Terminale di controllo accessi video

Manuale dell'utente

Manuale dell'utente

 Questo manuale si riferisce al terminale di controllo accessi video.

Serie	Modello
Terminale di controllo accessi video	DS-K1T501SF

Contiene istruzioni su come utilizzare il prodotto. Il software integrato nel prodotto è regolato dal contratto di licenza con l'utente relativo al prodotto stesso.

Informazioni sul presente manuale

Esclusione di responsabilità

NELLA MISURA MASSIMA CONSENTITA DALLA LEGGE APPLICABILE, HIKVISION NON RILASCIA ALCUNA GARANZIA, ESPRESSA O IMPLICITA, COMPRESE, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO PARTICOLARE, RELATIVAMENTE AL PRESENTE MANUALE. HIKVISION NON ASSICURA, GARANTISCE NÉ DICHIARA ALCUNCHÉ IN RELAZIONE ALL'USO DEL MANUALE O ALLA CORRETTEZZA, ALLA PRECISIONE O ALL'AFFIDABILITÀ DELLE INFORMAZIONI IVI CONTENUTE. L'UTILIZZO DEL PRESENTE MANUALE E L'EVENTUALE AFFIDAMENTO SU DI ESSO SONO INTERAMENTE A RISCHIO DELL'UTENTE E RIENTRANO NELLA SUA RESPONSABILITÀ.

IN RIFERIMENTO AI PRODOTTI CON ACCESSO A INTERNET, L'USO DEGLI STESSI È DA CONSIDERARSI TOTALMENTE A RISCHIO DELL'UTENTE. LA NOSTRA AZIENDA NON SI ASSUME ALCUNA RESPONSABILITÀ IN CASO DI FUNZIONAMENTO ANOMALO, VIOLAZIONI DELLA RISERVATEZZA, O ALTRI DANNI DERIVANTI DA ATTACCHI INFORMATICI, ATTACCHI DI HACKER, INFEZIONE DA VIRUS O ALTRI RISCHI LEGATI ALLA SICUREZZA SU INTERNET; IN OGNI CASO, L'AZIENDA FORNIRÀ TEMPESTIVO SUPPORTO TECNICO OVE NECESSARIO.

LE NORMATIVE CONCERNENTI LA SORVEGLIANZA VARIANO DA UNA GIURISDIZIONE ALL'ALTRA. VERIFICARE TUTTE LE NORMATIVE APPLICABILI NELLA PROPRIA GIURISDIZIONE PRIMA DI UTILIZZARE IL PRESENTE PRODOTTO IN MODO DA GARANTIRE CHE L'USO SIA CONFORME ALLA LEGGE VIGENTE. LA NOSTRA AZIENDA NON SARÀ RESPONSABILE NEL CASO IN CUI IL PRESENTE PRODOTTO SIA UTILIZZATO PER FINI ILLECITI.

IN CASO DI CONFLITTO TRA IL PRESENTE MANUALE E LA LEGGE VIGENTE, PREVARRÀ QUEST'ULTIMA. **Supporto**

In caso di domande, contattare il rivenditore locale. **Protezione dei dati**

Durante l'utilizzo del dispositivo, saranno raccolti, archiviati ed elaborati dati personali. Per proteggere i dati, sviluppiamo i dispositivi Hikvision applicando i principi della protezione dei dati fin dalla progettazione. Ad esempio, nel caso dei dispositivi con funzioni di riconoscimento facciale, i dati biometrici memorizzati nel dispositivo dell'utente vengono crittografati, mentre i dispositivi di lettura delle impronte digitali salvano solo il modello dell'impronta digitale, il che rende impossibile la ricostruzione di un'immagine dell'impronta stessa.

Ai responsabili del trattamento dei dati, si richiede di intraprendere azioni per la raccolta, l'archiviazione, l'elaborazione e il trasferimento dei dati in conformità alle leggi e ai regolamenti applicabili in materia di protezione dei dati, inclusi, senza limitazioni, implementazione di controlli di sicurezza per salvaguardare i dati personali, ad es. controlli di sicurezza amministrativi e fisici ragionevoli, nonché condurre revisioni e valutazioni periodiche dell'efficacia dei suddetti controlli di sicurezza.

Informazioni sulle normative

Informazioni sulle norme FCC

Tenere presente che modifiche o alterazioni non espressamente approvate dalla parte responsabile della conformità potrebbero invalidare l'autorità dell'utente ad utilizzare l'apparecchiatura.

Conformità alle norme FCC: la presente apparecchiatura è stata sottoposta a test e dichiarata conforme ai limiti stabiliti per i dispositivi digitali di Classe B, in conformità alla Parte 15 delle Norme FCC. Questi limiti sono pensati per fornire una ragionevole protezione contro le interferenze dannose in installazioni residenziali. Questo dispositivo genera, utilizza e può emettere energia a radiofrequenza e, se non installato e utilizzato in conformità alle istruzioni, può causare interferenze dannose alle comunicazioni radio. Tuttavia, non esistono garanzie che l'interferenza non si verifichi in una particolare installazione. Se l'apparecchio provoca interferenze dannose alle ricezioni radiotelevisive, riscontrabili spegnendo e accendendo l'apparecchio, si consiglia di provare a correggerle adottando uno o più dei seguenti accorgimenti:

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

Installare e utilizzare l'apparecchiatura mantenendo una distanza di almeno 20 cm tra il radiatore e il proprio corpo.

Norme FCC

Questo dispositivo è conforme alla parte 15 delle norme FCC. L'utilizzo è soggetto alle due condizioni seguenti:

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

Dichiarazione di Conformità UE

Questo prodotto e gli eventuali accessori in dotazione sono contrassegnati con il marchio "CE" e sono quindi conformi alle norme europee armonizzate vigenti di cui alla Direttiva 2014/53/UE sulle apparecchiature radio, alla Direttiva sulla compatibilità elettromagnetica CEM 2014/30/UE e alla Direttiva RoHS 2011/65/UE.

2012/19/UE (Direttiva RAEE): i prodotti contrassegnati con il presente simbolo non possono essere smaltiti come rifiuti municipali indifferenziati nell'Unione Europea. Per garantire un riciclaggio adeguato, restituire il presente prodotto al proprio rivenditore locale in occasione dell'acquisto di una nuova apparecchiatura equivalente, oppure smaltirlo nei punti di raccolta designati. Per ulteriori informazioni, visitare: www.recyclethis.info

2006/66/CE (Direttiva sulle batterie): questo prodotto contiene una batteria e non è possibile smaltirlo con i rifiuti municipali indifferenziati nell'Unione Europea. Fare riferimento alla documentazione del prodotto per le informazioni specifiche sulla batteria. La batteria è contrassegnata con il presente simbolo, che potrebbe includere le sigle di cadmio (Cd), piombo (Pb) o mercurio (Hg). Per garantire un riciclaggio adeguato, consegnare la batteria al proprio rivenditore locale oppure smaltirla nei punti di raccolta designati. Per ulteriori informazioni, visitare: www.recyclethis.info

Conformità alla normativa canadese ICES-003

Il presente dispositivo soddisfa i requisiti degli standard CAN ICES-3 (B)/NMB-3(B).

Questo dispositivo è conforme agli standard RSS di Industry Canada per i dispositivi esenti da licenza. L'utilizzo è soggetto alle due condizioni seguenti:

(1) Il dispositivo non deve causare interferenze e

(2) deve accettare qualsiasi interferenza, incluse le interferenze che possono causare un funzionamento indesiderato del dispositivo.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Ai sensi delle normative di Industry Canada, questo trasmettitore radio può funzionare solo utilizzando un'antenna di tipo e guadagno massimo (o inferiore) approvati per il trasmettitore da Industry Canada. Per ridurre le potenziali interferenze radio nei confronti di altri utenti, il tipo di antenna e il relativo guadagno devono essere scelti in modo che la potenza isotropica irradiata equivalente (EIRP) non sia superiore a quella necessaria per una comunicazione corretta.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Installare e utilizzare l'apparecchiatura mantenendo una distanza di almeno 20 cm tra il radiatore e il proprio corpo.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Utilizzare solo gli alimentatori indicati nel presente manuale:

Modello	Produttore	Standard
DSA-12PFT-12FUK 120100	Dee Van Enterprise Co., Ltd.	BS
DSA-12PFT-12FAU 120100	Dee Van Enterprise Co., Ltd.	AS
DSA-12PFT-12FIN 120100	Dee Van Enterprise Co., Ltd.	IS
DSA-12PFT-12FUS 120100	Dee Van Enterprise Co., Ltd.	IEC
DSA-12PFT-12 FBZ 120100	Dee Van Enterprise Co., Ltd.	NBR

Istruzioni di sicurezza

Le presenti istruzioni servono a garantire che l'utente possa utilizzare il prodotto correttamente, evitando pericoli e danni alla proprietà.

Le misure precauzionali sono indicate con le diciture "**Avvertenze**" e "**Attenzione**":

Avvertenze: ignorare le avvertenze può causare lesioni gravi o mortali.

Attenzione: ignorare le precauzioni può causare lesioni alle persone o danni all'apparecchiatura.

	
Avvertenze Seguire queste misure di sicurezza per evitare lesioni gravi o mortali.	**Attenzione** Seguire queste precauzioni per evitare lesioni alle persone o danni materiali.

 **Avvertenze**

- Tutte le operazioni elettroniche devono essere rigorosamente conformi alle disposizioni sulla sicurezza elettrica e sulla prevenzione degli incendi e a qualsiasi altra disposizione locale in materia.
- Utilizzare solo alimentatori forniti da produttori affidabili. La potenza nominale non può essere inferiore al valore indicato.
- Non collegare più dispositivi ad un unico adattatore di corrente, in quanto il sovraccarico potrebbe provocarne il surriscaldamento o causare un incendio.
- Accertarsi che la corrente sia stata scollegata prima di effettuare il cablaggio, installare o smontare il dispositivo.
- Fissare saldamente il prodotto se lo si installa su una parete o al soffitto.
- Se il dispositivo emana fumo, odori o rumori, spegnere l'alimentazione e scollegare il cavo di alimentazione, quindi rivolgersi al centro assistenza.
- Se il prodotto non funziona correttamente, rivolgersi al rivenditore o al centro di assistenza più vicino. Non cercare di smontare il dispositivo da soli. Non ci assumiamo alcuna responsabilità in relazione a problemi causati da interventi non autorizzati di riparazione o manutenzione.

Attenzione

- Non far cadere il dispositivo, non sottoporlo a urti e non esporlo a forti radiazioni elettromagnetiche. Evitare di installare il dispositivo su superfici vibranti o in luoghi a rischio di impatti (ignorare questa precauzione può causare danni all'apparecchiatura).
- Non mettere il dispositivo in luoghi troppo caldi (fare riferimento alle specifiche tecniche per informazioni dettagliate sulle temperature di funzionamento), freddi, polverosi o umidi e non esporlo a forti radiazioni elettromagnetiche.
- Tenere il coperchio del dispositivo per l'uso in ambienti chiusi lontano da pioggia e umidità.
- Per evitare il pericolo di incendio, non collocare l'apparecchio alla luce diretta del sole, in luoghi poco ventilati o vicino a fonti di calore.
- Non collocare il dispositivo al sole o in luoghi molto luminosi. Ciò potrebbe causare uno sbiadimento o la formazione di macchie (che tuttavia non sono segni di malfunzionamento) e avere effetti sulla durata del sensore.
- Utilizzare il guanto in dotazione per aprire il coperchio del dispositivo ed evitare il contatto diretto con il coperchio, in quanto l'acido contenuto nel sudore delle dita può corroderne il rivestimento.
- Pulire le superfici interne ed esterne del coperchio con un panno morbido e asciutto. Non utilizzare detergenti alcalini.
- Conservare il materiale d'imballaggio per un eventuale uso futuro. In caso di guasti, sarà necessario inviare il dispositivo al sito di produzione con l'imballaggio originale. Il trasporto senza l'imballaggio originale potrebbe causare danni al dispositivo e ulteriori costi.
- L'uso improprio o la sostituzione della batteria eseguita in modo non corretto possono provocare esplosioni. Sostituirla soltanto con una batteria dello stesso tipo o equivalente. Smaltire le batterie esaurite conformemente alle istruzioni fornite dal produttore della batteria.
- Custodire la propria tessera e segnalarne tempestivamente la perdita in caso di smarrimento.
- Se si desidera un maggiore livello di sicurezza, utilizzare più modalità di autenticazione.
- Sono supportati più tipi di tessere. Selezionare un tipo di tessera appropriato in base alle prestazioni della tessera e agli scenari di utilizzo.

Sommario

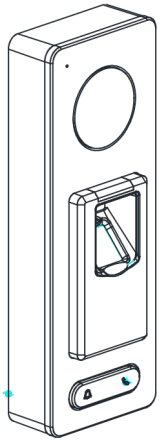
Capitolo 1 Panoramica 10
1.1 Introduzione 10
1.2 Funzioni principali 10
Capitolo 2 Aspetto 11
2.1 Aspetto del modello DS-K1T501SF 11
2.2 Connettore del terminale di controllo accessi video 12
Capitolo 3 Installazione 13
Capitolo 4 Collegamento dei terminali 14
Capitolo 5 Descrizione del cablaggio 16
5.1 Panoramica del cablaggio del dispositivo esterno 16
5.2 Cablaggio del lettore di tessere RS-485 esterno 17
5.3 Connessione del lettore di tessere 17
5.3.1 Cablaggio del lettore Wiegand 18
5.3.2 Cablaggio dell'uscita RS-485 19
Capitolo 6 Attivazione del terminale di controllo accessi 20
6.1 Attivazione tramite il software SADP 20
6.2 Attivazione tramite il software client 21
Capitolo 7 Funzionamento del client 24
7.1 Modulo Function 24
7.2 Registrazione e accesso utenti 28
7.3 Configurazione del sistema 29
7.4 Gestione del controllo degli accessi 30
7.4.1 Aggiunta di un dispositivo di controllo accessi 32
7.4.2 Visualizzazione dello stato del dispositivo 47
7.4.3 Modifica delle informazioni di base 48
7.4.4 Impostazioni di rete 48
7.4.5 Impostazioni di acquisizione 51
7.4.6 Impostazioni dei parametri RS-485 53
7.4.7 Configurazione remota 54
7.5 Gestione dell'organizzazione 67
7.5.1 Aggiunta di organizzazioni 68
7.5.2 Modifica ed eliminazione di organizzazioni 68
7.6 Gestione delle persone 68
7.6.1 Aggiunta di persone 68

7.6.2 Gestione di persone 76
7.6.3 Emissione di tessere in batch 77
7.7 Pianificazioni e modelli 79
7.7.1 Pianificazione settimanale 80
7.7.2 Gruppi di ferie 81
7.7.3 Modelli 82
7.8 Configurazione delle autorizzazioni 85
7.8.1 Aggiunta delle autorizzazioni 85
7.8.2 Applicazione delle autorizzazioni 86
7.9 Funzioni avanzate 87
7.9.1 Parametri di controllo accessi 88
7.9.2 Autenticazione del lettore di tessere 91
7.9.3 Autenticazione multipla 92
7.9.4 Apertura delle porte con la prima tessera 95
7.9.5 Anti-passback 97
7.10 Ricerca di eventi di controllo accessi 98
7.10.1 Ricerca di eventi locali di controllo accessi 99
7.10.2 Ricerca di eventi remoti di controllo accessi 99
7.11 Configurazione degli eventi di controllo accessi 99
7.11.1 Collegamento di eventi di controllo accessi 100
7.11.2 Collegamento di eventi delle tessere 102
7.11.3 Collegamenti tra dispositivi 104
7.12 Gestione dello stato delle porte 105
7.12.1 Gestione dei gruppi di controllo accessi 105
7.12.2 Controllo opposto dei punti di controllo accessi (porte) 107
7.12.3 Configurazione della durata dello stato 108
7.12.4 Record di passaggio delle tessere in tempo reale 110
7.12.5 Allarmi di controllo accessi in tempo reale 111
7.13 Controllo dell'attivazione 112
7.14 Impostazioni della visualizzazione dal vivo e della riproduzione 112
7.15 Visualizzazione dal vivo 114
7.15.1 Avvio e interruzione della visualizzazione dal vivo 117
7.15.2 Registrazione e acquisizione manuale 120
7.15.3 Riproduzione istantanea 123
7.15.4 Suddivisione personalizzata della finestra 125
7.15.5 Altre funzioni nella visualizzazione dal vivo 126

7.16 Riproduzione remota 127
7.16.1 Memorizzazione sui dispositivi di archiviazione 127
7.16.2 Riproduzione normale 130
7.16.3 Riproduzione di eventi 137
Appendice A Suggerimenti per la scansione delle impronte digitali 140
Appendice B Introduzione al DIP switch 141
Appendice C Descrizione dell'indicatore e dell'avvisatore acustico 142

Capitolo 1 Panoramica

1.1 Introduzione



DS-K1T501SF è un modello di terminale di controllo accessi video dotato di diverse tecnologia avanzate, quali riconoscimento delle impronte digitali, riconoscimento dei volti, Wi-Fi, riconoscimento delle smart card e telecamera HD (2 MP opzionale). Dispone inoltre di un modulo per il riconoscimento delle impronte digitali (con supporto delle modalità 1:1 e 1:N) e funzionamento offline.

1.2 Funzioni principali

- Modalità di trasmissione con rete cablata (TCP/TP), Wi-Fi, RS-485 e Wiegand
- Funzioni di riconoscimento dei volti e acquisizione delle immagini implementate tramite telecamera integrata (2 MP opzionale)
- Supporta la comunicazione con standard RS-485 per il collegamento di lettori di tessere esterni
- Può essere utilizzato come lettore di tessere e supporta le interfacce Wiegand e RS-485 per l'accesso al controller
- Supporta il protocollo EHome
- Memorizzazione: max 50.000 tessere, max 200.000 record di eventi di controllo accessi e max 3000 impronte digitali
- Adotta un modulo per le impronte digitali, che supporta la modalità 1:N (impronta digitale, tessera + impronta digitale) e la modalità 1:1 (tessera + impronta digitale)
- Supporta più modalità di autenticazione, quali tessera, impronta digitale, tessera + impronta digitale, tessera + password, impronta digitale + password, tessera + impronta digitale + password, ecc.
- Supporta la lettura di tessere Mifare/codici QR
- Rilevamento delle manomissioni, allarme durata eccessiva sblocco, allarme numero eccessivo di passaggi di tessera non valida, allarme tessera di coercizione, ecc.
- Supporta la connessione dell'unità di controllo della porta protetta
- Livello di protezione: IP65
- I dati possono essere salvati in modo permanente dopo lo spegnimento

Capitolo 2 Aspetto

2.1 Aspetto del modello DS-K1T501SF

Fare riferimento al contenuto seguente per informazioni dettagliate sul modello DS-K1T501SF.

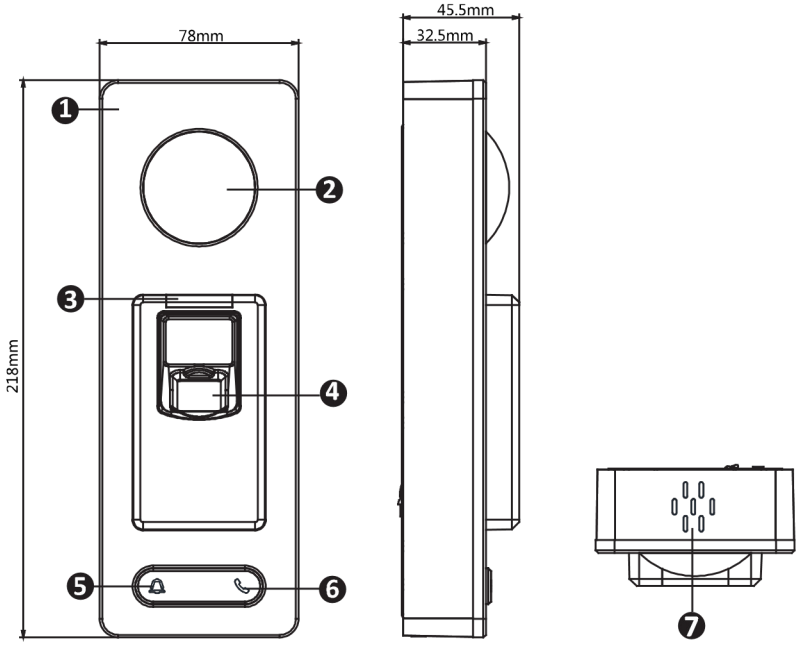
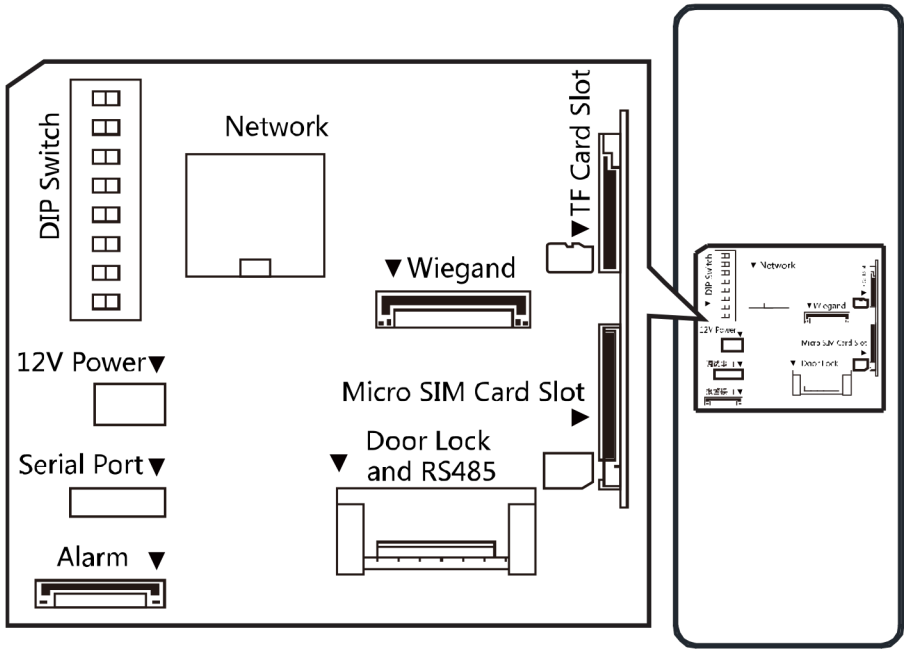


Tabella 2-1 Descrizione del modello serie DS-K1T501SF

N.	Descrizione
1	Microfono
2	Telecamera
3	Indicatore LED
4	Area scanner di impronte digitali e passaggio della tessera
5	Pulsante del campanello
6	Pulsante Voce
7	Altoparlante

2.2 Connettore del terminale di controllo accessi video

Il connettore del terminale di controllo accessi video è il seguente:



Capitolo 3 Installazione

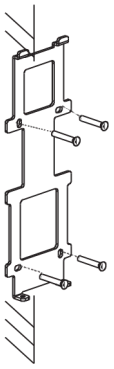
Prima di iniziare:

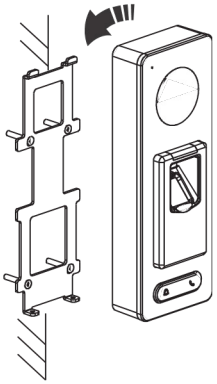
Assicurarsi che il dispositivo nell'imballaggio sia in buone condizioni e che siano presenti tutte le parti necessarie per l'assemblaggio.

Verificare che la parete sia abbastanza resistente da reggere un peso triplo rispetto a quello del terminale. Impostare l'indirizzo del DIP prima dell'installazione.

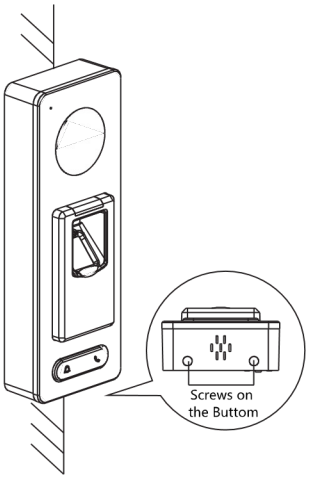
Passaggi:

1. Collegare i cavi con il connettore sul pannello posteriore del dispositivo. Instradare i cavi facendoli passare attraverso il foro della base di montaggio. I fori per i cavi si trovano sui lati destro, sinistro e inferiore del coperchio posteriore. Se si seleziona il foro per il cavo sul lato destro/sinistro, rimuovere la pellicola di plastica dal foro del cavo.
2. Fissare la piastra di montaggio alla parete utilizzando le 4 viti fornite in dotazione.
3. Collegare i cavi corrispondenti.
4. Spingere il terminale nella piastra di montaggio dal basso verso l'alto.





5. Stringere le viti alla base del terminale per fissarlo sulla piastra di montaggio e completare l'installazione.



Capitolo 4 Collegamento dei terminali

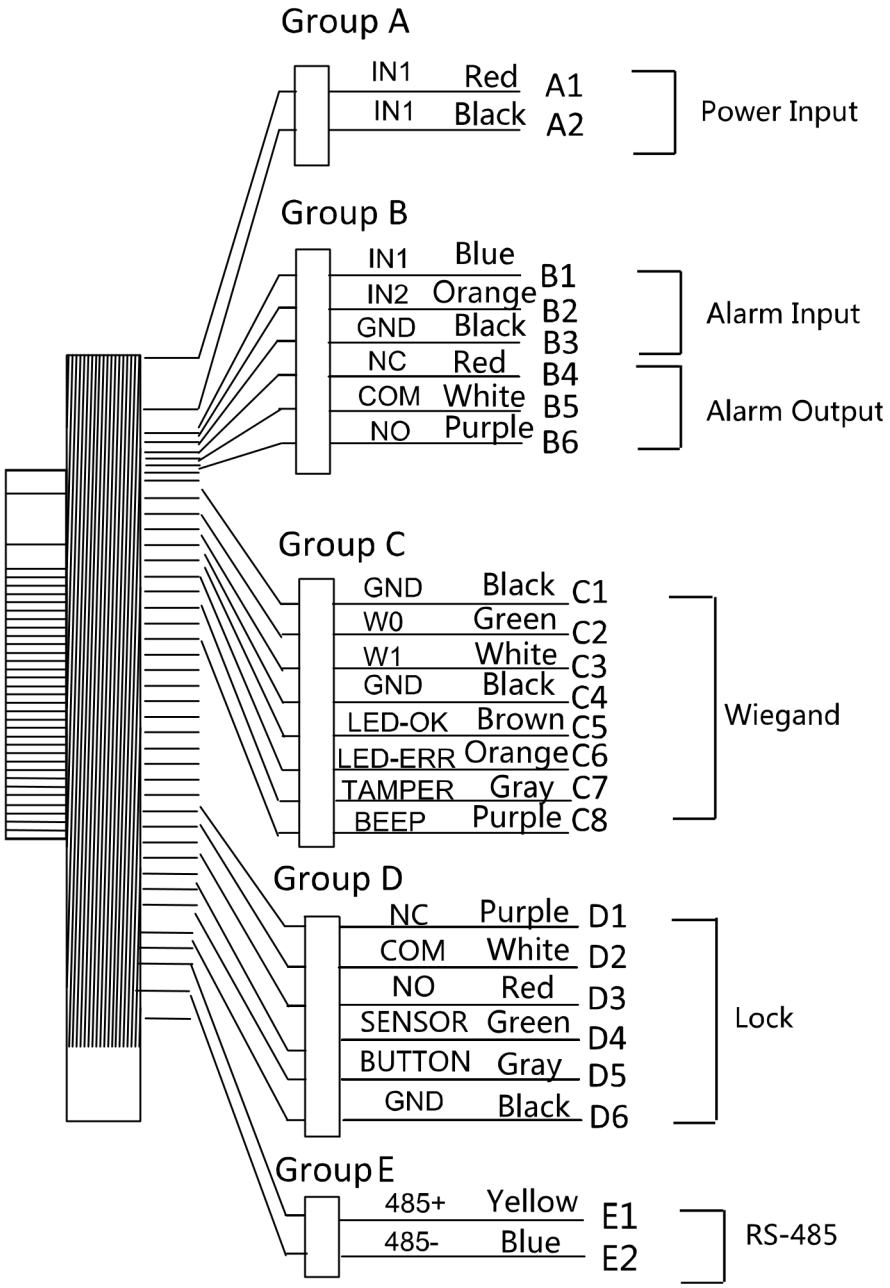


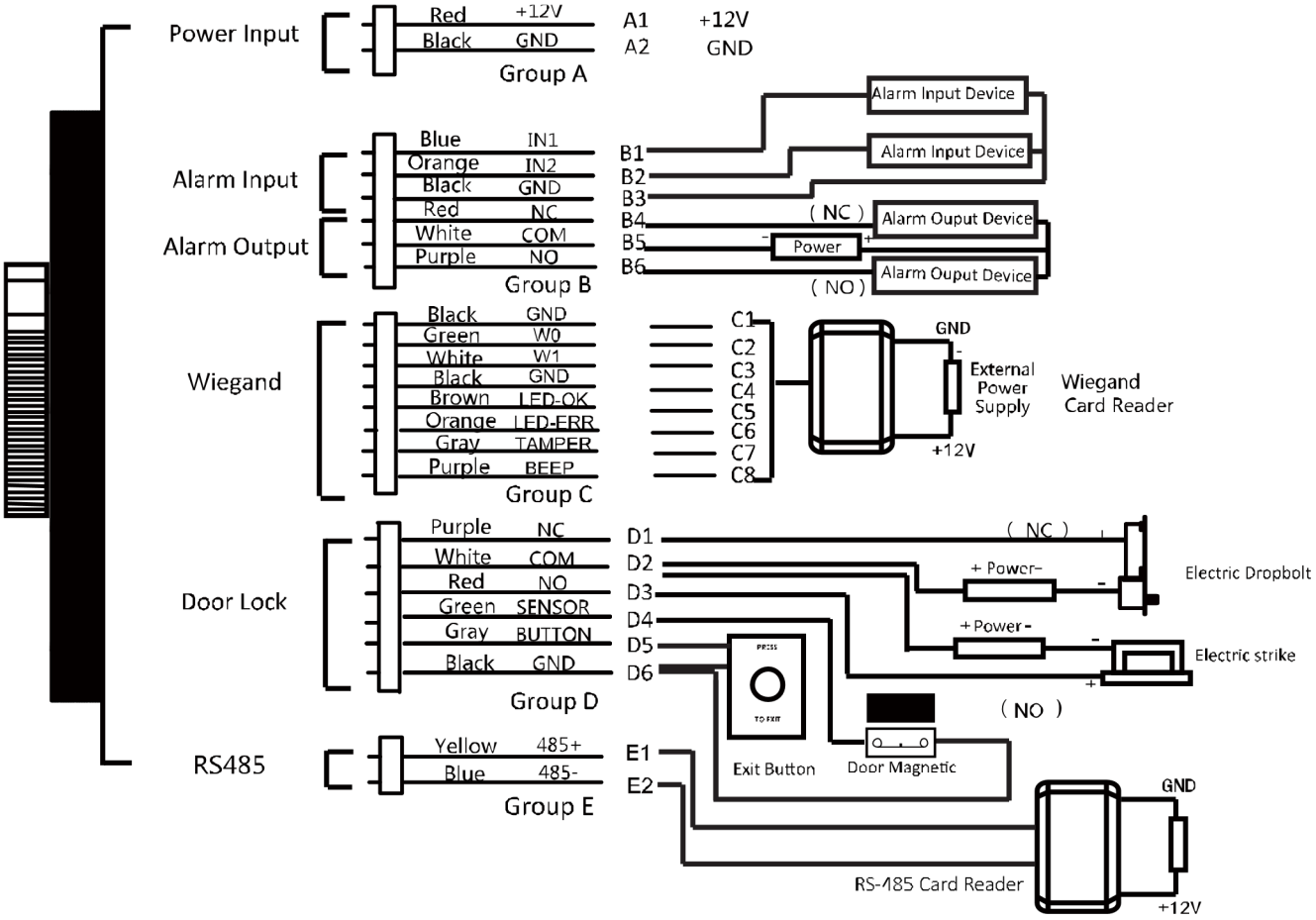
Tabella 4-1 Descrizione dei terminali

Gruppo	N.	Funzione	Colore	Nome terminale	Descrizione
Gruppo A	A1	Ingresso alimentazione	Rosso	+12 V	Alimentatore 12 V CC
	A2		Nero	GND	GND

Gruppo	N.	Funzione	Colore	Nome terminale	Descrizione
Gruppo B	B1	Ingresso allarme	Giallo	IN1	Ingresso allarme 1
	B2		Arancione	IN2	Ingresso allarme 2
	B3		Nero	GND	GND
	B4	Uscita allarme	Rosso	NC	Cablaggio uscita di allarme
	B5		Bianco	COM	
	B6		Viola	NO	
Gruppo C	C1	Wiegand	Nero	GND	GND
	C2		Verde	W0	Cablaggio Wiegand 0
	C3		Bianco	W1	Cablaggio Wiegand 1
	C4		Nero	GND	GND
	C5		Marrone	LED-OK	Wiegand autenticato
	C6		Arancione	LED-ERR	Wiegand Autenticazione non riuscita
	C7		Grigio	TAMPER	Cablaggio allarme antimanomissione
	C7		Viola	BEEP	Cablaggio avvisatore acustico
Gruppo D	D1	Blocco	Viola	NC	Cablaggio blocco
	D2		Bianco	COM	
	D3		Rosso	NO	
	D4		Verde	SENSOR	Ingresso segnale cablaggio magnetico porta
	D5		Grigio	BUTTON	Cablaggio porta d'uscita
	D6		Nero	GND	GND
Gruppo E	E1	RS-485	Giallo	485 +	Cablaggio RS-485
	E2		Blu	485 -	

Capitolo 5 Descrizione del cablaggio

5.1 Panoramica del cablaggio del dispositivo esterno



Note:

Se si imposta la modalità operativa come modalità controller, il terminale può collegare il lettore di tessere RS-485 o l'unità di controllo di sicurezza tramite il protocollo RS-485. Per i dettagli sul cablaggio del lettore di tessere RS-485, vedere 5.2 Cablaggio del lettore di tessere RS-485 esterno.

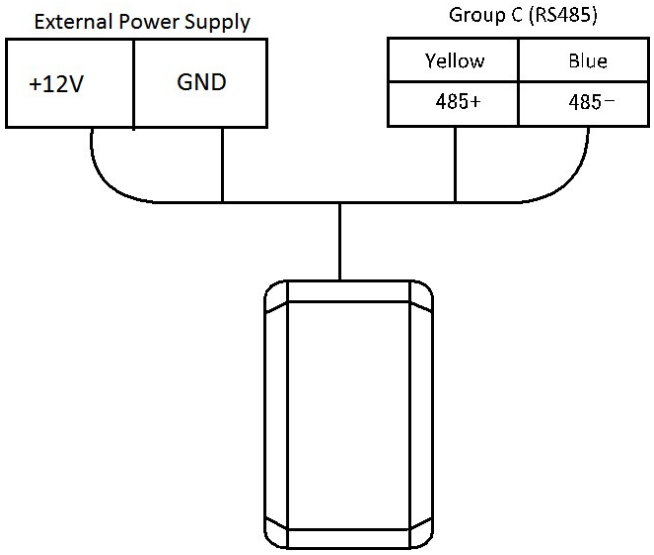
Se si imposta la modalità operativa come modalità controller, il terminale non può collegare il lettore di tessere Wiegand.

L'unità di controllo di sicurezza può anche collegare i dispositivi esterni. Per i dettagli, consultare il manuale dell'utente specifico dell'unità di controllo di sicurezza.

5.2 Cablaggio del lettore di tessere RS-485 esterno

Se si imposta la modalità operativa come modalità controller, il DIP switch n. 6 deve essere impostato su OFF.

Se si imposta la modalità operativa come modalità lettore di tessere, il DIP switch da 1 a 4 deve essere impostato su OFF. Impostare il DIP switch RS-485 del lettore di tessere esterno su 2. Per dettagli sulla configurazione del DIP switch, vedere l'Appendice B Introduzione al DIP switch.



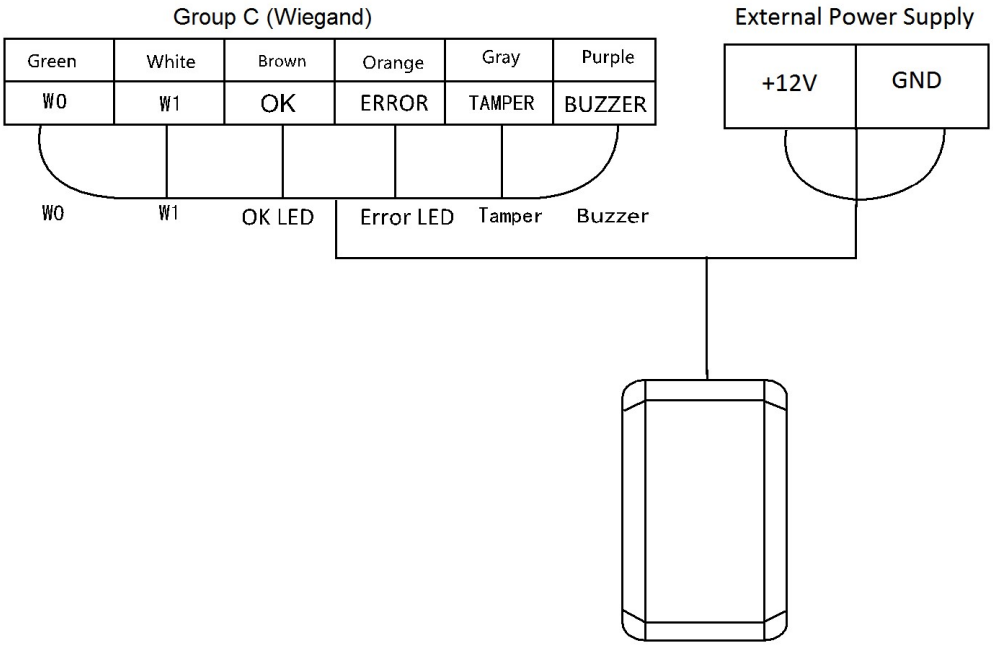
5.3 Connessione del lettore di tessere

Il terminale di controllo accessi può essere impostato in modalità di lettore di tessere. Può essere inserito in un sistema controllo accessi come lettore di tessere e supporta le porte di comunicazione Wiegand e RS-485.

NOTE

Quando il terminale di controllo accessi ha la funzione di lettore di tessere, supporta solo la connessione al controllore; l'ingresso o l'uscita di allarme oppure la connessione con dispositivi esterni non sono supportati.

5.3.1 Cablaggio del lettore Wiegand



NOTE

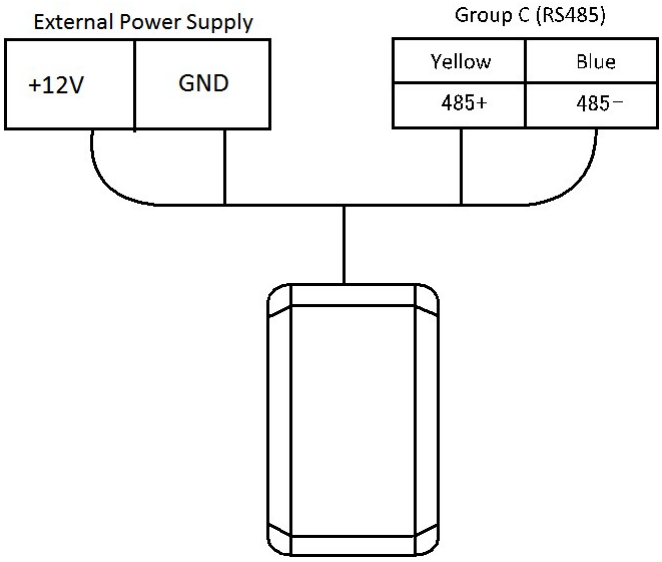
Quando il terminale di controllo accessi ha la funzione di lettore di tessere, è necessario collegare le interfacce **WG_ERR, BUZZER e WG_OK** se si desidera controllare le spie LED e l'avvisatore acustico del lettore di tessere Wiegand.

Impostare la modalità operativa del terminale come lettore di tessere, se il terminale deve funzionare come lettore di tessere. La modalità di lettore di tessere supporta la comunicazione con Wiegand o RS-485.

La distanza della comunicazione con l'unità Wiegand non deve superare 80 m.

L'alimentazione esterna e il terminale di controllo accessi devono utilizzare lo stesso cavo GND.

5.3.2 Cablaggio dell'uscita RS-485



NOTE

Impostare la modalità operativa del terminale come lettore di tessere, se il terminale richiede un funzionamento come lettore di tessere.

Quando il terminale di controllo accessi funziona come un lettore di tessere RS-485, è possibile impostare l'indirizzo RS-485 tramite il DIP switch.

L'alimentazione esterna e il terminale di controllo accessi devono utilizzare lo stesso cavo GND.

Capitolo 6 Attivazione del terminale di controllo accessi

Scopo:

È necessario attivare il terminale prima di poterlo utilizzare.

Sono supportate l'attivazione con SADP e quella con il software client. I valori predefiniti del terminale di controllo sono i seguenti.

Indirizzo IP predefinito: 192.0.0.64.

Numero di porta predefinito: 8000.

Nome utente predefinito: admin.

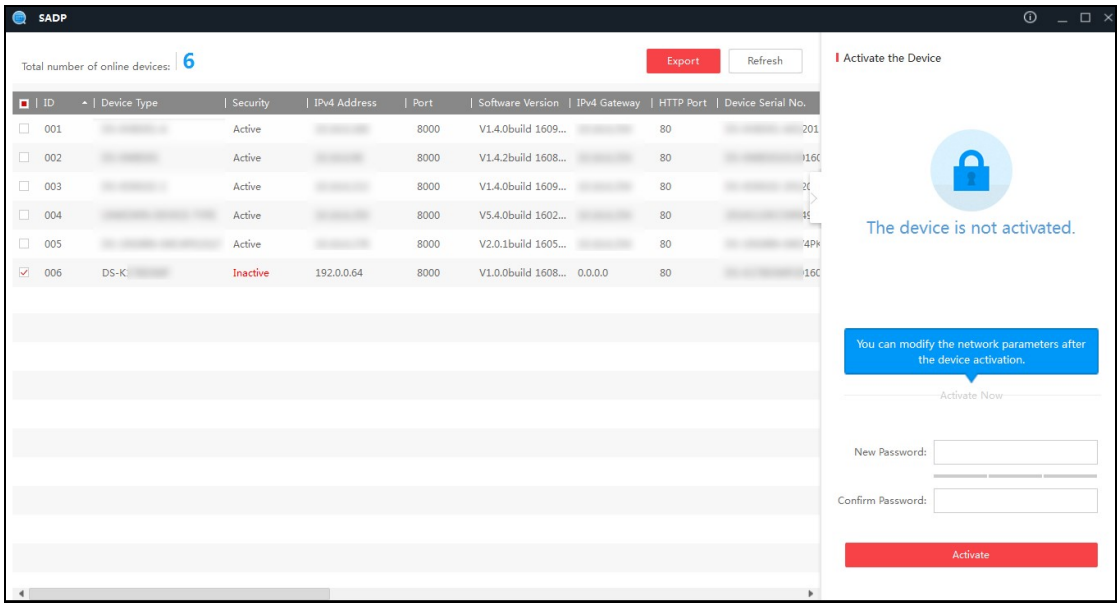
6.1 Attivazione tramite il software SADP

Il software SADP si utilizza per rilevare il dispositivo online, attivarlo e reimpostare la password.

Il software SADP è disponibile sul disco in dotazione o sul sito ufficiale; installare SADP seguendo le indicazioni sullo schermo. Seguire la procedura per attivare il pannello di controllo.

Passaggi:

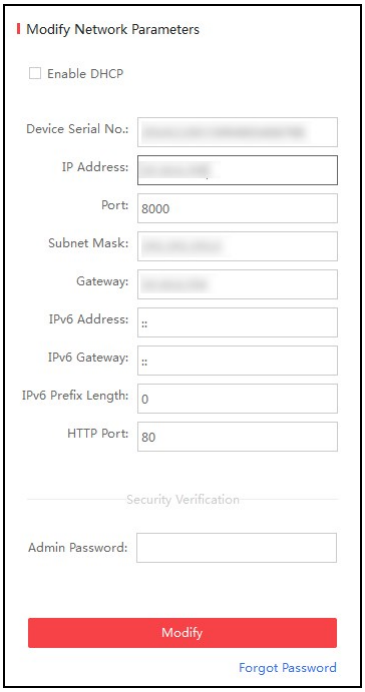
1. Eseguire il software SADP per cercare i dispositivi online.
2. Controllare lo stato dei dispositivi nell'elenco, quindi selezionare un dispositivo inattivo.



3. Inserire una password nel relativo campo e confermarla.

PASSWORD COMPLESSA CONSIGLIATA: *si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, che comprendano lettere maiuscole e minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.*

4. Fare clic su **Activate** per attivare il dispositivo.
5. Selezionare il dispositivo attivato; è possibile cambiare l'indirizzo IP del dispositivo con quello dello stesso segmento di rete al quale è connesso il computer modificando l'indirizzo IP manualmente oppure selezionando la casella di controllo Enable DHCP.



6. Inserire la password e fare clic sul pulsante **Modify** per confermare la modifica dell'indirizzo IP.

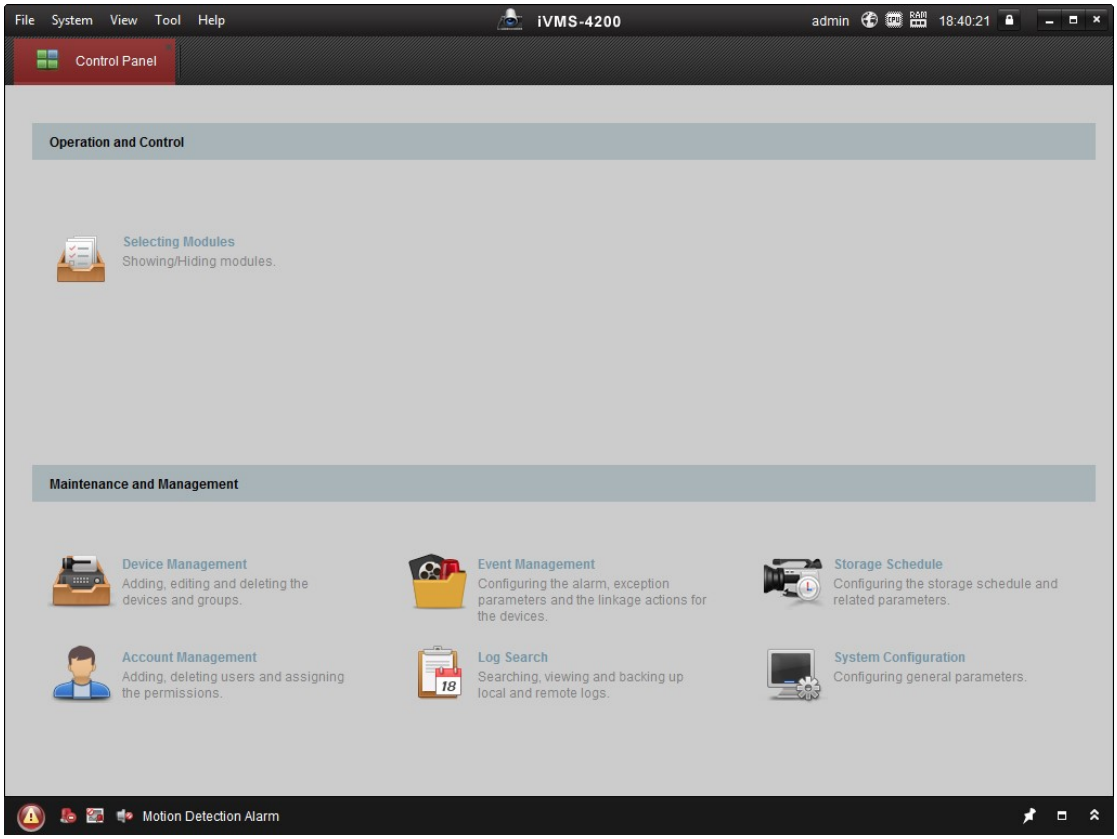
6.2 Attivazione tramite il software client

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

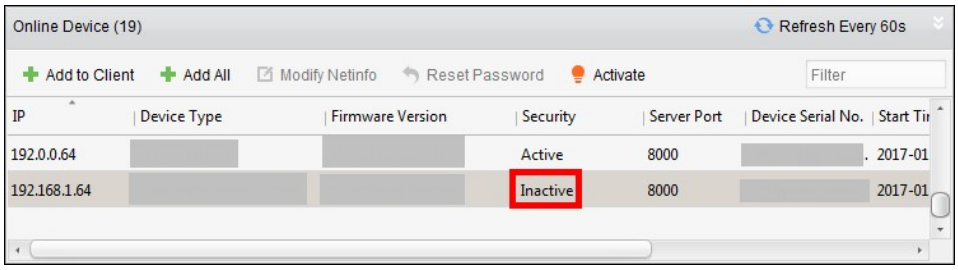
Il software client è disponibile sul disco in dotazione o sul sito ufficiale; installare il software seguendo le indicazioni sullo schermo. Seguire la procedura per attivare il pannello di controllo.

