



MANUALE D'USO, INSTALLAZIONE E AVVIAMENTO

V1.0.2

Prefazione

Generale

Questo manuale illustra le funzioni e le operazioni del dispositivo Access Standalone (di seguito denominato Dispositivo). Leggere attentamente prima di utilizzare il dispositivo e conservare il manuale per future consultazioni.

Istruzioni di sicurezza

Nel manuale potrebbero comparire le seguenti parole chiave.

Parole chiave	Senso
 DANGER	Indica un elevato potenziale pericolo che, se non evitato, può provocare morte o lesioni gravi.
 WARNING	Indica un rischio potenziale medio o basso che, se non evitato, potrebbe provocare lesioni lievi o moderate.
 CAUTION	Indica un potenziale rischio che, se non evitato, potrebbe causare danni materiali, perdita di dati, cali di prestazioni o risultati imprevedibili.
 ESD	Dispositivi sensibili alle scariche elettrostatiche. Indica un dispositivo sensibile alle scariche elettrostatiche.
 ELECTRIC SHOCK	Indica un'alta tensione pericolosa. Prestare attenzione ad evitare il contatto con l'elettricità.
 LASER RADIATION	Indica un rischio di radiazioni laser. Prestare attenzione ad evitare l'esposizione al raggio laser.
 TIPS	Offre metodi per aiutarti a risolvere un problema o a risparmiare tempo.
 NOTE	Fornisce informazioni aggiuntive a complemento del testo.

Cronologia delle revisioni

Versione	Contenuto della revisione	Orario di rilascio
V1.0.2	Contenuto rivisto.	Dicembre 2025
V1.0.1	Inizializzazione aggiunta descrizione.	Dicembre 2024
V1.0.0	Prima edizione.	Agosto 2024

Informativa sulla protezione della privacy

In qualità di utente del dispositivo o titolare del trattamento dei dati, potresti raccogliere dati personali di altri, come il volto, l'audio, le impronte digitali e il numero di targa. Devi rispettare le leggi e i regolamenti locali in materia di protezione della privacy per tutelare i diritti e gli interessi legittimi degli altri.

persone mediante l'attuazione di misure che includono, a titolo esemplificativo ma non esaustivo: fornire un'identificazione chiara e visibile per informare le persone dell'esistenza dell'area di sorveglianza e fornire le informazioni di contatto necessarie.

Informazioni sul manuale

- Il manuale è da intendersi solo a scopo di riferimento. Potrebbero esserci lievi differenze tra il manuale e il prodotto.
- Non ci assumiamo alcuna responsabilità per le perdite subite a causa di un utilizzo del prodotto non conforme al manuale.
- Il manuale verrà aggiornato in base alle leggi e ai regolamenti più recenti delle giurisdizioni competenti. Per informazioni dettagliate, consultare il manuale d'uso cartaceo, utilizzare il nostro CD-ROM, scansionare il codice QR o visitare il nostro sito web ufficiale. Il manuale è da intendersi solo come riferimento. Potrebbero esserci lievi differenze tra la versione elettronica e quella cartacea.
- Tutti i progetti e i software sono soggetti a modifiche senza preavviso scritto. Gli aggiornamenti del prodotto potrebbero comportare alcune differenze tra il prodotto reale e il manuale. Si prega di contattare il servizio clienti per ottenere il programma più recente e la documentazione supplementare.
- Potrebbero esserci errori di stampa o discrepanze nella descrizione delle funzioni, del funzionamento e dei dati tecnici. In caso di dubbi o controversie, ci riserviamo il diritto di fornire la spiegazione finale.
- Se il manuale (in formato PDF) non si apre, aggiorna il software del lettore o prova un altro programma di lettura diffuso.
- Tutti i marchi commerciali, i marchi registrati e i nomi delle aziende presenti nel manuale sono di proprietà dei rispettivi proprietari.
- In caso di problemi durante l'utilizzo del dispositivo, si prega di visitare il nostro sito web, contattare il fornitore o il servizio clienti.
- In caso di dubbi o controversie, ci riserviamo il diritto di fornire la spiegazione finale.

Sommario

Prefazione.....	I 1
Panoramica.....	1
2 Operazioni locali.....	2
2.1 Inizializzazione.....	2
2.2 Menù principale.....	3
2.3 Gestione utenti.....	4
2.3.1 Aggiunta utente.....	4
2.3.2 Eliminazione dell'utente.....	5
2.4 Configurazione della modalità di sblocco della porta.....	5
2.5 Configurazione della durata dello sblocco.....	6
2.6 Configurazione del sensore porta.....	6
2.7 Gestione delle password.....	6
2.7.1 Modifica della password dell'amministratore.....	6
2.7.2 Aggiunta della password pubblica.....	7
2.7.3 Eliminazione della password pubblica.....	7
2.8 Gestione della scheda principale.....	7
2.8.1 Aggiunta della scheda principale.....	7
2.8.2 Eliminazione della scheda principale.....	8
2.8.3 Gestione delle schede utente tramite la scheda principale.....	8
2.9 Configurazione del periodo di timeout della porta.....	8
2.10 Ripristino delle impostazioni di fabbrica.....	9
3 Operazioni sulle pagine web.....	10
3.1 Inizializzazione.....	10
3.2 Reimpostazione della password.....	11
3.3 Pagina iniziale.....	12
3.4 Gestione del personale.....	13
3.5 Monitoraggio degli accessi.....	17
3.6 Configurazione del controllo degli accessi.....	19
3.6.1 Configurazione dei parametri di controllo degli accessi.....	19
3.6.2 Allarme.....	23
3.6.3 Impostazioni della scheda.....	28
3.6.4 Configurazione dei periodi.....	33
3.6.5 Configurazione delle funzioni della porta.....	36
3.6.6 Configurazione dello sblocco tramite password.....	37
3.6.7 Configurazione dello sblocco in prima persona.....	37
3.6.8 Configurazione dell'Anti-Passback.....	38
3.7 Impostazioni di comunicazione.....	40

3.7.1 Impostazioni di rete.....	40
3.7.2 Impostazioni modalità.....	51
3.8 Configurazione del sistema.....	55
3.8.1 Gestione utenti.....	55
3.8.2 Visualizzazione degli utenti online.....	58
3.8.3 Tempo di configurazione.....	58
3.9 Centro di manutenzione.....	60
3.9.1 Diagnosi con un clic.....	60
3.9.2 Informazioni di sistema.....	60
3.9.3 Capacità dati.....	61
3.9.4 Visualizzazione dei registri.....	61
3.9.5 Gestione della manutenzione.....	62
3.9.6 Aggiornamento del sistema.....	64
3.9.7 Manutenzione avanzata.....	64
3.10 Impostazioni di sicurezza (facoltativo)	65
3.10.1 Stato di sicurezza.....	65
3.10.2 Configurazione del servizio di sistema.....	66
3.10.3 Attacco Difesa.....	67
3.10.4 Installazione del certificato del dispositivo.....	70
3.10.5 Installazione del certificato CA attendibile.....	73
3.10.6 Avviso di sicurezza.....	74
3.10.7 Autenticazione di sicurezza.....	75
4 Operazioni telefoniche.....	76
4.1 Inizializzazione.....	76
4.2 Accesso alla pagina Web.....	77
4.3 Pagina iniziale.....	78
4.4 Gestione del personale.....	80
4.5 Configurazione del sistema.....	83
4.5.1 Visualizzazione delle informazioni sulla versione.....	84
4.5.2 Manutenzione.....	84
4.5.3 Tempo di configurazione.....	84
4.5.4 Capacità dati.....	86
4.5.5 Lingua.....	86
4.6 Configurazione del controllo degli accessi.....	86
4.6.1 Configurazione dei metodi di sblocco.....	86
4.6.2 Configurazione dei parametri di controllo degli accessi.....	87
4.6.3 Configurazione degli allarmi.....	90
4.6.4 Configurazione del collegamento degli eventi di allarme.....	92
4.6.5 Configurazione del collegamento degli allarmi.....	93
4.6.6 Configurazione delle impostazioni della scheda.....	95

4.7 Impostazioni di comunicazione.....	97
4.7.1 Configurazione di TCP/IP.....	97
4.7.2 Configurazione del Wi-Fi.....	98
4.7.3 Configurazione dell'AP Wi-Fi.....	99
4.7.4 Configurazione del servizio cloud.....	100
4.7.5 Configurazione della registrazione automatica.....	100
4.7.6 Modalità di configurazione.....	101
4.8 Visualizzazione dei registri.....	104
4.8.1 Registri di sistema.....	104
4.8.2 Sblocca i record.....	105
4.8.3 Registri degli allarmi.....	105
5 Configurazione Smart PSS Lite.....	106
5.1 Installazione.....	106
5.2 Inizializzazione.....	106
5.3 Aggiunta di dispositivi.....	109
5.3.1 Aggiunta di un dispositivo tramite ricerca.....	110
5.3.2 Aggiunta dei dispositivi uno alla volta.....	111
5.3.3 Importazione del dispositivo in batch.....	112
5.4 Gestione utenti.....	113
5.4.1 Impostazione del tipo di scheda.....	113
5.4.2 Configurazione del tipo di scheda.....	113
5.4.3 Aggiunta di utenti.....	114
5.4.4 Assegnazione dei permessi di accesso.....	118
5.4.5 Assegnazione delle autorizzazioni di presenza.....	120
5.5 Monitoraggio del controllo accessi.....	123
Appendice 1 Punti importanti delle istruzioni per la registrazione delle impronte digitali.....	126
Appendice 2 Raccomandazione di sicurezza.....	128

1 Panoramica

Questo prodotto è un dispositivo di controllo accessi che integra lettura delle tessere, configurazione ed esecuzione. Il design è semplice ed elegante, e il prodotto è adatto a edifici per uffici, scuole, parchi, complessi residenziali, fabbriche, luoghi pubblici, centri commerciali, edifici governativi e altri contesti applicativi.

2 Operazioni locali

2.1 Inizializzazione

Dopo aver acceso il dispositivo per la prima volta, è necessario impostare la password di amministratore. La password di amministratore viene utilizzata per accedere al menu principale del dispositivo.

Procedura

Passo 1 Accendi il dispositivo e la spia luminosa lampeggerà lentamente in rosso.

Passo 2 Premi#, inserisci la password dell'amministratore e poi premi#.

La password deve essere lunga da 1 a 8 caratteri.

Se la spia luminosa è blu fissa, significa che il dispositivo è stato inizializzato.



Dopo l'inizializzazione, è possibile utilizzare solo le funzioni presenti sul Dispositivo. Se si desidera accedere alla pagina web del Dispositivo, è necessario inizializzare il Dispositivo tramite la relativa pagina web o attraverso il ConfigTool.

Operazioni correlate

- È possibile impostare numeri come password dell'account amministratore solo durante l'inizializzazione tramite il dispositivo.
- È possibile impostare numeri, lettere e altri caratteri come password dell'account amministratore durante la fase di inizializzazione tramite la piattaforma ConfigTool.

Dopo aver completato l'inizializzazione del dispositivo, è possibile eseguire operazioni solo sul dispositivo stesso. Se è necessario connettere il dispositivo alla rete, utilizzare ConfigTool o la piattaforma per inizializzarlo.

Quando si utilizza ConfigTool o la piattaforma per inizializzare il dispositivo, dopo aver configurato l'account di rete e la password, il dispositivo completerà automaticamente l'inizializzazione ed entrerà in modalità standby. La password di amministratore locale viene convertita dalla password di rete. Se la password supera gli 8 caratteri, vengono mantenuti solo i primi 8. Le lettere vengono convertite in cifre secondo lo standard E.161. La conversione della password non fa distinzione tra maiuscole e minuscole e tutti gli altri simboli vengono convertiti in 0.



- Dopo l'inizializzazione, se si modifica la password di rete, la password dell'amministratore locale non verrà modificata.
- Se si inizializza prima tramite il dispositivo e poi tramite ConfigTool o la piattaforma, la password dell'amministratore locale non verrà modificata.

Figura 2-1 E.161 (tastiera T9)

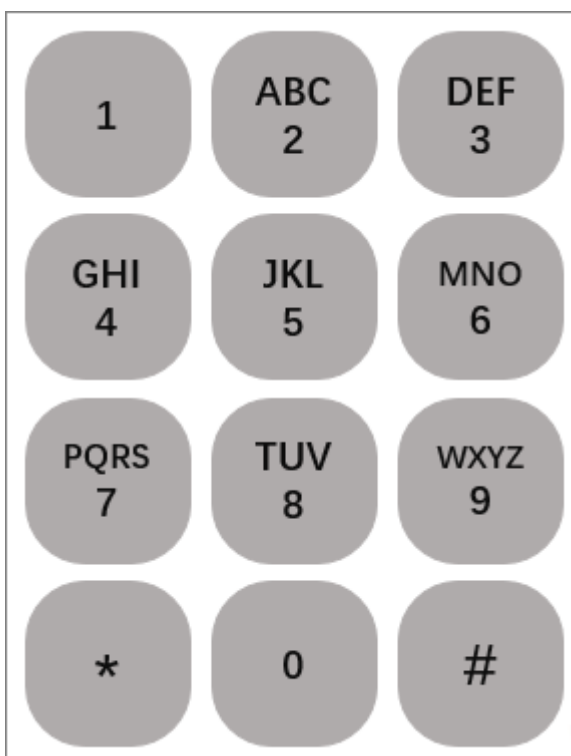


Tabella 2-1 Esempio di conversione

Password di rete	Password dell'amministratore locale
ABC12345	22212345
admin123	23646123
admin12!	23646120
admin123456	23646123

2.2 Menu principale

Accesso al menu principale

Premere#, inserisci la password dell'amministratore e poi premi#.

- L'indicatore lampeggia in blu e significa che sei entrato nel menu principale.
- L'indicatore lampeggia una volta in rosso, il cicalino emette 3 bip e poi l'indicatore diventa blu fisso, il che significa che la password è errata.

Suggerimenti correlati

- L'indicatore lampeggia una volta in verde e il cicalino emette un segnale acustico, a indicare che l'operazione o la verifica del controllo accessi è andata a buon fine.
- L'indicatore lampeggia una volta in rosso e il cicalino emette tre segnali acustici, il che significa che l'operazione o la verifica del controllo accessi non è andata a buon fine.
- Se l'indicatore lampeggia lentamente in rosso, significa che il dispositivo non è stato de-inizializzato.

- Se l'indicatore è blu fisso, significa che il dispositivo è in modalità standby.
- L'indicatore lampeggia in blu, a indicare che il dispositivo è entrato nel menu principale.
- La tastiera è bianca quando si utilizza il dispositivo. Se non viene rilevata alcuna operazione entro 10 secondi, la luce si spegne e il dispositivo esce dalla schermata corrente.

2.3 Gestione degli utenti

2.3.1 Aggiunta utente



- È possibile aggiungere una sola carta, una sola password o una sola impronta digitale per utente. È necessario aggiungere almeno un metodo di autenticazione tra carta, password e impronta digitale.
- La funzione di riconoscimento delle impronte digitali è disponibile su alcuni modelli.

Procedura

Passo 1 Premere#, inserisci la password dell'amministratore e poi premi#.

Accedi al menu principale e l'indicatore lampeggia in blu.

Passo 2 Premi1E#per aggiungere utenti. Inserisci l'ID utente e poi

Passo 3 premi#.

- Se l'indicatore non si accende e il dispositivo emette un segnale acustico, l'ID utente è stato aggiunto correttamente.
- Se l'indicatore lampeggia in rosso e il dispositivo emette un segnale acustico, l'aggiunta dell'ID utente non è andata a buon fine. Il motivo potrebbe essere che l'ID esiste già. Prova con un altro ID.



Sul dispositivo è possibile inserire solo numeri come ID.

Passo 4 Dopo aver strisciato la carta, premere#per aggiungere la scheda.

Se non è necessario aggiungere la carta, premere#per

Passo 5 saltarlo. Inserisci la password utente e poi premi#.

Se non è necessario impostare la password utente, premere#per saltarlo.



La password può essere lunga da 1 a 8 caratteri.

Passo 6 Aggiungi l'impronta digitale e poi premi#.

Se non è necessario impostare l'impronta digitale, premere#per saltarlo.



Questa funzione è disponibile su alcuni modelli.

Passo 7 RipeterePasso 2 APasso 6 per aggiungere altri utenti.

Dopo aver aggiunto l'utente, premere*per tornare al menu principale, quindi premere*per tornare allo stato di standby.

2.3.2 Eliminazione dell'utente

Procedura

Passo 1 Premere#, inserisci la password dell'amministratore e poi premi#.

Accedi al menu principale e l'indicatore lampeggia in blu.

Passo 2 Premi2E#.

Passo 3 Eliminare un utente.

- Fai scorrere la carta e poi premi#.



Se si striscia una carta che non è stata aggiunta, l'eliminazione non va a buon fine.

- Inserisci l'ID utente e poi premi#.



Se si inserisce un ID non ancora aggiunto, l'eliminazione non andrà a buon fine.

- Inserisci 0000 e poi premi#eliminare tutti gli utenti.

Dopo la cancellazione, premere*per tornare al menu principale, quindi premere*per uscire dal menu principale.

2.4 Configurazione della modalità di sblocco della porta

Informazioni di base



La funzione di riconoscimento delle impronte digitali è disponibile su alcuni modelli.

Procedura

Passo 1 Premere#, inserisci la password dell'amministratore e poi premi#.

Accedi al menu principale e l'indicatore lampeggia in blu.

Passo 2 Premi3E#.

Passo 3 Seleziona la modalità di sblocco.

- Premere0E#per impostare lo sblocco tramite carta, password o impronta digitale.

Per aprire la porta, striscia la tessera, inserisci la password o usa l'impronta digitale. La password prevede i seguenti metodi.

- ◇ Nella schermata di standby, inserire l'ID utente e premere#e il dispositivo emette un segnale acustico una volta. Inserisci la password e poi premi#per verificare l'identità.
- ◇ Nella schermata di standby, immettere la password pubblica e quindi premere#per verificare l'identità.
- ◇ Quando il**Autenticazione tramite codice PIN**Se questa funzione è abilitata sulla pagina web del Dispositivo, gli utenti possono verificare la propria identità semplicemente inserendo la password.
- ◇ Quando il dispositivo viene utilizzato con l'app DMSS, la password temporanea è supportata e può essere configurata tramite l'app.

- Premere1E#per impostare lo sblocco tramite scheda e password utente.

Prima striscia la carta. Dopo che il dispositivo emette un segnale acustico, inserisci la password e poi premi# per verificare l'identità.

- Premere2E#per impostare lo sblocco tramite tessera e impronta digitale.

Per prima cosa, striscia la carta. Dopo che il dispositivo emette un segnale acustico, premi il sensore di impronte digitali per verificare l'identità.

- Premere **3E#** per impostare lo sblocco tramite carta, password e impronta digitale.

Prima striscia la carta. Dopo che il dispositivo emette un segnale acustico, premi l'impronta digitale. Il dispositivo emette un altro segnale acustico. Inserisci la password e poi premi **#** per verificare l'identità.

Passo 4 Premere ***** per uscire dal menu principale.

2.5 Configurazione della durata dello sblocco

La porta rimane aperta per un determinato periodo di tempo dopo lo sblocco, consentendo il passaggio delle persone.

Procedura

Passo 1 Premere **#**, inserisci la password dell'amministratore e poi premi **#**.

Accedi al menu principale e l'indicatore lampeggia in blu.

Passo 2 Premi **4E#**.

Passo 3 Inserisci l'ora e poi premi **#**.

Il valore varia da 1 secondo a 600 secondi. Il valore predefinito è 3 secondi. Premi ***** per

Passo 4 uscire dal menu principale.

2.6 Configurazione del sensore della porta

Una volta attivato il sensore porta, l'allarme di timeout della porta viene attivato contemporaneamente per impostazione predefinita. Se la porta rimane aperta dopo il periodo di timeout impostato, il cicalino del dispositivo genera un allarme.

Procedura

Passo 1 Premere **#**, inserisci la password dell'amministratore e poi premi **#**.

Accedi al menu principale e l'indicatore lampeggia in blu.

Passo 2 Premi **5E#**.

Passo 3 Attiva o disattiva il sensore della porta.

Il sensore della porta è disattivato di default.

- Premere **0E#** per disattivare il sensore della porta.
- Premere **1E#** per attivare il sensore della porta.

Passo 4 Premere ***** per uscire dal menu principale.

2.7 Gestione delle password

- Password amministratore: utilizzata per accedere al menu principale del dispositivo.
- Password pubblica: utilizzata per verificare l'autenticazione e sbloccare la porta.

2.7.1 Modifica della password dell'amministratore

Per garantire la sicurezza del dispositivo, si consiglia di modificare periodicamente la password di amministratore.

Procedura

Passo 1 Premere **#**, inserisci la password dell'amministratore e poi premi **#**

Accedendo al menu principale, l'indicatore lampeggia in blu.

Passo 2 Premere **0E#**.

Passo 3 Inserisci la nuova password e poi premi **#**. Inserisci di

Passo 4 nuovo la nuova password e poi premi **#**.

- Il lampeggio verde indica che la password è stata modificata correttamente.
- Il lampeggio rosso indica che la modifica della password non è andata a buon fine.
- Dopo la modifica, il dispositivo esce automaticamente dal menu principale e l'indicatore diventa blu fisso. Se la modifica della password è andata a buon fine, accedi al menu principale utilizzando la nuova password. Se la modifica della password non riesce, accedi al menu principale utilizzando la password originale.

2.7.2 Aggiunta della password pubblica

Procedura

Passo 1 Premere **#**, inserisci la password dell'amministratore e poi premi **#**.

Accedi al menu principale e l'indicatore lampeggia in blu.

Passo 2 Premi **6E#**.

Passo 3 Inserisci la password pubblica e poi premi **#**.

La password può essere lunga da 1 a 8 caratteri.



È possibile aggiungere una sola password pubblica. Se si ripetono le operazioni, la nuova password sostituirà quella originale.

Passo 4 Premere ***** per uscire dal menu principale.

2.7.3 Eliminazione della password pubblica

Procedura

Passo 1 Premere **#**, inserisci la password dell'amministratore e poi premi **#**.

Accedi al menu principale e l'indicatore lampeggia in blu.

Passo 2 Premi **7E#**.

Passo 3 Inserisci la password pubblica e premi **#**.

Passo 4 Premere ***** per uscire dal menu principale.

2.8 Gestione della scheda principale

2.8.1 Aggiunta della scheda principale

Dopo aver aggiunto la scheda principale, è possibile aggiungere ed eliminare rapidamente altre schede utente tramite la scheda principale.

Informazioni di base



La tessera principale non può essere utilizzata per sbloccare la porta.

Procedura

- Passo 1** Premere#, inserisci la password dell'amministratore e poi premi#.
- Accedi al menu principale e l'indicatore lampeggia in blu.
- Passo 2** Premi8E#.
- Passo 3** Fai scorrere la carta e poi premi#.
- Se l'indicatore lampeggia in verde e il dispositivo emette un segnale acustico, significa che la scheda è stata aggiunta come scheda principale.
 - Se l'indicatore lampeggia in rosso e il dispositivo emette un segnale acustico, significa che non si è riusciti ad aggiungere la scheda come scheda principale.
- 
- Le schede utente aggiunte possono essere impostate anche come schede principali.
 - Se una tessera utente è impostata come tessera principale, non sarà in grado di sbloccare la porta.
 - Supporta una sola scheda madre. Se si aggiunge una nuova scheda madre, la precedente verrà sovrascritta.
- Passo 4** Premere*per uscire dal menu principale.

2.8.2 Eliminazione della scheda principale

Procedura

- Passo 1** Premere#, inserisci la password dell'amministratore e poi premi#.
- Accedi al menu principale e l'indicatore lampeggia in blu.
- Passo 2** Premi9E#.
- Passo 3** Passa la carta e premi#. Premere*
- Passo 4** per uscire dal menu principale.

2.8.3 Gestione delle schede utente tramite la scheda principale

Se non viene eseguita alcuna operazione entro 3 secondi dallo strisciamento della carta principale, il dispositivo entra in modalità carta principale e determina la funzione corrispondente in base al numero di strisciamenti della carta. In modalità carta principale, l'indicatore lampeggia alternativamente in rosso e blu e, se non viene eseguita alcuna operazione per 10 secondi o se si striscia nuovamente la carta principale una sola volta, il dispositivo torna allo stato di standby.

- Aggiungi una scheda utente: passa una volta la scheda principale, poi passa la scheda utente per aggiungerla. È possibile aggiungere schede utente in modo continuativo.
- Elimina la scheda utente: passa due volte la scheda principale, quindi passa la scheda utente per eliminarla. Le schede utente possono essere eliminate ripetutamente.
- Cancella tutte le carte utente: striscia la carta principale 5 volte di seguito.

2.9 Configurazione del periodo di timeout della porta

Dopo aver attivato il sensore per porte, se la porta rimane aperta oltre il tempo impostato, il cicalino del dispositivo emetterà un allarme.

Procedura

- Passo 1** Premere#, inserisci la password dell'amministratore e poi premi#.

Accedi al menu principale e l'indicatore lampeggia in blu.

Passo 2 Premi**10E#**.

Passo 3 Inserisci il periodo di timeout della porta e poi premi**#**.

Il valore può variare da 1 secondo a 9999 secondi. Il valore predefinito è 60 secondi. Premi*****per

Passo 4 uscire dal menu principale.

2.10 Ripristino delle impostazioni di fabbrica

Procedura

Passo 1 Premere**#**, inserisci la password dell'amministratore e poi premi**#**.

Accedi al menu principale e l'indicatore lampeggia in blu.

Passo 2 Premi**11E#**.

Passo 3 Ripristina il dispositivo alle impostazioni di fabbrica.

- Premere**00E#**per ripristinare le impostazioni di fabbrica (mantenere le informazioni utente).
- Premere**000E#**per ripristinare le impostazioni di fabbrica (ripristinare tutte le informazioni).

Operazioni correlate

È possibile utilizzare il pulsante di ripristino per riportare il dispositivo alle impostazioni di fabbrica.

3 Operazioni sulle pagine web

Sulla pagina web è inoltre possibile configurare e aggiornare il dispositivo.



Le configurazioni web variano a seconda del modello del dispositivo.

3.1 Inizializzazione

Inizializza il dispositivo al primo accesso alla pagina web o dopo il ripristino delle impostazioni di fabbrica.

Prerequisiti

Assicurati che il computer utilizzato per accedere alla pagina web si trovi sulla stessa rete LAN del dispositivo.

Procedura

Passo 1 Apri un browser e vai all'indirizzo IP (l'indirizzo predefinito è 192.168.1.108) del dispositivo.



Si consiglia di utilizzare la versione più recente di Chrome o Firefox.

Passo 2 Seleziona una lingua per il dispositivo.

Passo 3 Imposta la password e l'indirizzo email seguendo le istruzioni visualizzate sullo schermo.



- La password deve essere composta da 8 a 32 caratteri non vuoti e contenere almeno due dei seguenti tipi di caratteri: maiuscole, minuscole, numeri e caratteri speciali (esclusi ' , ; : e). Imposta una password ad alta sicurezza seguendo le istruzioni per la complessità della password.
- Dopo l'inizializzazione, conserva la password in un luogo sicuro e cambiala regolarmente per migliorare la sicurezza.

Operazioni correlate

- È possibile impostare numeri come password dell'account amministratore solo durante l'inizializzazione tramite il dispositivo.
- È possibile impostare numeri, lettere e altri caratteri come password dell'account amministratore durante la fase di inizializzazione tramite la piattaforma ConfigTool.

Dopo aver completato l'inizializzazione del dispositivo, è possibile eseguire operazioni solo sul dispositivo stesso. Se è necessario connettere il dispositivo alla rete, utilizzare ConfigTool o la piattaforma per iniziarlo.

