LAC21KI

Controller degli accessi

FUNZIONI:

- Server Web integrato, presenta modalità di controllo principale e secondaria.
- La modalità di controllo principale offre funzioni della piattaforma di controllo degli accessi, può connettersi e gestire fino a 19 sottocontroller. Le modalità di controllo secondario possono essere aggiunte a più piattaforme.
- Supporta 1000 utenti (modalità di controllo principale), 3000 impronte digitali, 5000 schede Bluetooth (modalità di controllo principale) e 300.000 record.
- Accede ai lettori di carte tramite i protocolli Wiegand e RS-485.
- Supporta la connessione TCP e IP e PoE standard.
- Fornisce alimentazione alla serratura tramite l'alimentatore in uscita da 12 V CC, che ha una corrente di uscita massima di 1000 mA.
- Supporta la configurazione della porta I/O hardware e l'esportazione dei diagrammi di configurazione.
- Conserva i dati memorizzati anche quando è spento.
- Gestione dei ruoli.
- Supporta molteplici funzioni avanzate di controllo degli accessi, come sblocco in prima persona, sblocco multi-persona, anti-passback globale, interblocco multiporta globale e allarme esterno globale.

V1.0.2

Introduzione

Generale

Questo manuale illustra le funzioni e l'utilizzo del controller degli accessi. Leggere attentamente il manuale prima di utilizzare il dispositivo e conservarlo per future consultazioni.

Istruzioni di sicurezza

Nel manuale possono comparire i seguenti indicatori di pericolo.

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.
SUGGERIMENTI	Descrivono metodi per risolvere problemi o risparmiare tempo.
NOTA	Fornisce informazioni aggiuntive che completano quelle riportate nel testo.

Cronologia delle revisioni

Versione	Contenuto della revisione	Data di rilascio
V1.0.2	Aggiornamento delle operazioni sulla pagina web.	Dicembre 2022
V1.0.1	Aggiornamento del cablaggio.	Settembre 2022
V1.0.0	Prima versione.	Settembre 2022

Informativa sulla protezione della privacy

È possibile che chi utilizza i dispositivi o gestisce i dati raccolga dati personali di altre persone, come il volto, le impronte digitali e il numero di targa dei veicoli. Gli utenti devono rispettare le norme e le leggi locali in materia di protezione della privacy per garantire il rispetto dei diritti e degli interessi legittimi di terzi. A questo scopo occorre adottare misure appropriate come, a titolo esemplificativo e non esaustivo, l'utilizzo di segnali chiari e ben visibili per informare le persone dell'esistenza di un impianto di sorveglianza nell'area, con l'indicazione delle informazioni di contatto richieste.

Informazioni sul manuale

- Questo manuale serve solo come riferimento. Possono esserci lievi differenze rispetto al prodotto effettivo.
- Decliniamo ogni responsabilità in relazione a eventuali perdite causate da utilizzi del prodotto non conformi a quanto riportato nel manuale.

- Il manuale verrà aggiornato in base alle leggi e ai regolamenti più recenti delle relative giurisdizioni. Per informazioni dettagliate, consultare il manuale d'uso in formato cartaceo, utilizzare il CD-ROM, scansionare il codice QR o visitare il nostro sito web ufficiale. Questo manuale serve solo come riferimento. È possibile che sussistano delle lievi differenze tra la
- versione elettronica e cartacea del manuale.
  Design e software sono soggetti a modifica senza preavviso. A seguito degli aggiornamenti del prodotto possono sorgere differenze tra il prodotto effettivo e le informazioni contenute nel manuale. Contattare il servizio di assistenza per il software e la documentazione supplementare più recenti.
- È possibile che siano presenti errori di stampa o discrepanze nella descrizione delle funzioni, delle operazioni e dei dati tecnici. In caso di dubbi o vertenze, ci riserviamo il diritto di
- interpretazione finale.
  Se non è possibile aprire il manuale in formato PDF, aggiornare il programma per la lettura dei file PDF o provarne un altro.
- 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, consultare il nostro sito web oppure contattare il fornitore o il servizio di assistenza al cliente.
- In caso di dubbi o controversie, ci riserviamo il diritto di interpretazione finale.

Norme di sicurezza e avvertenze importanti

Questa sezione descrive come gestire correttamente il controller degli accessi e come prevenire eventuali pericoli e danni materiali. Leggerla attentamente prima di usare il controller degli accessi e rispettare le linee guida per l'utilizzo.

Requisiti per il trasporto

Trasportare, utilizzare e conservare il controller degli accessi nelle condizioni di umidità e temperatura consentite.

Requisiti per lo stoccaggio

Stoccare il controller degli accessi nelle condizioni di umidità e temperatura consentite.

Requisiti per l'installazione

AVVERTENZA

- Non collegare l'adattatore di corrente al controller degli accessi mentre è acceso.
- Rispettare scrupolosamente le normative e gli standard locali sulla sicurezza elettrica. Accertarsi che la tensione fornita sia stabile e rispetti i requisiti di alimentazione del controller degli accessi.
- Per evitare danni al controller degli accessi, non collegarlo a due o più fonti di alimentazione diverse.
- L'uso improprio della batteria potrebbe causare incendi o esplosioni.

- Il personale che lavora in quota deve adottare le misure necessarie a tutelare la propria sicurezza, come indossare il casco e le cinture di sicurezza.
- Non collocare il controller degli accessi in luoghi esposti alla luce solare o in prossimità di fonti di calore.
- Tenere il controller degli accessi lontano da umidità, polvere e fuliggine.
- Installare il controller degli accessi su una superficie stabile per evitarne la caduta.
- Installare il controller degli accessi in un ambiente adeguatamente ventilato e non ostruire la circolazione dell'aria.
- Utilizzare l'adattatore o l'unità di alimentazione indipendente forniti dal produttore.
- Utilizzare i cavi di alimentazione consigliati per l'area geografica e conformi alle specifiche di alimentazione nominale.
- La fonte di alimentazione deve rispondere ai requisiti ES1 dello standard IEC 62368-1 e non deve superare il livello PS2. I requisiti di alimentazione elettrica sono riportati sull'etichetta del controller degli accessi.
- Il controller degli accessi è un apparecchio elettrico di classe I. Accertarsi che il controller degli accessi sia collegato a una presa di corrente con messa a terra di protezione.

Requisiti di funzionamento

⚠

- Prima dell'uso, verificare che l'alimentazione utilizzata sia corretta.
- Non scollegare il cavo di alimentazione sul lato del controller degli accessi mentre l'adattatore è acceso.
- Utilizzare il controller degli accessi rispettando l'intervallo di potenza nominale in ingresso e in uscita.
- Utilizzare il controller degli accessi nelle condizioni di umidità e temperatura consentite.
- Evitare di versare o schizzare liquidi sul controller degli accessi e accertarsi che non siano presenti contenitori pieni di liquidi sopra il dispositivo.
- Il controller degli accessi può essere smontato solo da personale qualificato.

Indice

1 Panoramica del prodotto

1.1 Introduzione al prodotto

Pratico e flessibile, questo dispositivo è caratterizzato da un sistema user-friendly che consente l'accesso ai controller da pagina web tramite indirizzo IP. Dotato di un sistema di gestione degli accessi professionale, rende semplice e veloce l'utilizzo delle modalità di controllo principale e secondaria, rispondendo alle esigenze di sistemi di piccole dimensioni o più avanzati.

1.2 Caratteristiche principali

- Design robusto ed elegante con certificazione IK06 realizzato in materiali PC e ABS ignifughi.
- Supporto delle connessioni TCP, IP e PoE standard.
- Accesso ai lettori di schede tramite protocollo Wiegand e RS-485.
- Alimentazione della serratura tramite uscita 12 V CC, con corrente di uscita massima di 1000 mA.
- Supporto di 1000 utenti, 5000 schede, 3000 impronte digitali e 300.000 record.
- Metodi di sblocco multipli, che comprendono scheda, password e impronta digitale. Possibilità di combinare i metodi di sblocco supportati per crearne di personalizzati.
- Supporto di varie tipologie di eventi di allarme, tra cui: coercizione, manomissione, intrusione, timeout di sblocco e scheda non valida.
- Supporto di un'ampia gamma di utenti, tra cui: generale, di pattuglia, VIP, ospite, bloccato.
- Sincronizzazione oraria manuale e automatica.
- Conservazione dei dati archiviati anche da spento.
- Numerose funzioni disponibili e configurabilità del sistema. Possibilità di aggiornare i dispositivi tramite pagina web.
- Modalità di controllo principale e secondaria. La modalità di controllo principale offre varie opzioni, come la gestione degli utenti o la gestione e la configurazione del dispositivo di controllo degli accessi. Possibilità di aggiungere i dispositivi in modalità di controllo secondaria a più piattaforme.
- Connessione e gestione di un massimo di 19 controller secondari da parte di un controller principale.
- Protezione watchdog del sistema, per una maggiore stabilità ed efficienza del dispositivo.
- Possibilità di aggiungere i controller secondari a SmartPSS Lite e DSS Pro.

1.3 Scenari applicativi

Ampiamente utilizzato nei parchi, nelle comunità, nei centri commerciali e nelle fabbriche, il dispositivo è particolarmente adatto per i luoghi come gli edifici governativi, le scuole e gli stadi.
Il controller degli accessi può essere impostato come controller degli accessi principale (da qui in avanti denominato controller principale) o come controller degli accessi secondario (da qui in avanti

denominato controller secondario). Il controller degli accessi ha a disposizione due metodi di gestione in rete diversi. È possibile selezionare il metodo più adatto alle proprie esigenze.

Tabella 1-1 Metodi di gestione in rete del controller degli accessi

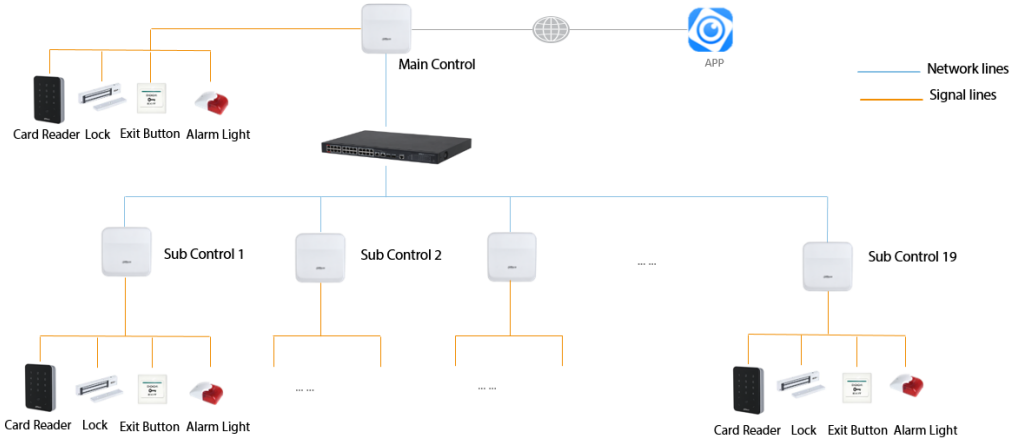
Metodo di gestione in rete	**Descrizione**
Controller principale-Controller secondario	Il controller principale è dotato di una piattaforma di gestione (da qui in avanti denominata piattaforma). I controller secondari devono essere aggiunti alla piattaforma del controller principale. Il controller principale può gestire fino a 19 controller secondari. Per ulteriori dettagli, consultare la sezione "2 Controller principale-Controller secondario".
SmartPSS Lite-Controller secondario	I controller secondari devono essere aggiunti a una piattaforma di gestione autonoma, come SmartPSS Lite. La piattaforma può gestire fino a 32 controller secondari. Per ulteriori dettagli, consultare la sezione "3 Smart PSS Lite-Controller secondari".

2 Controller principale-Controller secondario

2.1 Diagramma di rete

Il controller principale è dotato di una piattaforma di gestione (da qui in avanti denominata piattaforma). I controller secondari devono essere aggiunti alla piattaforma di gestione del controller principale. Il controller principale può gestire fino a 19 controller secondari.

Figura 2-1 Diagramma di rete



2.2 Configurazioni del controller principale

2.2.1 Diagramma di flusso della configurazione

Figura 2-2 Diagramma di flusso della configurazione

2.2.2 Inizializzazione

Inizializzare il controller principale quando si accede alla pagina web per la prima volta o dopo che si sono ripristinate le impostazioni predefinite di fabbrica.

Prerequisiti

Accertarsi che il computer utilizzato per accedere alla pagina web si trovi sulla stessa LAN del controller principale.

Procedura

Passaggio 1: Aprire un browser e accedere all'indirizzo IP del controller principale (l'indirizzo predefinito è 192.168.1.108).

Consigliamo di utilizzare l'ultima versione di Chrome o Firefox.

Passaggio 2: Selezionare una lingua, quindi fare clic su **Avanti** (Next).

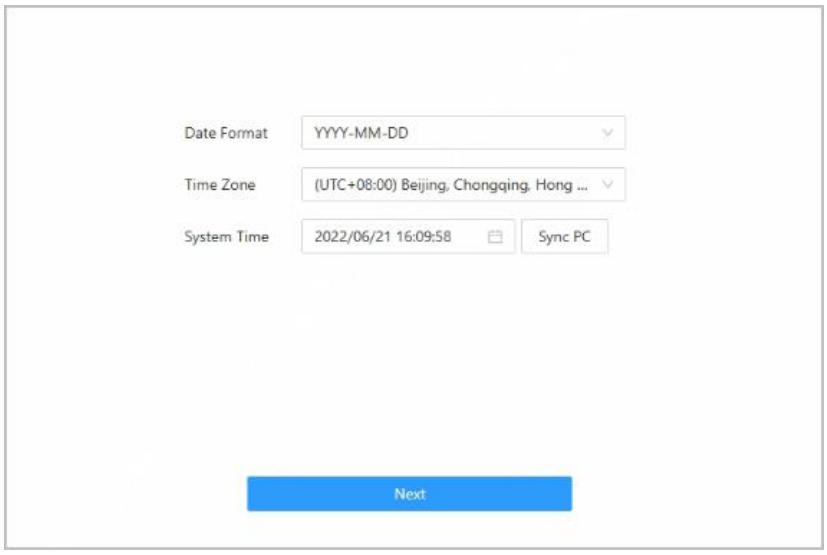
Passaggio 3: Leggere con attenzione l'accordo di licenza del software e la Politica sulla privacy, quindi selezionare **Ho letto il contratto di licenza del software e la politica sulla privacy e dichiaro di accettarne i termini** (I have read and agree to the terms of the Software License Agreement and Privacy Policy) e fare clic su **Avanti** (Next).

Passaggio 4: Impostare la password e l'indirizzo e-mail.

- La password deve contenere fra 8 e 32 caratteri, che non siano spazi, di almeno due tipologie diverse scelte tra lettere maiuscole, lettere minuscole, cifre e caratteri speciali (esclusi ' " ; : &). Impostare una password sicura seguendo le indicazioni visualizzate.
- Per una maggiore sicurezza, conservare la password in modo appropriato dopo l'inizializzazione e modificarla regolarmente.

Passaggio 5: Configurare la data e l'ora di sistema, quindi fare clic su **Avanti** (Next).

Figura 2-3 Configurazione della data e dell'ora



Passaggio 6: Selezionare **Controllo automatico degli aggiornamenti** (Autocheck for updates) e fare clic su **Fine** (Completed) (opzionale).

Il sistema verifica automaticamente se è disponibile una versione più recente e informa l'utente se è necessario effettuare un aggiornamento. Il sistema verifica automaticamente la presenza di nuovi aggiornamenti e comunica all'utente quando questi sono disponibili.

Passaggio 7: Fare clic su **Fine** (Completed).

Dopo che l'inizializzazione è stata completata, il sistema mostra automaticamente la pagina di accesso.

2.2.3 Accesso

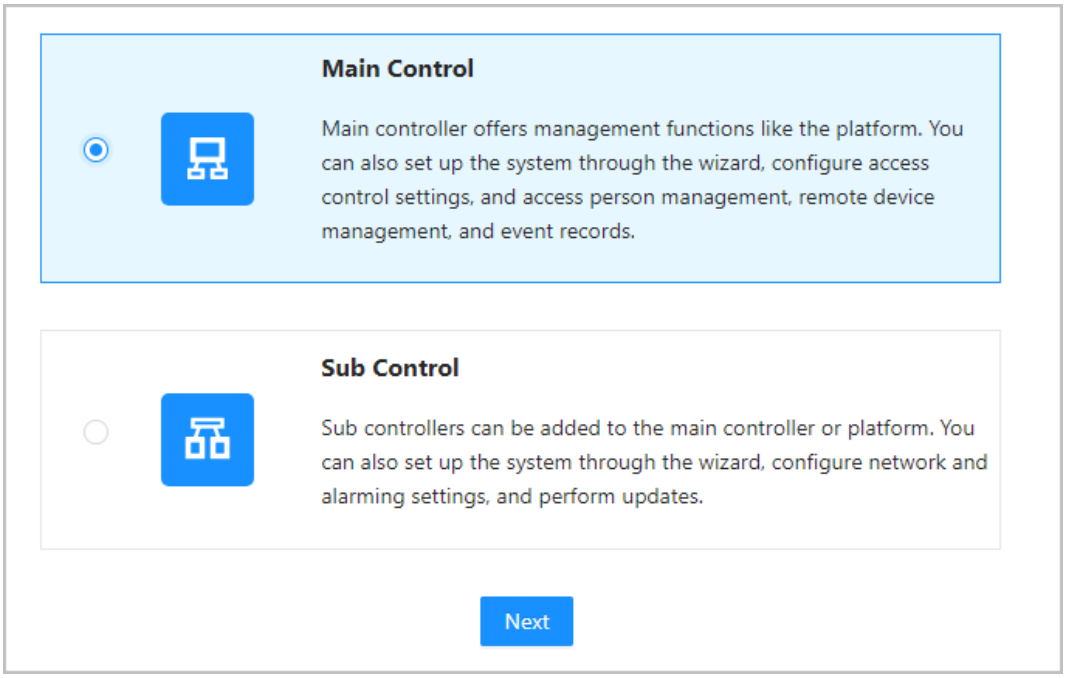
Per l'inizializzazione al primo accesso, è necessario seguire la procedura guidata per configurare il tipo di controller principale e il suo hardware.

Passaggio 1: Sulla pagina di accesso, inserire il nome utente e la password.

- Il nome utente predefinito dell'amministratore è admin, mentre la password è quella impostata durante l'inizializzazione. Consigliamo di modificare con regolarità la password dell'amministratore per migliorare la sicurezza della piattaforma.
- Se si dimentica la password di accesso dell'amministratore, fare clic su **Password dimenticata?** (Forget password?).

Passaggio 2: Selezionare **Controller principale** (Main Control) e fare clic su **Avanti** (Next).

Figura 2-4 Tipo di controller degli accessi



- Controller principale: il controller principale è dotato di una piattaforma di gestione, che consente di effettuare numerose operazioni, come gestire tutti i controller secondari, configurare il controllo degli accessi e accedere alla gestione del personale.
- Controller secondario: i controller secondari devono essere aggiunti alla piattaforma di gestione del controller principale o ad altre piattaforme di gestione come DSS Pro o SmartPSS Lite. È possibile effettuare le configurazioni locali solo sulla pagina web del controller secondario. Per ulteriori dettagli, consultare la sezione "2.3 Configurazione del controller secondario".

Passaggio 3: Selezionare il numero di porte e inserire il loro nome.

Passaggio 4: Configurare i parametri delle porte.

Figura 2-5 Configurazione dei parametri della porta

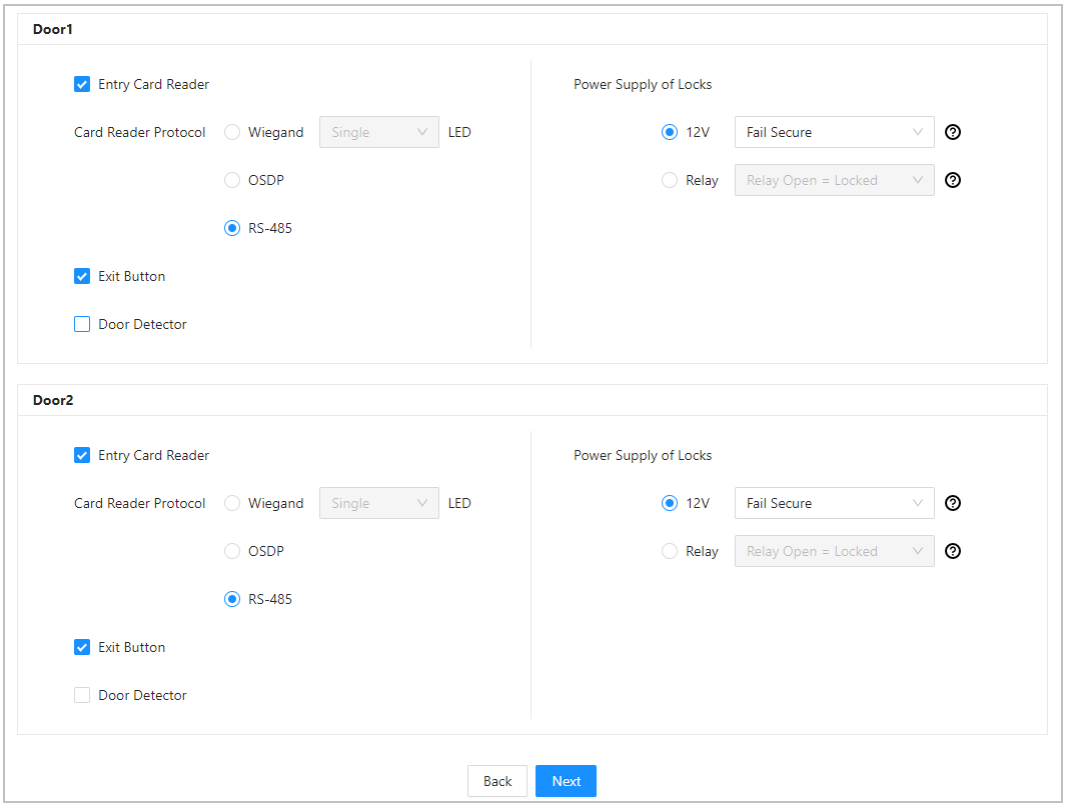


Tabella 2-1 Descrizione dei parametri

Parametro	Descrizione
Lettore di schede di ingresso	Selezionare il protocollo del lettore di schede. ● Wiegand: connessione a un lettore Wiegand. È possibile collegare il filo LED alla porta LED del controller, per far sì che il lettore emetta un segnale acustico e lampeggi quando la porta si sblocca. ● OSDP: connessione a un lettore OSDP. ● RS-485: connessione a un lettore OSDP.
Pulsante di uscita	Connessione a un pulsante di uscita.
Rilevatore per porte	Connessione a un rilevatore per porte.
Alimentazione delle serrature	● 12 V: il controller alimenta la serratura. ◇ Protezione guasti: quando si verifica un'interruzione di corrente o un guasto all'alimentazione, la porta resta chiusa. ◇ Sicurezza guasti: quando si verifica un'interruzione di corrente o un guasto all'alimentazione, la porta si apre automaticamente per consentire alle persone di uscire. ● Relè: il relè alimenta la serratura. ◇ Relè aperto = blocco: la serratura resta bloccata quando il relè è aperto. ◇ Relè aperto = sblocco: la serratura si sblocca quando il relè è aperto.

Passaggio 5: Configurare i parametri del controllo degli accessi.

Passaggio 6: Sulla schermata **Impostazioni di sblocco** (Unlock Settings) selezionare **O** (Or) oppure **E** (And) come **Metodo di combinazione** (Combination Method).

- O: utilizza uno dei metodi di sblocco selezionati per autorizzare l'apertura della porta.
  E: utilizza tutti i metodi di sblocco selezionati per autorizzare l'apertura della porta.
  Il controller supporta lo sblocco tramite scheda, impronta digitale e password.

Passaggio 7: Selezionare i metodi di sblocco e configurare gli altri parametri.

Figura 2-6 Impostazioni (scelta multipla)

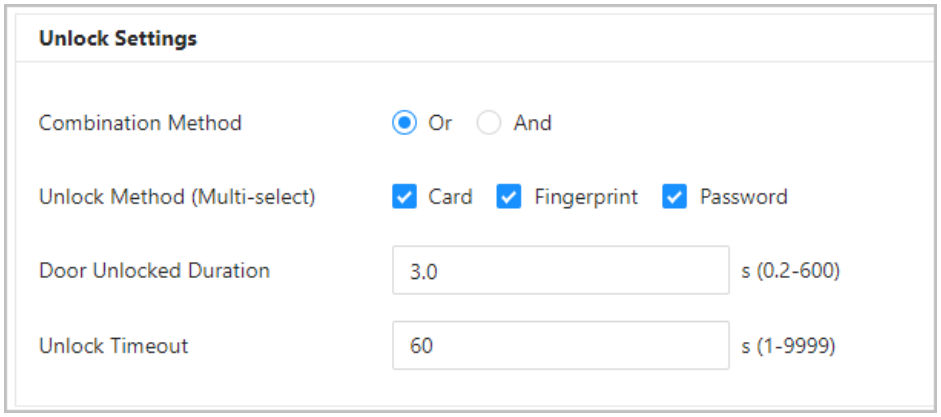


Tabella 2-2 Descrizione delle impostazioni di sblocco

Parametro	Descrizione
Durata sblocco porta	Quando viene autorizzato l'accesso di una persona, la porta resta sbloccata per un periodo di tempo definito che consenta alla persona di entrare. I valori selezionabili sono compresi tra 0,2 e 600 secondi.
Timeout sblocco	Quando la porta resta sbloccata più a lungo del tempo impostato, si attiva un allarme di timeout.