Passaggi:

1. Eseguire il software client; si aprirà il pannello di controllo del software come mostrato nella figura seguente.



2. Fare clic su **Device Management** per accedere all'interfaccia Device Management.
3. Controllare lo stato dei dispositivi nell'elenco, quindi selezionare un dispositivo inattivo.



4. Controllare lo stato dei dispositivi nell'elenco, quindi selezionare un dispositivo inattivo.
5. Fare clic sul pulsante **Activate** per far apparire l'interfaccia Activation.
6. Nella finestra a comparsa, creare una password nel relativo campo e confermarla.

PASSWORD COMPLESSA CONSIGLIATA: *si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, che comprendano lettere maiuscole e minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.*

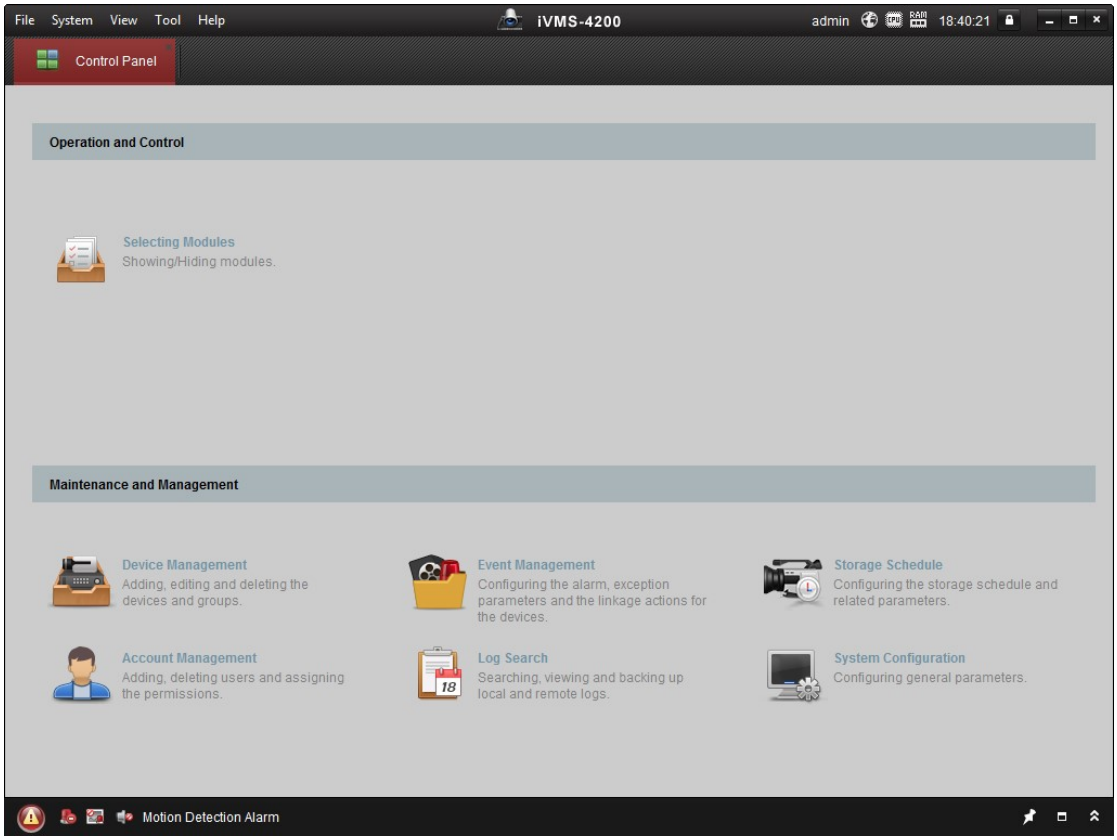
7. Fare clic sul pulsante **OK** per avviare l'attivazione.
8. Fare clic sul pulsante **Modify Netinfor** per visualizzare l'interfaccia Network Parameter Modification.
9. Cambiare l'indirizzo IP del dispositivo con quello dello stesso segmento di rete al quale è connesso il computer modificando l'indirizzo IP manualmente.
10. Immettere la password e fare clic sul pulsante **OK** per salvare le impostazioni.

Capitolo 7 Funzionamento del client

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

7.1 Modulo Function

Pannello di controllo di iVMS-4200:



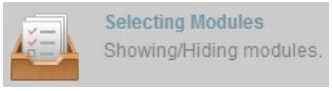
Barra dei menu:

File	**Open Image File**	Trova e visualizza le immagini acquisite e memorizzate sul PC locale.
	Open Video File	Trova e visualizza i file video registrati sul PC locale.
	Open Log File	Visualizza i file di registro di backup.
	Exit	Esce dal software client iVMS-4200.
System	**Lock**	Blocca le operazioni a video. Per lo sblocco, accedere nuovamente al client.
	Switch User	Cambia l'utente di accesso.
	Import System Config File	Importa il file di configurazione del client dal computer.
	Export System Config File	Esporta il file di configurazione del client sul computer.

	Auto Backup	Imposta la pianificazione automatica di backup del database comprendente dati personali, delle presenze e autorizzazioni.

View	**1024*768**	Visualizza le finestre nel formato 1024*768 pixel.
	1280*1024	Visualizza le finestre nel formato 1280*1024 pixel.
	1440*900	Visualizza le finestre nel formato 1440*900 pixel.
	1680*1050	Visualizza le finestre nel formato 1680*1050 pixel.
	Maximize	Mostra la finestra alla sua massima dimensione.
	Control Panel	Accede all'interfaccia Control Panel.
	Main View	Apre la pagina Main View.
	Remote Playback	Apre la pagina Remote Playback.
	Access Control	Accede al modulo Access Control.
	Status Monitor	Accede al modulo Status Monitor.
	Time and Attendance	Accede al modulo Time and Attendance.
	Security Control Panel	Accede al modulo Security Control Panel.
	Real-time Alarm	Accede al modulo Real-time Alarm.
	Video Wall	Apre la pagina Video Wall.
	E-map	Apre la pagina E-map.
	Auxiliary Screen Preview	Apre la finestra Auxiliary Screen Preview.
Tool	**Device Management**	Apre la pagina Device Management.
	Event Management	Apre la pagina Event Management.
	Storage Schedule	Apre la pagina Storage Schedule.
	Account Management	Apre la pagina Account Management.
	Log Search	Apre la pagina Log Search.
	System Configuration	Apre la pagina System Configuration.
	Broadcast	Seleziona la telecamera per l'avvio della trasmissione.
	Device Arming Control	Imposta lo stato di attivazione dei dispositivi.
	Alarm Output Control	Attiva/disattiva l'uscita di allarme.
	Batch Wiper Control	Avvia o arresta gruppi di tergicristalli dei dispositivi.
	Batch Time Sync	Sincronizza gli orari dei dispositivi in batch.
	Player	Apre il lettore per la riproduzione dei file video.
	Message Queue	Mostra l'informazione dei messaggi e-mail da inviare.

Help	**Open Video Wizard**	Apre la guida video per la configurazione della videosorveglianza.
	Open Video Wall Wizard	Apre la guida per la configurazione del video wall.
	Open Security Control Panel Wizard	Apre la guida per la configurazione del pannello di controllo di sicurezza.
	Open Access Control and Video Intercom Wizard	Apre la guida per la configurazione del controllo accessi e videocitofoni.
	Open Attendance Wizard	Apre la guida per la configurazione di orari e presenze.
	User Manual (F1)	Fare clic per aprire il manuale dell'utente; è possibile aprire il manuale anche premendo **F1** sulla tastiera.
	About	Visualizza le informazioni di base del software client.
	Language	Seleziona la lingua del software client e riavvia il software per l'attivazione delle impostazioni.

Quando il software è lanciato per la prima volta, è possibile fare clic su 

sul pannello di controllo per selezionare i moduli da visualizzare nell'area Operation and Control del pannello di controllo. ***Passaggi:***

1. Fare clic su  per far apparire la seguente finestra di dialogo.
2. Attivare le caselle di controllo dei moduli da visualizzare sul pannello di controllo in base alle proprie esigenze.
3. Fare clic su **OK** per salvare le impostazioni.

Note:

Dopo l'aggiunta del dispositivo di controllo accessi nel modulo Device Management, i moduli Access Control, Status e Time and Attendance saranno visualizzati automaticamente sul pannello di controllo.

Dopo l'aggiunta del pannello di controllo sicurezza nel modulo Device Management, i moduli Security Control Panel e Real-time Alarm saranno visualizzati automaticamente sul pannello di controllo.

Il software client iVMS-4200 è composto dai seguenti moduli funzionali:

	Il modulo Main View mostra le immagini dal vivo delle telecamere IP e dei codificatori video; inoltre supporta alcune operazioni di base, quali acquisizione di immagini, registrazione, controllo PTZ, ecc.
	Il modulo Remote Playback fornisce funzioni di ricerca, riproduzione ed esportazione di file video.
	Il modulo Access Control fornisce funzioni di gestione di organizzazioni, persone, autorizzazioni e funzioni avanzate di controllo accessi. Fornisce anche funzioni di videocitofono.
	Il modulo Status Monitor fornisce funzioni di monitoraggio e controllo dello stato delle porte, di visualizzazione dei record di passaggio delle tessere in tempo reale e degli eventi di controllo accessi.
	Il modulo Time and Attendance permette di definire le regole di presenza per i dipendenti e di generare i corrispondenti report.
	Il modulo Security Control Panel fornisce operazioni quali attivazione, disattivazione, bypass, bypass di gruppo e altre operazioni per partizioni e zone.
	Il modulo Real-time Alarm consente di visualizzare l'allarme in tempo reale del pannello di controllo di sicurezza, confermare gli allarmi e fare ricerche nella cronologia degli allarmi.
	Il modulo Alarm Event permette di visualizzare allarmi ed eventi ricevuti dal software client.
	Il modulo Video Wall consente la gestione di dispositivi di decodifica e video wall e fornisce funzioni di visualizzazione dei video decodificati su video wall.
	Il modulo E-map fornisce funzioni di visualizzazione e gestione di mappe elettroniche, ingressi di allarme, aree sensibili e punti caldi.
	Il modulo Device Management permette di aggiungere, modificare e rimuovere i vari dispositivi, nonché di importarli in gruppi per agevolarne la gestione.
	Il modulo Event Management permette l'impostazione di pianificazioni di attivazione, azioni di collegamento per allarmi e altri parametri relativi agli eventi.
	Il modulo Storage Schedule permette di definire le impostazioni di pianificazione relative a registrazioni e immagini.
	Il modulo Account Management permette l'aggiunta, la modifica e la cancellazione degli account utente, nonché l'assegnazione delle varie autorizzazioni ai relativi utenti.

	Il modulo Log Search permette l'interrogazione dei file di registro del sistema, con l'opzione di definire su di essi vari tipi di filtri.
	Il modulo System Configuration permette la configurazione dei parametri generali, quali percorsi di salvataggio file, suonerie di allarme e altre impostazioni di sistema.

I moduli funzionali sono facilmente accessibili facendo clic sui pulsanti di spostamento nel pannello di controllo o selezionando il modulo funzionale dai menu **View** o **Tool**.

Nell'angolo in alto a destra della pagina principale, è possibile consultare varie informazioni, quali utente connesso, utilizzo di rete, utilizzo della CPU, utilizzo di memoria e orario.

7.2 Registrazione e accesso utenti

Al primo utilizzo del software client iVMS-4200, occorre registrarsi come utente con privilegi di accesso avanzati.

Passaggi:

1. Inserire nome e password dell'utente con privilegi di accesso avanzati. Il software valuterà automaticamente la complessità della password; si consiglia di usare password complesse per garantire un'adeguata protezione dei dati.
2. Confermare la password.
3. Facoltativamente, è possibile, attivando la casella di controllo **Enable Auto-login**, abilitare l'accesso automatico al software.
4. Fare clic su **Register**. Quindi, sarà possibile accedere al software come utente privilegiato.

*Il nome utente non può contenere i caratteri seguenti: / \ : * ? " < > |. La lunghezza della password non può essere inferiore ai 6 caratteri.*

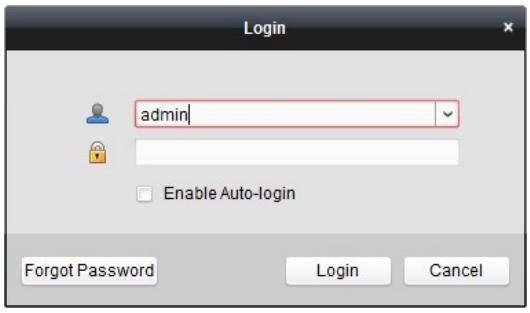
Per ragioni di riservatezza, si suggerisce di modificare la password in una stringa scelta dall'utente (lunga almeno 8 caratteri e comprendente lettere maiuscole e minuscole, nonché numeri e caratteri speciali) in modo da aumentare la sicurezza del prodotto.

Rientra nella responsabilità dell'installatore e/o dell'utente finale configurare correttamente tutte le password e altri parametri di sicurezza.

All'apertura di iVMS-4200 dopo la registrazione, l'utente può accedere al software client con nome utente e password di registrazione.

Passaggi:

1. Inserire nome utente e password di registrazione.
   Nota: se ci si dimentica la password, fare clic su **Forgot Password** e prendere nota della stringa crittografata visualizzata nella finestra a comparsa. Contattare il proprio rivenditore e inviargli la stringa crittografata per ottenere il ripristino della password.
2. Facoltativamente, è possibile, attivando la casella di controllo **Enable Auto-login**, abilitare l'accesso automatico al software.
3. Fare clic su **Login**.



Dopo aver lanciato il software client, è possibile aprire le procedure guidate (per video, video wall, pannello di controllo di sicurezza, controllo accessi, videocitofono e presenze), che aiutano l'utente ad aggiungere dispositivi e ad effettuare altre impostazioni e operazioni. Per una configurazione dettagliata delle procedure guidate, consultare la *Guida rapida di iVMS-4200*.

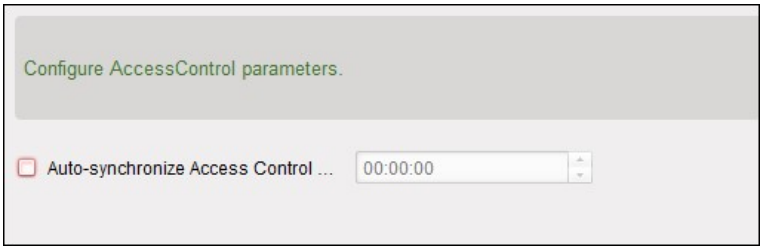
7.3 Configurazione del sistema

Scopo:

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

Passaggi:

1. Fare clic su **Tool** – **System Configuration**.
2. Nella finestra System Configuration, selezionare la casella di controllo **Auto-synchronize Access Control Event**.
3. Impostare l'ora di sincronizzazione.
   Il client sincronizzerà automaticamente l'evento di controllo accessi perso sul client all'ora impostata.



7.4 Gestione del controllo degli accessi

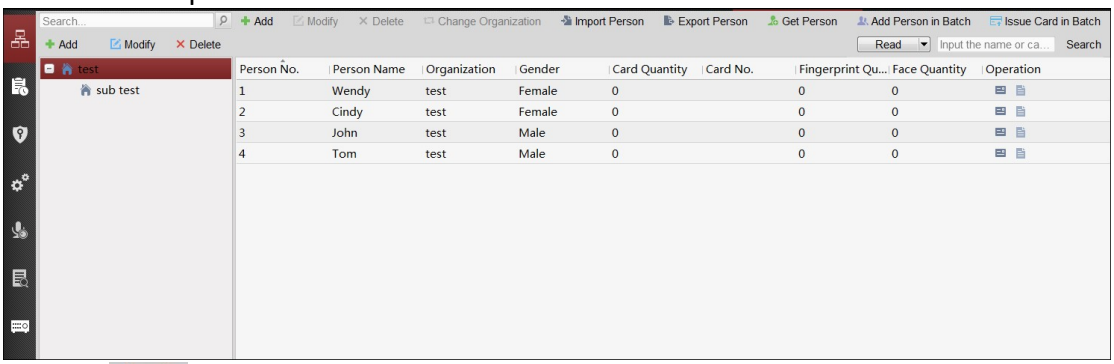
Scopo:

Il modulo Access Control si applica ai dispositivi di controllo accessi e ai videocitofoni. Tale modulo fornisce numerose funzionalità, quali gestione di persone e tessere, configurazione delle autorizzazioni, gestione dello stato di controllo accessi, videocitofoni e altre funzioni avanzate.

È anche possibile configurare gli eventi di controllo accessi e visualizzare punti di controllo accessi e le zone sulla mappa elettronica.

Nota: per definire le autorizzazioni del modulo di controllo degli accessi, è possibile accedere al modulo Access Control e configurare le impostazioni del controllo degli accessi.

Fare clic su  nel pannello di controllo e selezionare **Access Control** per aggiungere il modulo Access Control al pannello di controllo.



Fare clic su  per accedere al modulo Access Control.

Prima di iniziare:

Alla prima apertura del modulo Access Control, appare la seguente finestra di dialogo, in cui occorre selezionare la scena richiesta, in base alle esigenze.

Non-residence: è possibile impostare la regola di presenza quando si aggiunge una persona, impostando i parametri di controllo degli accessi.

Residence: non è possibile impostare la regola di presenza quando si aggiunge una persona.

Nota: quando la scena è configurata non è possibile modificarla successivamente.

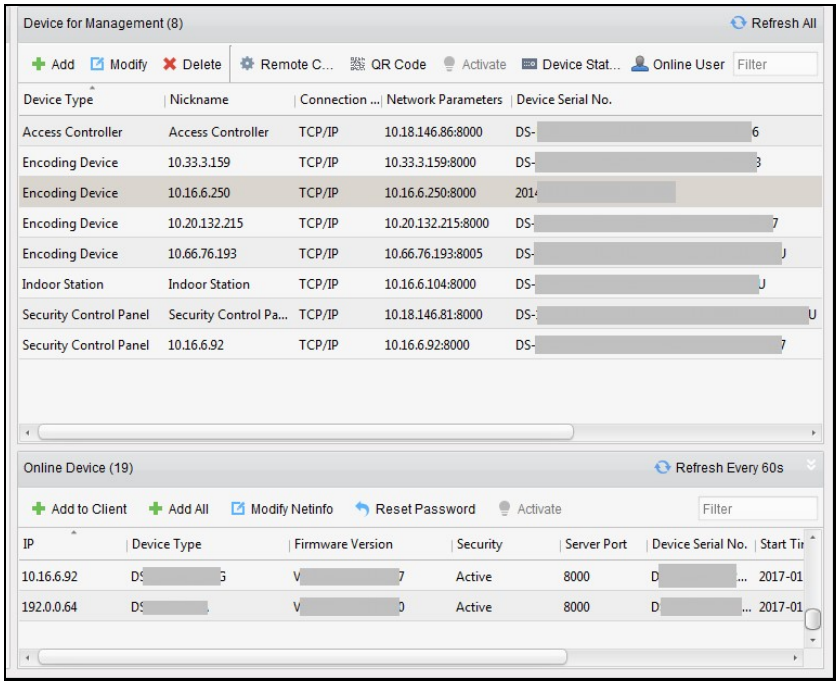
Il modulo Access Control è composto dai seguenti sotto-moduli.

	**Person and Card**	Permette di gestire organizzazioni, persone e assegnazione delle relative tessere.
	**Schedule and Template**	Permette di configurare le pianificazioni settimanali, i gruppi di ferie e di definire i relativi modelli.
	**Permission**	Permette di assegnare le autorizzazioni di controllo accessi alle persone e applicarle ai dispositivi.
	**Advanced Function**	Fornisce funzioni avanzate, quali definizione dei parametri di controllo accessi, autenticazione dei lettori di tessere, apertura porte con la prima tessera, anti-passback, interblocco multi-porta e password di autenticazione.
	**Video Intercom**	Fornisce funzioni di videocitofono tra il client e soggetti residenti, opzioni di ricerca nei registri di chiamate e rilascio di avvisi.
	**Search**	Permette di effettuare ricerche nelle cronologie di eventi di controllo accessi, nei registri di chiamate e sblocchi e tra gli avvisi rilasciati.
	**Device Management**	Permette di gestire i dispositivi di controllo accessi e i videocitofoni.

Nota: in questo capitolo, ci occuperemo solo delle operazioni di controllo accessi.

7.4.1 Aggiunta di un dispositivo di controllo accessi

Fare clic su nel modulo Access Control per accedere alla seguente interfaccia.



Nota: dopo aver aggiunto il dispositivo, controllarne lo stato di attivazione in **Tool** – **Device Arming Control**. Se il dispositivo non è attivato, è necessario attivarlo altrimenti non si riceveranno gli eventi in tempo reale tramite il software client. Per i dettagli sul controllo dell'attivazione del dispositivo, consultare la sezione *7.13 Controllo dell'attivazione*.

Creazione di password

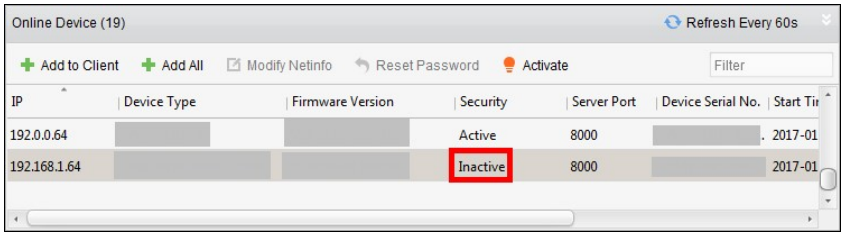
Scopo:

Alcuni dispositivi richiedono la creazione di una password di attivazione, per poter essere aggiunti al software e funzionare correttamente.

Nota: questa funzione deve essere supportata dal dispositivo.

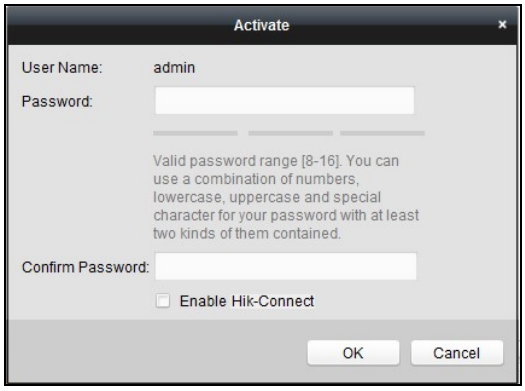
Passaggi:

1. Accedere alla pagina Device Management.
2. Nell'area **Device for Management** o **Online Device**, controllare lo stato del dispositivo (mostrato nella colonna **Security**) e selezionare un dispositivo non attivo.

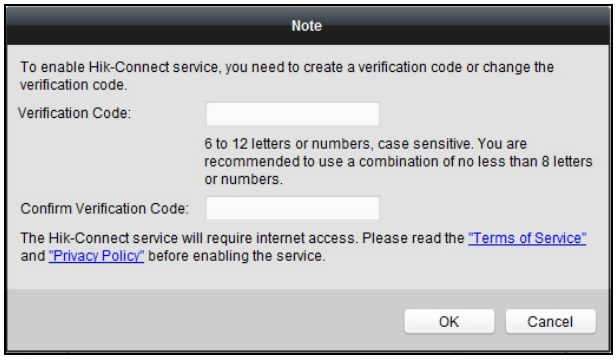


3. Fare clic sul pulsante **Activate** per far apparire l'interfaccia Activation.
4. Inserire una password nel relativo campo e confermarla.

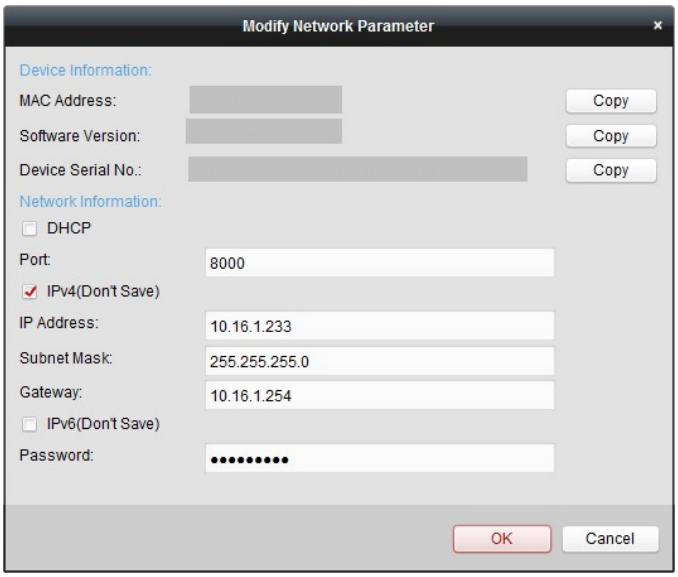
PASSWORD COMPLESSA CONSIGLIATA: *si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, che comprendano lettere maiuscole e minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.*



5. (Opzionale) Abilitare il servizio Hik-Connect all'attivazione del dispositivo, se da esso supportato.
   1) Attivare la casella di controllo **Enable Hik-Connect** per far apparire la finestra di dialogo Note.



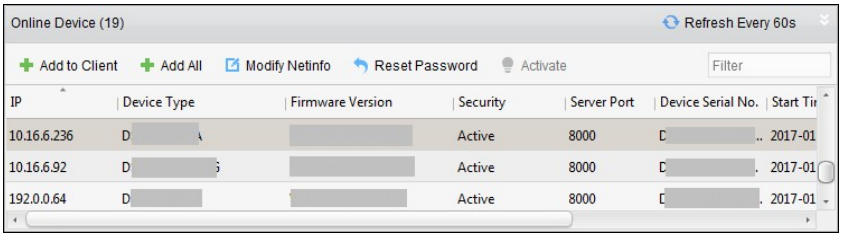
   2) Creare un codice di verifica.
   3) Confermare il codice di verifica.
   4) Fare clic su **Terms of Service** e **Privacy Policy** per leggere i requisiti. 5) Fare clic su **OK** per attivare il servizio Hik-Connect.
6. Fare clic su **OK** per attivare il dispositivo.
   Dopo aver definito la password, appare una finestra indicante "The device is activated".
7. Fare clic su **Modify Netinfo** per far apparire l'interfaccia Modify Network Parameter.
   Nota: questa funzione è disponibile solo nell'area **Online Device**. Se occorre aggiungere il dispositivo al software, è possibile modificare l'indirizzo IP del dispositivo, in modo che si trovi sulla stessa subnet a cui è connesso il computer.
8. Cambiare l'indirizzo IP del dispositivo con quello della subnet alla quale è connesso il computer modificando l'indirizzo IP manualmente oppure selezionando la casella di controllo DHCP.
9. Inserire la password definita al passaggio 4 e fare clic su **OK** per completare le impostazioni di rete.



Aggiunta di un dispositivo online

Scopo:

I dispositivi online attivi sulla stessa subnet locale del software client saranno visualizzati nell'area **Online Device**. È possibile fare clic sul pulsante **Refresh Every 60s**, per aggiornare le informazioni dei dispositivi online. ***Nota:*** facendo clic su , è possibile nascondere l'area **Online Device**.



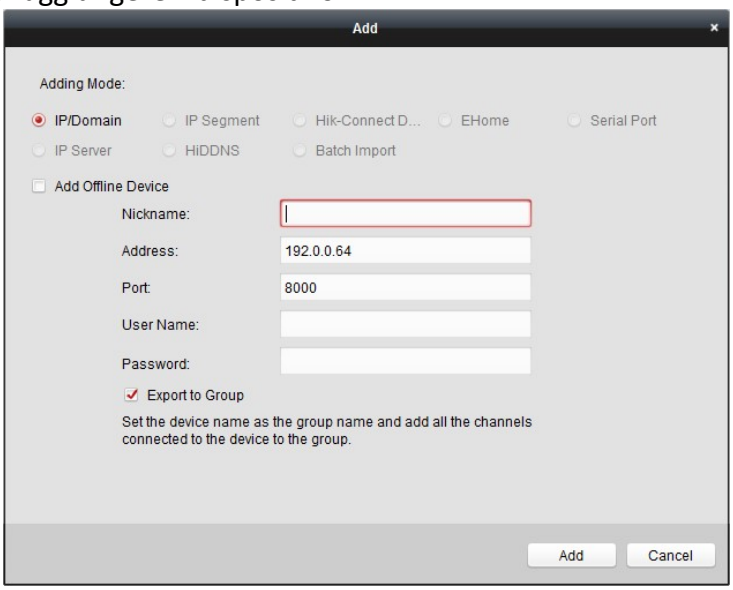
Passaggi:

1. Selezionare dall'elenco i dispositivi da aggiungere.
   Nota: per il dispositivo inattivo, è necessario crearne la password prima di poterlo aggiungere correttamente. Per i passaggi dettagliati, consultare il *Capitolo 6 Attivazione del terminale di controllo accessi*.
2. Fare clic su **Add to Client** per aprire la finestra di dialogo di aggiunta dei dispositivi.
3. Inserire le informazioni richieste.
   Nickname: modificare un nome per il dispositivo come si desidera.
   Address: inserire l'indirizzo IP del dispositivo. L'indirizzo IP del dispositivo si ottiene automaticamente in questa modalità di aggiunta.
   Port: immettere il numero di porta del dispositivo. Il valore predefinito è *8000*.
   User Name: immettere il nome utente del dispositivo. Per impostazione predefinita, il nome utente è *admin*.
   Password: inserire la password del dispositivo.

PASSWORD COMPLESSA CONSIGLIATA: *si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, che comprendano lettere maiuscole e minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.*

4. Facoltativamente, selezionare la casella di controllo **Export to Group** per creare un gruppo in base al nome del dispositivo.
   Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.
   Nota: iVMS-4200 fornisce anche un metodo per aggiungere i dispositivi offline.
   1) Selezionare la casella di controllo **Add Offline Device**.
   2) **I**nserire le informazioni richieste, compresi il numero di canale del dispositivo e il numero di ingresso allarme.
   3) Fare clic su **Add**.

   Quando il dispositivo offline passa online, il software si connetterà automaticamente.
5. Fare clic su **Add** per aggiungere il dispositivo.

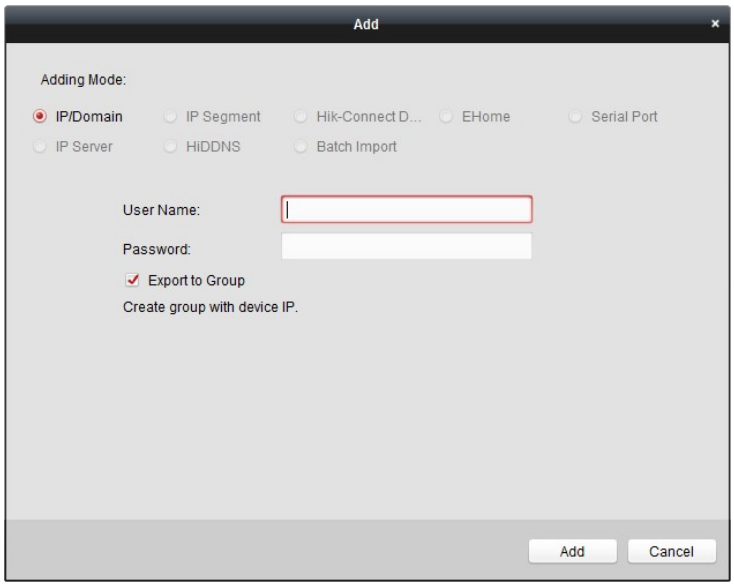


Aggiunta di più dispositivi online

Se si desidera aggiungere più dispositivi online al software client, fare clic e tenere premuto il tasto *Ctrl* per selezionare più dispositivi e fare clic su **Add to Client** per aprire la finestra di dialogo di aggiunta dei dispositivi. Nella casella con il messaggio a comparsa, immettere il nome utente e la password per i dispositivi da aggiungere.

Aggiunta di tutti i dispositivi online

Se si desidera aggiungere tutti i dispositivi online al software client, fare clic su **Add All** e fare clic su **OK** nella casella con il messaggio a comparsa. Quindi immettere il nome utente e la password per i dispositivi da aggiungere.



Aggiunta di dispositivi tramite indirizzo IP o nome di dominio

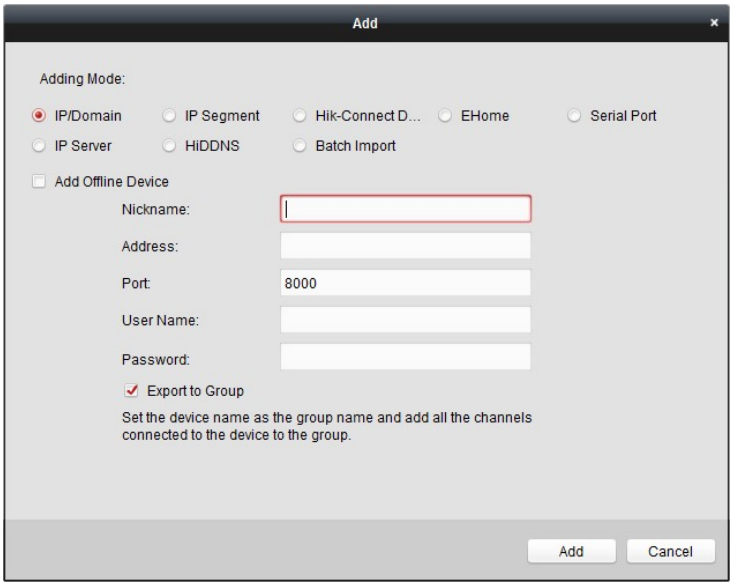
Passaggi:

1. Fare clic su **Add** per aprire la finestra di dialogo di aggiunta dei dispositivi.
2. Selezionare **IP/Domain** come modalità di aggiunta.
3. Inserire le informazioni richieste.
   Nickname: modificare un nome per il dispositivo come si desidera.
   Address: inserire l'indirizzo IP o il nome di dominio del dispositivo.
   Port: immettere il numero di porta del dispositivo. Il valore predefinito è *8000*.
   User Name: immettere il nome utente del dispositivo. Per impostazione predefinita, il nome utente è *admin*.
   Password: inserire la password del dispositivo.

   PASSWORD COMPLESSA CONSIGLIATA: *si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, che comprendano lettere maiuscole e minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.*
4. Facoltativamente, selezionare la casella di controllo **Export to Group** per creare un gruppo in base al nome del dispositivo.
   Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.
   Nota: iVMS-4200 fornisce anche un metodo per aggiungere i dispositivi offline.
   1) Selezionare la casella di controllo **Add Offline Device**.
   2) **I**nserire le informazioni richieste, compresi il numero di canale del dispositivo e il numero di ingresso allarme.
   3) Fare clic su **Add**.

   Quando il dispositivo offline passa online, il software si connetterà automaticamente.

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



Aggiunta di dispositivi tramite segmento IP

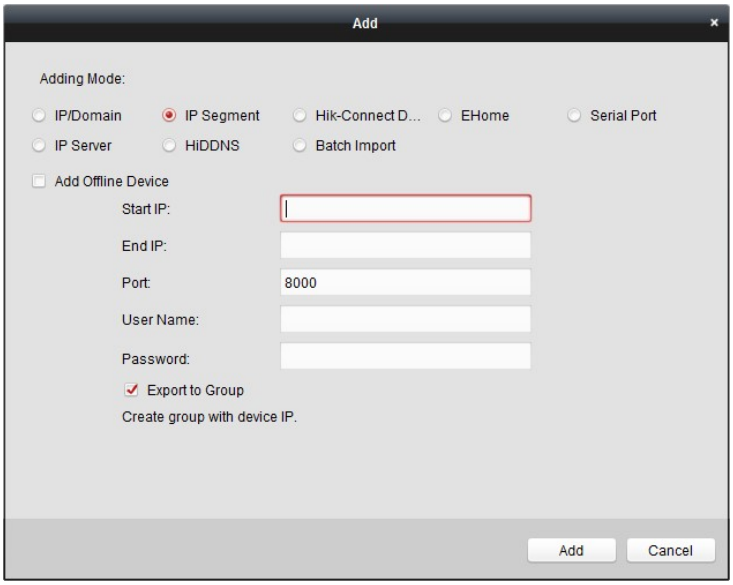
Passaggi:

1. Fare clic su **Add** per aprire la finestra di dialogo di aggiunta dei dispositivi.
2. Selezionare **IP Segment** come modalità di aggiunta.
3. Inserire le informazioni richieste.
   Start IP: inserire l'indirizzo IP iniziale.
   End IP: inserire un indirizzo IP finale nello stesso segmento di rete di quello iniziale.
   Port: inserire il numero di porta del dispositivo. Il valore predefinito è *8000*.
   User Name: immettere il nome utente del dispositivo. Per impostazione predefinita, il nome utente è *admin*.
   Password: inserire la password del dispositivo.

   PASSWORD COMPLESSA CONSIGLIATA: *si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, che comprendano lettere maiuscole e minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.*
4. Facoltativamente, selezionare la casella di controllo **Export to Group** per creare un gruppo in base al nome del dispositivo.
   Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.
   Nota: iVMS-4200 fornisce anche un metodo per aggiungere i dispositivi offline.
   1) Selezionare la casella di controllo **Add Offline Device**.
   2) **I**nserire le informazioni richieste, compresi il numero di canale del dispositivo e il numero di ingresso allarme.
   3) Fare clic su **Add**.

   Quando il dispositivo offline passa online, il software si connetterà automaticamente.

5. Fare clic su **Add**.
   È possibile aggiungere all'elenco dispositivi quei dispositivi il cui indirizzo IP è compreso tra gli indirizzi IP iniziale e finale.



Aggiunta di dispositivi tramite il dominio Hik-Connect

Scopo:

È possibile aggiungere dispositivi connessi via Hik-Connect, inserendo l'account e la password Hik-Connect.

Prima di iniziare: dapprima aggiungere i dispositivi all'account Hik-Connect tramite iVMS-4200, il client mobile iVMS-4500 o Hik-Connect. Per informazioni sull'aggiunta di dispositivi all'account Hik-Connect tramite iVMS-4200, consultare il *Manuale dell'utente del software client iVMS-4200*.

Aggiunta di un singolo dispositivo

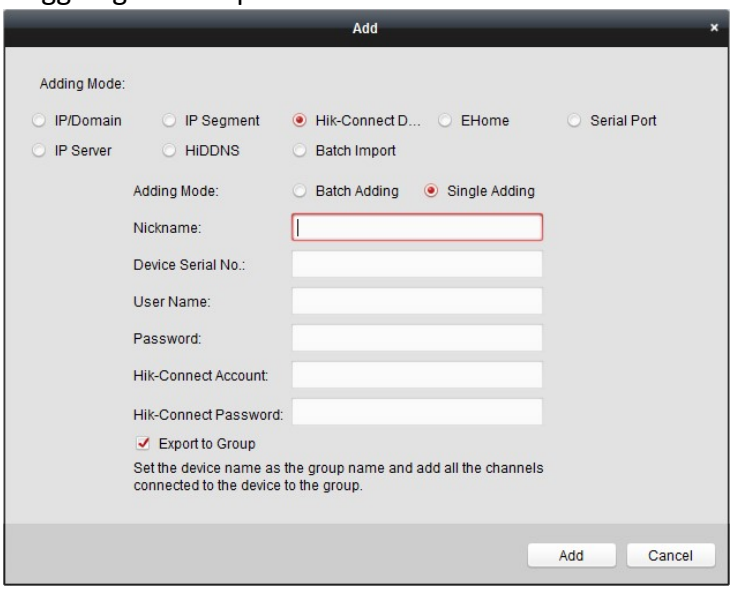
Passaggi:

1. Fare clic su **Add** per aprire la finestra di dialogo di aggiunta dei dispositivi.
2. Selezionare **Hik-Connect Domain** come modalità di aggiunta.
3. Selezionare **Single Adding**.
4. Inserire le informazioni richieste.
   Nickname: modificare un nome per il dispositivo come si desidera.
   Device Serial No.: inserire il numero di serie del dispositivo.
   User Name: immettere il nome utente del dispositivo. Per impostazione predefinita, il nome utente è *admin*.
   Password: inserire la password del dispositivo.

PASSWORD COMPLESSA CONSIGLIATA: *si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, che comprendano lettere maiuscole e minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.*

Hik-Connect Account: inserire l'account Hik-Connect.
Hik-Connect Password: inserire la password di Hik-Connect.

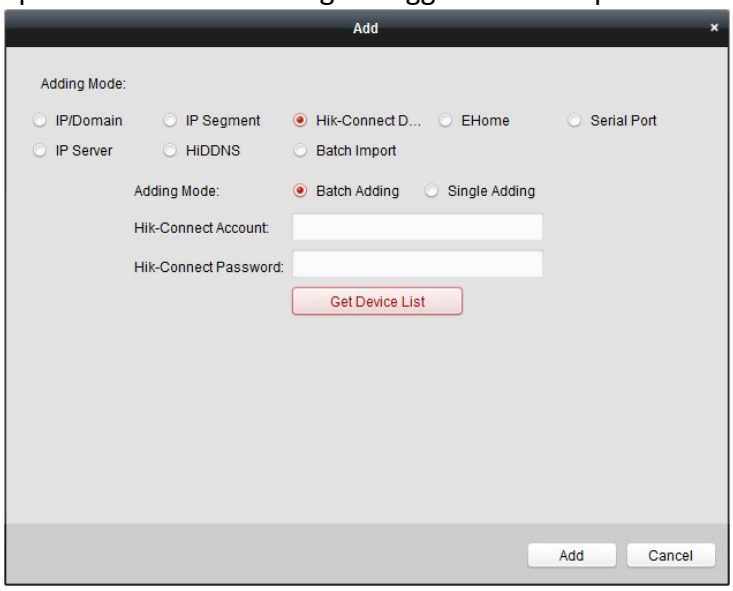
5. Facoltativamente, selezionare la casella di controllo **Export to Group** per creare un gruppo in base al nome del dispositivo. Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.
6. Fare clic su **Add** per aggiungere il dispositivo.



Aggiunta di dispositivi in batch

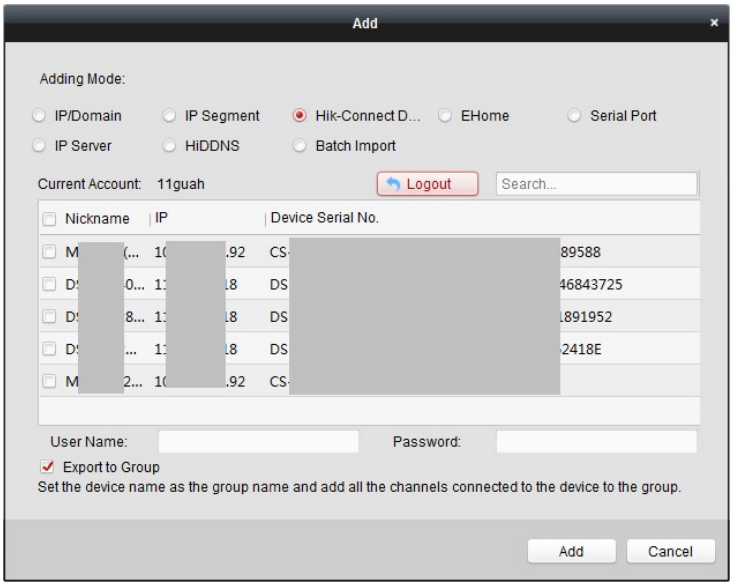
Passaggi:

1. Fare clic su **Add** per aprire la finestra di dialogo di aggiunta dei dispositivi.



2. Selezionare **Hik-Connect Domain** come modalità di aggiunta.
3. Selezionare **Batch Adding**.
4. Inserire le informazioni richieste.
   Hik-Connect Account: inserire l'account Hik-Connect.
   Hik-Connect Password: inserire la password di Hik-Connect.

5. Fare clic su **Get Device List** per visualizzare i dispositivi aggiunti all'account Hik-Connect.



6. Selezionare le caselle di controllo per selezionare il dispositivo desiderato.
7. Immettere il nome utente e la password per i dispositivi da aggiungere.
8. Facoltativamente, selezionare la casella di controllo **Export to Group** per creare un gruppo in base al nome del dispositivo.
   Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.
9. Fare clic su **Add** per aggiungere i dispositivi.

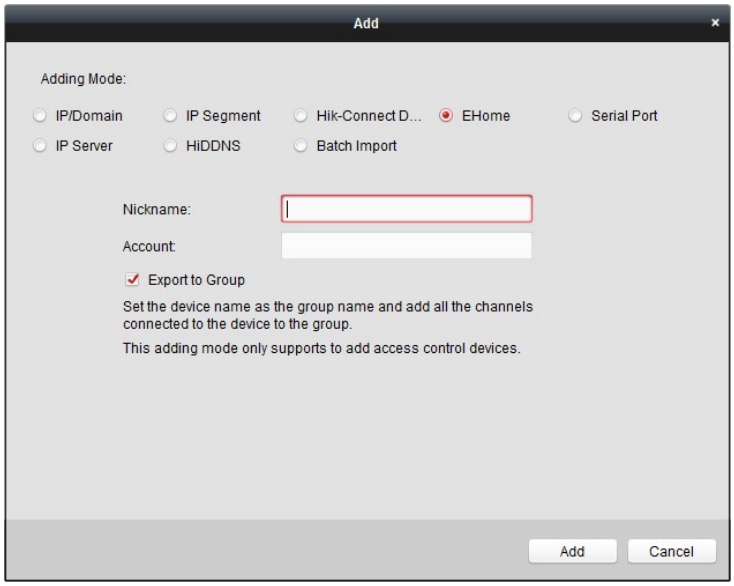
Aggiunta di dispositivi tramite account EHome

Scopo:

È possibile aggiungere dispositivi di controllo accessi connessi tramite protocollo EHome inserendo l'account EHome. ***Prima di iniziare:*** dapprima impostare i parametri del centro di rete. Per i dettagli, consultare il *Capitolo 7.4.4 Impostazioni di rete*.

Passaggi:

1. Fare clic su **Add** per aprire la finestra di dialogo di aggiunta dei dispositivi.
2. Selezionare **EHome** come modalità di aggiunta.



3. Inserire le informazioni richieste.
   Nickname: modificare un nome per il dispositivo come si desidera.
   Account: inserire il nome dell'account registrato sul protocollo EHome.
4. Facoltativamente, selezionare la casella di controllo **Export to Group** per creare un gruppo in base al nome del dispositivo.
   Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.
   Nota: iVMS-4200 fornisce anche un metodo per aggiungere i dispositivi offline.
   1) Selezionare la casella di controllo **Add Offline Device**.
   2) **I**nserire le informazioni richieste, compresi il numero di canale del dispositivo e il numero di ingresso allarme.
   3) Fare clic su **Add**.

   Quando il dispositivo offline passa online, il software si connetterà automaticamente.
5. Fare clic su **Add** per aggiungere il dispositivo.