Quando si utilizza ConfigTool o la piattaforma per inizializzare il dispositivo, dopo aver configurato l'account di rete e la password, il dispositivo completerà automaticamente l'inizializzazione ed entrerà in modalità standby. La password di amministratore locale viene convertita dalla password di rete. Se la password supera gli 8 caratteri, vengono mantenuti solo i primi 8. Le lettere vengono convertite in cifre secondo lo standard E.161. La conversione della password non fa distinzione tra maiuscole e minuscole e tutti gli altri simboli vengono convertiti in 0.



- Dopo l'inizializzazione, se si modifica la password di rete, la password dell'amministratore locale non verrà modificata.
- Se si inizializza prima tramite il dispositivo e poi tramite ConfigTool o la piattaforma, la password dell'amministratore locale non verrà modificata.

Figura 3-1 E.161 (tastiera T9)

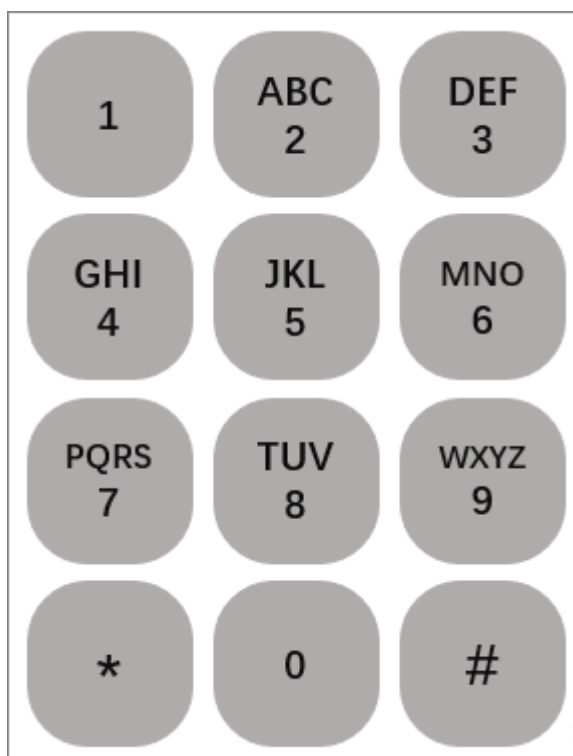


Tabella 3-1 Esempio di conversione

Password di rete	Password dell'amministratore locale
ABC12345	22212345
admin123	23646123
admin12!	23646120
admin123456	23646123

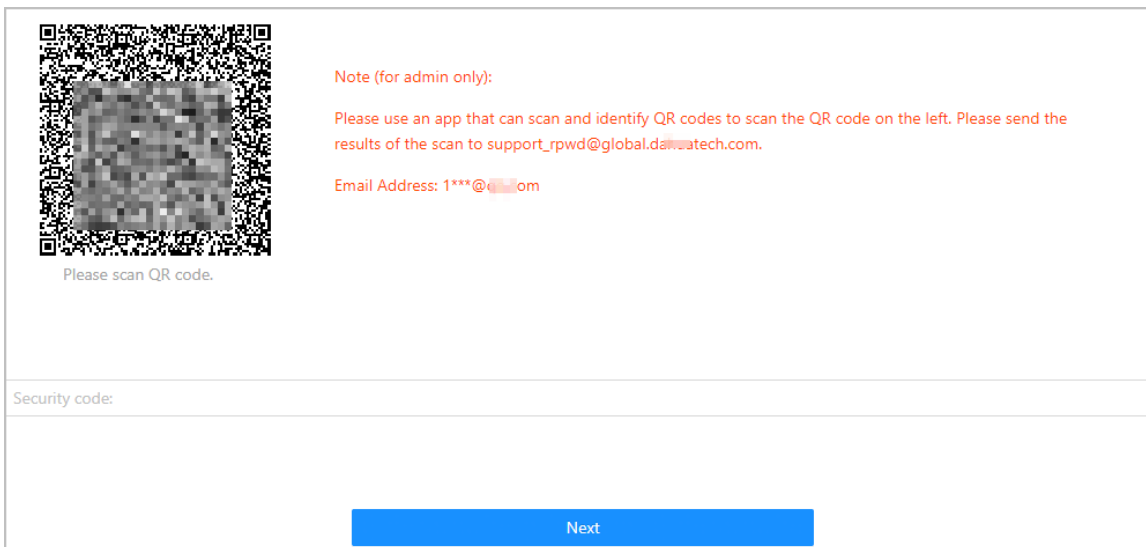
3.2 Reimpostazione della password

Se dimentichi la password di amministratore, reimpostala tramite l'e-mail allegata.

Procedura

- Passo 1** Nella pagina di accesso, fai clic **Ha dimenticato la password**.
- Passo 2** Leggi attentamente le istruzioni visualizzate sullo schermo, quindi fai
- Passo 3** clic **OK** Scansiona il codice QR e riceverai un codice di sicurezza.

Figura 3-2 Reimposta la password



Note (for admin only):

Please use an app that can scan and identify QR codes to scan the QR code on the left. Please send the results of the scan to support_rpwd@global.damtech.com.

Email Address: 1***@damtech.com

Please scan QR code.

Security code:

Next



- Quando si scansiona lo stesso codice QR, verranno generati fino a due codici di sicurezza. Se il codice di sicurezza non è più valido, aggiornare il codice QR e ripetere la scansione.
- Dopo aver scansionato il codice QR, riceverai un codice di sicurezza all'indirizzo e-mail associato al tuo account. Utilizza il codice di sicurezza entro 24 ore dalla ricezione. In caso contrario, non sarà più valido.
- Se viene inserito il codice di sicurezza errato per 5 volte consecutive, l'account amministratore verrà bloccato per 5 minuti.

Passo 4 Inserisci il codice di sicurezza. Fai

Passo 5 clic**Prossimo**.

Passo 6 Reimposta e conferma la password.



La password deve essere composta da 8 a 32 caratteri non vuoti e contenere almeno due dei seguenti tipi di caratteri: maiuscolo, minuscolo, numero e carattere speciale (esclusi ' " ; : &).

Passo 7 Clic**OK**.

3.3 Pagina iniziale

La pagina iniziale viene visualizzata dopo aver effettuato l'accesso con successo.

Figura 3-3 Pagina iniziale

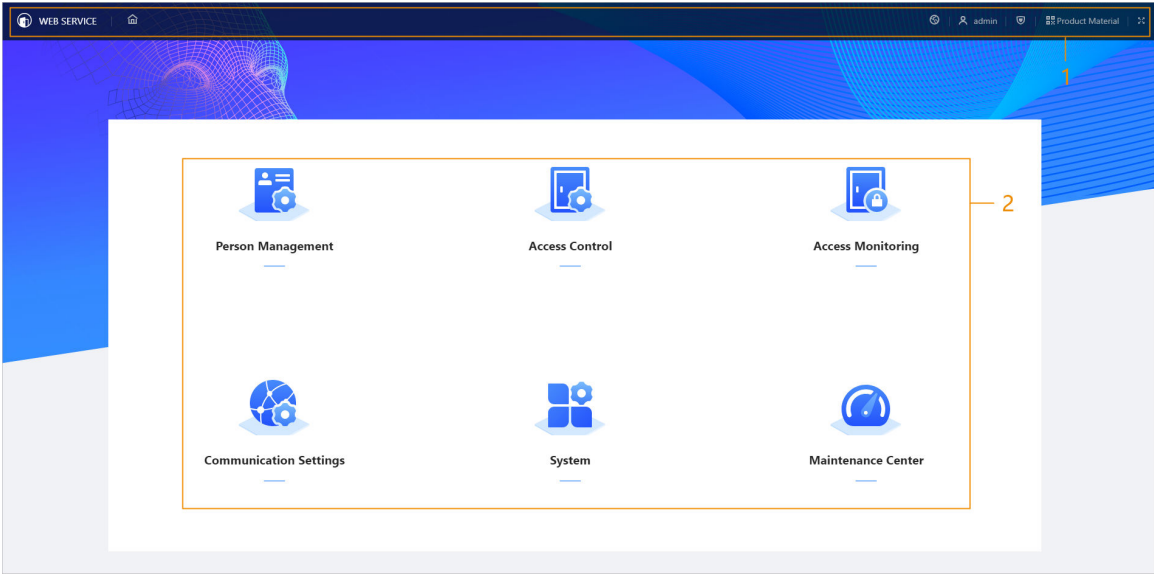


Tabella 3-2 Descrizione della pagina iniziale

NO.	Descrizione
1	🏠: Accedi alla pagina iniziale. 🌐: Seleziona una lingua sul dispositivo. 👤 admin: Disconnettiti o riavvia il dispositivo. 🔒: Inserisci il Sicurezza pagina. 📄 Materiale del prodotto: Scansiona il codice QR per visualizzare il materiale del prodotto.  Questa funzione è disponibile su alcuni modelli. 🖥️: Visualizza a schermo intero.
2	Menù principale.

3.4 Gestione del personale

Procedura

- Passo 1 Nella pagina iniziale, selezionare **Gestione del personale**, e poi fai clic **Aggiungere**
- Passo 2 Configura le informazioni utente.

Figura 3-4 Aggiungi utenti

Add
X

Basic Info

* No.

Name

* User Type
General User
v

* Times Used
Unlimited

* General Plan
255-Default x

* Holiday Plan
255-Default x

Validity Period
2037-12-31 23:59:59

Verification Mode

v Password
Not Added

Add

> Card
Not Added

> Fingerprint
Not Added

Add
Add More
Cancel

Tabella 3-3 Descrizione dei parametri

Parametro	Descrizione
NO.	Il numero è simile a un codice identificativo del dipendente, che può essere composto da numeri, lettere e loro combinazioni, e la lunghezza massima del numero è di 30 caratteri.
Nome	Il nome può contenere fino a 32 caratteri (inclusi numeri, simboli e lettere).

Parametro	Descrizione
Tipo di utente	● Utente generico: Gli utenti generici possono sbloccare la porta. ● Utente bloccato: Quando gli utenti presenti nella lista nera sbloccano la porta, il personale di servizio riceverà una notifica. ● Utente ospite: Gli ospiti possono sbloccare la porta entro un periodo di tempo definito o per un numero limitato di volte. Trascorso il periodo definito o il numero di volte in cui è possibile sbloccare la porta, non sarà più possibile farlo. ● Utente di pattuglia: Gli utenti addetti alla pattuglia possono registrare le presenze sul dispositivo, ma non hanno l'autorizzazione ad aprire le porte. ● Utente VIP: Quando i VIP sbloccano la porta, non sono limitati dalle modalità di sblocco, come Multi-carta e Sezione temporale. ● Altro utente: Quando sbloccano la porta, questa rimarrà sbloccata per altri 5 secondi. ● Utente personalizzato 1/Utente personalizzato 2: Uguali agli utenti generici.
Numero di volte utilizzato	Imposta un limite di tempo per lo sblocco degli utenti ospiti. Trascorso tale periodo, non potranno più aprire la porta.
Piano generale	Durante il periodo definito, le persone possono sbloccare la porta o effettuare il rilevamento delle presenze.  È possibile selezionare più di un piano.
Piano vacanze	Durante il periodo festivo definito, è possibile sbloccare la porta o effettuare il rilevamento delle presenze.  È possibile selezionare più di una festività.
Periodo di validità	Imposta una data di scadenza per l'accesso e l'autorizzazione alla presenza della persona.
Password	Inserisci la password utente. La lunghezza massima della password è di 8 cifre. La password di emergenza è la password di sblocco + 1. Ad esempio, se la password utente è 12345, la password di emergenza sarà 12346. Un allarme di emergenza si attiverà quando si utilizza la password di emergenza per sbloccare la porta.

Parametro	Descrizione
Carta	Ogni utente può registrare al massimo 5 carte. Inserisci il numero della tua carta oppure strisciala sul dispositivo o su un lettore di carte esterno; a quel punto, il dispositivo leggerà le informazioni della carta. ● Inserisci manualmente il numero della carta. 1. Fare clic Aggiungere. 2. Inserisci il numero della carta e poi fai clic Aggiungere. ● Il numero viene letto automaticamente tramite il lettore di registrazione o il dispositivo. 1. Fare clic Aggiungere, e poi fai clic Modificare per selezionare un lettore di registrazione o il Dispositivo. 2. Leggi la carta. ◇ Per il lettore di carte d'identità e IC per la registrazione, fare clic qui. Leggi la scheda e poi strisciare le carte sul lettore di carte. Viene visualizzato un conto alla rovescia di 60 secondi per ricordarti di strisciare le carte e il sistema leggerà automaticamente il numero della carta. Se il conto alla rovescia di 60 secondi scade, fai clic Leggi la scheda di nuovo per iniziare un nuovo conto alla rovescia. ◇ Per il lettore di registrazione della scheda Desfire, posizionare la scheda sul lettore di registrazione e quindi fare clic Leggi la scheda. Se sulla carta Desfire è stato scritto il numero della carta, questo verrà letto e visualizzato qui. Se la carta è vuota, è necessario prima scrivere il numero della carta. Il numero della carta sarà generato automaticamente sul computer e scritto sulla scheda. 3. Fare clic Aggiungere. È possibile abilitare il Carta di coercizione funzione. Si attiverà un allarme se si utilizza una tessera di emergenza per sbloccare la porta. ●  : Imposta la carta coercizione. ●  : Modifica il numero della carta.  Ogni utente può impostare una sola carta di coercizione.

Parametro	Descrizione
Impronta digitale	Registrazione delle impronte digitali. Un utente può registrare fino a 3 impronte digitali ed è possibile impostarne una come impronta digitale di emergenza. Un allarme si attiverà quando l'impronta digitale di emergenza viene utilizzata per sbloccare la porta. Registra le impronte digitali tramite un lettore di impronte o il dispositivo. 1. Fare clic Aggiungere, e poi fai clic Modificare per selezionare un lettore di registrazione o il Dispositivo. 2. Premere il dito sullo scanner seguendo le istruzioni visualizzate sullo schermo. 3. Fare clic Aggiungere.  ● La funzione di riconoscimento delle impronte digitali è disponibile solo su alcuni modelli. ● Non consigliamo di impostare la prima impronta digitale come impronta digitale di emergenza. ● Ogni utente può impostare una sola impronta digitale di emergenza. ● La funzione di riconoscimento delle impronte digitali è disponibile se il dispositivo supporta la connessione di un modulo per impronte digitali.

Passo 3 **Clic OK.**

Operazioni correlate

- Importa le informazioni utente: fai clic **Esportare**, Scarica il modello e inserisci le informazioni dell'utente al suo interno. Fai clic **Importare** per importare la cartella.



È possibile importare fino a 10.000 utenti contemporaneamente.

- Cancella: Cancella tutti gli utenti.
- Aggiorna: Aggiorna l'elenco degli utenti.
- Clic  per modificare le informazioni della persona.
- Seleziona le persone e poi fai clic **Eliminare** per eliminare gli utenti.
- Ricerca: cerca per nome utente o ID utente.

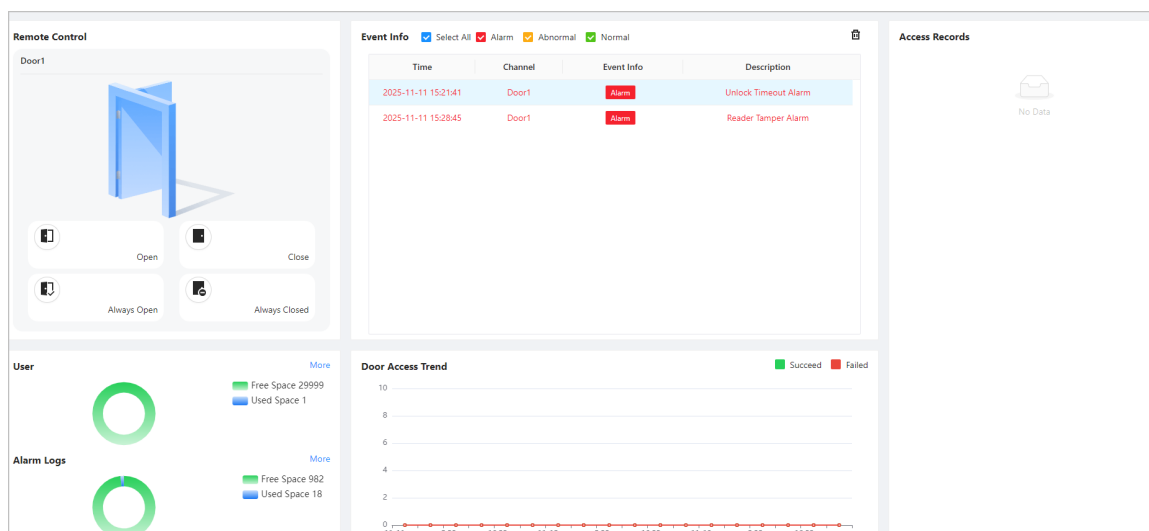
3.5 Monitoraggio degli accessi

Accedi alla pagina web e il sistema andrà automaticamente alla **Monitoraggio degli accessi** pagina.



- Al primo utilizzo, si prega di scaricare e installare il plug-in seguendo le istruzioni.
- È inoltre possibile fare clic sull'icona del servizio web nell'angolo in alto a sinistra per visualizzare la pagina di monitoraggio degli accessi.

Figura 3-5 Monitoraggio degli accessi



Telecomando

- Clic**Aprire**O**Vicino** accanto alla porta per controllarla a distanza.
- Clic**Sempre aperto**O**Sempre chiuso** per controllare la porta a distanza. Fare clic**Ripristinare** per ripristinare la porta al suo stato normale.

Tendenza all'accesso tramite porta

Viene mostrato l'andamento degli accessi negli ultimi 3 giorni. Il verde indica un accesso riuscito, il rosso un accesso non riuscito.

Accesso ai record

Vengono visualizzati i registri degli accessi in tempo reale, comprensivi di immagine, informazioni sulla persona, metodo di verifica e orario di verifica.

Informazioni sull'evento

Nel**Informazioni sull'evento** area, seleziona il tipo di evento per visualizzare gli eventi. Fai clic



per cancellare tutti gli eventi.

Registri utenti e allarmi

Visualizza le informazioni sullo spazio degli utenti e i registri degli allarmi. Fai clic**Di più** per visualizzare i dettagli.

3.6 Configurazione del controllo degli accessi

3.6.1 Configurazione dei parametri di controllo degli accessi

3.6.1.1 Configurazione dei parametri di base

Procedura

Passo 1 Selezionare **Controllo degli accessi** > **Parametri di controllo degli accessi**.

Passo 2 In **Impostazioni di base**, configurare i parametri di base per il controllo degli accessi.

Figura 3-6 Parametri di base

Tabella 3-4 Descrizione dei parametri di base

Parametro	Descrizione
Nome	Il nome della porta.
Stato della porta	Imposta lo stato della porta. ● Normale: La porta verrà sbloccata e bloccata in base alle impostazioni selezionate. ● Sempre aperto: la porta rimane sempre sbloccata. ● Sempre chiuso: la porta rimane sempre chiusa a chiave.
Periodo di apertura normale	Quando selezioni Normale È possibile selezionare un intervallo di tempo dall'elenco a discesa. La porta rimarrà aperta o chiusa durante il periodo di tempo definito.
Periodo di chiusura normale	 ● Quando il periodo normalmente aperto è in conflitto con il periodo normalmente chiuso, Il periodo normalmente aperto ha la priorità sul periodo normalmente chiuso. ● Quando il periodo coincide con i piani per le vacanze, questi ultimi hanno la precedenza.

Parametro	Descrizione
Intervallo di verifica	Se verifichi la tua identità più volte entro un periodo di tempo definito, solo la prima verifica sarà considerata valida e la porta non si aprirà dopo la seconda o le successive verifiche. Dal momento in cui la porta non si apre, dovrai attendere l'intervallo di tempo di verifica configurato prima di poter tentare nuovamente di verificare la tua identità.
Intervallo di strisciamento della carta	Al primo utilizzo della carta per la verifica, è normalmente possibile sbloccare la porta o effettuare la rilevazione delle presenze e i dati vengono generati. Entro il periodo configurato, se si utilizza nuovamente la carta per la verifica, non sarà possibile sbloccare la porta o effettuare la rilevazione delle presenze e i dati non verranno generati. Si prega di verificare l'identità dopo il periodo configurato.  IL Intervallo di strisciamento della carta ha la priorità su Intervallo di verifica.
Password pubblica	Dopo aver abilitato la password pubblica, configura la password. Puoi utilizzare la password pubblica senza inserire l'ID utente per sbloccare la porta. È supportata una sola password pubblica per dispositivo.

Passo 3 Clic **Fare domanda a.**

3.6.1.2 Configurazione dei metodi di sblocco

Per sbloccare la porta è possibile utilizzare diversi metodi, come l'impronta digitale, la tessera e la password. È anche possibile combinarli per creare un metodo di sblocco personalizzato.

Procedura

Passo 1 Selezionare **Controllo degli accessi** > **Parametri di controllo degli accessi**. In

Passo 2 **Sblocca le impostazioni**, selezionare un metodo di sblocco.

● Sblocco tramite combinazione

1. Seleziona **Sblocco tramite combinazione** dal **Metodo di sblocco** lista.

2. Seleziona **OOE**.

- ◇ Oppure: Utilizza uno dei metodi di sblocco selezionati per aprire la porta. E
- ◇ ancora: Utilizza tutti i metodi di sblocco selezionati per aprire la porta.

3. Seleziona i metodi di sblocco e poi configura gli altri parametri.

Figura 3-7 Sblocco tramite combinazione

- Sbloccabile da più utenti.

- ◇ Se viene aggiunto un solo gruppo, la porta si sblocca solo quando il numero di persone appartenenti a quel gruppo che concedono l'accesso raggiunge il numero valido predefinito.
- ◇ Se vengono aggiunti più gruppi, la porta si sblocca solo quando il numero di persone in ciascun gruppo che concedono l'accesso raggiunge il numero valido predefinito.

1. Nel **Modalità di sblocco** elenco, selezionare **Sbloccato da più utenti**.

2. Fare clic **Aggiungere** per aggiungere gruppi.

3. Seleziona il metodo di sblocco e gli utenti, configura il numero valido e poi fai clic **OK**.

- ◇ È possibile aggiungere fino a 4 gruppi.
- ◇ I metodi di sblocco supportano solo la relazione **di O**.
- ◇ Il valore "Numero valido" indica il numero di persone in ciascun gruppo che devono verificare la propria identità sul dispositivo prima che la porta si sblocchi. Ad esempio, se il valore "Numero valido" è impostato su 3 per un gruppo, 3 persone qualsiasi del gruppo dovranno verificare la propria identità per sbloccare la porta.

Il numero valido non può superare il numero di utenti presenti nell'elenco utenti.

Figura 3-8 Aggiungi gruppo

Add

No.1

Unlock Method ...Card x

Valid No.1

Select PersonUser ID/Name

	No.	User ID	Name
☒	1	1000...	10000001
☒	2	1000...	10000002
☐	3	1000...	10000003
☐	4	1000...	10000004
☐	5	1000...	10000005

Selected PeopleClear

No.	User ID	Name	Operation
1	100000...	100000...	
2	100000...	100000...	

OKCancel

Figura 3-9 Sblocco da parte di più utenti

Unlock MethodUnlock by Multiple Users

You can add up to 4 multi-person unlock groups.

Add

No.	User List	Unlock Method	Valid No.	Operation
1	1	Card	1	

Verification of Multi-person Unlock Timeout Duration20s (10-60)

PIN Code Authentication

Door Unlocked Duration3.0s (0.2-600)

Remote Verification

ApplyRefreshDefault

Tabella 3-5 Descrizione delle impostazioni di sblocco

Parametro	Descrizione
Metodo di sblocco (selezione multipla)	Le procedure di sblocco possono variare a seconda del modello del prodotto.
Verifica della durata del timeout di sblocco multiutente	Durante la verifica, l'intervallo tra ogni due verificatori deve rientrare in questo periodo di tempo.

Parametro	Descrizione
Autenticazione tramite codice PIN	Quando l'autenticazione tramite codice PIN è abilitata e si seleziona la password utente per sbloccare il dispositivo, è sufficiente inserire la password utente, senza bisogno dell'ID utente. Quando l'autenticazione tramite codice PIN è abilitata, la verifica remota non è supportata quando si utilizza la password utente per sbloccare il dispositivo.
Durata dello sblocco della porta	Una volta concesso l'accesso, la porta rimarrà sbloccata per un periodo di tempo predefinito, che va da 0,2 a 600 secondi, per permettere alla persona di attraversarla.
Verifica a distanza	Se questa funzione è abilitata, è possibile controllare la porta sulla piattaforma corrispondente.

● Sblocca per periodo

1. Nel **Metodo di sblocco** elenco, selezionare **Sblocco per periodo**.

2. Trascina il cursore per regolare il periodo di tempo per ogni giorno.



Puoi anche cliccare **Copia** per applicare il periodo di tempo configurato ad altri giorni.

3. Seleziona un metodo di sblocco per il periodo di tempo desiderato, quindi configura gli altri parametri.

Figura 3-10 Sblocco per periodo

Unlock Method: Unlock by Period

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Sun	Card/Fingerprint/Password																								Copy
Mon	Card/Fingerprint/Password																								Copy
Tue	Card/Fingerprint/Password																								Copy
Wed	Card/Fingerprint/Password																								Copy
Thu	Card/Fingerprint/Password																								Copy
Fri	Card/Fingerprint/Password																								Copy
Sat	Card/Fingerprint/Password																								Copy

Time: 00:00:00 - 23:59:59

Combination ... ☒ Or ☐ And

Unlock Method... ☒ Card ☒ Fingerprint ☒ Password

OK Delete

Door Unlocked Duration: s (0.2-600)

Remote Verification: ☐

Passo 3 ClicFare domanda a.

3.6.2 Allarme

3.6.2.1 Configurazione dell'allarme

Si attiverà un allarme in caso di accesso anomalo.

Procedura

Passo 1 Selezionare **Controllo degli accessi** > **Allarme** > **Allarme**

Passo 2 (Facoltativo) Selezionare il canale della porta.

Se hai selezionato **Modulo di estensione serratura** come il **Ora** Attraverso **Impostazioni di comunicazione>Impostazioni RS-485** Sul controller di accesso, qui è possibile selezionare il canale.

Figura 3-11 Selezionare il canale

Door Channel

1

▼

Passo 3 Configura i parametri di allarme.

Figura 3-12 Allarme

Duress Alarm

Anti-passback

Door Detector

NCNO

Intrusion Alarm

Unlock Timeout Alarm

Unlock Timeout

60

s (1-9999)

Excessive Attempts Ala...

Apply

Refresh

Default

Tabella 3-6 Descrizione dei parametri di allarme

Parametro	Descrizione
Allarme coercizione	Si attiverà un allarme qualora si utilizzi una tessera, una password o un'impronta digitale di emergenza per sbloccare la porta.

Parametro	Descrizione
Anti-passback	Gli utenti devono verificare la propria identità sia in entrata che in uscita; in caso contrario, scatterà un allarme. Questo sistema impedisce al titolare di una tessera di accesso di passarla a un'altra persona per entrare. Quando la funzione anti-passback è attiva, il titolare della tessera deve uscire dall'area protetta passando attraverso un lettore di uscita prima che il sistema possa consentirne un altro accesso. ● Se una persona entra dopo essere stata autorizzata ed esce senza autorizzazione, al successivo tentativo di accesso si attiverà un allarme e l'accesso verrà contemporaneamente negato. ● Se una persona entra senza autorizzazione ed esce dopo aver ottenuto l'autorizzazione, al successivo tentativo di accesso si attiverà un allarme e l'accesso verrà negato.  Se il dispositivo può connettersi a un solo lucchetto, la verifica sul dispositivo stesso corrisponde, per impostazione predefinita, alla direzione di ingresso, mentre la verifica sul lettore di schede esterno corrisponde alla direzione di uscita. È possibile modificare l'impostazione sulla piattaforma di gestione.
Rilevatore di porte	Con il rilevatore di porte collegato al dispositivo, l'allarme può attivarsi quando le porte vengono aperte o chiuse in modo anomalo. Il rilevatore di porte è disponibile in due tipologie: rilevatore NC e rilevatore NO. ● NC: Il sensore è in cortocircuito quando la porta o la finestra sono chiuse. ● NO: Si crea un circuito aperto quando la finestra o la porta sono effettivamente chiuse.
Allarme antintrusione	Se la porta viene aperta in modo anomalo, si attiverà un allarme antintrusione che durerà per un periodo di tempo predefinito.  Il rilevatore di porte e il sistema antintrusione devono essere attivati contemporaneamente.
Sblocca allarme timeout	Se la porta rimane sbloccata per un periodo superiore al tempo di timeout impostato, si attiverà l'allarme di timeout, che durerà per la durata definita.
Timeout di sblocco	 È necessario attivare contemporaneamente il rilevatore di porta e la funzione di apertura automatica della porta.
Allarme tentativi eccessivi	Se la password o la carta errata vengono utilizzate 5 volte di seguito entro 60 secondi, si attiverà l'allarme per utilizzo eccessivo di carta non valida, che durerà per un periodo di tempo predefinito.