Passaggio 8: Nella finestra **Impostazioni allarme** (Alarm Settings), configurare i parametri di allarme.

Figura 2-7 Allarme

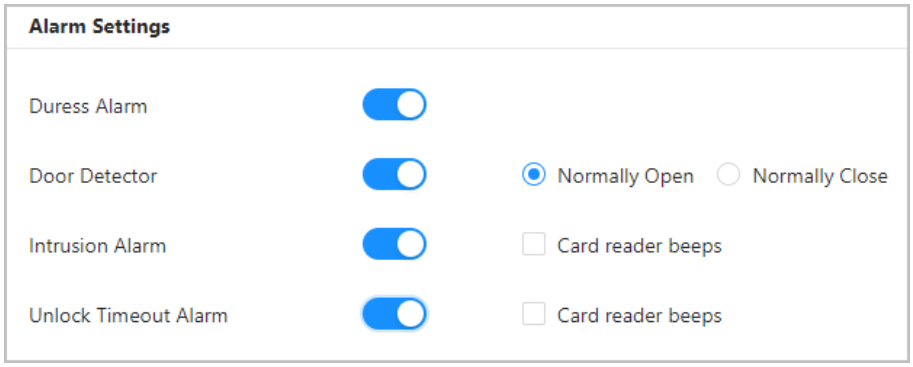


Tabella 2-3 Descrizione dei parametri di allarme

Parametro	Descrizione
Allarme coercizione	Un allarme si attiva se una scheda, una password o un'impronta coercizione viene utilizzata per sbloccare la porta.
Rilevatore per porte	Selezionare il tipo di rilevatore per porte.

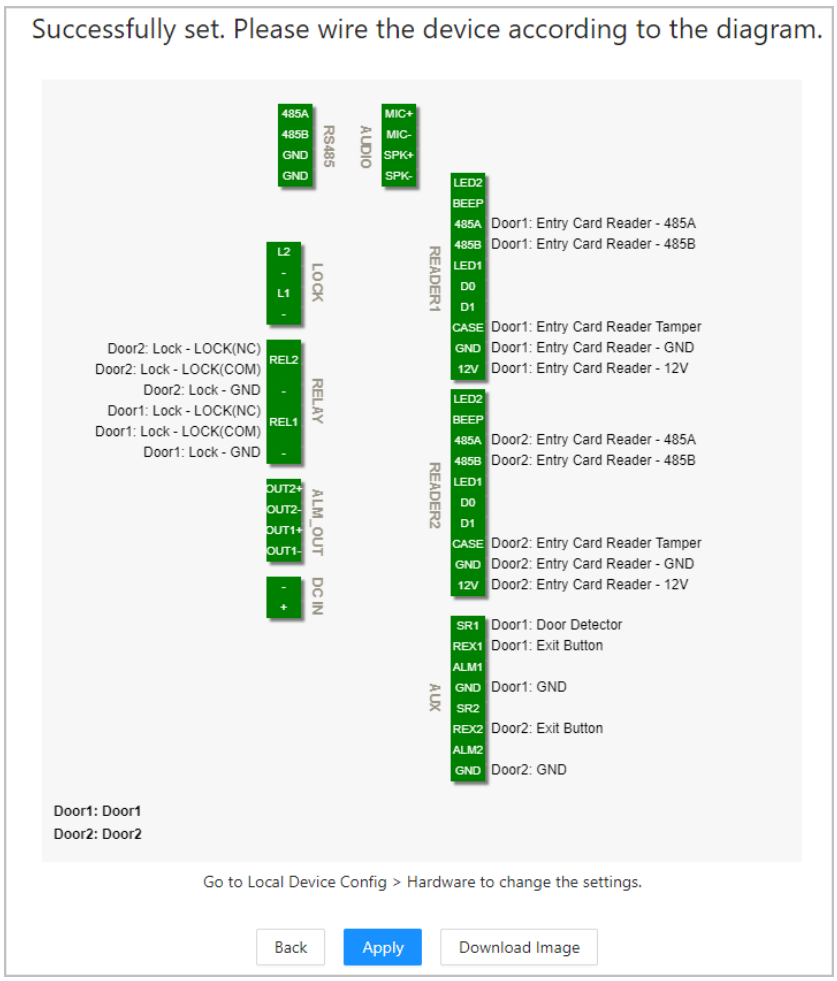
Parametro	Descrizione
Allarme intrusione	● Quando il rilevatore per porte è abilitato, se la porta viene aperta in modo anomalo si attiva un allarme intrusione. ● Se la porta resta sbloccata più a lungo del tempo impostato, si attiva un allarme di timeout. ● Quando l'opzione **Segnale acustico lettore di schede** (Card reader beeps) è abilitata, il lettore di schede emette un segnale acustico quando si attivano l'allarme intrusione o l'allarme di timeout.
Allarme timeout sblocco	

Passaggio 9: Fare clic su "**Avanti**" (Next).

Viene generato un diagramma di cablaggio sulla base delle configurazioni dell'utente. È possibile effettuare il cablaggio del dispositivo seguendo il diagramma.

La figura seguente serve solo come riferimento.

Figura 2-8 Diagramma di cablaggio



Passaggio 10: Fare clic su **Applica** (Apply).

- Accedere a **Config. dispositivi locali** > **Hardware** (Local Device Config > Hardware) per modificare le impostazioni dopo avere effettuato l'accesso alla piattaforma.
- Fare clic su **Scarica immagine** (Download Image) per scaricare il diagramma sul computer.

2.2.4 Dashboard

Una volta effettuato l'accesso, viene mostrata la pagina della dashboard della piattaforma. La dashboard mostra i dati visualizzati.

Figura 2-9 Dashboard

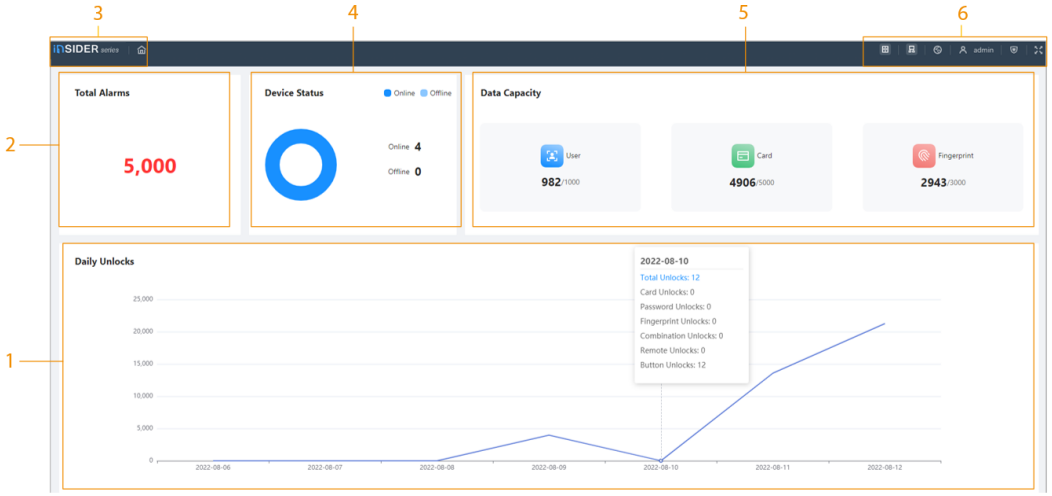


Tabella 2-4 Descrizione della pagina iniziale

N.	Descrizione
1	Mostra i metodi di sblocco utilizzati nei vari giorni. Passare il mouse sopra un giorno per visualizzare il tipo di sblocchi usati in quella data.
2	Mostra il numero totale di allarmi.
3	● Fare clic su iNSIDER series per accedere alla pagina della dashboard. ● Fare clic su per accedere alla pagina iniziale della piattaforma.
4	Mostra lo stato dei dispositivi offline e online.
5	Mostra i dati relativi al numero di schede, impronte digitali e utenti.
6	● Il numero di porte del controller. ◇ : Porta doppia ◇ : Porta singola ● Il tipo di controller. ◇ : Controller principale. ◇ : Controller secondario. ● : Selezione della lingua del dispositivo. ● : Accesso diretto alla pagina **Sicurezza** (Security). ● : Riavvio o uscita dalla piattaforma. ● : Mostra la pagina web a schermo intero.

2.2.5 Pagina iniziale

Una volta effettuato l'accesso, viene mostrata la pagina iniziale del controller principale.

Figura 2-10 Pagina iniziale

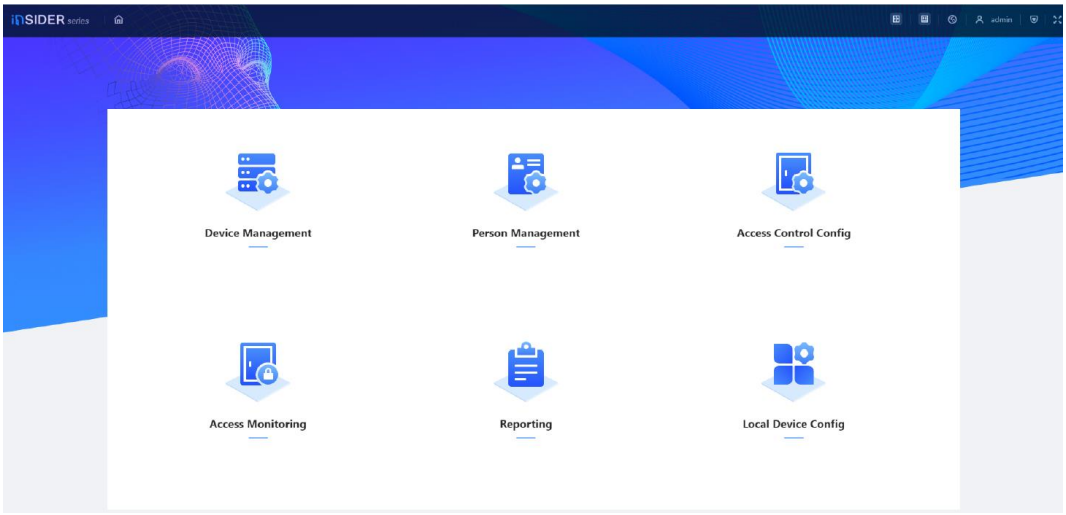


Tabella 2-5 Descrizione della pagina iniziale

Menu	Descrizione
Gestione dispositivo	Aggiunta dei dispositivi alla piattaforma del controller principale.
Gestione persone	Aggiunta del personale e assegnazione dei gruppi di autorizzazioni.
Configurazione controllo degli accessi	Aggiunta dei modelli orari, creazione e assegnazione dei gruppi di autorizzazioni, configurazione dei parametri delle porte e dei collegamenti di allarme globali, visualizzazione dello stato di avanzamento dell'assegnazione delle autorizzazioni.
Monitoraggio degli accessi	Controllo remoto delle porte e visualizzazione dei log degli eventi.
Reportistica	Visualizzazione ed esportazione dei record di allarme e di sblocco.
Configurazione dispositivi locali	Configurazione dei parametri dei dispositivi locali, come quelli di rete e dei collegamenti di allarme locali.

2.2.6 Aggiunta dei dispositivi

I dispositivi possono essere aggiunti alla piattaforma di gestione del controller principale uno per volta o in serie. Se il controller è stato impostato come controller principale durante la procedura guidata di accesso, è possibile aggiungere e gestire i controller secondari tramite la piattaforma.

Solo il controller principale è dotato di una piattaforma di gestione.

2.2.6.1 Aggiunta individuale dei dispositivi

Per aggiungere i controller secondari uno per volta, è necessario inserirne gli indirizzi IP o i nomi di dominio.

Procedura

Passaggio 1: Nella pagina iniziale, fare clic prima su **Gestione dispositivo** (Device Management), poi su **Aggiungi** (Add).

Passaggio 2: Inserire le informazioni relative al dispositivo.

Figura 2-11 Informazioni sul dispositivo

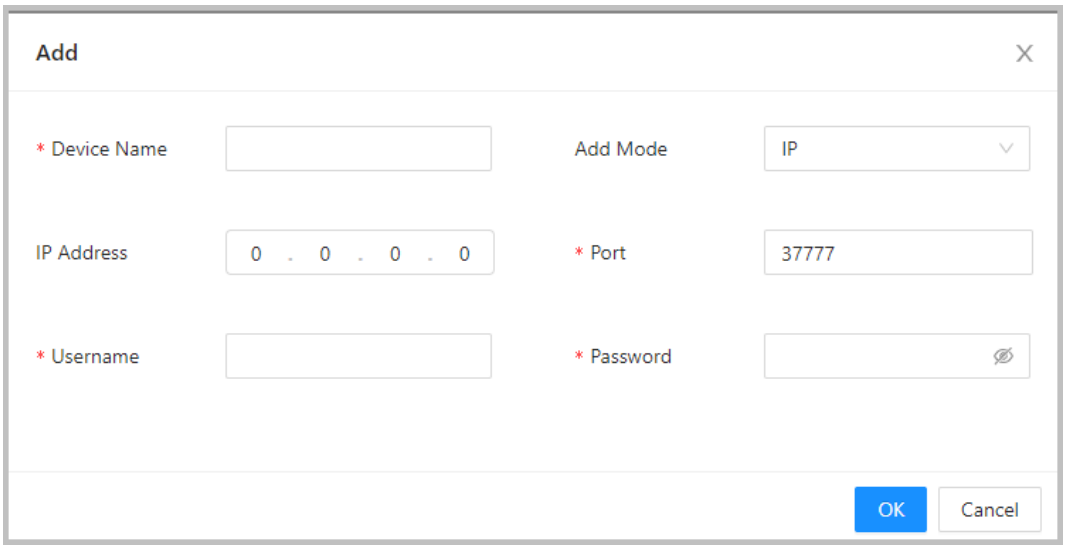


Tabella 2-6 Descrizione dei parametri del dispositivo

Parametro	Descrizione
Nome dispositivo	Inserire il nome del controller. Consigliamo di scegliere il nome sulla base della zona di installazione.
Modalità di aggiunta	Selezionare **IP** per aggiungere il controller degli accessi inserendone l'indirizzo IP.
Indirizzo IP	Inserire l'indirizzo IP del controller.
Porta	Il numero di porta predefinito è 37777.
Nome utente/password	Inserire il nome utente e la password del controller.

Passaggio 3: Fare clic su **OK**.

I controller aggiunti vengono mostrati nella pagina **Gestione dispositivo** (Device Management).

Figura 2-12 Dispositivi aggiunti correttamente

Se è stato impostato come controller principale durante la procedura guidata di accesso, il controller verrà aggiunto automaticamente alla piattaforma di gestione e funzionerà sia come controller principale che come controller secondario.

Operazioni correlate

- : Modifica delle informazioni sul dispositivo.
- Le operazioni che seguono sono supportate solo dai controller secondari.
  : Accesso alla pagina web del controller secondario.
- : Logout del dispositivo.
  : Eliminazione del dispositivo.

2.2.6.2 Aggiunta dei dispositivi in serie

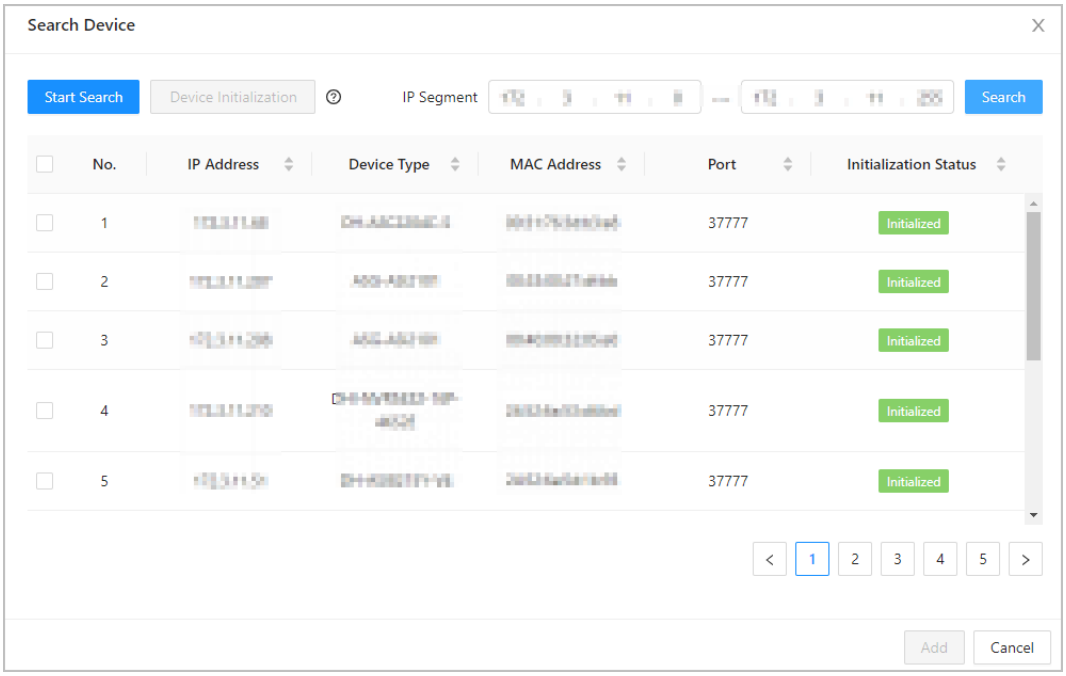
Quando si aggiungono i controller secondari in serie, è consigliabile utilizzare la funzione di ricerca automatica. Accertarsi che i controller secondari che si desidera aggiungere si trovino sullo stesso segmento di rete.

Procedura

Passaggio 1: Nella pagina iniziale, fare clic prima su **Gestione dispositivo** (Device Management), poi su **Cerca dispositivo** (Search Device).

- Fare clic su **Avvia ricerca** (Start Search) per cercare i dispositivi sulla stessa LAN. Inserire un intervallo per il segmento di rete e fare clic su **Cerca** (Search).

Figura 2-13 Ricerca automatica



Vengono mostrati tutti i dispositivi ricercati.

È possibile inizializzare i dispositivi in serie selezionandoli dall'elenco e facendo clic su **Inizializzazione dispositivo** (Device Initialization).

Per garantire la sicurezza dei dispositivi, non è possibile inizializzare dispositivi su segmenti di rete diversi.

Passaggio 2: Selezionare i controller che si desidera aggiungere alla piattaforma, quindi fare clic su **Aggiungi** (Add).

Passaggio 3: Inserire il nome utente e la password dei controller secondari e fare clic su **OK**.

I controller secondari aggiunti vengono mostrati sulla pagina **Gestione dispositivo** (Device Management).

Operazioni correlate

- Modifica IP: selezionare i dispositivi aggiunti e fare clic su **Modifica IP** (Modify IP) per modificarne gli indirizzi IP.
- Sincronizza ora: selezionare i dispositivi aggiunti e fare clic su **Sincronizza ora** (Sync Time) per sincronizzare l'ora dei dispositivi con il server NTP.
- Elimina: selezionare i dispositivi e fare clic su **Elimina** (Delete) per eliminarli.

2.2.7 Aggiunta degli utenti

È possibile aggiungere utenti, inserire le informazioni di base che li riguardano e impostare i metodi per verificarne l'identità.

Procedura

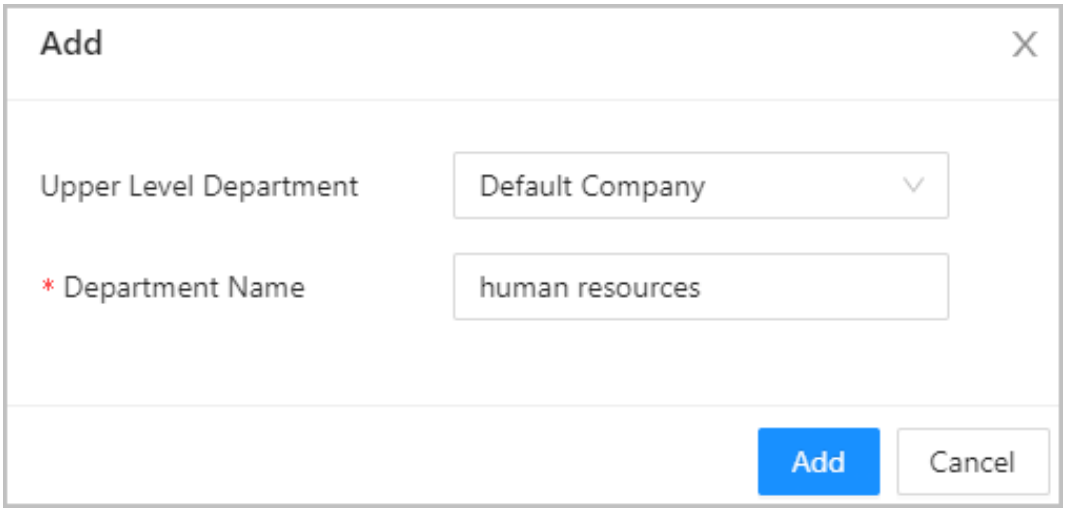
Passaggio 1: Nella pagina iniziale, selezionare **Gestione persone** (Person Management).

Passaggio 2: Creare un reparto.

1. Fare clic su ＋.
2. Inserire il nome del reparto e fare clic su **Aggiungi** (Add).

L'azienda predefinita non può essere eliminata.

Figura 2-14 Aggiunta di un reparto



Passaggio 3: Prima di assegnare le schede agli utenti, impostarne il tipo e il sistema di numerazione (opzionale).

1. Sulla pagina **Gestione persone** (Person Management), selezionare **Altro > Tipo di scheda** (More > Card Type).
2. Selezionare scheda ID o IC e fare clic su **OK**.

   Accertarsi che il tipo di scheda corrisponda a quello della scheda assegnata, altrimenti non sarà possibile leggere il numero di quest'ultima. Ad esempio, se si assegna una scheda ID, impostare il tipo di scheda su ID.
3. Selezionare **Altro > Sistema di numerazione schede** (More > Card No. System).
4. Selezionare il sistema di numerazione in formato decimale o esadecimale.

Passaggio 4: Aggiungere gli utenti.

- Aggiunta degli utenti uno per volta.

  Quando si desidera assegnare le autorizzazioni di accesso a una persona, è possibile aggiungere gli utenti singolarmente. Per informazioni dettagliate su come assegnare le autorizzazioni di accesso, consultare la sezione "2.2.9 Aggiunta dei gruppi di autorizzazioni".

  1. Fare clic su **Aggiungi** (Add) e inserire le informazioni di base relative all'utente.

Figura 2-15 Informazioni di base sull'utente

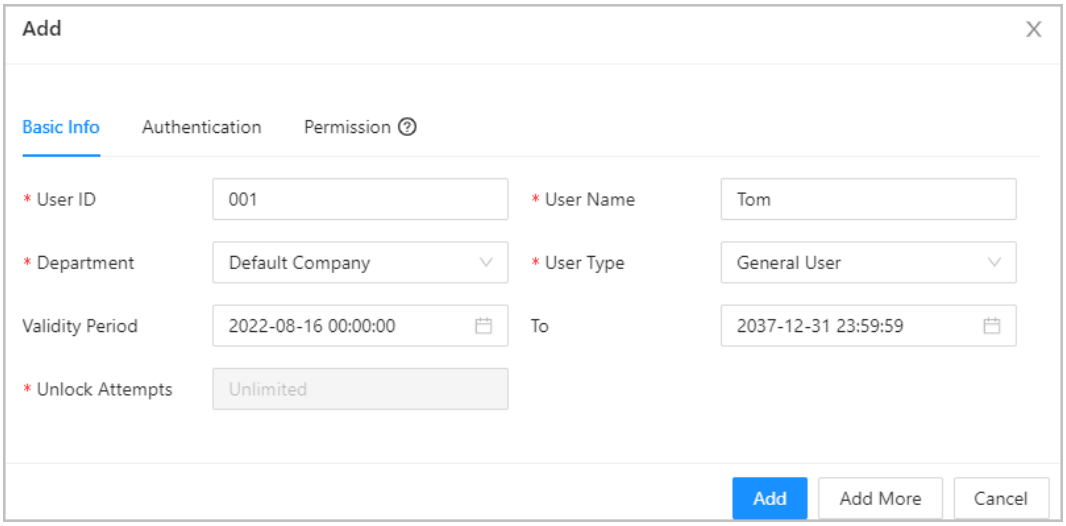


Tabella 2-7 Descrizione dei parametri

Parametro	Descrizione
ID utente	L'ID dell'utente.
Reparto	Il reparto a cui appartiene l'utente.
Inizio validità	Impostare la data in cui le autorizzazioni di accesso dell'utente diventano effettive.
Fine validità	Impostare la data in cui le autorizzazioni di accesso dell'utente scadono.
Nome utente	Il nome dell'utente.
Tipo di utente	Il tipo dell'utente. ● **Utente generico**: gli utenti generici possono sbloccare le porte. **Utente VIP**: quando gli utenti VIP sbloccano una porta, il personale di servizio riceve una notifica. ● **Utente ospite**: gli ospiti possono sbloccare le porte entro un periodo di tempo prestabiliti o per il numero di volte impostato. Una volta trascorso il periodo di tempo o esaurito il numero di ● tentativi impostati, gli ospiti non potranno più sbloccare le porte. **Utente di pattuglia**: gli utenti di pattuglia non hanno l'autorizzazione a sbloccare le porte, ma le loro presenze vengono monitorate. ● **Utente bloccato**: quando gli utenti presenti nell'elenco delle persone non autorizzate sbloccano una porta, il personale di ● servizio riceve una notifica. **Utente di altro tipo**: quando questi utenti sbloccano una porta, la porta resta aperta per 5 secondi aggiuntivi.
Tentativi di sblocco	Il numero di tentativi di sblocco degli ospiti.

