CONTROLLER DI ACCESSO A DUE PORTE

Guida Rapida

Hiltron Land S.r.l.
Strada Provinciale di Caserta, 218 - 80144 - Napoli
t: +39 081 185 39 000
www.hiltronsecurity.net

V1.0.1

Raccomandazioni sulla sicurezza informatica

Azioni obbligatorie da intraprendere per la sicurezza informatica

1. Utilizzare password sicure e modificarle:

Il motivo principale per cui i sistemi vengono violati dagli hacker sono l'utilizzo di password non sicure e la mancata modifica delle password predefinite. Per questo, è opportuno cambiare immediatamente le password predefinite del sistema e sostituirle con password complesse. Una password sicura deve essere composta da un minimo di 8 caratteri e contenere una combinazione di caratteri speciali, numeri e lettere maiuscole e minuscole.

2. Aggiornare il firmware

Per assicurare che il sistema sia sempre protetto dalle patch e dagli aggiornamenti di sicurezza più recenti, consigliamo di mantenere aggiornati i firmware dei videoregistratori di rete (NVR), dei videoregistratori digitali (DVR) e delle telecamere IP, come previsto dagli standard del settore tecnologico.

Raccomandazioni facoltative ma consigliate per migliorare la sicurezza di rete

1. Modificare le password con regolarità

Modifica con regolarità le credenziali dei tuoi dispositivi per garantire che solamente gli utenti autorizzati possano accedere al sistema.

2. Modificare le porte HTTP e TCP predefinite:

- Modificare le porte HTTP e TCP predefinite del sistema. Queste porte vengono utilizzate per comunicare e visualizzare i video da remoto.
- Il numero di queste porte può essere modificato, scegliendo un valore compreso tra 1025 e 65535. Evitare l'utilizzo dei numeri di porta predefiniti riduce il rischio che persone esterne possano scoprire quali porte utilizzi.

3. Attivare i protocolli HTTPS/SSL:

Imposta un certificato SSL per attivare il protocollo HTTPS. In questo modo, tutte le comunicazioni fra dispositivi e con il videoregistratore verranno criptate.

4. Attivare il filtro IP:

L'attivazione del filtro IP consentirà l'accesso al sistema solamente dagli indirizzi IP specificati.

5. Modificare la password ONVIF:

Sui firmware meno recenti delle telecamere IP, la password ONVIF rimane invariata quando modifichi le credenziali del sistema. In questi casi, dovrai aggiornare il firmware della telecamera alla versione più recente o modificare la password ONVIF.

6. Inoltrare solamente le porte necessarie:

- Inoltra soltanto le porte HTTP e TCP che devi utilizzare. Non inoltrare lunghi intervalli di numeri di porte. Non inserire l'indirizzo IP del dispositivo nella DMZ.
- Non è necessario inoltrare le porte delle singole telecamere se sono tutte connesse a un videoregistratore on site, è sufficiente inoltrare quella del videoregistratore di rete.

7. Disattivare il login automatico su SmartPSS:

Chi utilizza SmartPSS o un computer condiviso con altri utenti per visualizzare il proprio sistema deve disabilitare il login automatico. Questo aggiunge un livello di sicurezza in più, evitando che gli utenti privi di credenziali adeguate possano accedere al sistema.

8. Utilizzare nome utente e password diversi per SmartPSS:

Qualora uno dei tuoi account (di un social network, per l'accesso ai servizi bancari online, per la posta elettronica ecc.) sia stato compromesso, è bene che nessuno sia in grado di utilizzare la password per provare ad accedere al sistema di videosorveglianza. Utilizzare un nome utente e una password diversi per il sistema di videosorveglianza renderà più difficile l'accesso a utenti non autorizzati.

9. Limitare le funzionalità degli account guest:

Se hai impostato il tuo sistema in modo da poter essere utilizzato da più utenti, accertati che ogni utente abbia i privilegi per utilizzare solamente le funzioni strettamente necessarie allo svolgimento delle proprie mansioni.

10. UPnP:

- Il protocollo UPnP proverà a inoltrare automaticamente le porte del tuo router o del tuo modem. Normalmente questa è una buona cosa. Tuttavia, se il tuo sistema inoltra automaticamente le porte e tu hai lasciato le credenziali predefinite, potrebbero verificarsi accessi da parte di visitatori indesiderati.
- Se hai inoltrato manualmente le porte HTTP e TCP del tuo router/modem, questa funzione dovrebbe essere disattiva. È consigliabile disattivare l'UPnP quando non viene utilizzato.

11. SNMP:

Disattiva il protocollo SNMP se non lo utilizzi. Se invece lo utilizzi, è consigliabile che tu lo faccia solo temporaneamente, per condurre dei test o per motivi di localizzazione.

12. Multicast:

La funzione Multicast viene utilizzata per condividere streaming video fra due videoregistratori. Al momento non risultano problemi legati alla funzione Multicast, ma, se non la utilizzi, disattivarla può migliorare la sicurezza della tua rete.

13. Verificare il log:

Se sospetti che qualcuno sia in grado di accedere al tuo sistema senza autorizzazione, puoi controllare il log di sistema, dove potrai verificare quali indirizzi IP sono stati utilizzati per accedere e le attività svolte durante l'accesso.

14. Bloccare fisicamente il dispositivo:

In condizioni ideali, non dovrebbe essere possibile accedere fisicamente al sistema. Il modo migliore per ottenere questo risultato è installare il videoregistratore in un contenitore o in un armadio rack per server dotati di combinazione o in una stanza chiusa a chiave.

15. Collegare le telecamere IP alle porte PoE sul retro di un videoregistratore di rete:

Le telecamere collegate alle porte PoE sul retro di un videoregistratore di rete sono isolate rispetto all'esterno e non è possibile accedervi direttamente.

16. Isolare la rete del videoregistratore e delle telecamere IP

La rete a cui appartengono il videoregistratore e le telecamere IP dovrebbe essere diversa dalla rete pubblica del tuo computer. Questo impedirà agli utenti indesiderati di accedere alla rete utilizzata dal sistema di sicurezza per funzionare in modo corretto.

INTRODUZIONE

Generale

Il presente documento illustra la struttura, l'installazione, l'interfaccia e il cablaggio del controller di accesso a due porte.

Istruzioni di sicurezza

All'interno del manuale possono comparire i seguenti indicatori di pericolo, il cui significato è definito qui sotto.

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

Informativa sulla protezione della privacy

Gli utenti del dispositivo o gli analisti dei dati hanno la possibilità di raccogliere dati personali di terzi, quali volti, impronte digitali, numeri di targhe automobilistiche, indirizzi e-mail, numeri di telefono, dati GPS e simili. L'utente deve comportarsi in conformità con le locali norme e leggi sulla protezione della privacy per garantire il rispetto dei diritti e degli interessi legittimi di terzi, adottando misure adeguate, quali, tra le altre, la fornitura di indicazioni chiare e visibili che permettano ai titolari dei dati di individuare l'esistenza di aree di sorveglianza e i relativi contatti.

Indicazioni sul manuale

- Questo manuale serve solo come riferimento. In caso di discrepanza fra il manuale e il prodotto, quest'ultimo prevarrà.
- Non ci riteniamo responsabili per eventuali perdite causate da un utilizzo non conforme a quanto esposto nel manuale.

- Il manuale deve essere aggiornato sulla base delle più recenti leggi e normative in vigore nelle regioni interessate. Per ulteriori informazioni, consultare il manuale d'uso in formato cartaceo, il CD-ROM, il codice QR o il nostro sito web ufficiale. In caso di discordanza tra il formato cartaceo ed elettronico del manuale d'uso, prevalgono le informazioni della versione elettronica.
- Grafiche e software sono soggetti a modifica senza preavviso. Gli aggiornamenti del prodotto possono generare delle differenze tra il prodotto effettivo e le informazioni contenute nel manuale. Contattare il servizio di assistenza per le procedure più recenti e la documentazione supplementare.
- Potrebbero inoltre esserci delle differenze nei dati tecnici, nelle descrizioni di funzioni e operazioni, o errori di stampa. In caso di incoerenze o incertezze, fare riferimento alla nostra spiegazione finale.
- In caso non sia possibile aprire la guida (in formato PDF), aggiornare il proprio lettore software o provare un altro lettore software equivalente.
- Tutti i marchi commerciali, i marchi registrati e i nomi di società presenti nel manuale sono di proprietà dei rispettivi titolari.
- In caso di problemi durante l'utilizzo del dispositivo, è possibile consultare il nostro sito web o contattare il fornitore o il servizio di assistenza al cliente.
- In caso di incertezze o controversie, fare riferimento alla spiegazione finale.

NORME DI SICUREZZA E AVVERTENZE IMPORTANTI

Quanto segue indica il metodo di applicazione corretto del dispositivo. Leggere attentamente il manuale prima dell'uso, per evitare pericoli e danni alle proprietà. Attenersi strettamente al manuale durante l'applicazione e conservarlo dopo la lettura.