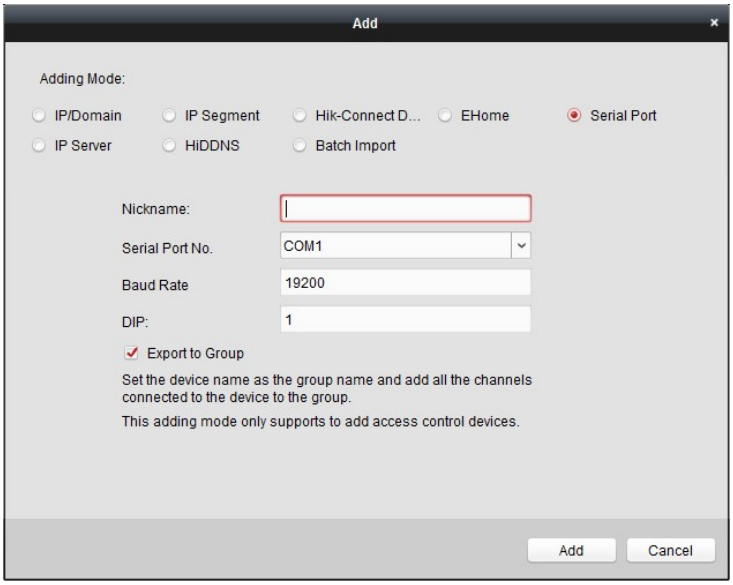
Aggiunta di dispositivi tramite porta seriale

Scopo:

È possibile aggiungere dispositivi di controllo accessi connessi tramite porta seriale.

Passaggi:

1. Fare clic su **Add** per aprire la finestra di dialogo di aggiunta dei dispositivi.
2. Selezionare **Serial Port** come modalità di aggiunta.



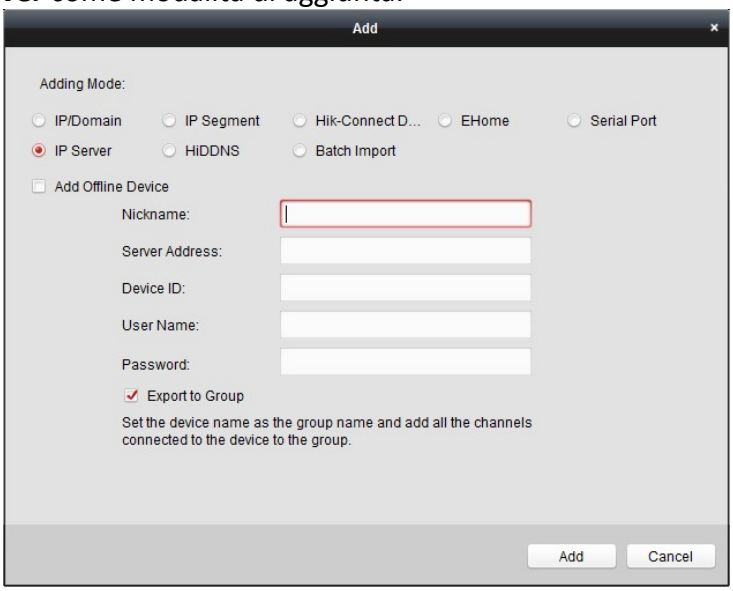
3. Inserire le informazioni richieste.
   Nickname: modificare un nome per il dispositivo come si desidera.
   Serial Port No.: selezionare il numero della porta seriale del dispositivo collegato.
   Baud Rate: immettere la velocità in baud del dispositivo di controllo accessi. **DIP:** immettere l'indirizzo del DIP del dispositivo.
4. Facoltativamente, selezionare la casella di controllo **Export to Group** per creare un gruppo in base al nome del dispositivo.
   Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.
   Nota: iVMS-4200 fornisce anche un metodo per aggiungere i dispositivi offline.
   1) Selezionare la casella di controllo **Add Offline Device**.
   2) Inserire le informazioni richieste, compresi il numero di canale del dispositivo e il numero di ingresso allarme.
   3) Fare clic su **Add**.

   Quando il dispositivo offline passa online, il software si connetterà automaticamente.
5. Fare clic su **Add** per aggiungere il dispositivo.

Aggiunta di dispositivi tramite server IP

Passaggi:

1. Fare clic su **Add** per aprire la finestra di dialogo di aggiunta dei dispositivi.
2. Selezionare **IP Server** come modalità di aggiunta.



3. Inserire le informazioni richieste.
   Nickname: modificare un nome per il dispositivo come si desidera.
   Server Address: inserire l'indirizzo IP del PC su cui è installato il server IP.
   Device ID: inserire l'ID del dispositivo registrato sul server IP.
   User Name: immettere il nome utente del dispositivo. Per impostazione predefinita, il nome utente è *admin*.
   Password: inserire la password del dispositivo.

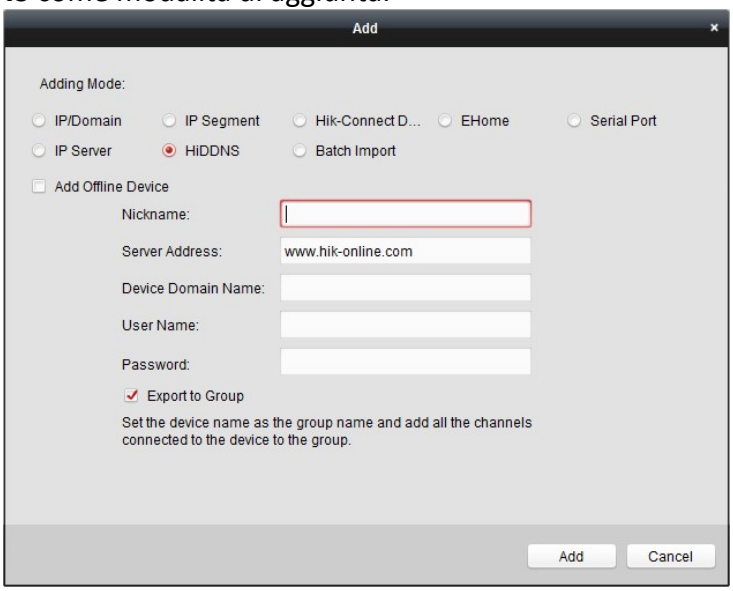
   PASSWORD COMPLESSA CONSIGLIATA: *si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, che comprendano lettere maiuscole e minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.*
4. Facoltativamente, selezionare la casella di controllo **Export to Group** per creare un gruppo in base al nome del dispositivo.
   Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.
   Nota: iVMS-4200 fornisce anche un metodo per aggiungere i dispositivi offline.
   1) Selezionare la casella di controllo **Add Offline Device**.
   2) Inserire le informazioni richieste, compresi il numero di canale del dispositivo e il numero di ingresso allarme.
   3) Fare clic su **Add**.

   Quando il dispositivo offline passa online, il software si connetterà automaticamente.
5. Fare clic su **Add** per aggiungere il dispositivo.

Aggiunta di dispositivi tramite HiDDNS

Passaggi:

1. Fare clic su **Add** per aprire la finestra di dialogo di aggiunta dei dispositivi.
2. Selezionare **HiDDNS** come modalità di aggiunta.



3. Inserire le informazioni richieste.
   Nickname: modificare un nome per il dispositivo come si desidera.
   Server Address: *www.hik-online.com*.
   Device Domain Name: inserire il nome di dominio del dispositivo registrato sul server HiDDNS.
   User Name: immettere il nome utente del dispositivo. Per impostazione predefinita, il nome utente è *admin*.
   Password: inserire la password del dispositivo.

   PASSWORD COMPLESSA CONSIGLIATA: *si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, che comprendano lettere maiuscole e minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.*
4. Facoltativamente, selezionare la casella di controllo **Export to Group** per creare un gruppo in base al nome del dispositivo.
   Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.
   Nota: iVMS-4200 fornisce anche un metodo per aggiungere i dispositivi offline.
   1) Selezionare la casella di controllo **Add Offline Device**.
   2) Inserire le informazioni richieste, compresi il numero di canale del dispositivo e il numero di ingresso allarme.
   3) Fare clic su **Add**.

   Quando il dispositivo offline passa online, il software si connetterà automaticamente.
5. Fare clic su **Add** per aggiungere il dispositivo.

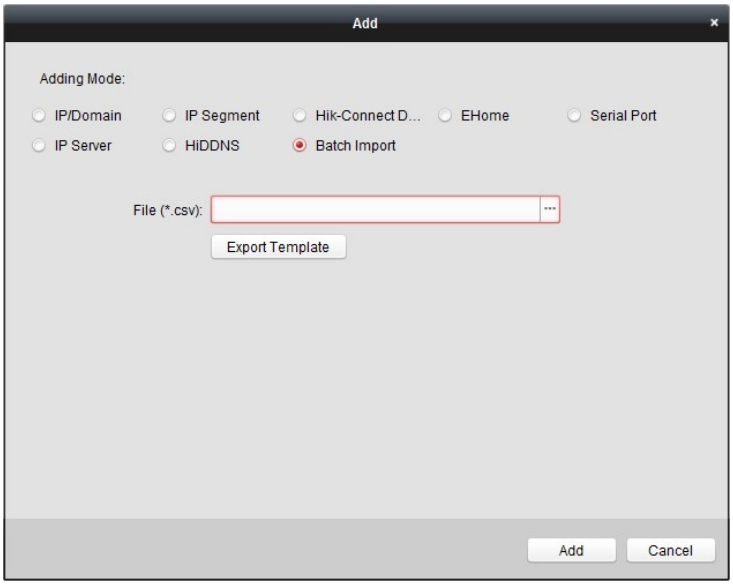
Importazione di dispositivi in batch

Scopo:

I dispositivi possono essere aggiunti in batch al software, inserendo le informazioni dei dispositivi in un file CSV predefinito.

Passaggi:

1. Fare clic su **Add** per aprire la finestra di dialogo di aggiunta dei dispositivi.
2. Selezionare **Batch Import** come modalità di aggiunta.



3. Fare clic su **Export Template** e salvare il modello predefinito (file CSV) sul PC.
4. Aprire il file di modello esportato e inserire le informazioni richieste relative ai dispositivi da aggiungere nella corrispondente colonna.

   Nickname: modificare un nome per il dispositivo come si desidera.

   Adding Mode: è possibile inserire i valori 0, 2, 3, 4, 5 o 6 che indicano le diverse modalità di aggiunta. 0 indica che il dispositivo è aggiunto tramite indirizzo IP o nome di dominio; 2 indica che il dispositivo è aggiunto tramite server IP; 3 indica che il dispositivo è aggiunto tramite HiDDNS; 4 indica che il dispositivo è aggiunto tramite protocollo EHome; 5 indica che il dispositivo è aggiunto tramite porta seriale; 6 indica che il dispositivo è aggiunto tramite dominio Hik-Connect.

   Address: modificare l'indirizzo del dispositivo. Se la modalità di aggiunta è impostata su 0, occorre inserire l'indirizzo IP o il nome di dominio del dispositivo; se la modalità di aggiunta è impostata su 2, occorre inserire l'indirizzo IP del PC su cui è installato il server IP; se la modalità di aggiunta è impostata su 3, occorre inserire l'indirizzo *www.hik-online.com*.

   Port: inserire il numero di porta del dispositivo. Il valore predefinito è *8000*.

   Device Information: se la modalità di aggiunta impostata è 0, questo campo non è richiesto; se la modalità di aggiunta impostata è 2, inserire l'ID del dispositivo registrato sul server IP; se la modalità di aggiunta impostata è 3, inserire il nome dominio del dispositivo registrato sul server HiDDNS; se la modalità di aggiunta impostata è 4, inserire l'account EHome; se la modalità di aggiunta impostata è 6, inserire il numero di serie del dispositivo.

   User Name: immettere il nome utente del dispositivo. Per impostazione predefinita, il nome utente è *admin*. **Password**: inserire la password del dispositivo.

PASSWORD COMPLESSA CONSIGLIATA: *si consiglia vivamente di creare una password complessa (lunga almeno 8 caratteri e comprendente lettere maiuscole e minuscole, nonché numeri e caratteri speciali) in modo da aumentare la sicurezza del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.*

Add Offline Device: è possibile inserire 1 per abilitare l'aggiunta di un dispositivo offline, quindi il software si connetterà automaticamente quando il dispositivo offline passa online. 0 indica la disattivazione di questa funzione.

Export to Group: è possibile immettere 1 per creare un gruppo in base al nome del dispositivo (soprannome). Per impostazione predefinita, tutti i canali del dispositivo verranno importati nel gruppo corrispondente. 0 indica la disattivazione di questa funzione.

Channel Number: se si imposta 1 per Add Offline Device, immettere il numero di canale del dispositivo. Se si imposta 0 per Add Offline Device, questo campo non è obbligatorio.

Alarm Input Number: se si imposta 1 per Add Offline Device, immettere il numero dell'ingresso di allarme del dispositivo. Se si imposta 0 per Add Offline Device, questo campo non è obbligatorio.

Serial Port No.: se la modalità di aggiunta è impostata su 5, inserire il numero di porta seriale del dispositivo di controllo accessi.

Baud Rate: se la modalità di aggiunta è impostata su 5, inserire la velocità in baud del dispositivo di controllo accessi.

DIP: se la modalità di aggiunta è impostata su 5, inserire l'indirizzo del DIP del dispositivo di controllo accessi.

Hik-Connect Account: se la modalità di aggiunta è impostata su 6, inserire l'account Hik-Connect.

Hik-Connect Password: se la modalità di aggiunta è impostata su 6, inserire la password di Hik-Connect.

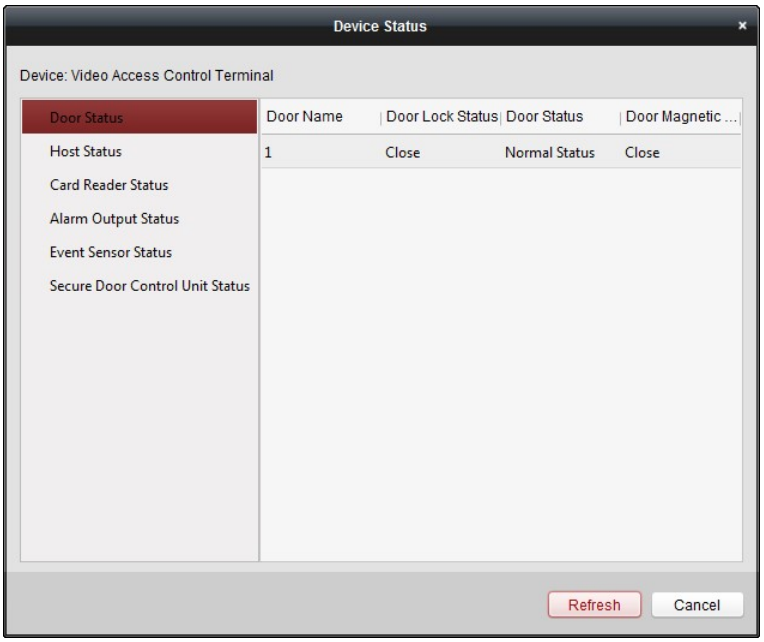
5. Fare clic su ··· e selezionare il file del modello.
6. Fare clic su **Add** per importare i dispositivi.

I dispositivi aggiunti correttamente saranno visualizzati nell'elenco di gestione dei dispositivi. In tale elenco, è possibile consultare l'utilizzo della risorsa, lo stato di HDD e registrazioni e altre informazioni relative ai dispositivi aggiunti.

Fare clic su **Refresh All** per aggiornare le informazioni relative a tutti i dispositivi aggiunti. Inserendo il nome del dispositivo nel campo filtro, è possibile effettuarne la ricerca.

7.4.2 Visualizzazione dello stato del dispositivo

È possibile selezionare un dispositivo dall'elenco e poi fare clic sul pulsante **Device Status** per visualizzarne lo stato.



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

Door Status: indica lo stato della porta collegata.

Host Status: indica lo stato dell'host, come Storage Battery Power Voltage, Device Power Supply Status, Multi-door Interlocking Status, Anti-passing Back Status e Host Anti-Tamper Status.

Card Reader Status: indica lo stato del lettore di tessere.

Nota: se si utilizza il lettore di tessere con una connessione RS-485 ad un controllore, è possibile visualizzare lo stato online o offline ed il codice prodotto. Se si utilizza il lettore di tessere con una connessione Wiegand, si visualizza lo stato Wiegand/485Offline.

Alarm Output Status: indica lo stato dell'uscita di allarme di ciascuna porta.

Event Sensor Status: indica lo stato del sensore di eventi di ciascuna porta.

Secure Door Control Unit Status: indica lo stato di collegamento online e di manomissione dell'unità di controllo porta protetta.

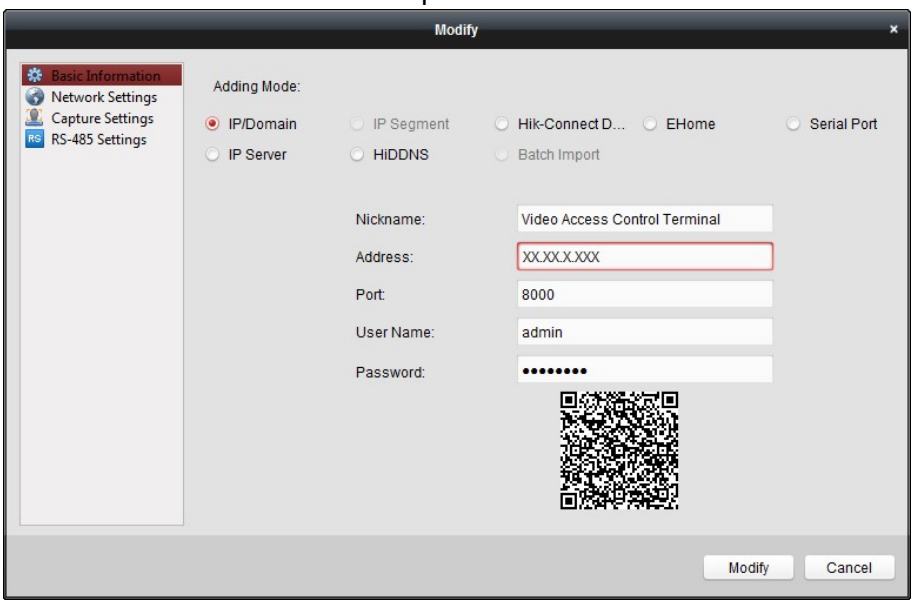
7.4.3 Modifica delle informazioni di base

Scopo:

Dopo aver aggiunto il dispositivo di controllo accessi, è possibile modificarne le informazioni di base.

Passaggi:

1. Selezionare il dispositivo dal relativo elenco.
2. Fare clic su **Modify** per far apparire la finestra di modifica del dispositivo.
3. Fare clic sulla schermata **Basic Information** per accedere all'interfaccia Basic Information.



4. Modificare le informazioni sul dispositivo, tra cui 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 l'aggiunta dei dispositivi di controllo accessi, è possibile impostare la modalità di caricamento, il centro di rete e il centro comunicazioni wireless.

Selezionare il dispositivo nell'elenco dei dispositivi e fare clic su **Modify** per far apparire la finestra con le informazioni di modifica del dispositivo.

Fare clic sulla schermata **Network Settings** per accedere all'interfaccia delle impostazioni di rete.

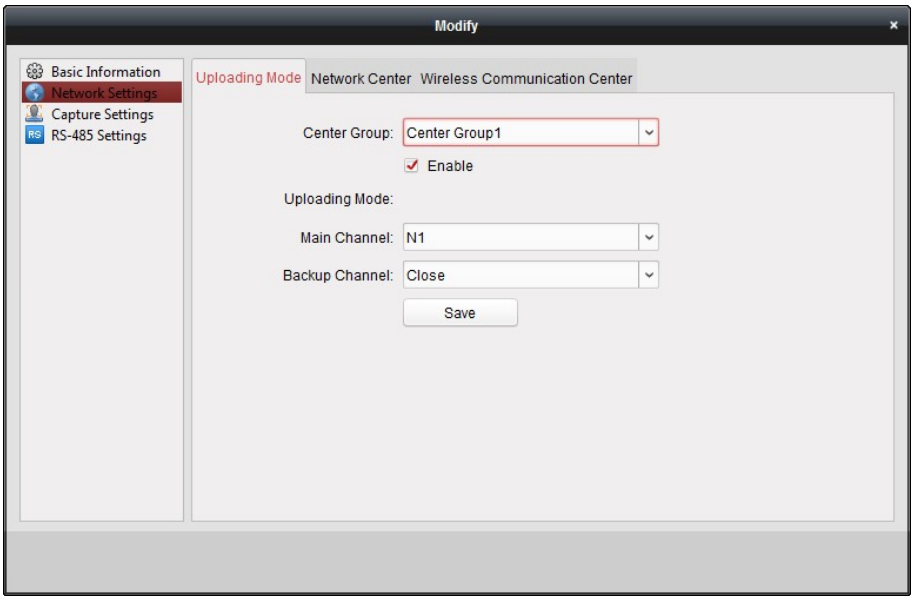
Impostazioni della modalità di caricamento

Scopo:

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

Passaggi:

1. Fare clic sulla schermata **Uploading Mode**.



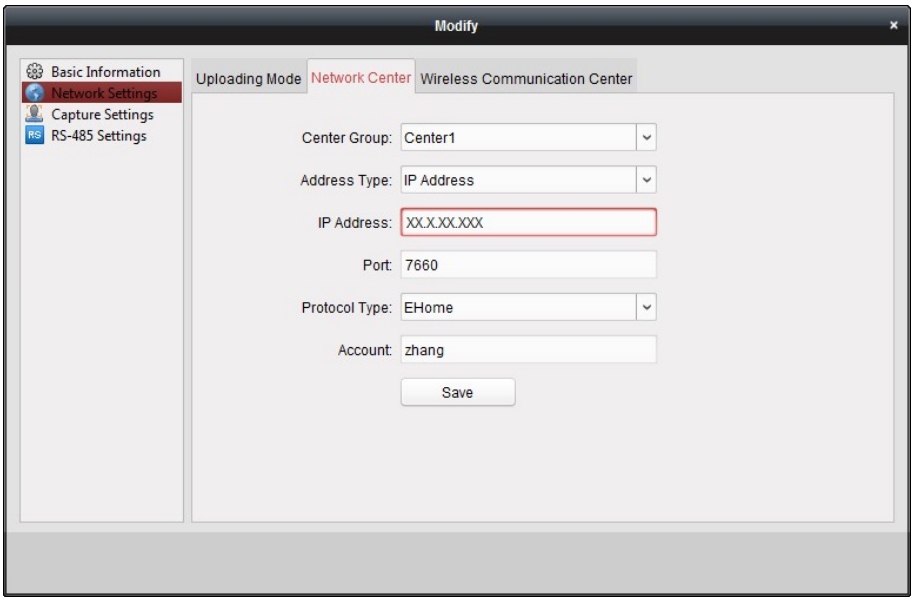
2. Selezionare il gruppo centrale dall'elenco a discesa.
3. Attivare la casella di controllo **Enable** per abilitare il gruppo centrale selezionato.
4. Selezionare dall'elenco a discesa la modalità di caricamento. È possibile abilitare l'opzione **N1/G1** per il canale principale e quello di backup, o selezionare **Close** per disabilitare il canale principale o quello di backup. ***Nota:*** il canale principale e quello di backup non possono attivare contemporaneamente N1 o G1.
5. Fare clic sul pulsante **Save** per salvare i parametri.

Impostazioni del centro di rete

È possibile impostare l'account per il protocollo EHome nella pagina Network Settings. Sarà poi possibile aggiungere dispositivi tramite il protocollo EHome.

Passaggi:

1. Fare clic sulla schermata **Network Center**.



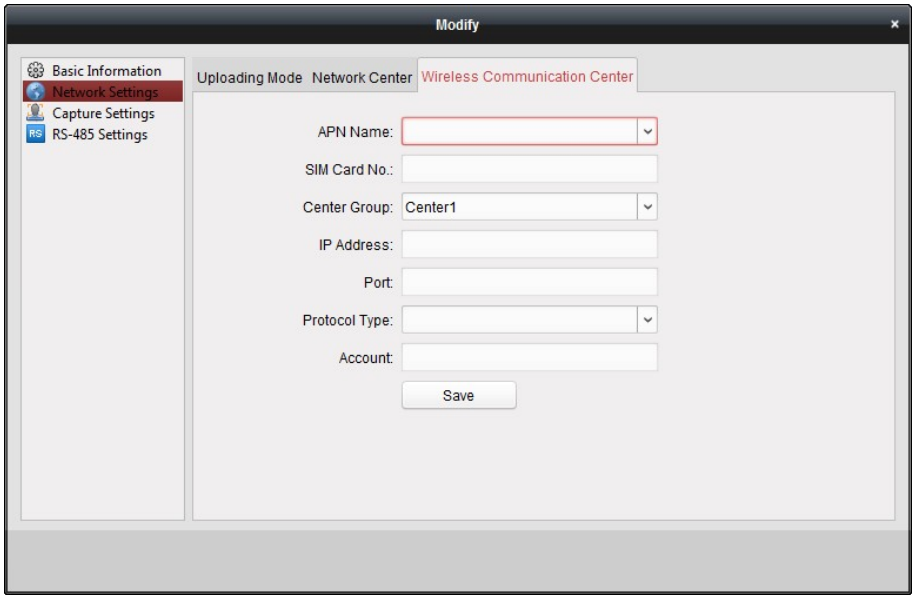
2. Selezionare il gruppo centrale dall'elenco a discesa.

3. Impostare Address Type su **IP Address** o **Domain Name**.
4. Immettere l'indirizzo IP o il nome di dominio in base al tipo di indirizzo.
5. Immettere il numero di porta del protocollo. Per impostazione predefinita, il numero di porta è 7660.
6. Impostare Protocol Type su EHome.
7. Impostare un nome account per il centro di rete.
   Nota: il nome per l'account può comprendere da 1 a 32 caratteri alfanumerici.
8. Fare clic sul pulsante **Save** per salvare i parametri.
   Note:
   Il numero di porta della rete wireless e di quella cablata deve essere coerente con il numero di porta di EHome.
   È possibile impostare il nome di dominio nell'area Enable NTP come illustrato in *Modifica dell'ora* nella sezione Configurazione remota. Per i dettagli, consultare *Ora* nella sezione *7.4.7 Configurazione remota*.

Impostazioni del centro comunicazioni wireless

Passaggi:

1. Fare clic sulla schermata **Wireless Communication Center**.



2. Selezionare come nome APN CMNET o UNINET.
3. Inserire il numero della tessera SIM.
4. Selezionare il gruppo centrale dall'elenco a discesa.
5. Inserire l'indirizzo IP e il numero di porta.
6. Impostare Protocol Type su EHome. Per impostazione predefinita, il numero di porta per EHome è 7660.
7. Impostare un nome account per il centro di rete. In ciascuna piattaforma, va usato un nome account coerente.
8. Fare clic sul pulsante **Save** per salvare i parametri.
   Nota: il numero di porta della rete wireless e di quella cablata deve essere coerente con il numero di porta di EHome.

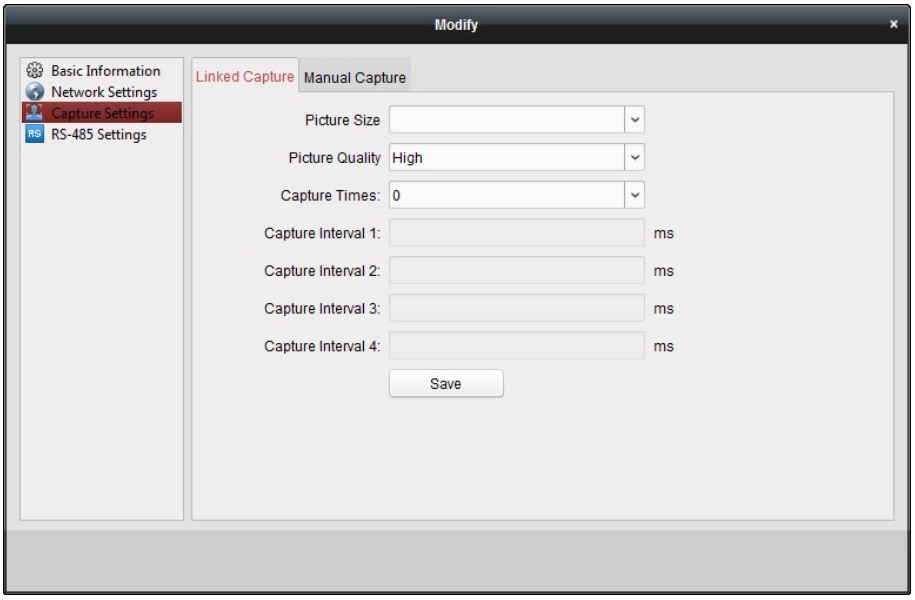
7.4.5 Impostazioni di acquisizione

È possibile impostare i parametri di collegamento acquisizioni e acquisizioni manuali.
Selezionare il dispositivo nell'elenco dei dispositivi e fare clic su **Modify** per far apparire la finestra con le informazioni di modifica del dispositivo.
Fare clic sulla schermata **Capture Settings** per accedere all'interfaccia delle impostazioni di acquisizione.
Note:
La funzione **Capture Settings** deve essere supportata dal dispositivo.
Prima di definire le impostazioni di acquisizione, occorre configurare il server di archiviazione per l'archiviazione di immagini.

Acquisizioni collegate

Passaggi:

1. Selezionare la schermata **Linked Capture**.

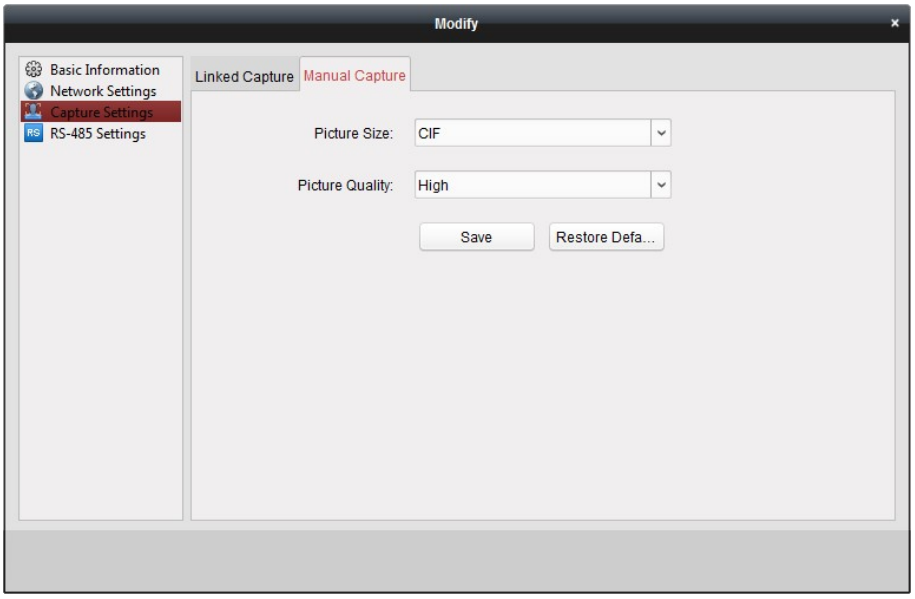


2. Impostare le dimensioni e la qualità dell'immagine.
3. Impostare i tempi dell'acquisizione collegata una volta attivata.
4. Impostare l'intervallo di acquisizione in base ai tempi di acquisizione.
5. Fare clic su **Save** per salvare le impostazioni.

Acquisizione manuale

Passaggi:

1. Selezionare la schermata **Manual Capture**.



2. Selezionare la risoluzione delle immagini acquisite dall'elenco a discesa.
   Nota: i tipi di risoluzione supportati sono CIF, QCIF, 4CIF/D1, SVGA, HD720P, VGA, WD1 e AUTO.
3. Impostare la qualità dell'immagine su High, Medium o Low.
4. Fare clic su **Save** per salvare le impostazioni.
5. È possibile fare clic su **Restore Default Value** per ripristinare i parametri alle impostazioni predefinite.

7.4.6 Impostazioni dei parametri RS-485

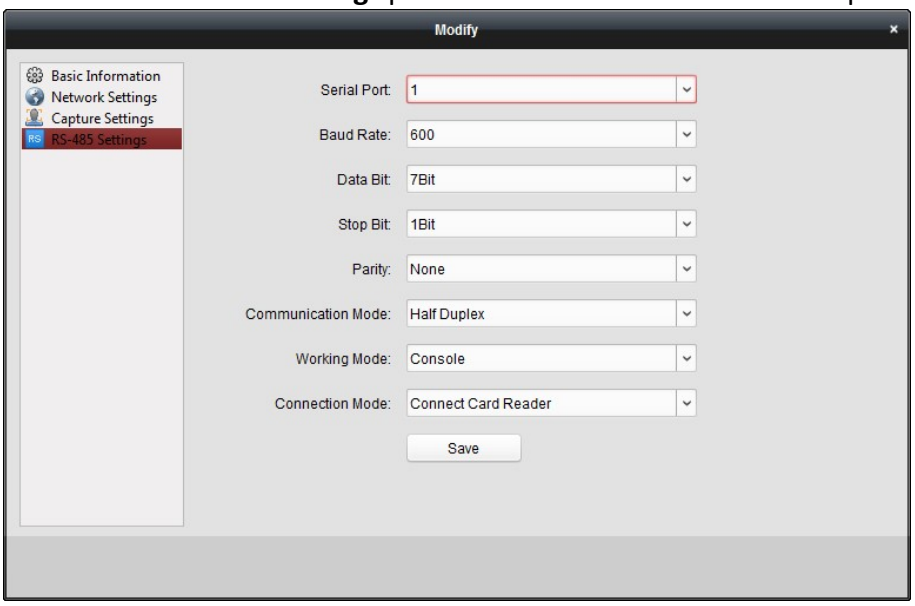
Scopo:

È possibile impostare i parametri RS-485 come la porta seriale, la velocità in baud, il bit dei dati, il bit di stop, il tipo di parità, la modalità di comunicazione, la modalità operativa e la modalità di connessione.

Nota: le impostazioni di RS-485 devono essere supportate dal dispositivo.

Passaggi:

1. Selezionare il dispositivo nell'elenco dei dispositivi e fare clic su **Modify** per far apparire la finestra con le informazioni di modifica del dispositivo.
2. Fare clic sulla schermata **RS-485 Settings** per accedere all'interfaccia delle impostazioni di RS-485.



3. Selezionare il numero di serie della porta dall'elenco a discesa per impostare i parametri RS-485.
4. Impostare la velocità in baud, il bit dei dati, il bit di stop, il tipo di parità, la modalità di comunicazione, la modalità operativa e la modalità di connessione nell'elenco a discesa.
5. Fare clic su **Save** per salvare le impostazioni e i parametri configurati verranno applicati automaticamente al dispositivo.

   Nota: dopo aver modificato la modalità operativa, il dispositivo verrà riavviato. Una volta modificata la modalità operativa, comparirà un messaggio.

7.4.7 Configurazione remota

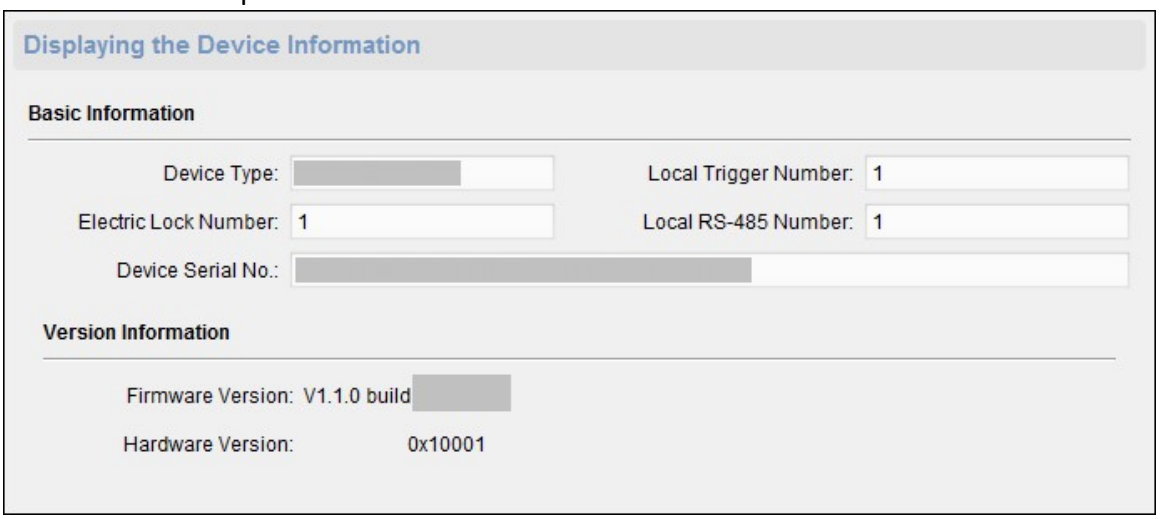
Scopo:

Nell'elenco dei dispositivi, selezionare il dispositivo e fare clic sul pulsante **Remote Configuration** per accedere all'interfaccia di configurazione remota. È possibile impostare i parametri dettagliati del dispositivo selezionato.

Controllo delle informazioni del dispositivo

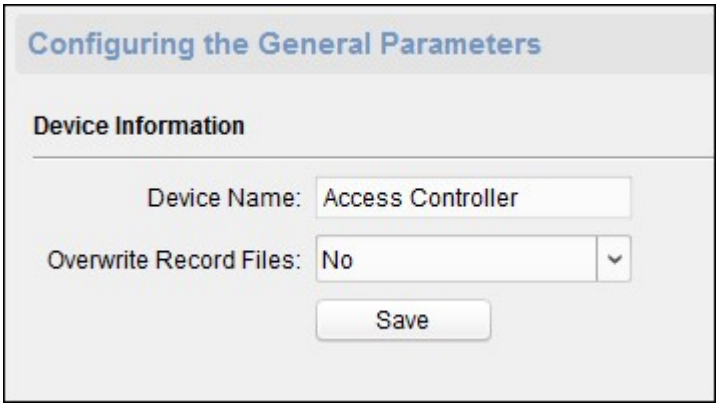
Passaggi:

1. Nell'elenco dei dispositivi, è possibile fare clic su **Remote Configuration** per accedere all'interfaccia di configurazione remota.
2. Fare clic su **System** -> **Device Information** per controllare le informazioni di base e quelle relative alla versione del dispositivo.



Modifica del nome del dispositivo

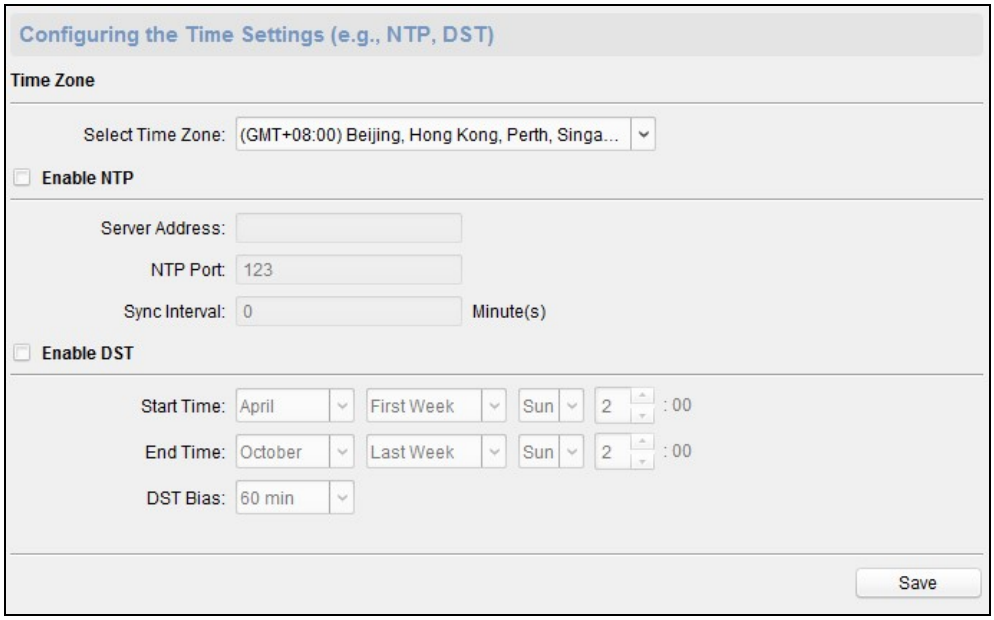
Nell'interfaccia Remote Configuration, fare clic su **System** -> **General** per configurare il nome del dispositivo e sovrascrivere il parametro dei file di registrazione. Fare clic su **Save** per salvare le impostazioni.



Modifica dell'ora

Passaggi:

1. Nell'interfaccia Remote Configuration, fare clic su **System** -> **Time** per configurare il fuso orario.
2. (Opzionale) Selezionare **Enable NTP** e configurare l'indirizzo del server NTP, la porta NTP e l'intervallo di sincronizzazione.
3. (Opzionale) Selezionare **Enable DST** e configurare l'ora di inizio, l'ora di fine e la differenza dell'ora legale.
4. Fare clic su **Save** per salvare le impostazioni.



Configurazione della manutenzione del sistema

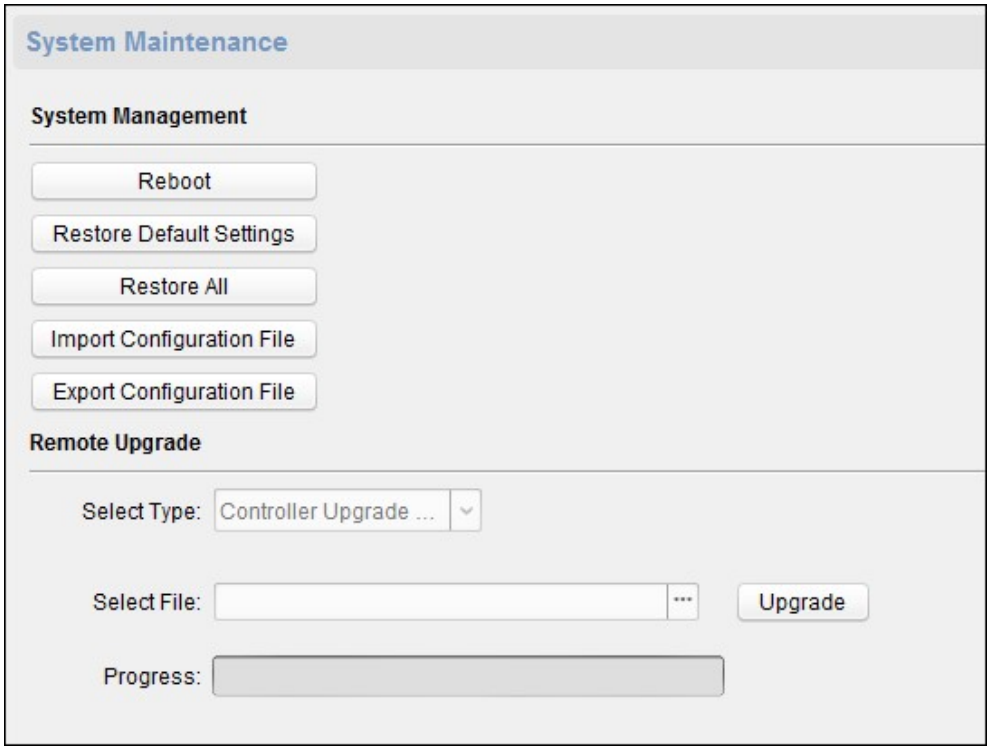
Scopo:

È possibile riavviare il dispositivo da remoto, ripristinarlo alle impostazioni predefinite, importarne il file di configurazione, aggiornarlo, ecc.

Passaggi:

1. Nell'interfaccia Remote Configuration, fare clic su **System** -> **System Maintenance**.
2. Fare clic su **Reboot** per riavviare il dispositivo.
   In alternativa, fare clic su **Restore Default Settings** per ripristinare le impostazioni predefinite del dispositivo, eccetto l'indirizzo IP.
   In alternativa, fare clic su **Restore All** per ripristinare i parametri predefiniti del dispositivo. Il dispositivo deve essere attivato dopo il ripristino.
   Nota: il file di configurazione contiene i parametri del dispositivo.
   In alternativa, fare clic su **Import Configuration File** per importare il file di configurazione dal computer locale al dispositivo.
   In alternativa, fare clic su **Export Configuration File** per esportare il file di configurazione dal dispositivo al computer locale.
   Nota: il file di configurazione contiene i parametri del dispositivo.

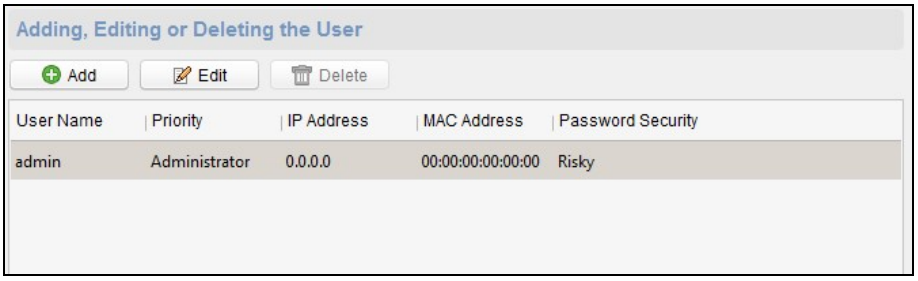
3. È possibile anche aggiornare il dispositivo da remoto.
   1) Nella sezione Remote Upgrade, fare clic su ··· per selezionare il file di aggiornamento.
   2) Fare clic su **Upgrade** per avviare l'aggiornamento.



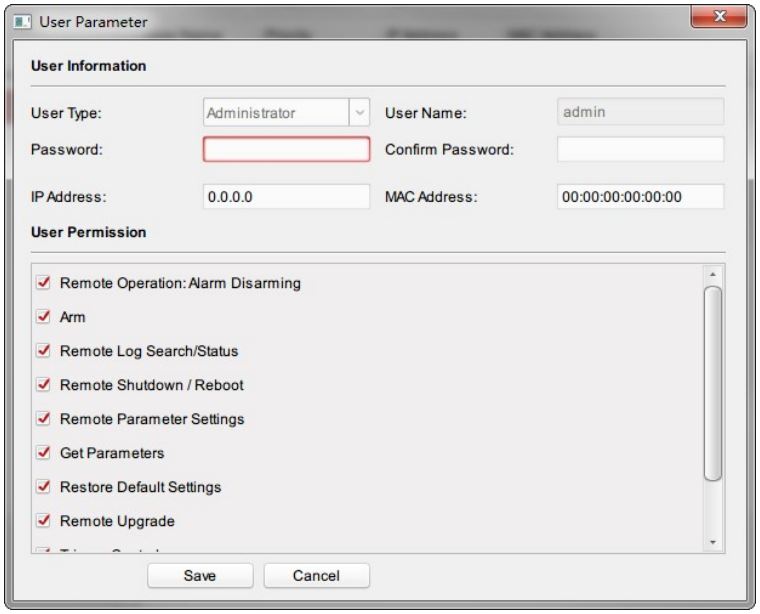
Gestione degli utenti

Passaggi:

1. Nell'interfaccia Remote Configuration, fare clic su **System** -> **User**.



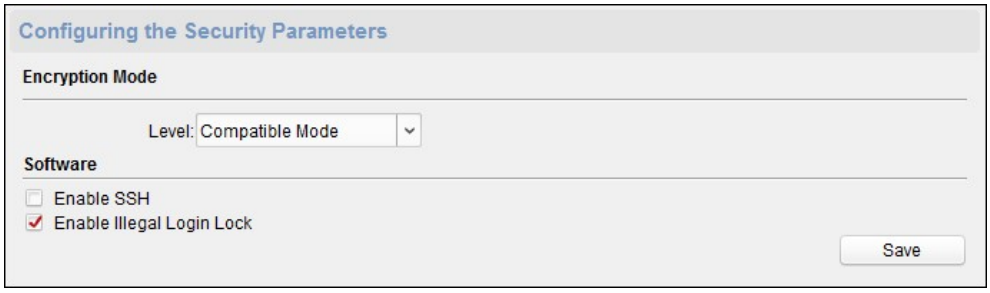
2. Fare clic su **Add** per aggiungere l'utente (non supportato dal controller dell'ascensore).
   In alternativa, selezionare un utente dall'elenco e fare clic su **Edit** per modificarlo. È possibile modificare la password, l'indirizzo IP, l'indirizzo MAC e l'autorizzazione dell'utente. Fare clic su **OK** per confermare la modifica.