2. Fare clic su **Aggiungi** (Add).
   Fare clic su **Aggiungi altri** (Add More) per aggiungere altri utenti.

- Aggiunta degli utenti in serie.
  1. Fare clic su **Importa** > **Scarica modello** (Import > Download Template) per scaricare il modello per gli utenti.

2. Inserire le informazioni sugli utenti nel modello e salvare quest'ultimo.
3. Fare clic su **Importa** (Import) e caricare il modello sulla piattaforma.
   Gli utenti vengono aggiunti automaticamente alla piattaforma.

Passaggio 5: Fare clic sulla scheda **Autenticazione** (Authentication) e impostare il metodo di autenticazione per verificare l'identità delle persone.

Ogni utente può avere una password, cinque schede e tre impronte digitali.

Tabella 2-8 Impostazione dei metodi di autenticazione

Metodo di autenticazione	Descrizione
Password	Inserire e confermare la password.
Scheda	● Inserimento manuale del numero di scheda. 1. Fare clic su **Aggiungi** (Add). 2. Inserire il numero della scheda e fare clic su **Aggiungi** (Add). ● Lettura automatica del numero tramite lettore di schede collegato al PC. 1. Fare clic su ⚙. 2. Selezionare **Lettore di schede collegato al PC** (Enrollment Reader) e fare clic su **OK**. Accertarsi che il lettore di schede sia collegato al computer. 3. Fare clic su **Aggiungi** (Add) e seguire le istruzioni a schermo per scaricare e installare il plug-in. 4. Passare la scheda sul lettore di schede collegato al PC. Viene mostrato un conto alla rovescia di 20 secondi per il passaggio della scheda; il sistema legge il numero di scheda automaticamente. Se il conto alla rovescia di 20 secondi termina, fare clic su **Leggi scheda** (Read Card) per riavviarlo. 5. Fare clic su **Aggiungi** (Add). ● Lettura automatica del numero tramite lettore di schede collegato al controller degli accessi. 1. Fare clic su ⚙. 2. Selezionare l'opzione **Dispositivo** (Dispositivo), scegliere il lettore di schede e fare clic su **OK**. Accertarsi che il lettore di schede sia collegato al controller degli accessi. 3. Passare la scheda sul lettore. Viene mostrato un conto alla rovescia di 20 secondi per il passaggio della scheda; il sistema legge il numero di scheda automaticamente. Se il conto alla rovescia di 20 secondi termina, fare clic su **Leggi scheda** (Read Card) per riavviarlo. 4. Fare clic su **Aggiungi** (Add).
Impronta digitale	Collegare uno scanner per le impronte digitali al computer e seguire le istruzioni a schermo per registrare l'impronta digitale.

Figura 2-16 Metodo di autenticazione

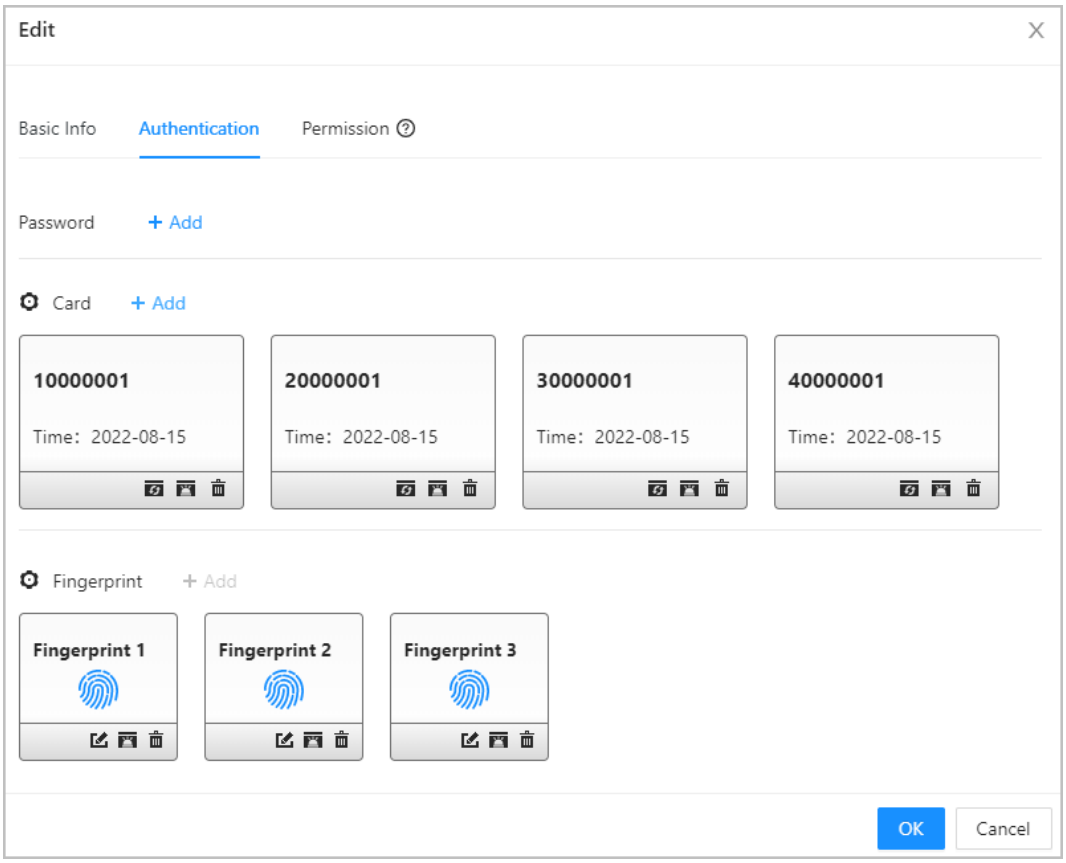


Tabella 2-9 Metodo di autenticazione

Parametro	Descrizione
Password	Gli utenti possono ottenere l'accesso inserendo la password.
Scheda	Gli utenti possono ottenere l'accesso passando la scheda. ● : modifica del numero della scheda. : impostazione della scheda come scheda coercizione. ● Quando si utilizza una scheda coercizione per aprire una porta, ● viene attivato un allarme. : Eliminazione della scheda.
Impronta digitale	Gli utenti possono ottenere l'accesso verificando l'impronta digitale.

Passaggio 6: Fare clic su **OK**.

Operazioni correlate

- Nella pagina **Gestione persone** (Person Management), fare clic su **Esporta** (Export) per
- esportare tutti gli utenti in un file Excel.
  Nella pagina **Gestione persone** (Person Management), fare clic su **Altro** > **Estrai** (More > Extract) e selezionare un dispositivo per esportare tutti gli utenti del controller secondario sulla piattaforma del controller principale.
- Nella pagina **Gestione persone** (Person Management), fare clic su **Altro** > **Tipo di scheda** (More > Card Type) per impostare il tipo di scheda prima di assegnare le schede agli utenti. Ad esempio, se si assegna una scheda ID, impostare il tipo di scheda su ID.

- Nella pagina **Gestione persone** (Person Management), fare clic su **Altro** > **Sistema di numerazione schede** (More > Card No. System) per impostare il sistema di numerazione delle schede in formato decimale o esadecimale.

2.2.8 Aggiunta di modelli orari

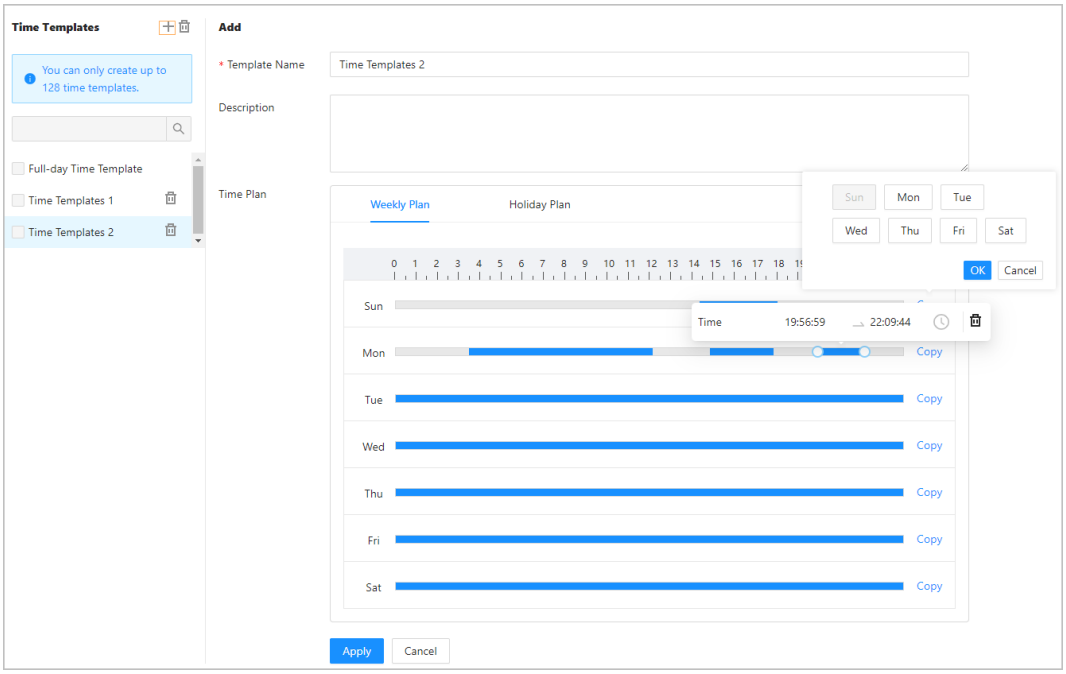
Un modello orario definisce le programmazioni di sblocco del controller. La piattaforma offre 4 modelli orari predefiniti. Inoltre, il modello è personalizzabile.

I modelli predefiniti non possono essere modificati.

Passaggio 1: Nella pagina iniziale, selezionare **Config. controllo degli accessi** > **Modello orario** (Access Control Config > Time Template) e fare clic su +.

Passaggio 2: Inserire il nome del modello orario.

Figura 2-17 Creazione dei modelli orari



- Il modello orario per la giornata piena non è modificabile.
- È possibile creare un massimo di 128 modelli orari.

Passaggio 3: Trascinare il cursore per modificare la fascia oraria dei vari giorni.

È anche possibile fare clic su **Copia** (Copy) per applicare l'orario impostato ad altri giorni.

È possibile configurare un massimo di 4 fasce orario per giorno.

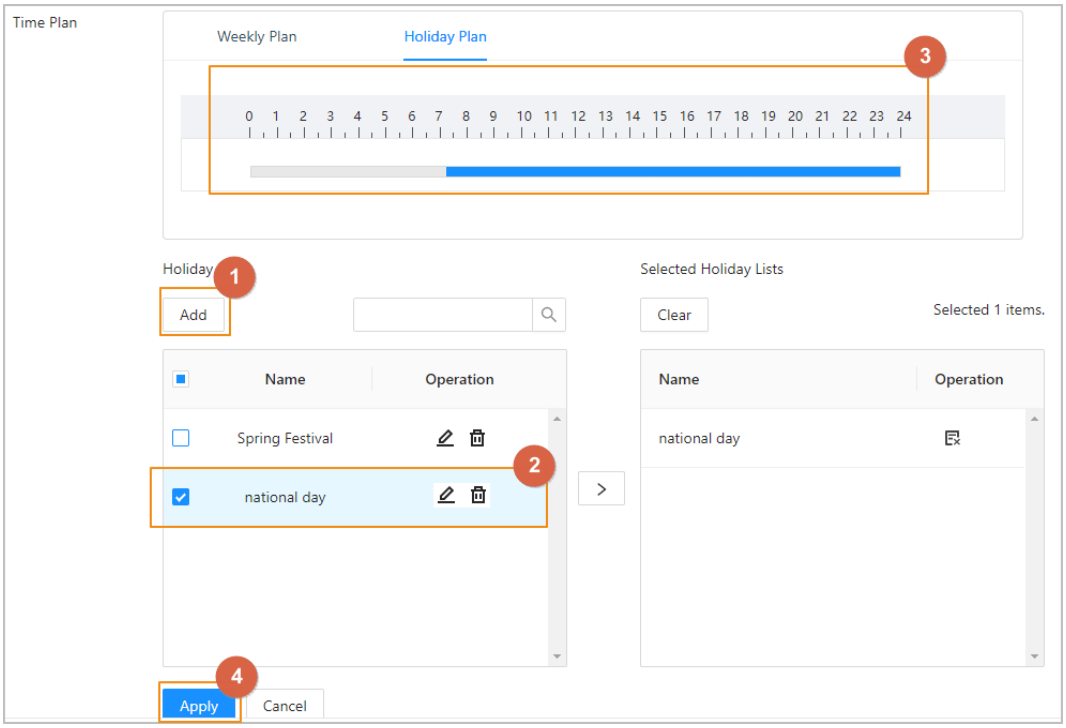
Passaggio 4: Fare clic su **Applica** (Apply).

Passaggio 5: Configurare i piani ferie.

1. Fare clic prima sulla scheda **Piano ferie** (Holiday Plan), poi su **Aggiungi** (Add) per aggiungere delle ferie.
   È possibile aggiungere un massimo di 64 ferie.
2. Selezionare un periodo di ferie.

3. Trascinare il cursore per modificare la fascia oraria delle ferie.
4. Fare clic su **Applica** (Apply).

Figura 2-18 Creazione dei piani ferie



2.2.9 Aggiunta dei gruppi di autorizzazioni

Un gruppo di autorizzazioni raccoglie le autorizzazioni di accesso alle porte in una fascia oraria prestabilita. Creare un gruppo di autorizzazioni e associarvi degli utenti consente di assegnare le autorizzazioni di accesso del gruppo agli utenti che ne fanno parte.

Passaggio 1: Fare clic su **Config. controllo degli accessi** > **Impostazioni autorizzazioni** (Access Control Config > Permission Settings).

Passaggio 2: Fare clic su ＋.

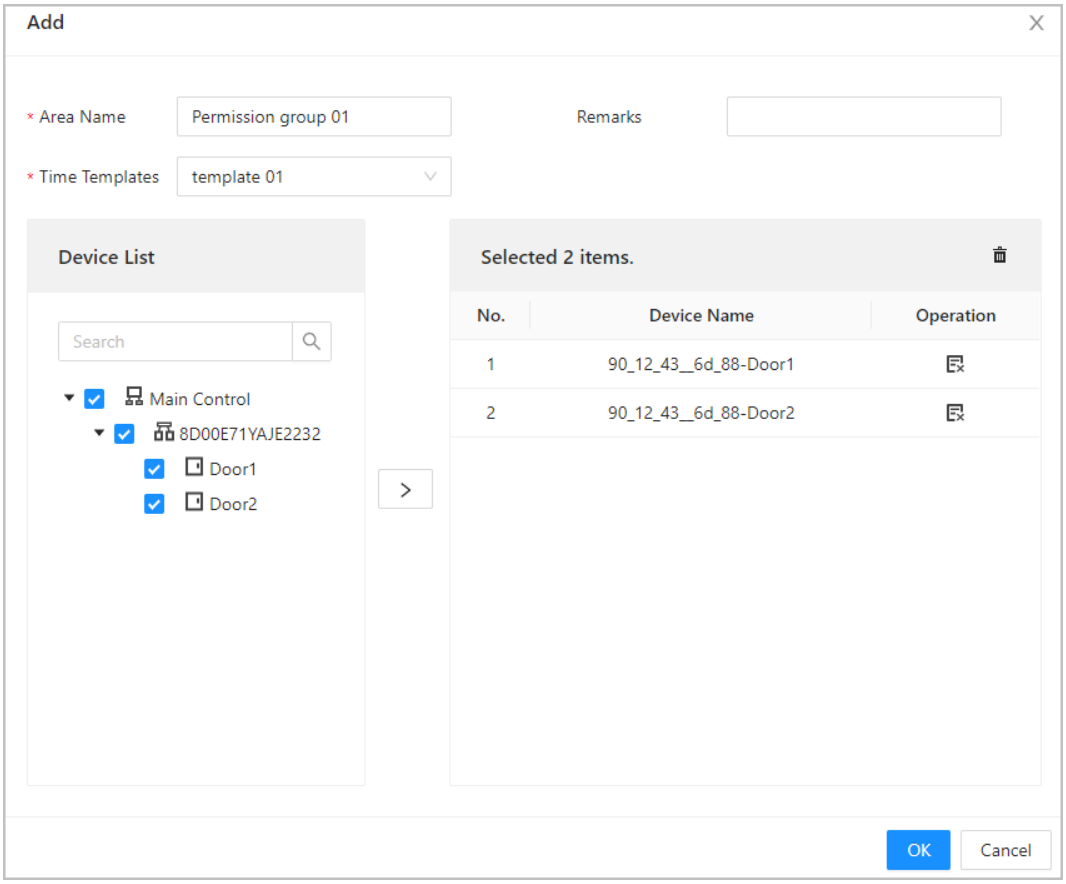
È possibile aggiungere un massimo di 128 gruppi di autorizzazioni.

Passaggio 3: Inserire il nome del gruppo di autorizzazioni, le note (opzionale) e selezionare un modello orario.

Passaggio 4: Selezionare le porte.

Passaggio 5: Fare clic su **OK**.

Figura 2-19 Creazione dei gruppi di autorizzazioni



2.2.10 Assegnazione dei gruppi di autorizzazioni

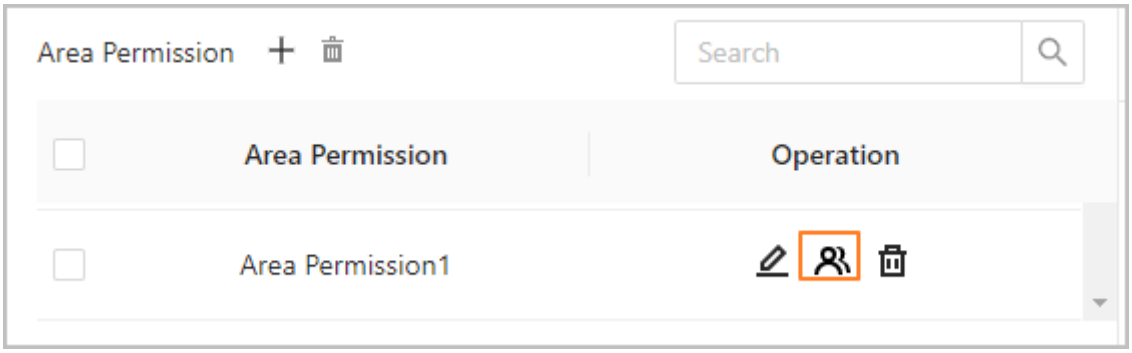
È possibile assegnare le autorizzazioni di accesso agli utenti collegando questi ultimi ai gruppi di autorizzazioni. IN questo modo, gli utenti possono ottenere l'accesso alle aree sicure.

Passaggio 1: Nella pagina iniziale, selezionare **Config. controllo degli accessi** > **Impostazioni autorizzazioni** (Access Control Config > Permission Settings).

Passaggio 2: Fare clic su per selezionare un gruppo di autorizzazioni esistente, quindi selezionare gli utenti di un reparto.

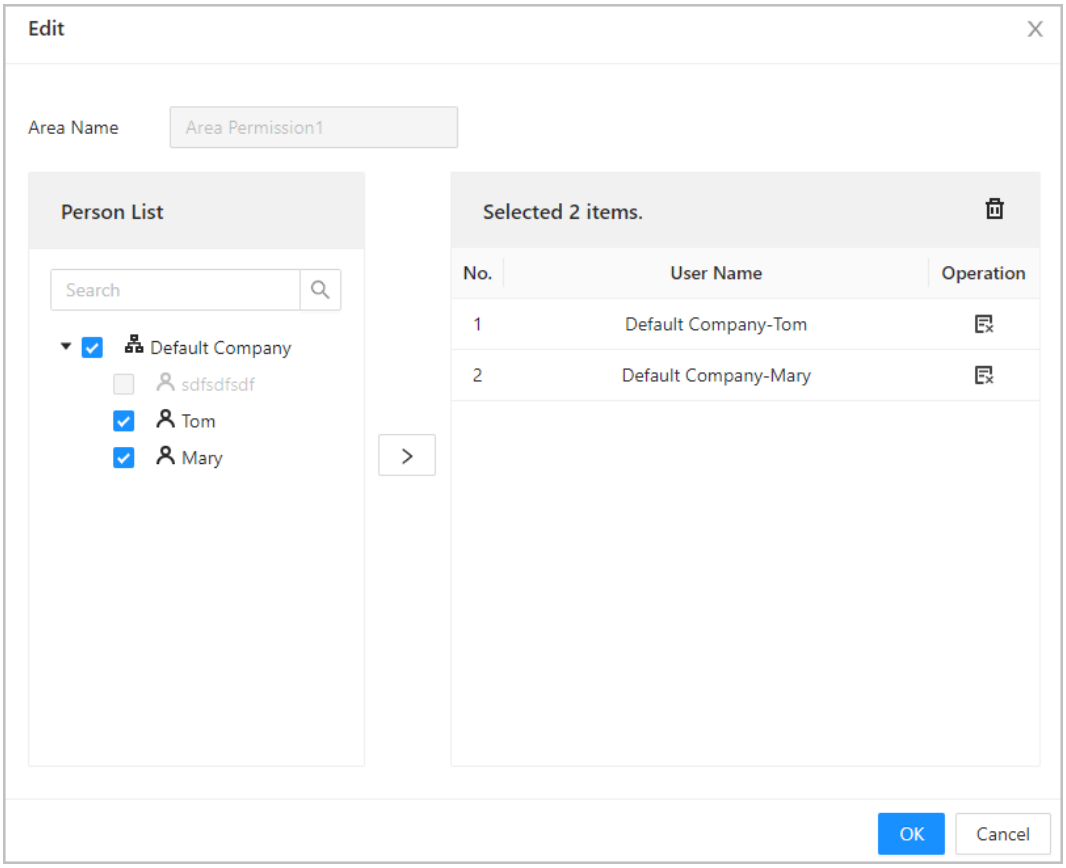
È possibile selezionare un intero reparto.

Figura 2-20 Selezione degli utenti



Fare clic su + per creare un nuovo gruppo di autorizzazioni. Per informazioni dettagliate su come creare i gruppi di autorizzazioni, consultare la sezione "2.2.9 Aggiunta dei gruppi di autorizzazioni".

Figura 2- 21 Assegnazione in serie delle autorizzazioni



Passaggio 3: Fare clic su **OK**.

Operazioni correlate

È possibile assegnare le autorizzazioni di accesso a una nuova persona o modificare quelle di una persona esistente con operazioni individuali.

1. Nella pagina iniziale, selezionare **Gestione persone** (Person Management).
2. Selezionare prima il reparto, poi un utente esistente.

   Se l'utente non è stato aggiunto in precedenza, fare clic su **Aggiungi** (Add) per aggiungerlo. Per informazioni dettagliate sulla creazione di un utente, consultare la sezione "2.2.7 Aggiunta degli utenti".
3. Fare clic sull'icona corrispondente all'utente.
4. Sulla scheda **Autorizzazioni** (Permission), selezionare i gruppi di autorizzazioni esistenti.

- Fare clic su **Aggiungi** (Add) per creare nuovi gruppi di autorizzazioni. Per informazioni dettagliate su come creare i gruppi di autorizzazioni, consultare la sezione "2.2.9 Aggiunta dei gruppi di autorizzazioni".
- È possibile collegare più gruppi di autorizzazioni a un utente.

5. Fare clic su **OK**.

2.2.11 Visualizzazione dello stato di avanzamento delle autorizzazioni

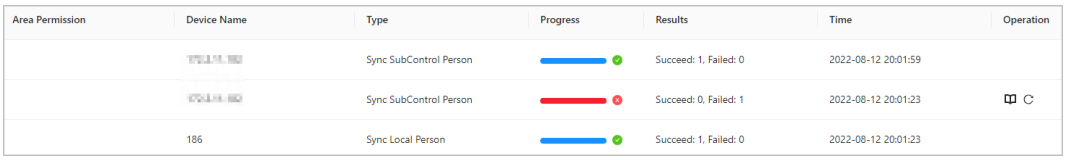
Una volta assegnate le autorizzazioni agli utenti, è possibile visualizzare lo stato di avanzamento della procedura.