Attenzione

- Dopo l'installazione, modificare immediatamente la password predefinita, per evitare che venga violata.
- Non posizionare e installare il dispositivo in una zona esposta a luce solare diretta o vicino a fonti di calore.
- Non installare il dispositivo in zone umide o polverose.
- Mantenere il dispositivo in orizzontale e installarlo in luoghi stabili per evitare che cada.
- Non versare o schizzare liquidi sul dispositivo né appoggiarvi sopra contenitori pieni di liquidi per evitare che questi possano rovesciarsi.
- Installare il dispositivo in luoghi ben aerati; non bloccarne le fessure di ventilazione.
- Utilizzare il dispositivo solo entro gli intervalli di ingresso e uscita nominali.
- Non smontare il dispositivo.
- Trasportare, utilizzare e conservare il dispositivo entro l'intervallo di umidità e temperatura consentito.

Avvertenza

- Assicurarsi di utilizzare le batterie secondo le istruzioni; in caso contrario, potrebbero verificarsi incendi, esplosioni o rischio di combustione delle batterie!
- Sostituire le batterie solo con modelli dello stesso tipo.
- Utilizzare cavi elettrici (cavi di alimentazione) previsti per questo Paese e prestare attenzione alle specifiche nominali in vigore.
- Utilizzare corrente elettrica che soddisfi i requisiti SELV (tensione di sicurezza molto bassa), con tensione nominale conforme ai requisiti delle fonti di alimentazione a potenza limitata, come previsto dalla norma IEC60950-1. Per i requisiti specifici di alimentazione, fare riferimento alle etichette del dispositivo.
- I prodotti con strutture di categoria I devono essere collegati a una presa elettrica equipaggiata con messa a terra di sicurezza.

- Questo dispositivo utilizza un accoppiatore come dispositivo di spegnimento. Durante il normale utilizzo, mantenere un angolo che faciliti il funzionamento.

Note

- Questo manuale ha scopo di solo riferimento. Fare riferimento al prodotto reale per maggiori dettagli.
- Questo manuale e il programma saranno regolarmente aggiornati in base alle modifiche apportate al prodotto. I contenuti aggiornati saranno inclusi nella nuova versione del manuale senza preavviso.
- L'utente è responsabile di eventuali perdite derivanti dalla non osservanza delle indicazioni contenute nel manuale.
- Il manuale può contenere contenuti tecnicamente imprecisi, incongruenze con le funzioni e le operazioni del prodotto o errori di stampa. Prevalgono le indicazioni finali dell'azienda.

INDICE

PANORAMICA

Il controller di accesso a due porte è un dispositivo di controllo che integra il monitoraggio video e il videocitofono. Ha un design semplice e moderno con solide funzionalità, adatto per l'edilizia commerciale, gli edifici aziendali e le comunità intelligenti.

Il suo ricco portafoglio di funzioni comprende:

- Adozione di un tipo di guida a scorrimento e di montaggio a serratura, installazione e manutenzione convenienti.
- Integrazione di allarme, controllo accessi, monitoraggio video, allarme antincendio e modulo di controllo in ingresso.
- Supporto di 4 set di lettori di schede (possibilità di impostarne 2 come lettori di schede bidirezionali).
- Supporto di 9 gruppi di segnale di ingresso (2 pulsanti di sblocco, 2 sensori porta, 1 allarme antivandalo, 4 allarmi antintrusione).
- Supporto di 6 gruppi di controllo in uscita (2 serrature elettriche, 2 uscite di allarme, 2 controlli dispositivo).
- Porta RS485, che consente l'estensione per collegare il modulo di controllo dell'ascensore, l'allarme o il modulo di controllo domestico.
- Capacità di memoria FLASH di 16 M (espandibile fino a 32 M), supporta un massimo di 100.000 titolari di schede e 150.000 record.
- Supporto allarme intrusione, allarme di sblocco oltre il tempo limite, allarme scheda di coercizione e configurazione del codice di coercizione. Supporto impostazione della lista bianca/nera e della scheda di perlustrazione.
- Supporto per la configurazione del periodo di validità della scheda, della password e della validità. Configurazione dei tempi di utilizzo della scheda ospite.
- Supporto per 128 gruppi di calendari, 128 gruppi di periodi e 128 gruppi di giorni festivi.
- Memorizzazione dei dati durante i blackout, RTC integrato (supporto DST), aggiornamento online.

ASPETTO E DIMENSIONI

L'aspetto e le dimensioni del controller di accesso a due porte sono illustrati nella Figura 2–1 e nella Figura 2–2. L'unità di misura è il mm.

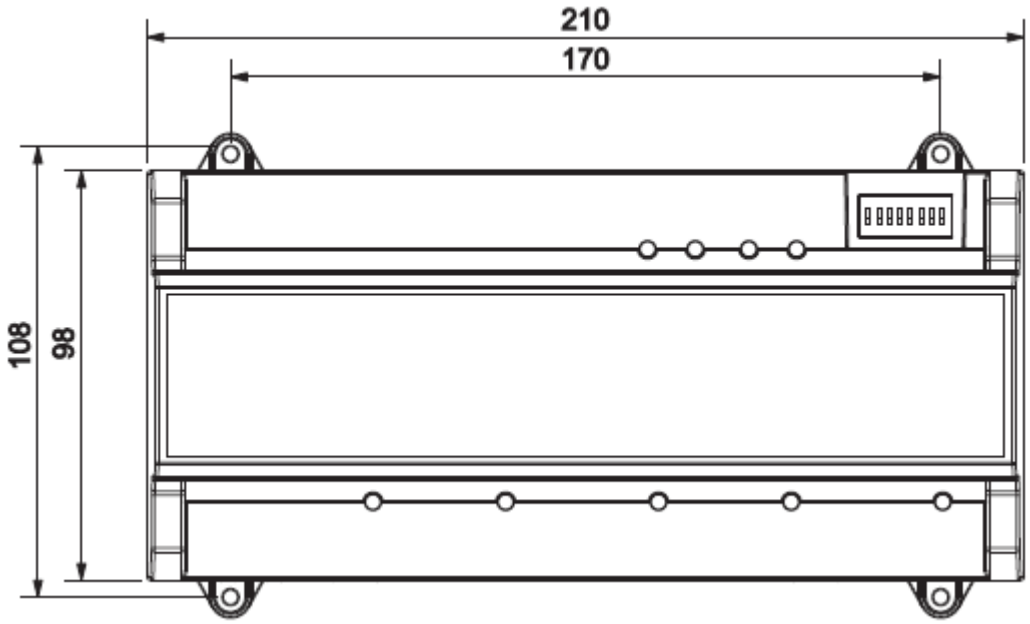

Figura 2–1

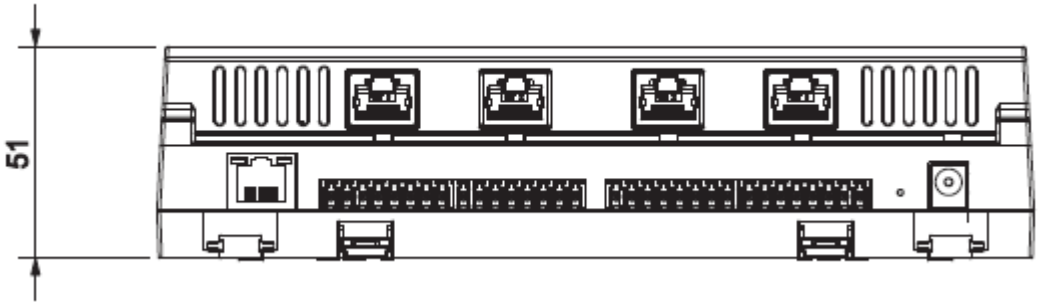

Figura 2–2

3.1 Montaggio

Sono possibili due tipi di montaggio:

- Montaggio 1: fissaggio dell'intero dispositivo alla parete con l'impiego di viti.
- Montaggio 2: fissaggio dell'intero dispositivo alla parete con una staffa.

Montaggio 1: fissare il dispositivo alla parete con le viti, come mostrato nella Figura 3–1.

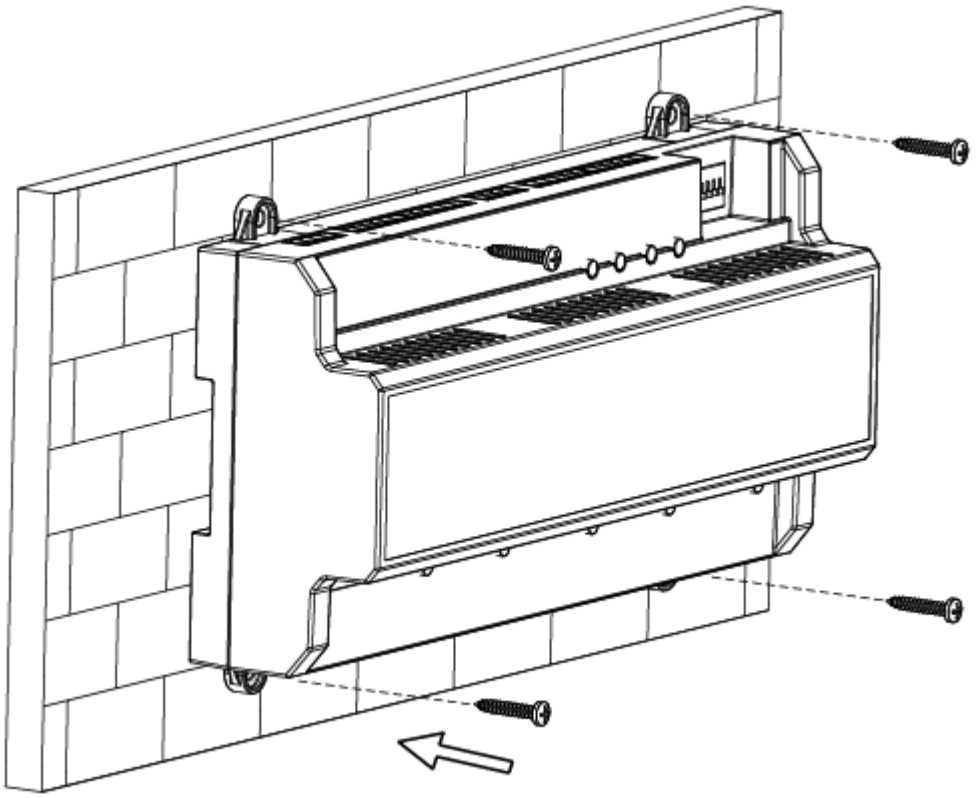

Figura 3–1

Il montaggio 2 è illustrato nella Figura 3–2.