Configurazione della sicurezza

Passaggi:

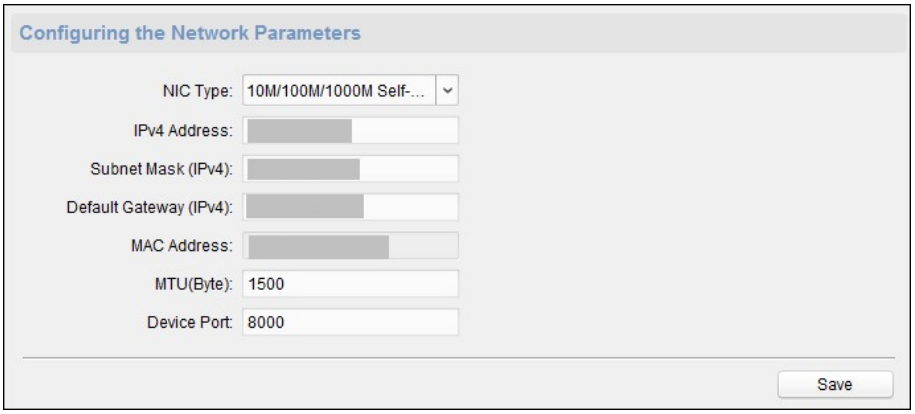
1. Fare clic su **System** -> **Security**.



2. Selezionare la modalità di crittografia dall'elenco a discesa.
   È possibile selezionare Compatible Mode o Encryption Mode.
3. Fare clic su **Save** per salvare le impostazioni.

Configurazione dei parametri di rete

Fare clic su **Network** -> **General**. È possibile configurare il tipo di NIC, l'indirizzo IPv4, la subnet mask (IPv4), il gateway predefinito (IPv4), l'indirizzo MTU, l'MTU e la porta del dispositivo. Fare clic su **Save** per salvare le impostazioni.



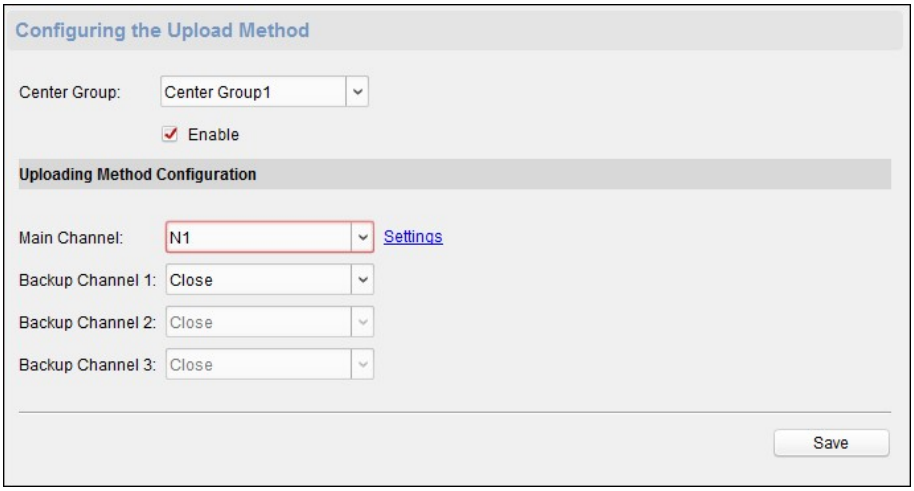
Configurazione del metodo di caricamento

Scopo:

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

Passaggi:

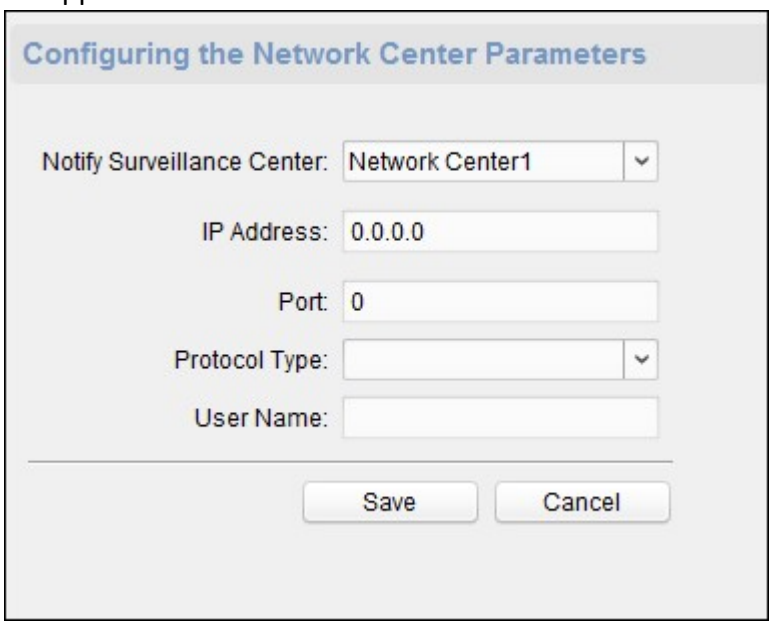
1. Fare clic su **Network** -> **Report Strategy**.



2. Selezionare un gruppo centrale dall'elenco a discesa.
3. Selezionare la casella di controllo **Enable**.
4. Impostare il metodo di caricamento.
   È possibile impostare il canale principale e quello di backup.
5. Fare clic su **Settings** a destra del campo del canale per impostare le informazioni dettagliate.
6. Fare clic su **Save** per salvare le impostazioni.

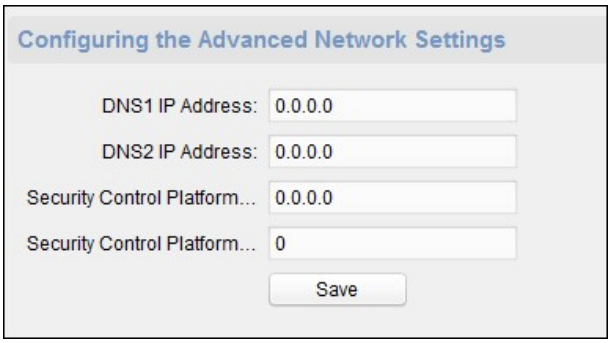
Configurazione del centro di rete

È possibile impostare il centro di sorveglianza delle notifiche, l'indirizzo IP del centro, il numero di porta, il protocollo (EHome) e il nome utente dell'account EHome, affinché trasmettano i dati tramite il protocollo EHome. Per i dettagli sulla trasmissione del protocollo EHome, consultare la sezione *Impostazioni del centro di rete* nel *capitolo 7.4.4 Impostazioni di rete.* Fare clic su **Save** per salvare le impostazioni oppure fare clic su



Configurazione avanzata della rete

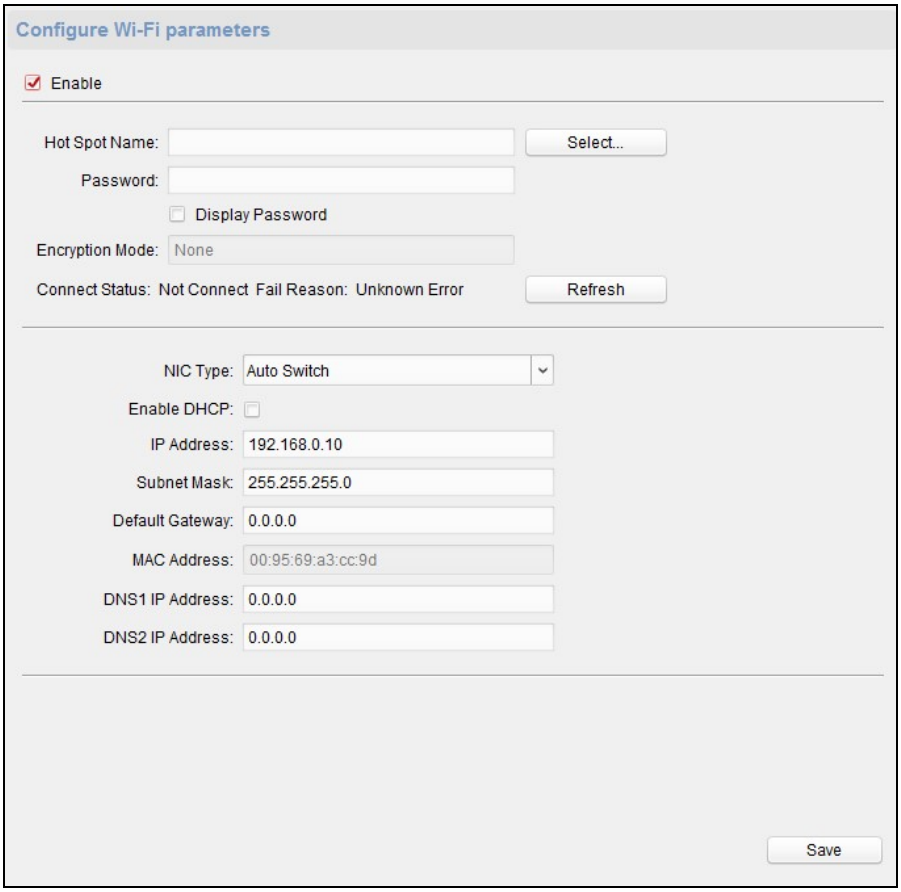
Fare clic su **Network** -> **Advanced Settings**. È possibile configurare l'indirizzo IP del DNS 1, l'indirizzo IP del DNS 2, l'IP e la porta della piattaforma di controllo della sicurezza. Fare clic su **Save** per salvare le impostazioni.



Configurazione della connessione Wi-Fi

Passaggi:

1. Fare clic su **Network** –> **Wi-Fi**.

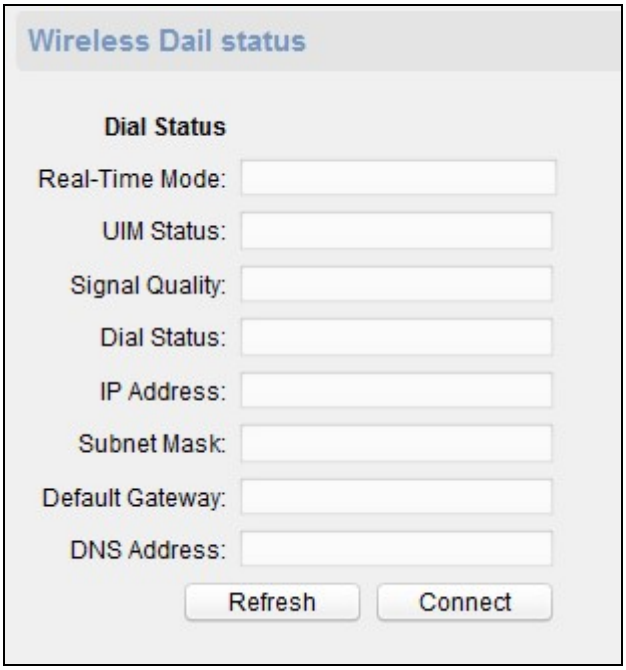


2. Selezionare **Enable** per attivare la funzione Wi-Fi.
3. Immettere il nome dell'hot spot.
   In alternativa, è possibile fare clic su **Select…** per selezionare una rete.
4. Immettere la password per il Wi-Fi.
5. (Opzionale) Fare clic su **Refresh** per aggiornare lo stato della rete.
6. (Opzionale) Selezionare il tipo di NIC.
7. (Opzionale) Deselezionare **Enable DHCP** e impostare l'indirizzo IP, la subnet mask, il gateway predefinito, l'indirizzo MAC, l'indirizzo IP DNS1 e l'indirizzo IP DNS2.
8. Fare clic su **Save** per salvare le impostazioni.

Configurazione dello stato di composizione wireless

Passaggi:

1. Fare clic su **Network** -> **Wireless Dial**.

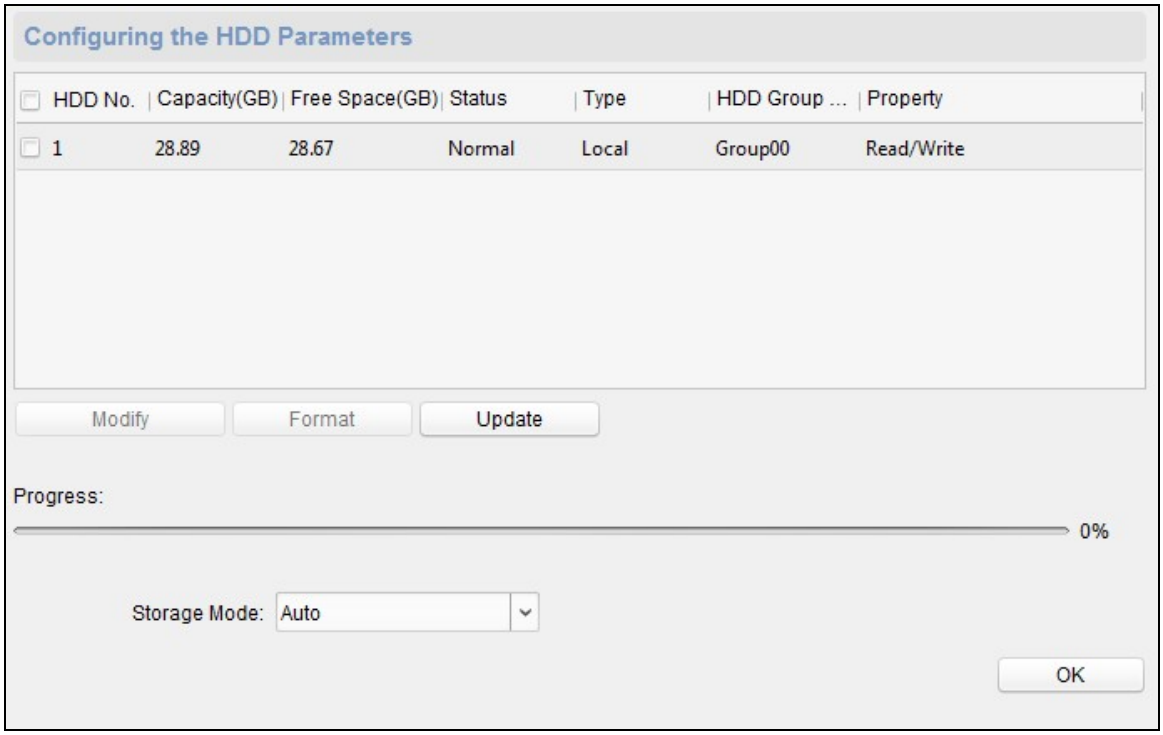


2. Modificare lo stato di composizione, inclusa la modalità in tempo reale, lo stato UIM, la qualità del segnale, lo stato di composizione, l'indirizzo IP, la subnet mask, il gateway predefinito e l'indirizzo DNS.
3. Fare clic su **Connect** per avviare la connessione.
   In alternativa, fare clic su **Refresh** per aggiornare lo stato.

Configurazione dei parametri dell'unità HDD

Passaggi:

1. Fare clic su **Storage** -> **General**.

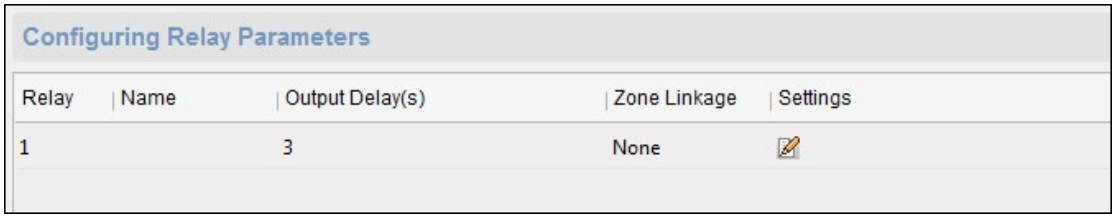


2. Verificare le voci relative al numero dell'unità HDD (tessera SD), alla capacità, allo spazio libero, allo stato, ecc.
   È possibile anche modificare e formattare l'HDD (tessera SD). In alternativa, fare clic su **Update** per aggiornare i dati.
3. Selezionare la modalità di archiviazione.
4. Fare clic su **Save** per salvare le impostazioni.

Configurazione dei parametri del relè

Passaggi:

1. Fare clic su **Alarm** -> **Relay**.
   È possibile visualizzare i parametri del relè.

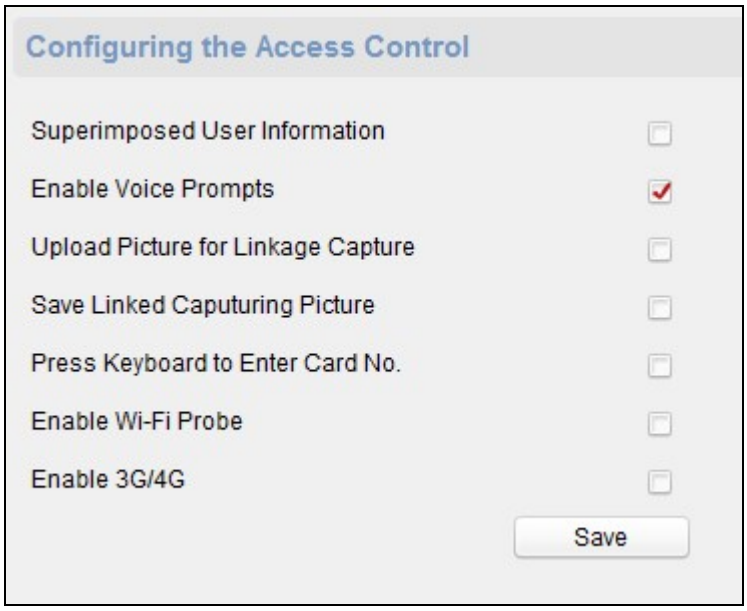


2. Fare clic su per visualizzare le impostazioni dei parametri del relè.
3. Impostare il nome del relè e il ritardo di uscita.
4. Fare clic su **Save** per salvare i parametri.
   In alternativa, fare clic su **Copy to…** per copiare le informazioni del relè in altri relè.

Configurazione dei parametri di controllo accessi

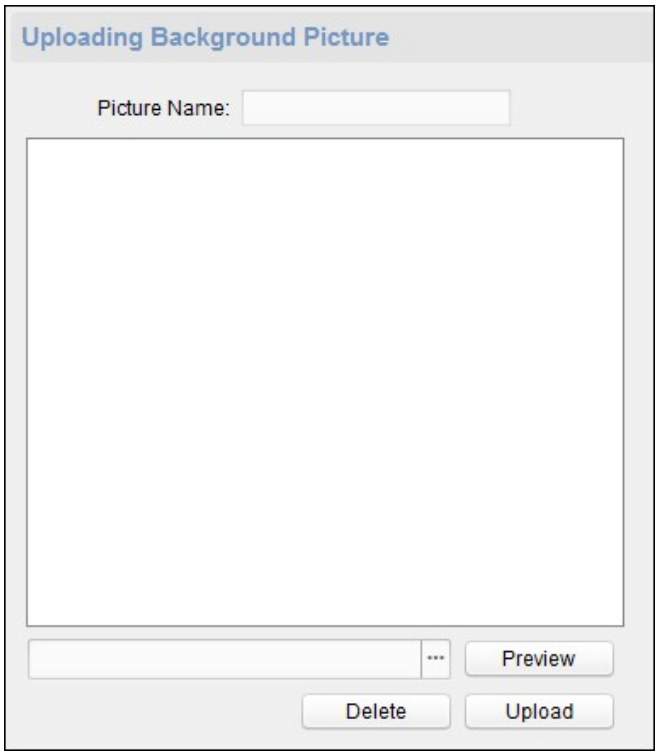
Passaggi:

Nell'interfaccia Remote Configuration, fare clic su **Other** -> **Access Control Parameters**. Selezionare **Superimposed user information**, **Enable voice prompts**, **Upload picture to capture whether the linkage**, **Save Linked Captured Pictures**, **Whether to allow key input card number**, **Enable WiFi detect** e **Enable 3G/4G**. Fare clic su **Save** per salvare le impostazioni.



Caricamento dell'immagine di sfondo

Fare clic su **Other** -> **Picture Upload**. Fare clic su ··· per selezionare l'immagine dal computer locale. È possibile anche fare clic su **Live View** per visualizzare un'anteprima dell'immagine. Fare clic su **Picture Upload** per caricare l'immagine. ***Nota:*** questa funzione deve essere supportata dal dispositivo.



Configurazione dei parametri di riconoscimento dei volti

Fare clic su **Other** -> **Face Detection**. È possibile selezionare la casella di controllo **Enable** per attivare la funzione di rilevamento dei volti del dispositivo.

Dopo aver attivato la funzione, il dispositivo dovrebbe rilevare il volto durante l'autenticazione. In caso contrario, l'autenticazione non verrà eseguita correttamente.

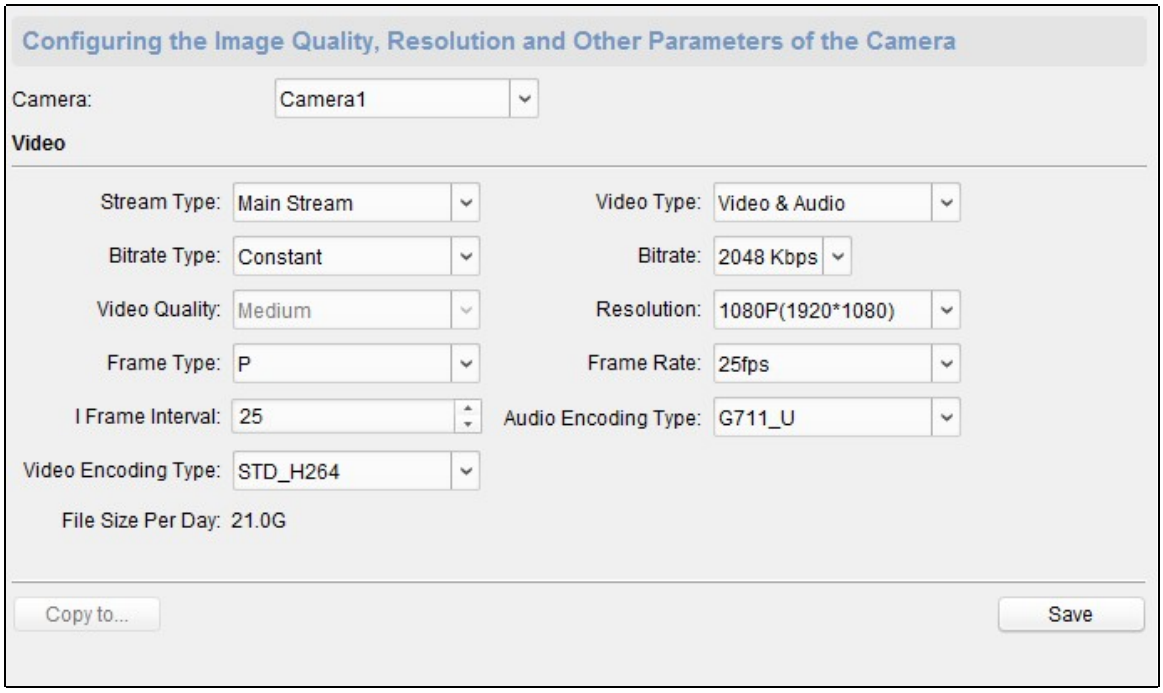
Nota: questa funzione è supportata solo dai dispositivi con funzione video.

Configurazione dei parametri video e audio

È possibile impostare i parametri della compressione video.

Passaggi:

1. Fare clic su **Image** -> **Video & Audio**



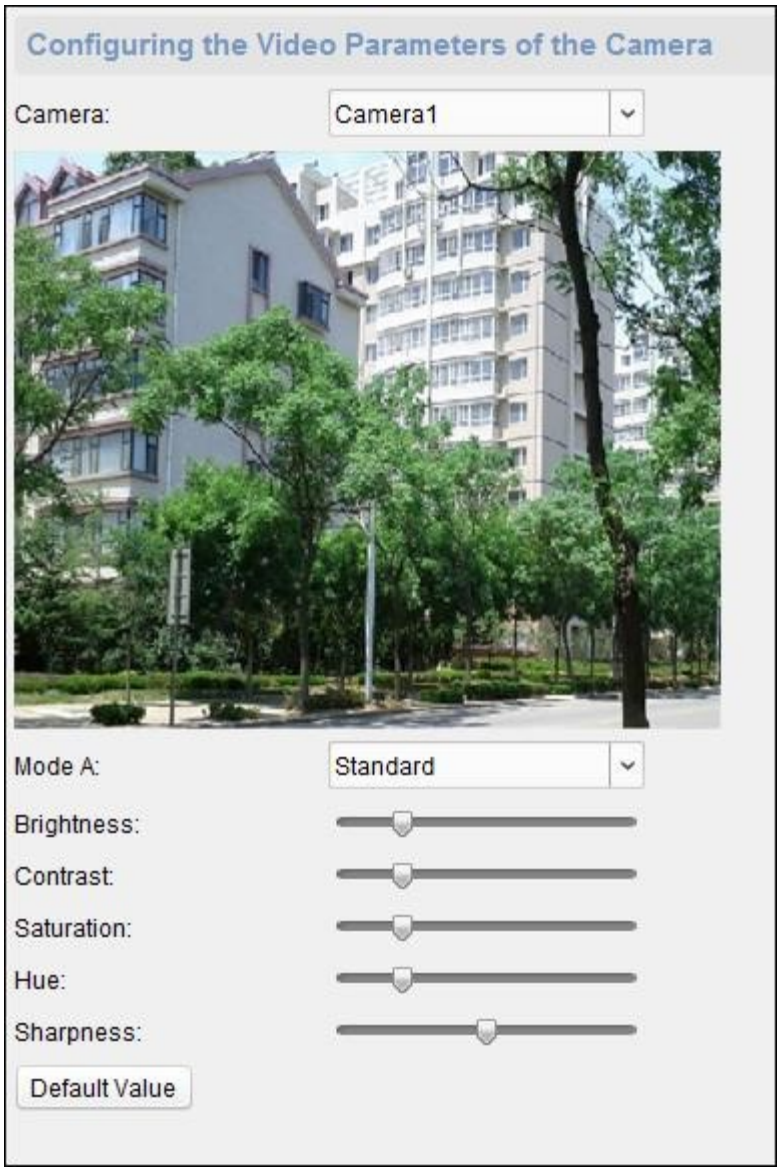
2. Selezionare una telecamera dall'elenco a discesa.
3. Impostare i parametri video della telecamera, tra cui il tipo di streaming, il tipo di bitrate, la qualità video, il tipo di fotogramma, il tipo di fotogramma I, il tipo di codifica video, il tipo di video, il bitrate, la risoluzione, la frequenza dei fotogrammi e il tipo di codifica audio.
4. Fare clic su **Save** per salvare le impostazioni.
   In alternativa, fare clic su **Copy to…** per copiare i parametri in altre telecamere.

Configurazione dei parametri delle immagini video

È possibile impostare la modalità, la luminosità, il contrasto, la saturazione, la tonalità e la nitidezza della telecamera.

Passaggi:

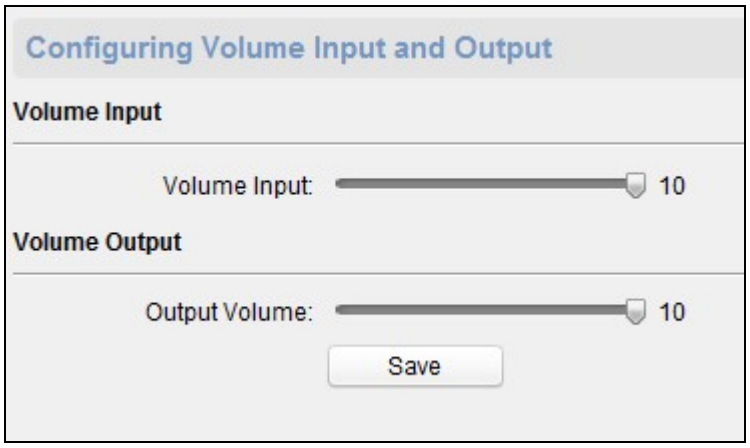
1. Fare clic su **Image** -> **Image Settings**.



2. Selezionare una telecamera dall'elenco a discesa.
3. Impostare la modalità, la luminosità, il contrasto, la saturazione, la tonalità e la nitidezza della telecamera.
   In alternativa, fare clic su **Default Value** per impostare i parametri predefiniti.

Configurazione dell'ingresso e dell'uscita del volume

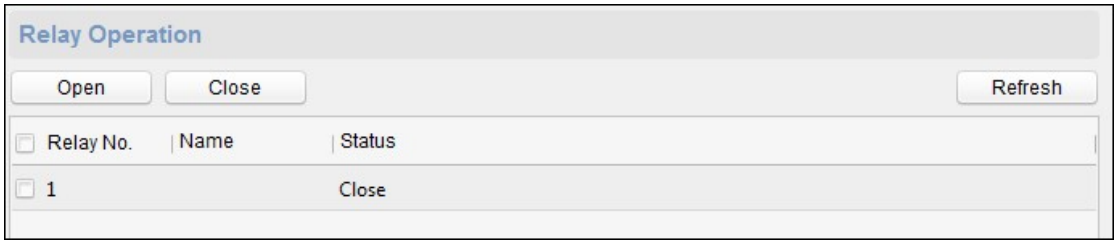
Fare clic su **Image** -> **Volume Input/Output**. È possibile impostare l'ingresso e l'uscita del volume. Fare clic su **Save** per salvare le impostazioni.



Utilizzo del relè

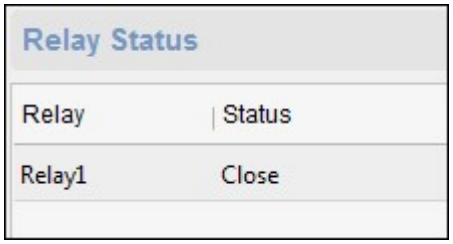
Passaggi:

1. Fare clic su **Operation** -> **Relay**.
   È possibile visualizzare lo stato del relè.
2. Selezionare la casella di controllo del relè.
3. Fare clic su **Open** o **Close** per aprire/chiudere il relè.
4. (Opzionale) Fare clic su **Refresh** per aggiornare lo stato del relè.



Visualizzazione dello stato del relè

Fare clic su **Status** -> **Relay** per visualizzare lo stato del relè.



7.5 Gestione dell'organizzazione

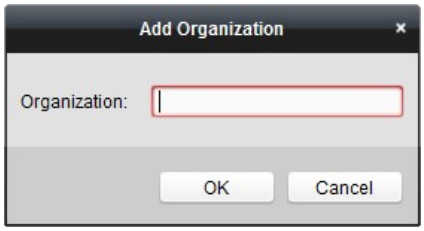
È possibile aggiungere, modificare o eliminare organizzazioni in base alle esigenze.

Fare clic sulla schermata  per accedere all'interfaccia Person and Card Management.

7.5.1 Aggiunta di organizzazioni

Passaggi:

1. Nell'elenco organizzazioni sulla sinistra, è necessario aggiungere l'organizzazione di livello più alto, come organizzazione padre di tutte le altre.
   Fare clic sul pulsante **Add** per far apparire l'interfaccia di aggiunta delle organizzazioni.



2. Inserire il nome preferito per l'organizzazione.
3. Fare clic su **OK** per salvare l'aggiunta.
4. È possibile aggiungere più livelli di organizzazioni, in base alle necessità.
   Per aggiungere organizzazioni secondarie, selezionare l'organizzazione padre e fare clic su **Add**.
   Ripetere i *Passaggi 2* e *3* per aggiungere le organizzazioni secondarie.
   In tal modo, le organizzazioni aggiunte figureranno come organizzazioni secondarie di quelle di livello superiore.
   Nota: è possibile creare un massimo di 10 livelli di organizzazioni.

7.5.2 Modifica ed eliminazione di organizzazioni

Selezionando un'organizzazione aggiunta e facendo clic su **Modify**, è possibile modificarne il nome.
Selezionando un'organizzazione e facendo clic sul pulsante **Delete**, è possibile eliminarla.

Note:

Eliminando un'organizzazione, anche quelle definite ai suoi livelli inferiori saranno cancellate.

Per poter eliminare un'organizzazione, è necessario che non vi siano state aggiunte persone.

7.6 Gestione delle persone

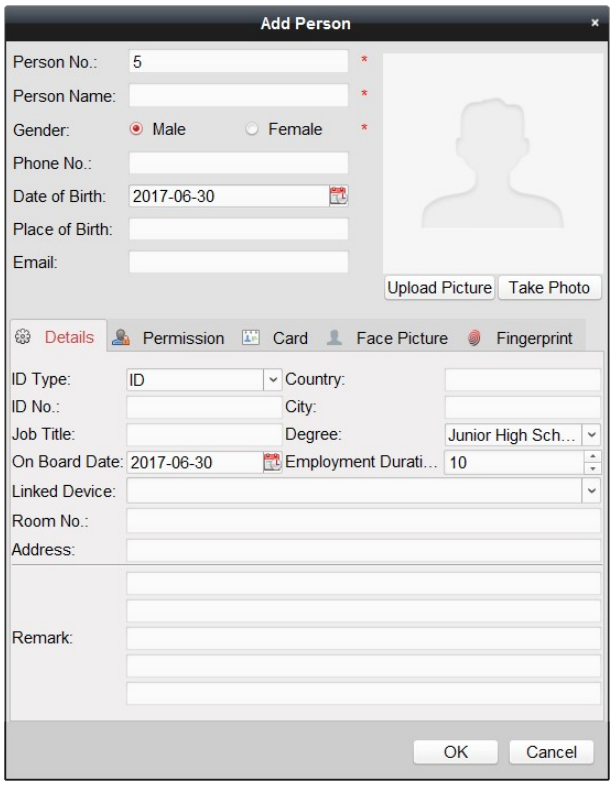
Dopo l'aggiunta di un'organizzazione, è possibile aggiungervi persone che poi possono essere gestite, eseguendo operazioni quali emissione di tessere in batch, importazione ed esportazione dati delle persone in batch, ecc. ***Nota:*** è possibile aggiungere fino a 10000 persone o tessere.

7.6.1 Aggiunta di persone

Aggiunta di persone (informazioni base)

Passaggi:

1. Selezionando un'organizzazione dall'elenco e facendo clic sul pulsante **Add** nel pannello Person, è possibile far apparire la finestra di dialogo di aggiunta di persone.

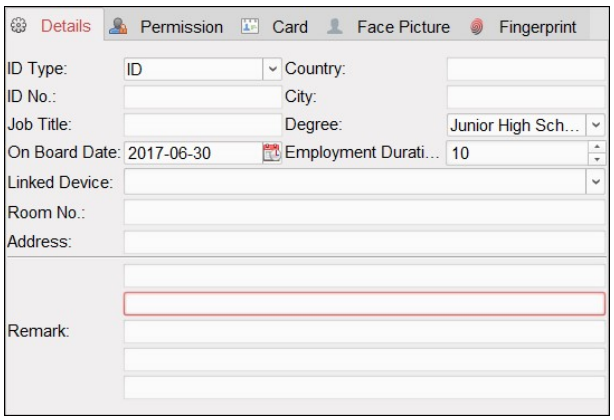


2. Il numero di ogni persona è generato automaticamente e non è modificabile.
3. Inserire le informazioni di base, tra cui nome della persona, sesso, numero di telefono, data di nascita e indirizzo e-mail.
4. Fare clic su **Upload Picture** per selezionare l'immagine della persona dal PC locale per caricarla sul client. ***Nota:*** l'immagine deve essere in formato *.jpg.
5. (Opzionale) È possibile anche fare clic su **Take Photo** per scattare la foto della persona con la fotocamera del PC.
6. Fare clic su **OK** per terminare l'aggiunta.

Aggiunta di persone (informazioni dettagliate)

Passaggi:

1. Fare clic sulla schermata da **Details** nell'interfaccia Add Person.



2. Inserire le informazioni dettagliate della persona, ad esempio il tipo e il numero del documento di identità, il paese, ecc., in base alle necessità.

   Linked Device: è possibile associare delle postazioni interne alle persone.

   Nota: selezionando **Analog Indoor Station** nella sezione Linked Device, viene visualizzato il campo **Door Station** in cui l'utente deve selezionare la postazione esterna che dovrà comunicare con la postazione interna analogica.

   Room No.: è possibile inserire il numero di stanza della persona.
3. Fare clic su **OK** per salvare le impostazioni.

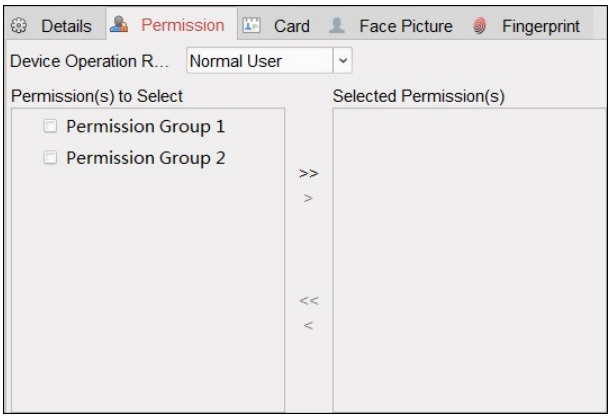
Aggiunta di persone (autorizzazioni)

Quando si aggiunge una persona, è possibile assegnarle delle autorizzazioni (come autorizzazioni operative per i dispositivi di controllo accessi e autorizzazioni per il controllo degli accessi).

Nota: per impostare l'autorizzazione per il controllo degli accessi, consultare il *Capitolo 7.8 Configurazione delle autorizzazioni*.

Passaggi:

1. Fare clic sulla schermata **Permission** nell'interfaccia Add Person.



2. Nel campo Device Operation Role, selezionare il ruolo dell'operatore per i dispositivi di controllo accessi. **Normal User:** la persona in questione è autorizzata a effettuare i check-in/out sul dispositivo, attraversare il punto di controllo accessi ecc.

   Administrator: la persona in questione ha tutte le autorizzazioni degli utenti normali, ma anche quelle di configurazione del dispositivo, compresa l'aggiunta di utenti normali, ecc.
3. Nell'elenco Permission(s) to Select sono indicate tutte le autorizzazioni configurate.

   Selezionare le caselle di controllo delle autorizzazioni e fare clic su **>** per aggiungerle all'elenco Selected Permission(s). (Opzionale) È possibile fare clic su **>>** per aggiungere all'elenco Selected Permission(s) tutte quelle visualizzate.

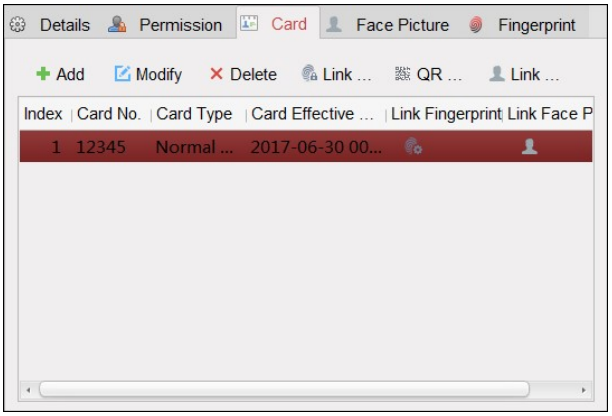
   (Opzionale) Nell'elenco Selected Permission(s), selezionare l'autorizzazione desiderata e fare clic su **<** per rimuoverla. È possibile anche fare clic su **<<** per rimuovere tutte le autorizzazioni selezionate.
4. Fare clic su **OK** per salvare le impostazioni.

Aggiunta di persone (tessere)

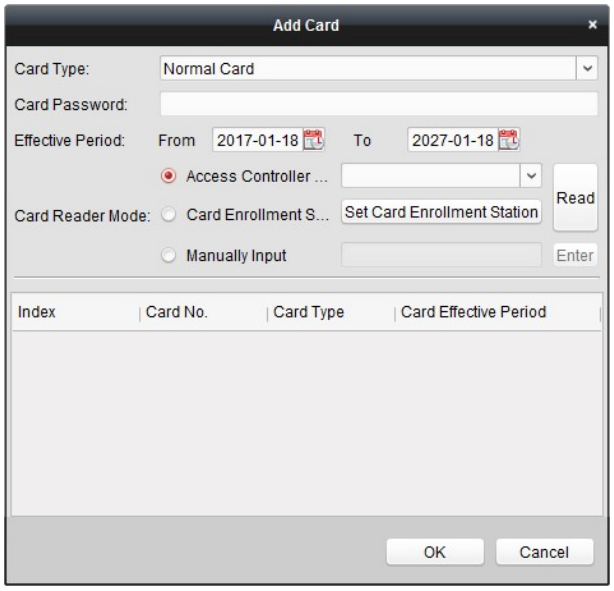
È possibile aggiungere delle tessere e assegnarle alle persone.

Passaggi:

1. Fare clic sulla schermata **Card** nell'interfaccia Add Person.



2. Fare clic su **Add** per visualizzare la finestra di dialogo Add Card.



3. Selezionare il tipo di tessera in base alle esigenze.

Normal Card

Card for Disabled Person: la porta resta aperta per il tempo definito per i titolari di tessere di questo tipo.

Card in Blacklist: l'azione del passaggio di tessere viene registrata e la porta non si apre.

Patrol Card: il passaggio delle tessere può essere usato per controllare lo stato lavorativo del personale addetto alle ispezioni. Le autorizzazioni di accesso del personale addetto alle ispezioni possono essere configurate.

Duress Card: il passaggio di tessere di coercizione permette di aprire le porte in caso di minacce. Allo stesso tempo, il client è in grado di segnalare l'evento di coercizione.

Super Card: questo tipo di tessera è valido su tutte le porte del sistema di controllo per periodi pianificabili in fase di configurazione.

Visitor Card: questo tipo di tessera è assegnata ai visitatori. Per le tessere dei visitatori, è possibile impostare **Max.**

Swipe Times.

Nota: il massimo numero di passaggi deve essere compreso tra 0 e 255. Impostando a 0 tale valore, la tessera è abilitata a un numero illimitato di passaggi.

4. Inserire la password della tessera nel campo Card Password. La password della tessera deve contenere da 4 a 8 cifre.

   Nota: la password sarà richiesta quando il titolare passerà la tessera per entrare o uscire dalla porta se si imposta la modalità di autenticazione del lettore di tessere su **Card and Password**, **Password and Fingerprint** e **Card, Password, and Fingerprint**. Per i dettagli, consultare il *Capitolo 7.9.2 Autenticazione del lettore di tessere.*

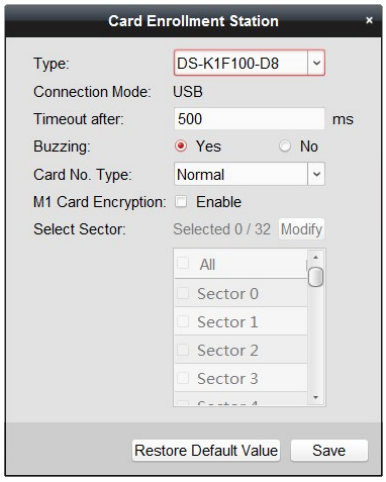
5. Fare clic su per definire l'orario di validità e la data di scadenza di una tessera.

6. Selezionare Card Reader Mode per leggere il numero di tessera.

   Access Controller Reader: per ottenere il numero della tessera, posizionare la tessera nel lettore del controller di accesso e fare clic su **Read**.

   Card Enrollment Station: per ottenere il numero della tessera, posizionare la tessera sulla postazione di registrazione di tessere e fare clic su **Read**.

   Nota: la postazione di registrazione di tessere deve essere collegata al PC su cui è in esecuzione il client. Facendo clic su **Set Card Enrollment Station**, è possibile accedere alla seguente finestra di dialogo.



   1) Selezionare il tipo di postazione di registrazione di tessere.

      Nota: attualmente, i tipi di lettori di tessere supportati comprendono i modelli DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E e DS-K1F180-D8E.

   2) Impostare il numero della porta seriale, la velocità in baud, il valore di timeout, l'avvisatore acustico o il tipo di numero della tessera.

   3) Fare clic sul pulsante **Save** per salvare le impostazioni.

      È possibile fare clic sul pulsante **Restore Default Value** per ripristinare le impostazioni predefinite.

      Manually Input: inserire il numero di tessera e fare clic su **Enter** per immettere il numero di tessera.

7. Facendo clic su **OK**, le tessere definite sono assegnate alle persone.

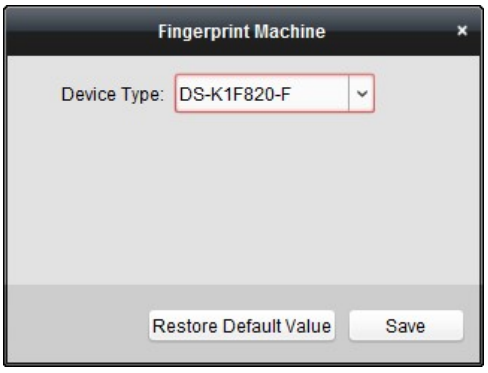
8. (Opzionale) È possibile selezionare una tessera aggiunta e fare clic su **Modify** o **Delete** per modificarla o eliminarla.
9. (Opzionale) È possibile generare e salvare il codice QR della tessera per l'autenticazione del codice QR.
   1) Selezionare una tessera aggiunta e fare clic su **QR Code** per generare il codice QR della tessera.
   2) Nella finestra a comparsa del codice QR, fare clic su **Download** per salvare il codice QR sul computer locale.
   È possibile stampare il codice QR per l'autenticazione sul dispositivo specificato.
   Nota: il dispositivo deve supportare la funzione di autenticazione del codice QR. Per i dettagli sull'impostazione della funzione di autenticazione del codice QR, consultare il manuale dell'utente del dispositivo.
10. (Opzionale) Facendo clic su **Link Fingerprint**, è possibile associare una tessera all'impronta digitale del titolare, in modo da abilitare la persona in questione ad attraversare la porta appoggiando il dito sullo scanner, senza passare la tessera sul lettore.
11. (Opzionale) È possibile fare clic su **Link Face Picture** per associare una tessera alla foto, in modo da abilitare la persona in questione ad attraversare la porta tramite scansione del volto tramite il dispositivo, senza passare la tessera sul lettore.
12. Fare clic su **OK** per salvare le impostazioni.

Aggiunta di persone (impronta digitale)

Passaggi:

1. Fare clic sulla schermata **Fingerprint** nell'interfaccia Add Person.

2. Selezionare **Local Collection** se necessario.
3. Prima di aggiungere l'impronta digitale, occorre collegare la macchina delle impronte digitali al PC e definirne i parametri.
   Fare clic su **Set Fingerprint Machine** per accedere alla seguente finestra di dialogo.



1) Selezionare DS-K1F820-F come tipo di dispositivo.
2) Fare clic sul pulsante **Save** per salvare le impostazioni.
   È possibile fare clic sul pulsante **Restore Default Value** per ripristinare le impostazioni predefinite.
   Note:
   Il numero di porta seriale deve corrispondere a quello del PC. È possibile controllare il numero della porta seriale in Device Manager sul PC.
   La velocità in baud impostata deve corrispondere a quella del lettore di tessere esterno con riconoscimento delle impronte digitali. Il valore predefinito è 19200.
   Il campo **Timeout after** permette di definire il tempo a disposizione per una corretta acquisizione dell'impronta digitale. Se l'utente non inserisce alcuna impronta digitale o ne inserisce una non valida, il dispositivo indicherà che il tempo di acquisizione dell'impronta digitale è scaduto.

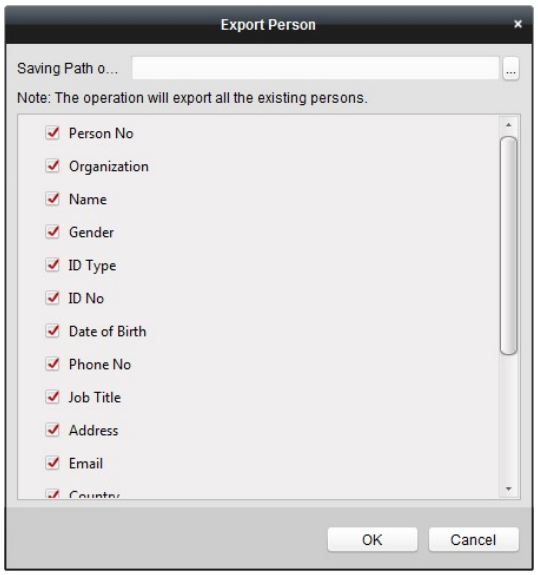
4. Fare clic sul pulsante **Start** per selezionare l'impronta digitale da acquisire.
5. Perché il client possa acquisire un'impronta, è necessario sollevare e appoggiare il dito in questione due volte sullo scanner di impronte digitali.
6. (Opzionale) È inoltre possibile fare clic su **Remote Collection** per acquisire l'impronta digitale dal dispositivo. ***Nota:*** questa funzione deve essere supportata dal dispositivo.
7. (Opzionale) Selezionando un'impronta registrata e facendo clic sul pulsante **Delete**, è possibile eliminarla.
   Facendo clic su **Clear**, è possibile cancellare tutte le impronte digitali.
8. Fare clic su **OK** per salvare le impronte digitali.