Passaggio 1: Nella pagina iniziale, selezionare **Config. controllo degli accessi** > **Avanzamento autorizzazioni** (Access Control Config > Authorization Progress).

Passaggio 2: Visualizzare lo stato di avanzamento delle autorizzazioni.

- Sincronizza persona sul controller secondario: sincronizzazione del personale sul controller principale con quello secondario.
- Sincronizza persona locale: sincronizzazione del personale della piattaforma di gestione con il suo server.
- Sincronizza orario locale: sincronizzazione dei modelli orari nei gruppi di autorizzazioni con il controller secondario.

Figura 2-22 Stato di avanzamento delle autorizzazioni



Passaggio 3: Se un'attività di autorizzazione non riesce, fare clic su per riprovare (opzionale).

Fare clic su per visualizzare i dettagli sull'attività di autorizzazione non riuscita.

2.2.12 Configurazione del controllo degli accessi (opzionale)

2.2.12.1 Configurazione dei parametri di base

Passaggio 1: Selezionare **Config. controllo degli accessi** > **Parametri porta** (Access Control Config > Door Parameters).

Passaggio 2: Nella finestra **Impostazioni di base** (Basic Settings), configurare i parametri di base del controllo degli accessi.

Figure 2-23 Parametri di base

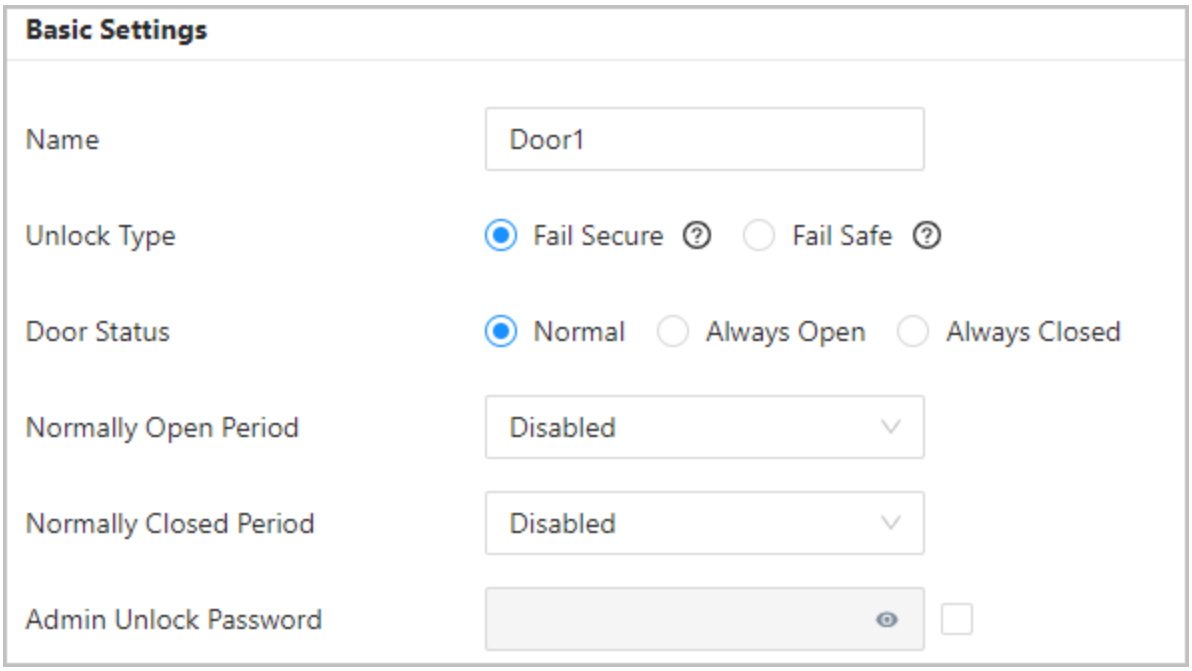


Tabella 2-10 Descrizione dei parametri di base

Parametro	Descrizione
Nome	Il nome della porta.
Tipo di sblocco	● Se durante la procedura guidata di accesso è stata selezionata l'opzione **12 V** per alimentare la serratura tramite controller, è possibile scegliere tra le opzioni Sicurezza guasti e Protezione guasti. ◇ Protezione guasti: quando si verifica un'interruzione di corrente o un guasto all'alimentazione, la porta resta ◇ chiusa. Sicurezza guasti: quando si verifica un'interruzione di corrente o un guasto all'alimentazione, la porta si apre automaticamente per consentire alle persone di uscire. ● Se durante la procedura guidata di accesso è stata selezionata l'opzione **Relè** (Relay) per alimentare la serratura tramite relè, è possibile scegliere tra le opzioni Relè aperto e Relè chiuso. ◇ Relè aperto = blocco: la serratura rimane bloccata quando ◇ il relè è aperto. Relè aperto = sblocco: la serratura si sblocca quando il relè è aperto.
Stato porta	Impostazione dello stato della porta. ● **Normale**: la porta sarà sbloccata o bloccata a seconda delle ● impostazioni. **Sempre aperta**: la porta resta sempre sbloccata. ● **Sempre chiusa**: la porta resta sempre bloccata.

Parametro	Descrizione
Fascia oraria normalmente aperta	Scegliendo **Normale** (Normal), è possibile selezionare un modello orario dall'elenco a discesa. La porta resta aperta o chiusa durante la fascia oraria stabilita.
Fascia oraria normalmente chiusa	
Password sblocco amministratore	Attivazione della funzione sblocco amministratore e successivo inserimento della password dell'amministratore. L'amministratore può sbloccare la porta semplicemente inserendo la sua password.

2.2.12.2 Configurazione dei metodi di sblocco

È possibile utilizzare metodi diversi per sbloccare una porta, come il riconoscimento del volto o dell'impronta digitale, la scheda oppure la password. È anche possibile combinare i metodi di sblocco per crearne uno personalizzato.

Passaggio 1: Selezionare **Config. controllo degli accessi** > **Parametri porta** (Access Control Config > Door Parameters).

Passaggio 2: Nella finestra **Impostazioni di sblocco** (Unlock Settings), selezionare una modalità di sblocco.

- Sblocco combinato
  1. Selezionare l'opzione **Sblocco combinato** (Combination Unlock) dall'elenco **Modalità di sblocco** (Unlock Mode).
  2. Selezionare **O** (Or) oppure **E** (And).
     - O: utilizza uno dei metodi di sblocco selezionati per aprire la porta.
       E: utilizza tutti i metodi di sblocco selezionati per aprire la porta.
       Il controller supporta lo sblocco tramite scheda, impronta digitale o password.
  3. Selezionare i metodi di sblocco e configurare gli altri parametri.

Figura 2-24 Impostazioni di sblocco

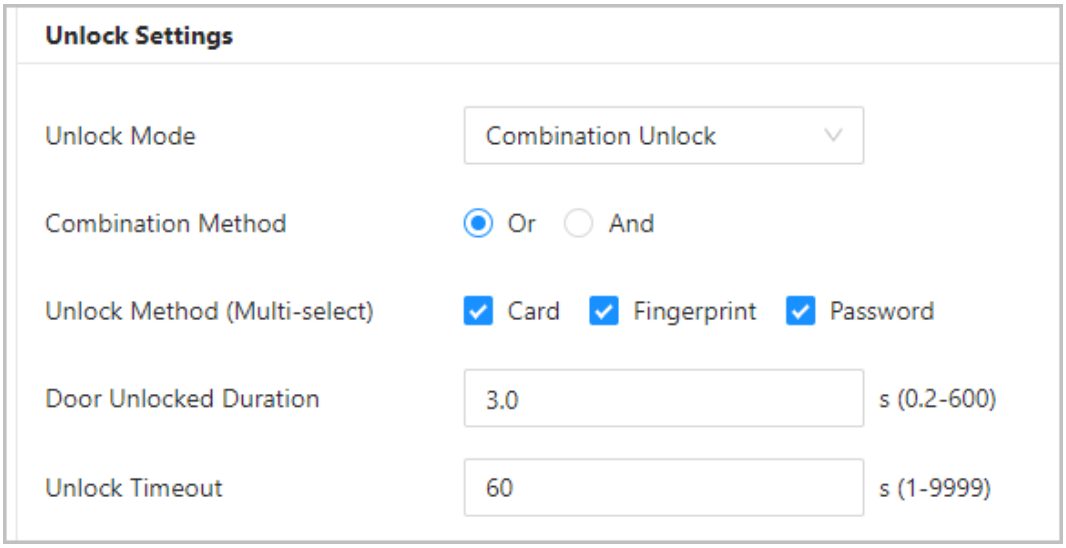


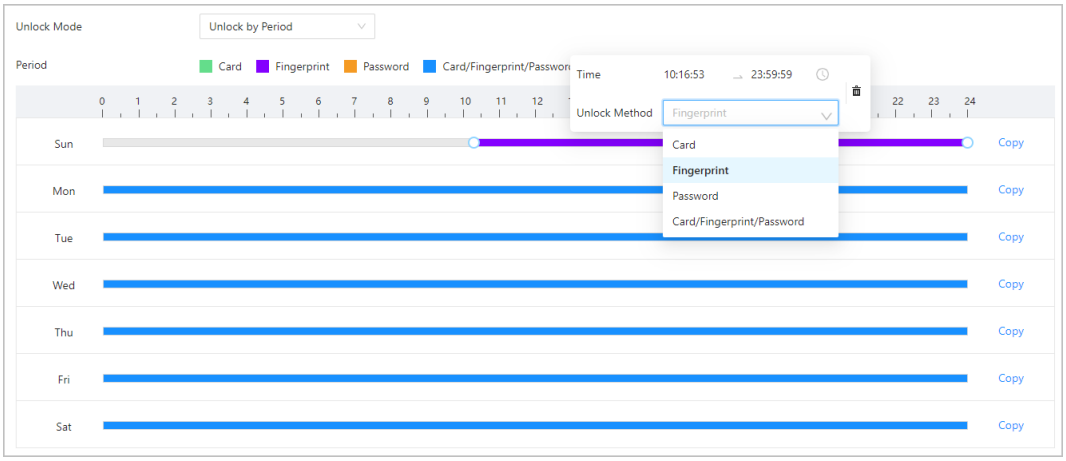
Tabella 2-11 Descrizione delle impostazioni di sblocco

Parametro	Descrizione
Durata sblocco porta	Quando viene autorizzato l'accesso di una persona, la porta resta sbloccata per un periodo di tempo definito che consenta alla persona di entrare. I valori selezionabili sono compresi tra 0,2 e 600 secondi.
Timeout sblocco	Quando la porta resta sbloccata più a lungo del tempo impostato, si attiva un allarme di timeout.

- Sblocco per fascia oraria
  1. Nell'elenco **Modalità di sblocco** (Unlock Mode), selezionare **Sblocco per fascia oraria** (Unlock by Period).
  2. Trascinare il cursore per modificare la fascia oraria dei vari giorni.

     È anche possibile fare clic su **Copia** (Copy) per applicare l'orario impostato ad altri giorni.
  3. Selezionare un metodo di sblocco per la fascia oraria, quindi configurare gli altri parametri.

Figura 2-25 Sblocco per fascia oraria



Passaggio 3: Fare clic su **Applica** (Apply).

2.2.12.3 Configurazione degli allarmi

Gli allarmi vengono attivati quando si verifica un evento anomalo.

Passaggio 1: Selezionare **Config. controllo degli accessi** > **Parametri porta** > **Impostazioni allarme** (Access Control Config > Door Parameters > Alarm Settings).

Passaggio 2: Configurare i parametri di allarme.

Figura 2-26 Allarme

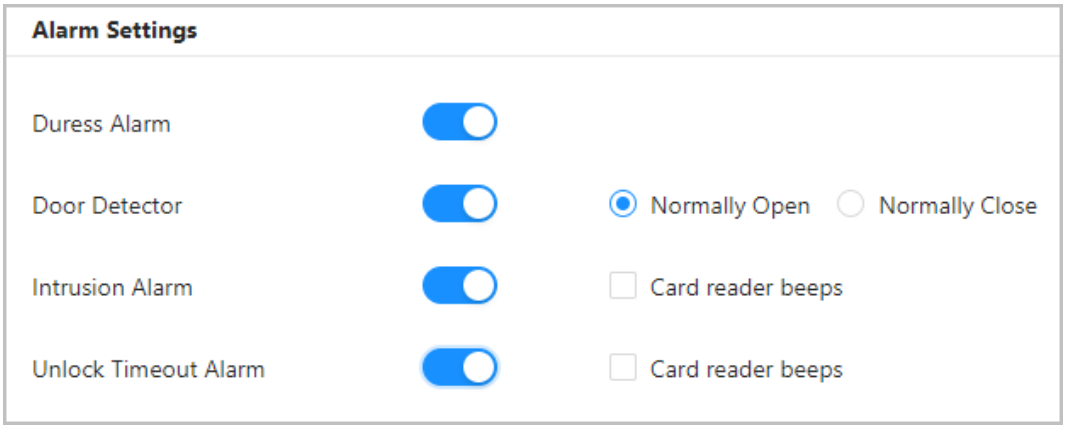


Tabella 2-12 Descrizione dei parametri di allarme

Parametro	Descrizione
Allarme coercizione	Un allarme si attiva se una scheda, una password o un'impronta coercizione viene utilizzata per sbloccare la porta.
Rilevatore per porte	Selezionare il tipo di rilevatore per porte.
Allarme intrusione	• Quando il rilevatore per porte è abilitato, se la porta viene aperta in modo anomalo si attiva un allarme intrusione. • Se la porta resta sbloccata più a lungo del tempo impostato, si attiva un allarme di timeout. • Quando l'opzione **Segnale acustico lettore di schede** (Card reader beeps) è abilitata, il lettore di schede emette un segnale acustico quando si attivano l'allarme intrusione o l'allarme di timeout.
Allarme timeout sblocco	

Passaggio 3: Fare clic su **Applica** (Apply).

2.2.13 Configurazione dei collegamenti di allarme globali (opzionale)

È possibile configurare i collegamenti di allarme globali su più controller degli accessi.

Informazioni preliminari

Se si configurano sia i collegamenti di allarme globali che quelli locali, qualora i due tipi di collegamenti siano in conflitto hanno effetto solamente gli ultimi collegamenti effettuati.

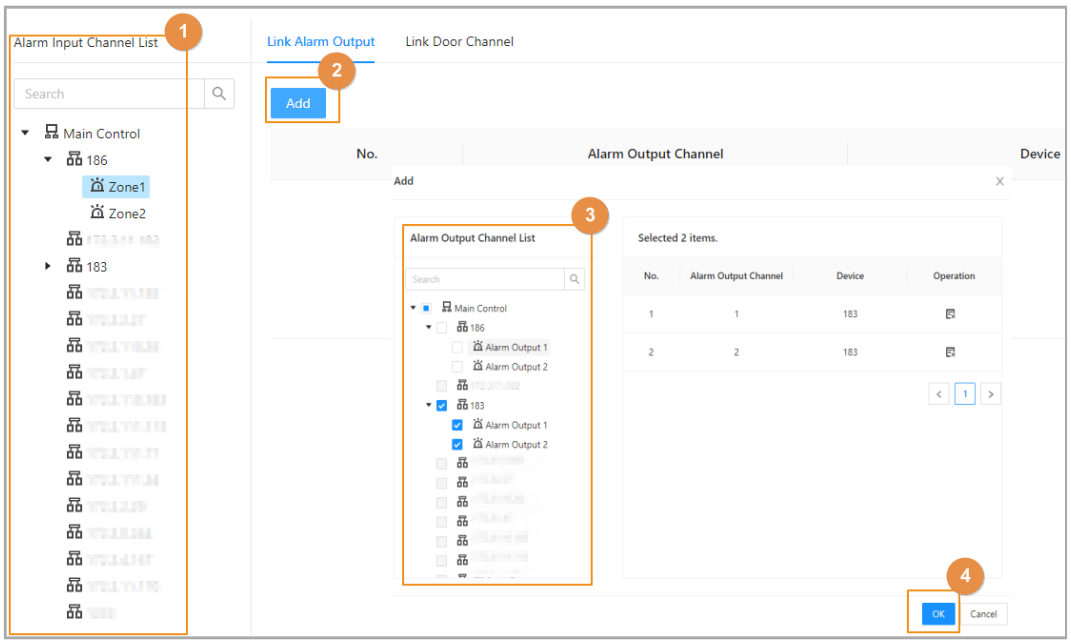
Procedura

Passaggio 1: Selezionare **Config. controllo degli accessi** > **Collegamento allarmi globali** (Access Control Config > Global Alarm Linkage).

Passaggio 2: Configurare l'uscita allarme.

1. Selezionare uno dei canali di ingresso allarme presenti nel relativo elenco, quindi fare clic su **Collega uscita di allarme** (Link Alarm Output).
2. Fare clic su **Aggiungi** (Add), selezionare un canale di uscita allarme, quindi fare clic su **OK**.

Figura 2-27 Uscita allarme

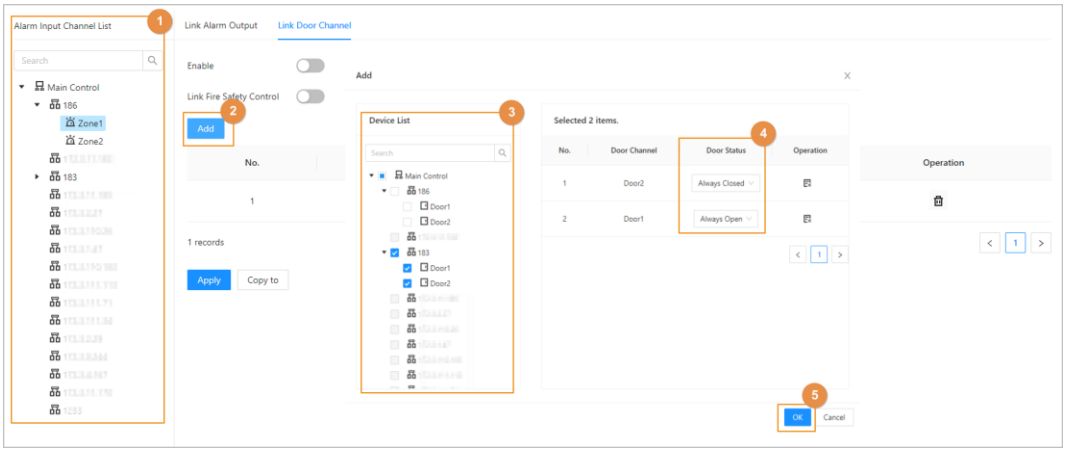


3. Attivare la funzione di uscita allarme e inserire la durata dell'allarme.
4. Fare clic su **Applica** (Apply).

Passaggio 3: Configurare il collegamento alle porte.

1. Selezionare un ingresso di allarme dall'elenco dei canali, quindi fare clic su **Aggiungi** (Add).
2. Selezionare prima le porte collegate, poi il loro stato, quindi fare clic su **OK**.
   - Sempre chiusa: la porta si blocca automaticamente quando viene attivato l'allarme.
   - Sempre aperta: la porta si sblocca automaticamente quando viene attivato l'allarme.

Figura 2-28 Collegamento alle porte



3. Fare clic su **Abilita** per attivare la funzione di collegamento alle porte.

Abilitando l'opzione Collega sicurezza antincendio, tutti i collegamenti vengono impostati automaticamente sullo stato **Sempre aperto** e tutte le porte si aprono quando si attiva l'allarme antincendio.

4. Fare clic su **Applica** (Apply).
   Fare clic su **Copia su** (Copy to) per applicare i collegamenti di allarme preconfigurati agli altri ingressi allarme.

2.2.14 Monitoraggio degli accessi (opzionale)

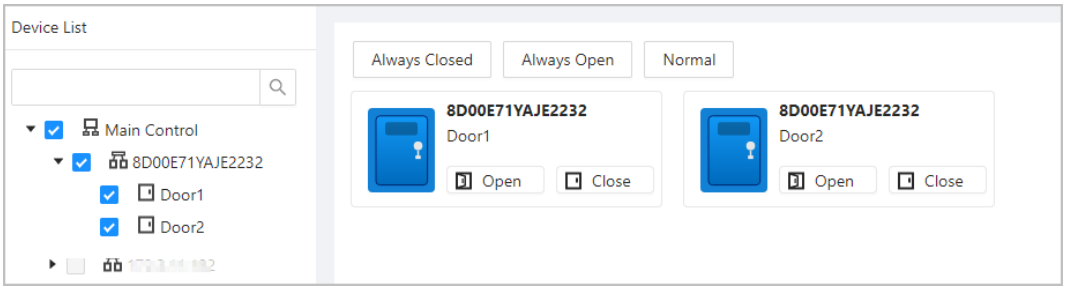
2.2.14.1 Apertura e chiusura delle porte da remoto

È possibile monitorare e controllare le porte da remoto. Ad esempio, le porte possono essere aperte o chiuse da remoto.

Procedura

Passaggio 1: Fare clic su **Monitoraggio degli accessi** (Access Monitoring) nella pagina iniziale.
Passaggio 2: Selezionare una porta e fare clic su **Apri** (Open) o **Chiudi** (Close) per controllarla da remoto.

Figura 2-29 Controllo di una porta da remoto



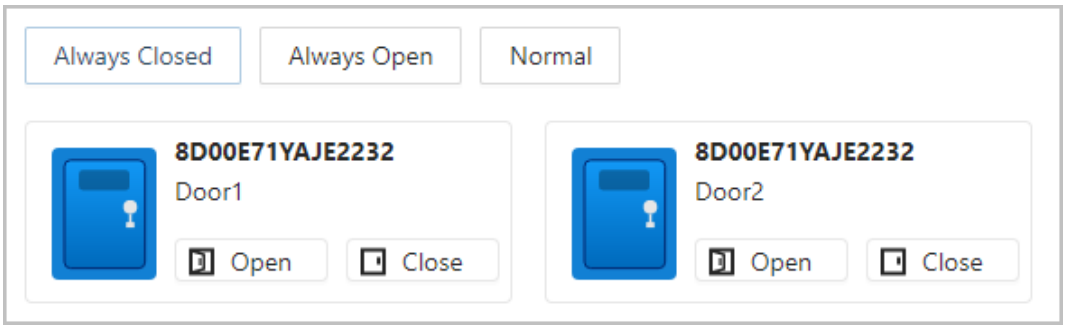
Operazioni correlate

- Filtraggio eventi: selezionare un tipo di evento nella sezione **Info evento** (Event Info) per visualizzare solo gli eventi di quel tipo, ad esempio gli eventi di allarme o gli eventi anomali.
- Eliminazione evento: fare clic su per cancellare tutti gli eventi dal relativo elenco.

2.2.14.2 Impostazioni Sempre aperta e Sempre chiusa

Quando si impostano le opzioni Sempre aperta o Sempre chiusa, la porta resta sempre aperta o sempre chiusa.
Passaggio 1: Fare clic su **Monitoraggio degli accessi** (Access Monitoring) nella pagina iniziale.
Passaggio 2: Fare clic su **Sempre aperta** (Always Open) o **Sempre chiusa** (Always Closed) per aprire o chiudere la porta.

Figura 2-30 Impostazioni Sempre aperta e Sempre chiusa



La porta resta sempre aperta o sempre chiusa. È possibile fare clic su **Normale** (Normal) per ripristinare il normale funzionamento del controllo degli accessi, in modo che la porta si apra e si chiuda usando i metodi di verifica configurati.

2.2.15 Configurazioni dei dispositivi locali (opzionale)

Le configurazioni dei dispositivi locali sono applicabili solo ai controller degli accessi locali.

2.2.15.1 Configurazione dei collegamenti di allarme locali

È possibile configurare i collegamenti di allarme locale su più controller degli accessi. Ogni controller ha due ingressi e due uscite di allarme.

Passaggio 1: Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Collegamento di allarme locale** (Local Device Config > Local Alarm Linkage).

Passaggio 2: Fare clic su per configurare un collegamento di allarme locale.