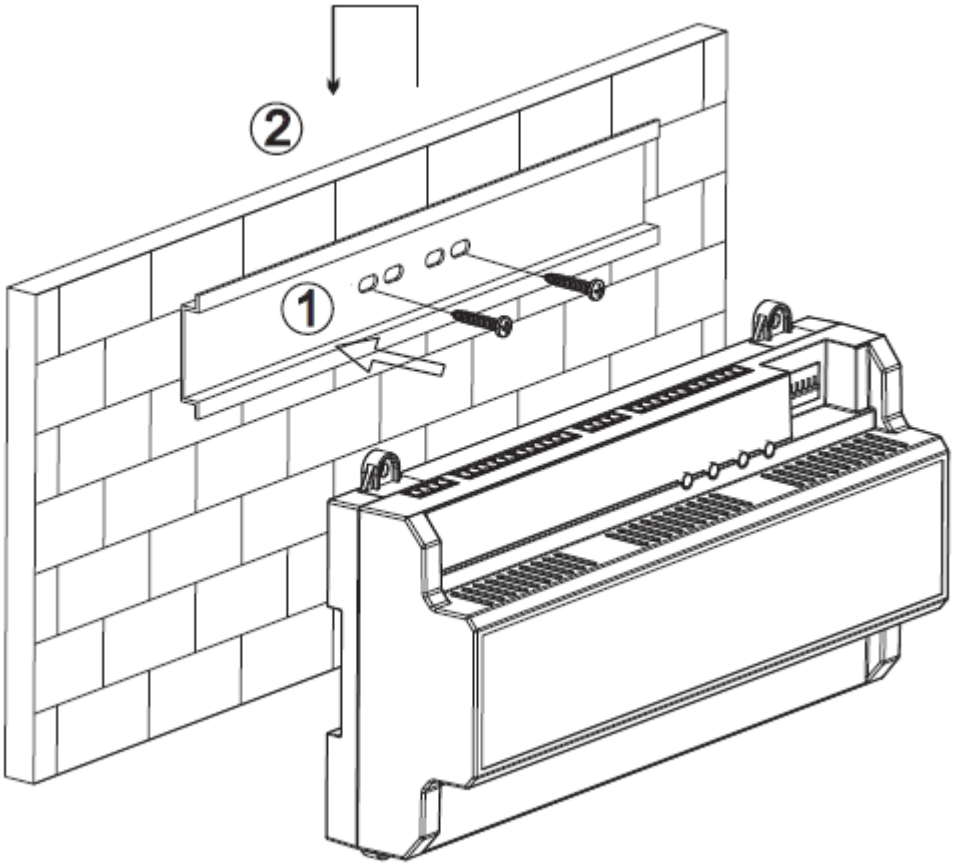

Figura 3–2

Seguire queste istruzioni per il montaggio 2:

Fase 1: Fissare la staffa alla parete con due viti.

Fase 2: Posizionare la parte superiore del lato posteriore del dispositivo nella scanalatura superiore della staffa, quindi premere la parte inferiore del dispositivo sulla staffa.

Fase 3: L'installazione è completata quando si sente che il giunto a scatto sul lato posteriore del dispositivo si inserisce in posizione.

3.2 Smontaggio

Seguire queste istruzioni per smontare un dispositivo montato con il metodo 2:

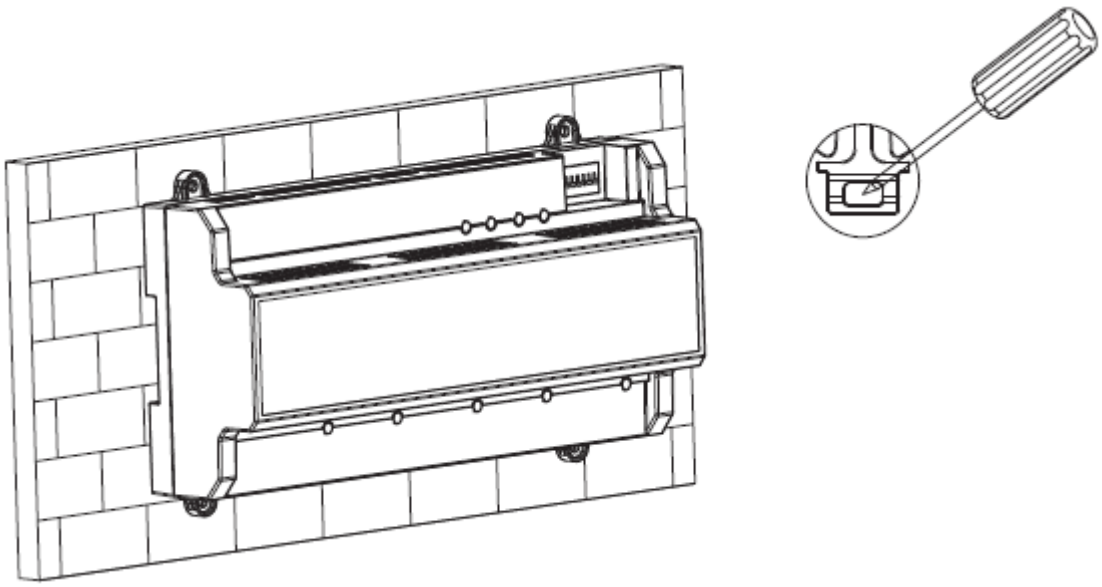

Figura 3–3

Passaggi per lo smontaggio:

Fase 1: Posizionare un cacciavite sul giunto a scatto e premerlo con forza verso il basso. Il giunto a scatto si aprirà.

Fase 2: Aprire il secondo giunto a scatto nello stesso modo, così da poter rimuovere l'intero dispositivo.

4.1 Schema dell'interfaccia

Lo schema dell'interfaccia è illustrato nella Figura 4–1.

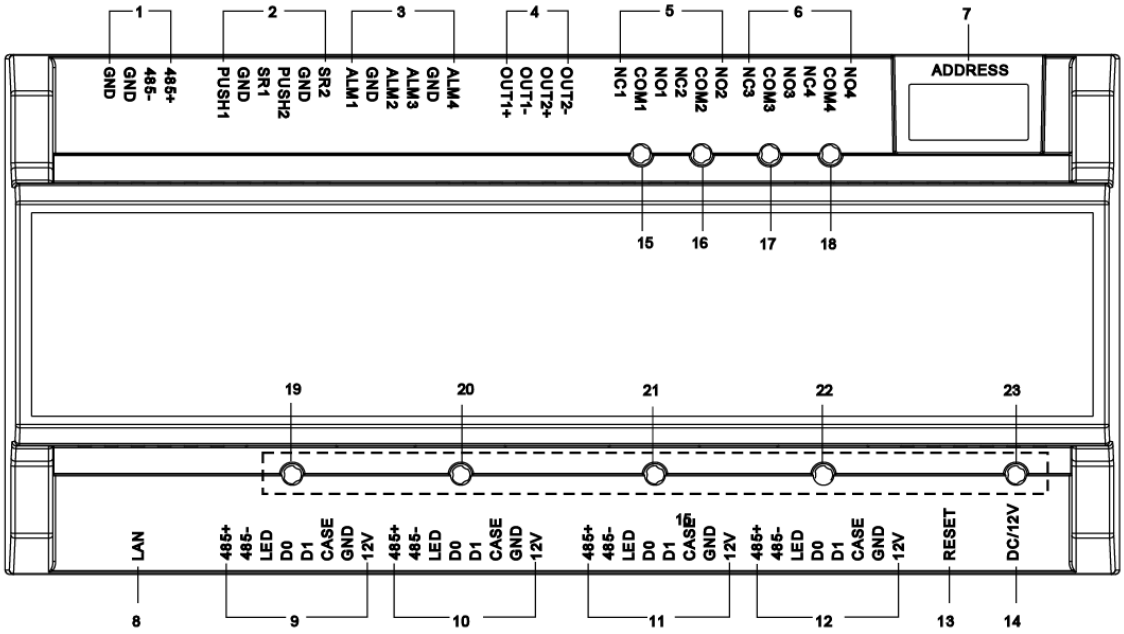

Figura 4–1

La descrizione dell'interfaccia è illustrata nella Tabella 4-1.