Passo 4

ClicFare domanda a.

3.6.2.2 Configurazione dei collegamenti di allarme (facoltativo)

È possibile configurare i collegamenti degli allarmi.

Procedura

Passo 1 Selezionare **Controllo degli accessi > Allarme > Impostazione collegamento allarme**.



- Se il dispositivo viene aggiunto a una piattaforma di gestione, le impostazioni di allarme verranno sincronizzate con la piattaforma.
- Questa funzione è disponibile solo sui modelli dotati di porte di ingresso e uscita allarme.
- Il numero di porte di ingresso e uscita per gli allarmi varia a seconda del modello del prodotto.

Passo 2 Clic  per configurare l'allarme.

Figura 3-13 Collegamento dell'allarme

Alarm-in Port: 1 Name: Zone1

Alarm Input Type: NO Link Fire Safety Control: ☐

Alarm-out Port: ☐

Duration: 30 s (1-300)

Alarm Output Channel: ☒ 1

Access Control Linkage: ☐

! When the heat alarm signal disappears, the door will automatically return to the normal authentication mode.

Linkage Mode: Weak Execution

Channel Type: NO

OK Cancel

Passo 3 Assegna un nome alla zona di allarme.

Passo 4 Abilitare **Collegamento al sistema di controllo antincendio** e selezionare un tipo per il dispositivo di ingresso allarme.

- Normalmente chiuso: l'ingresso di allarme si trova in uno stato di circuito normalmente chiuso (NC) quando l'allarme non è scattato. L'apertura di un circuito normalmente chiuso fa scattare l'allarme.
- Normalmente aperto: il dispositivo di ingresso allarme si trova in uno stato di circuito normalmente aperto (NA) quando l'allarme non è scattato. La chiusura del circuito fa scattare l'allarme.

Passo 5 Se si desidera collegare il controllo degli accessi quando viene attivato l'allarme antincendio, abilitare **Collegamento per il controllo degli accessi**.



Questa funzione ha effetto solo dopo **Collegamento Controllo antincendio** è abilitato.

Passo 6

Selezionare una modalità di collegamento.

- Esecuzione impeccabile: quando il segnale di allarme antincendio scompare, la porta mantiene lo stato attuale. Se lo si desidera, è possibile ripristinare manualmente lo stato precedente della porta.
- Esecuzione debole: quando il segnale di allarme antincendio scompare, la porta torna automaticamente al suo stato precedente.

Passo 7

Seleziona un tipo di canale.

- NO: La porta si apre automaticamente quando scatta l'allarme antincendio.
- NC: La porta si chiude automaticamente quando scatta l'allarme antincendio.

Passo 8

Clic **OK**.

3.6.2.3 Configurazione del collegamento degli eventi di allarme

Procedura

Passo 1 Sul **Menù principale**, selezionare **Controllo degli accessi** > **Allarme** > **Collegamento evento di allarme**

Passo 2 Configurare i collegamenti degli eventi di allarme.

Figura 3-14 Collegamento degli eventi di allarme

Intrusion Alarm Linkage ☒ Please enable Intrusion Alarm.

Buzzer ☒ Enable Duration 15 s (1-1800)

Link Alarm Output ☒ Enable Duration 15 s (1-1800)

Unlock Timeout Alarm Linkage ☒ Please enable Unlock Timeout Alarm.

Buzzer ☒ Enable Duration Custom Time 15 s (1-1800)

Link Alarm Output ☒ Enable Duration Custom Time 15 s (1-1800)

Max Use Alarm Link ☒

Buzzer ☒ Enable Duration 15 s (1-1800)

Link Alarm Output ☒ Enable Duration 15 s (1-1800)

Tamper Alarm Linkage ☒

Buzzer ☒ Enable Duration 3 s (1-1800)

Link Alarm Output ☐ Enable Duration 15 s (1-1800)

Buttons: Apply Refresh Default

Tabella 3-7 Collegamento degli eventi di allarme

Parametro	Descrizione
Collegamento del sistema di allarme antintrusione	Se la porta viene aperta in modo anomalo, si attiverà un allarme antintrusione. ● Buzzer: Il buzzer si attiva quando viene rilevato un allarme antintrusione. È possibile configurare la durata dell'allarme. ● Uscita allarme collegamento: il dispositivo di allarme esterno genera allarmi quando viene attivato l'allarme antintrusione. È possibile configurare la durata dell'allarme.
Sblocca allarme timeout Collegamento	Se la porta rimane sbloccata per un periodo superiore al tempo di timeout impostato, si attiverà l'allarme di timeout, che durerà per la durata definita. ● Buzzer: Il buzzer suona quando viene attivato l'allarme di timeout di sblocco. La durata supporta Orario personalizzato E Fino a quando la porta non si chiude. ◇ Fino alla chiusura della porta: il suono dell'allarme si interrompe dopo la chiusura della porta. ◇ Tempo personalizzato: è possibile configurare la durata. ● Uscita allarme locale: il dispositivo di allarme esterno genera allarmi quando viene attivato l'allarme di timeout di sblocco. La durata supporta Orario personalizzato E Fino a quando la porta non si chiude. ◇ Fino alla chiusura della porta: l'allarme si disattiva dopo la chiusura della porta. ◇ Tempo personalizzato: è possibile configurare la durata.
Collegamento allarme utilizzo massimo	Se la password o la carta errata vengono utilizzate 5 volte di seguito entro 60 secondi, si attiverà l'allarme per utilizzo eccessivo di carta non valida, che durerà per un periodo di tempo predefinito. ● Buzzer: Il buzzer si attiva quando viene rilevato un consumo eccessivo. È possibile configurare la durata dell'allarme. ● Uscita allarme locale: il dispositivo di allarme esterno genera allarmi quando si attiva l'allarme di timeout di sblocco. È possibile configurare la durata dell'allarme.
Collegamento dell'allarme antimanomissione	L'allarme di manomissione si attiva quando qualcuno tenta di danneggiare fisicamente il dispositivo. ● Buzzer: Il buzzer si attiva quando scatta l'allarme antimanomissione. È possibile configurare la durata dell'allarme. ● Uscita allarme locale: il dispositivo di allarme esterno genera allarmi quando viene attivato l'allarme di manomissione. È possibile configurare la durata dell'allarme.

Passo 3Clicca **Fare domanda a.****3.6.3 Impostazioni della scheda**

3.6.3.1 Configurazione delle impostazioni della scheda



Questa funzione è disponibile solo su alcuni modelli.

Procedura

- Passo 1

Accedi alla pagina web.
- Passo 2

Selezionare**Controllo degli accessi>Impostazioni della scheda>Impostazioni della**
- Passo 3

schedaConfigura i parametri della scheda.

Figura 3-15 Parametri della scheda

Card Settings

M1 Card

M1 Card Encryption & Verification

Block NFC Cards

DESFire Card

DESFire Card Decryption

Apply

Refresh

Default

Card No. System

After the number system is changed, the card numbers will become invalid.

Card No. System

Hexadecimal

Decimal

Apply

Refresh

Default

DESFire Card Write

Acquisition De...

Device

Please place the card on the swiping area and enable DESFire card and DESFire Card Decryption.

Card Number

Write

Tabella 3-8 Descrizione dei parametri della scheda

Articolo	Parametro	Descrizione
Impostazioni della scheda	Scheda M1	La scheda M1 può essere letta quando questa funzione è abilitata. Questa funzione è disponibile solo su alcuni modelli.
	Crittografia e verifica della carta M1	Solo la scheda IC crittografata può essere letta quando questa funzione è abilitata. AssicurarsiScheda M1è abilitato.

29

Articolo	Parametro	Descrizione
	Schede NFC a blocchi	Impedisci lo sblocco tramite scheda NFC duplicata dopo l'attivazione di questa funzione.  ● Questa funzione è disponibile solo sui modelli che supportano le schede IC. ● Assicurarsi Scheda M1 è abilitato. ● La funzione NFC è disponibile solo su alcuni modelli di telefono.
	Carta Desfire	Il dispositivo è in grado di leggere il numero della carta Desfire quando questa funzione è abilitata.  ● Questa funzione è disponibile solo sui modelli che supportano le schede IC. ● Supporta solo il formato esadecimale.
	Decrittazione della carta Desfire	Le informazioni contenute nella scheda Desfire possono essere lette quando Abilita la scheda Desfire e Decrittazione della carta Desfire vengono abilitati contemporaneamente.  ● Questa funzione è disponibile solo sui modelli che supportano le schede IC. ● Assicurati che la scheda Desfire sia abilitata.
Sistema n. scheda	Sistema n. scheda	Quando si collega un lettore di carte Wiegand, selezionare il formato decimale o esadecimale per il numero della carta. Il sistema di numerazione delle carte è lo stesso sia per l'inserimento che per l'output del numero.
Scrittura su scheda DESFire	Dispositivo di acquisizione	Seleziona il dispositivo, posiziona la carta sul lettore, inserisci il numero della carta e poi fai clic Scrivere scrivere il numero della carta sulla carta.  ● Funzione della scheda Desfire e scheda Desfire ● La funzione di decrittazione deve essere abilitata. ● Supporta solo il formato esadecimale. ● Supporta fino a 8 caratteri.
	Numero di carta	

Passo 4 ClicFare domanda a.

3.6.3.2 Configurazione dei parametri delle regole della scheda di accesso

La piattaforma supporta di default 5 tipi di formati Wiegand. È inoltre possibile aggiungere formati Wiegand personalizzati.

Procedura

Passo 1 Accedi alla pagina web.

Passo 2 Selezionare **Controllo degli accessi** > **Impostazioni della scheda** > **Impostazione delle regole per le carte**

Passo 3 **di accesso** Fare clic **Aggiungere** e quindi configurare nuovi formati Wiegand.

Figura 3-16 Aggiungi nuovi formati Wiegand

The 'Add' dialog box is used to configure Wiegand formats. It includes the following sections:

- Wiegand Format:** A text input field containing 'Wiegand88'.
- Total Bits:** A text input field containing '88' with a range '(1-128)'.
- Facility Code:** A button labeled 'Add'.
- Card Number:** A table with columns: No., Start Bit, End Bit, Total Bits, and Operation. It contains one row for 'FC' with Start Bit '2', End Bit '33', and Total Bits '32'.
- Parity Code:** A button labeled 'Add'.
- Parity Code Table:** A table with columns: Parity Code, Type, Start Bit, End Bit, Total Bits, and Operation. It contains two rows: one for '1' with Type 'Odd', Start Bit '2', End Bit '33', and Total Bits '32'; and another for '88' with Type 'Even', Start Bit '34', End Bit '87', and Total Bits '54'.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Tabella 3-9 Descrizione del formato Wiegand

Parametro	Descrizione
Formato Wiegand	Il nome del formato Wiegand.
Bit totali	Inserisci il numero totale di bit.
Codice struttura	Clic Aggiungere e quindi inserire il bit di inizio e il bit di fine per il codice della struttura.
Numero di carta	Clic Aggiungere e quindi inserire il bit iniziale e il bit finale del numero della carta.
Codice di parità	1. Fare clic Aggiungere. 2. Inserire il bit di inizio parità pari e il bit di fine parità pari. 3. Inserire il bit di inizio parità dispari e il bit di fine parità dispari.

Passo 4 Clic **OK**.

Operazioni correlate

- Puoi anche cliccare **Aggiungi protocollo** per importare un file Wiegand nella piattaforma.
- Codice struttura: se la funzione è abilitata e hai impostato **Sistema n. scheda** in formato decimale su **Gestione del personale** Nella pagina, il codice della struttura e il numero della carta vengono convertiti separatamente in formato decimale e poi combinati.
- HID26: Se la funzione è attivata:
 - ◇ È supportato solo il Wiegand 26.
 - ◇ La piattaforma supporta solo la visualizzazione delle carte in formato decimale.

- ◇ Il numero della carta deve avere 5 caratteri e il codice della struttura al massimo 3 caratteri. Quando si inserisce manualmente il numero della carta, il sistema aggiunge automaticamente uno zero iniziale per raggiungere la lunghezza desiderata. Ad esempio, se il numero della carta inserito è inferiore a 5 caratteri, come 56, viene aggiunto uno zero iniziale per fissare la lunghezza del numero a 5 caratteri, come 00056, e un altro zero viene aggiunto per fungere da codice della struttura. Pertanto, il numero finale della carta sarà 000056.

3.6.3.3 Configurazione della conversione personalizzata

Quando si leggono carte di terze parti utilizzando il lettore integrato del dispositivo, il lettore di carte RS-485 esterno o il lettore di carte Wiegand esterno, se il numero di carta effettivo non corrisponde a nessun numero di carta presente nel sistema, è possibile configurare una conversione personalizzata per il numero di carta in modo da garantire che il numero di carta convertito corrisponda a quello presente nel sistema.

Procedura

Passo 1 Accedi alla pagina web.

Passo 2 Selezionare **Controllo degli accessi** > **Impostazioni della scheda** > **Conversione**

Passo 3 **personalizzata** Attiva la funzione di conversione e seleziona la modalità di corrispondenza.

- Corrispondenza automatica: utilizza la regola di conversione integrata del dispositivo per convertire il numero della carta.

1. Selezionare il tipo di input.

- ◇ Inserimento nel dispositivo: strisciare la carta sul dispositivo per leggerla.
- ◇ Ingresso RS-485: strisciare la scheda sul lettore di schede RS-485 collegato per leggerla.
- ◇ Ingresso Wiegand: strisciare la carta sul lettore di carte Wiegand collegato per leggerla.

2. Leggere il numero della carta tramite il dispositivo oppure inserire il numero della carta prima della conversione, quindi inserire il numero della carta dopo la conversione.

3. Fare clic **Abbinamento automatico**.

- ◇ Se i numeri delle carte corrispondono correttamente, puoi fare clic **Esportare** Esportare la regola e importarla su un altro dispositivo per cambiare rapidamente le regole della partita.
- ◇ Se i numeri delle carte non corrispondono, significa che non esiste una regola di corrispondenza nel sistema. È necessario personalizzare lo script della regola di corrispondenza e selezionare **Regola di conversione per l'importazione** per importare la regola nel dispositivo.
- ◇ Se devi modificare la regola di corrispondenza, fai clic **Modifica la regola di corrispondenza**.

Figura 3-17 Corrispondenza automatica (corrispondenza riuscita)

Enable ☒

Matching Mode ☒ Auto Match ☐ Import Conversion Rule

Status **Applied**

* Input Type ☒ Device Input ☒ RS-485 Input ☒ Wiegand Input

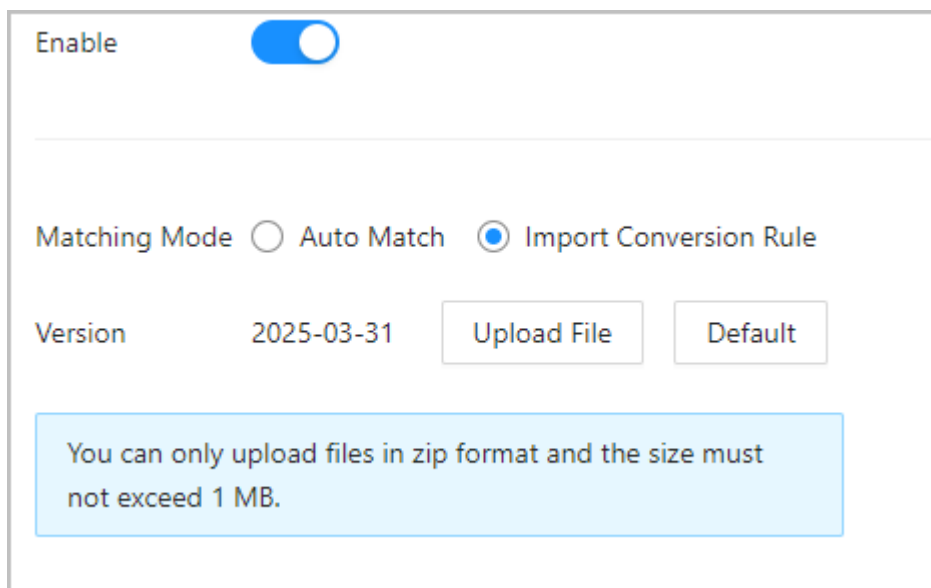
No.	Card No. Before Conversion (Device Input)	Card No. Before Conversion (RS-485 Input)	Card No. Before Conversion (Wiegand Input)	Card No. After Conversion
1	1A283C4D	1A283C4D	1A283C4D	403C281A
2				
3				

☒ **Successfully Matched**
This rule will automatically apply to this device.

- Importa la regola di conversione: Importa altre regole per convertire il numero della carta.

Clic **Carica file**, seleziona il file delle regole e poi fai clic **Aprire**.

Figura 3-18 Regola di conversione per l'importazione



3.6.4 Configurazione dei periodi

Configura piani generali e piani per le festività, dopodiché potrai definire quando un utente ha le autorizzazioni per sbloccare le porte.

3.6.4.1 Configurazione del piano generale

È possibile configurare fino a 128 periodi (dal n. 0 al n. 127) di piani generali. In ogni periodo, è necessario configurare gli orari di accesso alla porta per un'intera settimana. Le persone potranno sbloccare la porta solo durante l'orario programmato.

Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Selezionare **Controllo degli accessi** > **Configurazione del periodo** > **Piano generale** Fare clic
- Passo 3 Aggiungere.
1. Configurare il numero del piano e il nome del piano.
 2. Trascina il cursore temporale per configurare l'orario per ogni giorno.
 3. (Facoltativo) Fare clic **Copia** per copiare la configurazione per i giorni rimanenti.

Figura 3-19 Configurare il piano generale

Add [X]

No.

General Plan Name

Time Plan

Time - [OK] [Delete]

	0	1	2	3	4	5	6	7	8	9	10	11	
Sun													Copy
Mon													Copy
Tue													Copy
Wed													Copy
Thu													Copy
Fri													Copy
Sat													Copy

[OK] [Cancel]

Passo 4 **ClicOK.**

3.6.4.2 Configurazione del piano vacanze

È possibile configurare fino a 128 gruppi di festività (dal n. 0 al n. 127) e, per ciascun gruppo, è possibile aggiungere fino a 16 festività. Successivamente, è possibile assegnare i gruppi di festività configurati al piano festività. Gli utenti potranno sbloccare la porta solo durante il periodo definito dal piano festività.

Procedura

Passo 1 Accedi alla pagina web.

Passo 2 Selezionare **Controllo degli accessi** > **Configurazione del periodo** > **Piano**

Passo 3 **vacanze** Fare clic **Gestione delle festività**, e poi fai clic **Aggiungere**.

1. Seleziona un numero per il gruppo vacanze, quindi inserisci un nome per il gruppo.

Figura 3-20 Aggiungi un gruppo vacanze

Add

No.

Holiday Group Name

Holiday Group Config

No.	Holiday Name	Start Time	End Time	Operation
1	National Day	2023-10-01	2023-10-07	

2. Fare clic **Aggiungere**, aggiungi una festività a un gruppo di festività e poi fai clic **OK**.

Figura 3-21 Aggiungere una festività a un gruppo di festività

Edit

Holiday Name

* Period →

Passo 4 **Clic OK.**

Passo 5 Clic **Gestione della pianificazione**, e poi fai clic **Aggiungere**.

1. Seleziona un numero per il piano vacanze e poi inserisci un nome per esso.
2. Seleziona un gruppo di festività, quindi trascina il cursore per configurare l'orario per ogni giorno.

Consente di aggiungere fino a 4 fasce orarie in un giorno.

Figura 3-22 Aggiungi il piano vacanze

[illegible]

Passo 6 **ClicOK.**

3.6.5 Configurazione delle funzioni della porta

Alcune porte possono svolgere funzioni diverse; è possibile configurarle come porte differenti in base alle esigenze specifiche.

Informazioni di base



- Questa funzione è disponibile solo su alcuni modelli.
- Le porte possono variare a seconda del modello del prodotto.

Procedura

Passo 1 Nella pagina web, selezionare **Controllo degli accessi** > **Configurazione**

Passo 2 **porta**Selezionare il tipo di porta.

È **Campanello** per impostazione predefinita. Fare clic

Passo 3 Fare domanda a.

Figura 3-23 Configurare le porte

Function Port1 ☐ Alarm-out Port ☒ Doorbell

[Apply](#) [Refresh](#) [Default](#)

3.6.6 Configurazione dello sblocco tramite password

Quando il **Autenticazione tramite codice PIN** Se la funzione è abilitata, le persone possono sbloccare la porta semplicemente inserendo la password.

Informazioni di base



- Se l'autenticazione tramite codice PIN non è abilitata, è possibile sbloccare la porta inserendo la password di sblocco nel formato di **ID utente#password#**. Ad esempio, se l'ID utente è 123 e la password che hai impostato è 12345, allora devi inserire **123#12345#** per sbloccare la porta.
- Se l'autenticazione tramite codice PIN è abilitata, è possibile sbloccare la porta inserendo la password di sblocco nel formato di **password#**. Ad esempio, se l'ID utente è 123 e la password che hai impostato è 12345, allora devi inserire **12345#** per sbloccare la porta.

Procedura

Passo 1 Nella pagina iniziale, selezionare **Controllo degli accessi** > **Configurazione del metodo di sblocco**.

Passo 2 Accendere **Autenticazione tramite codice PIN**, e poi fai clic **Fare domanda a**.



L'attivazione dell'autenticazione tramite codice PIN comporta alcuni rischi per la sicurezza. Quando questa opzione è attiva, i tipi di utente e i ruoli diventano inefficaci e si verificano le seguenti situazioni.

- I titolari della prima carta e gli utenti nei gruppi di sblocco multiutente devono verificare la propria identità tramite i metodi di sblocco definiti, ad eccezione della password. Se la verifica avviene tramite password, la funzione di sblocco della prima carta o di sblocco multiutente risulterà inefficace.
- Gli utenti devono verificare le proprie credenziali tramite metodi di sblocco predefiniti, ad eccezione della password. Se ottengono l'accesso tramite password, la funzione anti-passback risulterà inefficace.
- Gli utenti con privilegi di pattugliamento e gli utenti bloccati possono semplicemente inserire la propria password per sbloccare la porta.
- Anche gli account bloccati o scaduti possono sbloccare le porte semplicemente inserendo la password.
- Quando il metodo di sblocco tramite password è disattivato, nessun tipo di utente può sbloccare la porta utilizzando la propria password.

3.6.7 Configurazione dello sblocco in prima persona

Chiunque può accedere alle porte solo dopo che le persone da te specificate siano passate. Se specifichi più persone, anche le altre potranno accedere alle porte solo dopo che una qualsiasi delle persone specificate sarà passata.

Prerequisiti

Le persone possono essere impostate come prime persone solo se dispongono delle autorizzazioni per accedere alle porte.

Procedura

Passo 1 Nella pagina iniziale, selezionare **Controllo degli accessi** > **Sblocco in prima**

Passo 2 **persona** Selezionare il canale della porta e quindi attivare la funzione.

Figura 3-24 Sblocco in prima persona

Passo 3 Configura i parametri.

Tabella 3-10 Descrizione dei parametri

Parametro	Descrizione
Modelli temporali	Seleziona quando questa regola è in vigore.
Stato della porta dopo lo sblocco con la prima tessera	● Normale: Le altre persone devono verificare la propria identità per poter passare. ● Sempre aperto: Chiunque può passare senza che venga verificata la propria identità.
Elenco del personale	Clic+ per selezionare una o più persone, alle quali verrà concesso il permesso di accedere alle porte.

Passo 4 Clic+Fare domanda a.

3.6.8 Configurazione dell'anti-passback

Gli utenti devono verificare la propria identità sia in entrata che in uscita; in caso contrario, si attiverà un allarme anti-passback. Questo sistema impedisce al titolare della tessera di cederla a un'altra persona per consentirle l'accesso. Quando l'anti-passback è attivo, il titolare della tessera deve lasciare l'area protetta prima che il sistema possa autorizzare un nuovo accesso.

- Se una persona entra dopo essere stata autorizzata ed esce senza autorizzazione, si attiverà un allarme al successivo tentativo di accesso e l'accesso verrà negato.
- Se una persona non autorizzata esce dopo essere stata autorizzata, si attiverà un allarme al suo successivo tentativo di accesso e l'accesso verrà contemporaneamente negato.



- Quando si configura la funzione anti-passback per i controller secondari tramite il controller principale e si prevede di ripristinare le impostazioni di fabbrica del controller principale, si consiglia di ripristinare contemporaneamente anche le impostazioni di fabbrica del controller secondario.
- Se la regola anti-passback viene utilizzata quando la rete non è stabile, la porta potrebbe aprirsi dopo la verifica dell'identità, ma potrebbe attivarsi un allarme di timeout sul lettore di schede. Assicurati che la tua rete sia stabile.

Procedura

- Passo 1** Nella pagina iniziale, selezionare **Controllo degli accessi > Configurazione del gruppo anti-passback**
- Passo 2** **passback** Attiva questa funzione e poi configura un orario di ripristino.
Specificare l'orario in cui verrà ripristinato lo stato anti-passback di tutto il personale.
- Passo 3** Selezionare il piano generale e il piano festivo.
La funzione anti-passback è efficace per la durata definita.
- Passo 4** Nel gruppo di voci, fare clic **Aggiungere** e quindi selezionare il lettore di schede. Nel
- Passo 5** gruppo di uscita, fare clic **Aggiungere** e quindi selezionare il lettore di schede.

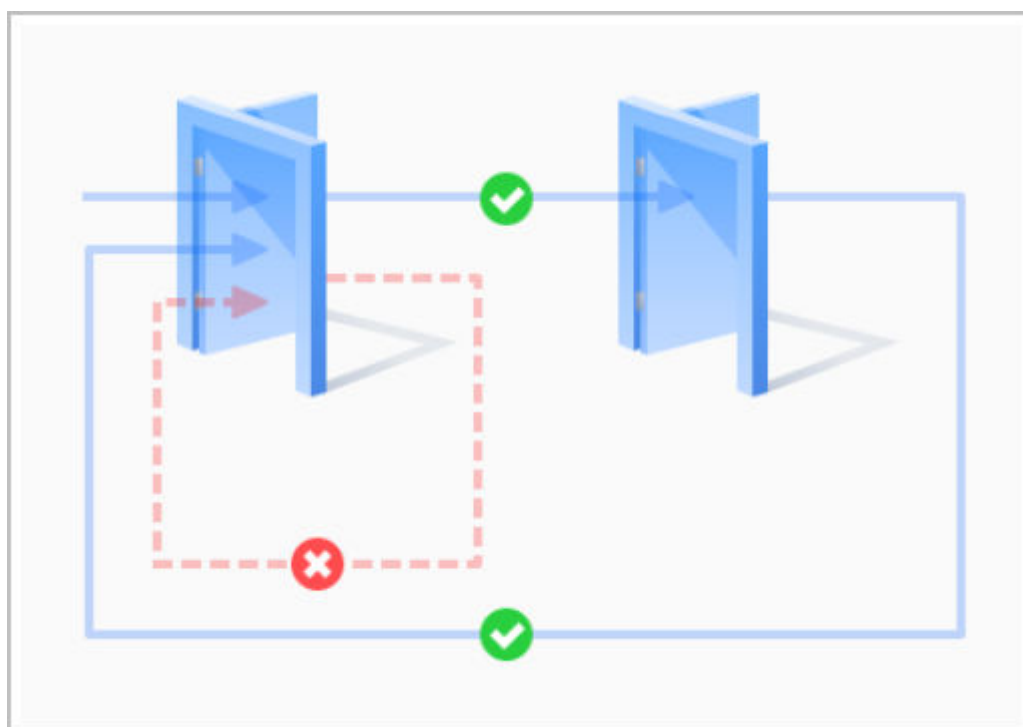
Figura 3-25 Anti-passback

Passo 6 Clic **Fare domanda a**.