Figura 2-31 Collegamento di allarme locale

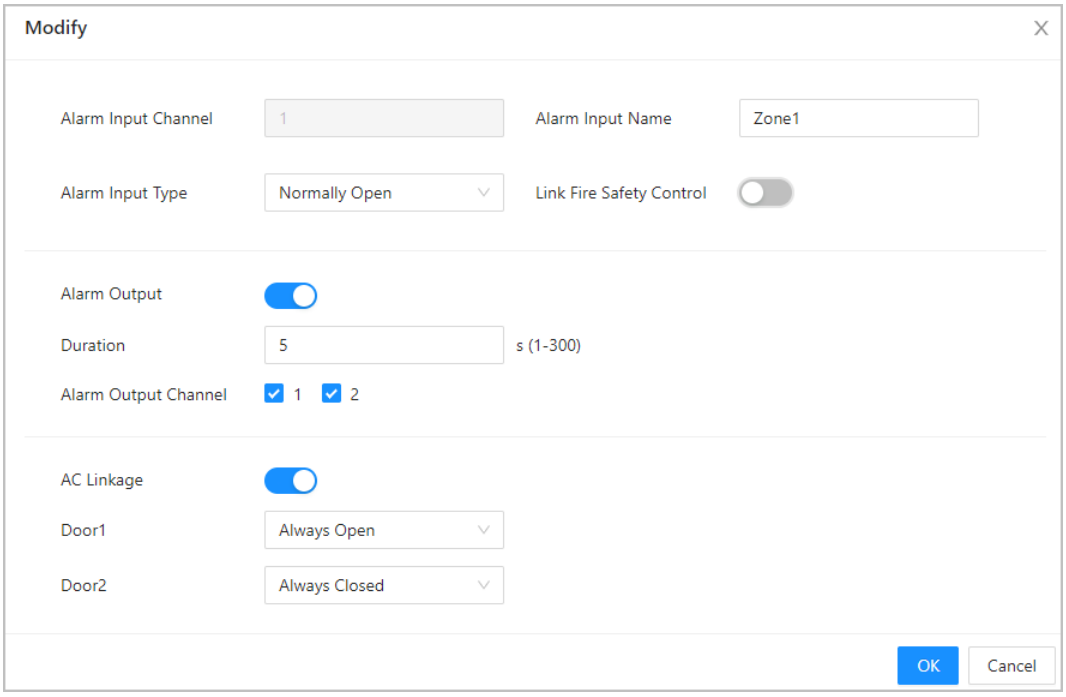


Tabella 2-13 Collegamento di allarme locale

Parametro	Descrizione
Canale ingresso allarme	Il numero di canale dell'ingresso allarme. Ogni controller ha due ingressi e due uscite di allarme.
Nome ingresso allarme	Il nome dell'ingresso allarme.
Tipo ingresso allarme	Il tipo di ingresso allarme. Normalmente aperto Normalmente chiuso
Collega sicurezza antincendio	Attivando l'opzione, tutte le porte si aprono quando viene attivato l'allarme antincendio.
Uscita allarme	Attivazione della funzione uscita allarme.
Durata	Stabilisce la durata dell'allarme quando si attiva.
Canale di uscita allarme	Selezione del canale di uscita allarme. Ogni controller ha due ingressi e due uscite di allarme.
Collegamento CA	Attivare l'opzione **Collegamento CA** per configurare il collegamento a una porta. Impostare la porta su sempre aperta o sempre chiusa. Quando si attiva l'allarme, la porta si apre o si chiude automaticamente.
Porta 1/Porta 2	

Passaggio 3: Fare clic su **OK**.

2.2.15.2 Configurazione delle regole per le schede

La piattaforma supporta cinque formati Wiegand predefiniti. È anche possibile aggiungere dei formati Wiegand personalizzati.

Passaggio 1: Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Config. regola scheda di accesso** (Local Device Config > Access Card Rule Config).

Passaggio 2: Fare clic su **Aggiungi** (Add) e configurare nuovi formati Wiegand.

Figura 2-32 Aggiunta di nuovi formati Wiegand

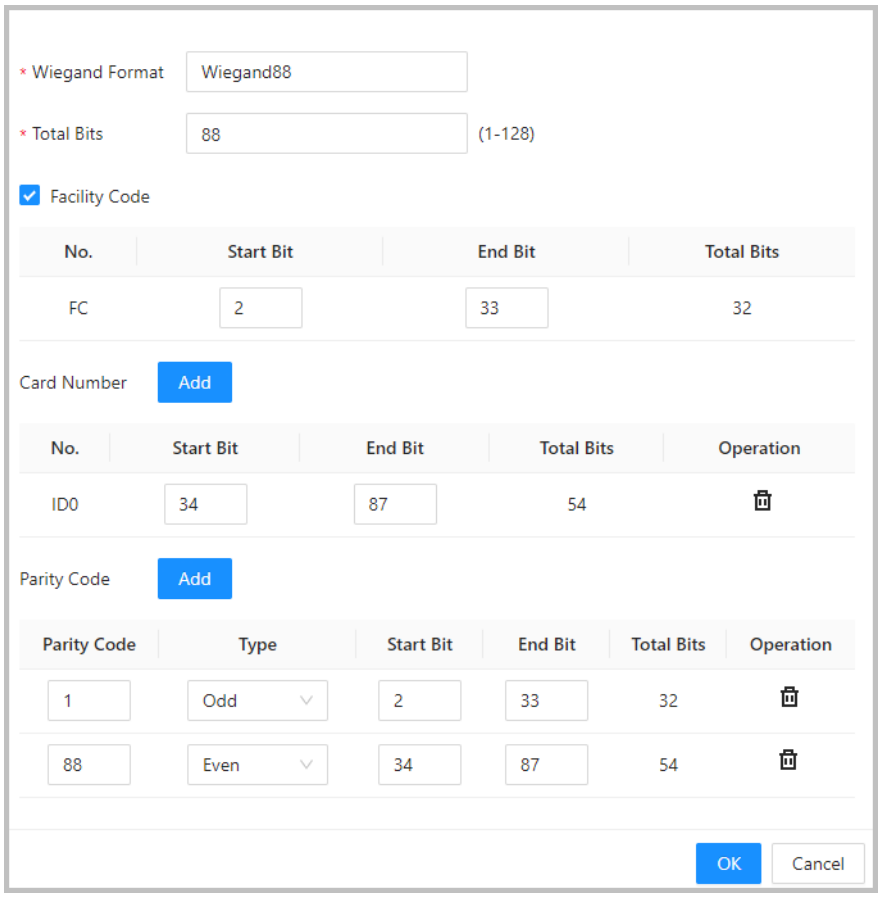


Tabella 2-14 Configurazione dei formati Wiegand

Parametro	Descrizione
Formato Wiegand	Il nome del formato Wiegand.
Bit totali	Inserire il numero totale di bit.
Codice struttura	Inserire il bit iniziale e il bit finale del codice struttura.
Numero scheda	Inserire il bit iniziale e il bit finale del numero di scheda.
Codice di parità	1. Inserire il bit di parità pari iniziale e il bit di parità pari finale. 2. Inserire il bit di parità dispari iniziale e il bit di parità dispari finale.

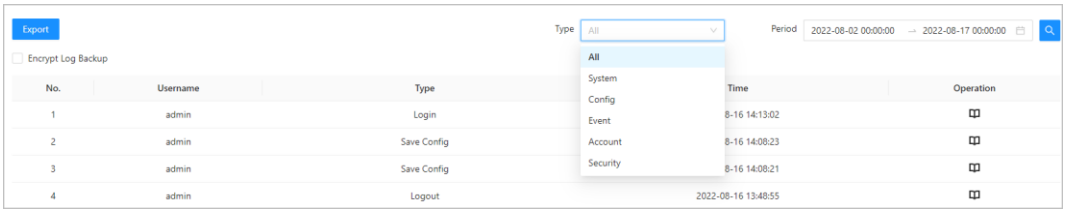
Passaggio 3: Fare clic su **OK**.

2.2.15.3 Backup dei log di sistema

Passaggio 1: Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Log di sistema** (Local Device Config > System Logs).

Passaggio 2: Seleziona prima il tipo di log, poi l'intervallo di tempo.

Figura 2-33 Backup dei log



Passaggio 3: Fare clic su **Cripta backup log** (Encrypt Log Backup) per effettuare il backup dei log criptati.

Passaggio 4: È anche possibile fare clic su **Esporta** (Export) per esportare i log.

2.2.15.4 Configurazione di rete

2.2.15.4.1 Configurazione TCP/IP

È necessario configurare l'indirizzo IP del controller degli accessi per far sì che possa comunicare con gli altri dispositivi.

Passaggio 1: Selezionare **Config. dispositivo locale** > **Impostazioni di rete** > **TCP/IP** (Local Device Config > Network Setting > TCP/IP).

Passaggio 2: Configurare i parametri.

Figura 2-34 TCP/IP

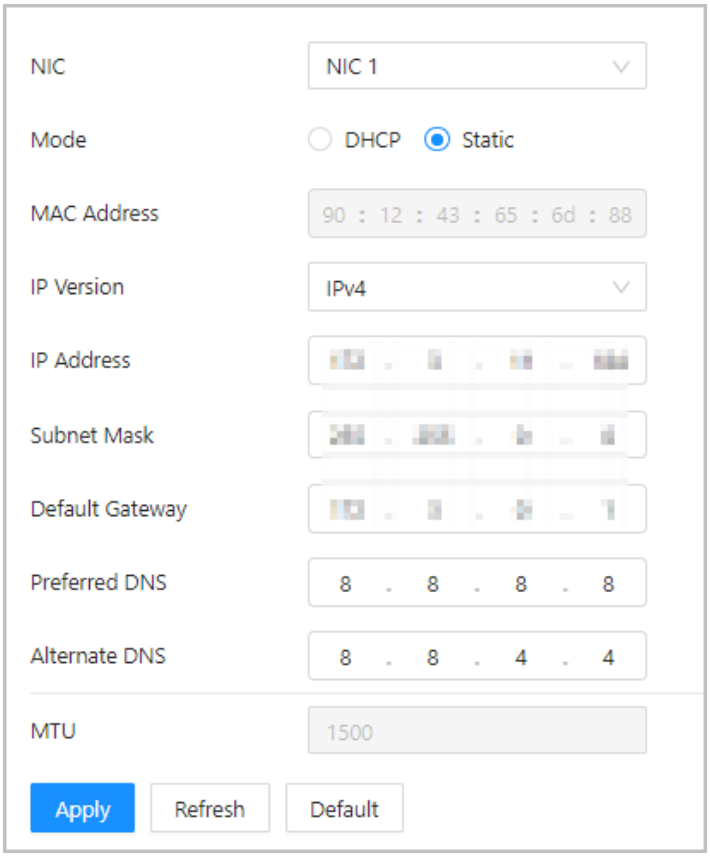


Tabella 2-15 Descrizione dei parametri TCP/IP

Parametro	Descrizione
Versione IP	IPv4.
Indirizzo MAC	L'indirizzo MAC del controller degli accessi.
Modalità	• **Statica**: inserimento manuale di indirizzo IP, subnet mask e gateway. • **DHCP**: protocollo di configurazione IP dinamica. Se l'opzione DHCP è attiva, al controller degli accessi verranno assegnati automaticamente un indirizzo IP, una subnet mask e un gateway.
Indirizzo IP	Se si seleziona la modalità statica, configurare l'indirizzo IP, la subnet mask e il gateway. L'indirizzo IP e il gateway devono trovarsi sullo stesso segmento di rete.
Subnet mask	
Gateway predefinito	
DNS preferito	Inserire qui l'indirizzo IP del server DNS preferito.
DNS alternativo	Inserire qui l'indirizzo IP del server DNS alternativo.

Passaggio 3: Fare clic su **OK**.

2.2.15.4.2 Configurazione delle porte

È possibile limitare l'accesso al controller in contemporanea tramite web, client per desktop e telefono.

Passaggio 1: Selezionare **Config. dispositivo locale** > **Impostazioni di rete** > **Porta** (Local Device Config > Network Setting > Port).

Passaggio 2: Configurare i numeri di porta.

È necessario riavviare il controller per rendere effettive le modifiche di tutti i parametri tranne **N. massimo connessioni** (Max Connection) e **Porta RTSP** (RTSP Port).

Figura 2-35 Configurazione delle porte

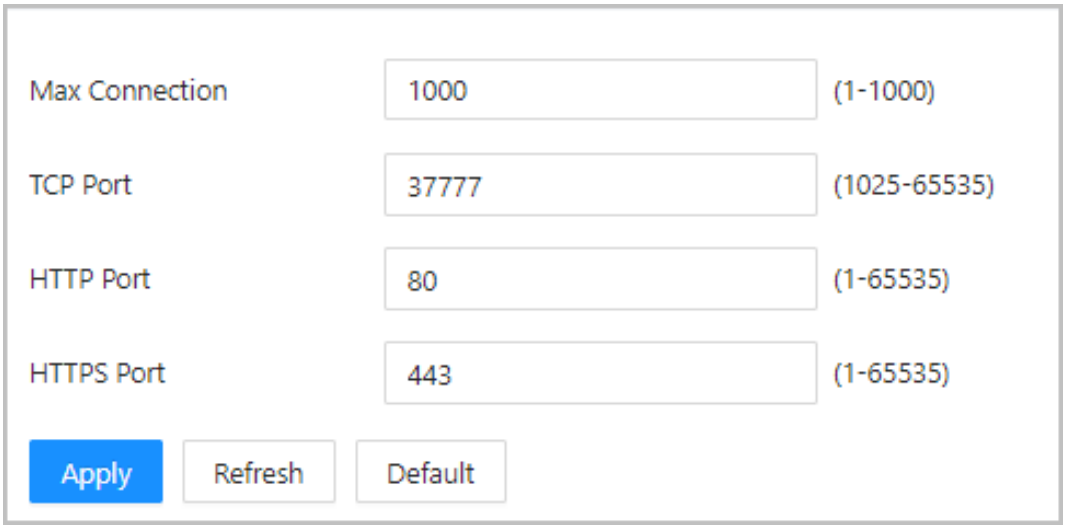


Tabella 2-16 Descrizione delle porte

Parametro	Descrizione
N. massimo connessioni	È possibile impostare il numero massimo di client (come client web, client per desktop e telefono) che possono accedere contemporaneamente al controller.
Porta TCP	Il valore predefinito è 37777.
Porta HTTP	Il valore predefinito è 80. Per modificare il numero di porta, aggiungere il nuovo valore dopo l'indirizzo IP quando si accede alla pagina web.
Porta HTTPS	Il valore predefinito è 443.

Passaggio 3: Fare clic su **OK**.

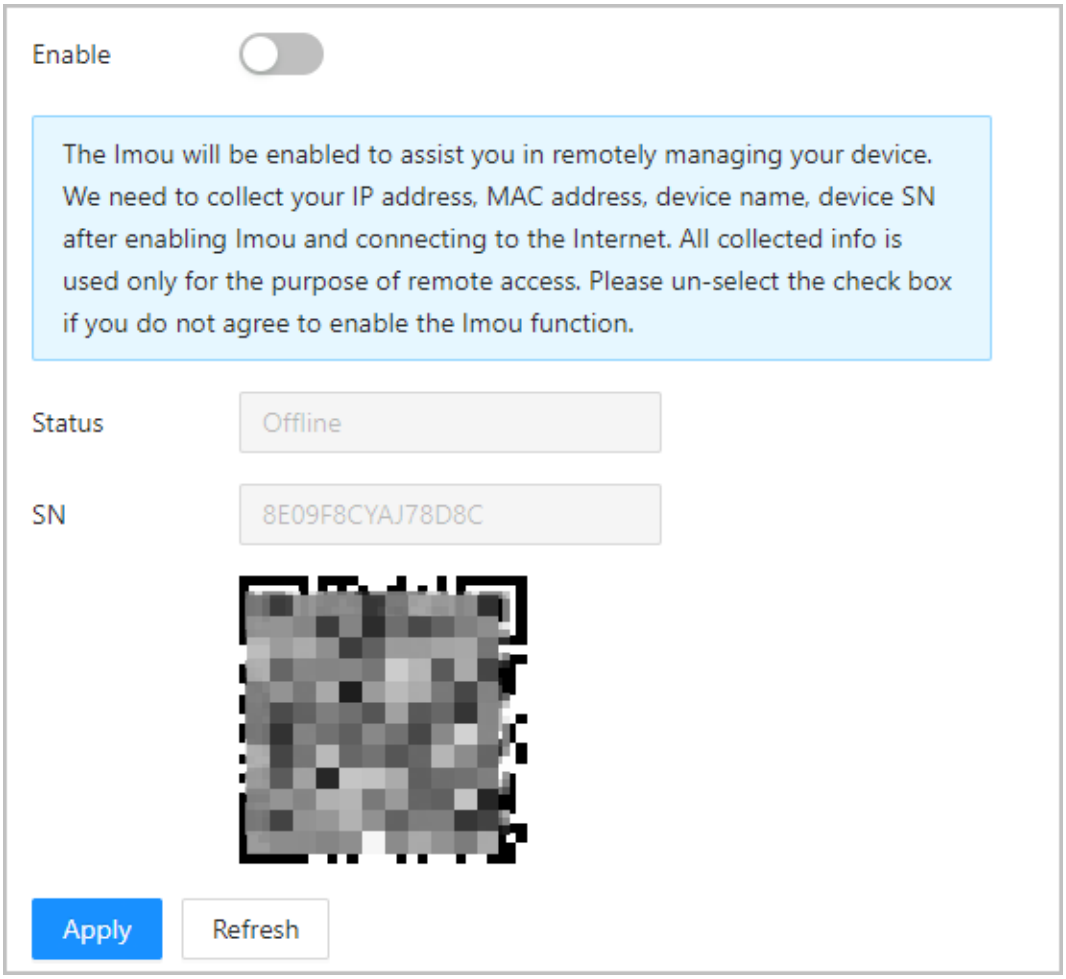
2.2.15.4.3 Configurazione del servizio cloud

Il servizio cloud fornisce un servizio di penetrazione NAT. Gli utenti possono gestire più dispositivi tramite DMSS (per i dettagli, consultare il manuale d'uso di DMSS). Con questo servizio non occorre richiedere nomi di dominio dinamici, definire la mappatura delle porte o implementare server.

Passaggio 1: Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Impostazioni di rete** > **Servizio cloud** (Local Device Config > Network Setting > Cloud Service).

Passaggio 2: Attivare il servizio cloud.

Figura 2- 36 Servizio cloud



Passaggio 3: Fare clic su **Applica** (Apply).

Passaggio 4: Scaricare DMSS e registrarsi, quindi scansionare il codice QR tramite DMSS per aggiungere il controller degli accessi.

Per i dettagli, consultare il manuale d'uso di DMSS.

2.2.15.4.4 Configurazione della registrazione automatica

Con questa funzione è possibile accedere al controller degli accessi tramite la piattaforma di gestione dopo che questo ha comunicato il suo indirizzo al server designato.

Passaggio 1: Sulla home page, selezionare **Impostazioni di rete** > **Registrazione** (Network Setting > Register).

Passaggio 2: Abilitare la funzione di registrazione automatica e configurare i parametri.

Figura 2-37 Registrazione

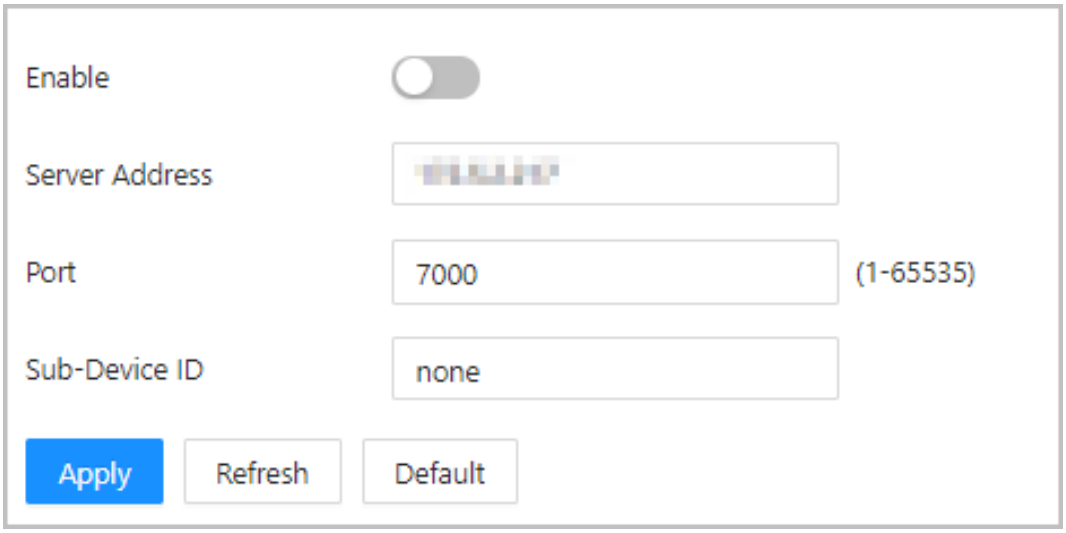


Tabella 2-17 Descrizione dei parametri per la registrazione automatica

Parametro	Descrizione
Indirizzo Server	L'indirizzo IP del server.
Porta	La porta del server utilizzata per la registrazione automatica.
ID dispositivo secondario	Inserire l'ID del dispositivo secondario (stabilito dall'utente). Quando si aggiunge il controller degli accessi alla piattaforma di gestione, l'ID del dispositivo secondario sulla piattaforma di gestione deve corrispondere a quello impostato sul controller degli accessi.

Passaggio 3: Fare clic su **Applica** (Apply).

2.2.15.4.5 Configurazione del servizio di base

Quando si desidera collegare il controller degli accessi a una piattaforma di terze parti, attivare le funzioni CGI e ONVIF.

Passaggio 1: Selezionare la voce **Impostazioni di rete** > **Servizio di base** (Network Setting > Basic Service).

Passaggio 2: Configurare il servizio di base.

Figura 2-38 Servizio di base

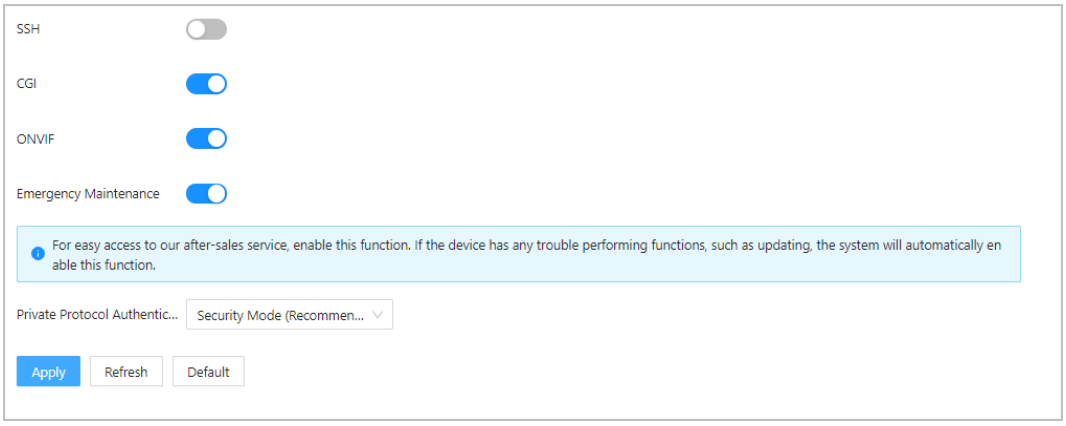


Tabella 2-18 Descrizione dei parametri del servizio di base

Parametro	Descrizione
SSH	Il Secure Shell Protocol (SSH) è un protocollo di amministrazione remota che consente agli utenti di accedere ai server remoti e di controllarli e modificarli su Internet.
CGI	La Common Gateway Interface (CGI) è una specifica di interfaccia per i server web che consente di eseguire programmi come applicazioni di console (chiamate anche programmi con interfaccia a linea di comando) in esecuzione su un server che genera pagine web in modo dinamico. Tali programmi sono chiamati script CGI o semplicemente CGI. Le specifiche di esecuzione dello script da parte del server sono determinate da quest'ultimo. Solitamente, uno script CGI viene eseguito nel momento in cui viene fatta una richiesta, generando codice HTML. Quando la funzione CGI è abilitata, è possibile utilizzare i comandi CGI. L'opzione CGI è abilitata per impostazione predefinita.
ONVIF	Consente ad altri dispositivi di acquisire il flusso video del VTO tramite il protocollo ONVIF.
Manutenzione di emergenza	La funzione è abilitata per impostazione predefinita.
Modalità di autenticazione protocollo privato	• Modalità sicura (consigliata) • Modalità di compatibilità

Passaggio 3: Fare clic su **Applica** (Apply).

2.2.15.5 Configurazione dell'ora

Passaggio 1: Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Ora** (Local Device Config > Ora).

Passaggio 2: Configurare l'ora della piattaforma.