Importazione ed esportazione di informazioni delle persone

Le informazioni delle persone possono essere importate ed esportate in batch.

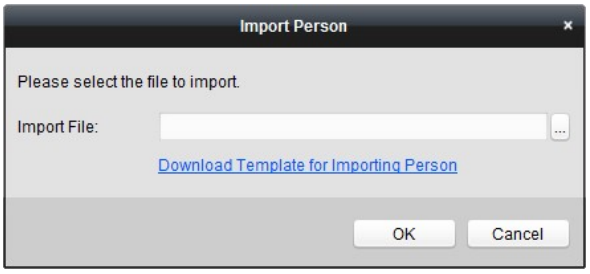
Passaggi:

1. **Esportazione di persone:** le informazioni delle persone aggiunte possono essere esportate in formato Excel sul PC locale.
   1) Dopo aver aggiunto la persona, è possibile fare clic sul pulsante **Export Person** nella schermata Person and Card e verrà visualizzata la seguente finestra di dialogo.
   2) Fare clic su ... per selezionare il percorso di salvataggio del file Excel esportato.
   3) Selezionare le caselle di controllo corrispondenti alle informazioni personali da esportare.



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

2. **Importazione di persone:** i file Excel con le informazioni delle persone possono essere importati in batch dal PC locale.
   1) Fare clic sul pulsante **Import Person** nella schermata Person and Card.



   2) Facendo clic su **Download Template for Importing Person**, è possibile scaricare prima di tutto il modello.
   3) Inserire le informazioni delle persone nel modello scaricato.
   4) Fare clic su ... per selezionare il file Excel con le informazioni delle persone. 5) Fare clic su **OK** per avviare l'importazione.

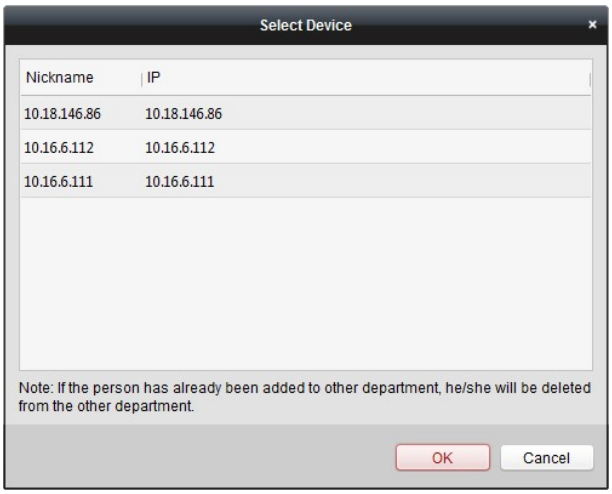
Recupero delle informazioni delle persone dal dispositivo di controllo accessi

Se il dispositivo di controllo accessi è stato configurato con le informazioni delle persone (quali dettagli personali, impronte digitali e informazioni delle tessere emesse), è possibile acquisire tali informazioni dal dispositivo e importarle nel client per ulteriori utilizzi.

Nota: tale funzione è supportata dai soli dispositivi che sono stati aggiunti con metodo di connessione TCP/IP.

Passaggi:

1. Fare clic e selezionare un'organizzazione dal relativo elenco sulla sinistra, per importarvi le persone.
2. Fare clic sul pulsante **Get Person** per visualizzare la seguente finestra di dialogo.



3. Il dispositivo di controllo accessi aggiunto viene visualizzato.
4. Per avviare l'acquisizione dei dati delle persone dal dispositivo, fare clic su di esso per selezionarlo e poi fare clic su **OK**.

   Per avviare l'acquisizione delle informazioni delle persone, è anche possibile fare doppio clic sul nome del dispositivo.

   Note:

   Le informazioni delle persone in questione, quali dettagli personali, impronte digitali (se configurate) e la tessera loro associata (se configurata), saranno importate nell'organizzazione selezionata.

   Se il nome della persona memorizzato nel dispositivo è vuoto, verrà compilato con il numero della tessera emessa dopo l'importazione nel client.

   Per impostazione predefinita, il sesso delle persone è **Male**. È possibile importare fino a 10000 persone.

7.6.2 Gestione di persone

Modifica ed eliminazione di persone

Per modificare le informazioni e le regole di presenza di una persona, fare clic su o nella colonna Operation oppure selezionare la persona e fare clic su **Modify** per aprire la finestra di dialogo di modifica delle persone.

È possibile fare clic su per visualizzare le registrazioni dei passaggi della tessera del titolare.

Selezionando una persona e facendo clic su **Delete**, è possibile eliminarla.

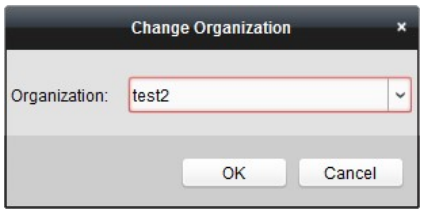
Nota: se esistono tessere rilasciate alla persona in questione, il collegamento non sarà più valido dopo l'eliminazione della persona.

Spostamento di persone in un'altra organizzazione

È possibile spostare le persone in un'altra organizzazione, se necessario.

Passaggi:

1. Selezionare una persona dall'elenco e fare clic sul pulsante **Change Organization**.



2. Selezionare l'organizzazione in cui spostare la persona.
3. Fare clic su **OK** per salvare le impostazioni.

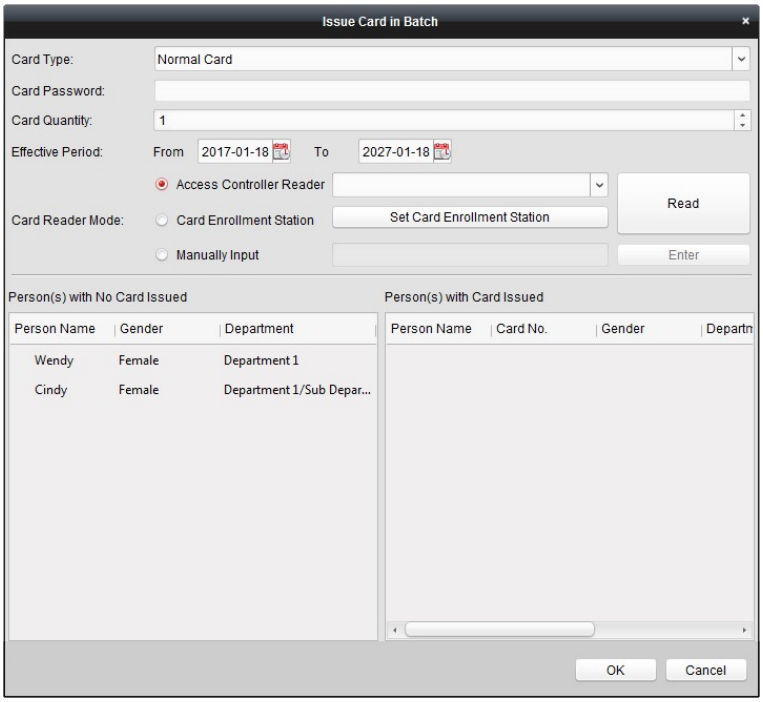
Ricerca di persone

È possibile inserire la parola chiave del numero di tessera o il nome della persona nel campo di ricerca e fare clic su **Search** per cercare la persona.
È possibile inserire il numero della stessera facendo clic su **Read** per ottenerne il numero tramite la postazione di registrazione di tessere collegata.
È possibile fare clic su **Set Card Enrollment Station** nell'elenco a discesa per impostare i parametri.

7.6.3 Emissione di tessere in batch

È possibile emettere più tessere in batch per persone alle quali non ne sono state ancora rilasciate.
Passaggi:

1. Facendo clic sul pulsante **Issue Card in Batch**, è possibile accedere alla seguente finestra di dialogo. Tutti coloro che non sono titolari di tesseere appariranno nell'elenco Person(s) with No Card Issued.

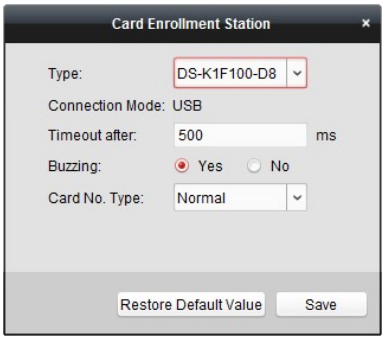


2. Selezionare il tipo di tessera in base alle esigenze.
   Nota: per i dettagli sul tipo di tessera, consultare la sezione *Aggiunta di persone.*

3. Inserire la password della tessera nel campo Card Password. La password della tessera deve contenere da 4 a 8 cifre.
   Nota: la password sarà richiesta quando il titolare passerà la tessera per entrare o uscire dalla porta se si abilita la modalità di autenticazione del lettore di tessere come **Card and Password**, **Password and Fingerprint** e **Card, Password, and Fingerprint**. Per i dettagli, consultare il *Capitolo 7.9.2 Autenticazione del lettore di tessere.*
4. Inserire la quantità di tessere emesse per ogni persona.
   Ad esempio, se Card Quantity è 3, sarà possibile leggere o inserire tre numeri di tessera per ogni persona.
5. Fare clic su per definire l'orario di validità e la data di scadenza di una tessera.
6. Dall'elenco Person(s) with No Card Issued a sinistra, selezionare la persona per cui emettere la tessera.
   Nota: è possibile fare clic sulle colonne Person Name, Gender e Department per ordinare le persone in base alle esigenze effettive.
7. Selezionare Card Reader Mode per leggere il numero di tessera.

   Access Controller Reader: per ottenere il numero della tessera, posizionare la tessera nel lettore del controller di accesso e fare clic su **Read**.

   Card Enrollment Station: per ottenere il numero della tessera, posizionare la tessera sulla postazione di registrazione di tessere e fare clic su **Read**.
   Nota: la postazione di registrazione di tessere deve essere collegata al PC su cui è in esecuzione il client. Facendo clic su **Set Card Enrollment Station**, è possibile accedere alla seguente finestra di dialogo.



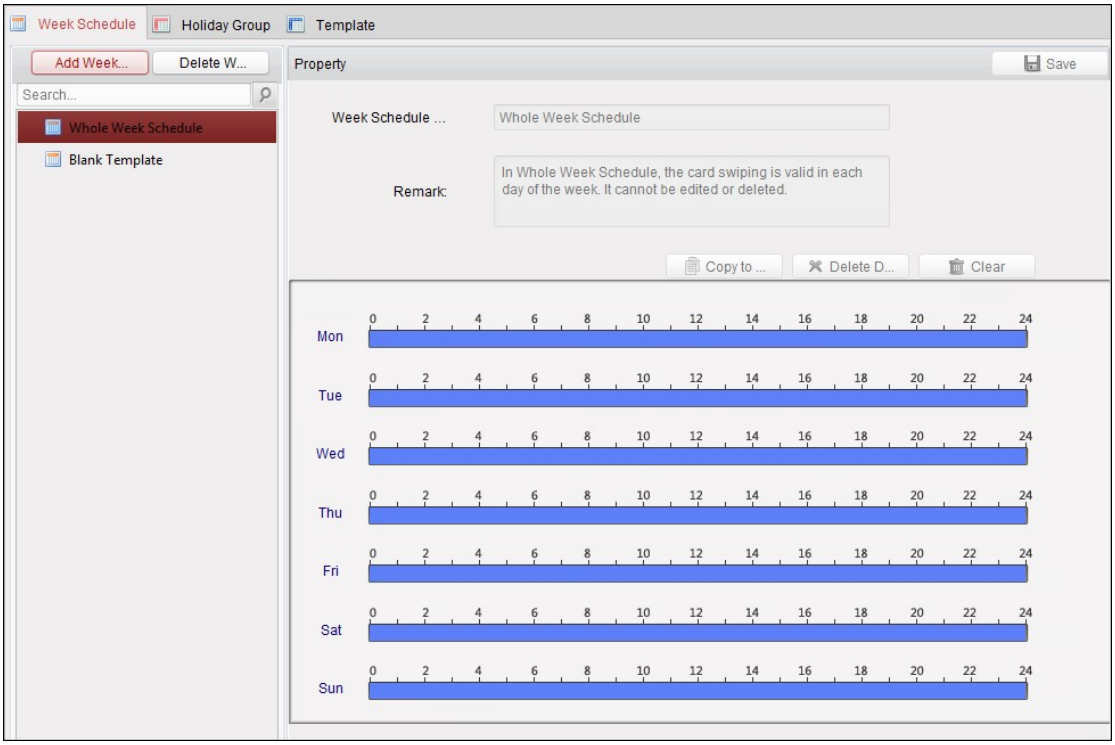
   1) Selezionare il tipo di postazione di registrazione di tessere.
      Nota: attualmente, i tipi di lettori di tessere supportati comprendono i modelli DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E e DS-K1F180-D8E.
   2) Impostare i parametri della postazione di registrazione tessere collegata.
   3) Fare clic sul pulsante **Save** per salvare le impostazioni.
      È possibile fare clic sul pulsante **Restore Default Value** per ripristinare le impostazioni predefinite.
      Manually Input: inserire il numero di tessera e fare clic su **Enter** per immettere il numero di tessera.
8. Dopo il rilascio di una tessera a una persona, le informazioni personali e della tessera in questione appariranno nell'elenco Person(s) with Card Issued.
9. Fare clic su **OK** per salvare le impostazioni.

7.7 Pianificazioni e modelli

Scopo:

È possibile configurare i modelli per le pianificazioni settimanali e quelle dei periodi di ferie. Dopo aver impostato i modelli, è possibile utilizzarli per configurare l'autorizzazione del controllo degli accessi, in modo che tale autorizzazione sia effettiva nei periodi di tempo indicati nel modello.

Fare clic su  per accedere all'interfaccia delle pianificazioni e dei modelli.



È possibile gestire la pianificazione delle autorizzazioni del controllo accessi, come Week Schedule, Holiday Schedule e Template. Per l'impostazione delle autorizzazioni, consultare il *Capitolo 7.8 Configurazione delle autorizzazioni*.

7.7.1 Pianificazione settimanale

Fare clic sulla schermata **Week Schedule** per accedere all'interfaccia Week Schedule Management.
Il client permette la definizione di due tipi di pianificazioni settimanali per impostazione predefinita: **Whole Week Schedule** e **Blank Schedule**, che non possono essere eliminati né modificati.

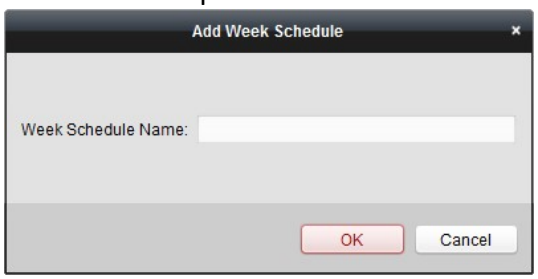
Whole Week Schedule: il passaggio delle tessere è valido in ogni giorno della settimana.

Blank Schedule: il passaggio delle tessere non è valido in nessun giorno della settimana.

Applicando la procedura seguente, è possibile definire pianificazioni personalizzate, in base alle esigenze.

Passaggi:

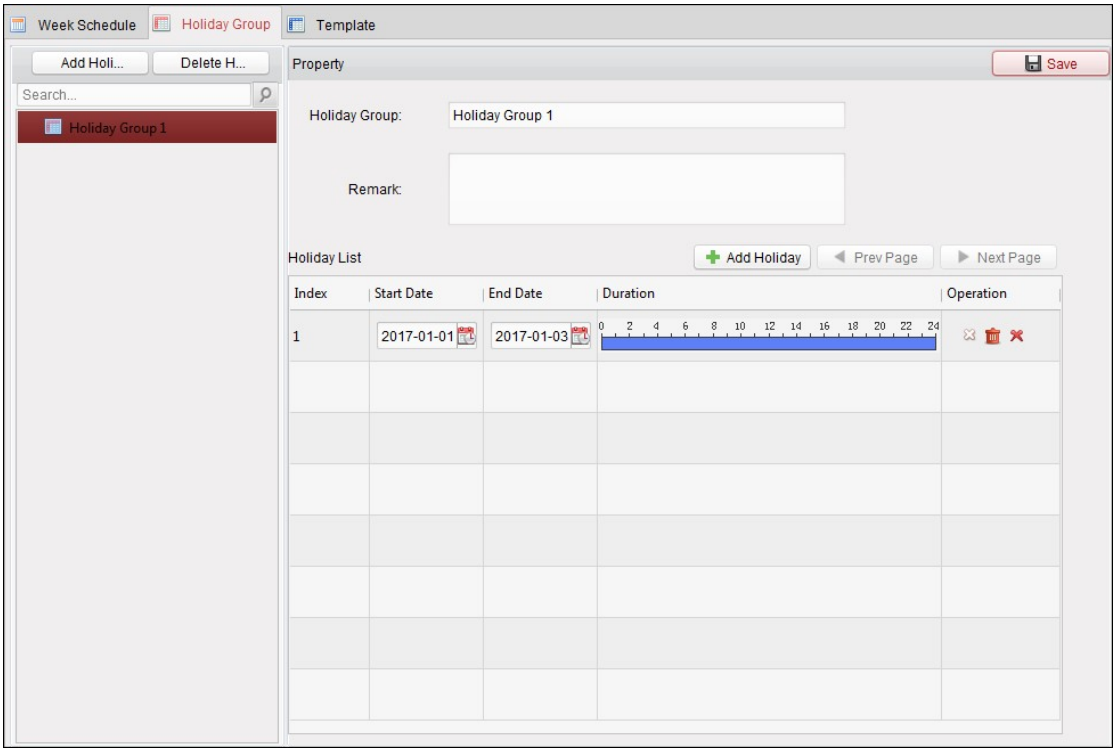
1. Fare clic sul pulsante **Add Week Schedule** per visualizzare l'interfaccia di aggiunta delle pianificazioni.



2. Inserire il nome della pianificazione settimanale e fare clic sul pulsante **OK** per aggiungerla.
3. Selezionare la pianificazione settimanale aggiunta dall'elenco per visualizzarne le proprietà sulla destra. È possibile modificare il nome della pianificazione settimanale e inserirvi dei commenti.
4. Nella pianificazione settimanale, fare clic e trascinare il mouse su un giorno della pianificazione per evidenziarne un periodo, che individua il periodo di attivazione dell'autorizzazione configurata.
   Nota: è possibile definire fino a 8 periodi di tempo per ciascun giorno della pianificazione.
5. Quando il cursore diventa  , è possibile spostare la barra temporale selezionata appena modificata. È anche possibile modificare il punto temporale visualizzato per definire accuratamente il periodo di tempo.
   Quando il cursore diventa  , è possibile allungare o accorciare la barra temporale selezionata.
6. Facoltativamente, è possibile selezionare la barra temporale della pianificazione e fare clic su **Delete Duration** per eliminare la barra temporale selezionata oppure fare clic su **Clear** per eliminare tutte le barre temporali oppure fare clic su **Copy to Week** per copiare le impostazioni della barra temporale nell'intera settimana.
7. Fare clic su **Save** per salvare le impostazioni.

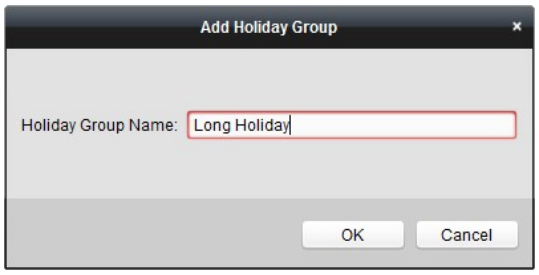
7.7.2 Gruppi di ferie

Fare clic sulla schermata **Holiday Group** per accedere all'interfaccia Holiday Group Management.



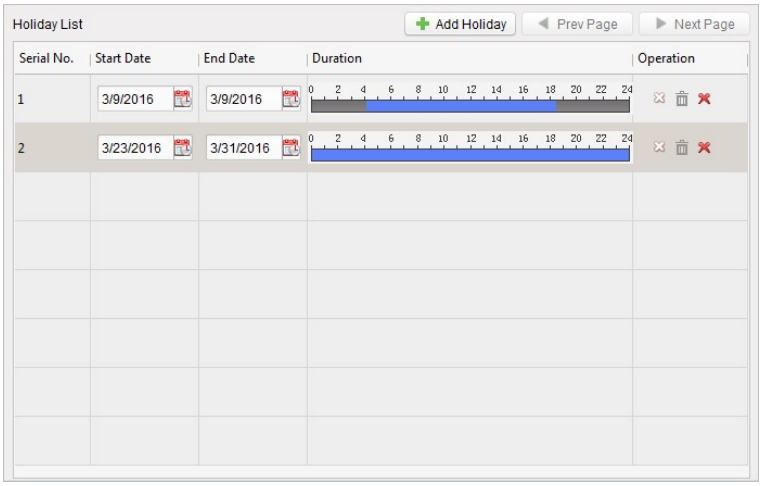
Passaggi:

1. Fare clic sul pulsante **Add Holiday Group** a sinistra per visualizzare l'interfaccia di aggiunta dei gruppi di ferie.



2. Inserire il nome del gruppo di ferie nel campo di testo e fare clic sul pulsante **OK** per aggiungerlo.
3. Selezionando il gruppo di ferie aggiunto, è possibile modificarne il nome e inserirvi dei commenti.
4. Fare clic sull'icona **Add Holiday** sulla destra per aggiungere un periodo di ferie al relativo elenco e configurarne la durata.

   Nota: ad ogni gruppo è possibile aggiungere fino a 16 periodi di ferie.



1) Nella pianificazione del periodo, fare clic e trascinare il mouse sul periodo, che individua il periodo di attivazione dell'autorizzazione configurata.
   Nota: è possibile definire fino a 8 durate per ciascun periodo della pianificazione.
2) Quando il cursore diventa , è possibile spostare la barra temporale selezionata appena modificata. È anche possibile modificare il punto temporale visualizzato per definire accuratamente il periodo di tempo.
3) Quando il cursore diventa , è possibile allungare o accorciare la barra temporale selezionata.
4) Opzionalmente, è possibile selezionare la barra temporale della pianificazione, quindi fare clic su per cancellarla oppure fare clic su per cancellare tutte le barre temporali delle ferie, altrimenti fare clic su per eliminare direttamente le ferie.

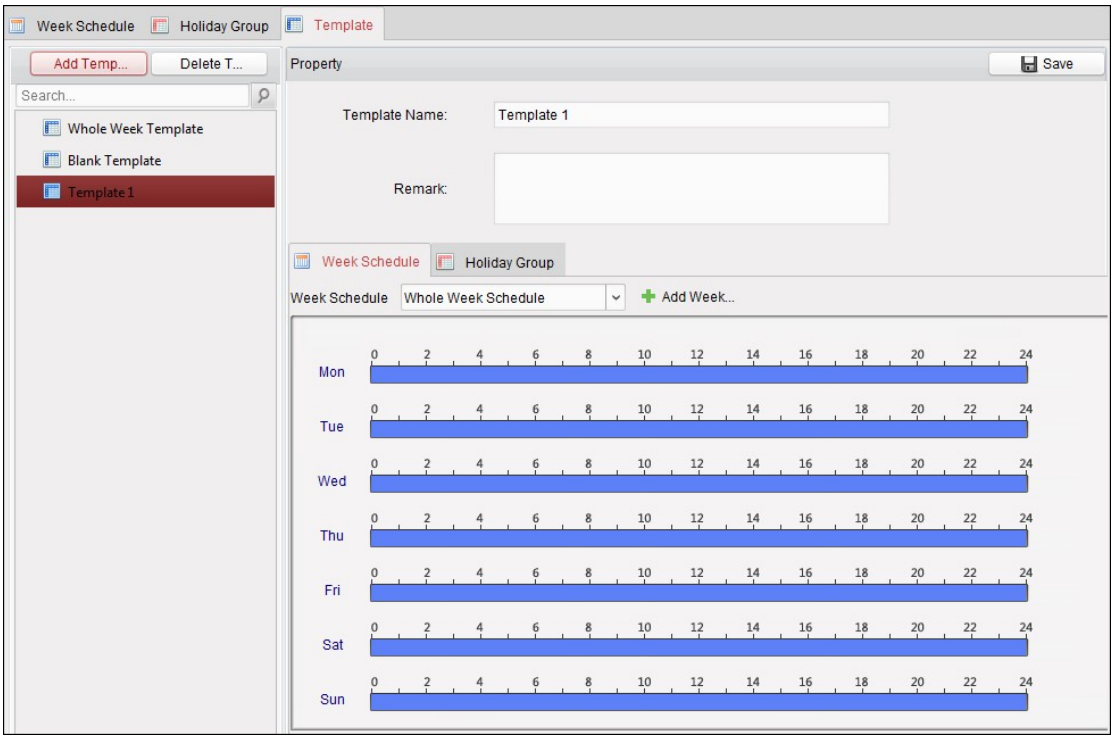
5. Fare clic su **Save** per salvare le impostazioni.
   Nota: i periodi di ferie non possono sovrapporsi.

7.7.3 Modelli

Dopo aver definito le pianificazioni settimanali e quelle dei gruppi di ferie, è possibile configurare i modelli che conterranno tali pianificazioni.

Nota: la priorità delle pianificazioni dei gruppi di ferie è più alta di quella delle pianificazioni settimanali.

Fare clic sulla schermata **Template** per accedere all'interfaccia Template Management.



Ci sono due modelli predefiniti: **Whole Week Template** e **Blank Template**, che non possono essere eliminati né modificati.

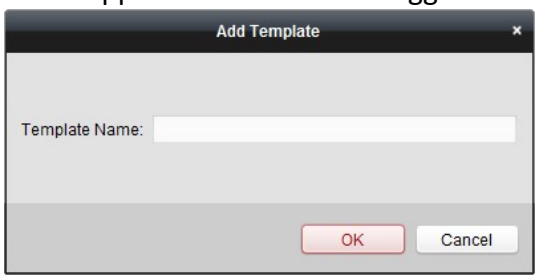
Whole Week Template: il passaggio delle tessere è valido ogni giorno della settimana e non ci sono pianificazioni di gruppi di ferie.

Blank Template: il passaggio delle tessere non è valido in alcun giorno della settimana e non ci sono pianificazioni di gruppi di ferie.

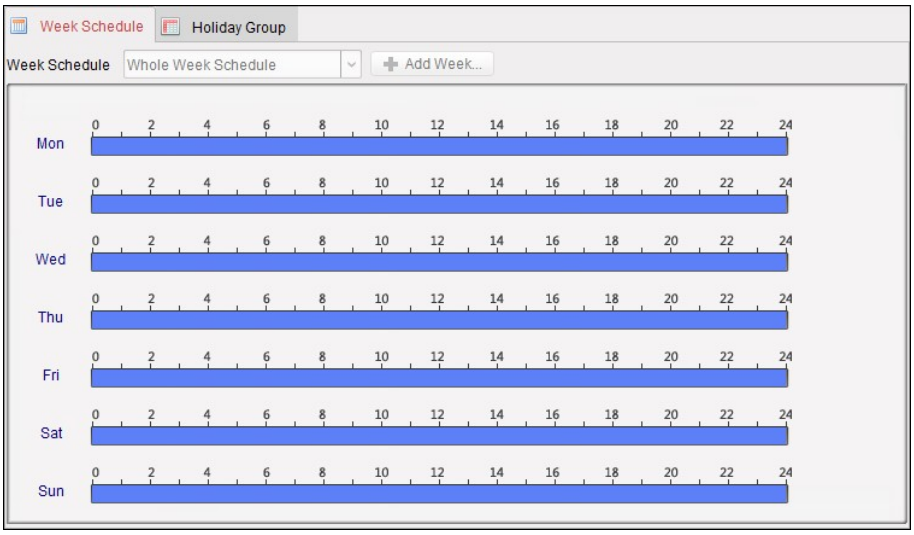
È possibile definire modelli personalizzati, in base alle esigenze.

Passaggi:

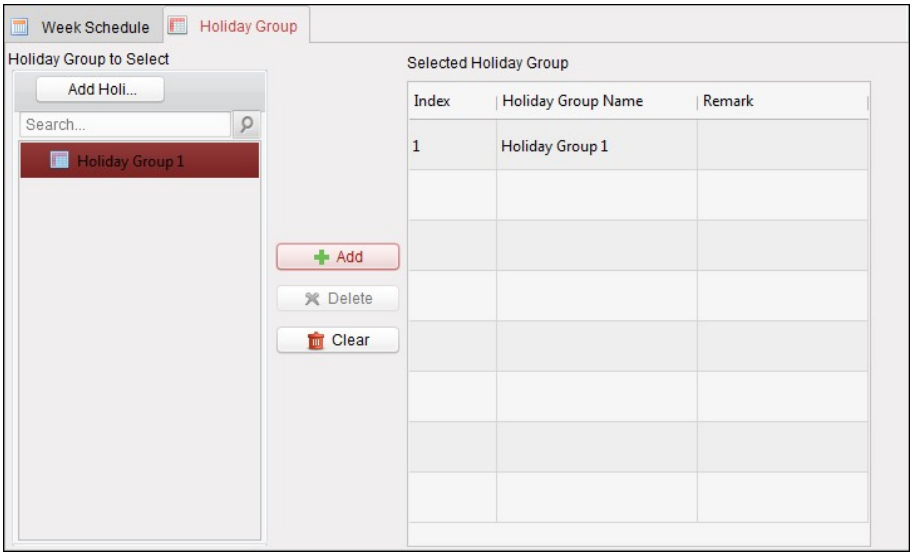
1. Fare clic su **Add Template** per far apparire l'interfaccia di aggiunta dei modelli.



2. Inserire il nome del modello nel campo di testo e fare clic sul pulsante **OK** per aggiungerlo.
3. Selezionare il modello aggiunto per modificarne le proprietà visualizzate sulla destra. È possibile modificare il nome del modello e inserirvi dei commenti.
4. Selezionare una pianificazione settimanale da applicare.
   Fare clic sulla schermata **Week Schedule** e selezionare una pianificazione dall'elenco a discesa.
   È anche possibile fare clic su **Add Week Schedule** per aggiungere una nuova pianificazione settimanale. Per i dettagli, fare riferimento al *Capitolo 7.7.1 Pianificazione settimanale*.



5. Selezionare i gruppi di ferie da applicare alla pianificazione. ***Nota:*** si possono aggiungere fino a 4 gruppi di ferie.



Fare clic su un gruppo di ferie per selezionarlo dall'elenco, poi fare clic su **Add** per aggiungerlo al modello. È anche possibile fare clic su **Add Holiday Group** per aggiungere un nuovo gruppo di ferie. Per i dettagli, consultare il *Capitolo 7.7.2 Gruppi di ferie*.

È possibile fare clic e selezionare un gruppo di ferie aggiunto dall'elenco sulla destra e poi fare clic su **Delete** per eliminarlo.

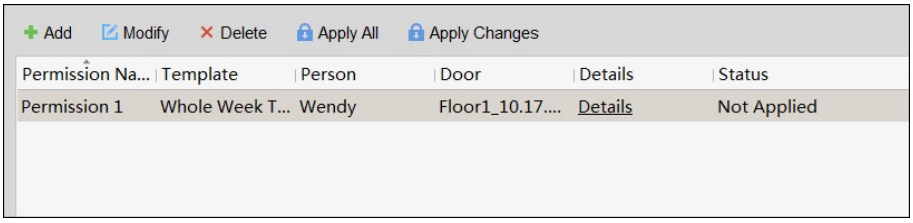
Facendo clic su **Clear**, è possibile eliminare tutti i gruppi di ferie aggiunti.

6. Fare clic sul pulsante **Save** per salvare le impostazioni.

7.8 Configurazione delle autorizzazioni

Nel modulo Permission Configuration è possibile aggiungere, modificare ed eliminare le autorizzazioni di controllo accessi e poi applicare le impostazioni ai dispositivi per renderle effettive.

Fare clic sull'icona per accedere all'interfaccia Access Control Permission.



7.8.1 Aggiunta delle autorizzazioni

Scopo:

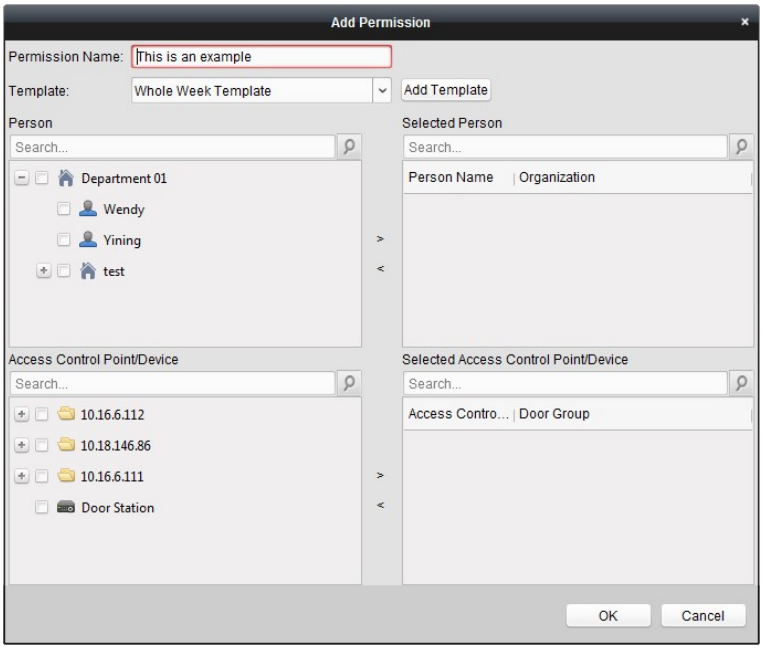
In questa sezione è possibile assegnare alle persone le autorizzazioni di ingresso/uscita per i punti di controllo accessi (porte).

Note:

È possibile aggiungere fino a 4 autorizzazioni a un punto di controllo accessi di un dispositivo.
Si possono aggiungere fino a 128 autorizzazioni in totale.

Passaggi:

1. Fare clic sull'icona **Add** per accedere alla seguente interfaccia.



2. Immettere il nome preferito per l'autorizzazione nel campo Permission Name.
3. Fare clic sul menu a discesa per selezionare un modello per le autorizzazioni.
   Nota: occorre configurare il modello prima di definire le impostazioni delle autorizzazioni. Facendo clic sul pulsante **Add Template**, è possibile aggiungere il modello. Per i dettagli, consultare il *Capitolo 7.7 Pianificazioni e modelli*.

4. Tutte le persone aggiunte sono visualizzate nell'elenco Person.
   Attivare una o più caselle di controllo per selezionare le persone corrispondenti e fare clic su **>** per aggiungerle all'elenco Selected Person.
   (Opzionale) È possibile selezionare una persona dall'elenco Selected Person e fare clic su **<** per rimuoverla.
5. L'elenco Access Control Point/Device mostra tutti i punti di controllo accessi (porte) e le postazioni esterne aggiunte al sistema.
   Attivare una o più caselle di controllo per selezionare le porte o le postazioni esterne corrispondenti e fare clic su **>** per aggiungerle all'elenco selezionato.
   (Opzionale) È possibile selezionare una porta o una postazione esterna dall'elenco selezionato e fare clic su **<** per rimuoverla.
6. Fare clic sul pulsante **OK** per completare l'aggiunta delle autorizzazioni. La persona selezionata avrà l'autorizzazione di ingresso/uscita dalle porte/postazioni esterne selezionate, tramite le relative tessere collegate o le impronte digitali.
7. (Opzionale) Dopo l'aggiunta di un'autorizzazione, è possibile fare clic su **Details** per modificarla. È anche possibile selezionare un'autorizzazione e fare clic su **Modify** per modificarla.
   È possibile selezionare un'autorizzazione aggiunta nell'elenco e fare clic su **Delete** per eliminarla.

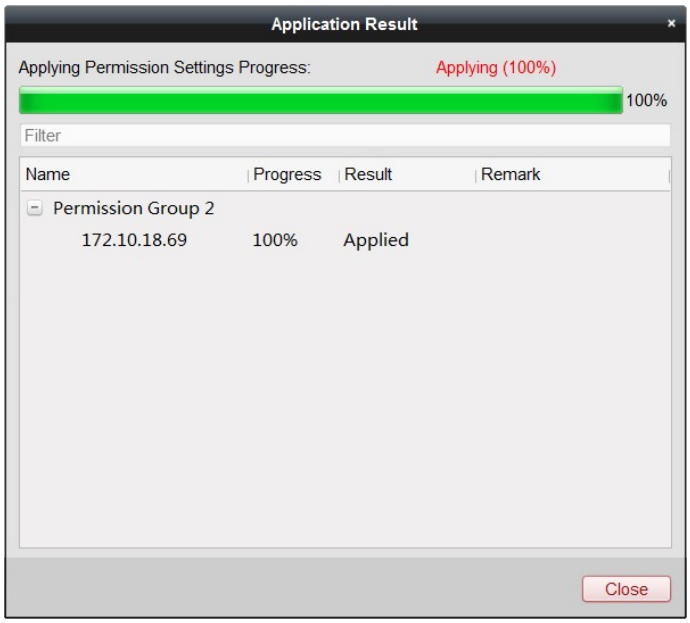
7.8.2 Applicazione delle autorizzazioni

Scopo:

Dopo la configurazione delle autorizzazioni, è necessario applicarle al dispositivo di controllo accessi per renderle effettive.

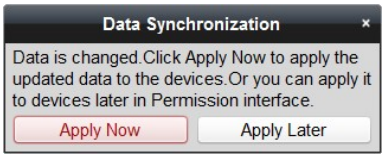
Passaggi:

1. Selezionare una o più autorizzazioni da applicare al dispositivo di controllo accessi.
   Per selezionare più autorizzazioni, è possibile tenere premuti i tasti *Ctrl* o *Shift* durante la selezione.
2. Fare clic su **Apply All** per iniziare ad applicare tutte le autorizzazioni selezionate al dispositivo di controllo accessi o alla postazione esterna.
   È possibile inoltre fare clic su **Apply Changes** per applicare la parte modificata delle autorizzazioni selezionate ai dispositivi.
3. Apparirà poi la seguente finestra, indicante il risultato dell'applicazione delle autorizzazioni.



Note:

Quando si modificano le impostazioni delle autorizzazioni, sarà visualizzata la seguente finestra di suggerimento.



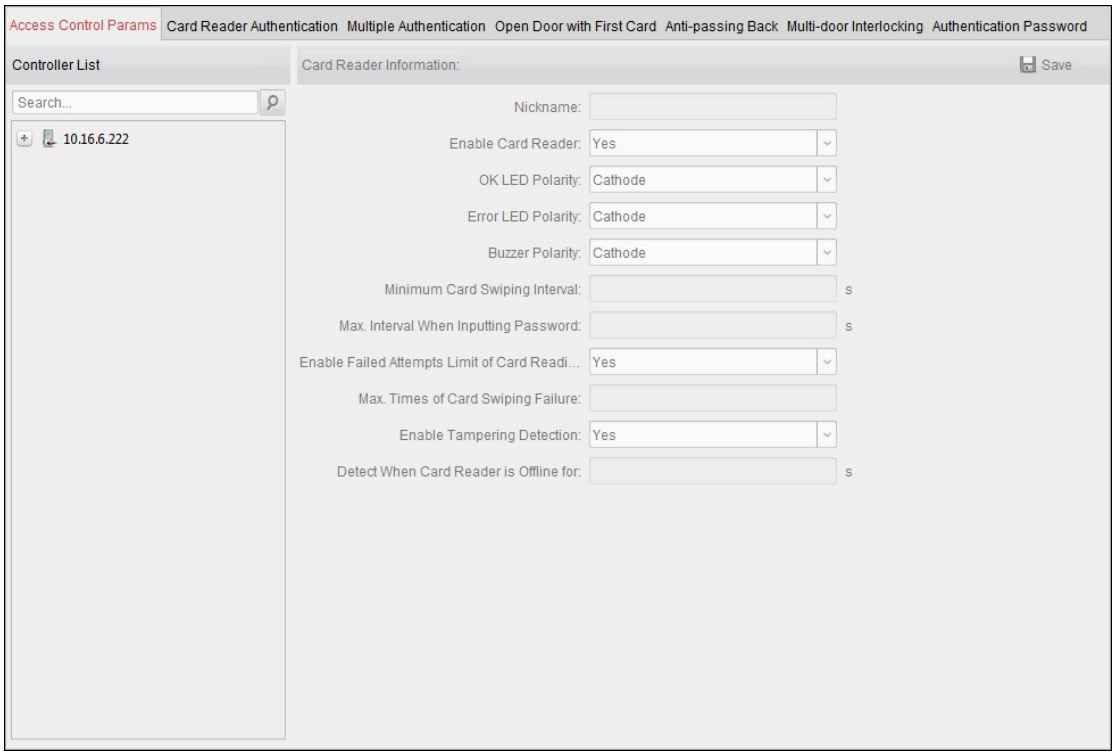
È possibile inoltre fare clic su **Apply Now** per applicare le autorizzazioni modificate al dispositivo.
In alternativa, è possibile fare clic su **Apply Later** per applicare le modifiche in un secondo momento nell'interfaccia Permission.
Le modifiche alle autorizzazioni includono modifiche della pianificazione e del modello, impostazioni delle autorizzazioni, impostazioni delle autorizzazioni personali e le relative impostazioni delle persone (tra cui numero di tessera, impronta digitale, immagine del volto, collegamento tra numero di tessera e impronta digitale, password della tessera, periodo di efficacia della tessera, ecc.).

7.9 Funzioni avanzate

Scopo:

Dopo aver definito persone, modelli e autorizzazioni di controllo accessi, è possibile configurare le funzioni avanzate dell'applicazione di controllo accessi, quali parametri di controllo accessi, password di autenticazione, apertura delle porte con la prima tessera, funzione anti-passback, ecc.
Nota: le funzioni avanzate devono essere supportate dal dispositivo.

Fare clic sull'icona per accedere alla seguente interfaccia.



7.9.1 Parametri di controllo accessi

Scopo:

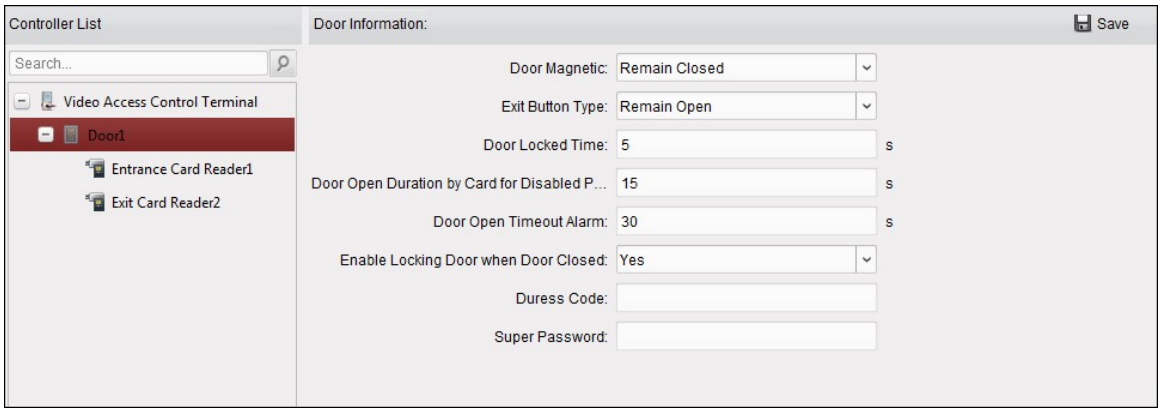
Dopo l'aggiunta del dispositivo di controllo accessi, è possibile configurare i parametri del relativo punto di controllo accessi (porta) e dei suoi lettori di tessere.

Fare clic sulla schermata **Access Control Parameters** per accedere all'interfaccia delle impostazioni dei parametri.

Parametri delle porte

Passaggi:

1. Espandere il dispositivo di controllo accessi nell'elenco dei controller, facendo clic su , quindi selezionare la porta (punto di controllo accessi) per modificarne le informazioni, visualizzate sulla destra.



2. È possibile modificare i parametri seguenti:

   Door Magnetic: l'opzione Door Magnetic è nello stato **Remain Closed** (eccetto situazioni speciali).

   Exit Button Type: l'opzione Exit Button Type è nello stato **Remain Open** (eccetto situazioni speciali).

   Door Locked Time: dopo il passaggio di una tessera normale e l'attivazione del relè, si avvia il timer di chiusura della porta.

   Door Open Duration by Card for Disabled Person: il componente magnetico della porta può essere abilitato con un opportuno ritardo, dopo il passaggio della tessera da parte di persone disabili.

   Door Open Timeout Alarm: l'allarme può attivarsi se la porta non è stata chiusa.

   nable Locking Door when Door Closed: è possibile bloccare la porta dopo la sua chiusura, anche se Door Locked Time non viene raggiunto.

   Duress Code: la porta può essere aperta immettendo la password anti-coercizione in caso di minacce. Allo stesso tempo, il client è in grado di segnalare l'evento di coercizione.

   Super Password: le persone autorizzate possono aprire la porta immettendo la password di livello superiore.

Note:

La password anti-coercizione e la password privilegiata devono essere diverse.

La password anti-coercizione e la password di livello superiore devono essere diverse dalla password di autenticazione.

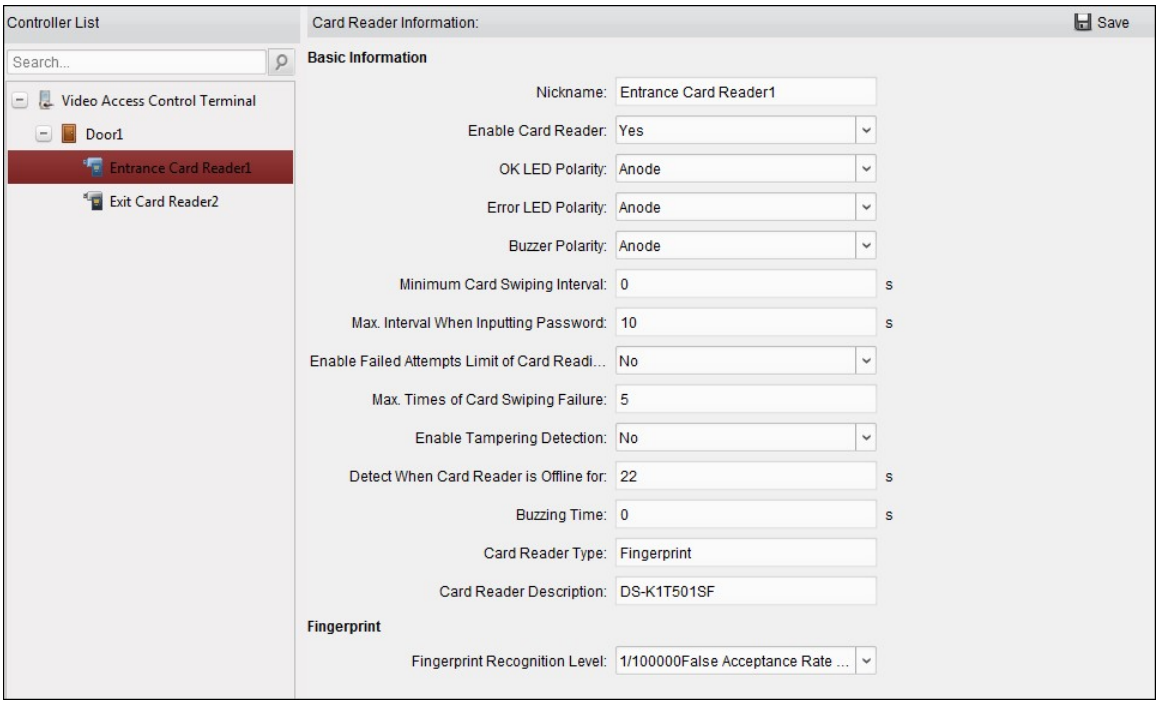
La password anti-coercizione e la password di livello superiore devono contenere da 4 a 8 numeri.