N.	Descrizione dell'interfaccia	N.	Descrizione dell'interfaccia
1	Porta di comunicazione RS485	8	TCP/IP, interfaccia piattaforma software
2	Pulsante di sblocca + sensore porta	9	Lettore ingresso n. 1
3	Ingresso allarme con segnale a 4 canali	10	Lettore uscita n. 1
4	Uscita controllo a 2 canali	11	Lettore ingresso n. 2
5	Uscita controllo serratura	12	Lettore uscita n. 2
6	Uscita controllo allarme	13	Interruttore di reset
7	Interruttore a levetta	14	Interfaccia di alimentazione 12 V CC

Tabella 4-1

Le spia luminose sono descritte nella Tabella 4-2.

N.	Descrizione
15	Spia luminosa stato serratura
16	

N.	Descrizione
17	Spia luminosa stato di inserimento
18	
19	Spia luminosa rilevamento lettore ingresso n. 1
20	Spia luminosa rilevamento lettore uscita n. 1
21	Spia luminosa rilevamento lettore ingresso n. 2
22	Spia luminosa rilevamento lettore uscita n. 2
23	Indicatore luminoso alimentazione

Tabella 4-2

Nota: la spia di indicazione dello stato del lettore non è disponibile in alcune versioni.

4.2 Descrizione del cablaggio

I terminali di cablaggio n. 1-7 sono illustrati nella Figura 4–2.

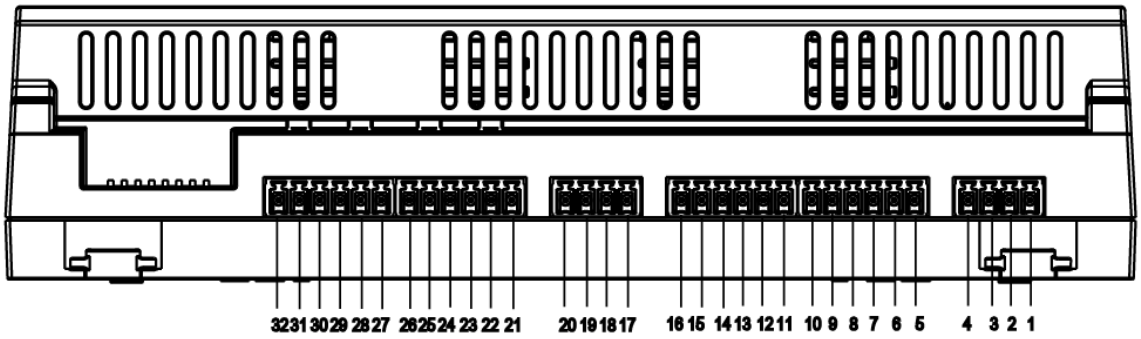

Figura 4–2

I terminali di cablaggio per la comunicazione RS485 sono illustrati nella Tabella 4-3.

Interfaccia	N.	Terminale di cablaggio
Comunicazione 485	1	GND
	2	GND
	3	485-
	4	485+

Tabella 4-3

I terminali di cablaggio per sblocco + sensore porta sono illustrati nella Tabella 4-4.

Interfaccia	N.	Terminale di cablaggio	Descrizione
Sblocco + sensore porta	5	PUSH1	Pulsante uscita n. 1
	6	GND	Condiviso dal pulsante uscita n. 1 e dall'ingresso sensore porta n. 1
	7	SR1	Ingresso sensore porta n. 1
	8	PUSH2	Pulsante uscita n. 2
	9	GND	Condiviso dal pulsante uscita n. 2 e dall'ingresso sensore porta n. 2
	10	SR2	Ingresso sensore porta n. 2

Tabella 4-4

I terminali di cablaggio per l'ingresso allarme con segnale a 4 canali sono illustrati nella Tabella 4-5.

Interfaccia	N.	Terminale di cablaggio	Descrizione
Ingresso allarme con segnale a 4 canali	11	ALM1	Può essere collegato al rilevatore fumo, all'allarme acustico e visivo, ecc.
	12	GND	-
	13	ALM2	-
	14	ALM3	-
	15	GND	-
	16	ALM4	-

Tabella 4-5

I terminali di cablaggio per l'uscita di controllo sono illustrati nella Tabella 4-6.

Interfaccia	N.	Terminale di cablaggio	Descrizione
Uscita controllo	17	OUT1+	Uscita segnale contatto pulito n. 1
	18	OUT1-	
	19	OUT2+	Uscita segnale contatto pulito n. 2
	20	OUT2-	

Tabella 4-6

I terminali di cablaggio per l'uscita di controllo serratura sono illustrati nella Tabella 4-7.

Interfaccia	N.	Terminale di cablaggio	Descrizione
Uscita controllo serratura	21	NC1	Sblocco spegnimento n. 1
	22	COM1	Ingresso alimentazione 12 V serratura n. 1
	23	NO1	Blocco spegnimento n. 1
	24	NC2	Sblocco spegnimento n. 2
	25	COM2	Ingresso alimentazione 12 V serratura n. 2
	26	NO2	Blocco spegnimento n. 2

Tabella 4-7

I terminali di cablaggio per l'uscita di controllo allarme sono illustrati nella Tabella 4-8.

Interfaccia	N.	Terminale di cablaggio	Descrizione
Uscita controllo allarme	27	NC3	Allarme sblocco spegnimento n. 1
	28	COM3	Ingresso alimentazione 12 V allarme porta n. 1
	29	NO3	Allarme blocco spegnimento n. 1
Uscita controllo allarme	30	NC4	Allarme sblocco spegnimento n. 2
	31	COM4	Ingresso alimentazione 12 V allarme porta n. 2
	32	NO4	Allarme blocco spegnimento n. 2

Tabella 4-8

I terminali di cablaggio per i lettori di schede sono illustrati nella Figura 4–3.

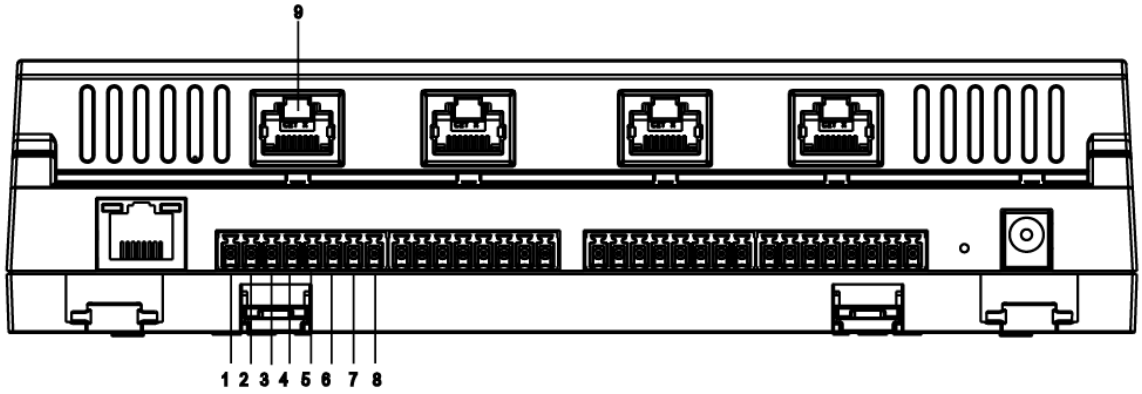

Figura 4–3

I terminali di cablaggio per il lettore ingresso n. 1 sono illustrati nella Tabella 4-9. Lettore uscita n. 1 e lettore ingresso n. 2 sono identici a lettore uscita n. 2 e lettore ingresso n. 1.

Interfaccia	N.	Terminale di cablaggio	Descrizione
Lettore di schede ingresso n. 1	1	485+	Lettore di schede 485
	2	485-	
	3	LED	Lettore di schede Wiegand
	4	D0	
	5	D1	
	6	CUSTODIA	
	7	GND	Alimentazione del lettore di schede
	8	12 V	

Tabella 4-9

I colori dei quattro RJ45 sono mostrati nella Tabella 4-10 (non standard).

N.	Terminale di cablaggio	Colore
9	485+	Bianco e arancione
	485-	Arancione
	LED	Bianco e verde
	D0	Blu
	D1	Bianco e blu
	CUSTODIA	Verde
	GND	Bianco e marrone
	12 V	Marrone