Figura 2-39 Impostazioni della data

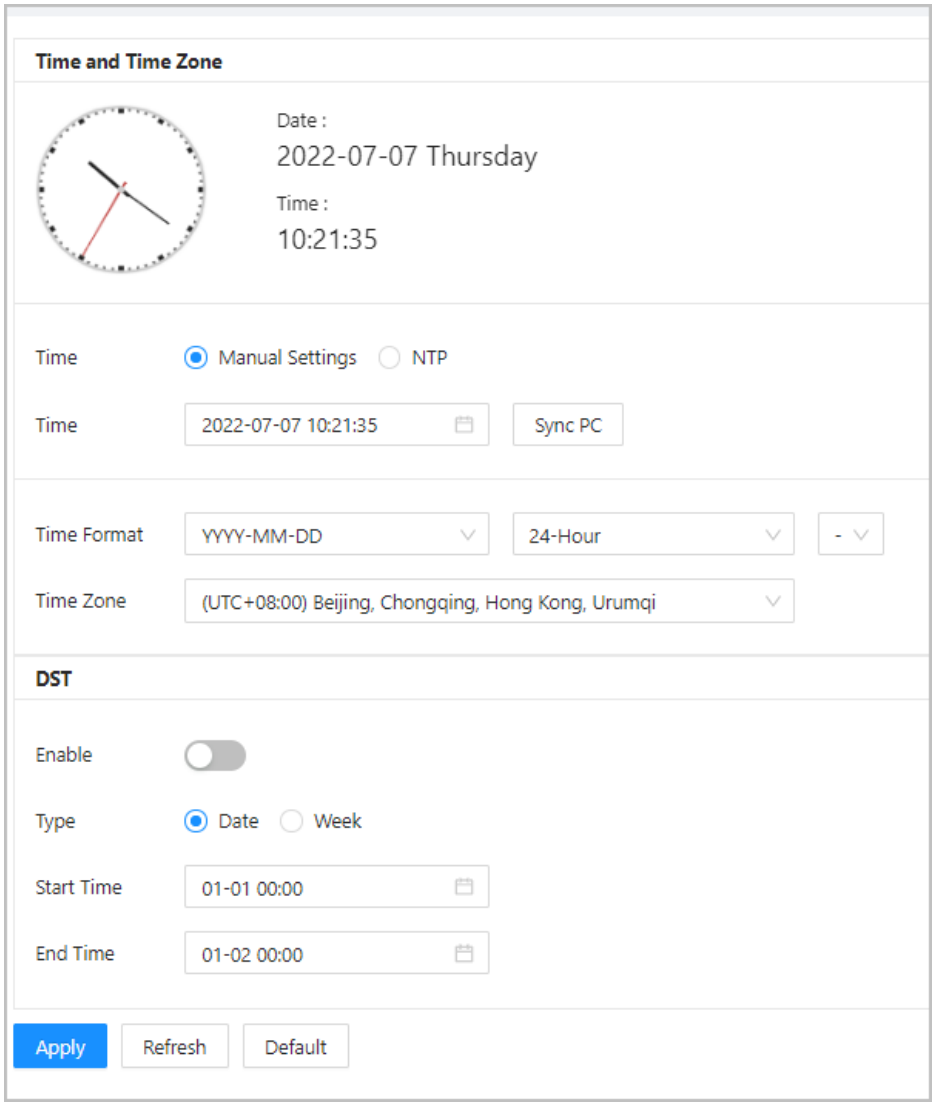


Tabella 2-19 Descrizione delle impostazioni dell'ora

Parametro	Descrizione
Ora	● Impostazione manuale: inserire manualmente l'ora o fare clic su **Sincronizzazione PC** (Sync PC) per sincronizzare l'ora con il computer. ● NTP: il controller degli accessi sincronizza automaticamente l'ora con il server NTP. ◇ **Server**: inserire il dominio del server NTP. ◇ **Porta**: inserire la porta del server NTP. ◇ **Intervallo**: inserire l'intervallo di sincronizzazione.
Formato ora	Selezionare il formato orario della piattaforma.
Fuso orario	Inserire Il fuso orario del controller degli accessi.
Ora legale	1. Abilitare il fuso orario (opzionale). 2. Selezionare **Data** (Date) o **Settimana** (Week) per l'opzione **Tipo** (Type). 3. Configurare l'ora di inizio e l'ora di fine.

Passaggio 3: Fare clic su **Applica** (Apply).

2.2.15.6 Gestione degli account

È possibile aggiungere ed eliminare utenti, modificarne le password e inserire un indirizzo e-mail per reimpostare una password dimenticata.

2.2.15.6.1 Aggiunta di utenti

È possibile aggiungere nuovi utenti che possono accedere alla pagina web del controller degli accessi.

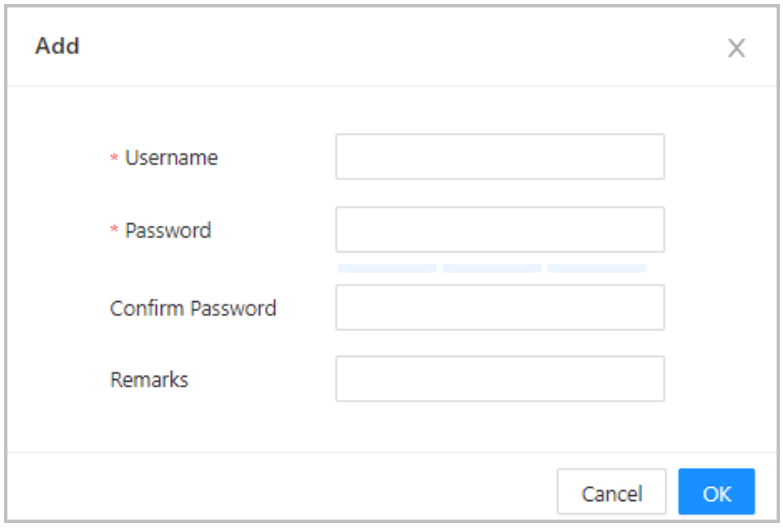
Procedura

Passaggio 1: Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Gestione account** > **Account** (Local Device Config > Account Management > Account).

Passaggio 2: Fare clic su **Aggiungi** (Add) e inserire le informazioni dell'utente.

- Il nome utente non può coincidere con quello di un account esistente. Il nome utente può contenere un massimo di 31 caratteri, scelti tra cifre, lettere, trattini bassi, punti e il simbolo @.
- La password deve contenere tra 8 e 32 caratteri, che non siano spazi, di almeno due tipologie diverse scelte tra lettere maiuscole, lettere minuscole, cifre e caratteri speciali (esclusi ' " ; : &).
  Impostare una password sicura seguendo le indicazioni visualizzate.

Figura 2-40 Aggiunta di un utente



Passaggio 3: Fare clic su **OK**.

L'account amministratore non può essere eliminato ed è l'unico che può modificare le password.

2.2.15.6.2 Ripristino delle password

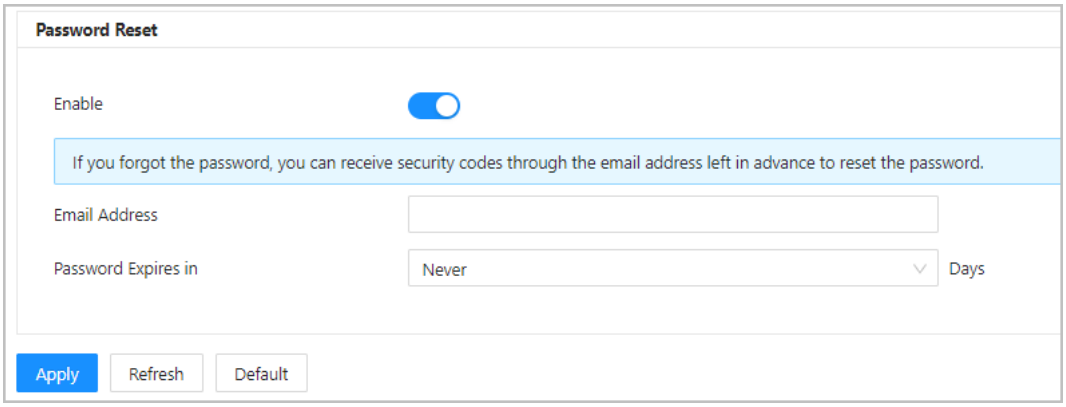
È possibile ripristinare una password dimenticata usando l'indirizzo e-mail collegato.

Passaggio 1: Selezionare **Config. dispositivo locale** > **Gestione account** > **Account** (Local Device Config > Account Management > Account).

Passaggio 2: Inserire l'indirizzo e-mail e impostare la durata della password.

Passaggio 3: Attivare la funzione di ripristino della password.

Figura 2-41 Ripristino di una password



Se si dimentica la password, è possibile ricevere i codici di sicurezza per ripristinarla all'indirizzo e-mail indicato in precedenza.

Passaggio 4: Fare clic su **Applica** (Apply).

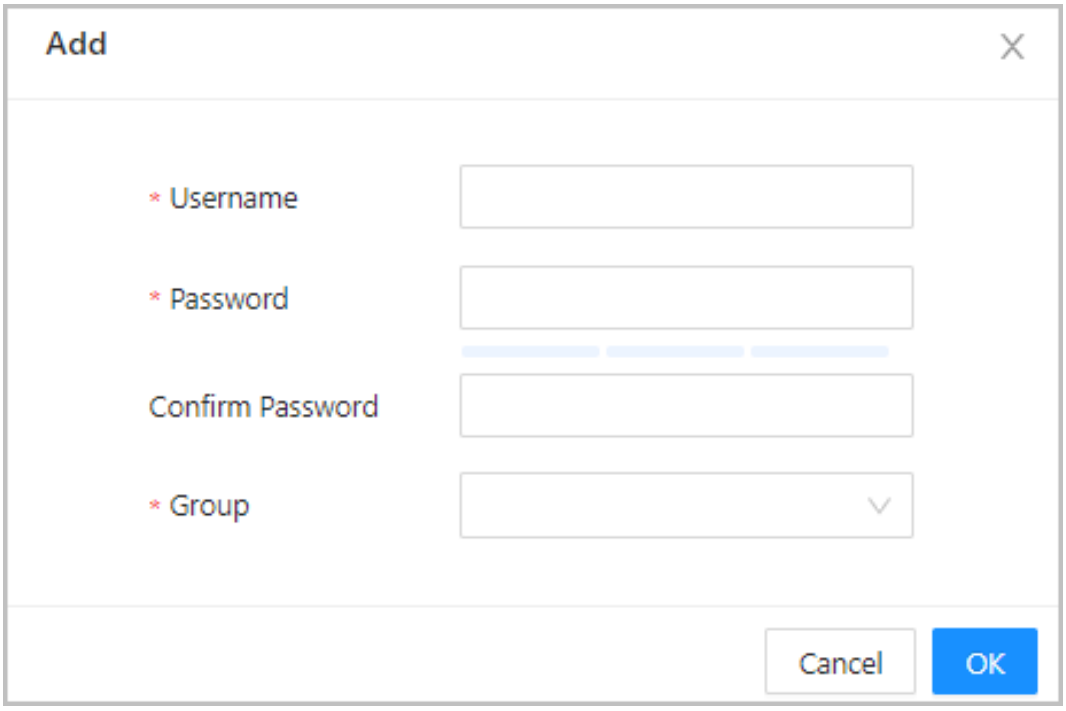
2.2.15.6.3 Aggiunta di utenti ONVIF

L'Open Network Video Interface Forum (ONVIF) è un forum di settore istituito per lo sviluppo di uno standard globale aperto per l'interfaccia dei prodotti di sicurezza fisici basati su IP, che offre compatibilità con produttori diversi. L'identità degli utenti ONVIF viene verificata attraverso il protocollo ONVIF. L'utente ONVIF predefinito è admin.

Passaggio 1: Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Gestione account** > **Account ONVIF** (Local Device Config > Account Management > ONVIF Account).

Passaggio 2: Fare clic su **Aggiungi** (Add) e configurare i parametri.

Figura 2-42 Aggiunta di un utente ONVIF



Passaggio 3: Fare clic su **OK**.

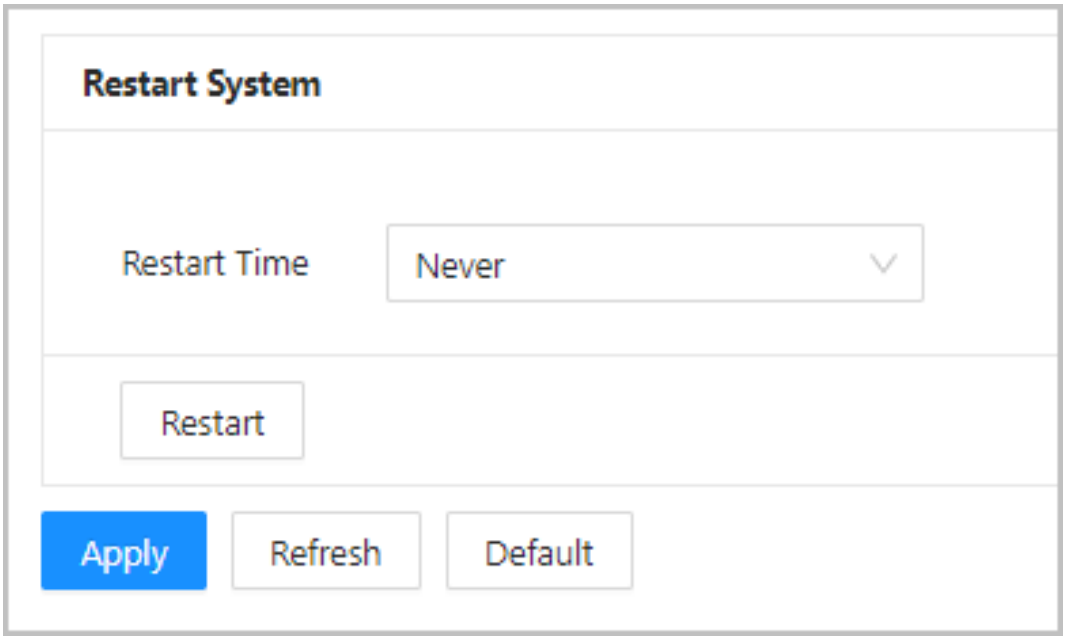
2.2.15.7 Manutenzione

È possibile riavviare con regolarità il controller degli accessi mentre è inattivo per migliorarne le prestazioni.

Passaggio 1: Accedere alla pagina web.

Passaggio 2: Selezionare **Config. dispositivo locale** > **Manutenzione** (Local Device Config > Maintenance).

Figura 2-43 Manutenzione



Passaggio 3: Impostare l'ora di riavvio e fare clic su **OK**.

Passaggio 4: Fare clic su **Riavvia** (Restart) per riavviare subito il controller degli accessi.

2.2.15.8 Gestione avanzata

È possibile applicare le stesse impostazioni a più di un controller di accesso importando o esportando i file di configurazione.

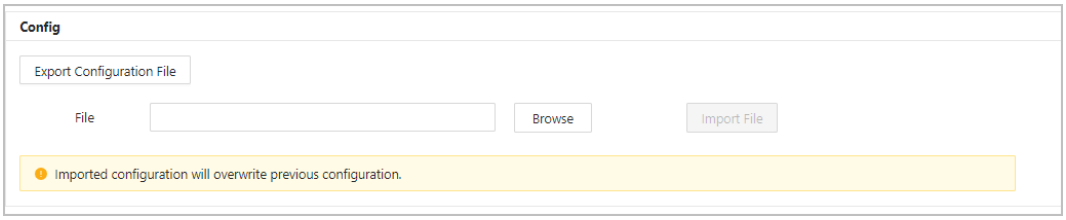
2.2.15.8.1 Esportazione e importazione dei file di configurazione

Il file di configurazione del controller degli accessi può essere importato ed esportato. Quando si desidera applicare le stesse impostazioni a più dispositivi, è possibile importare il file di configurazione sui dispositivi selezionati.

Passaggio 1: Accedere alla pagina web.

Passaggio 2: Selezionare **Config. dispositivo locale** > **Impostazioni avanzate** (Local Device Config > Advanced Settings).

Figura 2-44 Gestione della configurazione



Passaggio 3: Esportare o importare i file di configurazione.

- Esportazione del file di configurazione.
  Fare clic su **Esporta file di configurazione** (Export Configuration file) per esportare il file su un computer locale.

  La configurazione IP non sarà esportata.
- Importazione del file di configurazione.
  1. Fare clic su **Sfoglia** (Browse) per selezionare il file di configurazione.
  2. Fare clic su **Importa configurazione** (Import Configuration).

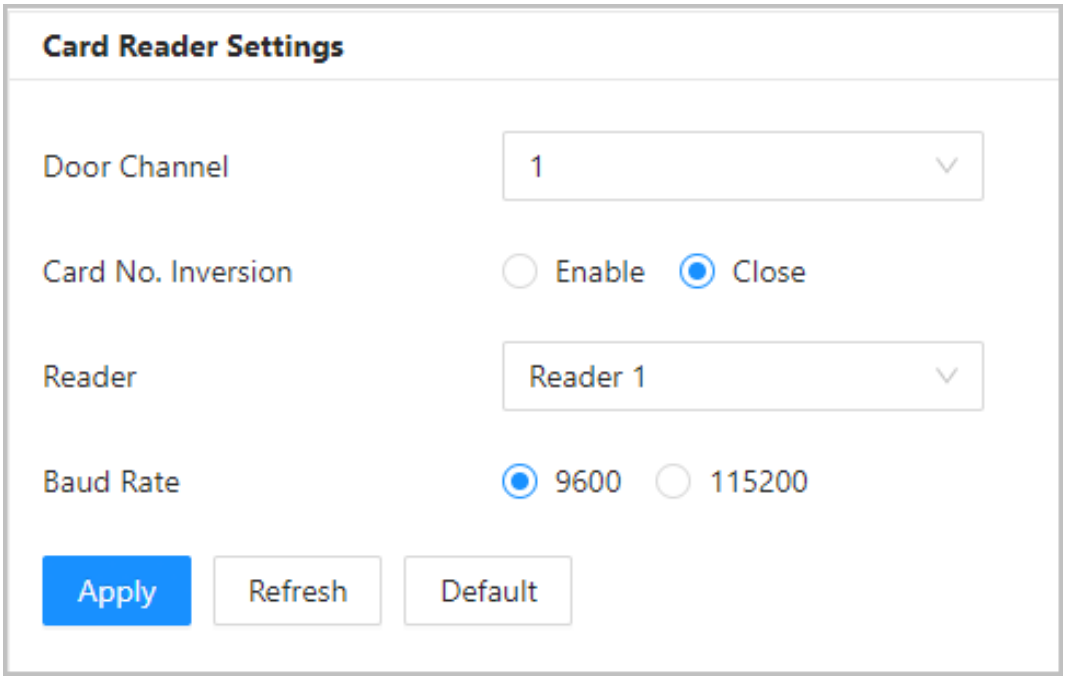
     I file di configurazione possono essere importati solo su dispositivi dello stesso modello.

2.2.15.8.2 Configurazione del lettore di schede

Passaggio 1: Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Impostazioni avanzate** (Local Device Config > Advanced Settings).

Passaggio 2: Configurare il lettore di schede.

Figura 2-45 Configurazione del lettore di schede



2.2.15.8.3 Configurazione del livello dell'impronta digitale

Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Impostazioni avanzate** (Local Device Config > Advanced Settings) e inserire la soglia dell'impronta digitale. La soglia può essere impostata in un intervallo compreso tra 1 e 10, dove un valore più alto rappresenta una maggiore accuratezza di rilevamento.

Figura 2-46 Livello dell'impronta digitale

2.2.15.8.4 Ripristino delle impostazioni di fabbrica

⚠

Il ripristino delle impostazioni di fabbrica del **Controller degli accessi** causa la perdita dei dati. Prestare attenzione.

Passaggio 1: Selezionare **Config. dispositivo locale** > **Impostazioni avanzate** (Local Device Config > Advanced Settings).

Passaggio 2: Se necessario, ripristinare le impostazioni di fabbrica.

- **Impostazioni di fabbrica**: ripristina tutte le configurazioni predefinite del controller ed elimina tutti i dati.

- **Ripristina impostazioni di fabbrica (tranne informazioni utente e log)**: ripristina tutte le configurazioni predefinite del controller ed elimina tutti i dati, tranne le informazioni relative agli utenti, i log e i parametri configurati durante la procedura guidata di accesso.

L'opzione **Ripristina impostazioni di fabbrica (tranne informazioni utente e log)** (Restore to Default (Except for User Info and Logs)) è supportata solo dal controller principale.

2.2.15.9 Aggiornamento del sistema

Utilizzare il file di aggiornamento corretto, che deve essere richiesto al servizio di assistenza tecnica.

- Non scollegare l'alimentazione o la connessione di rete e non riavviare o spegnere il controller degli accessi durante la procedura di aggiornamento.

2.2.15.9.1 Aggiornamento tramite file

Passaggio 1: Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Aggiornamento di sistema** (Local Device Config > System Update).
Passaggio 2: Nella sezione **Aggiornamento con file** (File Update), fare clic su **Sfoglia** (Browse) e caricare il file di aggiornamento.

Il file di aggiornamento deve avere un'estensione .bin.

Passaggio 3: Fare clic su **Aggiorna** (Update).

Il controller degli accessi si riavvia al termine della procedura di aggiornamento.

2.2.15.9.2 Aggiornamento online

Passaggio 1: Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Aggiornamento di sistema** (Local Device Config > System Update).
Passaggio 2: Nella sezione **Aggiornamento online** (Online Update), selezionare un metodo di aggiornamento.

- Selezionare **Verifica automatica aggiornamenti** (Auto Check for Updates) affinché il controller degli accessi controlli automaticamente la presenza di aggiornamenti.
- Selezionare **Verifica manuale** (Manual Check) per controllare subito se è disponibile una versione aggiornata.

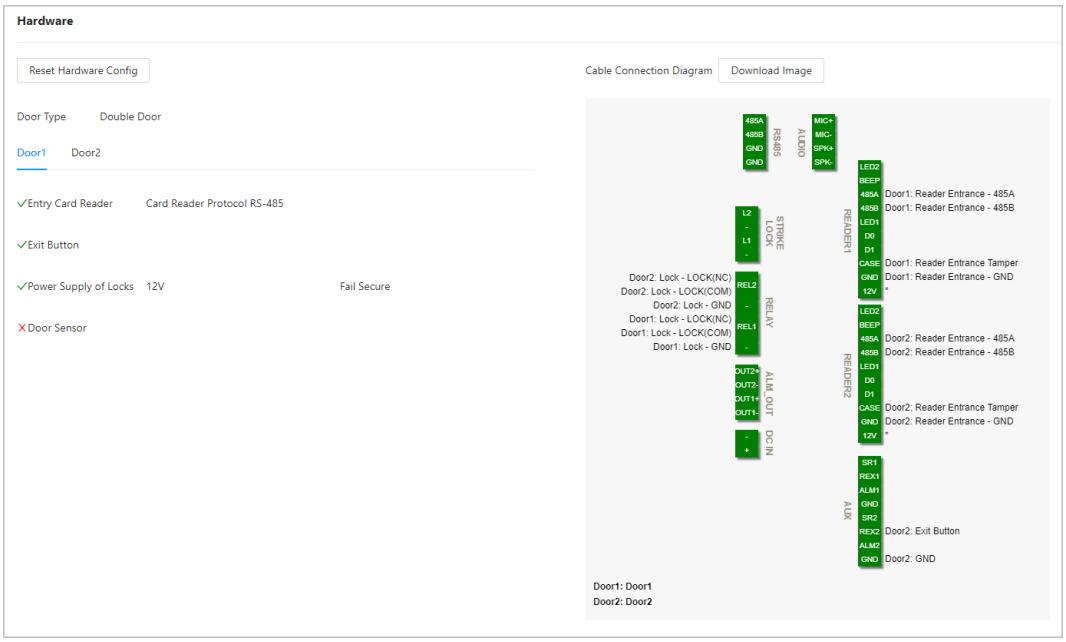
Passaggio 3: Se è disponibile una versione aggiornata, fare clic su **Verifica manuale** (Manual Check) per aggiornare il controller degli accessi.

2.2.15.10 Configurazione dell'hardware

Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Hardware** (Local Device Config > Hardware). Quando si accede alla piattaforma per la prima volta, è possibile visualizzare l'hardware configurato. È anche possibile riconfigurare l'hardware. Per i dettagli, consultare la tabella 2-1 "Descrizione dei parametri".

Quando si passa dall'opzione Porta singola a quella Porta doppia, il controller degli accessi si riavvia. Il diagramma di cablaggio viene generato a scopo illustrativo e può essere scaricato sul computer.

Figura 2-47 Hardware



2.2.15.11 Visualizzazione delle informazioni di versione

Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Info versione** (Local Device Config > Version Info) per visualizzare le informazioni sulla versione, come il modello e il numero di serie del dispositivo, la versione dell'hardware o le informazioni legali.

2.2.15.12 Visualizzazione delle informazioni legali

Nella pagina iniziale, selezionare **Config. dispositivo locale** > **Info legali** (Local Device Config > Legal Info) per visualizzare l'accordo di licenza del software, la politica sulla privacy e l'avviso sul software open source.

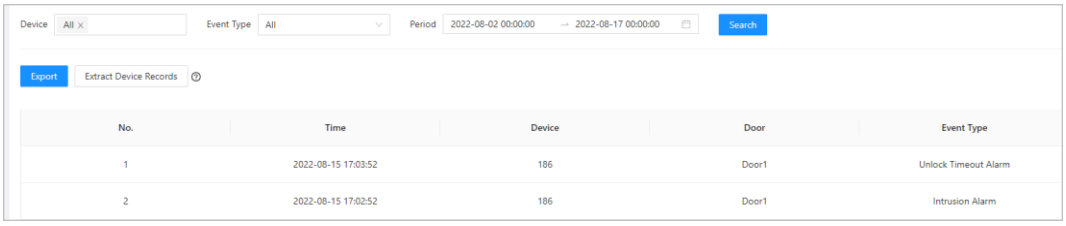
2.2.16 Visualizzazione dei record

È possibile visualizzare i log di allarme e di sblocco.

2.2.16.1 Visualizzazione dei record di allarme

Passaggio 1: Nella pagina iniziale, selezionare **Reportistica** > **Record di allarme** (Reporting > Alarm Records).
Passaggio 2: Selezionare il dispositivo, il reparto e la fascia oraria, quindi fare clic su **Cerca** (Search).