3. Fare clic sul pulsante **Save** per salvare i parametri.

Parametri del lettore di tessere

Passaggi:

1. Espandere la porta nell'elenco dei dispositivi sulla sinistra, facendo clic su , quindi selezionare il lettore di tessere per modificarne i parametri, visualizzati sulla destra.



2. È possibile modificare i parametri seguenti:

Nickname: inserire il nome preferito per il lettore di tessere.

Enable Card Reader: selezionare **Yes** per abilitare il lettore di tessere.

OK LED Polarity: selezionare OK LED Polarity nella tessera principale del lettore di tessere.

Error LED Polarity: selezionare Error LED Polarity nella tessera principale del lettore di tessere.

Buzzer Polarity: selezionare Buzzer LED Polarity nella tessera principale del lettore di tessere.

Minimum Card Swiping Interval: consente di definire l'intervallo di tempo minimo tra due passaggi della stessa tessera: al di sotto di tale valore il passaggio non è valido. È possibile impostare un valore da 0 a 255.

Max. Interval When Inputting Password: consente di definire l'intervallo di tempo massimo tra l'inserimento di due cifre durante l'immissione della password del lettore di tessere: al di sopra di tale valore le cifre inserite in precedenza vengono automaticamente cancellate.

Enable Failed Attempts Limit of Card Reading: consente di abilitare l'allarme di segnalazione dei casi in cui il numero di tentativi falliti di lettura di una tessera raggiunge il valore impostato.

Max. Times of Card Swiping Failure: consente di impostare il numero massimo di tentativi errati ammessi per la lettura di tessere.

Enable Tampering Detection: consente di abilitare il sistema di rilevamento antimanomissione del lettore di tessere.

Detect When Card Reader is Offline for: se il dispositivo di controllo accessi non è in grado di collegarsi al lettore di tessere per un tempo più lungo di quello definito, il lettore di tessere passa automaticamente offline.

Buzzing Time: impostare la durata dell'avvisatore acustico del lettore di tessere. La durata può variare da 0 a 5999 secondi. 0 indica l'avvisatore acustico continuo.

Card Reader Type: ottenere il tipo del lettore di tessere.

Card Reader Description: ottenere la descrizione del lettore di tessere.

Fingerprint Recognition Level: selezionare il livello di riconoscimento dell'impronta digitale nell'elenco a discesa. Per impostazione predefinita, il livello è Low.

3. Fare clic sul pulsante **Save** per salvare i parametri.

7.9.2 Autenticazione del lettore di tessere

Scopo:

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

Passaggi:

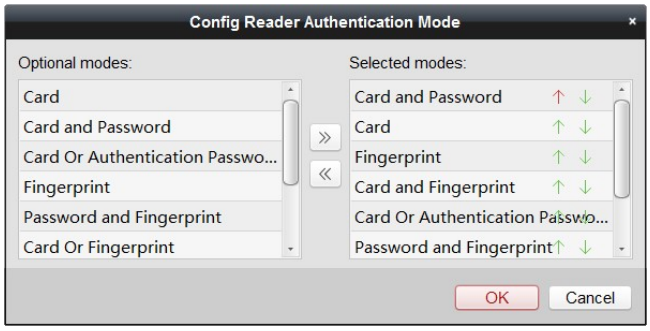
1. Fare clic sulla schermata **Card Reader Authentication** e selezionare un lettore di tessere sulla sinistra.
2. Fare clic sul pulsante **Configuration** per selezionare le modalità di autenticazione del lettore di tessere per impostare la pianificazione.

   Note:

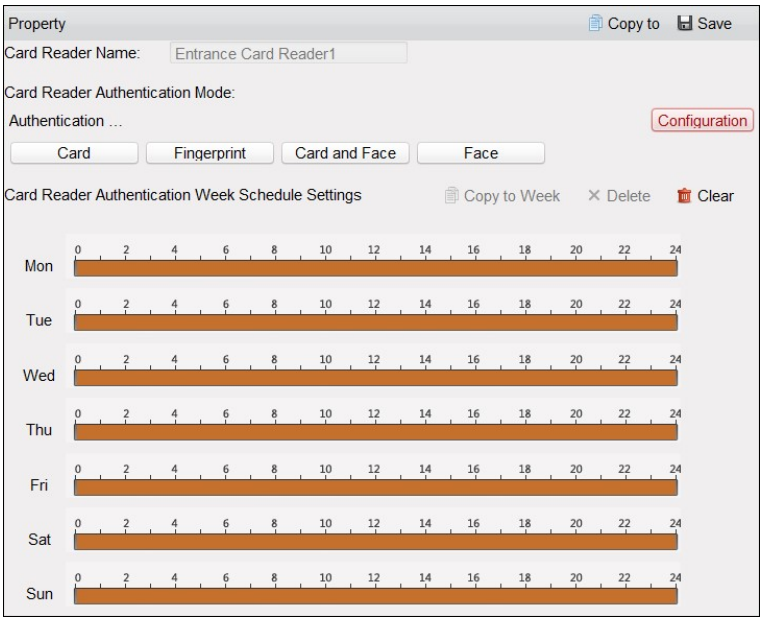
   Le modalità di autenticazione disponibili dipendono dal tipo di dispositivo.

   La password è quella della tessera, impostata durante l'emissione della stessa a una persona nel *Capitolo 7.6 Gestione delle persone.*

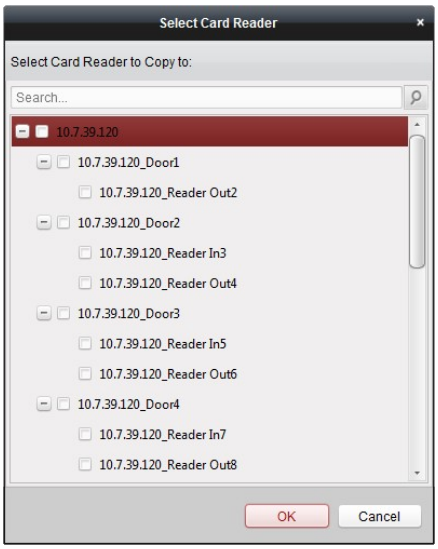
   1) Selezionare le modalità e fare clic su » per aggiungerle all'elenco delle modalità selezionate. È possibile fare clic su ↑ o su ↓ per definire l'ordine di visualizzazione.



   2) Fare clic su **OK** per confermare la selezione.
3. Una volta selezionate le modalità, queste saranno visualizzate come icone.
   Fare clic sull'icona per selezionare una modalità di autenticazione per il lettore di tessere.
4. Fare clic e trascinare il mouse su un giorno della pianificazione per tracciarvi una barra colorata, che individua il periodo di validità dell'autenticazione del lettore di tessere.



5. Ripetere la precedente operazione per definire altri periodi.
   È possibile anche selezionare un giorno configurato e fare clic sul pulsante **Copy to Week** per applicare le stesse impostazioni all'intera settimana.
   (Opzionale) È possibile fare clic sul pulsante **Delete** per eliminare il periodo di tempo selezionato, oppure fare clic sul pulsante **Clear** per eliminare tutti i periodi di tempo configurati.
6. (Opzionale) È possibile fare clic sul pulsante **Copy to** per copiare tali impostazioni ad altri lettori di tessere.



7. Fare clic sul pulsante **Save** per salvare i parametri.

7.9.3 Autenticazione multipla

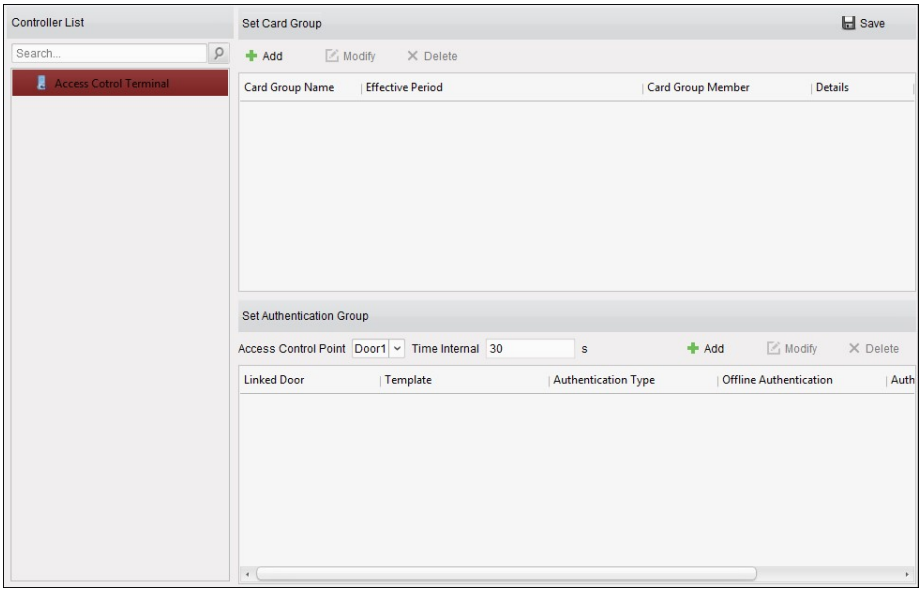
Scopo:

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

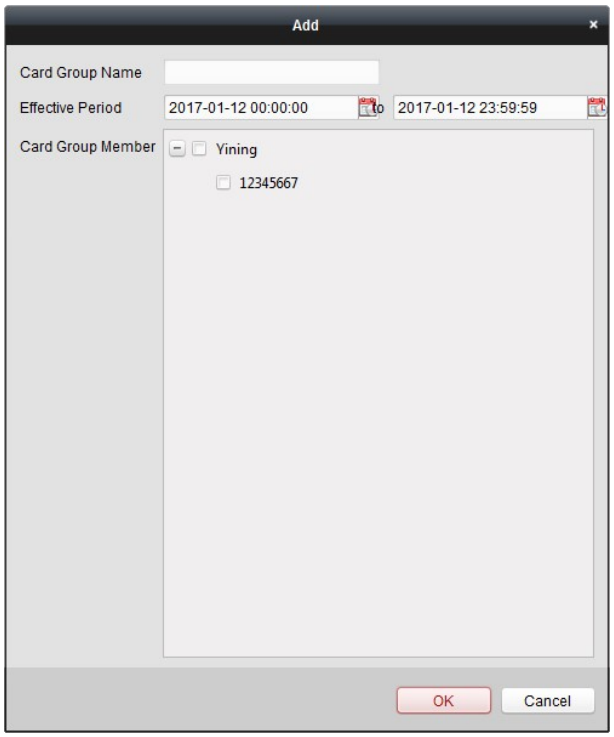
Nota: impostare prima di tutto l'autorizzazione per la tessera e applicare l'impostazione di autorizzazione al dispositivo di controllo accessi. Per i dettagli, consultare il *Capitolo 7.8 Configurazione delle autorizzazioni*.

Passaggi:

1. Fare clic sulla schermata **Multiple Authentication** per accedere alla seguente interfaccia.



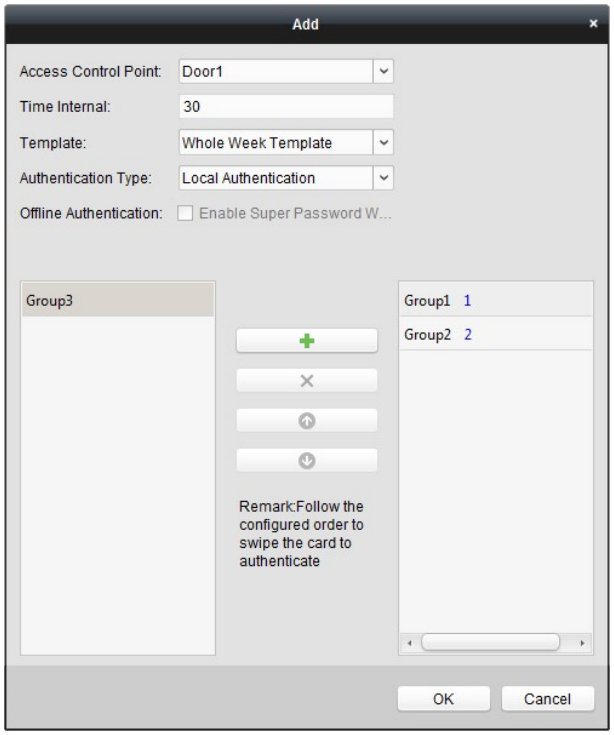
2. Selezionare un dispositivo di controllo accessi dall'elenco a sinistra.
3. Nel pannello Set Card Group a destra, fare clic sul pulsante **Add** per visualizzare la seguente finestra di dialogo:



1) Immettere il nome preferito per il gruppo nel campo Card Group Name.
2) Fare clic su per impostare l'orario di validità e la data di scadenza del gruppo di tessere.

3) Selezionare le caselle di controllo per selezionare le tessere da aggiungere al gruppo di tessere.
4) Fare clic su **OK** per salvare il gruppo di tessere.

4. Nel pannello Set Authentication Group, selezionare il punto di controllo accessi (porta) del dispositivo per eseguire autenticazioni multiple.
5. Immettere l'intervallo di tempo per il passaggio delle tessere.
6. Fare clic su **Add** per visualizzare la seguente finestra di dialogo.



1) Selezionare il modello del gruppo di autenticazione dall'elenco a discesa. Per i dettagli sull'impostazione del modello, consultare il *Capitolo 7.7 Pianificazioni e modelli*.
2) Selezionare il tipo di autenticazione del gruppo di autenticazione dall'elenco a discesa.

   Local Authentication: autenticazione tramite dispositivo di controllo accessi.

   Local Authentication and Remotely Open Door: autenticazione tramite dispositivo di controllo accessi e tramite client.

   Per i tipi Local Authentication e Remotely Open Door, è possibile selezionare la casella di controllo per abilitare l'autenticazione tramite password di livello superiore quando il dispositivo di controllo accessi è scollegato dal client.

   Local Authentication and Super Password: autenticazione tramite dispositivo di controllo accessi e password di livello superiore.
3) Il gruppo di tessere aggiunto appare nell'elenco sulla sinistra. Facendo clic sul gruppo di tessere e poi su +, è possibile aggiungerlo al gruppo di autenticazione.
   Facendo clic sul gruppo di tessere aggiunte e poi su ×, è possibile rimuoverlo dal gruppo di autenticazione.
   Facendo clic su ↑ o su ↓, è anche possibile impostare l'ordine di passaggio delle tessere.

4) Inserire un valore nel campo **Card Swiping Times** per il gruppo di tessere selezionato.

Note:

Il numero di passaggi delle tessere deve essere maggiore di 0 e minore della quantità di tessere aggiunte al gruppo in questione.

Il limite massimo di passaggio tessere è 16.

5) Fare clic su **OK** per salvare le impostazioni.

7. Fare clic su **Save** per salvare e applicare le nuove impostazioni.

Note:

È possibile aggiungere fino a 20 gruppi di autenticazione per ciascun punto di controllo accessi (porta).

Al gruppo di autenticazione per il quale il tipo di certificato è **Local Authentication**, è possibile aggiungere fino a 8 gruppi di tessere.

È possibile aggiungere fino a 7 gruppi di tessere al gruppo di autenticazione il cui tipo di certificato è **Local Authentication and Super Password** o **Local Authentication and Remotely Open Door**.

7.9.4 Apertura delle porte con la prima tessera

Scopo:

È possibile impostare più prime tessere per un punto di controllo accessi. Una volta passata la prima tessera, consente a più persone di accedere alla porta o di effettuare altre azioni di autenticazione. La modalità prima tessera contiene Remain Open with First Card e Disable Remain Open with First Card.

Remain Open with First Card: la porta resta aperta per il tempo stabilito dopo il passaggio della prima tessera, fino allo scadere della durata di apertura impostata.

Disable Remain Open with First Card: consente di disattivare la funzione.

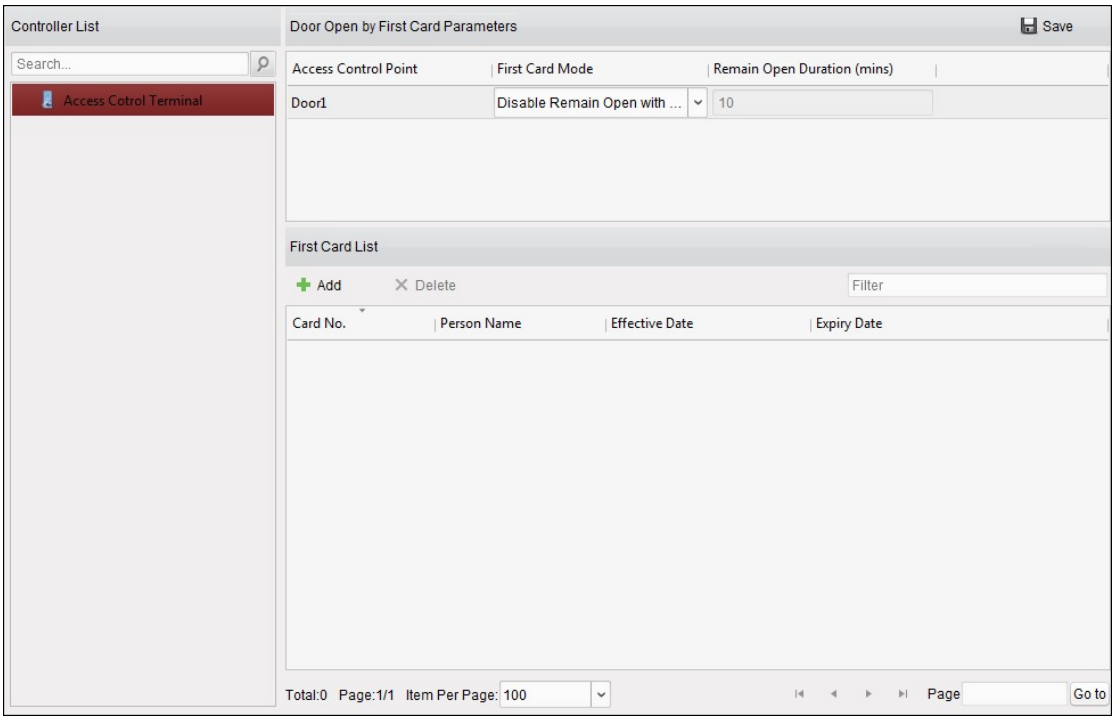
Note:

L'opzione First Card Authorization è efficace solo dal giorno corrente. L'autorizzazione scadrà dopo la mezzanotte del giorno corrente.

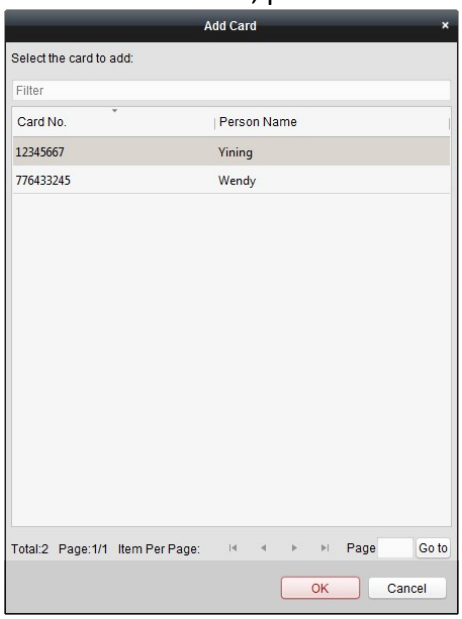
Per disattivare la modalità della prima tessera, passare nuovamente la prima tessera.

Passaggi:

1. Fare clic su **Open Door with First Card** per accedere alla seguente interfaccia.



2. Selezionare un dispositivo di controllo accessi dall'elenco a sinistra.
3. Selezionare la modalità prima tessera dall'elenco a discesa per il punto di controllo accessi.
4. (Opzionale) Se si seleziona Remain Open with First Card, occorre impostare per quanto tempo la porta resta aperta. ***Note:***
   La durata di apertura della porta deve essere compresa tra 0 e 1440 minuti. Per impostazione predefinita è 10 minuti.
   Per disattivare la modalità della prima tessera, passare nuovamente la prima tessera.
5. Fare clic sul pulsante **Add** nell'elenco First Card, per visualizzare la seguente finestra di dialogo.



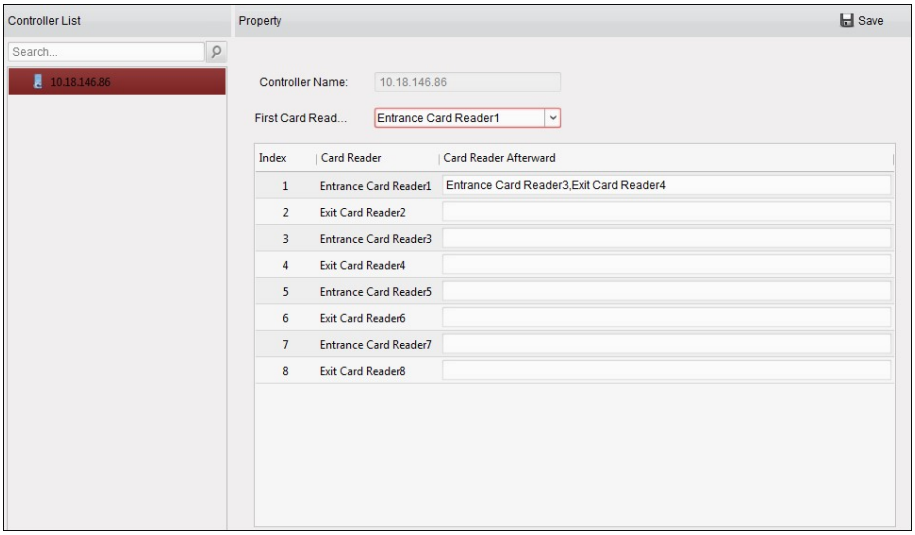
1) Selezionare le tessere da aggiungere come prima tessera per la porta.
Nota: impostare prima di tutto l'autorizzazione per la tessera e applicare l'impostazione di autorizzazione al dispositivo di controllo accessi. Per i dettagli, consultare il *Capitolo 7.8 Configurazione delle autorizzazioni*. 2) Fare clic sul pulsante **OK** per salvare la tessera aggiunta.

6. Facendo clic sul pulsante **Delete** è possibile rimuovere una tessera dall'elenco delle prime tessere.
7. Fare clic su **Save** per salvare e applicare le nuove impostazioni.

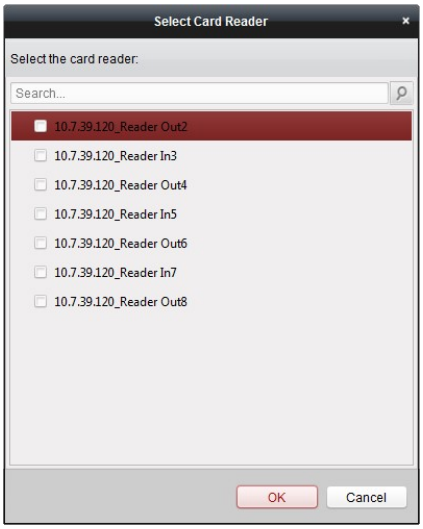
7.9.5 Anti-passback

Scopo:
Per un dato punto di controllo accessi, è possibile definire l'unico percorso consentito e l'unica persona cui è consentito il transito dopo il passaggio della tessera.
Note:
Su un dispositivo di controllo accessi, è possibile configurare la funzione anti-passback o quella di interblocco multiporta.
Abilitare prima di tutto la funzione anti-passback del dispositivo di controllo accessi in questione.
Passaggi:

1. Fare clic sulla schermata **Anti-passing Back** per accedere alla seguente interfaccia.



2. Selezionare un dispositivo di controllo accessi dall'elenco dei dispositivi a sinistra.
3. Nel campo First Card Reader, selezionare il lettore di tessere che funge come inizio del percorso.
4. Nell'elenco, fare clic sul campo di testo **Card Reader Afterward** e selezionare i lettori di tessere collegati. ***Esempio:*** supponiamo la selezione di Reader In_01 come inizio, Reader In_02 e Reader Out_04 come lettori di tessere collegati. In tal modo sarà possibile attraversare il punto di controllo accessi solo passando la tessera nell'ordine specificato: Reader In_01, Reader In_02 e Reader Out_04.



Nota: per ogni lettore di tessere è possibile aggiungerne fino a quattro successivi.

5. (Opzionale) È possibile accedere nuovamente alla finestra di dialogo Select Card Reader per modificare i lettori di tessere successivi.
6. Fare clic su **Save** per salvare e applicare le nuove impostazioni.

7.10 Ricerca di eventi di controllo accessi

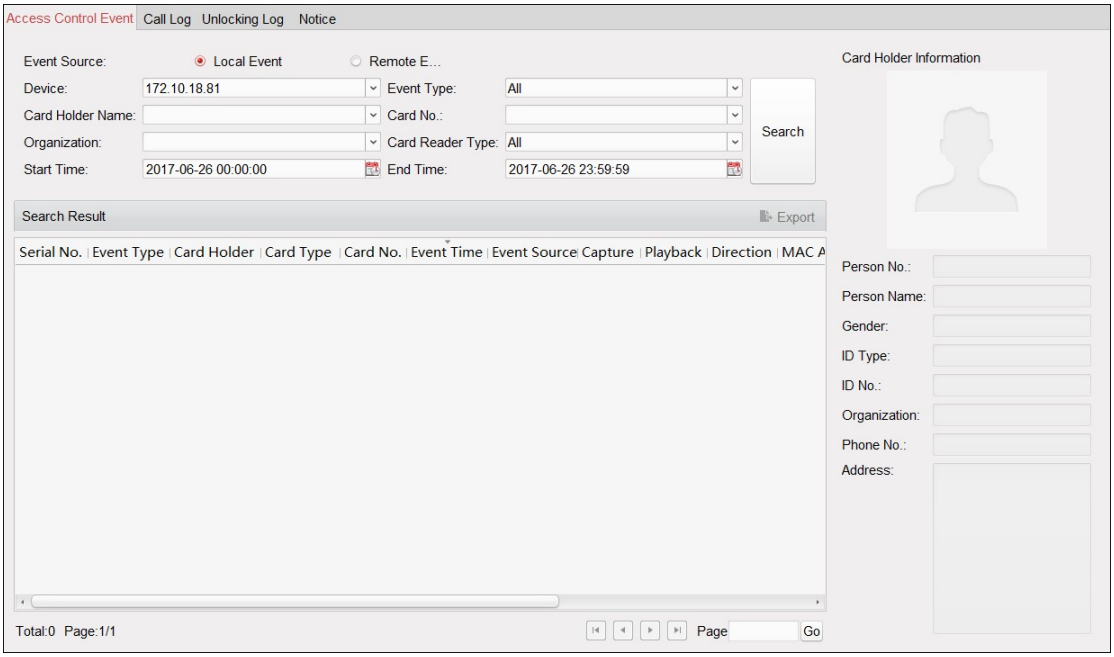
Scopo:

Tramite il client è possibile cercare gli eventi della cronologia di controllo accessi tra cui evento remoto ed evento locale.

Local Event: cercare l'evento di controllo accessi dal database del client di controllo.

Remote Event: cercare l'evento di controllo accessi dal dispositivo.

Fare clic sull'icona e poi sulla schermata Access Control Event per accedere alla seguente interfaccia.



7.10.1 Ricerca di eventi locali di controllo accessi

Passaggi:

1. Impostare Event Source su **Local Event**.
2. Inserire le condizioni di ricerca in base alle esigenze.
3. Fare clic su **Search**. I risultati saranno elencati di seguito.
4. Per un evento di controllo accessi attivato dal titolare di una tessera, è possibile fare clic sull'evento per visualizzare i dettagli del titolare, quali il numero, il nome, l'organizzazione, il numero di telefono, l'indirizzo di contatto e la foto della persona.
5. (Opzionale) Se l'evento presenta immagini collegate, è possibile fare clic sulla colonna **Capture** per visualizzare l'immagine acquisita dalla telecamera che si attiva allo scattare dell'allarme.
6. (Opzionale) Se l'evento presenta video collegati, è possibile fare clic sulla colonna **Playback** per visualizzare il file video registrato dalla telecamera che si attiva allo scattare dell'allarme.

   Nota: per impostare la telecamera che si attiva, consultare il *Capitolo 7.11.1 Collegamento di eventi di controllo accessi*.
7. Facendo clic su **Export**, è possibile esportare i risultati di ricerca in un file *.csv sul PC locale.

7.10.2 Ricerca di eventi remoti di controllo accessi

Passaggi:

1. Impostare Event Source su **Remote Event**.
2. Inserire le condizioni di ricerca in base alle esigenze.
3. (Opzionale) È possibile selezionare la casella di controllo **With Alarm Picture** per cercare gli eventi con le immagini di allarme.
4. Fare clic su **Search**. I risultati saranno elencati di seguito.
5. Facendo clic su **Export**, è possibile esportare i risultati di ricerca in un file *.csv sul PC locale.

7.11 Configurazione degli eventi di controllo accessi

Scopo:

Per i dispositivi di controllo accessi aggiunti, è possibile configurare i relativi collegamenti, quali collegamenti di eventi e ingressi allarme di controllo accessi, collegamenti di eventi delle tessere e collegamenti tra dispositivi.

Fare clic sull'icona  del pannello di controllo o fare clic su **Tool->Event Management** per aprire la pagina Event Management.

7.11.1 Collegamento di eventi di controllo accessi

Scopo:

È possibile assegnare azioni di collegamento all'evento di controllo accessi, definendo una regola. Ad esempio, quando viene rilevato un evento di controllo accessi, viene emesso un avviso acustico oppure vengono eseguite altre azioni di collegamento.

Nota: il collegamento in questo caso fa riferimento al collegamento relativo alle azioni del software client.

Passaggi:

1. Fare clic sulla schermata **Access Control Event**.
2. I dispositivi di controllo accessi aggiunti saranno visualizzati nel pannello Access Control Device a sinistra. Selezionare un dispositivo di controllo accessi, un ingresso allarme, un punto di controllo accessi (porta) o un lettore di tessere per configurare il collegamento all'evento.
3. Selezionare il tipo di evento per impostare il collegamento.
4. Selezionare la telecamera attivata. Quando si verifica l'evento selezionato, l'immagine o il video della telecamera attivata saranno visualizzati.
   Per acquisire l'immagine della telecamera attivata dall'occorrenza dell'evento selezionato, è possibile anche impostare la pianificazione e l'archiviazione delle acquisizioni nella sezione Storage Schedule.
5. Selezionare le caselle di controllo per attivare le azioni di collegamento richieste. Per i dettagli, consultare la *Tabella 14.1 Azioni di collegamento per gli eventi di controllo accessi*.
6. Fare clic su **Save** per salvare le impostazioni.
7. Facendo clic sul pulsante Copy to, è possibile copiare l'evento di controllo accessi in altri dispositivi di controllo accessi, ingressi di allarme, punti di controllo accessi o lettori di tessere.
   Selezionare i parametri da copiare e la destinazione in cui copiarli, poi fare clic su **OK** per confermare.

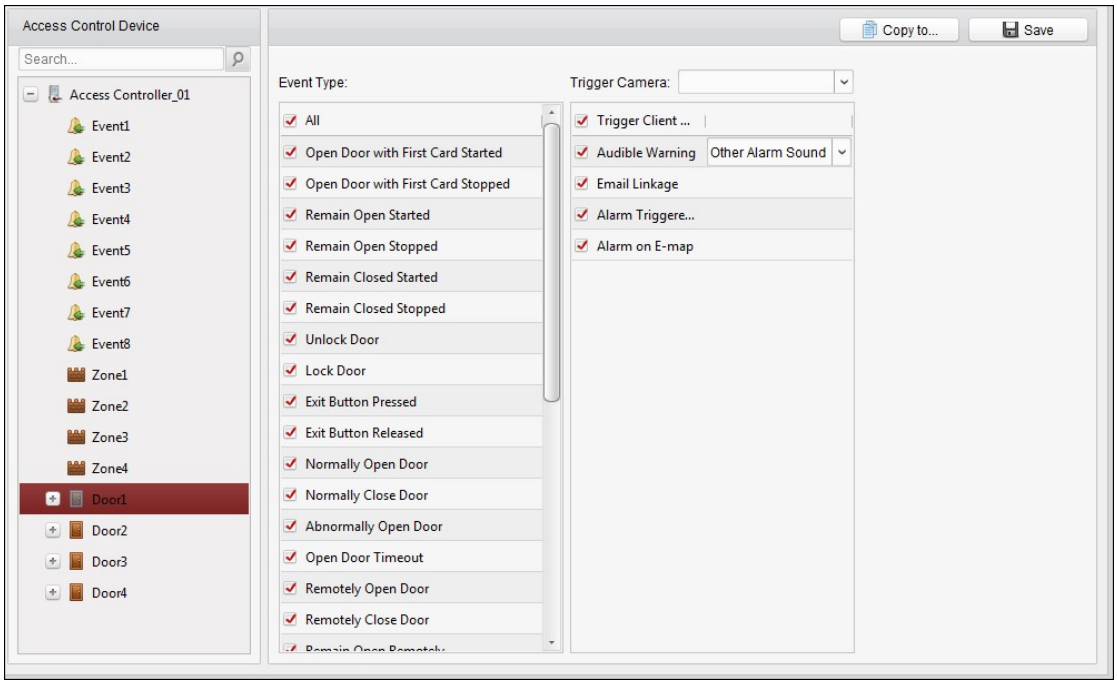
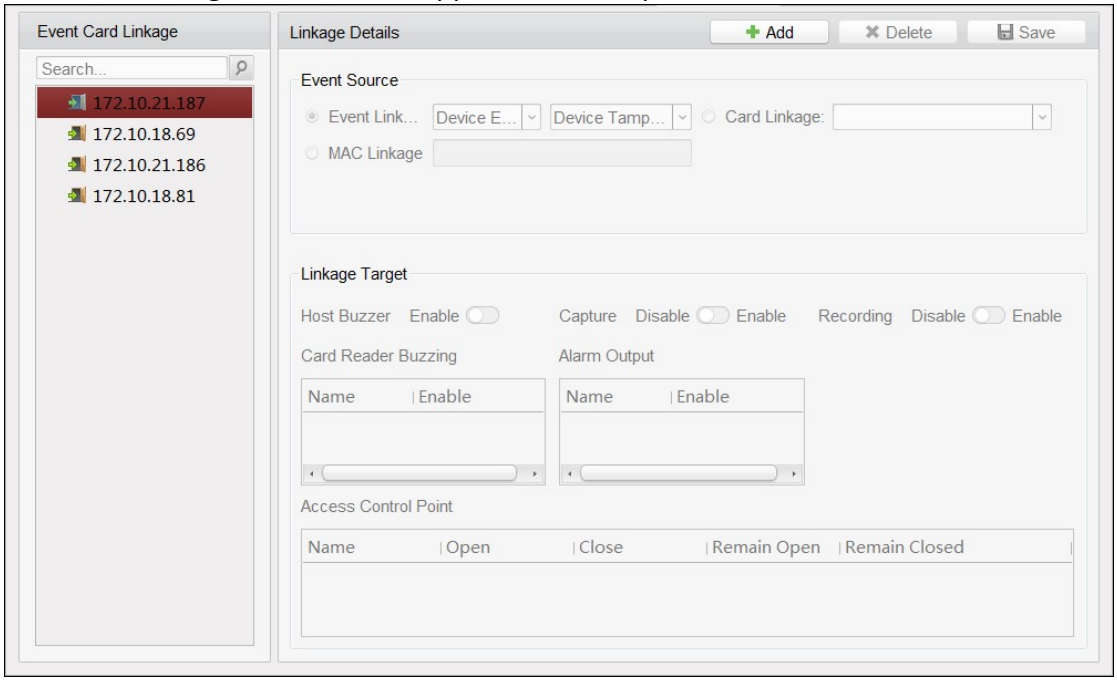


Tabella 1. 1 Azioni di collegamento per gli eventi di controllo accessi

Azioni di collegamento	Descrizioni
Audible Warning	Il software client emette un avviso acustico all'attivazione dell'allarme. È possibile selezionare la suoneria di allarme per l'avviso acustico.
Email Linkage	Consente di inviare un'e-mail di notifica contenente informazioni sull'allarme a uno o più destinatari.
Alarm on E-map	Mostra le informazioni di allarme sulla mappa elettronica. ***Nota:*** questo collegamento è disponibile solo per i punti di controllo accessi e gli ingressi di allarme.
Alarm Triggered Pop-up Image	All'attivazione dell'allarme, appare la relativa immagine con le informazioni di allarme.

7.11.2 Collegamento di eventi delle tessere

Fare clic sulla schermata **Event Card Linkage** per accedere alla seguente interfaccia.
Nota: Event Card Linkage deve essere supportato dal dispositivo.



Selezionare il dispositivo di controllo accessi dall'elenco a sinistra.
Fare clic sul pulsante **Add** per aggiungere un nuovo collegamento. È possibile impostare la sorgente dell'evento su **Event Linkage, Card Linkage** o **MAC Linkage**.

Event Linkage

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

1. Fare clic per selezionare il tipo di collegamento **Event Linkage** e selezionare il tipo di evento dall'elenco a discesa.

   Per Device Event, selezionare il tipo di evento dettagliato dall'elenco a discesa.

   Per Alarm Input, selezionare il tipo di allarme o il ripristino dell'allarme e selezionare il nome dell'ingresso di allarme dalla tabella.

   Per Door Event, selezionare il tipo di evento dettagliato e selezionare la porta di origine dalla tabella.

   Per Card Reader Event, selezionare il tipo di evento dettagliato e il lettore di tessere dalla tabella.
2. Impostare la destinazione di collegamento, quindi modificare la proprietà da a  per abilitare questa funzione.

   Host Buzzer: consente di attivare/disattivare l'avviso acustico del controller.

   Capture: si attiverà l'acquisizione in tempo reale.

   Card Reader Buzzer: consente di attivare/disattivare l'avviso acustico del lettore di tessere.

Alarm Output: consente di attivare/disattivare l'uscita di allarme per la notifica.

Access Control Point: consente di attivare i possibili stati della porta (Open, Close, Remain Open e Remain Closed).

Note:

i possibili stati della porta (aperta, chiusa, resta aperta, resta chiusa) non possono essere attivati simultaneamente.

La porta di destinazione e quella di origine non possono coincidere.

3. Fare clic su **Save** per salvare e applicare i parametri.

Collegamento delle tessere

Passaggi:

1. Fare clic per selezionare il tipo di collegamento **Card Linkage**.
2. Immettere il numero della tessera o selezionare la tessera dall'elenco a discesa.
3. Selezionare il lettore di tessere dalla tabella per l'attivazione.
4. Impostare la destinazione di collegamento, quindi modificare la proprietà da a per abilitare questa funzione.

   Host Buzzer: consente di attivare/disattivare l'avviso acustico del controller.

   Capture: si attiverà l'acquisizione in tempo reale.

   Card Reader Buzzer: consente di attivare/disattivare l'avviso acustico del lettore di tessere.

   Alarm Output: consente di attivare/disattivare l'uscita di allarme per la notifica.

   Access Control Point: consente di attivare i possibili stati della porta (Open, Close, Remain Open e Remain Closed).
5. Fare clic su **Save** per salvare e applicare i parametri.

Collegamento MAC

Passaggi:

1. Fare clic per selezionare il tipo di collegamento **MAC Linkage**.
2. Inserire l'indirizzo MAC della sorgente dell'evento.
   MAC Address Format: AA:BB:CC :DD:EE:F F.
3. Impostare la destinazione di collegamento e modificare la proprietà da a per abilitare questa funzione.

   Host Buzzer: si attiverà l'avviso acustico del controller.

   Capture: verrà attivata l'acquisizione in tempo reale.

   Recording: verrà attivata la registrazione.

   Nota: il dispositivo deve supportare la registrazione.

   Card Reader Buzzing: l'avviso acustico del lettore di tessere verrà attivato.

   Alarm Output: l'uscita di allarme verrà attivata per le notifiche.

   Zone: consente di attivare o disattivare la zona.

   Nota: il dispositivo deve supportare la funzione di zona.

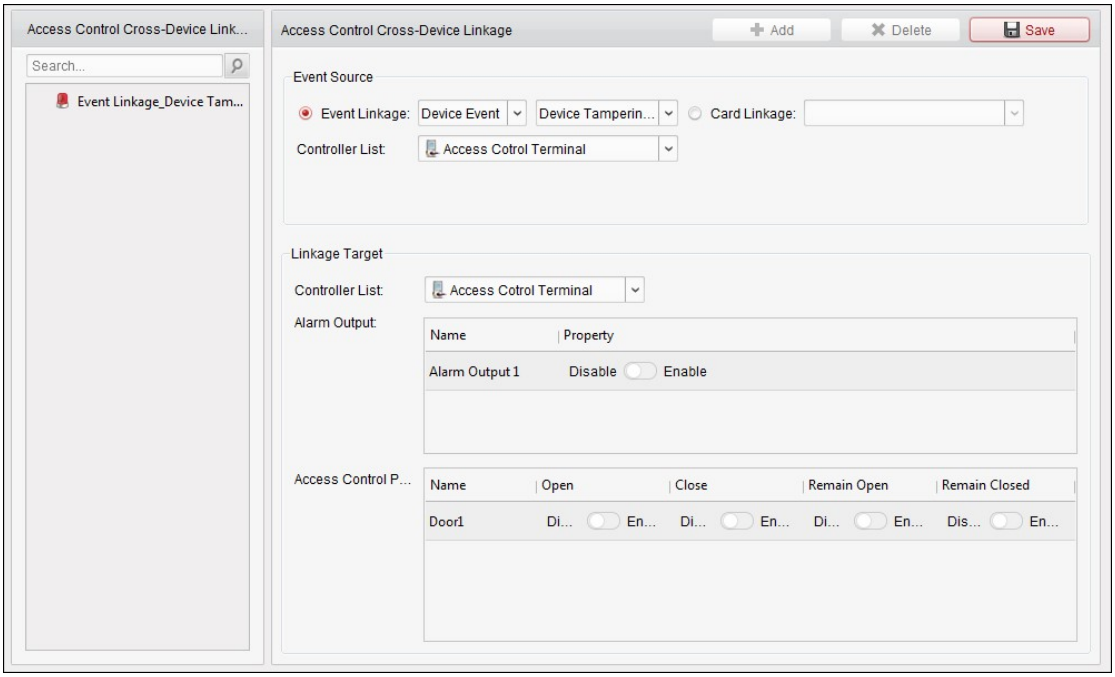
   Access Control Point: consente di attivare i possibili stati della porta (Open, Close, Remain Open e Remain Closed).
4. Fare clic su **Save** per salvare e applicare i parametri.

7.11.3 Collegamenti tra dispositivi

Scopo:

È possibile assegnare l'attivazione di un'azione su un altro dispositivo di controllo accessi, impostando una regola nel caso in cui venga attivato un evento di controllo accessi.

Fare clic sulla schermata **Cross-Device Linkage** per accedere alla seguente interfaccia.



Fare clic sul pulsante **Add** per aggiungere un nuovo collegamento del client. È possibile selezionare la sorgente dell'evento **Event Linkage** o **Card Linkage**.

Event Linkage

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

Passaggi:

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

   Per Device Event, selezionare il tipo di evento dettagliato dall'elenco a discesa.

   Per Alarm Input, selezionare il tipo di allarme o il ripristino dell'allarme e selezionare il nome dell'ingresso di allarme dalla tabella.

   Per Door Event, selezionare il tipo di evento dettagliato e selezionare la porta dalla tabella.

   Per Card Reader Event, selezionare il tipo di evento dettagliato e il lettore di tessere dalla tabella.

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

   Alarm Output: l'uscita di allarme verrà attivata per le notifiche.

   Access Control Point: verrà attivato lo stato della porta (aperta, chiusa, resta aperta o resta chiusa).

   Nota: i possibili stati della porta (aperta, chiusa, resta aperta, resta chiusa) non possono essere attivati simultaneamente.
3. Fare clic sul pulsante **Save** per salvare i parametri.

Collegamento delle tessere

Passaggi:

1. Fare clic per selezionare il tipo di collegamento **Card Linkage**.
2. Selezionare la tessera dall'elenco a discesa e selezionare il dispositivo di controllo accessi come sorgente dell'evento.
3. Selezionare il lettore di tessere dalla tabella per l'attivazione.
4. Impostare la destinazione del collegamento, selezionare il dispositivo di controllo accessi dall'elenco a discesa come destinazione di collegamento e passare dalla proprietà a per abilitare questa funzione. **Alarm Output**: l'uscita di allarme verrà attivata per le notifiche.
5. Fare clic sul pulsante **Save** per salvare i parametri.

7.12 Gestione dello stato delle porte

Scopo:

Lo stato della porta del dispositivo di controllo accessi aggiunto verrà visualizzato in tempo reale. È possibile controllare lo stato della porta selezionata e degli eventi collegati. Oltre a controllare lo stato della porta, è possibile anche impostare la durata di tali stati.

7.12.1 Gestione dei gruppi di controllo accessi

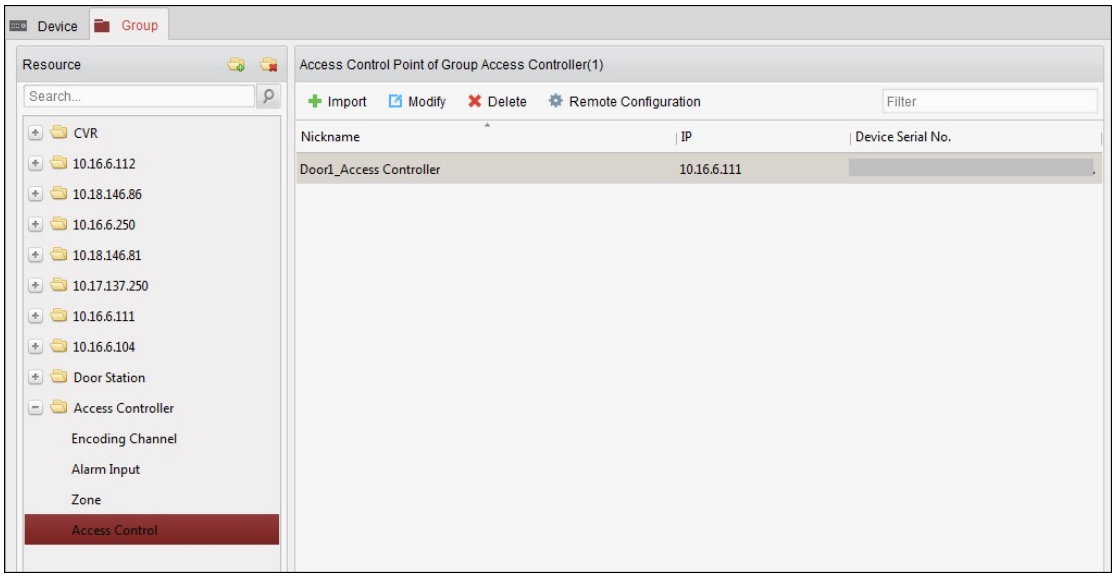
Scopo:

Prima di controllare lo stato delle porte e impostarne la durata, è necessario organizzarle in un gruppo per una gestione pratica.