Tabella 4-10

4.3 Descrizione del cablaggio del dispositivo periferico

4.3.1 Descrizione del cablaggio del lettore di schede

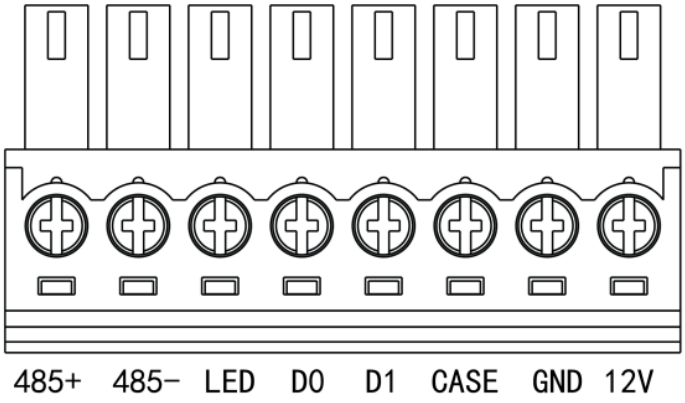

Figura 4–4

4.3.2 Descrizione del cablaggio del pulsante di uscita/sensore porta

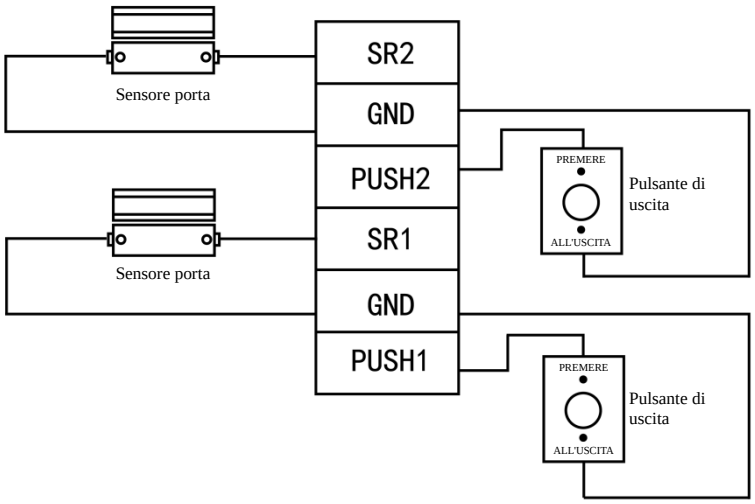

Figura 4–5

4.3.3 Descrizione del cablaggio della serratura

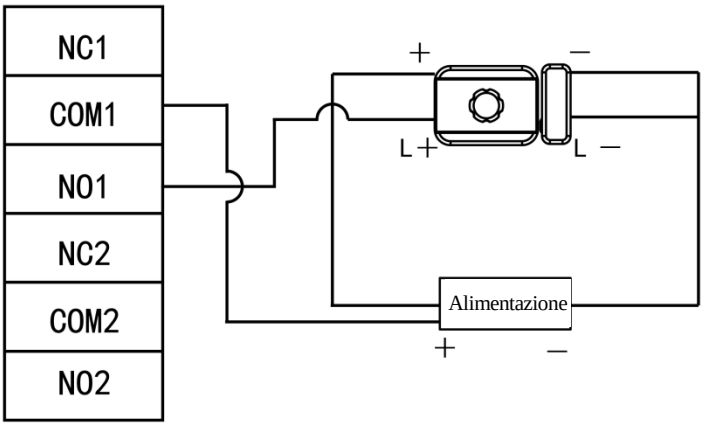

Figura 4–6

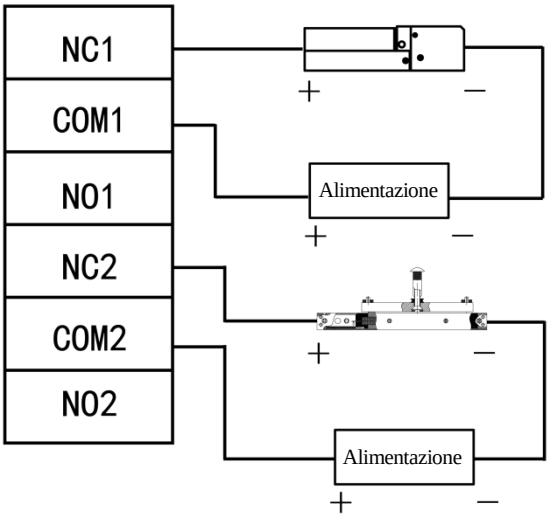

Figura 4–7

CONFIGURAZIONE DEL CLIENT

Il controller di accesso è gestito con client Smart PSS, in modo da ottenere il controllo e la giusta configurazione di una porta e di gruppi di porte.

5.1 Accesso al client

Installare il client Smart PSS corrispondente, quindi fare doppio clic su  per avviarlo. Eseguire la configurazione di inizializzazione secondo le indicazioni sull'interfaccia, quindi completare la procedura di accesso.

5.2 Aggiunta del controller degli accessi

Aggiungere il controller degli accessi in Smart PSS; selezionare "Ricerca automatica" (Auto Search) e "Aggiungi" (Add).

5.2.1 Ricerca automatica

I dispositivi devono appartenere allo stesso segmento di rete.

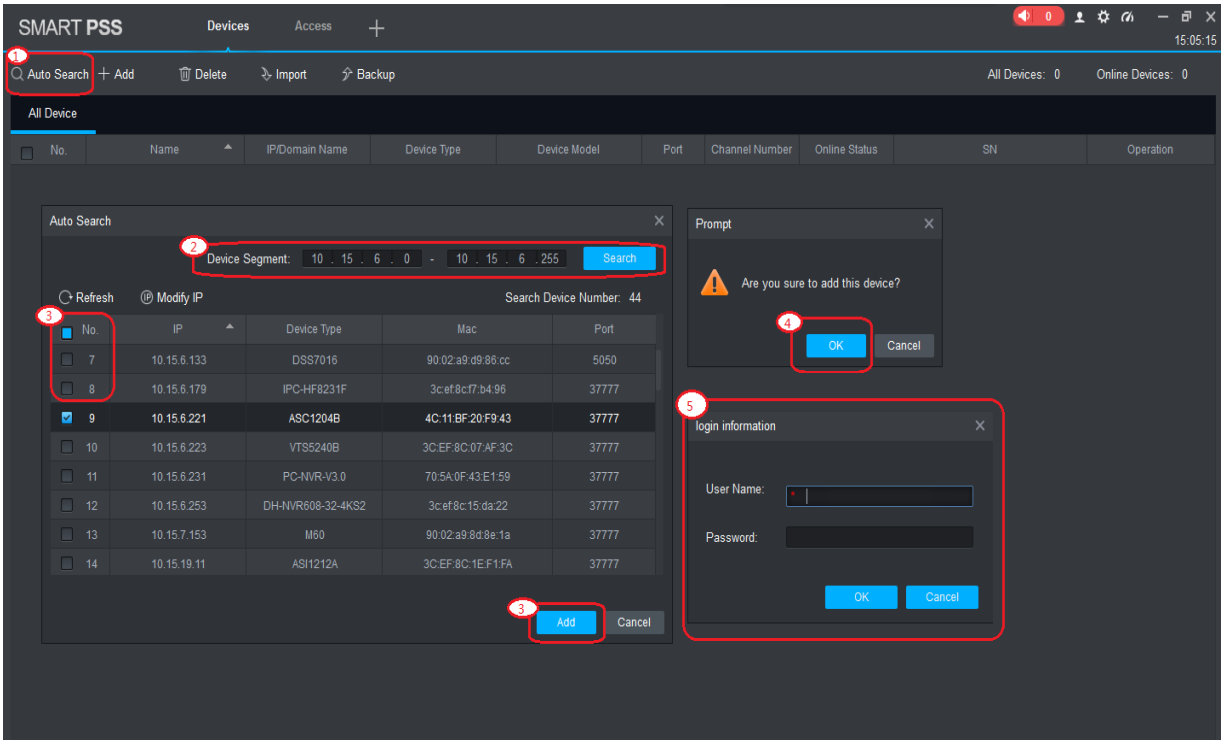

Figura 5–1

Fase 1: Fare clic su "Ricerca automatica" (Auto Search) nella schermata "Dispositivi" (Devices). Si aprirà la schermata di ricerca automatica (Auto Search).

Fase 2: Immettere il segmento del dispositivo, quindi fare clic su "Cerca" (Search). Il sistema mostrerà i risultati della ricerca.

Nota

- Fare clic su "Aggiorna" (Refresh) per aggiornare le informazioni sul dispositivo.
- Selezionare un dispositivo, quindi fare clic su "Modifica IP" (Modify IP) per modificare l'indirizzo IP del dispositivo. Per le procedure specifiche, fare riferimento al manuale d'uso del Client Smart PSS.

Fase 3: Selezionare il dispositivo che si desidera aggiungere, quindi fare clic su "Aggiungi" (Add). Sullo schermo apparirà un prompt.

Fase 4: Dopo aver fatto click su "OK" apparirà la finestra di dialogo "Informazioni sull'accesso" (Login Information).

Fase 5: Immettere il "nome utente" (User Name) e la "password" per accedere al dispositivo, quindi fare clic su "OK".

Il sistema mostrerà l'elenco dei dispositivi aggiunti, come illustrato nella Figura 5–2. Le operazioni disponibili sono mostrate nella Tabella 5-1.

Nota

- Dopo aver aggiunto il dispositivo, il sistema continuerà a mostrare la schermata della ricerca automatica (Auto Search). È possibile continuare ad aggiungere altri dispositivi, oppure fare clic su "Annulla" (Cancel) per uscire dall'interfaccia di ricerca automatica (Auto Search).
- Al termine dell'operazione, SmartPSS accede automaticamente al dispositivo. Se l'accesso è andato a buon fine, lo stato online mostra "Online". In caso contrario, viene visualizzato "Offline".