Figura 2-48 Record di allarme

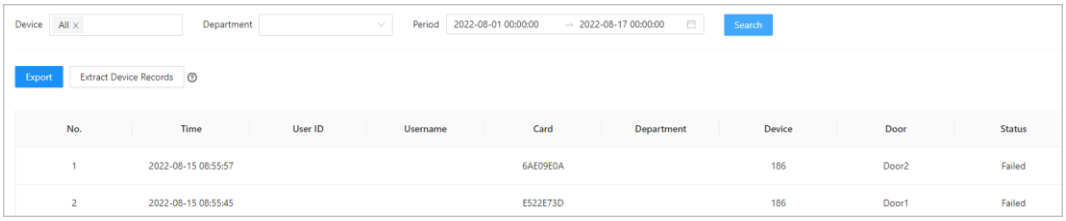


- **Esporta**: esporta i log di allarme del controller principale su un computer locale.
- **Estrai record dispositivo**: quando i controller secondari sono online e generano i log, questi ultimi possono essere esportati sul controller principale.

2.2.16.2 Visualizzazione dei record di sblocco

Passaggio 1: Nella pagina iniziale, selezionare **Reportistica** > **Record di sblocco** (Reporting > Unlock Records).
Passaggio 2: Selezionare il dispositivo, il reparto e la fascia oraria, quindi fare clic su **Cerca** (Search).

Figura 2-49 Log di sblocco



- Esporta: esportazione dei log di sblocco.
- Estrai record dispositivo: quando i controller secondari sono online e generano i log, è possibile esportare questi ultimi sul controller principale.

2.2.17 Impostazioni di sicurezza (opzionale)

2.2.17.1 Stato di sicurezza

Informazioni preliminari

È possibile scansionare gli utenti, i servizi e i moduli di sicurezza per verificare lo stato di sicurezza del controller degli accessi.

- Rilevamento di utenti e servizi: verifica se la configurazione in uso rispetta le raccomandazioni.
- Scansione dei moduli di sicurezza: controlla lo stato di funzionamento dei moduli di sicurezza, come trasmissione audio e video, protezione attendibile, avvisi di sicurezza e difesa dagli attacchi, senza verificare se sono abilitati.

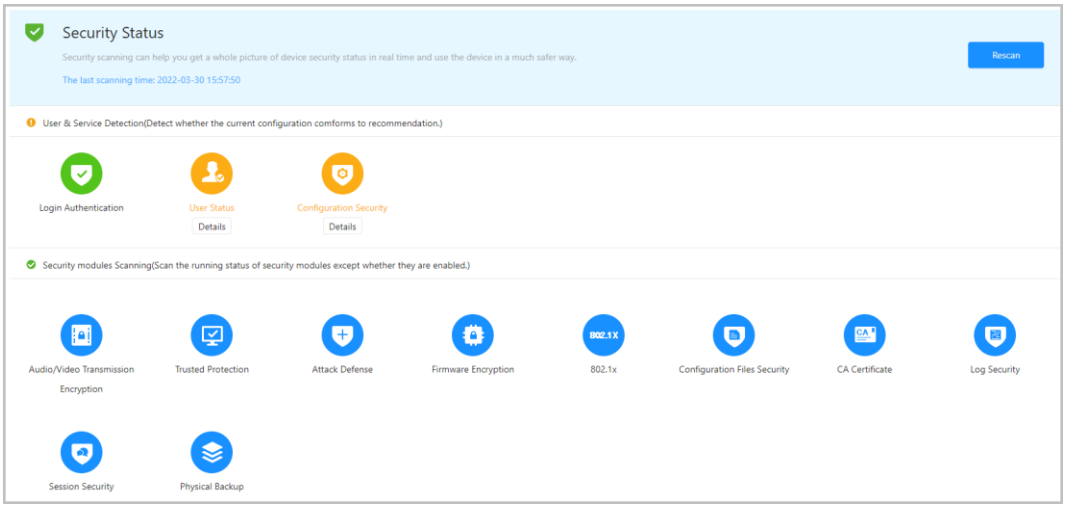
Procedura

Passaggio 1: Selezionare **Sicurezza** > **Stato sicurezza** (Security > Security Status).

Passaggio 2: Fare clic su **Ripeti scansione** (Rescan) per effettuare una scansione di sicurezza del controller degli accessi.

Passare il mouse sopra le icone dei moduli di sicurezza per visualizzarne lo stato di funzionamento.

Figure 2-50 Stato della sicurezza



Operazioni correlate

Una volta effettuata la scansione, i risultati vengono mostrati usando colori diversi. Il giallo indica che i moduli di sicurezza presentano delle anomalie, il verde che funzionano normalmente.

- Fare clic su **Dettagli** (Details) per visualizzare i risultati dettagliati della scansione.
- Fare clic su **Ignora** (Ignore) per ignorare un'anomalia e non scansionarla più. L'anomalia ignorata viene evidenziata in grigio.
- Fare clic su **Riprendi rilevamento** (Rejoin Detection) per riprendere la scansione dell'anomalia ignorata.
- Fare clic su **Ottimizza** (Optimize) per provare a risolvere l'anomalia.

2.2.17.2 Configurazione del protocollo HTTPS

Creando o caricando un certificato di autenticazione, è possibile accedere alla pagina web dal computer usando il protocollo HTTPS. Il protocollo HTTPS rende le comunicazioni di rete tra computer sicure.

Procedura

Passaggio 1: Selezionare **Sicurezza** > **Servizi di sistema** > **HTTPS** (Security > System Service > HTTPS).

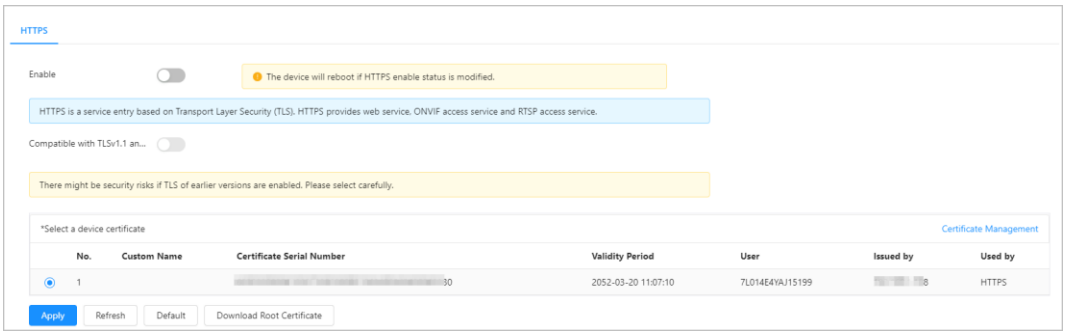
Passaggio 2: Attivare il servizio HTTPS.

Attivare la compatibilità con TLS 1.1 e versioni precedenti può causare rischi per la sicurezza. Prestare attenzione.

Passaggio 3: Selezionare un certificato.

Se non sono presenti certificati nell'elenco, fare clic su **Gestione certificati** (Certificate Management) per caricarne uno. Per ulteriori dettagli, consultare la sezione "2.2.17.4 Installazione di un certificato per il dispositivo".

Figura 2-51 HTTPS



Passaggio 4: Fare clic su **Applica** (Apply).

Scrivere "https://*indirizzo IP*:*porta https*" nella barra degli indirizzi di un web browser. Se il certificato viene installato, sarà possibile accedere alla pagina web. Altrimenti, la pagina web segnalerà che il certificato è errato o inattendibile.

2.2.17.3 Difesa dagli attacchi

2.2.17.3.1 Configurazione del firewall

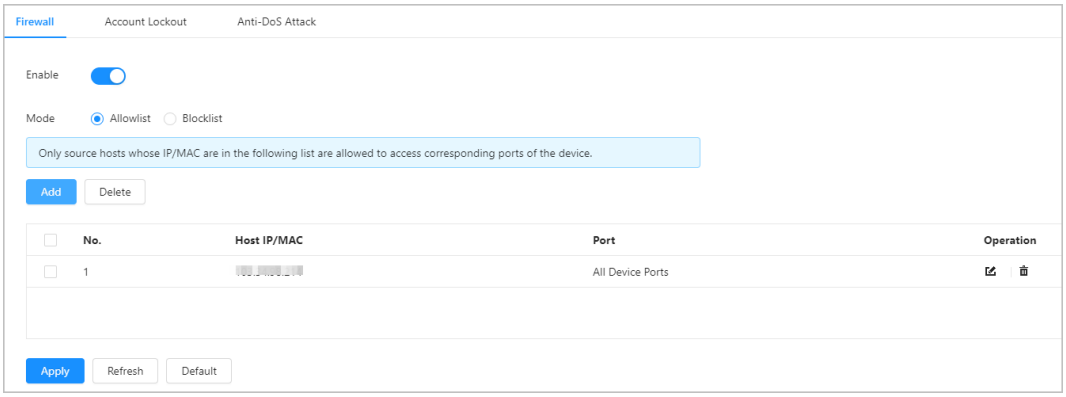
La configurazione del firewall consente di limitare l'accesso al controller.

Procedura

Passaggio 1: Selezionare **Sicurezza** > **Difesa dagli attacchi** > **Firewall** (Security > Attack Defense > Firewall).

Passaggio 2: Fare clic su per abilitare il firewall.

Figura 2-52 Firewall

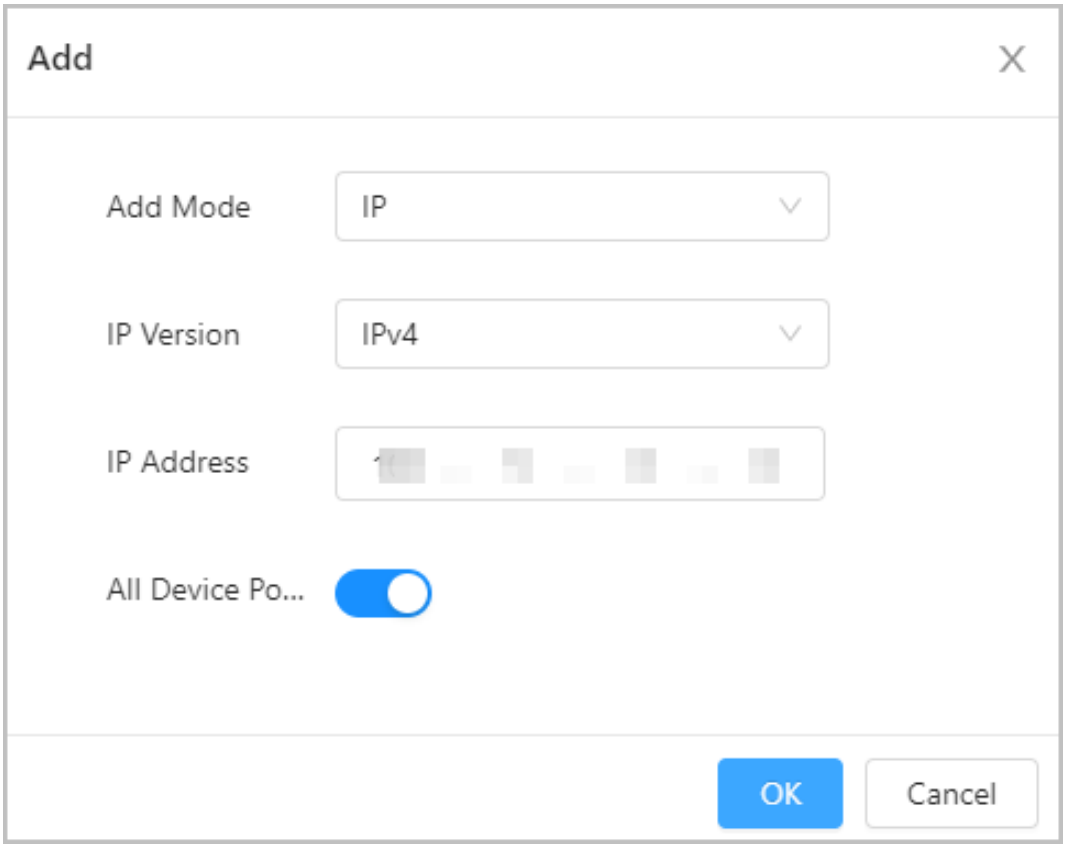


Passaggio 3: Selezionare una modalità tra **Elenco autorizzati** o **Elenco bloccati**.

- **Elenco autorizzati**: l'accesso al controller è consentito solo agli indirizzi IP/MAC autorizzati presenti nel relativo elenco.
- **Elenco bloccati**: gli indirizzi IP/MAC presenti nell'elenco bloccati non possono accedere al controller.

Passaggio 4: Fare clic su **Aggiungi** (Add) per inserire le informazioni IP.

Figura 2-53 Informazioni IP



Passaggio 5: Fare clic su **OK**.

Operazioni correlate

- Fare clic su per modificare le informazioni IP.
- Fare clic su per eliminare un indirizzo IP.

2.2.17.3.2 Configurazione del blocco dell'account

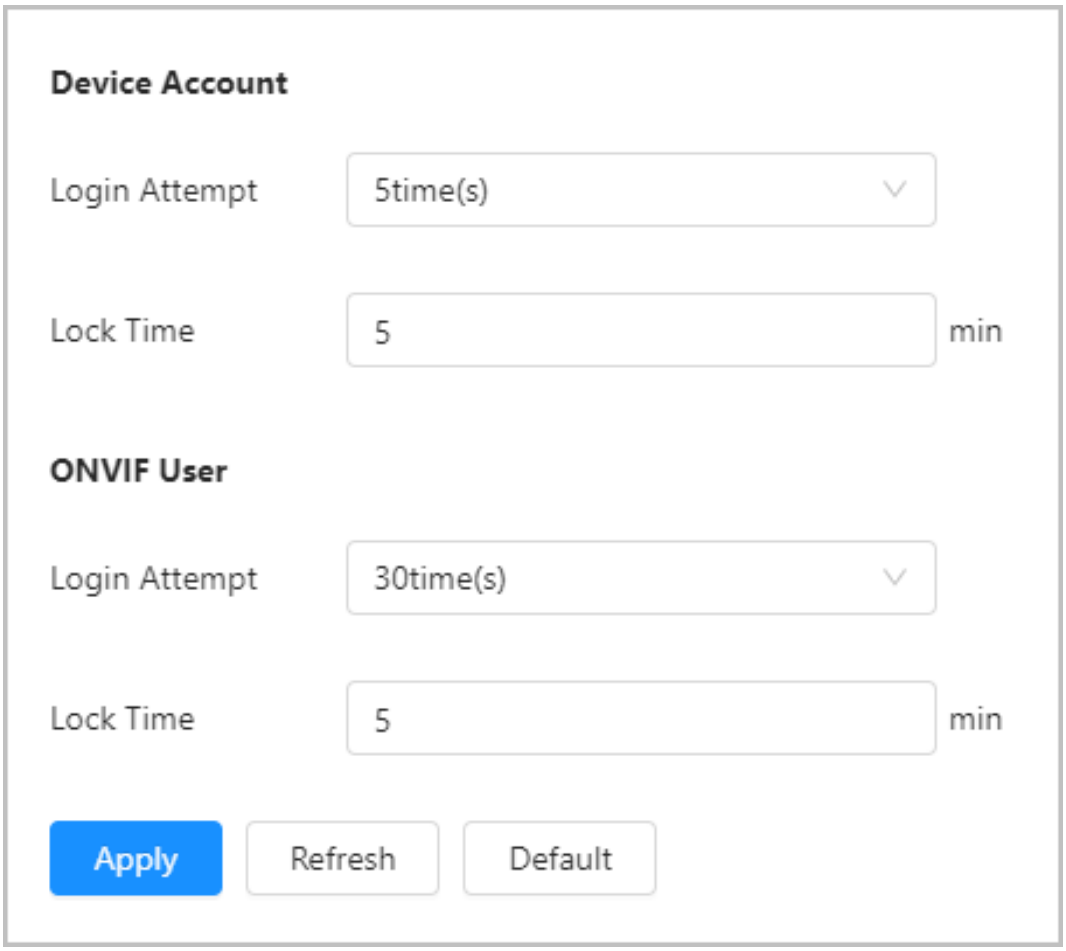
Se viene inserita una password errata per un numero di volte prestabilito, l'account viene bloccato.

Passaggio 1: Selezionare **Sicurezza** > **Difesa dagli attacchi** > **Blocco account** (Security > Attack Defense > Account Lockout).

Passaggio 2: Inserire il numero di tentativi di accesso e la durata del blocco dell'account amministratore e dell'utente ONVIF.

- Tentativi di accesso: il numero massimo di tentativi di accesso. Se viene inserita una password errata per un numero di volte prestabilito, l'account viene bloccato.
- Durata blocco: il periodo di tempo durante il quale non è possibile accedere dopo che l'account è stato bloccato.

Figura 2-54 Blocco dell'account



Passaggio 3: Fare clic su **Applica** (Apply).

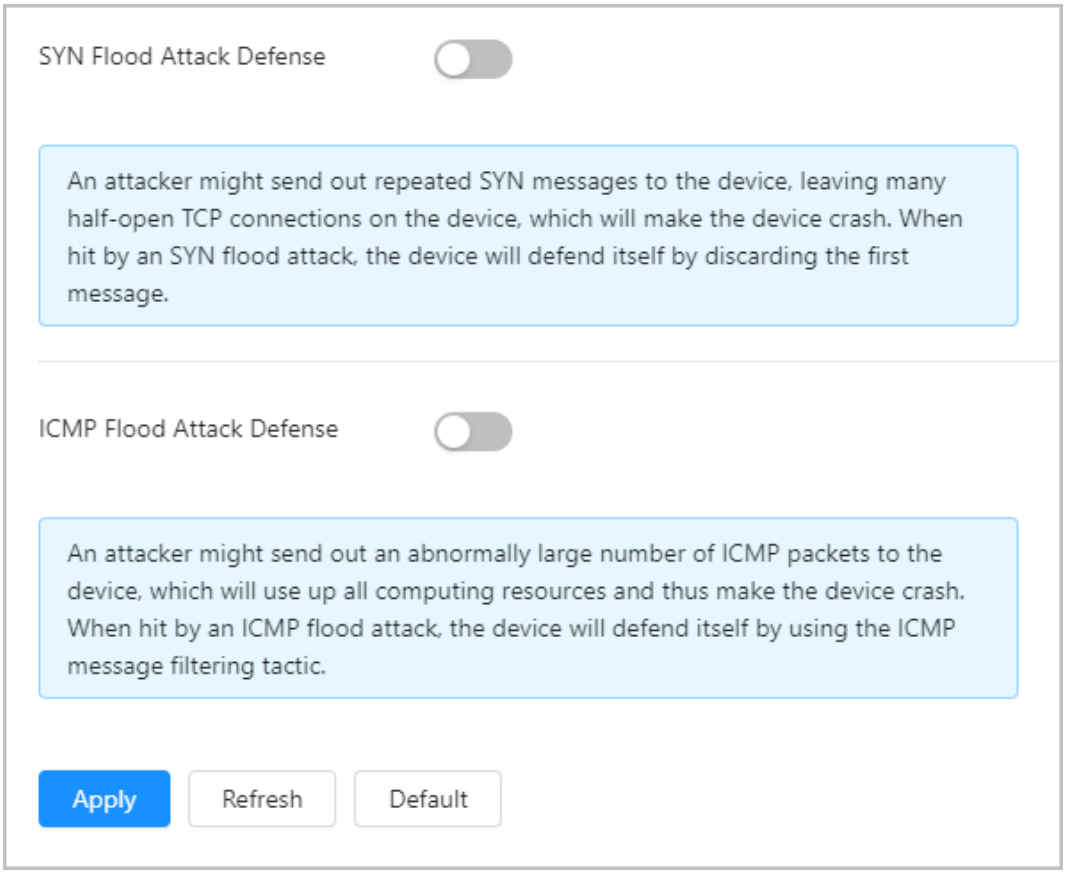
2.2.17.3.3 Configurazione della difesa dagli attacchi DoS

Per proteggere il controller degli accessi dagli attacchi DoS è possibile abilitare le funzioni **Difesa da attacchi SYN flood** (SYN Flood Attack Defense) e **Difesa da attacchi ICMP flood** (ICMP Flood Attack Defense).

Passaggio 1: Selezionare **Sicurezza** > **Difesa dagli attacchi** > **Difesa da attacchi DoS** (Security > Attack Defense > Anti-DoS Attack).

Passaggio 2: attivare l'opzione **Difesa da attacchi SYN flood** (SYN Flood Attack Defense) o **Difesa da attacchi ICMP flood** (ICMP Flood Attack Defense) per proteggere il controller degli accessi dagli attacchi DoS.

Figure 2-55 Difesa dagli attacchi DoS



Passaggio 3: Fare clic su **Applica** (Apply).

2.2.17.4 Installazione di un certificato per il dispositivo

Creando o caricando un certificato di autenticazione, è possibile accedere dal computer usando il protocollo HTTPS.

2.2.17.4.1 Creazione di un certificato

È possibile creare un certificato per il controller degli accessi.

Procedura

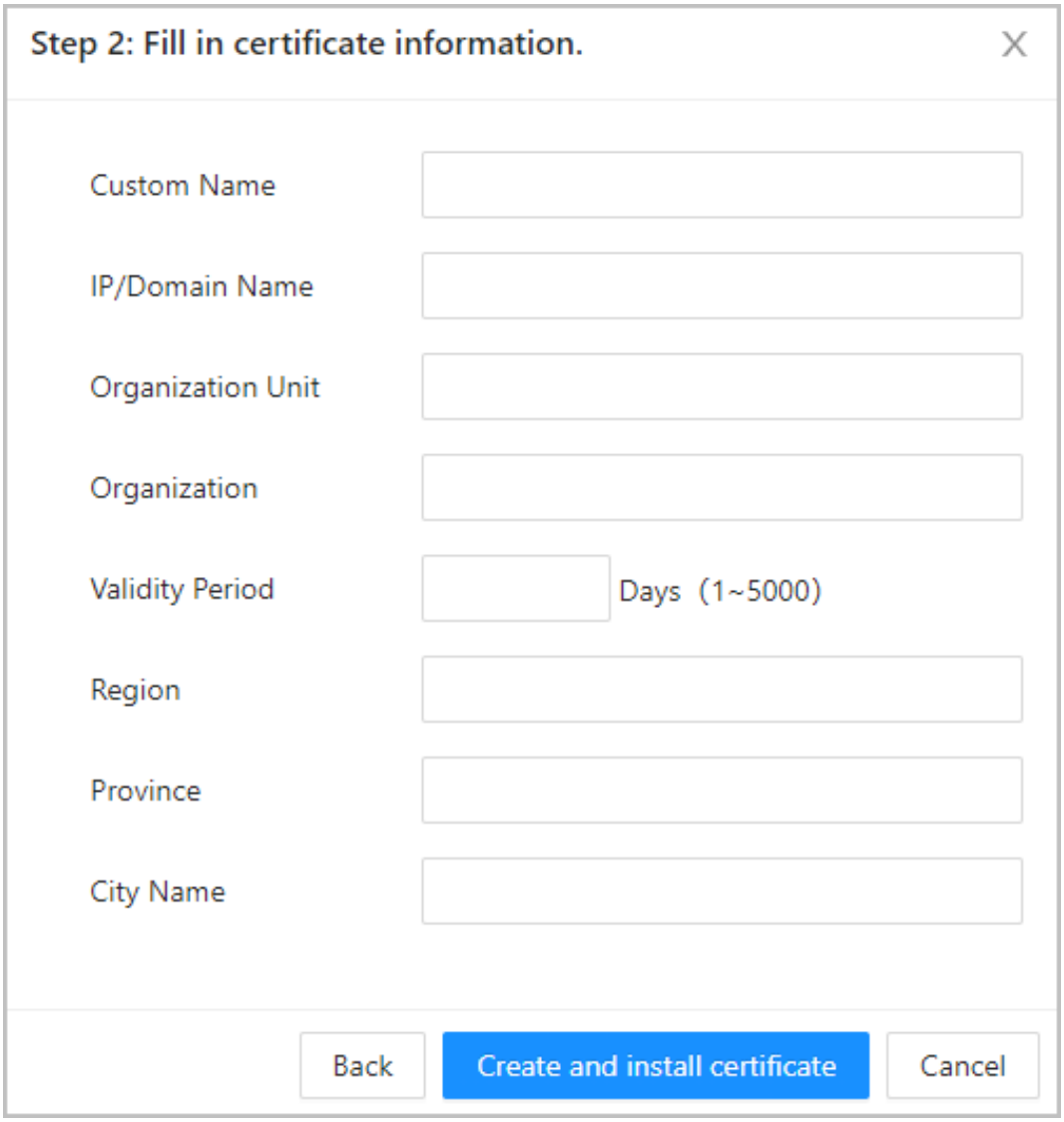
Passaggio 1: Selezionare **Sicurezza** > **Certificato CA** > **Certificato dispositivo** (Security > CA Certificate > Device Certificate).

Passaggio 2: Selezionare **Installa certificato dispositivo** (Install Device Certificate).

Passaggio 3: Selezionare **Crea certificato** (Create Certificate) e fare clic su **Avanti** (Next).

Passaggio 4: Inserire le informazioni relative al certificato.

Figura 2-56 Informazioni sul certificato



Il nome della regione non può superare i 2 caratteri. Consigliamo di utilizzare l'abbreviazione del nome della regione.

