12.



020000001080620


See Far, Go Further