Risultati

Il numero del gruppo indica la sequenza di strisciamento delle carte. La carta deve essere utilizzata seguendo la sequenza specificata per ciascun gruppo. Ad esempio, è necessario strisciare la carta su un lettore del gruppo di ingresso e poi su un lettore del gruppo di uscita. Seguendo la sequenza stabilita, il sistema funziona correttamente.

Figura 3-26 Funzione anti-passback



3.7 Impostazioni di comunicazione

3.7.1 Impostazioni di rete

3.7.1.1 Configurazione di TCP/IP

È necessario configurare l'indirizzo IP del dispositivo per garantire che possa comunicare con altri dispositivi.

Procedura

- Passo 1 Selezionare **Impostazioni di comunicazione > Impostazioni di rete > TCP/**
- Passo 2 **IP** Configura i parametri.

Figura 3-27 TCP/IP

NIC

NIC 1

Mode

DHCP

Static

MAC Address

IP Version

IPv4

IP Address

Subnet Mask

Default Gateway

Preferred DNS

Alternate DNS

MTU

1500

Apply

Refresh

Default

Tabella 3-11 Descrizione di TCP/IP

Parametro	Descrizione
Modalità	● Statico: Inserire manualmente l'indirizzo IP, la subnet mask e il gateway. ● DHCP: Acronimo di Dynamic Host Configuration Protocol. Quando il DHCP è attivo, al dispositivo vengono assegnati automaticamente indirizzo IP, subnet mask e gateway.
Indirizzo MAC	Indirizzo MAC del dispositivo.
Versione IP	IPv4 o IPv6.

Parametro	Descrizione
Indirizzo IP	Se imposti la modalità su Statico Configurare l'indirizzo IP, la subnet mask e il gateway.
Maschera di sottorete	
Gateway predefinito	
	 ● L'indirizzo IPv6 è rappresentato in formato esadecimale. ● La versione IPv6 non richiede l'impostazione delle maschere di sottorete. ● L'indirizzo IP e il gateway predefinito devono trovarsi nello stesso segmento di rete.
DNS preferito	Imposta l'indirizzo IP del server DNS preferito.
DNS alternativo	Imposta l'indirizzo IP del server DNS alternativo.
MTU	L'MTU (Maximum Transmission Unit) si riferisce alla dimensione massima dei dati che possono essere trasmessi in un singolo pacchetto di rete nelle reti di computer. Un valore MTU più elevato può migliorare l'efficienza della trasmissione di rete riducendo il numero di pacchetti e il relativo overhead di rete. Se un dispositivo lungo il percorso di rete non è in grado di gestire pacchetti di una determinata dimensione, ciò può causare la frammentazione dei pacchetti o errori di trasmissione. Nelle reti Ethernet, il valore MTU comune è di 1500 byte. Tuttavia, in alcuni casi, come ad esempio con PPPoE o VPN, potrebbero essere necessari valori MTU inferiori per soddisfare i requisiti di specifici protocolli o servizi di rete. Di seguito sono riportati i valori MTU consigliati a titolo di riferimento: ● 1500: Valore massimo per i pacchetti Ethernet, nonché valore predefinito. Si tratta di un'impostazione tipica per le connessioni di rete senza PPPoE e VPN, utilizzata in alcuni router, schede di rete e switch. ● 1492: Valore ottimale per PPPoE ● 1468: Valore ottimale per DHCP. ● 1450: Valore ottimale per VPN.

Passo 3 **ClicOK.**

3.7.1.2 Configurazione del Wi-Fi



- La funzione Wi-Fi è disponibile su alcuni modelli.
- Il Wi-Fi e il punto di accesso Wi-Fi non possono essere attivati contemporaneamente.

Procedura

Passo 1 Selezionare **Impostazioni di comunicazione>Impostazioni di rete>**

Passo 2 **Wifi** Attiva il Wi-Fi.

Vengono visualizzate tutte le reti Wi-Fi disponibili.

Figura 3-28 Wi-Fi

Wi-Fi ☐

Mode ☒ DHCP ☐ Static

MAC Address f8 : ce : 07 : 6b : b2 : cc

IP Address 192 . 168 . 0 . 108

Subnet Mask 255 . 255 . 0 . 0

Default Gateway 192 . 168 . 0 . 1

Preferred DNS 8 . 8 . 8 . 8

Alternate DNS 8 . 8 . 4 . 4

Name	Signal Strength	Status	Connect
No Data			



- Il Wi-Fi e il Wi-Fi AP non possono essere attivati contemporaneamente.
- La funzione Wi-Fi è disponibile solo su alcuni modelli.

Passo 3 Clic+e poi inserisci la password del Wi-Fi. Il Wi-Fi è connesso.

Operazioni correlate

- DHCP: Abilita questa funzione e fai clic**Fare domanda a**, al dispositivo verrà assegnato automaticamente un indirizzo Wi-Fi.
- Statico: abilita questa funzione, inserisci manualmente un indirizzo Wi-Fi e poi fai clic**Fare domanda a**Il dispositivo si conatterà al Wi-Fi.

3.7.1.3 Configurazione dell'AP Wi-Fi



- La funzione Wi-Fi è disponibile su alcuni modelli.
- Il Wi-Fi e il punto di accesso Wi-Fi non possono essere attivati contemporaneamente.

Procedura

Passo 1 Selezionare**Impostazioni di comunicazione>Impostazioni di rete>Punto di accesso Wi-Fi**.

Passo 2 Abilita la funzione e poi fai clic**Fare domanda a**.

Figura 3-29 Punto di accesso Wi-Fi

The screenshot displays the configuration page for a Wi-Fi access point. It includes the following elements:

- Enable:** A toggle switch currently in the 'off' position.
- SSID:** A text input field containing a default or masked name.
- Security:** A dropdown menu currently set to 'None'.
- IP Address:** A text input field showing a default IP address.
- QR Code:** A large QR code used for quick configuration via a mobile device.
- Buttons:** Three buttons at the bottom: 'Apply' (blue), 'Refresh' (white), and 'Default' (white).

Risultati

Una volta attivata, è possibile connettersi al Wi-Fi del dispositivo tramite il telefono e accedere alla pagina web del dispositivo dal telefono.

3.7.1.4 Configurazione della porta

È possibile limitare l'accesso al dispositivo contemporaneamente tramite pagina web, client desktop e client mobile.

Procedura

- Passo 1 Selezionare **Impostazioni di comunicazione > Impostazioni di rete > Porta**
- Passo 2 Configura le porte.

Figura 3-30 Configurare le porte

Max Connection

50

(1-50)

TCP Port

37777

(1025-65535)

HTTP Port

80

HTTPS Port

443

Apply

Refresh

Default



Dopo aver configurato i parametri, è necessario riavviare il dispositivo affinché le modifiche abbiano effetto.

Tabella 3-12 Descrizione delle porte

Parametro	Descrizione
Connessione massima	È possibile impostare il numero massimo di client (come pagine web, client desktop e client mobile) che possono accedere al dispositivo contemporaneamente.
Porta TCP	Il valore predefinito è 37777.
Porta HTTP	Il valore predefinito è 80. Se hai modificato il numero di porta, aggiungilo dopo l'indirizzo IP quando accedi alla pagina web.
Porta HTTPS	Il valore predefinito è 443.

Passo 3 ClicFare domanda a.

3.7.1.5 Configurazione del servizio di base

Quando si desidera connettere il dispositivo a una piattaforma di terze parti, è necessario attivare le funzioni CGI e ONVIF.

Procedura

- Passo 1

Selezionare**Impostazioni di comunicazione>Impostazioni di rete>Servizi di base**
- Passo 2

Configura il servizio di base.

Figura 3-31 Servizio di base

SSH☒

Multicast/Broadcast Search☒

CGI☒

ONVIF☒

Emergency Maintenance☐

1

For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.

Private Protocol Authentication Mode

Security Mode (Recommended) ▾

Private Protocol

☒

*Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.

TLSv1.1

☐

LLDP

☐

Apply

Refresh

Default

Tabella 3-13 Descrizione dei parametri di servizio di base

Parametro	Descrizione
SSH	SSH, o Secure Shell Protocol, è un protocollo di amministrazione remota che consente agli utenti di accedere, controllare e modificare i propri server remoti tramite Internet.
Ricerca multi-trasmissione/trasmissione	Ricerca dispositivi tramite protocollo multicast o broadcast.
CGI	La Common Gateway Interface (CGI) è un'interfaccia tra server web che consente lo scambio standardizzato di dati tra applicazioni esterne e server.
ONVIF	ONVIF è l'acronimo di Open Network Video Interface Forum. Il suo obiettivo è fornire uno standard per l'interfaccia tra diversi dispositivi di sicurezza basati su IP. Queste specifiche ONVIF standardizzate sono come un linguaggio comune che tutti i dispositivi possono utilizzare per comunicare.
Manutenzione di emergenza	È attivato di default.
Modalità di autenticazione tramite protocollo privato	Imposta la modalità di autenticazione, inclusa la modalità sicura e la modalità di compatibilità. Si consiglia di scegliereModalità di sicurezza. ● Modalità di sicurezza (consigliata): non supporta l'accesso al dispositivo tramite metodi di autenticazione Digest, DES e in chiaro, migliorando la sicurezza del dispositivo. ● Modalità compatibile: supporta l'accesso al dispositivo tramite metodi di autenticazione Digest, DES e testo in chiaro, con sicurezza ridotta.
Protocollo privato	La piattaforma aggiunge dispositivi tramite protocollo privato.

Parametro	Descrizione
TLSv1.1	TLSv1.1 si riferisce alla versione 1.1 del Transport Layer Security. TLS è un protocollo crittografico progettato per fornire comunicazioni sicure e autenticate su una rete di computer.  L'attivazione di TLSv1.1 potrebbe comportare rischi per la sicurezza. Si prega di tenerne conto.
LLDP	LLDP è l'acronimo di Link Layer Discovery Protocol, un protocollo di livello di collegamento dati. Consente ai dispositivi di rete, come switch, router o server, di scambiarsi informazioni sulla propria identità e sulle proprie capacità. Il protocollo LLDP aiuta gli amministratori di rete a comprendere meglio la topologia di rete e fornisce un metodo standardizzato per automatizzare il rilevamento e la mappatura delle connessioni tra i dispositivi di rete. Ciò semplifica la configurazione della rete, la risoluzione dei problemi e l'ottimizzazione delle prestazioni.

Passo 3

ClicFare domanda a.

3.7.1.6 Configurazione del servizio cloud

Il servizio cloud offre un servizio di penetrazione NAT. Gli utenti possono gestire più dispositivi tramite DMSS. Non è necessario richiedere un nome di dominio dinamico, configurare il port mapping o implementare un server.

Procedura

Passo 1 Nella pagina iniziale, selezionare **Impostazioni di comunicazione > Impostazioni di rete > Servizio cloud**.

Passo 2 Attiva la funzione di servizio cloud.

Il servizio cloud si attiva se il P2P e il PaaS sono online.

Figura 3-32 Servizio cloud

Enable
☒

After the function is enabled and the device connects to the network, we will collect device information such as the IP address, MAC address, device name and serial number. The collected information will only be used to remotely access the device. If you do not want to enable this function, please clear the selection from the check box.

P2P Status
● Offline

PaaS Status
● Offline

SN
8[REDACTED]759



Apply

Refresh

Passo 3 Cliccare domanda a.

Passo 4 Scansiona il codice QR con DMSS per aggiungere il dispositivo.

3.7.1.7 Configurazione della registrazione automatica dell'SDK

La registrazione automatica consente di aggiungere i dispositivi alla piattaforma di gestione senza dover inserire manualmente informazioni quali indirizzo IP e porta.

Informazioni di base



La registrazione automatica è supportata solo dall'SDK.

Procedura

- Passo 1 Nella pagina iniziale, selezionare **Impostazioni di rete** > **Registrazione automatica**
- Passo 2 **dell'SDK** Attiva la funzione di registrazione automatica e configura i parametri.

Figura 3-33 Registrazione automatica

Enable

Status

Offline

Server Address

172.52.2.7

Port

7000

(1-65535)

Registration ID

none

Apply

Refresh

Default

Tabella 3-14 Descrizione della registrazione automatica

Parametro	Descrizione
Stato	Visualizza lo stato della connessione per la registrazione automatica.
Indirizzo del server	L'indirizzo IP o il nome di dominio del server.
Porta	La porta del server utilizzata per la registrazione automatica.
ID di registrazione	L'ID di registrazione (definito dall'utente) del dispositivo. Aggiungere il dispositivo alla gestione inserendo l'ID di registrazione sulla piattaforma.

Passo 3 ClicFare domanda a.

3.7.1.8 Configurazione della registrazione automatica CGI

Connettiti a una piattaforma di terze parti tramite protocollo CGI.

Informazioni di base



Supporta solo IPv4.

Procedura

Passo 1 Nella pagina iniziale, selezionare**Impostazioni di comunicazione>Impostazioni di rete>Registrazione automatica CGI**.

Passo 2 Abilita questa funzione e poi fai clic  per configurare i parametri.

Tabella 3-15 Descrizione della registrazione automatica

Parametro	Descrizione
ID dispositivo	Supporta fino a 32 byte, inclusi caratteri cinesi, numeri, lettere e caratteri speciali.
Tipo di indirizzo	Supporta 2 metodi di registrazione.
Indirizzo IP host	● Indirizzo IP dell'host: Inserire l'indirizzo IP della piattaforma di terze parti.
Nome di dominio	● Nome di dominio: Inserire il nome di dominio della piattaforma di terze parti.
HTTPS	Accedi alla piattaforma di terze parti tramite HTTPS. HTTPS protegge la comunicazione su una rete informatica.

Passo 3 **Clic****OK**.

3.7.1.9 Configurazione del caricamento automatico

Invia le informazioni utente e sblocca i record alla piattaforma di gestione.

Procedura

Passo 1 Nella pagina iniziale, selezionare **Impostazioni di comunicazione>Impostazioni di rete>Caricamento automatico**.

Passo 2 (Opzionale) Abilita **Spingere le informazioni della persona**.

Quando le informazioni dell'utente vengono aggiornate o vengono aggiunti nuovi utenti, il dispositivo invierà automaticamente tali informazioni alla piattaforma di gestione.

Passo 3 Abilita la modalità di caricamento HTTP.

Passo 4 Clic **Aggiungere** e quindi configurare i parametri.

Figura 3-34 Caricamento automatico

Tabella 3-16 Descrizione dei parametri

Parametro	Descrizione
Indirizzo IP/Nome di dominio	L'indirizzo IP o il nome di dominio della piattaforma di gestione.
Porta	La porta della piattaforma di gestione.
HTTPS	Accedi alla piattaforma di gestione tramite HTTPS. HTTPS protegge la comunicazione su una rete informatica.
Autenticazione	Per accedere alla piattaforma di gestione, è necessario abilitare l'autenticazione dell'account. Sono richiesti nome utente e password.

Parametro	Descrizione
Tipo di evento	Seleziona il tipo di evento che verrà inviato alla piattaforma di gestione.  ● Prima di utilizzare questa funzione, abilita Spingere le informazioni della persona. ● Le informazioni relative agli utenti possono essere inviate a una sola piattaforma di gestione, mentre i dati di sblocco possono essere inviati a più piattaforme di gestione.

Passo 5

Clic **Fare domanda a**.

3.7.2 Impostazioni modalità

Accedi alla pagina web e seleziona **Impostazioni di comunicazione > Impostazioni modalità**.

Modalità lettore di schede

Selezionare **Modalità COME Lettore di schede**. Il dispositivo funge da lettore di schede collegato esternamente a un controller di controllo accessi. Non esegue l'autenticazione, ma trasmette direttamente le informazioni di controllo accessi (come scheda, password, impronta digitale) al controller, che provvede quindi all'autenticazione e allo sblocco della porta.

Figura 3-35 Modalità lettore di schede

Mode

☒ Card Reader ☐ Access Controller

RS-485 Settings

Baud Rate

9600

▼

Data Bit

8

▼

Stop Bit

1

▼

Parity Code

None

▼

Wiegand Settings

Wiegand Output Type

Wiegand 34

▼

Pulse Width (μs)

200

(20-200)

Pulse Interval (μs)

1000

(200-5000)

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Apply

Refresh

Default

Modalità controller di accesso

ImpostatoModalitàCOMEController di accesso.

Figura 3-36 Modalità del controller di accesso

Mode

☐ Card Reader ☒ Access Controller

RS-485 Settings

External Device

Card Reader

?

Baud Rate

9600

Data Bit

8

Stop Bit

1

Parity Code

None

Wiegand Settings

Wiegand Settings

☒ Wiegand Input ☐ Wiegand Output

Card No. Inversion

☒

Apply

Refresh

Default

Tabella 3-17 Descrizione di RS-485

Ora	Descrizione
Controller di accesso	Selezionare Controller di accesso quando il dispositivo funziona come lettore di schede e invia dati ad altri controller di accesso esterni per controllare l'accesso. Tipo di dati di output: ● Numero di tessera: visualizza i dati in base al numero di tessera quando l'utente striscia la tessera per sbloccare la porta; visualizza i dati in base al primo numero di tessera dell'utente quando vengono utilizzati altri metodi di sblocco. ● ID: Visualizza i dati in base all'ID utente.  ● In caso di autenticazione riuscita, le informazioni pertinenti vengono trasmesse al controller di accesso. In questo caso, il risultato dell'autenticazione visualizzato è quello del controller di accesso. ● In caso di errore di autenticazione, le informazioni pertinenti non vengono trasmesse al controller di accesso e il risultato visualizzato rimane "fallimento".
Lettore di schede	Il dispositivo è collegato esternamente a un lettore di schede e trasmette le informazioni della scheda di controllo accessi a un controller di accesso o a una piattaforma di gestione.
Lettore di schede (OSDP)	Il dispositivo è collegato esternamente a un lettore di schede OSDP e trasmette le informazioni della scheda di controllo accessi a un controller di accesso o a una piattaforma di gestione.
Modulo di sicurezza per porte	Il pulsante di uscita, la serratura e il collegamento antincendio non funzionano dopo l'attivazione del modulo di sicurezza. ● Supporta l'autenticazione tramite riconoscimento facciale, tessera, impronta digitale, password e altri metodi per controllare il modulo di sicurezza della porta ai fini dello sblocco. ● Supporta lo sblocco tramite un lettore di schede RS-485 collegato esternamente o un pulsante di apertura a pressione collegato al modulo di sicurezza per il controllo della porta.  Lo sblocco a distanza della serratura esterna tramite il modulo di sicurezza della porta non è supportato.
Modulo di estensione serratura	Quando il controller di accesso è collegato al modulo di estensione della serratura esterna, se si seleziona Modulo di estensione serratura la serratura locale viene sbloccata dopo aver verificato l'identità sul dispositivo locale, mentre la serratura dell'estensione viene sbloccata dopo aver verificato l'identità sul lettore di schede esterno. Dopo aver selezionato Modulo di estensione serratura, è possibile selezionare il canale 2 su Parametri di controllo degli accessi e Allarme pagina sulla pagina web del Responsabile degli accessi.

Tabella 3-18 Descrizione di Wiegand

Parametro		Descrizione
Impostazioni di Wiegand		● Quando si collega un dispositivo lettore di schede esterno, selezionare Input di Wiegand. ● Quando il dispositivo funziona come lettore di schede e devi collegarlo a un altro controller di accesso, seleziona Configurazione di output di Wiegand.
Wiegand Ingresso	Numero di carta Inversione	Se la sequenza del numero di carta ottenuta tramite l'input Wiegand non corrisponde alla sequenza effettiva del numero di carta quando si interagisce con dispositivi di terze parti, abilitare questa funzione.
Wiegand Produzione	Wiegand Tipo di output	La lunghezza in bit dei numeri di carta o ID che il dispositivo è in grado di riconoscere e riprodurre. ● Wiegand 26: Legge 3 byte o 6 cifre. ● Wiegand 34: Legge 4 byte o 8 cifre. ● Wiegand 66: Legge 8 byte o 16 cifre.
	Larghezza dell'impulso	Configurare la larghezza e l'intervallo dell'impulso per l'uscita Wiegand.
	Intervallo di impulso	
	Dati di output Tipo	Selezionare un formato Wiegand per leggere i numeri di carta o i numeri di identificazione. ● ID utente: visualizza i dati in base all'ID utente. ● Carta: visualizza i dati in base al primo numero di carta dell'utente.
	Wiegand Formato	Quando Tipo di dati di output è impostato come ID È possibile selezionare il formato di output decimale o esadecimale.

3.8 Configurazione del sistema

3.8.1 Gestione utenti

È possibile aggiungere o eliminare utenti, modificare le password degli utenti e inserire un indirizzo email per reimpostare la password in caso di smarrimento.

3.8.1.1 Aggiunta di amministratori

È possibile aggiungere nuovi account amministratore, che potranno quindi accedere alla pagina web del dispositivo.

Procedura

Passo 1 Nella pagina iniziale, selezionare **Sistema > Account > Account** Fare clic

Passo 2 **Aggiungere** e inserire le informazioni dell'utente.



- Il nome utente non può essere uguale a quello di un account già esistente. Il nome utente può contenere fino a 31 caratteri e ammette solo numeri, lettere, trattini bassi, linee intermedie, punti o il simbolo @.
- La password deve essere composta da 8 a 32 caratteri non vuoti e contenere almeno due dei seguenti tipi di caratteri: lettere maiuscole, lettere minuscole, numeri e caratteri speciali (esclusi ' " ; : &).

Imposta una password ad alta sicurezza seguendo le istruzioni relative alla complessità della password.

Figura 3-37 Aggiungi amministratori

The 'Add' dialog box has a title bar with a close button (X). Inside, there are four labeled input fields: 'Username', 'Password', 'Confirm Password', and 'Remarks'. The 'Password' and 'Confirm Password' fields have a blue strength indicator bar below them. At the bottom right, there are two buttons: 'OK' (blue) and 'Cancel' (white with a grey border).

Passo 3 Clic**OK**.



Solo l'account amministratore può cambiare la password e l'account amministratore non può essere eliminato.

3.8.1.2 Reimpostazione della password

Se dimentichi la password, reimpostala tramite l'indirizzo e-mail indicato nel link.

Procedura

Passo 1 Selezionare **Sistema>Account>Account**.

Passo 2 Inserisci l'indirizzo email e imposta la data di scadenza della password. Attiva la

Passo 3 funzione di reimpostazione della password.

Figura 3-38 Reimposta password

The 'Password Reset' settings page has a title bar. Below it, there is an 'Enable' toggle switch which is turned on. A blue highlighted box contains the text: 'If you forgot the password, you can receive security codes through the email address left in advance to reset the password.' Below this, there are two input fields: 'Email Address' with the value '1***@.com' and 'Password Expires in' with a dropdown menu showing 'Never' and a 'Days' label to its right.



Se hai dimenticato la password, puoi ricevere i codici di sicurezza tramite l'indirizzo email collegato per reimpostarla.

Passo 4 ClicFare domanda a.

3.8.1.3 Aggiunta di utenti ONVIF

Informazioni di base

L'Open Network Video Interface Forum (ONVIF) è un forum industriale globale e aperto, istituito per lo sviluppo di uno standard aperto globale per l'interfaccia dei prodotti di sicurezza fisici basati su IP, che consente la compatibilità tra diversi produttori. Gli utenti ONVIF vedono la propria identità verificata tramite il protocollo ONVIF. L'utente ONVIF predefinito è "admin".

Procedura

- Passo 1 Nella pagina iniziale, selezionare**Sistema>Account>Utente ONVIF**Fare clic
- Passo 2 **Aggiungere**e quindi configurare i parametri.

Figura 3-39 Aggiungi utente ONVIF

Add

* Username

* Password

* Confirm Password

* Group

OK

Cancel

Tabella 3-19 Descrizione utente ONVIF

Parametro	Descrizione
Nome utente	Il nome utente non può essere uguale a quello di un account già esistente. Il nome utente può contenere fino a 31 caratteri e ammette solo numeri, lettere, trattini bassi, linee intermedie, punti o il simbolo @.
Password	La password deve essere composta da 8 a 32 caratteri non vuoti e contenere almeno due dei seguenti tipi di caratteri: lettere maiuscole, lettere minuscole, numeri e caratteri speciali (esclusi ' " ; : &).

Parametro	Descrizione
Gruppo	Esistono tre gruppi di autorizzazioni che rappresentano diversi livelli di autorizzazione. ● amministratore: È possibile visualizzare e gestire altri account utente su ONVIF Device Manager. ● Operatore: Non è possibile visualizzare o gestire altri account utente su ONVIF Device Manager. ● Utente: Non è possibile visualizzare o gestire altri account utente e registri di sistema in ONVIF Device Manager.

Passo 3 **ClicOK.**

3.8.2 Visualizzazione degli utenti online

È possibile visualizzare gli utenti online attualmente connessi alla pagina web. Nella pagina iniziale, selezionare **Sistema>Utente online**.

3.8.3 Configurazione dell'ora

Procedura

- Passo 1 Accedi alla pagina web. Seleziona
- Passo 2 **Sistema>Tempo**Configura l'ora della
- Passo 3 piattaforma.

Figura 3-40 Impostazioni dell'ora

Time and Time Zone



Date :

2024-08-05 Monday

Time :

18:50:31

Time

☒ Manually Set

☐ NTP

System Time

2024-08-05 18:50:31



Sync PC

Time Format

YYYY-MM-DD



24-Hour



Time Zone

(UTC+09:30)



DST

Enable

☐

Type

☒ Date

☐ Week

Start Time

Jan



1



00:00



End Time

Jan



2



00:00



Apply

Refresh

Default

Tabella 3-20 Descrizione delle impostazioni dell'ora

Parametro	Descrizione
Tempo	● Impostazione manuale: inserisci manualmente l'ora oppure puoi fare clic Sincronizza PC per sincronizzare l'ora con il computer. ● NTP: Il dispositivo sincronizzerà automaticamente l'ora con il server NTP. ◇ Server:Inserisci il dominio del server NTP. ◇ Porta:Inserisci la porta del server NTP. ◇ Intervallo:Inserisci il suo orario con l'intervallo di sincronizzazione.
Formato orario	Seleziona il formato dell'ora.
Fuso orario	Seleziona il fuso orario.

Parametro	Descrizione
ora legale	1. (Facoltativo) Attivare l'ora legale. 2. Seleziona Data O Settimana dal Tipo. 3. Configurare l'ora di inizio e l'ora di fine dell'ora legale.

Passo 4 Clic **Fare domanda a.**

3.9 Centro di manutenzione

3.9.1 Diagnosi con un clic

Il sistema diagnostica automaticamente le configurazioni e lo stato del dispositivo per migliorarne le prestazioni.