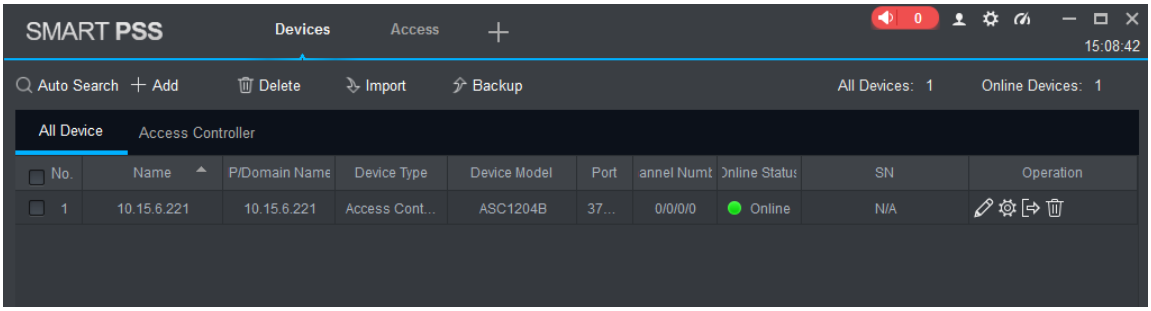

Figura 5–2

Icona	Descrizione
	Fare clic sull'icona per accedere all'interfaccia "Modifica dispositivo" (Modify Device). È possibile modificare le informazioni sul dispositivo, tra cui nome del dispositivo, IP/nome di dominio, porta, nome utente e password. In alternativa, fare doppio clic sul dispositivo per accedere all'interfaccia "Modifica dispositivo" (Modify Device).
	Fare clic su questa icona per accedere alla schermata "Config. dispositivo" (Device Config). Configurare la telecamera del dispositivo, la rete, gli eventi, le risorsa di archiviazione, le informazioni di sistema, ecc.

Icona	Descrizione
e	• Quando il dispositivo è connesso, appare l'icona . Fare clic sull'icona per uscire; l'icona cambia in . • Quando il dispositivo è offline, appare l'icona . Fare clic sull'icona per accedere al dispositivo (le informazioni del dispositivo devono essere corrette); l'icona cambia in .
	Fare clic sull'icona per eliminare un dispositivo.
	Selezionando "Mostra ID dispositivo" (Display Device ID) nelle impostazioni di sistema, questa icona appare nella barre delle operazioni. Fare clic su questa icona per personalizzare il codice del dispositivo, in modo da poter utilizzare il dispositivo quando la tastiera è collegata.

Tabella 5-1

5.2.2 Aggiunta manuale

Per aggiungere un dispositivo occorre conoscerne l'indirizzo IP o il nome di dominio.

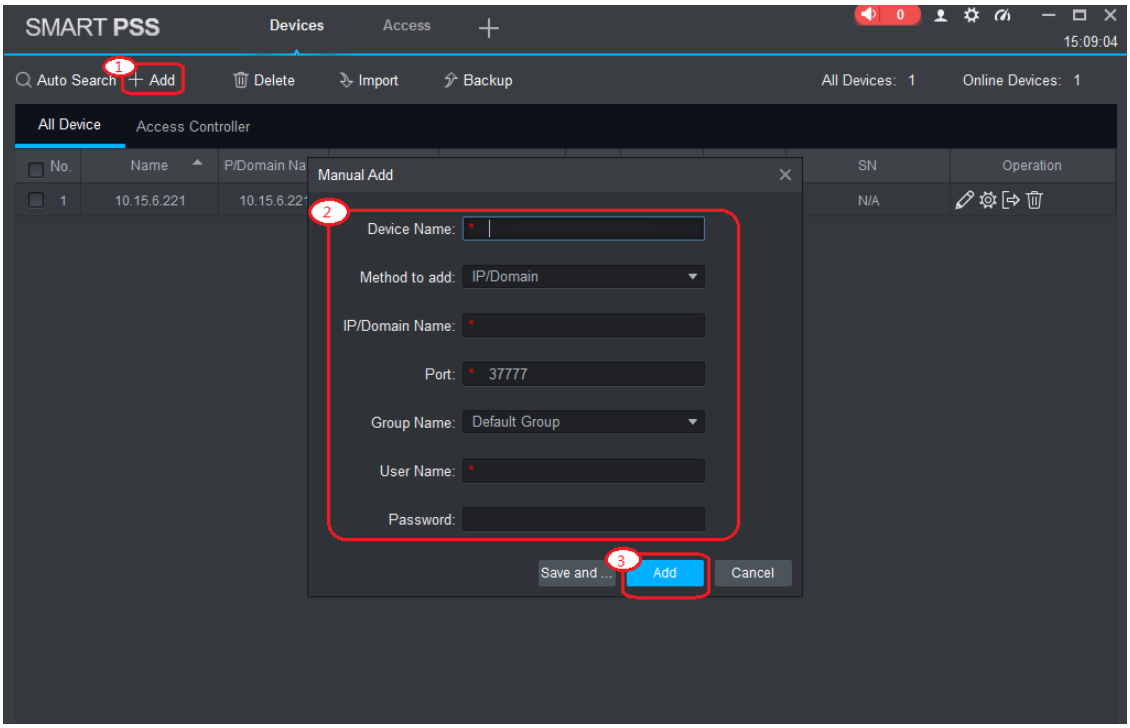

Figura 5–3

Fase 1: Fare clic su "Aggiungi" (Add) nella schermata "Dispositivi" (Devices). Apparirà la schermata "Aggiunta manuale" (Manual Add).

Fase 2: Impostare i parametri del dispositivo. Fare riferimento alla Tabella 5-2 per la descrizione dei parametri.

Parametro	Descrizione
Nome dispositivo	Si consiglia di assegnare il nome del dispositivo in base alla zona di monitoraggio, in modo da facilitare la manutenzione.
Modalità di aggiunta	Selezionare "IP/Nome di dominio" (IP/Domain Name). Aggiungere i dispositivi tramite indicazione dell'indirizzo IP o del nome di dominio degli stessi.
IP/Nome dominio	Indirizzo IP o nome di dominio del dispositivo.
Porta	Il numero di porta del dispositivo. Il numero di porta predefinito è 37777. Digitare il valore in base alle condizioni attuali.
Nome gruppo	Selezionare il gruppo del dispositivo.
Nome utente e password	Il nome utente e la password del dispositivo.

Tabella 5-2

Fase 3: Fare clic su "Aggiungi" (Add) per aggiungere un dispositivo. Le operazioni disponibili sono mostrate nella Tabella 5-1.

Nota

- Per aggiungere altri dispositivi e restare nella schermata "Aggiunta manuale" (Manual Add), fare clic su "Salva e continua" (Save and Continue).
- Per terminare e uscire dalla schermata di aggiunta manuale (Manual Add), fare clic su "Annulla" (Cancel).
- Al termine dell'operazione, SmartPSS accede automaticamente al dispositivo. Se l'accesso è andato a buon fine, lo stato online mostra "Online". In caso contrario, viene visualizzato "Offline".

5.3 Aggiungi persone

Le persone aggiunte corrispondono a schede, per facilitare l'assegnazione delle autorizzazioni.

Nella schermata "Nuovo" (New), fare clic su 

per accedere alla schermata "Accesso" (Access) e completare le configurazioni per l'accesso.

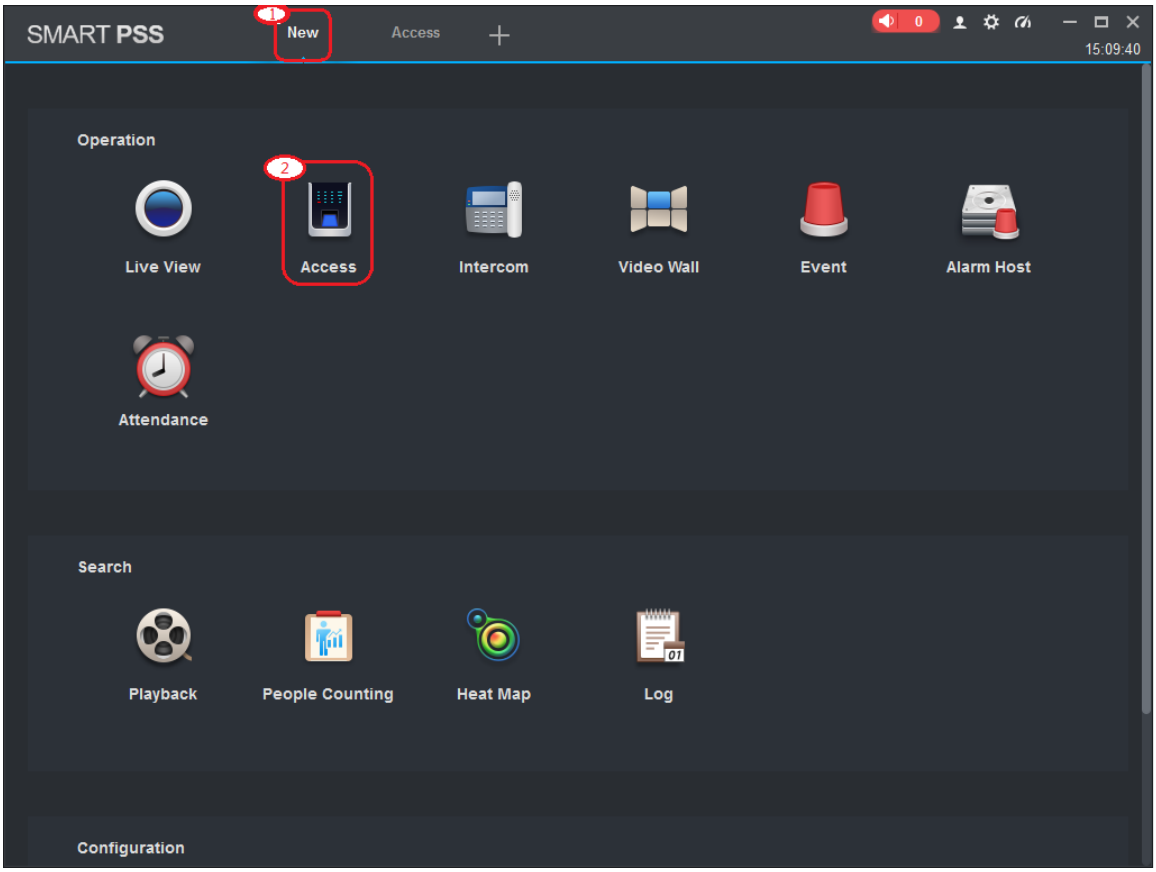

Figura 5–4

5.3.1 Impostazione del tipo di scheda

Attenzione

Il tipo di scheda deve corrispondere all'emittente della scheda. Altrimenti, non sarà possibile leggere il numero della scheda.