Applicare la seguente procedura per creare il gruppo per il dispositivo di controllo accessi:

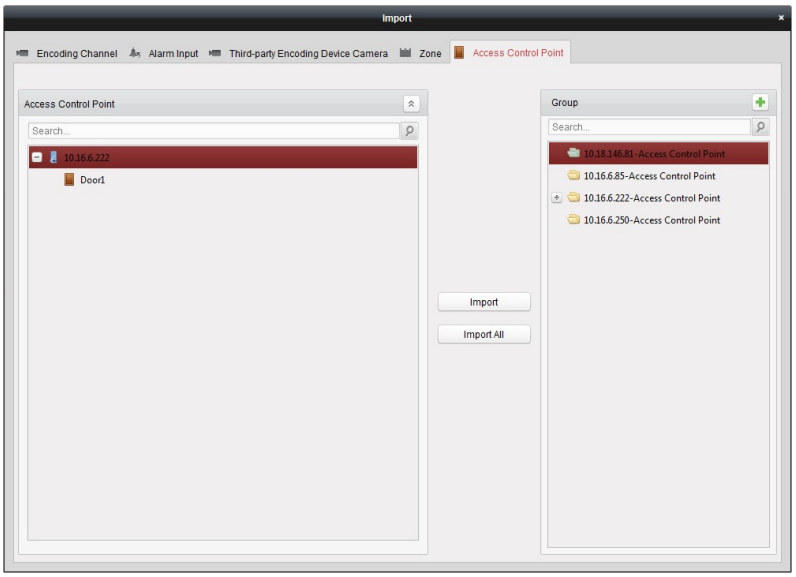
Passaggi:

1. Fare clic su sul pannello di controllo per aprire la pagina Device Management.
2. Fare clic sulla schermata **Group** per accedere all'interfaccia Group Management.



3. Per aggiungere il gruppo, procedere come segue.
   1) Fare clic su per aprire la finestra di dialogo Add Group.
   2) Immettere il nome del gruppo.
   3) Fare clic su **OK** per aggiungere il nuovo gruppo all'elenco dei gruppi.
      È possibile anche selezionare la casella di controllo **Create Group by Device Name** per creare il nuovo gruppo in base al nome del dispositivo selezionato.

4. Per importare i punti di controllo accessi nel gruppo, procedere come segue:
   1) Fare clic su **Import** nell'interfaccia Group Management, quindi fare clic sulla schermata **Access Control** per aprire la pagina Import Access Control.
      Note:
      È inoltre possibile selezionare la schermata **Alarm Input** e importare gli ingressi di allarme nel gruppo.
      Per Video Access Control Terminal, è possibile aggiungere le telecamere come canale di codifica al gruppo.
   2) Selezionare i nomi dei punti di controllo accessi dall'elenco.
   3) Selezionare un gruppo dall'elenco dei gruppi.
   4) Fare clic su **Import** per importare punti di controllo accessi selezionati nel gruppo.
      È possibile anche fare clic su **Import All** per importare tutti i punti di controllo accessi in un gruppo selezionato.



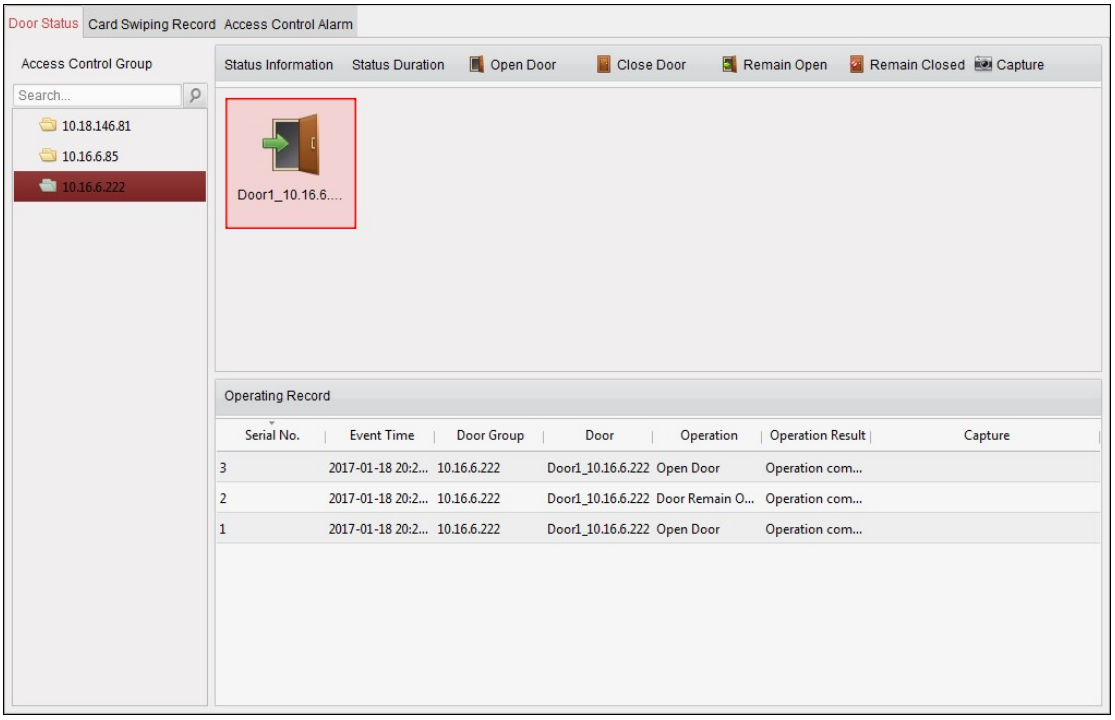
5. Dopo aver importato i punti di controllo accessi nel gruppo, è possibile fare clic su o fare doppio clic sul nome del gruppo/punto di controllo accessi per modificarlo.

7.12.2 Controllo opposto dei punti di controllo accessi (porte)

Scopo:

È possibile controllare lo stato di un singolo punto di controllo accessi (una porta), incluse operazioni di apertura e chiusura della porta o lasciandola aperta o chiusa.

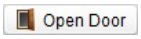
Fare clic sull'icona del pannello di controllo per accedere all'interfaccia Status Monitor.

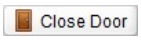


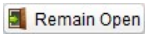
Passaggi:

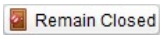
1. Selezionare un gruppo di controllo accessi sulla sinistra. Per la gestione del gruppo di controllo accessi, consultare il *Capitolo 7.12.1 Gestione dei gruppi di controllo accessi*.
2. I punti di controllo accessi del gruppo di controllo accessi selezionato verranno visualizzati a destra.

   Fare clic sull'icona  del pannello Status Information per selezionare una porta.
3. Per controllare la porta, fare clic sui pulsanti seguenti, elencati nel pannello **Status Information**.

    : fare clic per aprire la porta una volta.

    : fare clic per chiudere la porta una volta.

    : fare clic per tenere la porta aperta.

    : fare clic per tenere la porta chiusa.

    : fare clic per acquisire l'immagine manualmente.
4. È possibile visualizzare il risultato dell'operazione di controllo opposto sul pannello Operation Log.

   Note:

   Se si seleziona lo stato **Remain Open/Remain Closed**, la porta rimarrà aperta/chiusa fino a quando non verrà eseguito un nuovo comando di controllo opposto.

   Il pulsante **Capture** è disponibile quando il dispositivo supporta la funzione di acquisizione. E non è possibile realizzarla fino a quando non viene configurato il server di archiviazione.

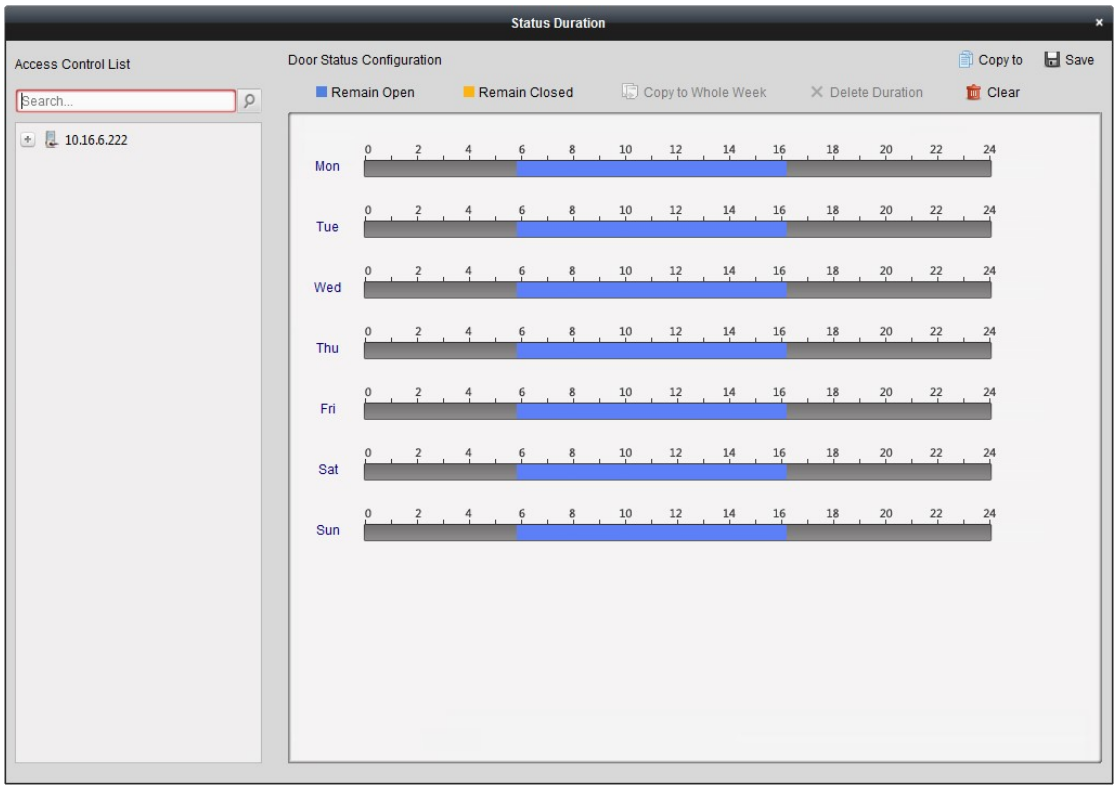
   Se la porta è impostata per restare chiusa, è possibile aprirla solo tramite la tessera di livello superiore o il software client.

7.12.3 Configurazione della durata dello stato

Scopo:

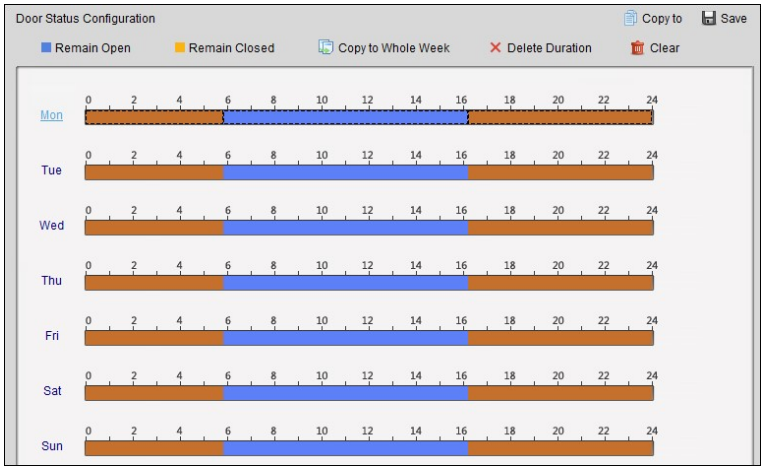
È possibile configurare pianificazioni settimanali che consentano a un punto di controllo accessi (porta) di restare aperto o chiuso.

Nel modulo Door Status, fare clic sul pulsante **Status Duration** per accedere all'interfaccia Status Duration.



Passaggi:

1. Fare clic per selezionare una porta dall'elenco dei dispositivi di controllo accessi a sinistra.
2. Sul pannello Door Status Configuration a destra, disegnare una pianificazione per la porta selezionata.
   1) Selezionare un pennello di stato della porta come Remain Open o Remain Closed.
   Remain Open: la porta resterà aperta durante il periodo di tempo configurato. Il pennello è contrassegnato con .
   Remain Closed: la porta resterà chiusa durante la durata configurata. Il pennello è contrassegnato con .
   2) Fare clic e trascinare il mouse sulla sequenza temporale per tracciare una barra colorata sulla pianificazione per impostarne la durata.

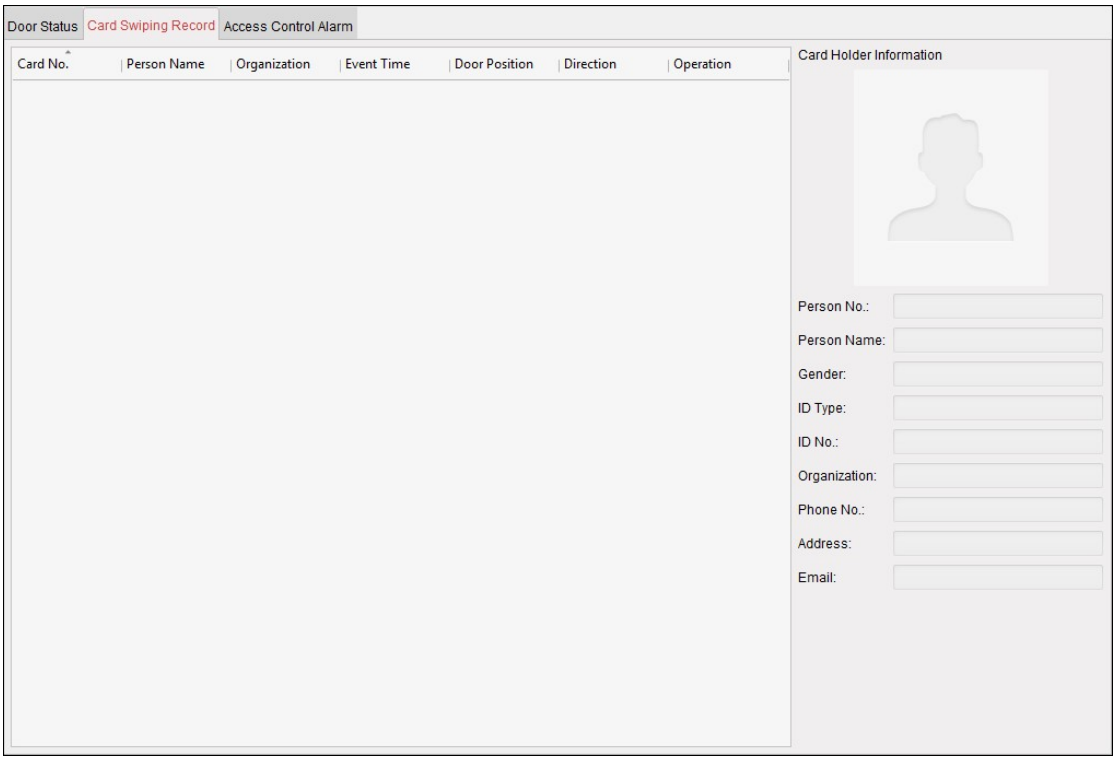


3) Quando il cursore diventa , è possibile spostare la barra temporale selezionata appena modificata. È anche possibile modificare il punto temporale visualizzato per definire accuratamente il periodo di tempo.
   Quando il cursore diventa , è possibile allungare o accorciare la barra temporale selezionata.

3. Facoltativamente, è possibile selezionare la barra temporale della pianificazione e fare clic su **Copy to Whole Week** per copiare le impostazioni della barra temporale anche agli altri giorni della settimana.
4. È possibile selezionare la barra temporale e fare clic su **Delete Duration** per eliminare il periodo di tempo in questione.
   In alternativa, è possibile fare clic su **Clear** per cancellare tutte le durate configurate nella pianificazione.
5. Fare clic su **Save** per salvare le impostazioni.
6. È possibile fare clic sul pulsante **Copy to** per copiare la pianificazione su altre porte.

7.12.4 Record di passaggio delle tessere in tempo reale

Fare clic sulla schermata **Card Swiping Record** per accedere alla seguente interfaccia.



Saranno visualizzati in tempo reale i record di passaggio delle tessere di tutti i dispositivi di controllo accessi. È possibile visualizzare i dettagli dell'evento di passaggio della tessera, quali numero di tessera, nome della persona, organizzazione, ora dell'evento, ecc.

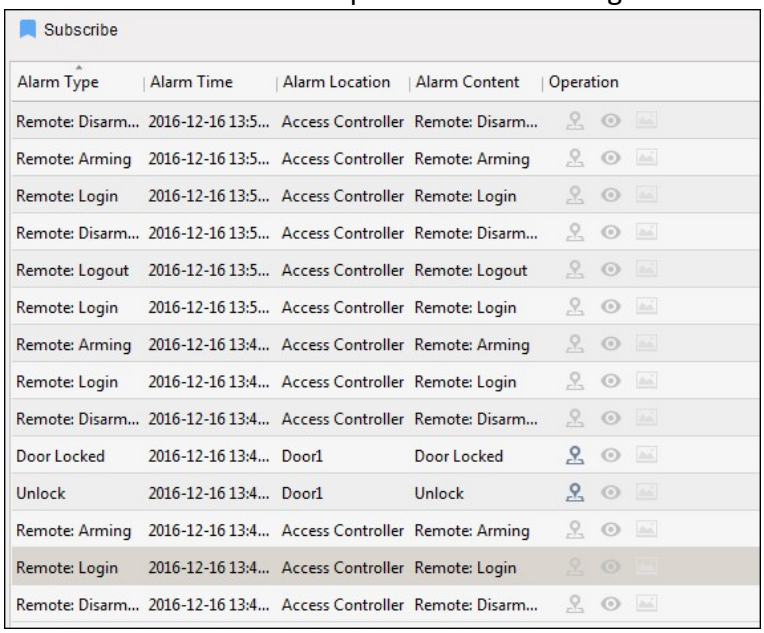
È possibile anche fare clic sull'evento per visualizzare i dettagli del titolare della tessera, quali numero della persona, nome, organizzazione, telefono, indirizzo di contatto, ecc.

7.12.5 Allarmi di controllo accessi in tempo reale

Scopo:

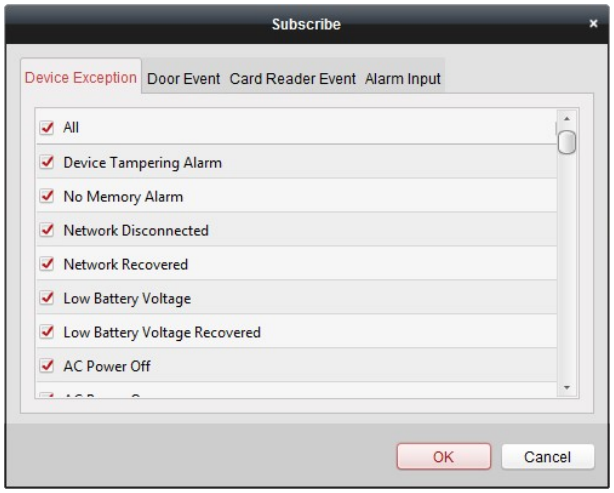
I registri degli eventi di controllo accessi sono visualizzati in tempo reale e contengono informazioni quali eccezioni dispositivi, eventi di porte, eventi di lettori di tessere e ingressi allarme.

Fare clic sulla schermata **Access Control Alarm** per accedere alla seguente interfaccia.



Passaggi:

1. Tutti gli allarmi di controllo accessi saranno visualizzati nell'elenco in tempo reale.
   È possibile visualizzare il tipo e l'orario dell'allarme, la posizione, ecc.
2. Fare clic su per visualizzare l'allarme sulla mappa elettronica.
3. È possibile fare clic su o per visualizzare le immagini in tempo reale o l'immagine acquisita dalla telecamera che si attiva quando scatta l'allarme.
   Nota: per impostare la telecamera che si attiva, consultare il *Capitolo 7.11.1 Collegamento di eventi di controllo accessi.*
4. Fare clic su **Subscribe** per selezionare l'allarme che, alla sua attivazione, sarà ricevuto dal client.



1) Attivare una o più caselle di controllo corrispondenti agli allarmi da selezionare, tra i quali allarmi di eccezione di dispositivi, allarmi attivati da eventi di porte e lettori di tessere e ingressi di allarme. 2) Fare clic su **OK** per salvare le impostazioni.

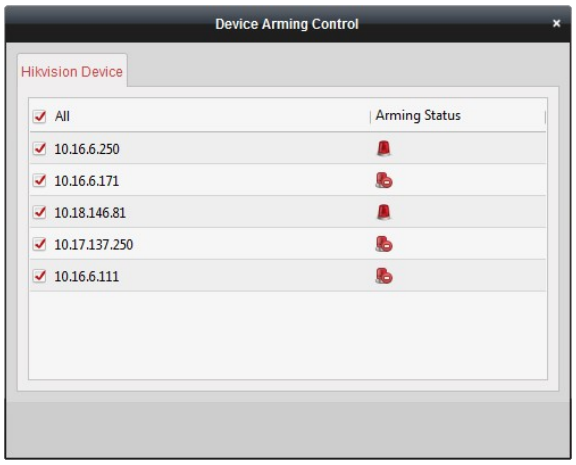
7.13 Controllo dell'attivazione

Scopo:

È possibile attivare o disattivare il dispositivo. Dopo l'attivazione del dispositivo, il client è in grado di ricevere le informazioni degli allarmi dal dispositivo.

Passaggi:

1. Fare clic su **Tool->Device Arming Control** per visualizzare la finestra Device Arming Control.
2. Attivare il dispositivo selezionando la casella di controllo corrispondente.
   In tal modo le informazioni di allarme saranno caricate automaticamente sul software client all'attivarsi dell'allarme.



7.14 Impostazioni della visualizzazione dal vivo e della riproduzione

Scopo:

È possibile definire i parametri di visualizzazione dal vivo e riproduzione, come il formato, la durata di preriproduzione, ecc.

Passaggi:

1. Aprire la pagina System Configuration.
2. Fare clic sulla schermata **Live View and Playback** per accedere all'interfaccia Live View and Playback Parameter Settings.
3. Configurare i parametri di visualizzazione dal vivo e di riproduzione. Per i dettagli, vedere la *Tabella 8-1 Parametri della visualizzazione dal vivo e della riproduzione*.
4. Fare clic su **Save** per salvare le impostazioni.

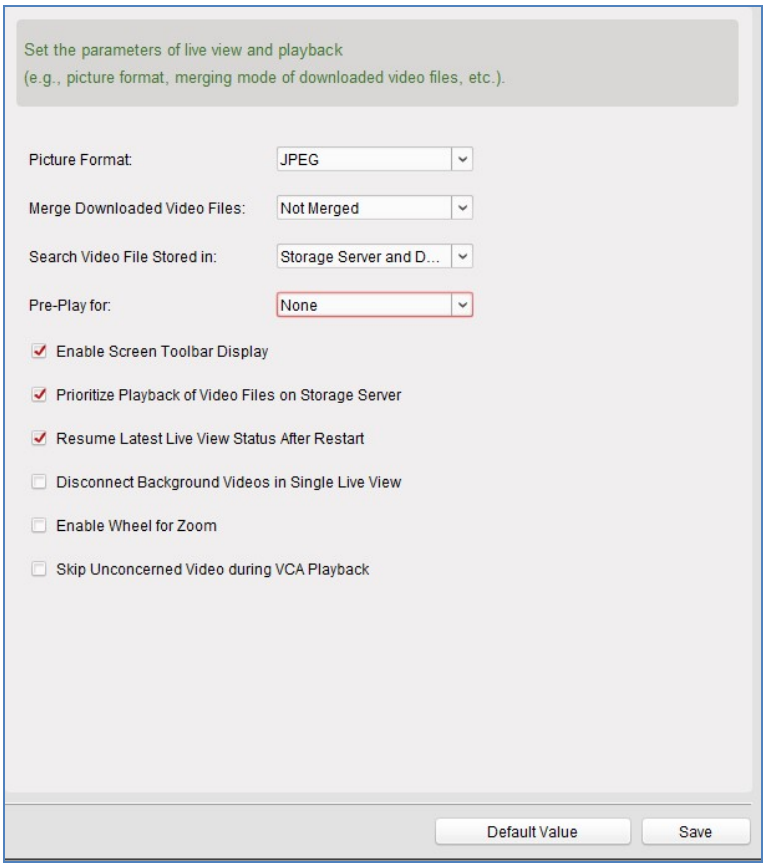


Tabella 7-1 Parametri della visualizzazione dal vivo e della riproduzione

Parametri	Descrizione
Picture Format	Imposta il formato dei file delle immagini acquisite durante la visualizzazione dal vivo e la riproduzione.
Merge Downloaded Video Files	Imposta le dimensioni massime dei file video uniti durante il download dei file video per data.
Search Video Files Stored in	Definisce se effettuare ricerche a scopo di riproduzione solo nei file video memorizzati nel dispositivo locale, solo in quelli memorizzati nel server di archiviazione o in quelli di entrambi i supporti.
Pre-play for	Definisce la durata di pre-riproduzione per la funzione playback dell'evento. ***Nota:*** è necessario impostare questo parametro su None per controllare la visualizzazione dal vivo e la riproduzione.
Enable Screen Toolbar Display	Mostra la barra degli strumenti su tutte le finestre di visualizzazione dal vivo o di riproduzione.
Prioritize Playback of Video Files on Storage Server	Dà priorità alla riproduzione dei file video registrati nel server di archiviazione. Altrimenti, riproduce i file video registrati su dispositivo locale.

Resume Latest Live View Status After Restart	Riprende l'ultima visualizzazione dal vivo dopo un nuovo accesso al client.
Disconnect Background Videos	In modalità di suddivisione multipla delle finestre, fare doppio clic su un video dal vivo per visualizzarlo in modalità di suddivisione a 1 finestra e gli altri video dal vivo
in Single Live View	vengono interrotti per risparmiare risorse.
Enable Wheel for Zoom	Abilita l'utilizzo della rotellina del mouse sia per fare zoom avanti o indietro sui video in modalità PTZ, che per lo zoom in avanti o il ripristino dei video in modalità di zoom digitale. In tal modo, scorrendo il mouse è possibile fare zoom avanti o indietro sui video dal vivo (o ripristinarne la dimensione).
Skip Unconcerned Video during VCA Playback	Consente di ignorare e di evitare la riproduzione dei video non rilevanti durante la riproduzione VCA.

7.15 Visualizzazione dal vivo

Scopo:

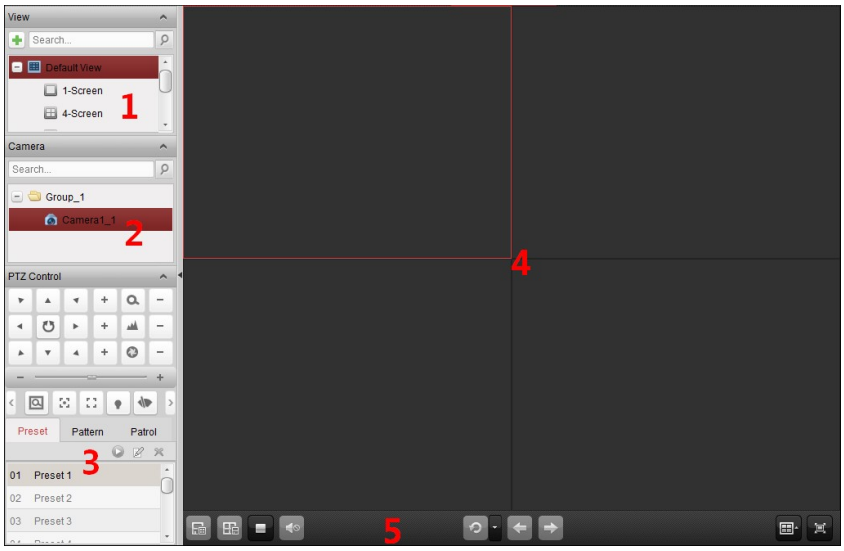
Per le attività di sorveglianza, è possibile mostrare sulla pagina Main View le riprese dal vivo dei dispositivi aggiunti, quali telecamere IP, dispositivi di codifica video e videocitofoni. Sono supportate anche alcune operazioni di base, quali acquisizione di immagini, registrazione manuale, controllo PTZ, ecc.

Prima di iniziare:

Per la visualizzazione dal vivo, occorre la definizione di un gruppo di telecamere.

In Group Management è possibile anche definire il tipo di rotazione, se necessario. Per i dettagli, fare riferimento al *Manuale dell'utente del software client iVMS-4200*.

Fare clic sull'icona  del pannello di controllo o fare clic su **View**->**Main View** per aprire la pagina Main View.



Pagina Main View

1 Elenco di visualizzazione
2 Elenco di telecamere
3 Pannello di controllo PTZ
4 Finestra della visualizzazione dal vivo
5 Barra degli strumenti della visualizzazione dal vivo

Camera Status:

La telecamera è online e funziona correttamente.
La telecamera è in modalità di visualizzazione dal vivo.
La telecamera è in stato di registrazione.
La telecamera è offline. ***Note:***

In caso di eventi individuati dalla telecamera (ad es., rilevamento di movimenti), l'icona della telecamera sarà e quella del gruppo sarà .

Se la telecamera è offline, il client può ottenere ugualmente il video dal vivo tramite il server dei flussi multimediali, previa opportuna configurazione del server. L'icona della telecamera sarà .

Barra degli strumenti della visualizzazione dal vivo:

I seguenti pulsanti sono disponibili sulla pagina Main View:

	Save View	Salva le nuove impostazioni per la visualizzazione corrente.
	Save View as	Salva la visualizzazione corrente come nuova visualizzazione distinta.
	Stop Live View	Interrompe la visualizzazione dal vivo di tutte le telecamere.
	Mute/Audio On	Attiva/disattiva l'audio della visualizzazione dal vivo.
	Resume/Pause	
	Auto-switch	Fare clic per riavviare/mettere in pausa il cambio automatico della visualizzazione dal vivo.
	Show/Hide the	Mostra/nasconde il menu di configurazione del cambio automatico. Fare di nuovo clic su **Menu** per nasconderlo.
	Previous	Consente di accedere alla visualizzazione dal vivo della pagina precedente.
	Next	Consente di accedere alla visualizzazione dal vivo della pagina successiva.
	Window Division	Imposta la suddivisione della finestra.
	Full Screen	Mostra la visualizzazione dal vivo in modalità a schermo intero. Premere **Esc** o spostare il mouse in cima allo schermo e fare clic sul pulsante **Quit Full Screen** per uscire dalla visione a schermo intero. Facendo clic sul pulsante **Lock**, è possibile bloccare lo schermo, mentre facendo clic su **Unlock** e inserendo la password amministratore del client, è possibile sbloccarlo. Per il cambio automatico a schermo intero, fare clic sul pulsante **Previous** o **Next** per passare alla telecamera precedente o a quella successiva.

Facendo clic con il tasto destro del mouse sulla finestra della visualizzazione dal vivo, si apre il menu Live View Management:

Facendo clic con il tasto destro del mouse sul menu Live View Management saranno disponibili i seguenti pulsanti:

Stop Live View Interrompe la visualizzazione dal vivo nella relativa finestra.

Capture Acquisisce l'immagine durante la visualizzazione dal vivo.

Print Captured Picture Acquisisce l'immagine corrente e la stampa.

Acquisisce l'immagine corrente e invia un'email di notifica.

Send Email a uno o più destinatari. L'e-mail può contenere in allegato l'immagine acquisita.

Start/Stop Recording Avvia/interrompe la registrazione manuale. Il file video viene memorizzato nel PC.

Open PTZ Control Attivare la funzione di controllo PTZ nella finestra di visualizzazione. Fare nuovamente clic per disattivare la funzione.

Attivare la funzione di tracciamento automatico dello Speed Dome. In questo modo lo Speed Dome traccerà automaticamente gli oggetti che appaiono nel video.

Enable Auto-tracking Questo pulsante è disponibile solo sugli Speed Dome che supportano la funzione di tracciamento automatico.

Attivare la funzione di zoom digitale. Fare nuovamente clic per disattivare la funzione **Open Digital Zoom**.

Switch to Instant

Passa in modalità riproduzione istantanea.

Playback

Start/Stop Two-way Fare clic su questo pulsante per avviare/bloccare l'audio bidirezionale con il dispositivo nella visualizzazione **Audio** dal vivo.

Fare clic su questo pulsante per avviare/bloccare l'audio bidirezionale con la telecamera nella visualizzazione **Start/Stop IP** dal vivo. Tale pulsante è disponibile solo in telecamere che supportano **Two-way Audio** la funzione audio bidirezionale IP.

Enable/Disable Audio Fare clic per abilitare/disabilitare l'audio nella visualizzazione dal vivo.

Mostra lo stato della telecamera nella visualizzazione dal vivo, quali **Camera Status** stato di registrazione, stato del segnale, numero di connessioni, ecc.

Remote

Apre la pagina di configurazione remota della telecamera in visualizzazione dal vivo.

Configuration

Accede all'interfaccia di configurazione VCA del dispositivo se si tratta di un dispositivo **VCA Configuration** VCA.

Synchronization Sincronizza la telecamera in visualizzazione dal vivo col PC su cui il software client è in esecuzione.

Batch Time Sync Imposta la sincronizzazione dell'ora dei dispositivi in batch.

Entra in modalità espansione fish-eye. Disponibile solo in caso di **Fisheye Expansion** telecamere fish-eye.

Fare clic per avviare/bloccare la localizzazione o il tracciamento dell'obiettivo in base alle **Start/Stop Speed** proprie esigenze. Disponibile solo in caso di telecamere fish-eye.

Dome linkage Per i dettagli, consultare il *Capitolo 2.4.8 Avvio del collegamento dello Speed Dome*.

Fare clic su questo pulsante per sbloccare in remoto la porta, in caso di dispositivi quali una postazione esterna, **Unlock Door** una postazione esterna condominiale o una postazione esterna (serie V).

Mostra la visualizzazione dal vivo in modalità a schermo intero. Fare di nuovo clic sull'icona per **Full Screen** uscire.

7.15.1 Avvio e interruzione della visualizzazione dal vivo

Avvio della visualizzazione dal vivo per una telecamera

Passaggi:

1. Aprire la pagina Main View.
2. C'è anche la possibilità di fare clic sull'icona nella barra degli strumenti della visualizzazione dal vivo per selezionare la modalità di suddivisione della finestra di visualizzazione.

3. Fare clic e trascinare la telecamera nella finestra di visualizzazione o fare doppio clic sul nome della telecamera dopo aver selezionato la finestra, per avviare la visualizzazione dal vivo. ***Nota:*** si può anche fare clic e trascinare il video della telecamera in visualizzazione dal vivo su un'altra finestra di visualizzazione, se necessario.

Avvio della visualizzazione dal vivo per gruppi di telecamere

Passaggi:

1. Aprire la pagina Main View.
2. Fare clic e trascinare il gruppo nella finestra di visualizzazione o fare doppio clic sul nome del gruppo per avviare la visualizzazione dal vivo.
   Nota: il numero della finestra di visualizzazione si adatta automaticamente al numero della telecamera del gruppo.

Avvio della visualizzazione dal vivo in modalità di visualizzazione predefinita

Scopo:

Il video delle telecamere aggiunte può essere visualizzato in varie modalità. Si possono selezionare 4 modalità di visualizzazione predefinite usate frequentemente: 1-Screen, 4-Screen, 9-Screen e 16-Screen.

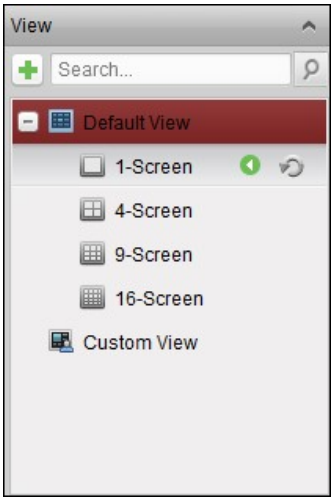
Passaggi:

1. Aprire la pagina Main View.
2. Nel pannello View, fare clic sull'icona per espandere l'elenco delle visualizzazioni predefinite.
3. Fare clic sulla modalità di visualizzazione predefinita richiesta per selezionarla; i video delle telecamere aggiunte saranno visualizzati in sequenza nella modalità selezionata.
   Nota: facendo clic su , è possibile salvare la visualizzazione predefinita come personalizzata.

Spostando il mouse sulla visualizzazione, sono disponibili le seguenti icone:

Start Instant Playback Avvia la riproduzione istantanea della visualizzazione.

Start Auto-switch Avvia il cambio automatico della visualizzazione.



Avvio della visualizzazione dal vivo in modalità di visualizzazione personalizzata

Scopo:

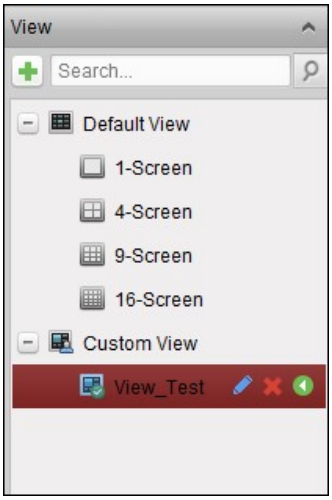
È possibile personalizzare anche la modalità di visualizzazione dal vivo.

Passaggi:

1. Aprire la pagina Main View.
2. Nel pannello View, fare clic sull'icona per espandere l'elenco delle visualizzazioni personalizzate. Se è disponibile una visualizzazione personalizzata, è possibile fare clic su di essa per avviare la visualizzazione dal vivo personalizzata.
3. Fare clic su per creare una nuova visualizzazione.
4. Inserire il nome della visualizzazione e fare clic su **Add**. Per impostazione predefinita, la nuova visualizzazione è in modalità 4-Screen.
5. C'è anche la possibilità di fare clic sull'icona nella barra degli strumenti della visualizzazione dal vivo, per selezionare il layout dello schermo per la nuova visualizzazione.
6. Fare clic e trascinare la telecamera/gruppo nella finestra di visualizzazione o fare doppio clic sul nome della telecamera/gruppo in modalità di visualizzazione personalizzata per avviare la visualizzazione dal vivo.
7. Fare clic sull'icona per salvare la nuova visualizzazione. Si può anche fare clic su per salvare la visualizzazione come visualizzazione personalizzata distinta.

Spostando il mouse sulla visualizzazione personalizzata, sono disponibili le seguenti icone:

- **Edit View Name** Modifica il nome della visualizzazione personalizzata.
- **Delete View** Elimina la visualizzazione personalizzata.
- **Start Instant Playback** Avvia la riproduzione istantanea della visualizzazione.



Interruzione della visualizzazione dal vivo

Passaggi:

1. Selezionare la finestra di visualizzazione.
2. Fare clic sull'icona nell'angolo in alto a destra, quando il puntatore del mouse si trova sulla finestra di visualizzazione o fare clic su **Stop Live View** nel menu di scelta rapida, per interrompere la visualizzazione dal vivo nella finestra. Si può anche fare clic sul pulsante nella barra degli strumenti della visualizzazione dal vivo per interrompere tutte le visualizzazioni dal vivo.

7.15.2 Registrazione e acquisizione manuale

Barra strumenti in ogni finestra della visualizzazione dal vivo:

I seguenti pulsanti sono disponibili sulla barra strumenti di ogni finestra di visualizzazione dal vivo:


Acquisisce l'immagine durante la visualizzazione dal vivo. L'immagine **Capture** acquisita è memorizzata nel PC.


Start/Stop Avvia/interrompe la registrazione manuale. Il file video è memorizzato **Recording** nel PC.


Switch to Instant Playback Passa alla modalità di riproduzione istantanea.

Registrazione manuale in visualizzazione dal vivo

Scopo:

La funzione Manual Recording permette di registrare manualmente il video dal vivo sulla pagina Main View e i relativi file video vengono salvati nel PC locale.

Passaggi:

1. Spostare il puntatore del mouse sulla finestra di visualizzazione dal vivo per far apparire la barra degli strumenti.
2. Fare clic su  nella barra degli strumenti della finestra di visualizzazione o accedere al menu di scelta rapida Live View Management per avviare la registrazione manuale. L'icona  diventa  .
3. Fare clic sull'icona  per interrompere la registrazione manuale.

   Se tutte le operazioni sono andate a buon fine, appare una casella di richiesta del percorso di salvataggio dei file appena registrati. ***Note:***

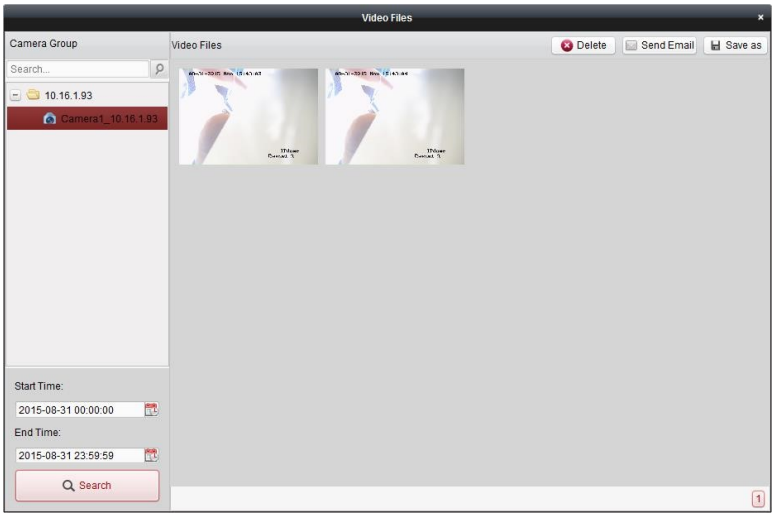
   Durante la registrazione manuale, appare l'indicatore  nell'angolo in alto a destra della finestra di visualizzazione.
   Il percorso di salvataggio dei file video può essere impostato nell'interfaccia System Configuration. Per i dettagli, vedere la *Sezione 14.2.3 Impostazioni del percorso di salvataggio dei file*.
   La registrazione manuale in visualizzazione dal vivo non è supportata dal dispositivo Hik Cloud P2P.

Visualizzazione di file video locali

Passaggi:

1. Fare clic su **File->Open Video File** per aprire la pagina Video Files.
2. Selezionare la videocamera da cercare nell'elenco Camera Group.
3. Fare clic sull'icona  per specificare l'ora di inizio e di fine della ricerca.

4. Fare clic su **Search**. Vengono visualizzati i file video registrati tra l'ora di inizio e l'ora di fine.
   Selezionare il file video e fare clic su **Delete**. È possibile eliminare il file video.
   Selezionare il file video e fare clic su **Send Email**. È possibile inviare un'e-mail di notifica con il file video selezionato in allegato.
   Selezionare il file video e fare clic su **Save as**. È possibile salvare una nuova copia del file video.
   Nota: per poter inviare un'email di notifica, occorre prima aver configurato le impostazioni Email.



Facendo doppio clic sul file video, il video può essere riprodotto localmente.

Sulla pagina di riproduzione locale sono disponibili i seguenti pulsanti:

CIF/4CIF	Mostra il video con risoluzione cif/4cif.
Full Screen	Mostra la pagina di riproduzione locale in modalità a schermo intero.
Close	Chiude la pagina di riproduzione locale dei file video.
Pause/Play	Mette in pausa/avvia la riproduzione dei file video.
Stop	Interrompe la riproduzione dei file video.
Speed	Imposta la velocità di riproduzione.
Single Frame	Riproduce i file video fotogramma per fotogramma.
Digital Zoom	Attiva la funzione di zoom digitale. Fare di nuovo clic per disabilitare la funzione.

	**Enable/Disable**	Fare clic per abilitare/disabilitare l'audio nella riproduzione **Audio** locale.
	Capture	Acquisisce l'immagine durante la riproduzione.

Acquisizione di immagini nella visualizzazione dal vivo

Passaggi:

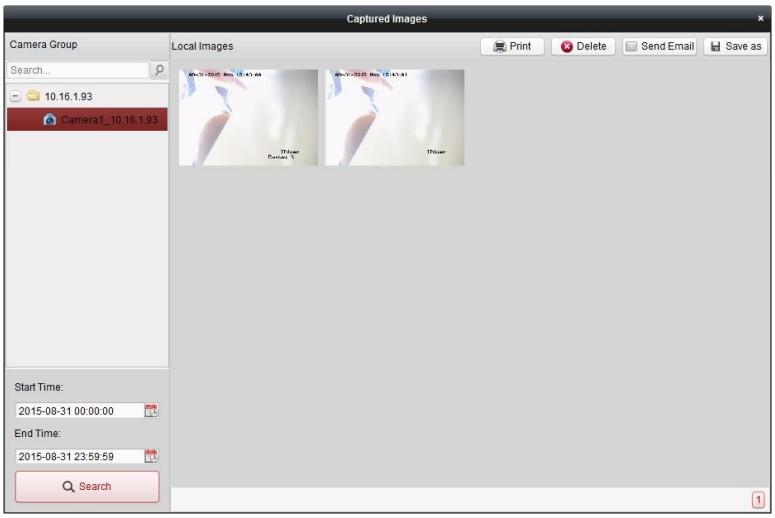
1. Spostare il puntatore del mouse sulla finestra di visualizzazione dal vivo per far apparire la barra degli strumenti.
2. Fare clic sull'icona  nella barra degli strumenti della finestra di visualizzazione o accedere al menu di scelta rapida Live View Management.
   Appare una piccola finestra con l'immagine acquisita, per indicare se l'operazione di acquisizione è andata a buon fine o meno.
   Nota: il percorso di salvataggio delle immagini acquisite può essere impostato nell'interfaccia System Configuration. Per i dettagli, consultare il *Manuale dell'utente del software client iVMS-4200*.

Visualizzazione delle immagini acquisite

Le immagini acquisite durante la visualizzazione dal vivo vengono memorizzate nel PC su cui è in esecuzione il software. Se necessario, è possibile visualizzare le immagini acquisite.

Passaggi:

1. Fare clic su **File**->**Open Image File** per aprire la pagina Captured Images.
2. Selezionare la videocamera da cercare nell'elenco Camera Group.
3. Fare clic sull'icona  per specificare l'ora di inizio e di fine della ricerca.
4. Fare clic su **Search**. Saranno visualizzate le immagini acquisite tra gli orari iniziale e finale indicati.
5. Fare doppio clic sull'immagine acquisita per ingrandirla e averne una migliore visualizzazione.
   Selezionare l'immagine acquisita e fare clic su **Print**. È possibile stampare l'immagine selezionata.
   Selezionare l'immagine acquisita e fare clic su **Delete**. È possibile cancellare l'immagine selezionata.
   Selezionare l'immagine acquisita e fare clic su **Send Email**. È possibile inviare un'email di notifica con allegata l'immagine selezionata.
   Selezionare l'immagine acquisita e fare clic su **Save as**. Si può salvare una nuova copia dell'immagine selezionata.



7.15.3 Riproduzione istantanea

Scopo:

Sulla pagina Main View è possibile riprodurre all'istante i file video. La riproduzione istantanea permette di visualizzare un frammento del video particolarmente significativo, o che era risultato poco chiaro a prima vista. Così, se necessario, è possibile un controllo immediato del video.

Prima di iniziare:

I file video devono essere registrati su dispositivi di archiviazione, quali schede SD/SDHC e HDD, su DVR, NVR, telecamere IP, ecc., o su server di archiviazione.

Passaggi:

1. Avviare la visualizzazione dal vivo e spostare il mouse sulla finestra di visualizzazione per far apparire la barra degli strumenti. È anche possibile spostare il mouse sulla visualizzazione predefinita o su quella personalizzata e fare clic su per abilitare la riproduzione istantanea della visualizzazione selezionata.
2. Fare clic sull'icona nella barra degli strumenti e comparirà un elenco dei periodi di tempo.

   È possibile selezionare 30s, 1 min, 3 min, 5 min, 8 min e 10 min.
3. Selezionare un periodo di tempo per avviare la riproduzione istantanea.

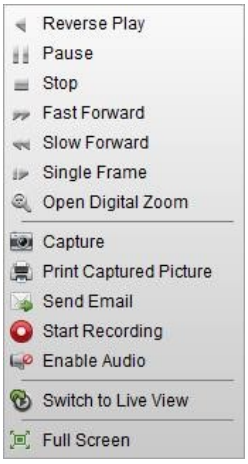
   Esempio: se l'ora corrente della visualizzazione dal vivo è 09:30:00 e si seleziona 3 min, la riproduzione istantanea inizierà alle 09:27:00.
4. Fare nuovamente clic sull'icona per interrompere la riproduzione istantanea e tornare alla visualizzazione dal vivo.

   Nota: durante la riproduzione istantanea, viene visualizzato un indicatore nell'angolo superiore destro della finestra di visualizzazione.

Nella pagina di riproduzione istantanea sono disponibili i seguenti pulsanti nella barra degli strumenti:

Reverse Playback	Riproduce il file video in senso inverso.
Pause/Start Playback	Mette in pausa/avvia la riproduzione dei file video.
Stop Playback	Interrompe la riproduzione di tutte le telecamere.
Slow Forward/Fast Forward	Diminuisce/aumenta la velocità di riproduzione.
Single Frame (Reverse)	Riproduce i file video fotogramma per fotogramma (al contrario).