Procedura

Passo 1 Nella pagina iniziale, selezionare **Centro di manutenzione** > **Diagnosi con un clic** Fare clic

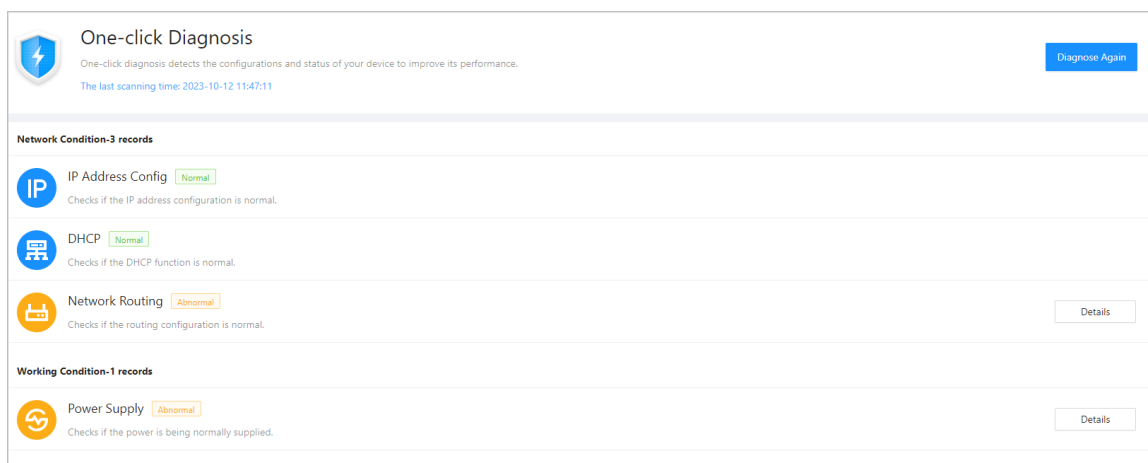
Passo 2 **Diagnosticare.**

Il sistema diagnostica automaticamente le configurazioni e lo stato del dispositivo e visualizza i risultati della diagnosi al termine del processo.

Passo 3 (Facoltativo) Fare clic **Dettagli** per visualizzare i dettagli degli elementi anomali.

Puoi ignorare l'anomalia o ottimizzarla. Puoi anche fare clic **Diagnosi di nuovo** per eseguire nuovamente la diagnosi automatica.

Figura 3-41 Diagnosi con un clic



3.9.2 Informazioni di sistema

3.9.2.1 Visualizzazione delle informazioni sulla versione

Nella pagina web, selezionare **Centro di manutenzione** > **Informazioni di sistema** > **Versione** e puoi visualizzare le informazioni sulla versione del dispositivo.

3.9.2.2 Visualizzazione delle informazioni legali

Nella pagina iniziale, selezionare **Centro di manutenzione** > **Informazioni di sistema** > **Informazioni legali** e puoi visualizzare il contratto di licenza del software, l'informativa sulla privacy e l'avviso sul software open source.

3.9.3 Capacità dati

È possibile visualizzare il numero di utenti e di schede che il dispositivo può memorizzare.

Accedi alla pagina web e seleziona **Centro di manutenzione** > **Capacità dati**.

3.9.4 Visualizzazione dei registri

Visualizza i registri, come i registri di sistema, i registri amministrativi e i registri di sblocco.

3.9.4.1 Registri di sistema

Visualizza e cerca i registri di sistema.

Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Selezionare **Centro di manutenzione** > **Tronco d'albero** > **Tronco d'albero**.
- Passo 3 Seleziona l'intervallo di tempo e il tipo di registro, quindi fai clic **Ricerca**.

Operazioni correlate

- clic **Esportare** per esportare i registri ricercati sul computer locale.
- Clic **Crittografa il backup dei log** e poi inserisci una password. Il file esportato potrà essere aperto solo dopo aver inserito la password.
- Clic  per visualizzare i dettagli di un registro.

3.9.4.2 Sblocca i record

Cerca i record di sblocco ed esportali.

Procedura

- Passo 1 Accedi alla pagina web.
 - Passo 2 Selezionare **Centro di manutenzione** > **Tronco d'albero** > **Sblocca i**
 - Passo 3 **record** Seleziona l'intervallo di tempo e il tipo, quindi fai clic **Ricerca**.
- Puoi cliccare **Esportare** per scaricare il registro.

3.9.4.3 Registri degli allarmi

Visualizza i registri degli allarmi.

Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Selezionare **Centro di manutenzione** > **Tronco d'albero** > **Registri degli**
- Passo 3 **allarmi** Seleziona il tipo e l'intervallo di tempo.
- Passo 4 Inserisci l'ID amministratore e poi fai clic **Ricerca**.

3.9.4.4 Registri di amministrazione

Cerca i log di amministrazione utilizzando l'ID amministratore.

Procedura

- Passo 1** Accedi alla pagina web.
- Passo 2** Selezionare **Centro di manutenzione>Tronco d'albero>Registri**
- Passo 3** **amministrativi** Inserisci l'ID amministratore e poi fai clic **Ricerca**.
- Clic **Esportare** per esportare i log di amministrazione.

3.9.5 Gestione della manutenzione

Quando più dispositivi necessitano delle stesse configurazioni, è possibile configurare i parametri per ciascuno di essi importando o esportando i file di configurazione.

3.9.5.1 Esportazione e importazione di file di configurazione

È possibile importare ed esportare il file di configurazione del dispositivo. Quando si desidera applicare le stesse configurazioni a più dispositivi, è possibile importare il file di configurazione su ciascuno di essi.

Procedura

- Passo 1** Accedi alla pagina web.
- Passo 2** Selezionare **Centro di manutenzione>Gestione>Configurazione**.

Figura 3-42 Gestione della configurazione

The screenshot shows a web interface titled 'Config'. Under the heading 'Export Configuration File', there is a text input field labeled 'File', a 'Browse' button, and an 'Import File' button. Below these elements is a yellow warning box with an information icon and the text: 'Imported configuration will overwrite previous configuration.'

- Passo 3** Esporta o importa file di configurazione.
- Esporta il file di configurazione.
- Clic **File di configurazione per l'esportazione** per scaricare il file sul computer locale.



La proprietà intellettuale non verrà esportata.

- Importa il file di configurazione.
1. Fare clic **Sfoglia** per selezionare il file di configurazione.
 2. Fare clic **Importa configurazione**.



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

3.9.5.2 Configurazione della soglia di similarità delle impronte digitali

Configura la soglia di somiglianza dell'impronta digitale. Maggiore è il valore, maggiore è la precisione e minore è la percentuale di successo.

Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Selezionare **Centro di manutenzione>Gestione>Configurazione** Inserisci la
- Passo 3 soglia di similarità e poi fai clic **Fare domanda a**.



- Il parametro è disponibile sul controller di accesso modulare con modulo per impronte digitali.
- Il parametro è disponibile sul controller di accesso con funzione di riconoscimento delle impronte digitali.

Figura 3-43 Soglia di similarità delle impronte digitali

3.9.5.3 Ripristino delle impostazioni predefinite di fabbrica

Procedura

- Passo 1 Selezionare **Centro di manutenzione>Gestione>Configurazione**.



Ripristino del **Dispositivo** Ripristinare le impostazioni predefinite comporterà la perdita di dati. Si prega di tenerne conto.

- Passo 2 Se necessario, ripristinare le impostazioni predefinite di fabbrica.
- **Impostazioni predefinite di fabbrica:** Ripristina tutte le configurazioni del dispositivo ed elimina tutti i dati.
 - **Ripristina le impostazioni predefinite (ad eccezione delle informazioni utente e dei registri):** Ripristina le configurazioni del dispositivo ed elimina tutti i dati ad eccezione delle informazioni utente e dei registri.

3.9.5.4 Manutenzione

Riavviare regolarmente il dispositivo durante i periodi di inattività per migliorarne le prestazioni.

Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Selezionare **Centro di manutenzione>Gestione>Manutenzione** Imposta l'ora e
- Passo 3 poi fai clic **Fare domanda a**.

Il dispositivo si riavvierà all'ora programmata oppure puoi fare clic **Ricominciare** per riavviarlo immediatamente.

3.9.6 Aggiornamento del sistema



- Utilizza il file di aggiornamento corretto. Assicurati di ottenere il file di aggiornamento corretto dal supporto tecnico.
- Non scollegare l'alimentazione o la rete e non riavviare o spegnere il dispositivo durante l'aggiornamento.
- L'aggiornamento a una versione precedente potrebbe comportare potenziali rischi. Si prega di tenerne conto.
- Se si avvia il dispositivo per la prima volta o lo si ripristina alle impostazioni di fabbrica, il dispositivo esegue automaticamente un backup dei file di sistema entro i primi 10 minuti. Si prega di non effettuare aggiornamenti durante questo periodo.

3.9.6.1 Aggiornamento file

Procedura

Passo 1 Nella pagina iniziale, selezionare **Centro di manutenzione > Aggiornamento**. In

Passo 2 **Aggiornamento file**, clic **Sfoglia** e quindi caricare il file di aggiornamento.



Il file di aggiornamento deve essere un file .bin.

Passo 3 Clic **Aggiornamento**.

Il dispositivo si riavvierà al termine dell'aggiornamento.

3.9.6.2 Aggiornamento online

Procedura

Passo 1 Nella pagina iniziale, selezionare **Centro di manutenzione > Aggiornamento**. Nel

Passo 2 **Aggiornamento online** area, selezionare un metodo di aggiornamento.

- Selezionare **Verifica automatica della presenza di aggiornamenti** il dispositivo verificherà automaticamente la disponibilità di aggiornamenti alla versione più recente.
- Selezionare **Controllo manuale** e puoi verificare immediatamente se è disponibile l'ultima versione.

Passo 3 (Facoltativo) Fare clic **Aggiorna ora** per aggiornare immediatamente il dispositivo.

3.9.7 Manutenzione avanzata

Acquisire informazioni sul dispositivo e catturare i pacchetti per facilitare al personale di manutenzione la risoluzione dei problemi.

3.9.7.1 Esportazione

Procedura

Passo 1 Nella pagina iniziale, selezionare **Centro di manutenzione > Manutenzione avanzata > Esportare**.

Passo 2 Clic **Esportare** per esportare il numero di serie, la versione del firmware, i registri operativi del dispositivo e le informazioni di configurazione.

3.9.7.2 Acquisizione dei pacchetti

Procedura

Passo 1 Nella pagina iniziale, selezionare **Centro di manutenzione** > **Manutenzione avanzata** > **Acquisizione dei pacchetti**.

Figura 3-44 Acquisizione del pacchetto

Packet Capture							
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0	1 166	Optional	Optional	Optional	Optional	0.00MB	►
eth2	1 101	Optional	Optional	Optional	Optional	0.00MB	►

Passo 2 Inserisci l'indirizzo IP, fai clic su ►

► cambia in . II

Passo 3 Dopo aver raccolto dati sufficienti, fai clic su . II

I pacchetti acquisiti vengono scaricati automaticamente sul computer locale.

3.10 Impostazioni di sicurezza (facoltativo)

3.10.1 Stato della sicurezza

Eseguire una scansione dei moduli utenti, servizi e sicurezza per verificare lo stato di sicurezza del dispositivo.

Informazioni di base

- Rilevamento di utenti e servizi: verifica se la configurazione corrente è conforme alle raccomandazioni.
- Scansione dei moduli di sicurezza: viene analizzato lo stato di funzionamento dei moduli di sicurezza, come la trasmissione audio e video, la protezione affidabile, gli avvisi di sicurezza e la difesa dagli attacchi, senza tuttavia rilevarne l'attivazione.

Procedura

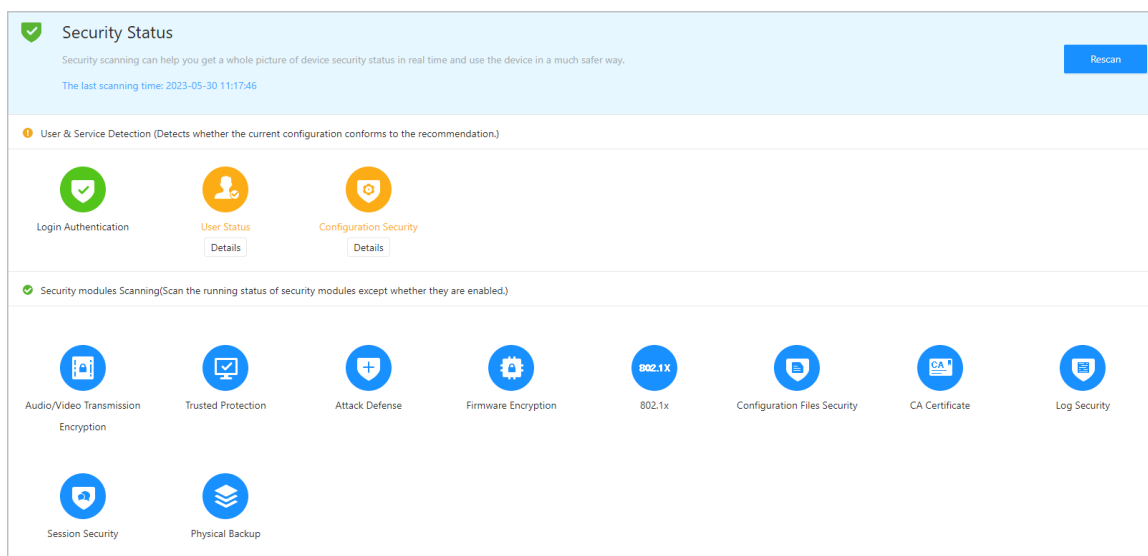
Passo 1 Selezionare  > **Stato di sicurezza**.

Passo 2 Clic **Riscansione** per eseguire una scansione di sicurezza del dispositivo.



Passa il mouse sopra le icone dei moduli di sicurezza per visualizzarne lo stato di esecuzione.

Figura 3-45 Stato di sicurezza



Operazioni correlate

Dopo aver eseguito la scansione, i risultati verranno visualizzati con colori diversi. Il giallo indica che i moduli di sicurezza sono anomali, mentre il verde indica che i moduli di sicurezza sono normali.

- Clic**Dettagli** per visualizzare i dettagli sui risultati della scansione.
- Clic**Ignorare** Ignorando l'anomalia, questa non verrà rilevata. L'anomalia ignorata verrà evidenziata in grigio.
- Clic**Ottimizzare** per risolvere l'anomalia.

3.10.2 Configurazione del servizio di sistema

Crea un certificato o carica un certificato autenticato, dopodiché potrai accedere alla pagina web tramite HTTPS dal tuo computer. HTTPS protegge la comunicazione su una rete informatica.

Procedura

Passo 1 Selezionare  > **Servizio di sistema** > **Servizio di sistema**.

Passo 2 Attiva il servizio HTTPS.



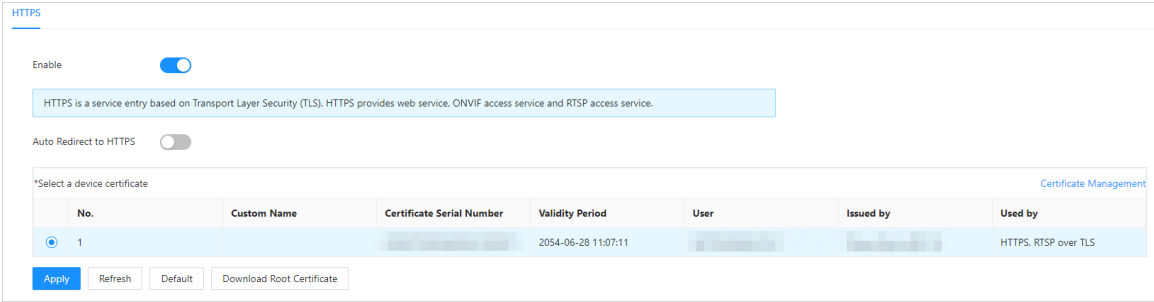
Se si attiva la compatibilità con TLS v1.1 e versioni precedenti, potrebbero verificarsi rischi per la sicurezza. Si prega di tenerne conto.

Passo 3 Selezionare il certificato.



Se nell'elenco non sono presenti certificati, fare clic su **Gestione dei certificati** per caricare un certificato.

Figura 3-46 Servizio di sistema



Passo 4 Clic**Fare domanda a.**

Inserisci “https://indirizzo IP:httpsport” in un browser web. Se il certificato è installato, è possibile accedere alla pagina web correttamente. In caso contrario, la pagina web visualizzerà il certificato come errato o non attendibile.

3.10.3 Attacco Difesa

3.10.3.1 Configurazione del firewall

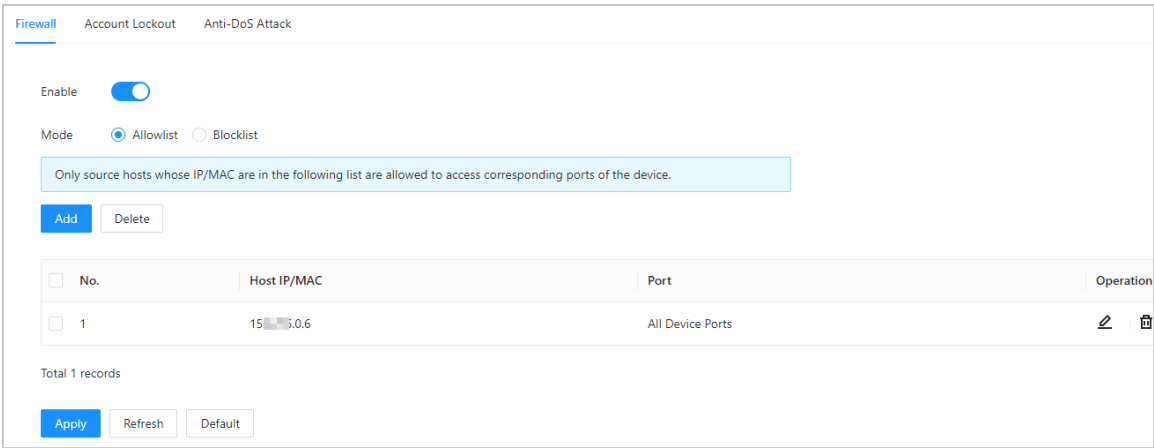
Configura il firewall per limitare l'accesso al dispositivo.

Procedura

Passo 1 Selezionare > **Difesa dall'attacco>Firewall**

Passo 2 Clic ...per abilitare la funzione firewall.

Figura 3-47 Firewall



Passo 3 Seleziona la modalità:**Lista consentita****E****Lista bloccata.**

- **Lista consentita:**Solo gli indirizzi IP/MAC presenti nella lista di accesso consentito possono accedere al dispositivo.
- **Lista bloccata:**Gli indirizzi IP/MAC presenti nella lista nera non possono accedere al dispositivo.

Passo 4 Clic**Aggiungere**per inserire le informazioni IP.

Figura 3-48 Aggiungi informazioni IP

The 'Add' dialog box is used to configure IP settings. It includes the following elements:

- Add Mode:** A dropdown menu currently set to 'IP'.
- IP Version:** A dropdown menu currently set to 'IPv4'.
- IP Address:** A text input field with three dots, indicating a placeholder for the IP address.
- All Device Ports:** A toggle switch that is currently turned on (blue).
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Passo 5 Clic **OK**.

Operazioni correlate

- Clic  Per modificare le informazioni
- Clic  IP. Per eliminare l'indirizzo IP.

3.10.3.2 Configurazione del blocco dell'account

Se la password viene inserita in modo errato per un numero predefinito di volte, l'account verrà bloccato.

Procedura

Passo 1 Selezionare  > **Difesa dall'attacco>Blocco dell'account**.

Passo 2 Inserisci il numero di tentativi di accesso e la durata del blocco dell'account amministratore e dell'utente ONVIF.

Figura 3-49 Blocco dell'account

The screenshot shows the 'Account Lockout' configuration page. It features three tabs at the top: 'Firewall', 'Account Lockout' (which is the active tab), and 'Anti-DoS Attack'. Below the tabs, the 'Device Account' section contains two configuration fields. The 'Login Attempt' field is a dropdown menu currently showing '5time(s)'. The 'Lock Time' field is a text input showing '5', followed by a 'min' unit label. At the bottom of the configuration area, there are three buttons: a blue 'Apply' button, a 'Refresh' button, and a 'Default' button.

- Tentativi di accesso: il limite di tentativi di accesso. Se la password errata viene inserita per un numero predefinito di volte, l'account verrà bloccato.
- Tempo di blocco: la durata durante la quale non è possibile accedere dopo il blocco dell'account. Clicca **Fare**

Passo 3 domanda a.

3.10.3.3 Configurazione della protezione dagli attacchi DoS

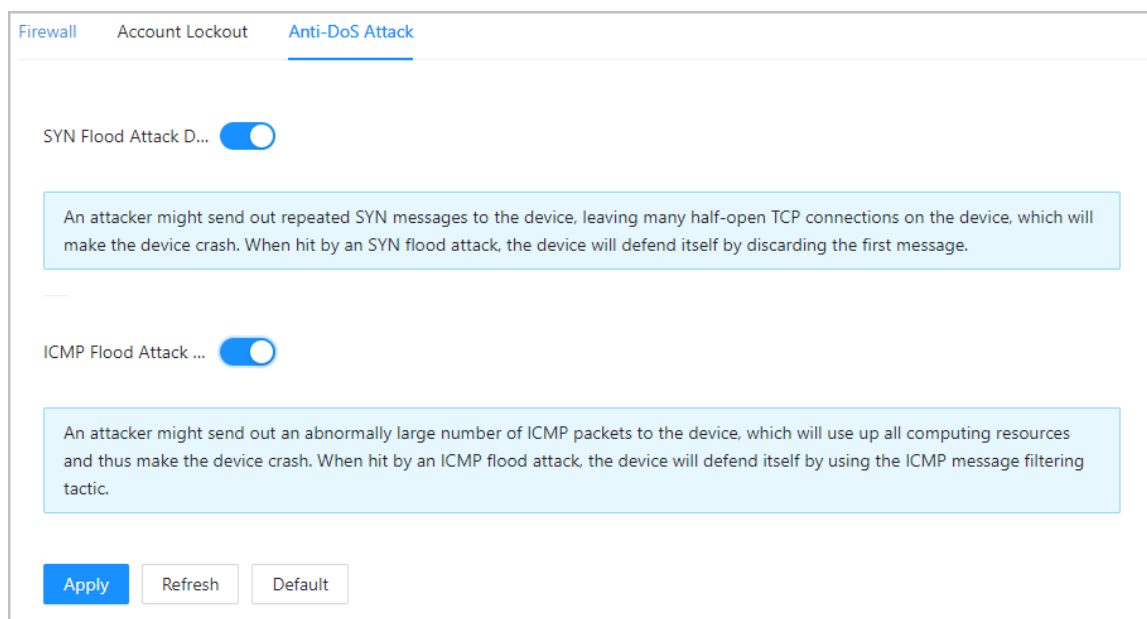
È possibile abilitare **Difesa dall'attacco di alluvione SYN** e **Difesa dagli attacchi di alluvione ICMP** per difendere il dispositivo dagli attacchi DoS.

Procedura

Passo 1 Selezionare  > **Difesa dall'attacco** > **Attacco anti-DoS**.

Passo 2 Accendere **Difesa dall'attacco di alluvione SYN** e **Difesa dagli attacchi di alluvione ICMP** per proteggere il dispositivo dagli attacchi DoS.

Figura 3-50 Attacco anti-DoS



Passo 3 Cliccare domanda a.

3.10.4 Installazione del certificato del dispositivo

Crea un certificato o carica un certificato autenticato, dopodiché potrai accedere tramite HTTPS dal tuo computer.

3.10.4.1 Creazione del certificato

Creare un certificato per il dispositivo.

Procedura

- Passo 1** Selezionare  > **Certificato CA** > **Certificato del dispositivo**.
- Passo 2** Selezionare **Installa il certificato del dispositivo**
- Passo 3** Seleziona **Crea certificato**, e clicca **Prossimo** Inserire le
- Passo 4** informazioni del certificato.

Figura 3-51 Informazioni sul certificato

Step 2: Fill in certificate information.

Custom Name

* IP/Domain Name

Organization Unit

Organization

* Validity Period Days (1~5000)

* Region

Province

City Name

Back Create and install certificate Cancel



Il nome della regione non può superare i 2 caratteri. Si consiglia di inserire l'abbreviazione del nome della regione.

Passo 5 Clic**Creare e installare il certificato.**

Il certificato appena installato viene visualizzato su**Certificato del dispositivo**pagina dopo l'installazione corretta del certificato.

Operazioni correlate

- Clic**Accedi alla modalità di modifica**sulla**Certificato del dispositivo**pagina per modificare il nome del certificato.
- Clic  Per scaricare il certificato. Per
- Clic  eliminare il certificato.

3.10.4.2 Richiesta e importazione del certificato CA

Importa il certificato CA di terze parti sul dispositivo.

Procedura

- Passo 1** Selezionare  > **Certificato CA>Certificato del dispositivo.**
- Passo 2** Clic**Installa il certificato del dispositivo.**
- Passo 3** Selezionare**Richiedi il certificato CA e l'importazione (consigliato)**,e clicca**Prossimo**
- Passo 4** Inserire le informazioni del certificato.
- IP/Nome di dominio: l'indirizzo IP o il nome di dominio del dispositivo.

- Regione: Il nome della regione non deve superare i 3 caratteri. Si consiglia di inserire l'abbreviazione del nome della regione.

Figura 3-52 Informazioni sul certificato (2)

Step 2: Fill in certificate information.

* IP/Domain Name

Organization Unit

Organization

* Region

Province

City Name

Back Create and Download Cancel

Passo 5 **ClicCrea e scarica.**

Salva il file di richiesta sul tuo computer.

Passo 6 Richiedi il certificato a un'autorità di certificazione (CA) di terze parti utilizzando il file di richiesta.

Passo 7 Importa il certificato CA firmato.

1. Salva il certificato CA sul tuo computer.

2. Fare clic**Installazione del certificato del dispositivo**.

3. Fare clic**Sfoglia**per selezionare il certificato CA.

4. Fare clic**Importa e installa**.

Il certificato appena installato viene visualizzato su**Certificato del dispositivo**pagina dopo l'installazione corretta del certificato.

- Clic**Ricreare**per ricreare il file di richiesta.
- Clic**Importa in seguito**per importare il certificato in un secondo momento.

Operazioni correlate

- Clic**Accedi alla modalità di modifica**sulla**Certificato del dispositivo**pagina per modificare il nome del certificato.
- Clic  Per scaricare il certificato. Per
- Clic  eliminare il certificato.

3.10.4.3 Installazione di un certificato esistente

Se disponi già di un certificato e di un file di chiave privata, importali.

Procedura

Passo 1 Selezionare**Sicurezza>Certificato CA>Certificato del dispositivo**.

- Passo 2** Clic**Installa il certificato del dispositivo**.
- Passo 3** Selezionare**Installa il certificato esistente**,e clicca**Prossimo**.
- Passo 4** Clic**Sfoglia**Selezionare il file del certificato e della chiave privata e inserire la password della chiave privata.

Figura 3-53 Certificato e chiave privata

- Passo 5** Clic**Importa e installa**.
- Il certificato appena installato viene visualizzato su**Certificato del dispositivo**pagina dopo l'installazione corretta del certificato.

Operazioni correlate

- Clic**Accedi alla modalità di modifica**sulla**Certificato del dispositivo**pagina per modificare il nome del certificato.
- Clic  Per scaricare il certificato. Per
- Clic  eliminare il certificato.