Nella schermata "Accesso" (Access), selezionare "Utente" (User), quindi fare clic su per impostare il tipo di scheda, come illustrato nella Figura 5–5.

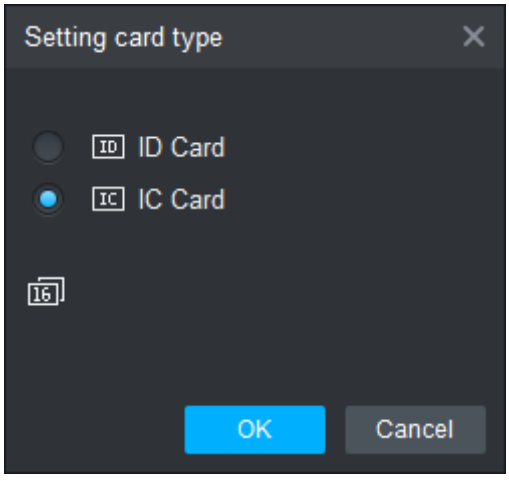

Figura 5–5

5.3.2 Aggiungi utente

Qui è possibile aggiungere un nuovo utente, emettere una scheda e inserire le informazioni sull'utente.

Nella schermata "Accesso" (Access), selezionare "Utente (User), quindi fare clic su  per aggiungere manualmente le informazioni, come informazioni base, impronta digitale e dettagli. Fare clic su "Fine" (Finish) per completare l'operazione, come illustrato nella Figura 5–6.

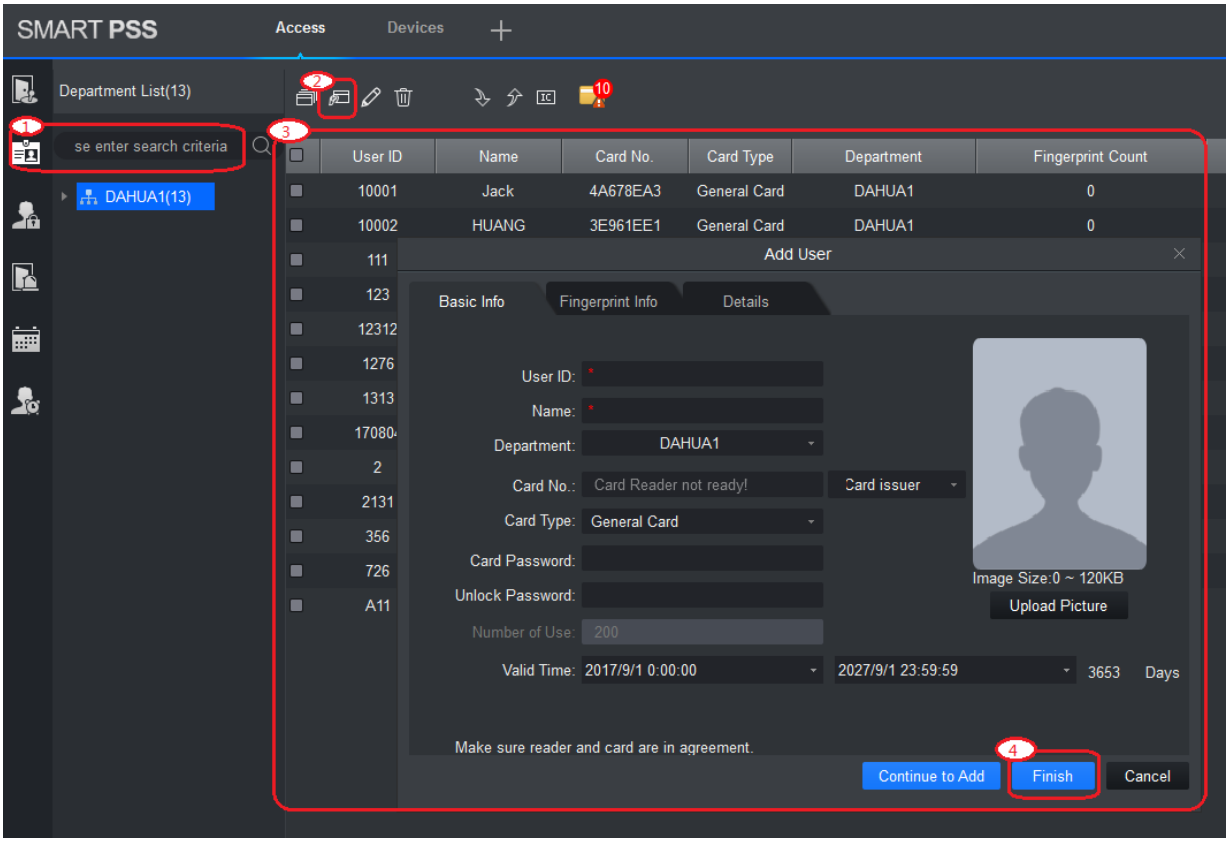

Figura 5–6

5.4 Aggiungi gruppi

Qui è possibile suddividere l'accesso in gruppi ed effettuare una gestione congiunta.

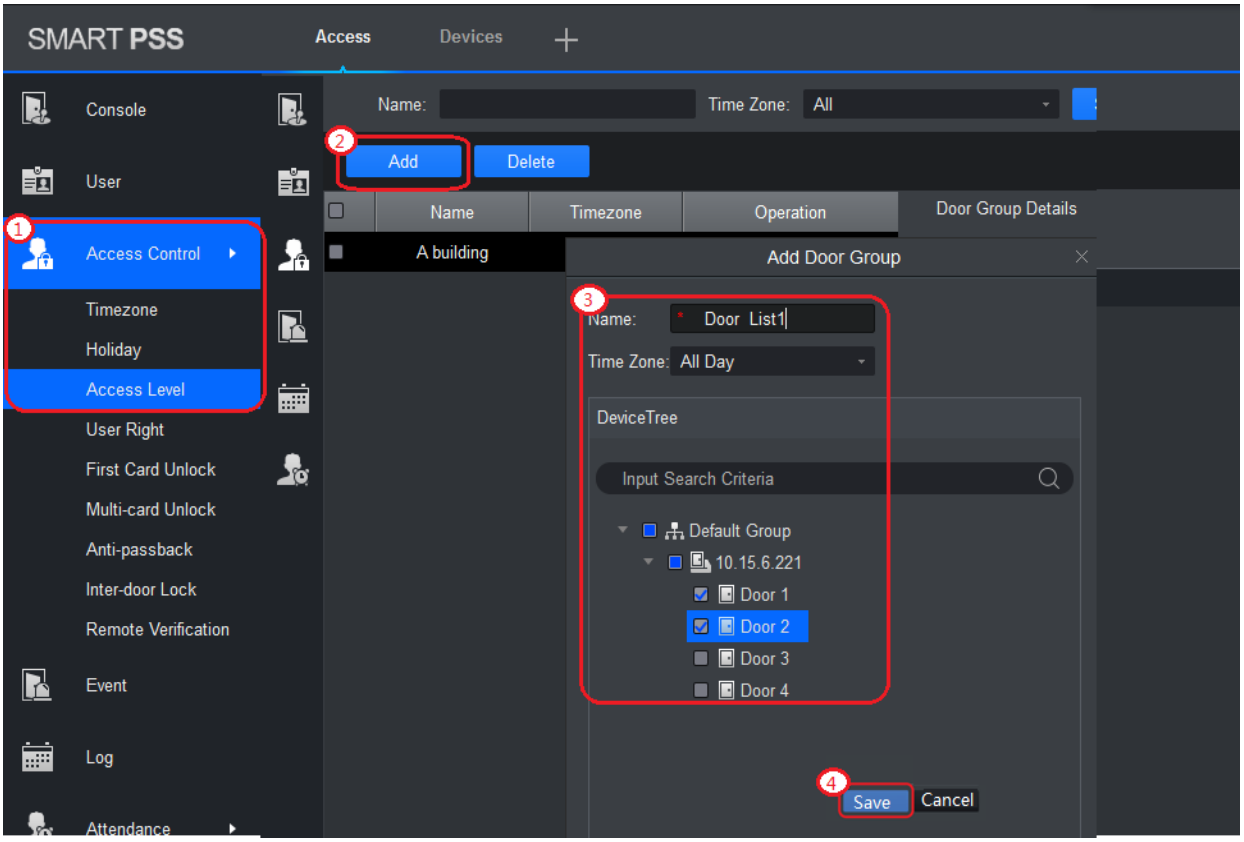

Figura 5–7

Fase 1: Nella schermata "Accesso" (Access), selezionare "Utente > Controllo degli accessi (User > Access Control).

Fase 2: Fare clic su "Aggiungi" (Add). Si aprirà la finestra di dialogo "Aggiungi gruppo porta" (Add Door Group).