Facendo clic col tasto destro sulla finestra di visualizzazione, si apre il menu Instant Playback Management:



Facendo clic con il tasto destro del mouse sul menu Instant Playback Management saranno disponibili i seguenti pulsanti:

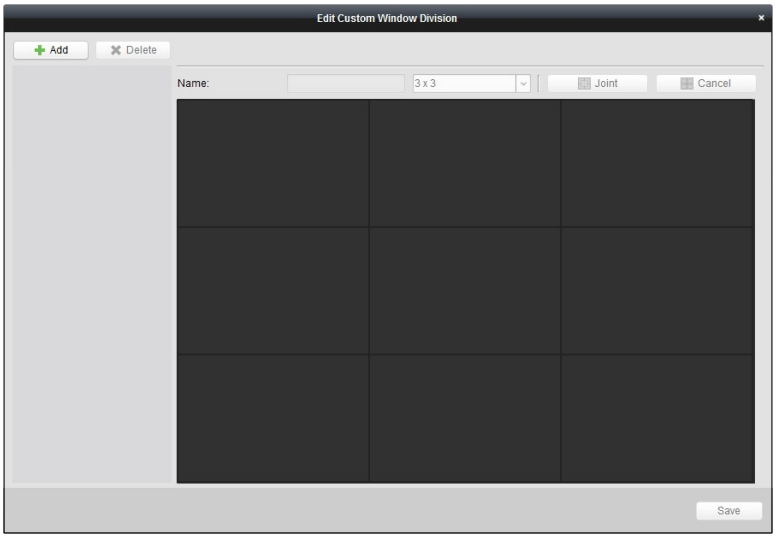
Reverse Playback	Riproduce il file video in senso inverso.
Pause/Play	Mette in pausa/avvia la riproduzione istantanea nella finestra di visualizzazione.
Stop	Arresta la riproduzione istantanea e ripristina la visualizzazione dal vivo.
Fast Forward/Slow Forward	Aumenta/diminuisce la velocità di riproduzione istantanea.
Single Frame (Reverse)	Riproduce i file video fotogramma per fotogramma (al contrario).
Open Digital Zoom	Attiva la funzione di zoom digitale. Fare nuovamente clic per disattivare la funzione **Open Digital Zoom**.
Capture	Acquisisce un'immagine durante la riproduzione istantanea.
Print Captured Picture	Acquisisce l'immagine corrente e la stampa.
Send Email	Acquisisce l'immagine corrente e invia un'email di notifica a uno o più destinatari. L'e-mail può contenere in allegato l'immagine acquisita.
Start/Stop Recording	Avvia/interrompe il ritaglio dai file video.
Enable/Disable Audio	Fare clic su questa opzione per attivare/disattivare l'audio nella visualizzazione istantanea.
Switch to Live View	Consente di passare alla modalità di visualizzazione dal vivo.
Full Screen	Mostra la riproduzione istantanea in modalità a schermo intero. Fare di nuovo clic per uscire.

7.15.4 Suddivisione personalizzata della finestra

Scopo:

Il software client fornisce numerose modalità di suddivisione predefinita per la finestra. È possibile anche impostare la suddivisione personalizzata della finestra. ***Passaggi:***

1. Fare clic su sulla barra degli strumenti della visualizzazione dal vivo e selezionare Edit per far apparire la finestra di dialogo di suddivisione personalizzata della finestra.



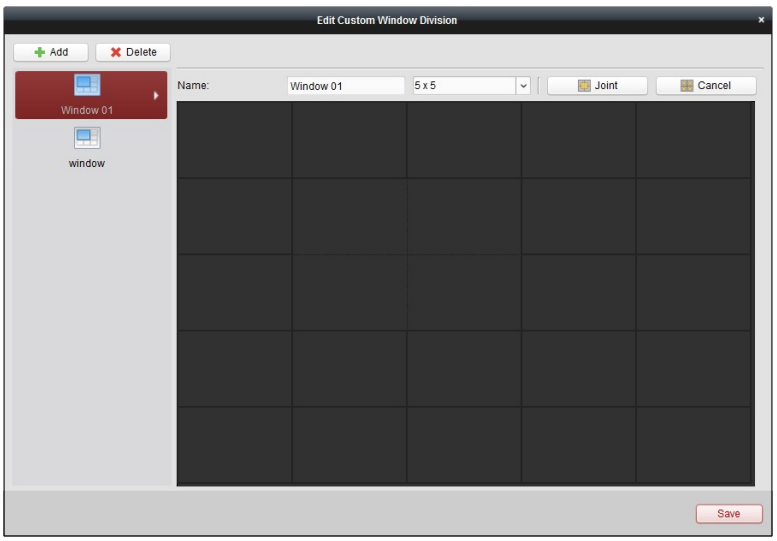
2. Fare clic su **Add** per aprire la finestra di dialogo di aggiunta di suddivisioni personalizzate per la finestra.

   Nota: si possono aggiungere fino a 5 suddivisioni personalizzate per la finestra.

3. Inserire un nome per la nuova suddivisione della finestra e poi fare clic su **OK** per salvare le impostazioni.

4. È possibile modificare il nome e il tipo di suddivisione della finestra (3x3, 4x4, 5x5).
5. Fare clic e trascinare il mouse per selezionare le finestre adiacenti, quindi fare clic su **Joint** per unirle a formare una finestra unica. Facendo clic su **Cancel** è possibile annullare l'unione.

6. Fare clic su **Save** per confermare le impostazioni. Fare clic per tornare alla pagina Main View. Poi fare clic su e selezionare la suddivisione personalizzata della finestra per la riproduzione del video dal vivo.



Note:

La procedura precedente per la configurazione della suddivisione personalizzata della finestra può essere eseguita anche accedendo alla pagina Remote Playback.

In riproduzione remota, è possibile avviare la riproduzione in un massimo di 16 finestre allo stesso tempo. Perciò, le suddivisioni personalizzate con più di 16 finestre non sono valide per la riproduzione.

7.15.5 Altre funzioni nella visualizzazione dal vivo

Ci sono varie altre funzioni disponibili nella visualizzazione dal vivo, quali zoom digitale, audio bidirezionale, stato telecamera e sincronizzazione.

Auxiliary Screen Preview

I video dal vivo possono essere visualizzati in vari schermi ausiliari, per consentire un'adeguata anteprima di più scene di sorveglianza. Sono supportati fino a 3 schermi ausiliari.

Channel-zero

Per quanto riguarda il canale zero del dispositivo, tenendo premuto il tasto *Ctrl* e facendo doppio clic, è possibile visualizzare il canale specifico. Tenere premuto il tasto *Ctrl* e fare doppio clic di nuovo, per ripristinare la visione normale.

Two-way Audio

La funzione di audio bidirezionale consente di parlare attraverso la telecamera. In tal modo è possibile ottenere non solo il video dal vivo, ma anche l'audio in tempo reale della telecamera. Se il dispositivo è dotato di più canali audio bidirezionali, è possibile scegliere quello da cui avviare la modalità bidirezionale.

L'audio bidirezionale può essere usato per una sola telecamera alla volta.

Camera Status

Il sistema è in grado di rilevare e visualizzare a scopo di verifica le informazioni di stato della telecamera, quali stato di registrazione e segnale, numero di connessioni, ecc. Le informazioni di stato si aggiornano ogni 10 secondi.

Synchronization

La funzione di sincronizzazione permette di sincronizzare l'orologio del dispositivo con quello del PC su cui è in esecuzione il software client.

7.16 Riproduzione remota

Se i dispositivi di archiviazione video in uso sono HDD, HDD di rete, o schede SD/SDHC sul dispositivo locale, oppure server di archiviazione remota connessi al sistema, è possibile definire per le telecamere pianificazioni di registrazioni e acquisizioni immagini in modalità continua, o attivate da allarme e da comando. È anche possibile effettuare ricerche sui file video per la riproduzione remota.

7.16.1 Memorizzazione sui dispositivi di archiviazione

Scopo:

È possibile aggiungere dispositivi di archiviazione al client, per la memorizzazione di file video e immagini acquisiti dai dispositivi di codifica aggiunti; tali file possono essere oggetto di ricerche per la riproduzione remota. I dispositivi di archiviazione possono essere server di archiviazione, CVR (Center Video Recorder) o altri NVR. Qui a titolo di esempio, mostriamo le impostazioni di un server di archiviazione.

Prima di iniziare:

Il software applicativo del server di archiviazione, compreso nel pacchetto software iVMS-4200, deve essere installato. Durante l'installazione dell'iVMS-4200, attivare la casella di controllo **Storage Server** per abilitare l'installazione del server di archiviazione.

Aggiunta del server di archiviazione

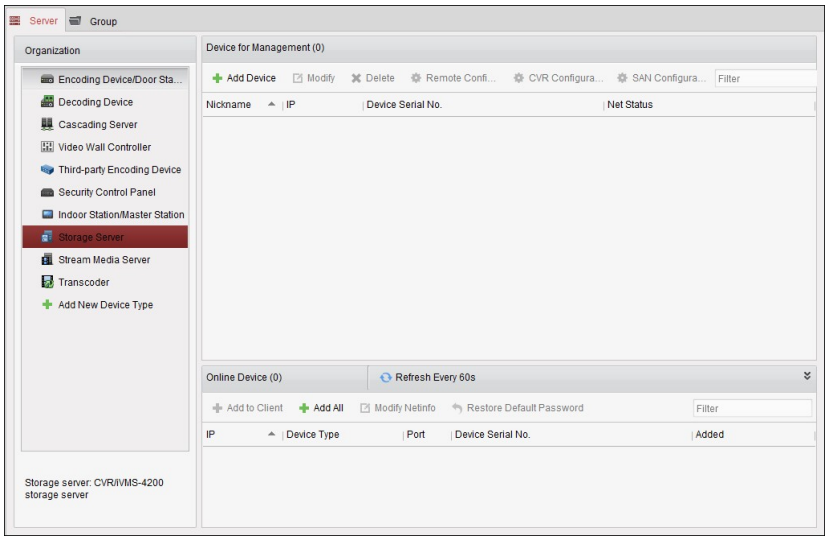
Passaggi:

1. Fare clic sull'icona di collegamento  sul desktop per lanciare il server di archiviazione.

   Note:

   È anche possibile registrare i file video su server di archiviazione installati su altri PC.

   Se la porta del server di archiviazione (valore: 8000) è già occupata da altri servizi, apparirà una finestra di dialogo. In tal caso occorre inserire un altro numero di porta, per garantire il corretto funzionamento del server di archiviazione.
2. Aprire la pagina Device Management e fare clic sulla schermata **Server**.
3. Fare clic su **Add New Device Type**, selezionare **Storage Server** e fare clic **su OK**.
4. Fare clic su **Storage Server** nell'elenco per accedere all'interfaccia Storage Server Adding.



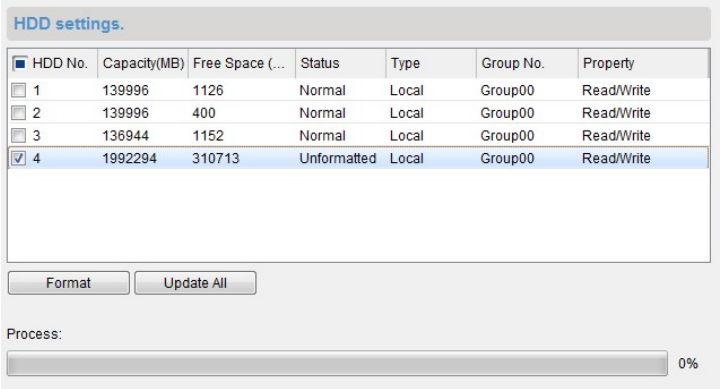
5. Aggiungere il server di archiviazione.

Formattazione degli HDD

I dischi rigidi del server di archiviazione devono essere formattati per l'archiviazione di immagini e file video.

Passaggi:

1. Selezionare il server di archiviazione aggiunto dall'elenco e fare clic su **Remote Configuration**.
2. Fare clic su **Storage**->**General** per accedere all'interfaccia HDD Formatting.
3. Selezionare l'HDD dall'elenco e fare clic su **Format**. È possibile controllare il processo di formattazione dalla barra dei processi e lo stato del disco rigido formattato passa da *Unformatted* a *Normal Status*. ***Nota:*** la formattazione delle unità disco rigido consente di preallocare lo spazio su disco per l'archiviazione e i dati originali dei dischi rigidi formattati non verranno eliminati.



Configurazione delle funzioni SAN e CVR

Scopo:

Il client fornisce la configurazione delle funzioni SAN e CVR per definire comodamente il volume logico e la funzione CVR per il dispositivo CVR. Per un'introduzione dettagliata alla configurazione delle funzioni SAN e CVR, fare riferimento al *Manuale dell'utente* del CVR.

Nota: questa funzione deve essere supportata dal dispositivo.

Selezionare il CVR aggiunto dall'elenco e fare clic su **CVR Configuration** o **SAN Configuration**.

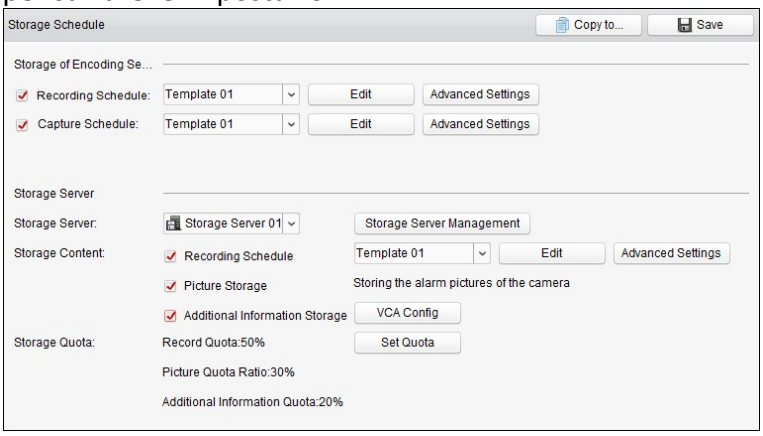
Configurazione della pianificazione di archiviazione

Prima di iniziare:

Il server di archiviazione deve essere aggiunto al software client e i dischi rigidi devono essere formattati per l'archiviazione dei file video.

Passaggi:

1. Aprire la pagina Storage Schedule.
2. Selezionare la videocamera dall'elenco Camera Group.
3. Selezionare il server di archiviazione dall'elenco a discesa **Storage Server**.
   Nota: è possibile fare clic su **Storage Server Management** per aggiungere, modificare o eliminare il server di archiviazione.
4. Selezionare la casella di controllo **Recording Schedule** per abilitare la memorizzazione dei file video. È inoltre possibile selezionare la casella di controllo **Picture Storage** per memorizzare le immagini di allarme della telecamera al verificarsi di un evento.
   Per le telecamere IP con la funzione di mappa termica o conteggio delle persone, è disponibile la casella di controllo **Additional Information Storage**. È possibile fare clic su **VCA Config** per impostare la regola VCA per la telecamera e selezionare la casella di controllo **Additional Information Storage** e la mappa termica, i dati di conteggio delle persone e quelli sul traffico stradale verranno caricati sul server di archiviazione.
   Nota: per la configurazione dettagliata dell'impostazione della regola VCA, fare riferimento al *Manuale dell'utente* della telecamera.
5. Selezionare il modello di pianificazione per la registrazione dall'elenco a discesa.
   Se è necessario modificare o personalizzare il modello, vedere *Configurazione del modello di pianificazione della registrazione*.
6. Fare clic su **Advanced Settings** per impostare l'ora di preregistrazione, l'ora di post-registrazione e altri parametri per la registrazione.
7. Fare clic su **Set Quota** per accedere all'interfaccia di gestione dell'HDD del server di archiviazione. È possibile impostare il rapporto di quota corrispondente per record, immagini e informazioni aggiuntive.
   Esempio: se si imposta la quota di registrazione su 60%, è possibile utilizzare il 60% dello spazio di archiviazione per memorizzare i file video.
8. Fare clic su **Save** per salvare le impostazioni.



Nota: il server di archiviazione consente la memorizzazione di registrazioni relative ad allarmi quali rilevamento di attraversamento di linee, rilevamento di intrusioni, rilevamento di ingresso e uscita aree, rilevamento di movimento rapido, rilevamento di assembramento di persone, rilevamento di stazionamenti sospetti, rilevamento di parcheggio, rilevamento rimozione di oggetti e rilevamento di bagagli abbandonati.

7.16.2 Riproduzione normale

Scopo:

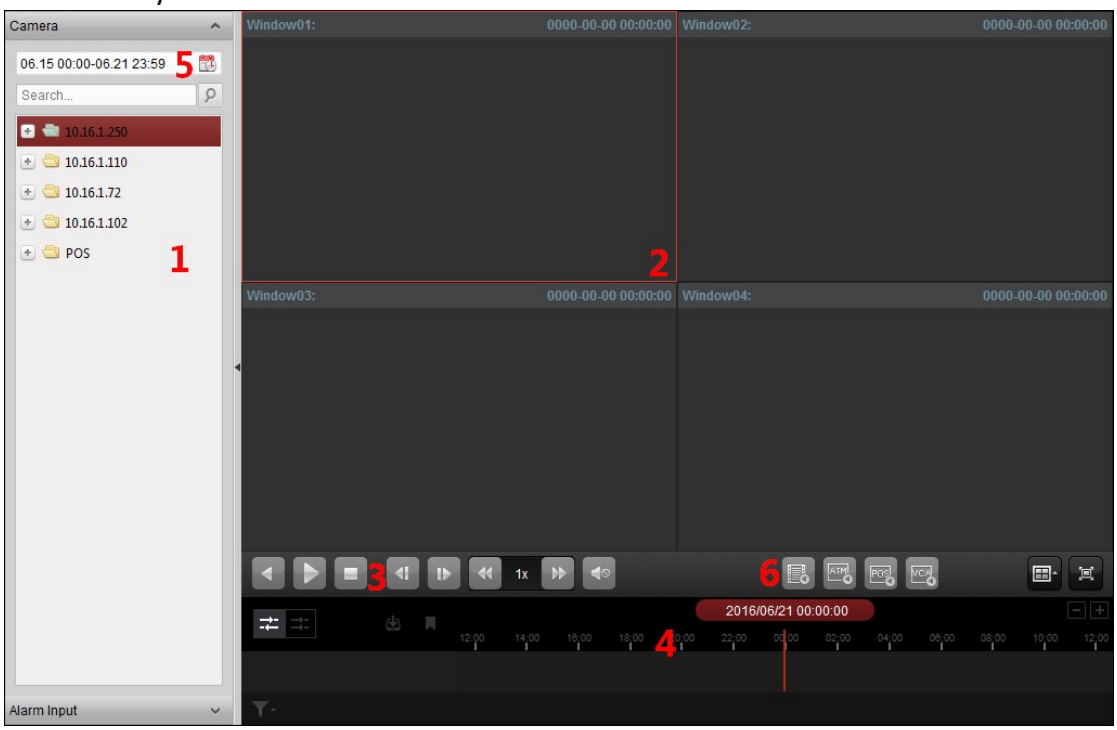
I file video memorizzati su dispositivo locale o su server di archiviazione possono essere oggetto di ricerca in base alla telecamera o all'evento scatenante, per poi essere riprodotti da remoto.

Prima di iniziare:

È possibile impostare la riproduzione dei file video memorizzati su dispositivo locale, su server di archiviazione o su entrambe le apparecchiature. Per i dettagli, fare riferimento alla sezione *8.5.1 Memorizzazione sui dispositivi di archiviazione*.

In Group Management, è possibile anche impostare la direzione di rotazione delle telecamere per la riproduzione. Fare riferimento alla sezione *Modifica del gruppo/telecamera* del *Capitolo 8.3 Gestione di gruppi*.

Fare clic sull'icona  del pannello di controllo, o fare clic su **View**->**Remote Playback** per aprire la pagina Remote Playback.



Pagina Remote Playback

1 Elenco di telecamere
2 Finestra di visualizzazione della riproduzione
3 Pulsanti di controllo di riproduzione
4 Sequenza temporale
5 Calendari
6 Condizioni di ricerca

Cambiamento del flusso video per la riproduzione

Scopo:

È possibile passare dal flusso principale al flusso secondario e viceversa per la riproduzione.

Prima di iniziare:

Impostare il flusso video per la registrazione come Dual-Stream.

Nota: questa funzione deve essere supportata dal dispositivo.

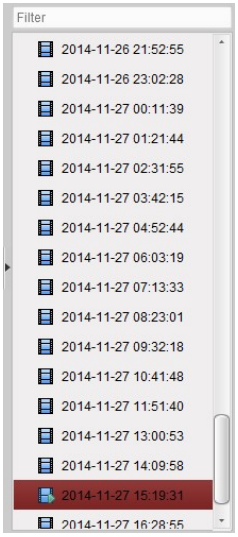
Passaggi:

1. Accedere all'interfaccia Group Management e aprire la finestra di dialogo Modify Camera (consultare la sezione *Modifica del gruppo/telecamera* del *Capitolo 8.3 Gestione di gruppi*).
2. Impostare il flusso video della telecamera come flusso primario o secondario.

Ricerca di file video per la riproduzione normale

Passaggi:

1. Aprire la pagina Remote Playback.
2. Fare clic sull'icona dei calendari per attivare la corrispondente finestra di dialogo. Selezionare la data di inizio e fine del periodo, quindi impostare l'ora esatta. Fare clic su **OK** per salvare il periodo di ricerca.
3. Fare clic e trascinare la telecamera o il gruppo nella finestra di visualizzazione o fare doppio clic sul nome della telecamera o del gruppo per avviare la riproduzione.
4. I file video trovati nella ricerca del gruppo o della telecamera selezionati saranno elencati sulla destra dell'interfaccia in ordine cronologico. È possibile filtrare i risultati di ricerca tramite il campo di testo **Filter**. Il primo file video sarà riprodotto automaticamente per impostazione predefinita.



Note:

Le ricerche possono essere effettuate in un massimo di 16 telecamere alla volta.

Nel calendario, la data con le registrazioni pianificate verrà contrassegnata con e la data con le registrazioni degli eventi verrà contrassegnata con .

Riproduzione di file video

Dopo aver cercato i file video per la riproduzione normale, è possibile riprodurli in due modi:

Riproduzione in base all'elenco dei file

Selezionare il file video dall'elenco dei risultati di ricerca, quindi fare clic sull'icona sul file video oppure fare doppio clic sul file video per riprodurre il video nella finestra di visualizzazione della riproduzione.

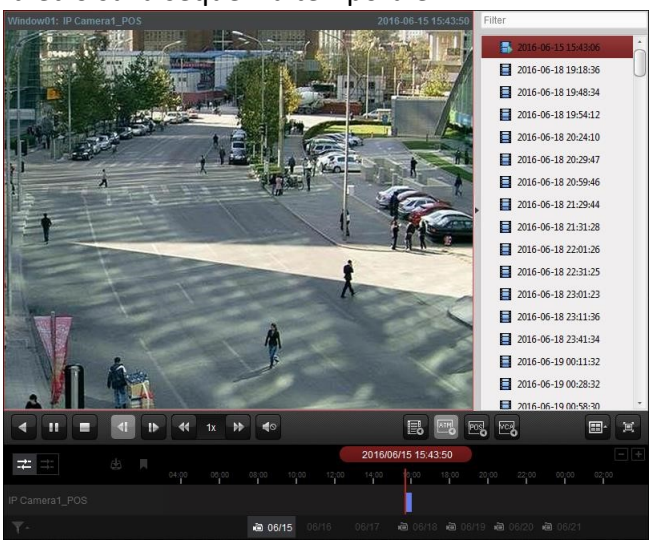
È inoltre possibile selezionare una finestra di visualizzazione e fare clic sull'icona nella barra degli strumenti per riprodurre il file video corrispondente.

Riproduzione in base alla sequenza temporale

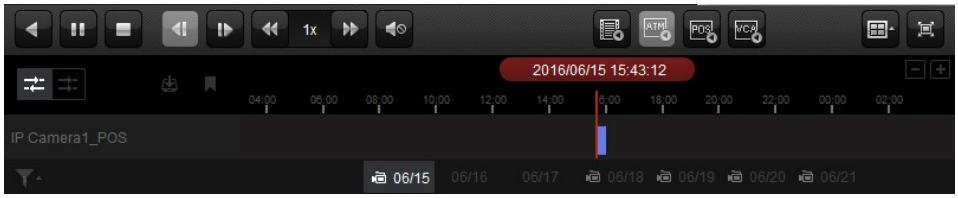
La sequenza temporale indica la durata del file video e i file video di diversi tipi vengono codificati da colori diversi. Fare clic sulla sequenza temporale per riprodurre il video dell'ora specifica.

È possibile fare clic su o su per aumentare o ridurre la barra della sequenza temporale.

È possibile anche trascinare la barra della sequenza temporale per spostarsi sul periodo precedente o successivo. Anche con la rotellina del mouse è possibile fare zoom avanti o indietro sulla sequenza temporale.



Barra degli strumenti della riproduzione normale:



I seguenti pulsanti sono disponibili sulla barra strumenti della pagina Normal Playback:

	Reverse Playback	Riproduce il file video in senso inverso.
	Pause/Start Playback	Mette in pausa/avvia la riproduzione dei file video.
	Stop Playback	Interrompe la riproduzione di tutte le telecamere.
	Single Frame (Reverse)	Riproduce i file video fotogramma per fotogramma all'inverso. Anche scorrendo verso il basso la rotellina del mouse, è possibile riprodurre il file video fotogramma per fotogramma all'inverso.

Riproduce i file video fotogramma per fotogramma. Anche scorrendo **Single Frame** verso il basso la rotellina del mouse, è possibile riprodurre il file video fotogramma per fotogramma.

Slow Forward/Fast Forward Diminuisce/aumenta la velocità di riproduzione.

Volume Fare clic per abilitare/disabilitare l'audio e regolare il livello del volume audio.

Effettua ricerche nelle registrazioni attivate da eventi, quali **Event Playback** rilevamento movimenti, perdita video o manomissione video.

ATM Playback Effettua ricerche nelle registrazioni dei dispositivi ATM.

POS Playback Effettua ricerche nelle registrazioni che contengono informazioni POS.

Imposta per i file video oggetto della ricerca la regola VCA che definisce l'evento VCA, **VCA Playback** tra cui ricerche VCA, intrusioni e attraversamento di linee.

Window Division Imposta la suddivisione della finestra.

Mostra la riproduzione video in modalità a schermo intero. Premere **ESC** per uscire. **Full Screen**

Async/Sync Fare clic per riprodurre i file video **Playback** in modo sincrono/asincrono.

Scarica i file video della telecamera che vengono **Download** memorizzati nel PC. È possibile scegliere di effettuare il download per file, data o tag.

Aggiunge il tag predefinito ai file video, per contrassegnare il punto importante del **Tag** video. Tramite il menu di scelta rapida, è possibile modificare il tag o spostarsi nella posizione del tag.

Permette di visualizzare i tipi di registrazione richiesti. Ad es., è possibile scegliere di visualizzare **Filter** solo la registrazione dell'evento.

2016/05/31 10:39:37 **Accurate Positioning** Definisce la posizione temporale esatta da cui avviare la riproduzione del file video.

09/13 09/14 **Date** I giorni che presentano file video saranno evidenziati con .

Facendo clic col tasto destro sulla finestra di visualizzazione della riproduzione, si apre il menu Playback Management:

Sul menu di scelta rapida Playback Management, sono disponibili le seguenti voci:

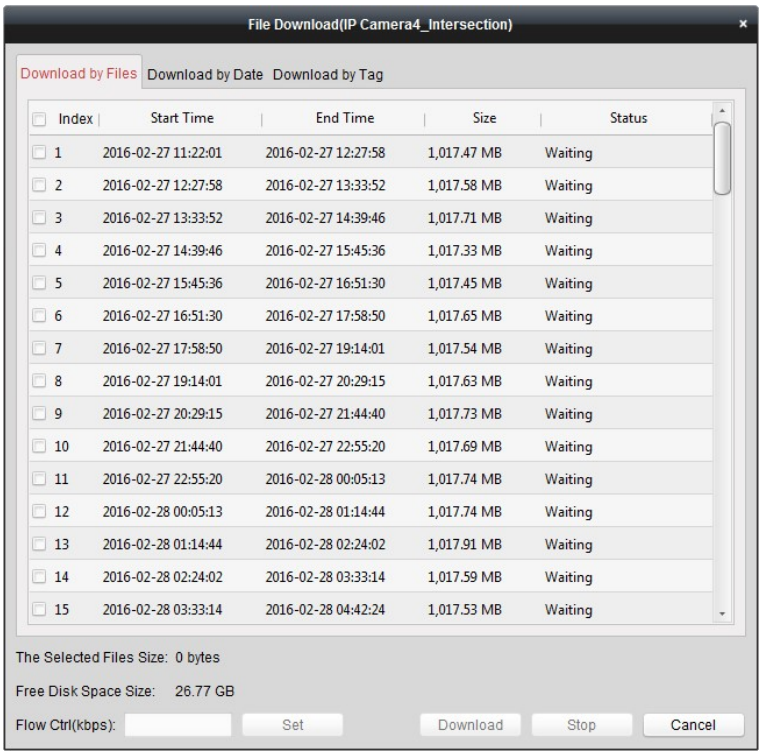
	**Reverse Playback**	Riproduce il file video in senso inverso.
	**Pause/Start**	Mette in pausa/avvia la riproduzione.
	**Stop**	Interrompe la riproduzione.
	**Fast Forward**	Riproduce il file video a velocità maggiore.
	**Slow Forward**	Riproduce il file video a una velocità minore.
	**Single Frame (Reverse)**	Riproduce i file video fotogramma per fotogramma (al contrario).
	**Open Digital Zoom**	Attiva la funzione di zoom digitale. Fare nuovamente clic per disattivare la funzione.
	Aggiunge il tag predefinito (nome tag predefinito *TAG*) o un tag personalizzato (con nome personalizzato **Tag Control**) al file video, per indicarne i punti più importanti. È possibile anche modificare il tag o spostarsi facilmente sulla posizione del tag.	
	**Accurate Positioning**	Definisce la posizione temporale esatta da cui avviare la riproduzione del file video.
	**Capture**	Acquisisce l'immagine durante la riproduzione.
	Print Captured Picture:	acquisisce un'immagine e la stampa.
	Send Email:	acquisisce l'immagine corrente e invia un'email di notifica a uno o più destinatari. L'immagine acquisita può.
	**Other Capture Modes**	essere allegata.
	Custom Capture:	acquisisce l'immagine corrente. Quindi è possibile modificarne il nome e salvarla.
	Avvia/interrompe la registrazione manuale. Il file video viene memorizzato nel **Start/Stop Recording** PC.	
	Scarica i file video della telecamera che vengono **Download** memorizzati nel PC. È possibile scegliere di effettuare il download per file o data.	
	**Enable/Disable Audio**	Fare clic per abilitare/disabilitare l'audio nella riproduzione.
	**Fisheye Expansion**	Entra in modalità di riproduzione fish-eye.
	Mostra la riproduzione in modalità a schermo intero. Fare di nuovo clic sull'icona o premere il tasto *Esc* per uscire dalla modalità.	**Full Screen**

Scaricamento di file video

Durante la riproduzione, è possibile fare clic su  nella barra degli strumenti per scaricare i file video dalla telecamera al PC locale. È possibile scegliere di effettuare il download per file, data o tag.

Download in base ai file *Passaggi:*

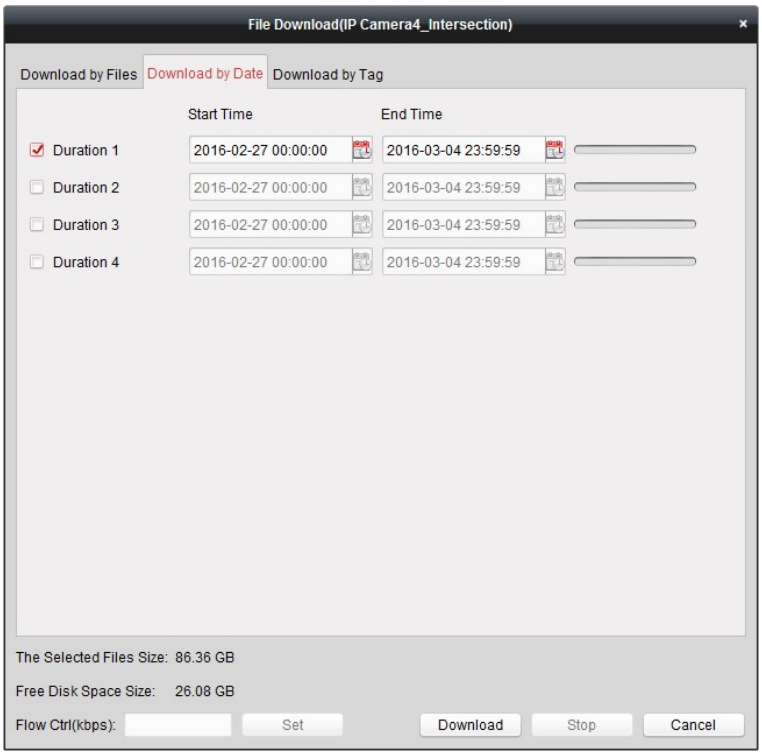
1. Fare clic sulla schermata **Download by Files** nell'interfaccia File Download. È possibile visualizzare le informazioni dei file video della telecamera selezionata.
2. Attivare le caselle di controllo per i file video da selezionare e la loro dimensione totale sarà indicata sotto.
3. Fare clic su **Download** per iniziare a scaricare il file nel PC locale.
   È possibile indicare la velocità di flusso (da 0 a 32768 kbps) e fare clic su **Set** per controllare la velocità di download.
4. Facendo clic su **Stop**, è possibile anche interrompere il download manualmente.



Download in base alla data

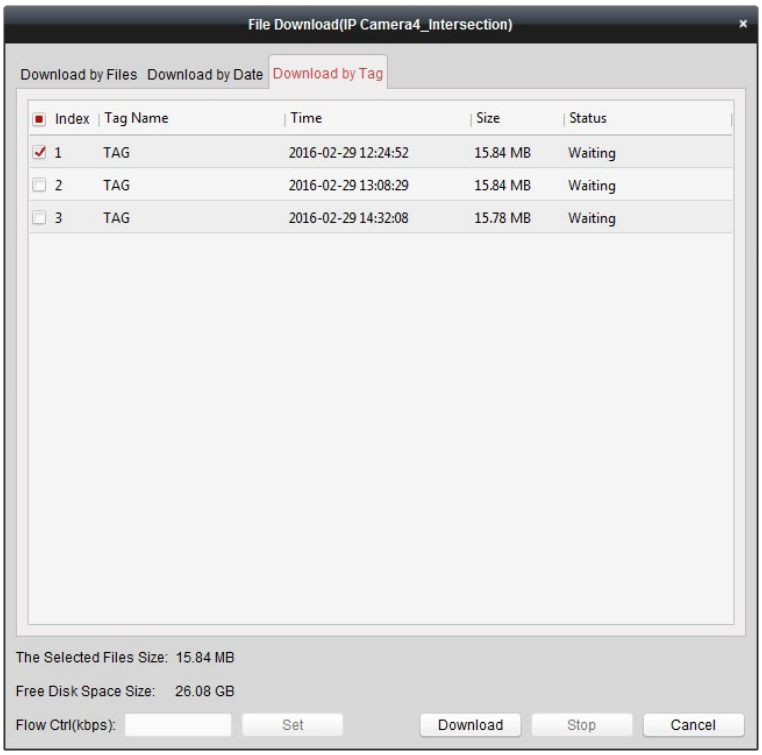
Passaggi:

1. Fare clic sulla schermata **Download by Date** nell'interfaccia File Download.
2. Attivare la casella di controllo della durata per abilitare la funzione, quindi fare clic su per impostare l'ora di inizio e fine.
3. Fare clic su **Download** per iniziare a scaricare il file nel PC locale. La barra dei processi mostra l'avanzamento del processo di download.
   È possibile indicare la velocità di flusso (da 0 a 32768 kbps) e fare clic su **Set** per controllare la velocità di download.
4. Facendo clic su **Stop**, è possibile anche interrompere il download manualmente.



Nota: durante il download di file video relativi allo stesso periodo, è possibile impostare l'opzione di unione dei file video. I file video definiti nello stesso periodo possono essere uniti per il download. Per configurare l'unione dei file video scaricati, consultare la sezione *8.2 Impostazioni della visualizzazione dal vivo e della riproduzione*. **Download in base ai tag *Passaggi:***

1. Fare clic sulla schermata **Download by Tag** nell'interfaccia File Download. Saranno visualizzati i tag aggiunti.
2. Attivare le caselle di controllo relative ai tag dei file selezionati la loro dimensione totale sarà indicata sotto.
3. Fare clic su **Download** per iniziare a scaricare i file selezionati (da 30 secondi prima a 30 secondi dopo il tag selezionato) sul PC locale. È possibile indicare la velocità di flusso (da 0 a 32768 kbps) e fare clic su **Set** per controllare la velocità di download.
4. Facendo clic su **Stop**, è possibile anche interrompere il download manualmente.



7.16.3 Riproduzione di eventi

Scopo:

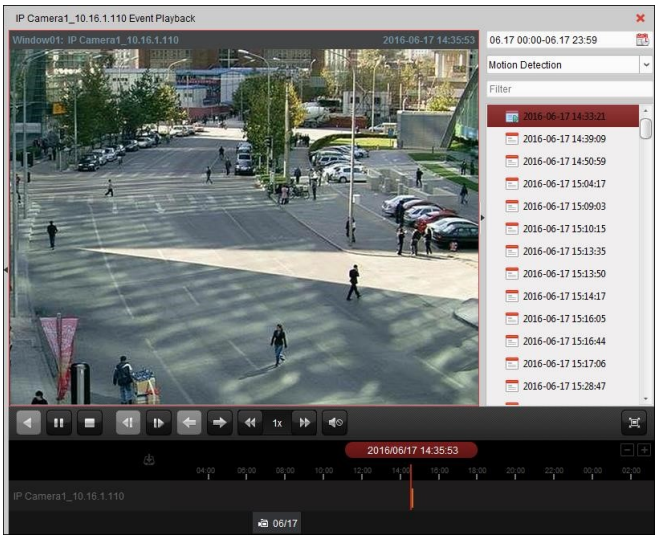
Le registrazioni attivate da eventi, quali rilevamento di movimenti, rilevamenti VCA o analisi del comportamento, possono essere oggetto di ricerca per Event Playback, ma questa funzione deve essere supportata dal dispositivo collegato.

Ricerca di file video per la riproduzione di eventi

Passaggi:

1. Aprire la pagina Remote Playback.
2. Selezionare la telecamera e avviare la riproduzione normale. Consultare il *Capitolo 8.5.2 Riproduzione normale*.
3. Facendo clic su , le registrazioni attivate dal rilevamento movimenti saranno oggetto di ricerca per impostazione predefinita.
4. Fare clic sull'icona calendari per attivare la corrispondente finestra di dialogo.
   Selezionare la data di inizio e fine del periodo, quindi impostare l'ora esatta.
   Fare clic su **OK** per salvare il periodo di ricerca.
   Nota: nel calendario, la data con le registrazioni pianificate verrà contrassegnata con e la data con le registrazioni degli eventi verrà contrassegnata con .
5. Selezionare il tipo di evento dall'elenco a discesa per visualizzare i file video trovati. È possibile filtrare i risultati immettendo la parola chiave nel campo di testo **Filter**. In alternativa, è possibile fare clic su per tornare alla riproduzione normale.

6. Selezionare il file video dall'elenco dei risultati di ricerca, quindi fare clic sull'icona sul file video oppure fare doppio clic sul file video per riprodurre il video nella relativa finestra di visualizzazione della riproduzione.



Riproduzione di file video

Dopo aver cercato le registrazioni attivate dagli eventi, è possibile riprodurre i file video nei due modi seguenti:

Riproduzione in base all'elenco dei file

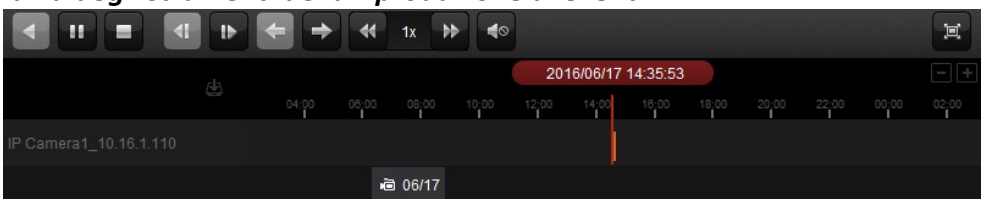
Selezionare il file video dall'elenco dei risultati di ricerca, quindi fare clic sull'icona nella barra degli strumenti oppure fare clic sull'icona sul file video; in alternativa, fare doppio clic sul file video per riprodurre il video nella relativa finestra di visualizzazione della riproduzione.

Riproduzione in base alla sequenza temporale

La sequenza temporale indica la durata del file video. Fare clic sulla sequenza temporale per riprodurre il video dell'ora specifica.

È possibile fare clic su o su per aumentare o ridurre la barra della sequenza temporale.

È possibile anche trascinare la barra della sequenza temporale per spostarsi sul periodo precedente o successivo. Anche con la rotellina del mouse è possibile fare zoom avanti o indietro sulla sequenza temporale. ***Barra degli strumenti della riproduzione di eventi:***



I seguenti pulsanti sono disponibili sulla barra strumenti della pagina Remote Playback:

	Reverse Playback	Riproduce il file video in senso inverso.
	Pause/Start Playback	Mette in pausa/avvia la riproduzione dei file video.
	Stop Playback	Interrompe la riproduzione di tutte le telecamere.
	Single Frame (Reverse)	Riproduce i file video fotogramma per fotogramma (al contrario).
	Single Frame	Riproduce i file video fotogramma per fotogramma.
	Previous Event	Va alla riproduzione dell'evento precedente.
	Next Event	Va alla riproduzione dell'evento successivo.
	Slow Forward/Fast Forward	Diminuisce/aumenta la velocità di riproduzione.
		Fare clic per abilitare/disabilitare l'audio e per regolare il livello del volume **Volume** audio.
	Mostra la riproduzione video in modalità a schermo intero. Premere **Full Screen ESC** per uscire.	
	Scarica i file video della telecamera che vengono **Download** memorizzati nel PC.	
2016/05/31 10:39:37	**Accurate Positioning**	Definisce la posizione temporale esatta da cui avviare la riproduzione del file video.
09/13 09/14	**Date**	I giorni che presentano file video saranno evidenziati con .

Consultare il *Capitolo 7.16.2 Riproduzione normale* per la descrizione del menu di scelta rapida. Alcune icone potrebbero non essere disponibili per la riproduzione di eventi.

Nota: è possibile definire la durata di riproduzione pre-evento nella pagina System Configuration. Per impostazione predefinita, è 30 secondi. Per configurare il tempo di riproduzione pre-evento, consultare *Impostazioni della visualizzazione dal vivo e della riproduzione* nel *Capitolo 7.16.3 Riproduzione di eventi*.

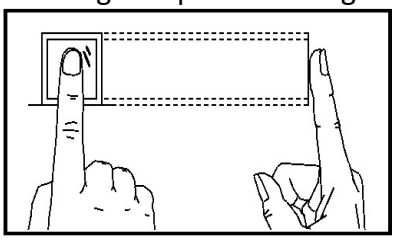
Appendice A Suggerimenti per la scansione delle impronte digitali

Dita consigliate

Indice, medio o anulare.

Scansione corretta

L'immagine riportata di seguito mostra il modo corretto per scansionare il dito:

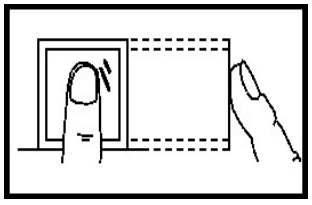


Premere il dito orizzontalmente sullo scanner. Il centro del dito scansionato deve essere allineato con il centro dello scanner.

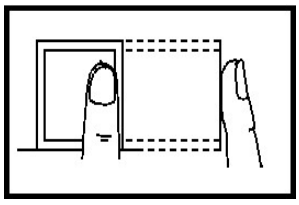
Scansione errata

Le immagini qui sotto mostrano le posizioni errate del dito durante la scansione:

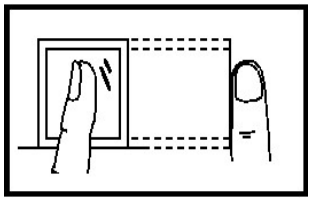
Vertica le



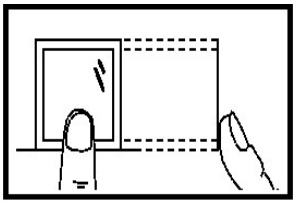
Bordo I



Lato



Bordo II



Ambiente

Non collocare lo scanner alla luce diretta del sole, non sottoporlo a temperature elevate, umidità e pioggia.

In caso di clima secco, lo scanner potrebbe non riconoscere correttamente l'impronta digitale. È possibile soffiare sul dito e ripetere la scansione dopo averlo asciugato.

Altro

Se i solchi dell'impronta sono poco profondi o si incontrano difficoltà durante la scansione, consigliamo di utilizzare altri metodi di autenticazione.

In caso di ferite al dito scansionato, lo scanner potrebbe non riconoscere l'impronta. È possibile cambiare dito e riprovare.

Appendice B Introduzione al DIP switch

Lo schema del DIP switch è il seguente:

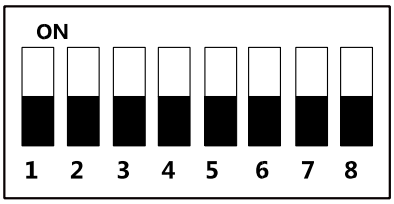


Tabella 7-2 Descrizione del DIP switch

Icona	Descrizione
	Rappresenta 1 in modalità binaria
	Rappresenta 0 in modalità binaria

Ad esempio, il valore binario dello stato seguente è: 0000 1100.

Tabella 7-3 Descrizione del DIP switch

N.	Descrizione	Stato del DIP Switch
1 ~ 4	Indirizzo RS-485	2: modulo Security 0: lettore di tessere
5	Direzione RS-485 in Terminal Mode	1: a monte; 0: a valle
6	Metodo di lavoro	1: lettore di tessere; 0: terminale.
7	Protocollo Wiegand (disponibile quando n. 6 è 1)	1: protocollo Wiegand di 26 bit; 0: protocollo Wiegand di 34 bit.
8	Resistenza allocata (disponibile per il protocollo RS-485)	1: attivato; 0: disattivato.

Appendice C Descrizione dell'indicatore e dell'avvisatore acustico

L'avvisatore acustico si attiva dopo 10 secondi ed emette un segnale acustico una volta. Quando il dispositivo è acceso, l'avvisatore acustico emette un altro segnale acustico (una volta). L'indicatore rimane rosso durante questa fase. Le descrizioni dell'avvisatore acustico sono le seguenti:

Tipo	Descrizione
Un segnale acustico	Passaggio della tessera
	Pressione del pulsante
	Dopo il passaggio della tessera e prima della scansione dell'impronta digitale in caso di autenticazioni multiple
Segnale acustico veloce due volte	Passaggio della tessera valido
Segnale acustico lento per tre volte	Passaggio della tessera non valido
Segnale acustico rapido e continuo	Allarme anti-manomissione
	Allarme dell'avvisatore acustico
Segnale acustico lento e continuo	Lettore di tessera non crittografato

Le descrizioni dell'indicatore del lettore di tessere sono le seguenti:

Indicatore	Descrizione
Verde lampeggiante una volta e rosso lampeggiante per 3 volte	Accensione
Verde lampeggiante continuo	Dopo il passaggio della tessera e prima della scansione dell'impronta digitale in caso di autenticazioni multiple
Verde fisso per 3 secondi	Autenticazione dell'impronta digitale completata dopo il passaggio della tessera in caso di autenticazioni con passaggio della tessera/multiple
Rosso fisso	Funzionamento corretto
Rosso lampeggiante per 3 volte	Passaggio della tessera non valido
Rosso lampeggiante continuo	Modalità lettore di tessere offline ed errore di registrazione

0200001090312


See Far, Go Further