3.10.5 Installazione del certificato CA attendibile

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

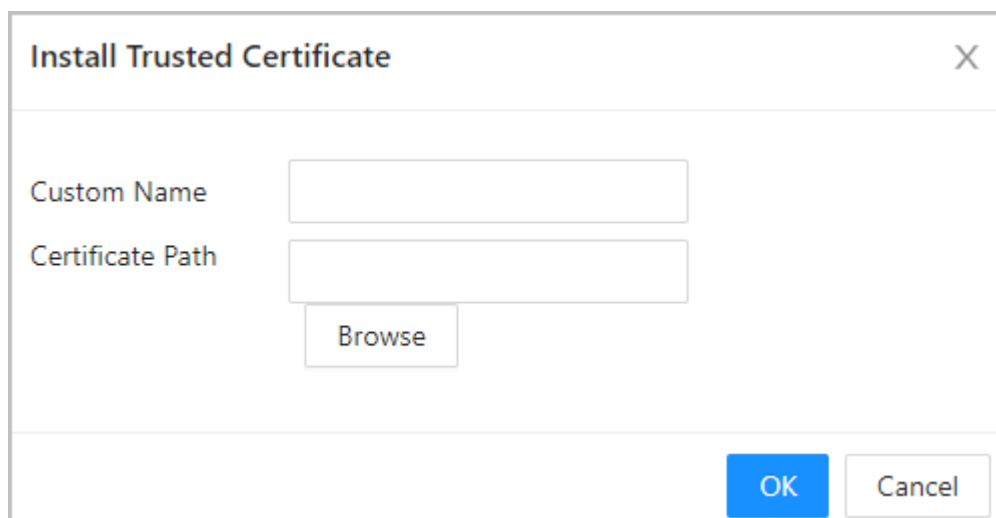
Informazioni di base

802.1X è un protocollo di autenticazione di rete che apre le porte per l'accesso alla rete quando un'organizzazione autentica l'identità di un utente e lo autorizza ad accedere alla rete.

Procedura

- Passo 1** Selezionare  > **Certificato CA>Certificati CA affidabili**.
- Passo 2** Selezionare**Installa il certificato attendibile**.
- Passo 3** Clic**Sfoglia**per selezionare il certificato attendibile.

Figura 3-54 Installare il certificato attendibile



Passo 4 Clic **OK**.

Il certificato appena installato viene visualizzato su **Certificati CA affidabili** pagina dopo l'installazione corretta del certificato.

Operazioni correlate

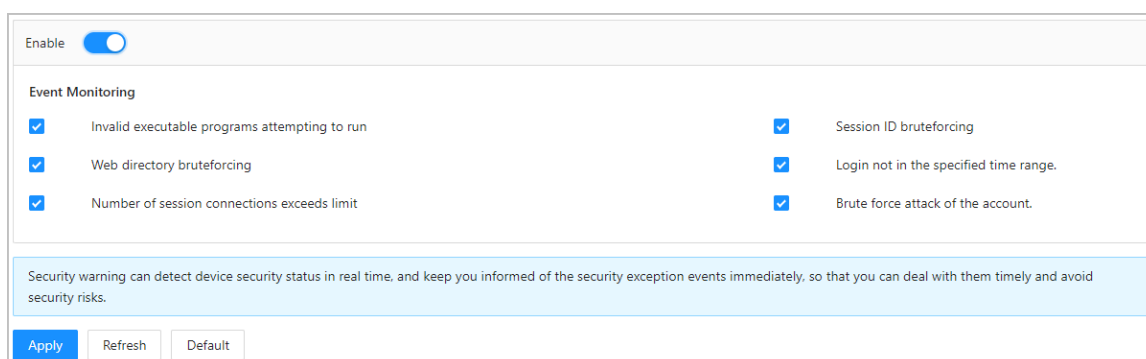
- Clic **Accedi alla modalità di modifica** sulla **Certificato del dispositivo** pagina per modificare il nome del certificato.
- Clic  Per scaricare il certificato. Per
- Clic  eliminare il certificato.

3.10.6 Avviso di sicurezza

Procedura

- Passo 1** Selezionare  > **Avviso di sicurezza**.
- Passo 2** Attiva la funzione di avviso di sicurezza.
- Passo 3** Seleziona gli elementi da monitorare.

Figura 3-55 Avviso di sicurezza



Passo 4 Clic **Fare domanda a**.

3.10.7 Autenticazione di sicurezza

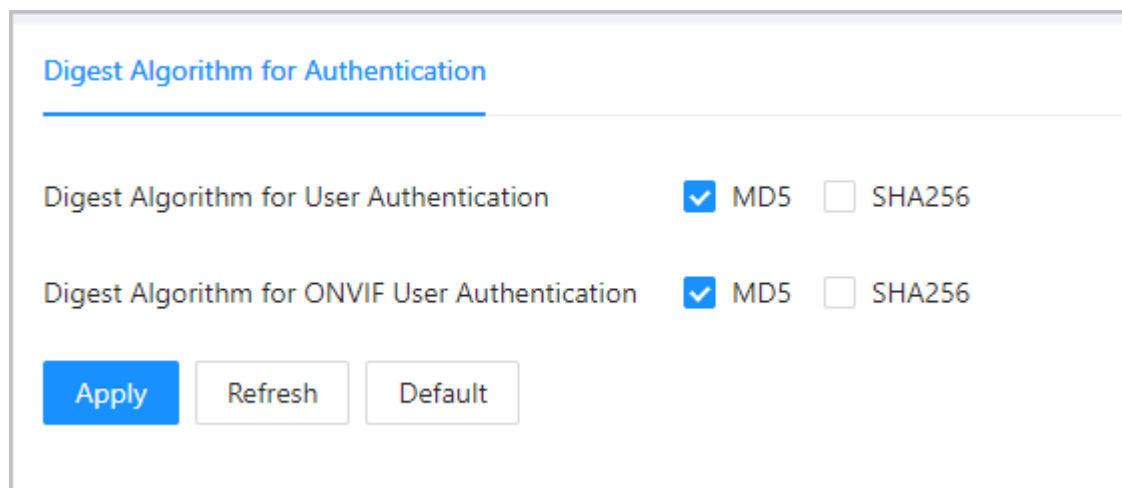
Procedura

Passo 1 Selezionare **Sicurezza>Autenticazione di sicurezza**

Passo 2 Selezionare un algoritmo di digest del messaggio.

Passo 3 Clic **Fare domanda a**.

Figura 3-56 Autenticazione di sicurezza



Digest Algorithm for Authentication

Digest Algorithm for User Authentication ☒ MD5 ☐ SHA256

Digest Algorithm for ONVIF User Authentication ☒ MD5 ☐ SHA256

Apply Refresh Default

4 Operazioni telefoniche

Prima di accedere alla pagina web del dispositivo sul telefono, assicurati di aver inizializzato il dispositivo tramite la pagina web sul computer.

Si consiglia di utilizzare il telefono in modalità verticale e in modalità diurna. È possibile accedere alla pagina web del dispositivo dal telefono tramite i seguenti metodi.

- Collega il dispositivo alla rete tramite il cavo di rete. Assicurati che il telefono e il dispositivo siano connessi alla stessa rete. Apri il browser sul telefono e inserisci l'indirizzo IP del dispositivo.
- Collega il dispositivo e il telefono alla stessa rete Wi-Fi. Apri il browser sul telefono e inserisci l'indirizzo IP corrispondente alla rete Wi-Fi a cui sei connesso.
- Collega il telefono alla rete tramite il Wi-Fi del dispositivo. Apri il browser sul telefono e inserisci l'indirizzo IP corrispondente all'AP Wi-Fi del dispositivo (di default è 192.168.3.1).



Il nome Wi-Fi del dispositivo viene visualizzato in **Numero di serie del dispositivo + Modello del dispositivo** modalità.



- Il Wi-Fi e il Wi-Fi AP sono disponibili su alcuni modelli.
- Quando si accede alla pagina web tramite telefono, è supportata solo la lingua inglese.

4.1 Inizializzazione

Quando il telefono si trova sulla stessa rete LAN del controller di accesso, è possibile inizializzare quest'ultimo per la prima volta o dopo il ripristino delle impostazioni di fabbrica del dispositivo tramite la pagina web del telefono.

Prerequisiti

Assicurarsi che il controller di accesso non sia connesso alla rete Wi-Fi o 4G.

Esistono principalmente 3 modi per connettere il dispositivo e il telefono alla stessa rete. Questa sezione illustra l'inizializzazione sul telefono tramite punto di accesso Wi-Fi.

- Collega il dispositivo alla rete tramite il cavo di rete. Assicurati che il telefono e il dispositivo siano connessi alla stessa rete. Apri il browser sul telefono e inserisci l'indirizzo IP del dispositivo.
- Collega il dispositivo e il telefono alla stessa rete Wi-Fi. Apri il browser sul telefono e inserisci l'indirizzo IP corrispondente alla rete Wi-Fi a cui sei connesso.
- Collega il telefono alla rete tramite il Wi-Fi del dispositivo. Apri il browser sul telefono e inserisci l'indirizzo IP corrispondente all'AP Wi-Fi del dispositivo (di default è 192.168.3.1).



Il Wi-Fi e il Wi-Fi AP sono disponibili su alcuni modelli.

Procedura

Passo 1 Accendere il controller di accesso.

Passo 2 Connettiti all'hotspot Wi-Fi sul tuo telefono. Il nome dell'hotspot è **numero di serie del prodotto + modello del dispositivo**.

Se non ti connetti all'hotspot Wi-Fi entro 30 minuti, l'hotspot è disattivato.

Passo 3 Apri un browser sul tuo telefono e vai all'indirizzo IP (l'indirizzo predefinito è 192.168.3.1) dell'hotspot.

Passo 4 Rubinetto **Avvio dell'inizializzazione**.

Passo 5 Inserisci e conferma la password, inserisci un indirizzo email.



- La password deve essere composta da 8 a 32 caratteri non vuoti e contenere almeno due dei seguenti tipi di caratteri: maiuscole, minuscole, numeri e caratteri speciali (esclusi ' , ; , : e). Imposta una password ad alta sicurezza seguendo le istruzioni per la complessità della password.
- Dopo l'inizializzazione, conserva la password in un luogo sicuro e cambiala regolarmente per migliorare la sicurezza.

Passo 6 (Facoltativo) Abilitare l'indirizzo e-mail e quindi configurarlo.



Se si desidera reimpostare la password dell'amministratore tramite la scansione del codice QR, è necessario abilitare la funzione e-mail e configurare l'indirizzo e-mail per la ricezione del codice di sicurezza.

Passo 7 (Facoltativo) Seleziona **Ho letto e accetto il Contratto di licenza del software e l'Informativa sulla privacy**. Rubinetto

Passo 8 **Prossimo**.

Passo 9 Abilitare **Verifica automatica della presenza di aggiornamenti** secondo necessità, quindi toccare **Completato**.

Viene visualizzata la pagina di accesso.

4.2 Accesso alla pagina web

Prerequisiti

Assicurati che il telefono utilizzato per accedere alla pagina web sia connesso alla stessa rete LAN del dispositivo.

Procedura

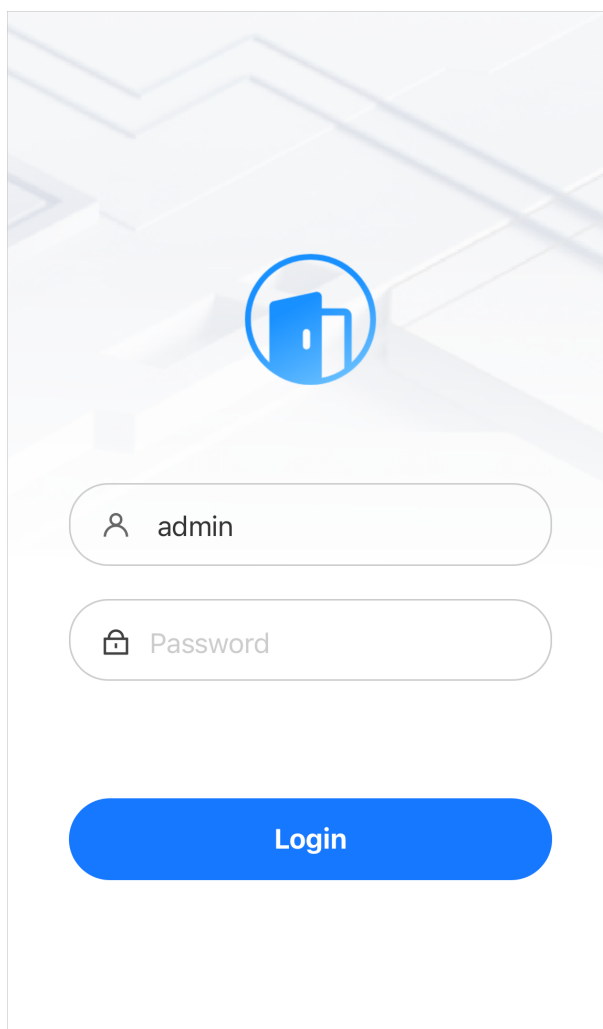
Passo 1 Apri un browser e accedi all'indirizzo IP del dispositivo.

Passo 2 Inserisci nome utente e password.



- Il nome amministratore predefinito è admin e la password è quella impostata durante l'inizializzazione. Si consiglia di cambiare regolarmente la password dell'amministratore per aumentare la sicurezza.
- Se dimentichi la password di accesso dell'amministratore, puoi reimpostarla tramite la pagina web sul computer.

Figura 4-1 Pagina di accesso

The image shows a login page with a light gray background featuring a subtle geometric pattern of overlapping planes. At the top center is a blue circular icon containing a white door handle. Below this icon are two input fields: the first contains the text 'admin' preceded by a small person icon, and the second contains the text 'Password' preceded by a small lock icon. At the bottom center is a large, rounded blue button with the word 'Login' in white text.

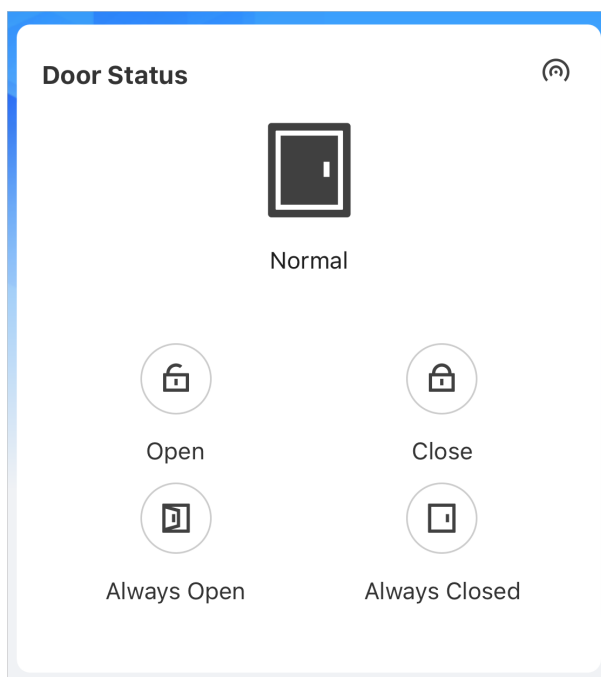
Passo 3 Clic**Login**.

4.3 Pagina iniziale

La pagina iniziale viene visualizzata dopo aver effettuato l'accesso con successo.

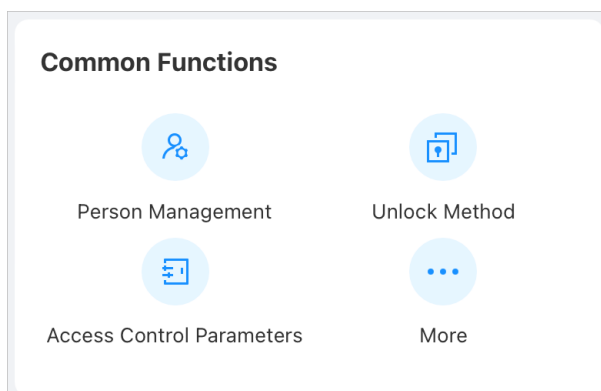
- **ILStato della porta**L'area visualizza lo stato della porta. È possibile aprire o chiudere la porta a distanza. È inoltre possibile configurare lo stato della porta come**Sempre aperto**O**Sempre chiuso**.

Figura 4-2 Stato della porta



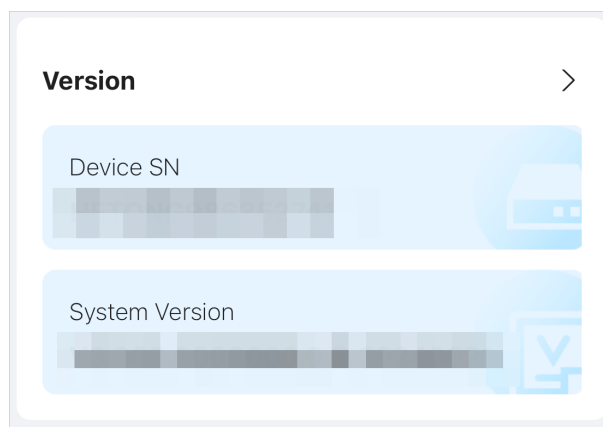
- IL **Funzione comune** area visualizza il menu di configurazione del dispositivo. Fare clic **Di più** per visualizzare tutti i menu di configurazione.

Figura 4-3 Funzioni comuni



- Visualizza il numero di serie e le informazioni sulla versione su **Versione** area. Fare clic **>** per visualizzare i dettagli della versione.

Figura 4-4 Versione



4.4 Gestione del personale

Aggiungi la persona e configura le autorizzazioni.

Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Clic **Gestione del personale**, e poi fai clic+
- Passo 3 Configura le informazioni utente.

Figura 4-5 Aggiungi la persona (1)

A screenshot of a mobile application form titled 'Basic Info'. The form has a light grey background. It contains several input fields and a table. The first section has a red asterisk followed by 'User ID' and a text input field. Below it is a 'Name' text input field. The second section is titled 'Verification Mode' and contains a table with three rows: 'Password' (with 'Not Added' and a right arrow), 'Card' (with '0' and a right arrow), and 'Fingerprint' (with '0' and a right arrow).

Figura 4-6 Aggiungi la persona (2)

Verification Mode	Custom >
Combination Method	Or >
Unlock Method	Card, Fingerprint, Password >
Validity Period	2037-12-31 23:59:59 >
General Plan	255-Default >
Holiday Plan	255-Default >
User Type	General User >
Times Used	Unlimited
Add	

Tabella 4-1 Descrizione dei parametri

Parametro	Descrizione
ID utente	L'ID utente è simile all'ID dipendente, ovvero può essere costituito da numeri, lettere e loro combinazioni, e la lunghezza massima del numero è di 30 caratteri.
Nome	Il nome può contenere fino a 32 caratteri (inclusi numeri, simboli e lettere).
Password	Configura la password utente. La lunghezza massima della password è di 8 cifre. La password di emergenza è la password di sblocco + 1. Ad esempio, se la password utente è 12345, la password di emergenza sarà 12346. Un allarme di emergenza si attiverà quando si utilizza la password di emergenza per sbloccare la porta.

Parametro	Descrizione
Carta	● Inserisci manualmente il numero della carta. 1. Fare clic Aggiungere. 2. Inserisci il numero della carta e poi fai clic Aggiungere. ● Il numero viene letto automaticamente dal dispositivo. 1. Fare clic Aggiungere. 2. Passare le carte sul lettore di carte. Viene visualizzato un conto alla rovescia di 60 secondi per ricordarti di strisciare le carte e il sistema leggerà automaticamente il numero della carta. Se il conto alla rovescia di 60 secondi scade, fai clic Leggi la scheda di nuovo per iniziare un nuovo conto alla rovescia. 3. Fare clic OK. Ogni utente può registrare al massimo 5 carte. Inserisci il numero della tua carta o strisciala, e il dispositivo leggerà le informazioni relative. È possibile abilitare il Carta di coercizione funzione. Si attiverà un allarme se si utilizza una tessera di emergenza per sbloccare la porta. ● Carta di coercizione: Fai clic per impostare la carta di coercizione. ● Cambiare il numero della carta.: Fai clic per modificare il numero della carta.  Ogni utente può impostare una sola carta di coercizione.
Impronta digitale	Registrazione delle impronte digitali. Un utente può registrare fino a 3 impronte digitali ed è possibile impostarne una come impronta digitale di emergenza. Un allarme si attiverà quando l'impronta digitale di emergenza viene utilizzata per sbloccare la porta. Registra le impronte digitali tramite un lettore di impronte o il dispositivo. 1. Fare clic Aggiungere. 2. Premere il dito sullo scanner seguendo le istruzioni visualizzate sullo schermo. 3. Fare clic OK.  ● La funzione di riconoscimento delle impronte digitali è disponibile solo su alcuni modelli. ● Non consigliamo di impostare la prima impronta digitale come impronta digitale di emergenza. ● Ogni utente può impostare una sola impronta digitale di emergenza.

Parametro	Descrizione
Modalità di verifica	Configura la modalità di verifica per la persona. Puoi utilizzare la stessa modalità del dispositivo oppure personalizzarla. ● Uguale al dispositivo: La modalità è la stessa del dispositivo. ● Costume: Dopo aver selezionato Costume, Metodo combinato e Metodo di sblocco vengono visualizzati. Selezionare il metodo di combinazione e i metodi di sblocco necessari. ◇ Oppure: Utilizza uno dei metodi di sblocco selezionati per aprire la porta. E ◇ ancora: Utilizza tutti i metodi di sblocco selezionati per aprire la porta.  ◇ La modalità di verifica personalizzata è valida solo per il dispositivo locale. Non può essere utilizzata con lettori di schede esterni. ◇ Quando la modalità di verifica personalizzata è diversa dalla modalità del dispositivo, la modalità personalizzata ha la priorità.
Periodo di validità	Imposta una data di scadenza per l'accesso e l'autorizzazione alla presenza della persona.
Piano generale	Durante il periodo definito, le persone possono sbloccare la porta o effettuare il rilevamento delle presenze.  È possibile selezionare più di un piano.
Piano vacanze	Durante il periodo festivo definito, è possibile sbloccare la porta o effettuare il rilevamento delle presenze.  È possibile selezionare più di una festività.
Tipo di utente	● Utente generico: Gli utenti generici possono sbloccare la porta. ● Utente bloccato: Quando gli utenti presenti nella lista nera sbloccano la porta, il personale di servizio riceverà una notifica. ● Utente ospite: Gli ospiti possono sbloccare la porta entro un periodo di tempo definito o per un numero limitato di volte. Trascorso il periodo definito o il numero di volte in cui è possibile sbloccare la porta, non sarà più possibile farlo. ● Utente di pattuglia: Gli utenti addetti alla pattuglia possono registrare le presenze sul dispositivo, ma non hanno l'autorizzazione ad aprire le porte. ● Utente VIP: Quando i VIP sbloccano la porta, non sono limitati dalle modalità di sblocco, come Multi-carta e Sezione temporale. ● Altro utente: Quando sbloccano la porta, questa rimarrà sbloccata per altri 5 secondi. ● Utente personalizzato 1/Utente personalizzato 2: Uguale agli utenti generici.
Tempo impiegato	Imposta un limite di tempo per lo sblocco degli utenti ospiti. Trascorso tale periodo, non potranno più aprire la porta.

Passo 4

Rubinetto Aggiungere.

4.5 Configurazione del sistema

4.5.1 Visualizzazione delle informazioni sulla versione

Nella pagina web, selezionare **Di più>Sistema>Versione** e puoi visualizzare le informazioni sulla versione sul dispositivo.

4.5.2 Manutenzione

Riavviare regolarmente il dispositivo durante i periodi di inattività per migliorarne le prestazioni.

Procedura

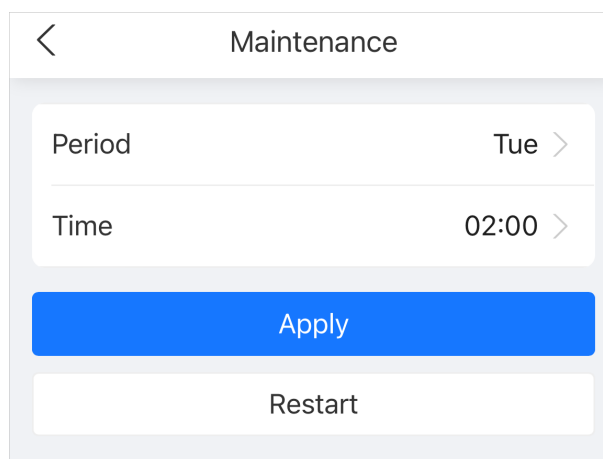
Passo 1 Accedi alla pagina web.

Passo 2 Selezionare **Di più>Sistema>Manutenzione**

Passo 3 Imposta l'ora e poi fai clic **Fare domanda a**.

Il dispositivo si riavvierà all'ora programmata oppure puoi fare clic **Ricomincia** per riavviarlo immediatamente.

Figura 4-7 Manutenzione



4.5.3 Configurazione dell'ora

Procedura

Passo 1 Accedi alla pagina web.

Passo 2 Seleziona **Di più>Sistema>**

Passo 3 **Tempo** Configura l'ora.

Figura 4-8 Configurare i parametri temporali

<

Time

Time

Manually Set >

System Time

2024-06-25 11:13:03 >

Sync Time

Sync Phone

Date Format

YYYY-MM-DD >

Time Format

24-Hour >

Time Zone

(UTC+08:00) Beijing, >

DST

☐

Type

Date >

Start Time

01-01 00:00 >

End Time

01-02 00:00 >

Tabella 4-2 Descrizione delle impostazioni dell'ora

Parametro	Descrizione
Tempo	● Impostazione manuale: inserisci manualmente l'ora oppure puoi fare clicSincronizza il telefono per sincronizzare l'ora con il telefono. ● NTP: Il dispositivo sincronizzerà automaticamente l'ora con il server NTP. ◇ Server:Inserisci il dominio del server NTP. ◇ Porta:Inserisci la porta del server NTP. ◇ Intervallo:Inserisci il suo orario con l'intervallo di sincronizzazione.
Formato data	Seleziona il formato della data e il formato dell'ora.
Formato orario	
Fuso orario	Seleziona il fuso orario.
ora legale	1. (Facoltativo) Attivare l'ora legale. 2. SelezionaData O Settimanacome ilTipo. 3. Configurare l'ora di inizio e l'ora di fine dell'ora legale.

Passo 4 Clic **Fare domanda a.**

4.5.4 Capacità dati

È possibile visualizzare il numero di utenti, carte, impronte digitali, registri, dati di sblocco e altre informazioni che il dispositivo può memorizzare.

Accedi alla pagina web e seleziona **Di più>Sistema>Capacità dati**.

4.5.5 Lingua

Accedi alla pagina web, seleziona **Di più>Sistema>Lingua**. Cambia la lingua e poi tocca **Fare domanda a.**

4.6 Configurazione del controllo degli accessi

4.6.1 Configurazione dei metodi di sblocco

Per sbloccare la porta è possibile utilizzare diversi metodi, come l'impronta digitale, la tessera e la password. È anche possibile combinarli per creare un metodo di sblocco personalizzato.

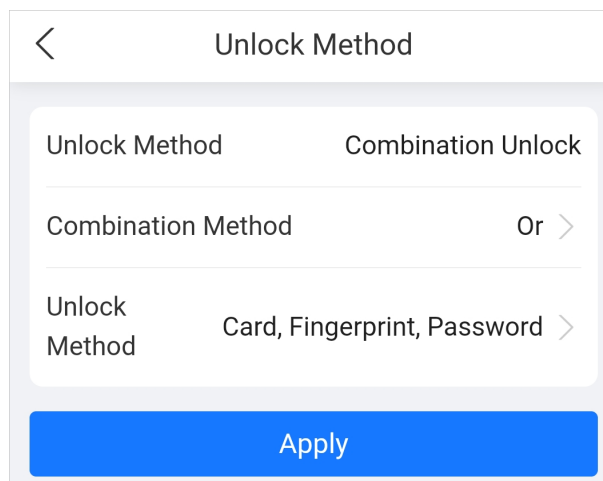
Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Clic **Metodo di sblocco** nel menu principale oppure selezionare **Di più>Controllo degli accessi>Metodo di sblocco**.
- Passo 3 (Facoltativo) Configura il metodo di combinazione e il metodo di sblocco, quindi fai clic **Fare domanda a.**

- Metodo combinato
 - ◇ Oppure: Utilizza uno dei metodi di sblocco selezionati per aprire la porta. E
 - ◇ ancora: Utilizza tutti i metodi di sblocco selezionati per aprire la porta.
- Metodo di sblocco

Selezionare il metodo di sblocco in base alle funzionalità supportate dal dispositivo.