Fase 3: Immettere il "nome" (Name), quindi selezionare il "fuso orario" (Time Zone) e le porte gestite dal gruppo.

Fase 4: Fare clic su "Salva" (Save) per completare l'aggiunta.

5.5 Assegnazione delle autorizzazioni

Ci sono due tipi di autorizzazioni assegnati in base al gruppo porta e all'utente.

5.5.1 Autorizzazione del gruppo porta.

Selezionare il gruppo porta e aggiungere utenti. In questo modo, gli utenti del gruppo porta fruiscono dei privilegi di tutte le porte del gruppo.

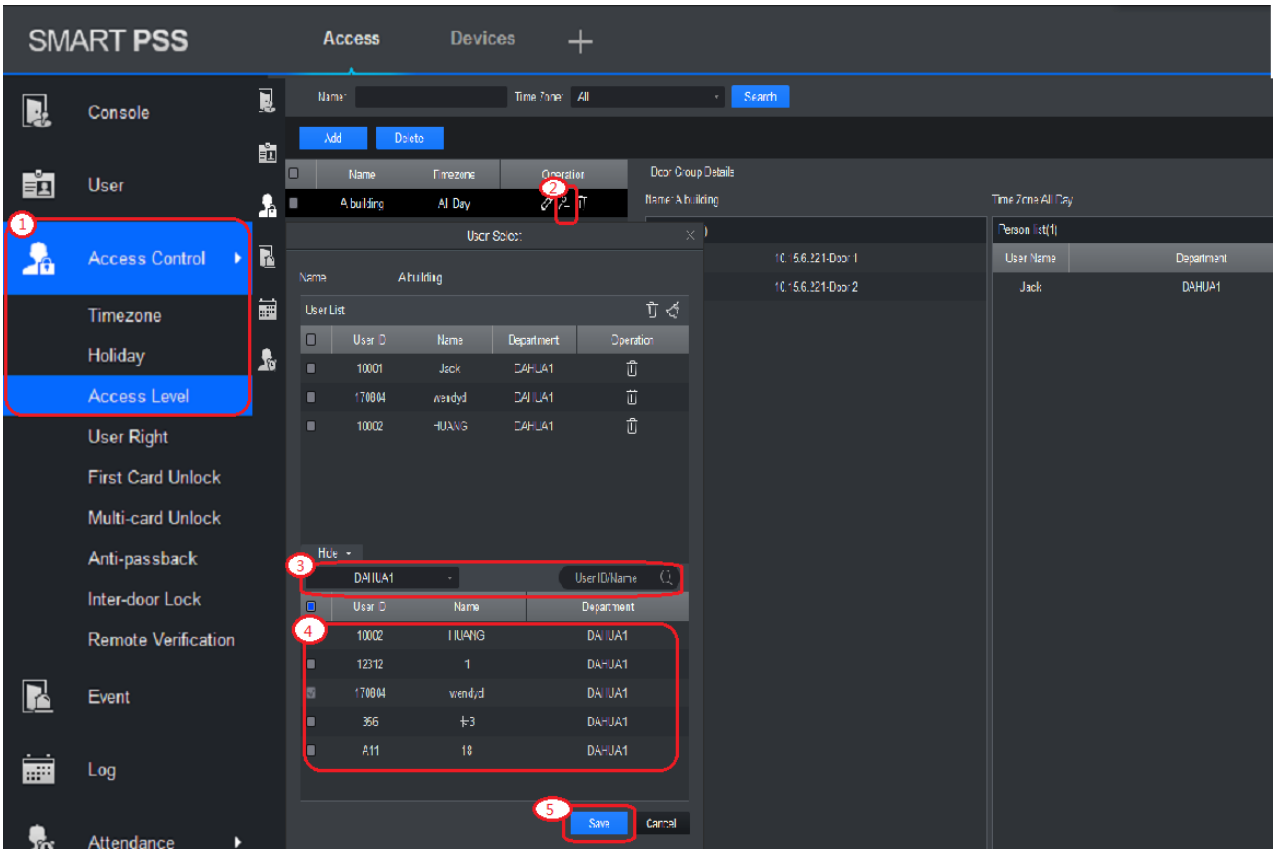

Figura 5–8

Fase 1: Nella schermata "Accesso" (Access), selezionare "Utente > Controllo degli accessi (User > Access Control).

Fase 2: Fare clic su  . Si aprirà la finestra di dialogo "Selezione utente" (User Select).

Fase 3: Nell'elenco a discesa, selezionare il dipartimento utente o inserire l'ID utente oppure il nome.

Fase 4: Selezionare gli utenti dall'elenco di ricerca e aggiungerli all'elenco utenti.

Fase 5: Fare clic su "Salva" (Save) per completare l'assegnazione delle autorizzazioni.

5.5.2 Autorizzazione utente

Selezionare un utente, assegnare gruppi porta all'utente. In questo modo, l'utente fruisce dell'autorizzazione per tutte le porte nei gruppi porta selezionati.

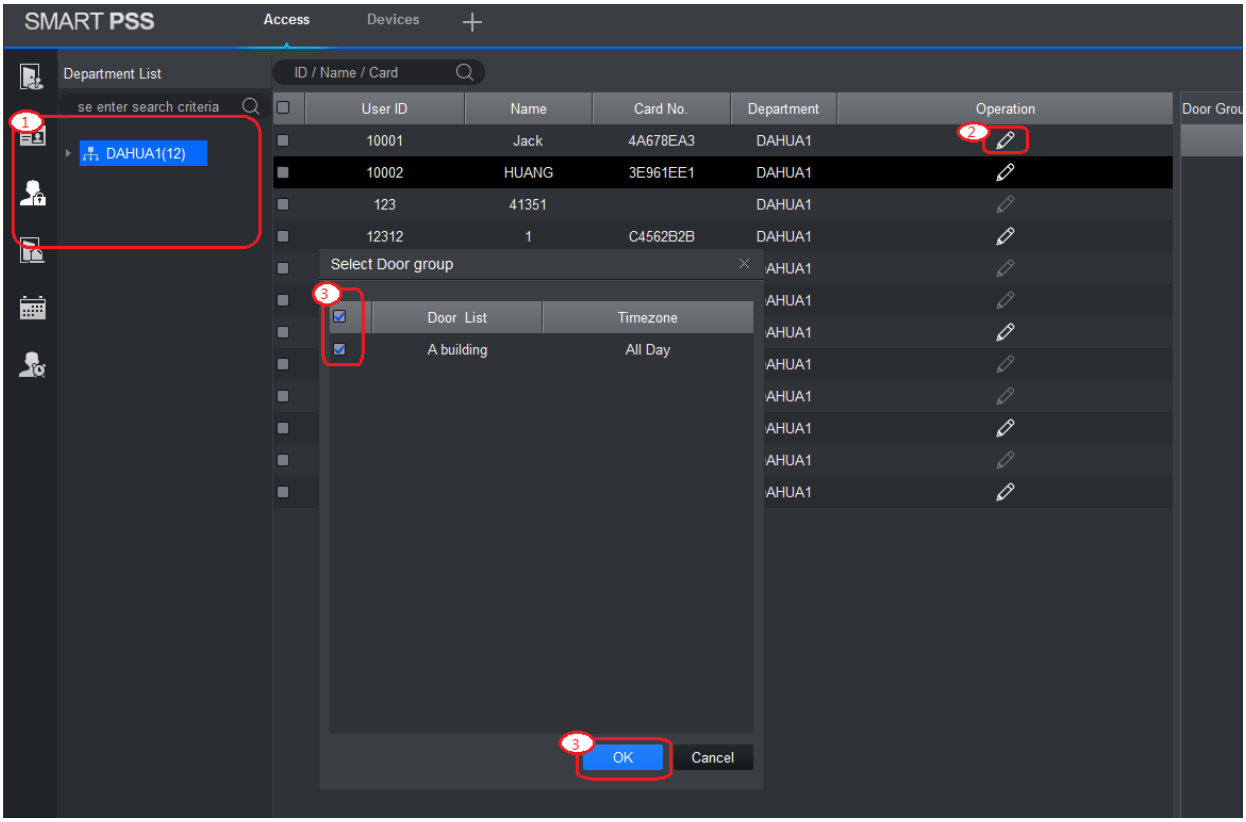

Figura 5–9

Fase 1: Nella schermata "Accesso" (Access), selezionare "Utente > Controllo degli accessi (User > Access Control).

Fase 2: Fare clic su  . Si aprirà la finestra di dialogo "Seleziona gruppo porta" (Select Door Group).

Fase 3: Selezionare i gruppi porta a cui si desidera concedere l'autorizzazione, quindi fare clic su "OK" per completare l'operazione.

PARAMETRI TECNICI

Parametro	Specifica
Responsabile del Trattamento dei Dati	Processore ARM 32 bit
Capacità d'archiviazione	16 M
N. max utenti	100.000
N. max registrazioni	150.000
Porta di comunicazione del lettore	Wiegand, RS485
Porta di comunicazione della piattaforma	TCP/IP
Quantità di lettori connessi	4 gruppi
Alimentazione	Potenza nominale 10V~15V CC, Corrente nominale 0,75 A
Pianificazione	128
Periodo	128
Vacanze	128
Modalità sblocco	Scheda, scheda+password, password, scheda o password, scheda+impronta, impronta+password, impronta o scheda o password, per intervallo di tempo.