Passaggio 5: Fare clic su **Crea e installa certificato** (Create and install certificate).

Una volta installato, il certificato compare nella pagina **Certificato dispositivo** (Device Certificate).

Operazioni correlate

- Nella pagina **Certificato dispositivo** (Device Certificate), fare clic su **Attiva modalità di modifica** (Enter Edit Mode) per cambiare il nome del certificato.
- Fare clic su per scaricare il certificato.
- Fare clic su per eliminare il certificato.

2.2.17.4.2 Richiesta e importazione di certificati CA

È possibile importare certificati CA di terze parti sul controller degli accessi.

Procedura

Passaggio 1: Selezionare **Sicurezza** > **Certificato CA** > **Certificato dispositivo** (Security > CA Certificate > Device Certificate).

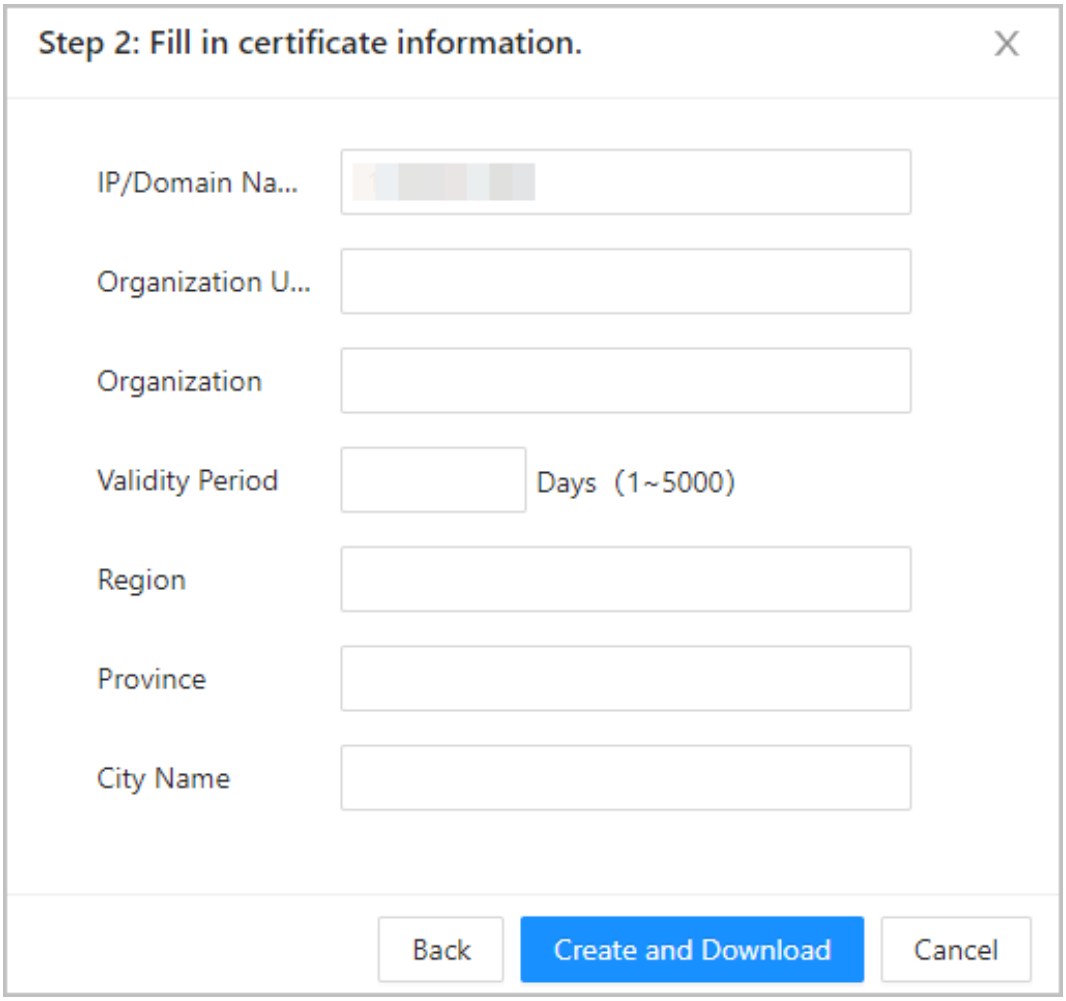
Passaggio 2: Fare clic su **Installa certificato dispositivo** (Install Device Certificate).

Passaggio 3: Selezionare **Richiedi certificato CA e importa (consigliato)** (Apply for CA Certificate and Import (Recommended)), quindi fare clic su **Avanti** (Next).

Passaggio 4: Inserire le informazioni relative al certificato.

- IP/nome di dominio: l'indirizzo IP o il nome di dominio del controller degli accessi.
- Regione: il nome della regione non può superare i 3 caratteri. Consigliamo di utilizzare l'abbreviazione del nome della regione.

Figura 2-57 Informazioni sul certificato (2)



Passaggio 5: Fare clic su **Crea e scarica** (Create and Download).

Salvare il file di richiesta sul computer.

Passaggio 6: Richiedere il certificato a un'organizzazione CA terza utilizzando il file di richiesta.

Passaggio 7: Importare il certificato CA firmato.

1) Salvare il certificato CA sul computer.
2) Fare clic su **Installa certificato dispositivo** (Install Device Certificate).

3) Fare clic su **Sfoglia** (Browse) per selezionare il certificato CA.
4) Fare clic su **Importa e installa** (Import and Install).
   Una volta installato, il certificato compare nella pagina **Certificato dispositivo** (Device Certificate).
   - Fare clic su **Ricrea** (Recreate) per creare un nuovo file di richiesta.
   - Fare clic su **Importa dopo** (Import Later) per importare il certificato in un secondo momento.

Operazioni correlate

- Nella pagina **Certificato dispositivo** (Device Certificate), fare clic su **Attiva modalità di modifica** (Enter Edit Mode) per cambiare il nome del certificato.
- Fare clic su per scaricare il certificato.
- Fare clic su per eliminare il certificato.

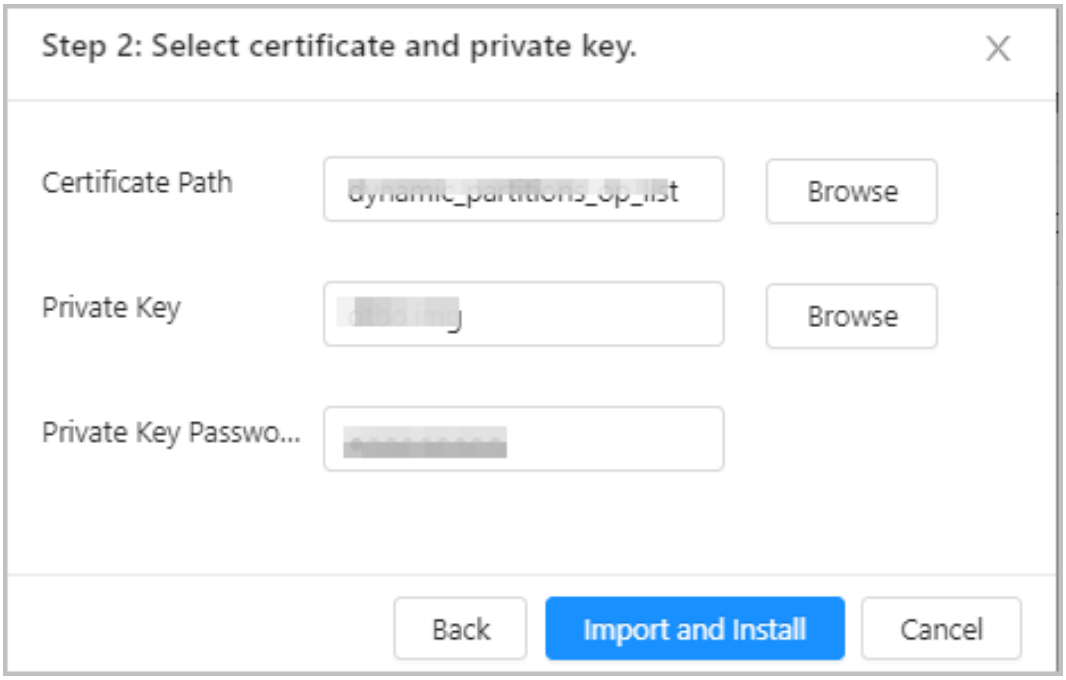
2.2.17.4.3 Installazione di un certificato esistente

Se si possiedono già un certificato e un file con una chiave privata, importarli come segue.

Procedura

Passaggio 1: Selezionare **Sicurezza** > **Certificato CA** > **Certificato dispositivo** (Security > CA Certificate > Device Certificate).
Passaggio 2: Fare clic su **Installa certificato dispositivo** (Install Device Certificate).
Passaggio 3: Selezionare **Installa certificato esistente** (Install Existing Certificate) e fare clic su **Avanti** (Next).
Passaggio 4: Fare clic su **Sfoglia** (Browse) per selezionare il certificato e la chiave privata, quindi inserire la password della chiave privata.

Figura 2-58 Certificato e chiave privata



Passaggio 5: Fare clic su **Importa e installa** (Import and Install).

Una volta installato, il certificato compare nella pagina **Certificato dispositivo** (Device Certificate).

Operazioni correlate

- Nella pagina **Certificato dispositivo** (Device Certificate), fare clic su **Attiva modalità di modifica** (Enter Edit Mode) per cambiare il nome del certificato.
- Fare clic su per scaricare il certificato.
- Fare clic su per eliminare il certificato.

2.2.17.5 Installazione di un certificato CA attendibile

Un certificato CA attendibile è un certificato digitale utilizzato per convalidare le identità dei siti web e dei server. Ad esempio, quando si utilizza il protocollo 802.1x, per autenticarne l'identità è richiesto un certificato CA per gli switch.

Il protocollo di rete 802.1X apre delle porte per l'accesso di rete quando un'organizzazione autentica l'identità di un utente e ne autorizza l'accesso alla rete.

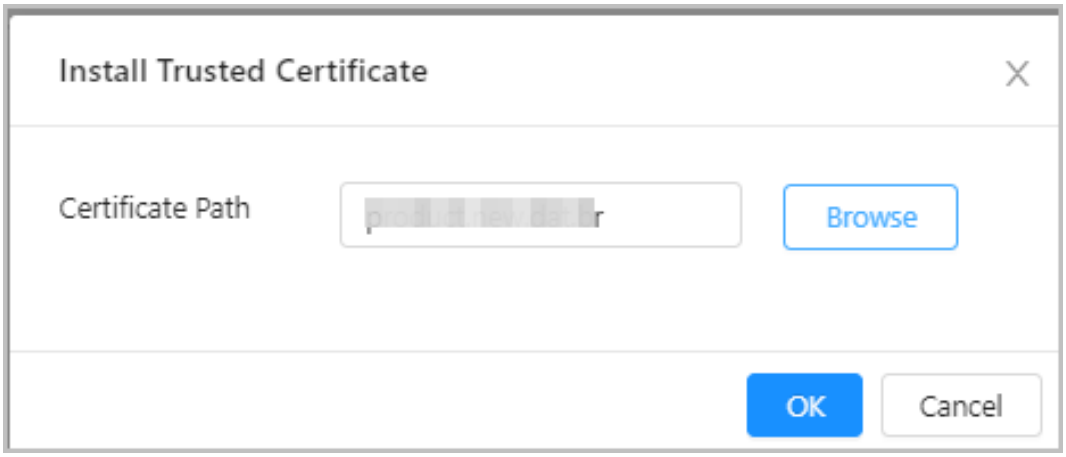
Procedura

Passaggio 1: Selezionare **Sicurezza** > **Certificato CA** > **Certificati CA attendibili** (Security > CA Certificate > Trusted CA Certificates).

Passaggio 2: Selezionare **Installa certificato attendibile** (Install Trusted Certificate).

Passaggio 3: Fare clic su **Sfoglia** (Browse) per selezionare il certificato attendibile.

Figura 2-59 Installazione di un certificato attendibile



Passaggio 4: Fare clic su **OK**.

Una volta installato, il certificato compare sulla pagina **Certificati CA attendibili** (Trusted CA Certificates).

Operazioni correlate

- Nella pagina **Certificato dispositivo** (Device Certificate), fare clic su **Attiva modalità di modifica** (Enter Edit Mode) per cambiare il nome del certificato.
- Fare clic su per scaricare il certificato.
- Fare clic su per eliminare il certificato.

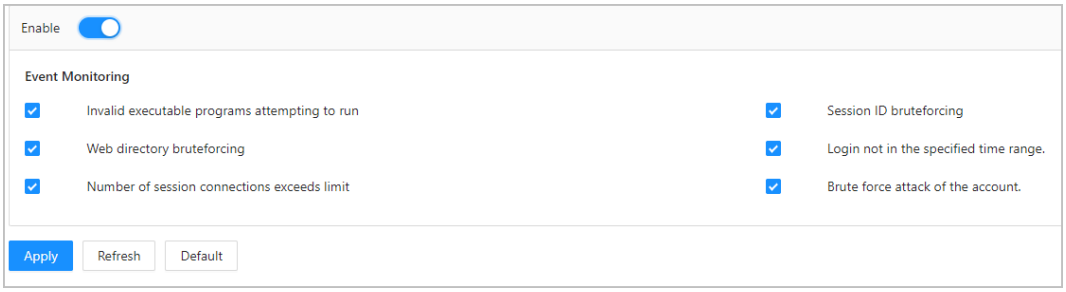
2.2.17.6 Avvisi di sicurezza

Passaggio 1: Selezionare **Sicurezza** > **Certificato CA** > **Avvisi di sicurezza** (Security > CA Certificate > Security Warning).

Passaggio 2: Abilitare gli avvisi di sicurezza.

Passaggio 3: Selezionare gli elementi da monitorare.

Figure 2-60 Avvisi di sicurezza



Passaggio 4: Fare clic su **Applica** (Apply).

2.3 Configurazioni del controller secondario

È possibile accedere alla pagina web del controller secondario per configurarlo localmente.

2.3.1 Inizializzazione

Inizializzare il controller secondario quando si accede alla pagina web per la prima volta o dopo che si sono ripristinate le impostazioni di fabbrica. Per informazioni dettagliate su come inizializzare il controller secondario, consultare la sezione "2.2.2 Inizializzazione".

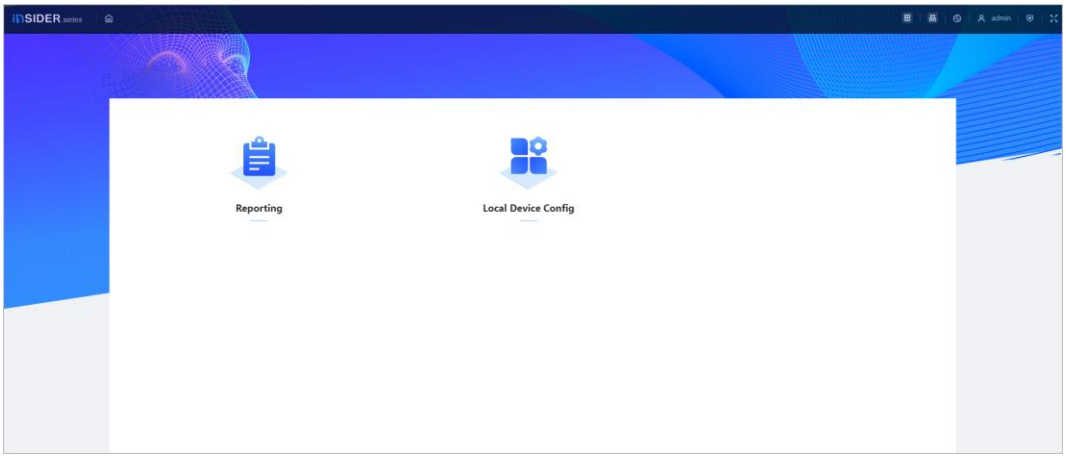
2.3.2 Accesso

Impostare il controller degli accessi come controller secondario durante la procedura guidata di accesso. Per ulteriori dettagli, consultare la sezione "2.2.3 Accesso".

2.3.3 Pagina iniziale

La pagina web del controller secondario include solamente i menu **Config. dispositivo locale** (Local Device Config) e **Reportistica** (Reporting). Per ulteriori dettagli, consultare la sezione "2.2.15 Configurazione dei dispositivi locali (opzionale)" e "2.2.16 Visualizzazione dei record".

Figura 2-61 Pagina iniziale

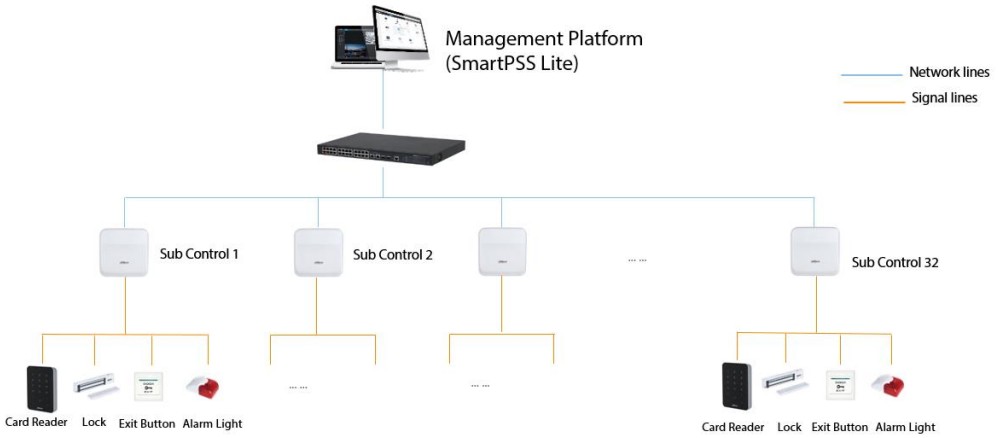


3 SmartPSS Lite-Controller secondari

3.1 Diagramma di rete

I controller secondari vengono aggiunti a una piattaforma di gestione autonoma, come SmartPSS Lite. È possibile gestire tutti i controller secondari tramite SmartPSS Lite.

Figura 3-1 Diagramma di rete



3.2 Configurazioni su SmartPSS Lite

È possibile aggiungere controller secondari a SmartPSS Lite e configurarli sulla piattaforma. Per i dettagli, consultare il manuale d'uso di SmartPSS Lite.

3.3 Configurazioni sul controller secondario

Per ulteriori dettagli, consultare la sezione "2.3 Configurazione del controller secondario".

Appendice 1 Raccomandazioni sulla sicurezza informatica

La sicurezza informatica non è solamente una parola di moda: è qualcosa che ha a che fare con tutti i dispositivi collegati a Internet. La sorveglianza video IP non è immune ai rischi informatici, ma adottare semplici misure di protezione e rafforzamento delle reti e dei dispositivi di rete rende questi ultimi meno suscettibili agli attacchi. Di seguito sono riportati alcuni consigli e raccomandazioni di Dahua su come creare un sistema di sorveglianza più sicuro.

Azioni obbligatorie da intraprendere per la sicurezza di rete di base dei dispositivi:

1. **Utilizzare password sicure**

   Seguire queste raccomandazioni quando si impostano le password:

   - La lunghezza non deve essere inferiore a 8 caratteri.
   - Utilizzare almeno due tipi di caratteri diversi scelti fra lettere maiuscole e minuscole, numeri e simboli.
   - Le password non devono contenere il nome dell'account o il nome dell'account al contrario.
   - Non utilizzare caratteri in sequenza, come 123, abc ecc.
   - Non utilizzare caratteri ripetuti, come 111, aaa ecc.

2. **Aggiornare il firmware e il software del client con regolarità**

   - Per assicurare che il sistema sia sempre protetto dalle patch e dagli aggiornamenti di sicurezza più recenti, è consigliabile mantenere aggiornati i firmware dei propri dispositivi (come NVR, DVR, telecamere IP ecc.), come previsto dagli standard del settore tecnologico. Quando i dispositivi sono collegati a una rete pubblica, è consigliabile attivare la funzione Verifica automaticamente la presenza di aggiornamenti (auto-check for updates) per ottenere informazioni regolari sugli aggiornamenti del firmware rilasciati dai produttori.
   - È consigliabile scaricare e utilizzare l'ultima versione del software del client.

Raccomandazioni facoltative ma consigliate per migliorare la sicurezza di rete dei dispositivi:

1. **Protezione fisica**

   È consigliabile proteggere fisicamente le apparecchiature, specialmente i dispositivi di archiviazione. Ad esempio, posizionare le apparecchiature all'interno di un armadio in una stanza dei computer e implementare misure per il controllo degli accessi e la gestione delle chiavi adatte a evitare che il personale non autorizzato possa danneggiare l'hardware, collegare senza permesso dispositivi rimovibili (come chiavette USB e porte seriali) ecc.

2. **Modificare le password con regolarità**

   È consigliabile modificare le password regolarmente per ridurre il rischio che vengano scoperte o violate.

3. **Impostare e aggiornare tempestivamente le informazioni per il ripristino delle password**

   Il dispositivo supporta la funzione di ripristino della password. Configurare per tempo le informazioni relative al ripristino della password, compreso l'indirizzo e-mail dell'utente finale e le domande di sicurezza. Se le informazioni cambiano, modificarle tempestivamente. Quando si impostano le domande di sicurezza per il ripristino della password, è consigliabile non utilizzare domande le cui risposte possono essere facilmente indovinate.

4. **Attivare il blocco dell'account**

La funzione di blocco dell'account è attiva per impostazione predefinita ed è consigliabile non disattivarla per garantire la sicurezza dell'account. Se un malintenzionato cerca di accedere ripetutamente con una password errata, l'account corrispondente e l'indirizzo IP utilizzato verranno bloccati.

5. **Modificare i valori predefiniti delle porte HTTP e relative agli altri servizi**
   Per ridurre il rischio che venga scoperto il numero di porta utilizzato, è consigliabile modificare i valori predefiniti delle porte HTTP e relative agli altri servizi scegliendo una qualsiasi combinazione di numeri compresa fra 1024 e 65535.
6. **Attivare il protocollo HTTPS**
   È consigliabile attivare il protocollo HTTPS, così da poter accedere al servizio web tramite un canale di comunicazione sicuro.
7. **Associare l'indirizzo MAC**
   È consigliabile associare gli indirizzi IP e MAC del gateway alle apparecchiature per ridurre il rischio di spoofing ARP.
8. **Assegnare account e autorizzazioni in modo ragionevole**
   Aggiungere gli utenti con ragionevolezza e assegnare loro il minimo set di permessi in base alle esigenze lavorative e di gestione.
9. **Disattivare i servizi non necessari e scegliere modalità sicure**
   Per ridurre i rischi, è consigliabile disattivare servizi come SNMP, SMTP, UPnP ecc quando non sono necessari.
   Se sono necessari, è vivamente consigliato utilizzare le modalità sicure per i servizi che seguono (l'elenco non è esaustivo):
   - SNMP: scegliere SNMP v3 e impostare password crittografiche e di autenticazione sicure.
     SMTP: scegliere TLS per accedere al server e-mail.
   - FTP: scegliere SFTP e impostare password sicure.
     Hotspot AP: scegliere la crittografia WPA2-PSK e impostare password sicure.
10. **Utilizzare la trasmissione crittografata di audio e video**
    Se i contenuti audio e video sono molto importanti o sensibili, è consigliabile utilizzare la funzione di trasmissione crittografata per ridurre il rischio che i dati vengano rubati.
    Nota: la trasmissione crittografata rende la trasmissione meno efficiente.
11. **Verifiche di sicurezza**
    - Verifica degli utenti online: è consigliabile verificare regolarmente gli utenti online per
    - controllare se qualcuno ha eseguito l'accesso al dispositivo senza autorizzazione.
      Verifica dei registri delle apparecchiature: controllando i registri, è possibile conoscere gli indirizzi IP utilizzati per accedere ai propri dispositivi e alle operazioni chiave.
12. **Registro di rete**
    A causa della limitata capacità di archiviazione delle apparecchiature, il registro salvato è limitato. Se è necessario archiviare il registro per un tempo maggiore, è consigliabile attivare il registro di rete per assicurarsi che i registri critici siano sincronizzati con il server del registro di rete, garantendo una tracciatura efficiente.
13. **Costruire un ambiente di rete sicuro**
    Per garantire la sicurezza delle apparecchiature e ridurre i rischi informatici potenziali, è consigliabile:
    - Disattivare la funzione di mappatura delle porte del router per evitare l'accesso diretto ai dispositivi intranet da una rete esterna.

- La rete deve essere suddivisa e isolata in base alle effettive esigenze di rete. In assenza di requisiti di comunicazione fra due sottoreti, è consigliabile utilizzare tecnologie come VLAN, GAP e altre per suddividere la rete e isolarla.
- Utilizzare il sistema di autenticazione degli accessi 802.1x per ridurre il rischio di accessi non autorizzati alle reti private.
- Attivare la funzione di filtraggio degli indirizzi IP/MAC per limitare il numero di host che possono accedere al dispositivo.

Ulteriori informazioni

Visitare il centro per le risposte alle emergenze di sicurezza sul sito ufficiale Dahua per consultare gli avvisi e i consigli sulla sicurezza più recenti.

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