Figura 4-9 Metodo di sblocco



4.6.2 Configurazione dei parametri di controllo degli accessi

Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Clic **Parametri di controllo degli accessi** nel menu principale oppure selezionare **Di più > Controllo degli accessi > Parametri di controllo degli accessi**.
- Passo 3 Configura i parametri di base per il controllo degli accessi, quindi tocca **Fare domanda a**.

Figura 4-10 Parametri di controllo degli accessi (1)

Name	Door1
Door Status	Normal >
Verification Interval	0 s
Card Swiping Interval	0 s (0-86400)
Public Password	☐
Normally Open Period	
General Plan	Disabled >
Holiday Plan	Disabled >
Normally Closed Period	
General Plan	Disabled >
Holiday Plan	Disabled >

Figura 4-11 Parametri di controllo degli accessi (2)

Unlock Settings

Unlock Method

Combination Unlock

Combination Method

Or >

Unlock Method

Card, Fingerprint, Password >

PIN Code Authentication

☐

Door Unlocked Duration

3 s

Remote Verification

☐

Apply

Tabella 4-3 Descrizione dei parametri di controllo degli accessi

Parametro		Descrizione
Impostazioni di base	Nome	Il nome della porta.
	Stato della porta	Imposta lo stato della porta. ● Normale: La porta verrà sbloccata e bloccata in base alle impostazioni selezionate. ● Sempre aperto: la porta rimane sempre sbloccata. ● Sempre chiuso: la porta rimane sempre chiusa a chiave.
	Intervallo di verifica	Se verifichi la tua identità più volte entro un determinato periodo, solo la prima verifica sarà considerata valida e la porta non si aprirà dopo la seconda o le successive verifiche. Dal momento in cui la porta non si apre, dovrai attendere l'intervallo di tempo di verifica configurato prima di poter tentare nuovamente di verificare la tua identità.

Parametro		Descrizione
	strisciamento della carta Intervallo	Al primo utilizzo della carta per la verifica, è normalmente possibile sbloccare la porta o effettuare la rilevazione delle presenze e i dati vengono generati. Entro il periodo configurato, se si utilizza nuovamente la carta per la verifica, non sarà possibile sbloccare la porta o effettuare la rilevazione delle presenze e i dati non verranno generati. Si prega di verificare l'identità dopo il periodo configurato.  IL Intervallo di strisciamento della carta ha la priorità su Intervallo di verifica.
	Password pubblica	Dopo aver abilitato la password pubblica, configura la password. Puoi utilizzare la password pubblica senza inserire l'ID utente per sbloccare la porta. È supportata una sola password pubblica per dispositivo.
Normalmente aperto Periodo	Piano per periodo/vacanze	Quando selezioni Normale È possibile selezionare un intervallo di tempo dall'elenco a discesa. La porta rimarrà aperta o chiusa durante il periodo di tempo definito.
Normalmente chiuso Periodo	Piano per periodo/vacanze	 ● Quando il periodo normalmente aperto è in conflitto con periodo di chiusura normale, periodo di apertura normale ha la priorità rispetto al periodo di chiusura normale. ● Qualora il periodo coincidesse con i piani per le vacanze, questi ultimi avrebbero la precedenza.
Sblocca le impostazioni	Metodo di sblocco	Sblocco tramite combinazione per impostazione predefinita.
	Combinazione Metodo	● Oppure: utilizzare uno dei metodi di sblocco selezionati per aprire la porta. ● Inoltre: utilizza tutti i metodi di sblocco selezionati per aprire la porta.
	Metodo di sblocco	Selezionare il metodo di sblocco in base alle funzionalità supportate dal dispositivo.
	Porta sbloccata Durata	Configura il tempo per cui la porta rimane aperta. Il valore predefinito è di 3 secondi. Quando la porta rimane aperta per un tempo superiore a quello configurato, si chiude.
	Codice PIN Autenticazione	Quando l'autenticazione tramite codice PIN è abilitata, è possibile aprire la porta utilizzando solo la password.  Non è necessario inserire l'ID utente se questa funzione è abilitata. La verifica remota non è supportata.
	Verifica a distanza	Apri la porta a distanza.

4.6.3 Configurazione degli allarmi

Si attiverà un allarme in caso di accesso anomalo.

Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Selezionare **Di più>Controllo degli accessi>Allarme**Configura i
- Passo 3 parametri dell'allarme e poi fai clic **Fare domanda a.**

Figura 4-12 Impostazioni di allarme

Duress Alarm

☒

Anti-passback

☐

Door Detector

☒

Door Detector Status

NO >

Intrusion Alarm

☐

Unlock Timeout Alarm

☐

Unlock Timeout

60 s

Excessive Attempts Alarm

☒

Apply

Tabella 4-4 Descrizione dei parametri di allarme

Parametro	Descrizione
Allarme coercizione	Si attiverà un allarme qualora si utilizzi una tessera, una password o un'impronta digitale di emergenza per sbloccare la porta.

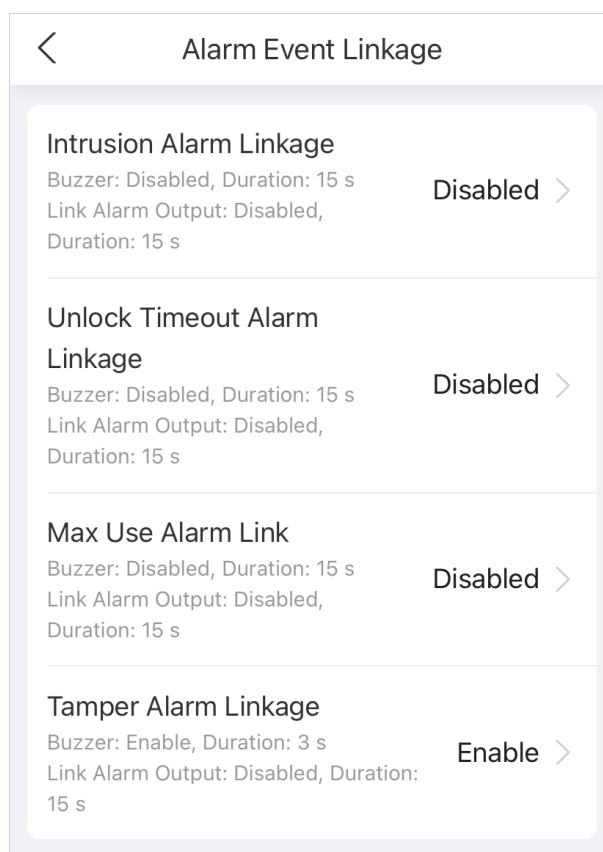
Parametro	Descrizione
Anti-passback	Gli utenti devono verificare la propria identità sia in entrata che in uscita; in caso contrario, scatterà un allarme. Questo sistema impedisce al titolare di una tessera di accesso di passarla a un'altra persona per entrare. Quando la funzione anti-passback è attiva, il titolare della tessera deve uscire dall'area protetta passando attraverso un lettore di uscita prima che il sistema possa consentirne un altro accesso. ● Se una persona entra dopo essere stata autorizzata ed esce senza autorizzazione, al successivo tentativo di accesso si attiverà un allarme e l'accesso verrà contemporaneamente negato. ● Se una persona entra senza autorizzazione ed esce dopo aver ottenuto l'autorizzazione, al successivo tentativo di accesso si attiverà un allarme e l'accesso verrà negato.  Se il dispositivo può connettersi a un solo lucchetto, la verifica sul dispositivo stesso corrisponde, per impostazione predefinita, alla direzione di ingresso, mentre la verifica sul lettore di schede esterno corrisponde alla direzione di uscita. È possibile modificare l'impostazione sulla piattaforma di gestione.
Rilevatore di porte	Con il rilevatore di porte collegato al dispositivo, l'allarme può attivarsi quando le porte vengono aperte o chiuse in modo anomalo. Il rilevatore di porte è disponibile in due tipologie: rilevatore NC e rilevatore NO. ● NC: Il sensore è in cortocircuito quando la porta o la finestra sono chiuse. ● NO: Si crea un circuito aperto quando la finestra o la porta sono effettivamente chiuse.
Allarme antintrusione	Se la porta viene aperta in modo anomalo, si attiverà un allarme antintrusione che durerà per un periodo di tempo predefinito.  Il rilevatore di porte e il sistema antintrusione devono essere attivati contemporaneamente.
Sblocca allarme timeout	Se la porta rimane sbloccata per un periodo superiore al tempo di timeout impostato, si attiverà l'allarme di timeout, che durerà per la durata definita.
Timeout di sblocco	 È necessario attivare contemporaneamente il rilevatore di porta e la funzione di apertura automatica della porta.
Allarme tentativi eccessivi	Se la password o la carta errata vengono utilizzate 5 volte di seguito entro 60 secondi, si attiverà l'allarme per utilizzo eccessivo di carta non valida, che durerà per un periodo di tempo predefinito.

4.6.4 Configurazione del collegamento degli eventi di allarme

Procedura

- Passo 1** Accedi alla pagina web.
- Passo 2** Selezionare **Di più** > **Controllo degli accessi** > **Collegamento evento di allarme**.

Figura 4-13 Collegamento degli eventi di allarme



- Passo 3** Tocca il collegamento per configurare il collegamento dell'allarme, quindi tocca **OK**.

Tabella 4-5 Collegamento degli eventi di allarme

Parametro	Descrizione
Collegamento del sistema di allarme antintrusione	Se la porta viene aperta in modo anomalo, si attiverà un allarme antintrusione. ● Buzzer: Il buzzer si attiva quando viene rilevato un allarme antintrusione. È possibile configurare la durata dell'allarme. ● Uscita allarme collegamento: il dispositivo di allarme esterno genera allarmi quando viene attivato l'allarme antintrusione. È possibile configurare la durata dell'allarme.

Parametro	Descrizione
Sblocca allarme timeout Collegamento	Se la porta rimane sbloccata per un periodo superiore al tempo di timeout impostato, si attiverà l'allarme di timeout, che durerà per la durata definita. ● Buzzer: Il buzzer suona quando viene attivato l'allarme di timeout di sblocco. La durata supporta Orario personalizzato E Fino a quando la porta non si chiude. ◇ Fino alla chiusura della porta: il suono dell'allarme si interrompe dopo la chiusura della porta. ◇ Tempo personalizzato: è possibile configurare la durata. ● Uscita allarme locale: il dispositivo di allarme esterno genera allarmi quando viene attivato l'allarme di timeout di sblocco. La durata supporta Orario personalizzato E Fino a quando la porta non si chiude. ◇ Fino alla chiusura della porta: l'allarme si disattiva dopo la chiusura della porta. ◇ Tempo personalizzato: è possibile configurare la durata.
Collegamento allarme utilizzo massimo	Se la password o la carta errata vengono utilizzate 5 volte di seguito entro 60 secondi, si attiverà l'allarme per utilizzo eccessivo di carta non valida, che durerà per un periodo di tempo predefinito. ● Buzzer: Il buzzer si attiva quando viene rilevato un consumo eccessivo. È possibile configurare la durata dell'allarme. ● Uscita allarme locale: il dispositivo di allarme esterno genera allarmi quando si attiva l'allarme di timeout di sblocco. È possibile configurare la durata dell'allarme.
Collegamento dell'allarme antimanomissione	L'allarme di manomissione si attiva quando qualcuno tenta di danneggiare fisicamente il dispositivo. ● Buzzer: Il buzzer si attiva quando scatta l'allarme antimanomissione. È possibile configurare la durata dell'allarme. ● Uscita allarme locale: il dispositivo di allarme esterno genera allarmi quando viene attivato l'allarme di manomissione. È possibile configurare la durata dell'allarme.

4.6.5 Configurazione del collegamento degli allarmi

Procedura

- Passo 1** Accedi alla pagina web.
- Passo 2** Selezionare **Di più > Controllo degli accessi > Impostazione collegamento allarme**
- Passo 3** Selezionare la zona per la quale configurare l'allarme.

Figura 4-14 Collegamento dell'allarme

Alarm-in Port 1

Name Zone1

Alarm Input Type NO >

Link Fire Safety Control ☐

Alarm-out Port ☐

Duration 30 s

Alarm Output Channel 1 >

Access Control Linkage ☐

Linkage Mode Weak Execution >

When the fire alarm signal disappears, the door will automatically return to the normal authentication mode.

Channel Type NC >

OK

Passo 4 Assegna un nome alla zona di allarme.

Passo 5 Abilitare **Collegamento al sistema di controllo antincendio** e selezionare un tipo per il dispositivo di ingresso allarme.

- NC: L'ingresso di allarme si trova in uno stato di circuito normalmente chiuso (NC) quando l'allarme non è scattato. L'apertura di un circuito normalmente chiuso fa scattare l'allarme.
- NO: Il dispositivo di ingresso allarme è in uno stato di circuito normalmente aperto (NA) quando l'allarme non è scattato. La chiusura del circuito fa scattare l'allarme.

Passo 6 Se si desidera collegare il controllo degli accessi quando viene attivato l'allarme antincendio, abilitare **Collegamento per il controllo degli accessi**.



Questa funzione ha effetto solo dopo **Collegamento Controllo antincendio** è abilitato.

Passo 7 Selezionare una modalità di collegamento.

- Esecuzione impeccabile: quando il segnale di allarme antincendio scompare, la porta mantiene lo stato attuale. Se lo si desidera, è possibile ripristinare manualmente lo stato precedente della porta.
- Esecuzione debole: quando il segnale di allarme antincendio scompare, la porta torna automaticamente al suo stato precedente.

Passo 8 Seleziona il tipo di canale.

- NO: La porta si apre automaticamente quando scatta l'allarme antincendio.
- NC: La porta si chiude automaticamente quando scatta l'allarme antincendio.

Passo 9

RubinettoOK.

4.6.6 Configurazione delle impostazioni della scheda**Procedura****Passo 1**

Accedi alla pagina web.

Passo 2Selezionare **Di più** > **Controllo degli accessi** > **Impostazioni della scheda**.

Figura 4-15 Impostazioni della scheda

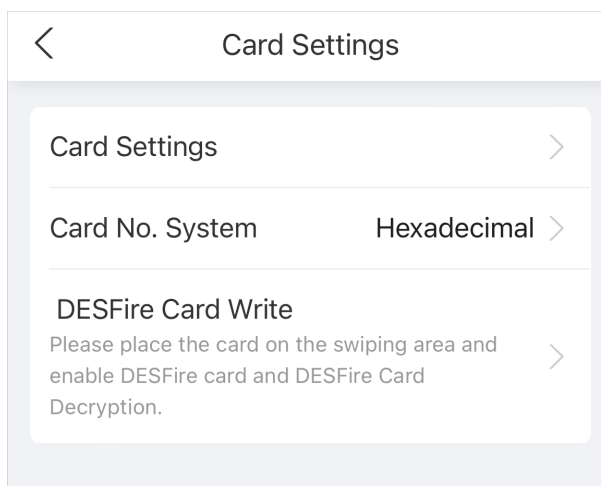
**Passo 3**Rubinetto**Impostazioni della scheda**, configura i parametri della scheda e poi tocca **Fare domanda a**.

Figura 4-16 Parametri della scheda

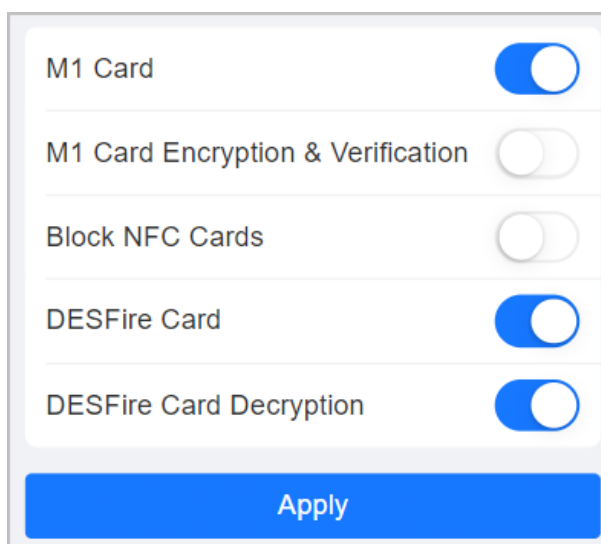


Tabella 4-6 Descrizione dei parametri della scheda

Parametro	Descrizione
Scheda M1	La scheda M1 può essere letta quando questa funzione è abilitata.  Questa funzione è disponibile solo su alcuni modelli.
Crittografia e verifica della carta M1	Solo la scheda IC crittografata può essere letta quando questa funzione è abilitata.  Assicurarsi Scheda M1 è abilitato.
Schede NFC a blocchi	Impedisci lo sblocco tramite scheda NFC duplicata dopo l'attivazione di questa funzione.  ● Questa funzione è disponibile solo sui modelli che supportano le schede IC. ● Assicurarsi Scheda M1 è abilitato. ● La funzione NFC è disponibile solo su alcuni modelli di telefono.
Carta Desfire	Il dispositivo è in grado di leggere il numero della carta Desfire quando questa funzione è abilitata.  ● Questa funzione è disponibile solo sui modelli che supportano le schede IC. ● Supporta solo il formato esadecimale.
Decrittazione della carta Desfire	Le informazioni contenute nella scheda Desfire possono essere lette quando Abilita la scheda Desfire e Decrittazione della carta Desfire vengono abilitati contemporaneamente.  ● Questa funzione è disponibile solo sui modelli che supportano le schede IC. ● Assicurati che la scheda Desfire sia abilitata.

Passo 4 Rubinetto **Sistema n. scheda**, seleziona il formato e poi fai clic **Fare domanda a**.

Quando si collega un lettore di carte Wiegand, selezionare il formato decimale o esadecimale per il numero della carta. Il sistema di numerazione delle carte è lo stesso sia per l'inserimento che per l'output del numero.

Passo 5 Rubinetto **Scrittura su scheda DESFire**.

Posiziona la carta sul lettore, inserisci il numero della carta e poi fai clic **Scrivere** e scrivere il numero della carta sulla carta.



- Le funzioni Desfire Card Function e Desfire Card Desfire Card Desfire Function devono essere abilitate.
- Supporta solo il formato esadecimale.
- Supporta fino a 8 caratteri.

4.7 Impostazioni di comunicazione

4.7.1 Configurazione di TCP/IP

È necessario configurare l'indirizzo IP del dispositivo per garantire che possa comunicare con altri dispositivi.

Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Selezionare **Di più** > **Impostazioni di comunicazione** > **TCP/IP**
- Passo 3 Configura i parametri e poi fai clic **Fare domanda a**.

Figura 4-17 TCP/IP

The screenshot displays the 'TCP/IP' configuration interface. At the top, there is a back arrow and the title 'TCP/IP'. Below this, the settings are organized into sections. The first section contains 'NIC' (set to 'NIC 1') and 'Mode' (set to 'Static'). The second section contains 'MAC Address' (represented by a greyed-out field). The third section contains 'IP Version' (set to 'IPv4'). Below these are five fields marked with a red asterisk, indicating they are required: 'IP Address', 'Subnet Mask', 'Default Gateway', 'Preferred DNS', and 'Alternate DNS'. Each of these fields is followed by a greyed-out input area. At the bottom of the form, there is an 'MTU' field set to '1500'. A large blue 'Apply' button is positioned at the very bottom of the screen.

Tabella 4-7 Descrizione di TCP/IP

Parametro	Descrizione
Modalità	● Statico: Inserire manualmente l'indirizzo IP, la subnet mask e il gateway. ● DHCP: Acronimo di Dynamic Host Configuration Protocol. Quando il DHCP è attivo, al dispositivo vengono assegnati automaticamente indirizzo IP, subnet mask e gateway.
Indirizzo MAC	Indirizzo MAC del dispositivo.
Versione IP	IPv4 o IPv6.
Indirizzo IP	Se imposti la modalità su Statico Configurare l'indirizzo IP, la subnet mask e il gateway.
Maschera di sottorete	
Gateway predefinito	
	 ● L'indirizzo IPv6 è rappresentato in formato esadecimale. ● La versione IPv6 non richiede l'impostazione delle maschere di sottorete. ● L'indirizzo IP e il gateway predefinito devono trovarsi nello stesso segmento di rete.
DNS preferito	Imposta l'indirizzo IP del server DNS preferito.
DNS alternativo	Imposta l'indirizzo IP del server DNS alternativo.
MTU	L'MTU (Maximum Transmission Unit) si riferisce alla dimensione massima dei dati che possono essere trasmessi in un singolo pacchetto di rete nelle reti di computer. Un valore MTU più elevato può migliorare l'efficienza della trasmissione di rete riducendo il numero di pacchetti e il relativo overhead di rete. Se un dispositivo lungo il percorso di rete non è in grado di gestire pacchetti di una determinata dimensione, ciò può causare la frammentazione dei pacchetti o errori di trasmissione. Nelle reti Ethernet, il valore MTU comune è di 1500 byte. Tuttavia, in alcuni casi, come ad esempio con PPPoE o VPN, potrebbero essere necessari valori MTU inferiori per soddisfare i requisiti di specifici protocolli o servizi di rete. Di seguito sono riportati i valori MTU consigliati a titolo di riferimento: ● 1500: Valore massimo per i pacchetti Ethernet, nonché valore predefinito. Si tratta di un'impostazione tipica per le connessioni di rete senza PPPoE e VPN, utilizzata in alcuni router, schede di rete e switch. ● 1492: Valore ottimale per PPPoE ● 1468: Valore ottimale per DHCP. ● 1450: Valore ottimale per VPN.

4.7.2 Configurazione del Wi-Fi

Procedura

- Passo 1** Accedi alla pagina web.
- Passo 2** Selezionare **Di più > Impostazioni di comunicazione > Wifi**
- Passo 3** Attiva il Wi-Fi.

Vengono visualizzate tutte le reti Wi-Fi disponibili.



- La funzione Wi-Fi è disponibile su alcuni modelli.
- Il Wi-Fi e il punto di accesso Wi-Fi non possono essere attivati contemporaneamente.

Passo 4 Fai clic su Wi-Fi e poi inserisci la password.

La connessione Wi-Fi è attiva.

Operazioni correlate

- DHCP: Selezionare il **DHCP** modalità e clic **Fare domanda a**, al dispositivo verrà assegnato automaticamente un indirizzo Wi-Fi.
- Statico: Seleziona il **Statico** modalità, immettere manualmente un indirizzo Wi-Fi e quindi fare clic **Fare domanda a** Il dispositivo si conatterà al Wi-Fi.

4.7.3 Configurazione dell'AP Wi-Fi



- La funzione Wi-Fi è disponibile su alcuni modelli.
- Il Wi-Fi e il punto di accesso Wi-Fi non possono essere attivati contemporaneamente.

Procedura

Passo 1 Accedi alla pagina web.

Passo 2 Selezionare **Di più** > **Impostazioni di comunicazione** > **Punto di accesso Wi-Fi**

Passo 3 . Abilita la funzione e poi fai clic **Fare domanda a**.

Figura 4-18 Punto di accesso Wi-Fi

<

Wi-Fi AP

Enable

☒

SSID

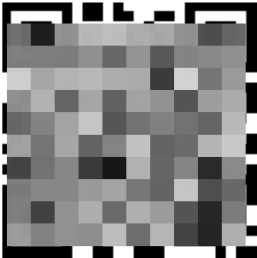
XXXXXXXXXXXX-XXXXXX

Security

None >

IP Address

192.168.1.1



Apply

4.7.4 Configurazione del servizio cloud

Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Selezionare **Di più>Impostazioni di comunicazione>Servizio cloud**
- Passo 3 Attiva la funzione del servizio cloud.
Il servizio cloud va online se P2P e PaaS sono online. Fai clic **Fare**
- Passo 4 **domanda a.**

4.7.5 Configurazione della registrazione automatica

Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Selezionare **Di più>Impostazioni di rete>Immatricolazione automatica.**
- Passo 3 Abilita la funzione di registrazione automatica, configura i parametri e poi fai clic **Fare domanda a.**

Figura 4-19 Registrazione automatica

Tabella 4-8 Descrizione della registrazione automatica

Parametro	Descrizione
Stato	Visualizza lo stato della connessione per la registrazione automatica.
Indirizzo del server	L'indirizzo IP o il nome di dominio del server.
Porta	La porta del server utilizzata per la registrazione automatica.
ID di registrazione	L'ID di registrazione (definito dall'utente) del dispositivo. Aggiungere il dispositivo alla gestione inserendo l'ID di registrazione sulla piattaforma.

4.7.6 Modalità di configurazione

Accedi alla pagina web e seleziona **Impostazioni di comunicazione** > **Impostazioni modalità**.

Modalità lettore di schede

Selezionare **Modalità COME Lettore di schede**. Il dispositivo funge da lettore di schede collegato esternamente a un controller di controllo accessi. Non esegue l'autenticazione, ma trasmette direttamente le informazioni di controllo accessi (come scheda, password, impronta digitale) al controller, che provvede quindi all'autenticazione e allo sblocco della porta.

Figura 4-20 Modalità lettore di schede

The screenshot shows the 'Card Reader' configuration page. At the top, the 'Mode' is set to 'Card Reader'. Below this, there are two main sections: 'RS-485 Settings' and 'Wiegand Settings'. The 'RS-485 Settings' section includes fields for 'Baud Rate' (9600), 'Data Bit' (8), 'Stop Bit' (1), and 'Parity Code' (None). The 'Wiegand Settings' section includes a 'Wiegand Output Type' set to 'Wiegand 34', a 'Pulse Width (μs)' set to 200, and a 'Pulse Interval (μs)' set to 1000. Both the pulse width and interval sections include a note: 'The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.' At the bottom of the page is a blue 'Apply' button.

Mode	Card Reader >
RS-485 Settings	
Baud Rate	9600 >
Data Bit	8 >
Stop Bit	1 >
Parity Code	None >
Wiegand Settings	
Wiegand Output Type	Wiegand 34 >
Pulse Width (μs)	200
The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.	
Pulse Interval (μs)	1000
The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.	
Apply	

Modalità controller di accesso

ImpostatoModalitàCOMEController di accesso.

Figura 4-21 Modalità controller di accesso

External Device

Access Controller >

Access controller: This device acts as a card reader, and connects to an access controller, which manages the opening of doors.

Baud Rate9600 >

Data Bit8 >

Stop Bit1 >

Parity CodeNone >

Output Data TypeCard Number >

Wiegand Settings

Wiegand Settings

Wiegand Input >

Card No. Inversion

Tabella 4-9 Descrizione di RS-485

Ora	Descrizione
Controller di accesso	Selezionare Controller di accesso quando il dispositivo funziona come lettore di schede e invia dati ad altri controller di accesso esterni per controllare l'accesso. Tipo di dati di output: ● Numero di tessera: visualizza i dati in base al numero di tessera quando l'utente striscia la tessera per sbloccare la porta; visualizza i dati in base al primo numero di tessera dell'utente quando vengono utilizzati altri metodi di sblocco. ● ID: Visualizza i dati in base all'ID utente.  ● In caso di autenticazione riuscita, le informazioni pertinenti vengono trasmesse al controller di accesso. In questo caso, il risultato dell'autenticazione visualizzato è quello del controller di accesso. ● In caso di errore di autenticazione, le informazioni pertinenti non vengono trasmesse al controller di accesso e il risultato visualizzato rimane "fallimento".
Lettore di schede	Il dispositivo è collegato esternamente a un lettore di schede e trasmette le informazioni della scheda di controllo accessi a un controller di accesso o a una piattaforma di gestione.
Lettore di schede (OSDP)	Il dispositivo è collegato esternamente a un lettore di schede OSDP e trasmette le informazioni della scheda di controllo accessi a un controller di accesso o a una piattaforma di gestione.
Modulo di sicurezza per porte	Il pulsante di uscita, la serratura e il collegamento antincendio non funzionano dopo l'attivazione del modulo di sicurezza. ● Supporta l'autenticazione tramite riconoscimento facciale, tessera, impronta digitale, password e altri metodi per controllare il modulo di sicurezza della porta ai fini dello sblocco. ● Supporta lo sblocco tramite un lettore di schede RS-485 collegato esternamente o un pulsante di apertura a pressione collegato al modulo di sicurezza per il controllo della porta.  Lo sblocco a distanza della serratura esterna tramite il modulo di sicurezza della porta non è supportato.
Modulo di estensione serratura	Quando il controller di accesso è collegato al modulo di estensione della serratura esterna, se si seleziona Modulo di estensione serratura la serratura locale viene sbloccata dopo aver verificato l'identità sul dispositivo locale, mentre la serratura dell'estensione viene sbloccata dopo aver verificato l'identità sul lettore di schede esterno. Dopo aver selezionato Modulo di estensione serratura, è possibile selezionare il canale 2 su Parametri di controllo degli accessi e Allarme pagina sulla pagina web del Responsabile degli accessi.

Tabella 4-10 Descrizione di Wiegand

Parametro		Descrizione
Impostazioni di Wiegand		● Quando si collega un dispositivo lettore di schede esterno, selezionare Input di Wiegand. ● Quando il dispositivo funziona come lettore di schede e devi collegarlo a un altro controller di accesso, seleziona Configurazione di output di Wiegand.
Wiegand Ingresso	Numero di carta Inversione	Se la sequenza del numero di carta ottenuta tramite l'input Wiegand non corrisponde alla sequenza effettiva del numero di carta quando si interagisce con dispositivi di terze parti, abilitare questa funzione.
Wiegand Produzione	Wiegand Tipo di output	La lunghezza in bit dei numeri di carta o ID che il dispositivo è in grado di riconoscere e riprodurre. ● Wiegand 26: Legge 3 byte o 6 cifre. ● Wiegand 34: Legge 4 byte o 8 cifre. ● Wiegand 66: Legge 8 byte o 16 cifre.
	Larghezza dell'impulso	Configurare la larghezza e l'intervallo dell'impulso per l'uscita Wiegand.
	Intervallo di impulso	
	Dati di output Tipo	Selezionare un formato Wiegand per leggere i numeri di carta o i numeri di identificazione. ● ID utente: visualizza i dati in base all'ID utente. ● Carta: visualizza i dati in base al primo numero di carta dell'utente.
	Wiegand Formato	Quando Tipo di dati di output è impostato come ID È possibile selezionare il formato di output decimale o esadecimale.

4.8 Visualizzazione dei registri

Visualizza i registri, come i registri di sistema, i registri di sblocco e i registri degli allarmi.

4.8.1 Registri di sistema

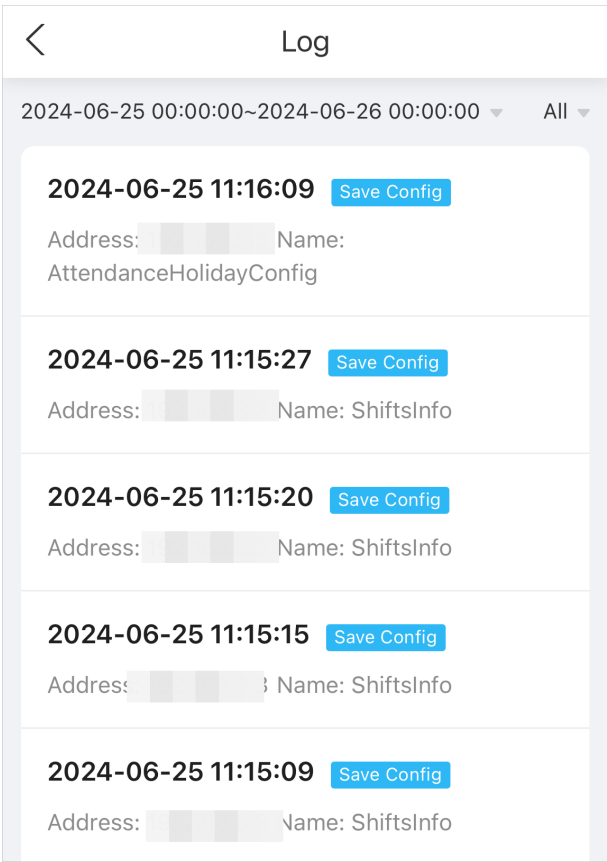
Visualizza e cerca i registri di sistema.

Procedura

Passo 1 Accedi alla pagina web. Seleziona **Di più**>

Passo 2 **Tronco d'albero**>**Tronco d'albero**.

Figura 4-22 Log



4.8.2 Sblocca i record

Cerca i record di sblocco.

Procedura

- Passo 1 Accedi alla pagina web.
- Passo 2 Selezionare**Di più>Tronco d'albero>Sblocca i record**
- Passo 3 Fai clic sul record per visualizzarne i dettagli.

4.8.3 Registri degli allarmi

Visualizza i registri degli allarmi.

Procedura

- Passo 1 Accedi alla pagina web. Seleziona**Di più>**
- Passo 2 **Tronco d'albero>Registro allarmi.**

5 Configurazione Smart PSS Lite

Questa sezione illustra come gestire e configurare il dispositivo tramite Smart PSS Lite. Per maggiori dettagli, consultare il manuale utente di Smart PSS Lite.

5.1 Installazione

Contatta l'assistenza tecnica o visita il sito web ufficiale per ottenere SmartPSS Lite. Se ottieni il pacchetto software di SmartPSS Lite, installalo ed esegilo seguendo le istruzioni presenti sulla pagina.

5.2 Inizializzazione

Inizializza SmartPSS Lite al primo accesso, impostando una password per l'accesso e domande di sicurezza per il ripristino della password.

Procedura

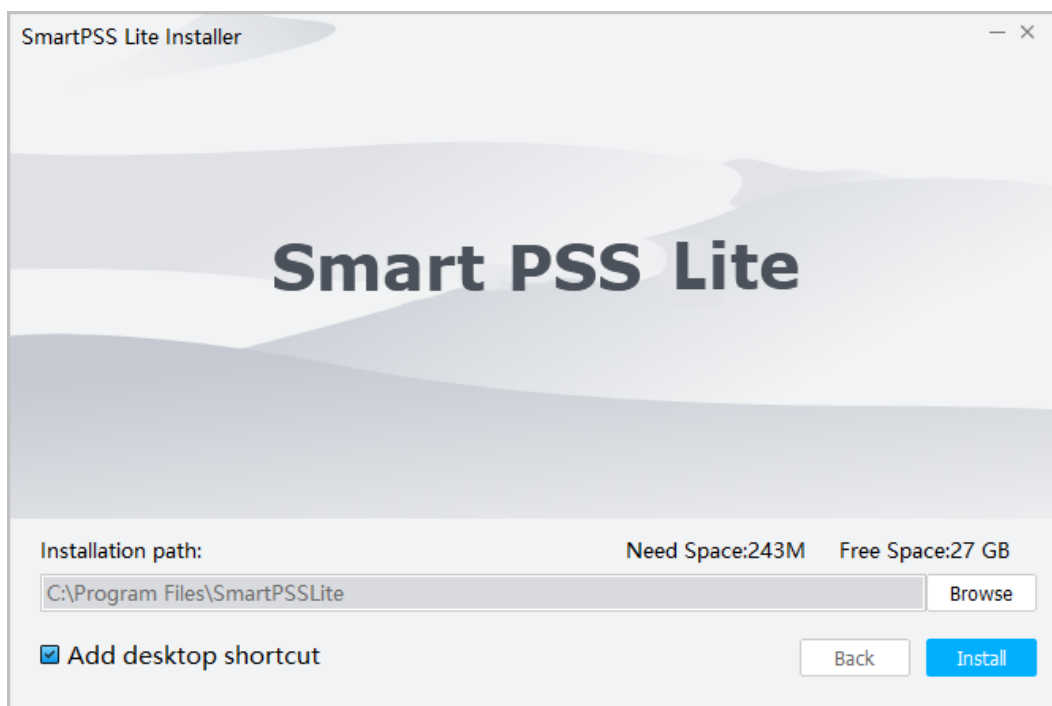
- Passo 1 Fare doppio clic su SmartPSSLite.exe.
- Passo 2 Seleziona la lingua dall'elenco a discesa, seleziona **Ho letto e accetto il contratto di licenza del software.**, e poi fai clic **Prossimo**.

Figura 5-1 Seleziona la lingua



- Passo 3 Clic **Sfoglia** per selezionare il percorso di installazione, quindi fare clic **Installare**.

Figura 5-2 Selezionare il percorso di installazione

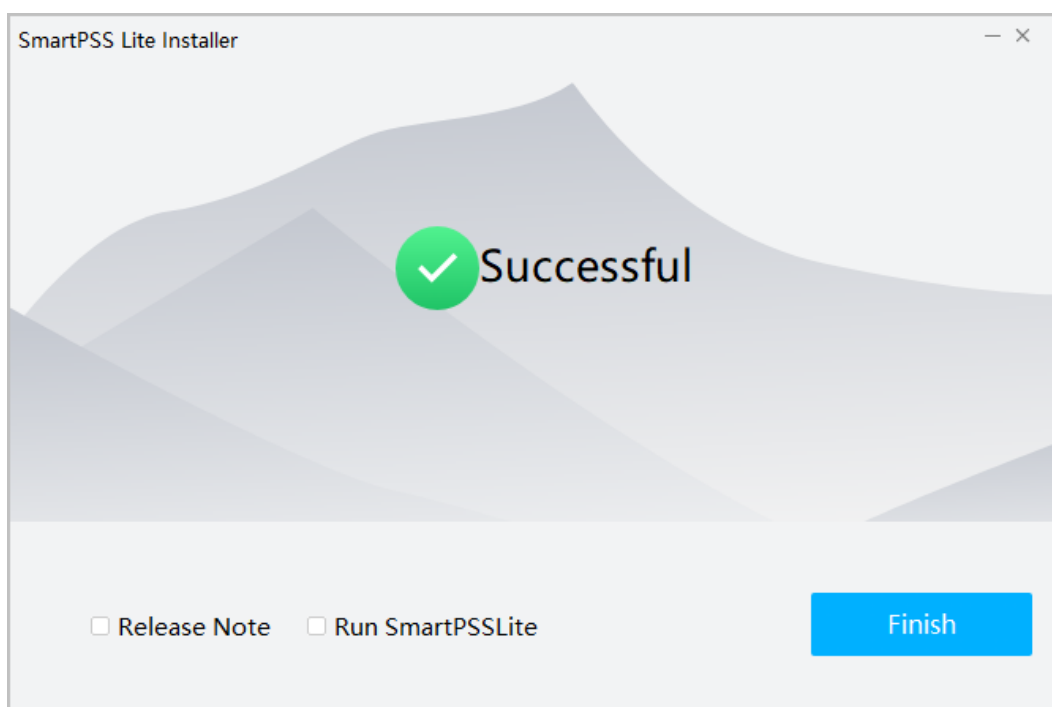


Passo 4 Clic**Fine** per completare l'installazione.



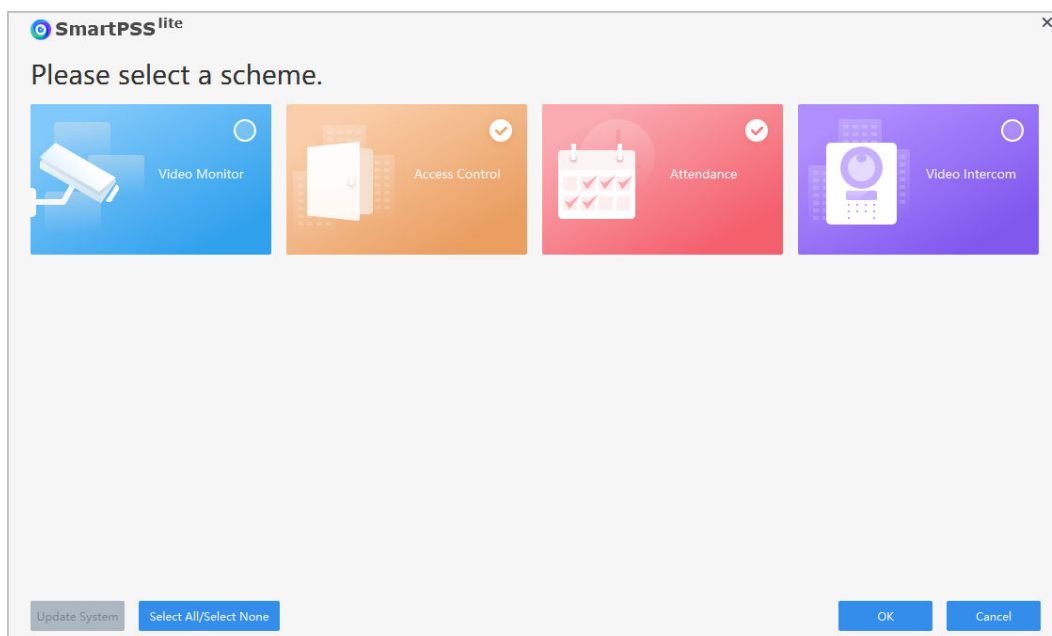
Selezionare **Esegui SmartPSSlite** per avviare SmartPSS Lite.

Figura 5-3 Installazione completata



Passo 5 Seleziona le scene dell'applicazione che desideri aggiungere, quindi fai clic **OK**.

Figura 5-4 Selezione di scenari applicativi



Passo 6 Clic**Accetto e continuo** per concordare **Contratto di licenza software** **Informativa sulla privacy del prodotto**.

Passo 7 Imposta la password su **Inizializzazione** pagina e quindi fai clic **Prossimo**.

Figura 5-5 Imposta password

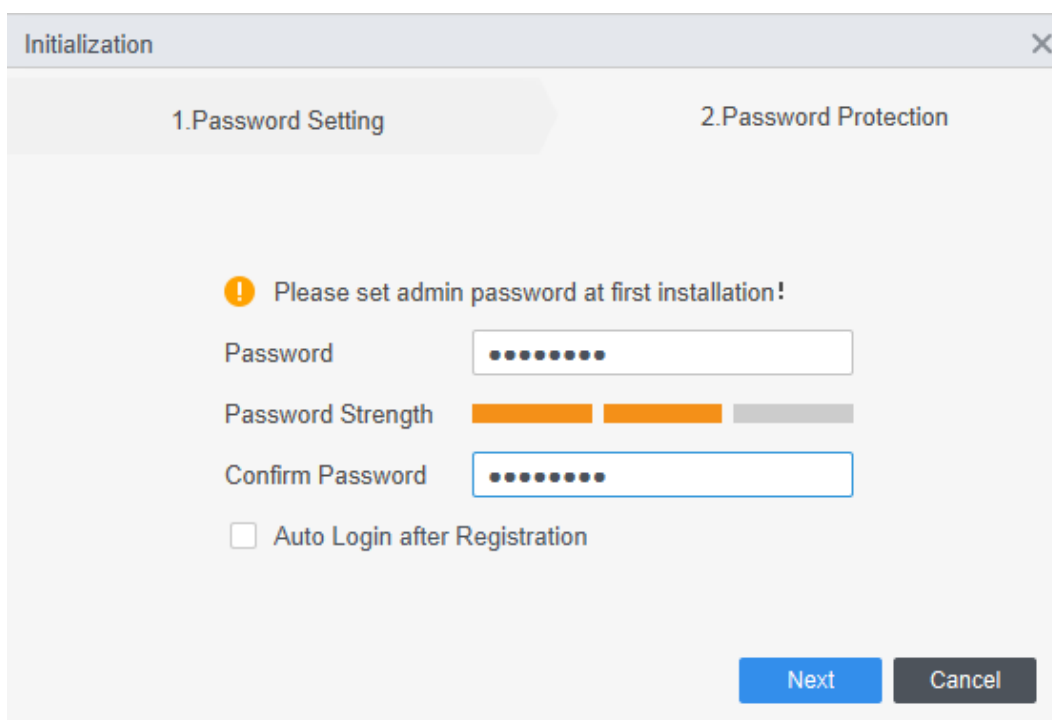


Tabella 5-1 Parametri di inizializzazione

Parametro	Descrizione
Password	La password deve essere composta da 8 a 32 caratteri non vuoti e contenere almeno due tipi di caratteri tra maiuscole, minuscole, numeri e caratteri speciali (esclusi ' " ; &).
Forza della password	Mostra l'efficacia di una password contro tentativi di indovinare o attacchi di forza bruta. Il verde indica che la password è sufficientemente sicura, mentre il rosso indica che è meno sicura. Imposta una password con un livello di sicurezza elevato in base alle indicazioni sulla robustezza della password.
Conferma password	Inserisci nuovamente la password per confermarla.
Accesso automatico dopo la registrazione	Abilitare Accesso automatico dopo la registrazione in modo che SmartPSS Lite effettui l'accesso automaticamente dopo l'inizializzazione; altrimenti viene visualizzata la pagina di accesso.

Passo 8 Imposta le domande di sicurezza, quindi fai clic **Fine**.

Figura 5-6 Imposta le domande di sicurezza

Initialization [X]

1.Password Setting 2.Password Protection

! Please set security questions!

Question 1: What is your favorite children's book? [v]

Answer: []

Question 2: What was the first name of your first boss? [v]

Answer: []

Question 3: What is the name of your favorite fruit? [v]

Answer: []

Finish

5.3 Aggiunta di dispositivi

Sono disponibili diversi metodi per aggiungere dispositivi.

- Ricerca automatica
- Aggiunta manuale
- Importazione in lotti

5.3.1 Aggiunta del dispositivo tramite ricerca

È possibile aggiungere più dispositivi cercandoli nel segmento di rete corrente o in altri segmenti di rete.

Informazioni di base



Si consiglia di aggiungere i dispositivi tramite la funzione di ricerca quando si desidera aggiungere più dispositivi che si trovano sullo stesso segmento di rete, oppure quando si desidera aggiungere dispositivi con un segmento di rete noto ma non si conosce l'indirizzo IP esatto dei dispositivi.

Procedura

Passo 1 Nella pagina iniziale, fai clic **Dispositivi**

Passo 2 Seleziona un metodo di ricerca.

- **Ricerca automatica:** inserisci il nome utente e la password del dispositivo. Il sistema cercherà automaticamente i dispositivi presenti sulla stessa rete del tuo computer.
- **Segmento di rete del dispositivo:** Inserire il nome utente e la password del dispositivo, quindi definire l'indirizzo IP iniziale e l'indirizzo IP finale. Il sistema cercherà automaticamente i dispositivi all'interno di questo intervallo di indirizzi IP.

Passo 3 **ClicRicerca automatica.**

Passo 4 Inserisci un intervallo IP, quindi fai clic **Ricerca**.

Il sistema cerca automaticamente i dispositivi in questo intervallo IP. Puoi anche fare clic **Ricerca automatica** per cercare automaticamente i dispositivi sulla stessa rete a cui è connesso il computer.

Figura 5-7 Ricerca di dispositivi

Auto Search

☒ Auto Search
 Device Network Segm... 10

☐ Change IP
 Initialize
 Found Device:

☐ No.	IP ▲	Device Type	MAC Address	Port	Initialization Status
------------------------------	------	-------------	-------------	------	-----------------------

Passo 5 Seleziona i dispositivi e poi fai clic **Aggiungere**.

Passo 6 Inserisci il nome utente e la password di accesso dei dispositivi selezionati, quindi fai clic **OK**

Passo 7 Inserisci il nome utente e la password di accesso, quindi fai clic su **OK**.

I dispositivi verranno aggiunti alla piattaforma.

Figura 5-8 Dispositivi aggiunti

Total Devices										
☐	No.	Name	IP	Device Type	Device Model	Port	Number of Chann	Online Status	SN	Operation
☐	1	AC		Door Station		37777	2/0/10/2	● Online		   
☐	2	AC2		Access Controller		37777	2/0/0/0	● Offline		   

-  : Modifica le informazioni del dispositivo.
-  : Va al **Configurazione del dispositivo** modulo nella piattaforma.
-  : Consente di accedere alla pagina web del dispositivo.
-  : Disconnettiti dal dispositivo e lo stato del dispositivo diventerà **Offline**.
-  : Accedi al dispositivo e lo stato del dispositivo diventerà **Online**.
-  : Elimina il dispositivo.

Operazioni correlate

- Cambiare l'indirizzo IP uno per uno: selezionare un dispositivo e quindi fare clic su **Cambia IP** per modificare l'indirizzo IP del dispositivo.
- Modifica IP in blocco: seleziona più dispositivi e poi fai clic **Modifica** per cambiare il loro indirizzo IP.



Inserisci l'indirizzo IP iniziale e il sistema assegnerà automaticamente gli indirizzi IP ai dispositivi incrementandoli di uno in base all'indirizzo IP iniziale. Ad esempio, se l'indirizzo IP iniziale è 10.XX.XXX.52, gli indirizzi IP successivi dei dispositivi saranno 10.XX.XXX.53, 10.XX.XXX.54 e così via.

- Inizializza i dispositivi: fai clic **Inizializzare** per inizializzare i dispositivi.



È supportata l'attivazione solo dei dispositivi che si trovano nella stessa rete del computer.

5.3.2 Aggiunta dei dispositivi uno alla volta

Se conosci già l'indirizzo IP di un dispositivo, puoi aggiungerlo manualmente alla piattaforma.

Procedura

- Passo 1** Nella pagina iniziale, fai clic **Dispositivi**.
- Passo 2** Clic **Aggiungere** e quindi inserire le informazioni del dispositivo.

Figura 5-9 Aggiungi dispositivi

Add Device

Device Name:

*

Add Mode:

IP/Domain Name

IP/Domain Name:

*

Port No.:

* 37777

Username:

*

Password:

*

Add and Continue

Add

Cancel

Tabella 5-2 Parametri di aggiunta IP

Parametro	Descrizione
Nome del dispositivo	Il nome del dispositivo.
Aggiungi modalità	● IP/Nome di dominio: Aggiungi dispositivi tramite indirizzo IP. ● SN (Disponibile sui dispositivi che supportano P2P): Aggiungi dispositivi tramite il loro numero di serie.
Indirizzo IP/Nome di dominio	Inserisci l'indirizzo IP o il nome di dominio del dispositivo.
Numero di porta	Inserisci il numero di porta (80 per impostazione predefinita).
Nome utente	Inserisci il nome utente e la password del dispositivo.
Password	

Passo 3 Clic**Aggiungere**.

Puoi anche cliccare**Aggiungi e continua**per aggiungere altri dispositivi.

5.3.3 Importazione del dispositivo in batch

È possibile esportare le informazioni sui dispositivi e quindi importarle in un'altra piattaforma per aggiungerli in blocco. Si consiglia di aggiungere i dispositivi importandoli quando non si trovano sullo stesso segmento di rete.

Prerequisiti

È stato esportato un file .xml contenente le informazioni sul dispositivo. Per maggiori dettagli, consultare il relativo manuale utente.

Procedura

- Passo 1** Nella pagina iniziale, fai clic **Dispositivi**.
- Passo 2** Clic **Importare** per importare il file nella piattaforma.



I dispositivi verranno autenticati automaticamente dopo l'aggiunta.

5.4 Gestione degli utenti

Aggiungi utenti, assegna loro delle schede e configura i relativi permessi di accesso.

5.4.1 Impostazione del tipo di scheda

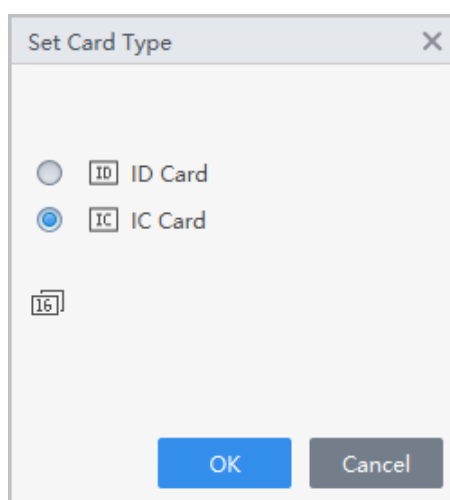
Selezionare **Persona > Gestione del personale**, poi **Tipo di carta**.

Prima di emettere la carta, impostare innanzitutto il tipo di carta. Ad esempio, se la carta da emettere è una carta d'identità, selezionare "Carta d'identità" come tipo.



Il sistema utilizza di default il numero di carta in formato esadecimale. Fare clic su  per convertirlo in carta decimale "Numero".

Figura 5-10 Tipo di carta Set



5.4.2 Configurazione del tipo di scheda

Imposta il tipo di carta prima di assegnarle agli utenti. Ad esempio, se la carta assegnata è una carta d'identità, imposta il tipo di carta su "Carta d'identità".

Procedura

- Passo 1** Accedi a Smart PSS Lite.
- Passo 2** Clic **Soluzione di accesso > Responsabile del personale > Utente**. Sul **Tipo di emissione della cartae** quindi selezionare un tipo di carta.
- Passo 3**



Assicurati che il tipo di carta corrisponda a quello della carta effettivamente assegnata; in caso contrario, il numero della carta non potrà essere letto.

Passo 4

Clic **OK**.

5.4.3 Aggiunta di utenti

5.4.3.1 Aggiunta del personale uno alla volta

Procedura

Passo 1

Selezionare **Persona** > **Gestione del personale** e poi fai clic **Aggiungere** **Inserire**

Passo 2

le informazioni di base della persona.

1. Seleziona **Informazioni di base**.

2. Aggiungere le informazioni di base del personale.

3. Scatta una foto o carica un'immagine, quindi fai clic **Fine**.

4. Configurare i metodi di verifica dell'identità.

- Imposta password

Clic **Aggiungere** Per aggiungere la password. Per i controller di accesso di seconda generazione, impostare le password personali; per gli altri dispositivi, impostare le password delle tessere. Le nuove password devono essere composte da 6 a 8 cifre.

- Scheda di configurazione

a. Fare clic  per selezionare **Dispositivo** o **Emittente della carta** come lettore di schede.

b. Aggiungi carta.

c. Dopo averla aggiunta, è possibile selezionare la carta come carta principale o carta di emergenza, oppure sostituirla con una nuova, o ancora eliminarla.

d. Fare clic  per visualizzare il codice QR della carta.



Solo i numeri di carta a 8 cifre in formato esadecimale possono visualizzare il codice QR della carta.

- Configura l'impronta digitale

a. Fare clic  per selezionare **Dispositivo** o **Scanner di impronte digitali** in qualità di addetto alla raccolta delle impronte digitali.

b. Aggiungi impronta digitale. Seleziona **Aggiungere** > **Aggiungi impronta digitale** e quindi premere il dito sullo scanner per tre volte consecutive.

- Configura i codici funzione

a. Fare clic  , quindi selezionare un dispositivo.

b. Fare clic **Estrarre** e quindi il dispositivo estrarrà i tratti del viso.

Figura 5-11 Aggiungere informazioni di base

Add User

Basic Info
More Info

Person ID: *

Name: *

Department: ult Company\HumanResource

Person Type: Normal User

Effective Time: 2023/12/29 0:00:00

2023/12/29 23:59:59

3654 Day

Times Used: Unlimited

Profile Picture

Take Snapshot
Upload Picture

Image size: 0-100 KB

Face1

Take Snapshot
Upload Picture

Image size: 0-100 KB

Face2

Take Snapshot
Upload Picture

Image size: 0-100 KB

Password Add ! For the second-generation access control device, it is the person password. Otherwise it is the card password.

Card Add ! The card number must be added if non-2nd generation access controller is used.

Fingerprint

+ Add
Delete

	Fingerprint Name	Operation
☐		

Add More
Complete
Cancel

Passo 3 Clic**Ulteriori informazioni** scheda per aggiungere informazioni estese sul personale, quindi fai clic**Completare**.

Figura 5-12 Aggiungi ulteriori informazioni

Passo 4 Clic **Completare**.

Dopo aver completato l'aggiunta, puoi cliccare sulla  per modificare le informazioni o aggiungere dettagli all'elenco persona.

Operazioni correlate

- Clic  per modificare le informazioni o aggiungere dettagli all'elenco del personale.
- Clic  eliminare tutte le informazioni della persona.
- Clic  per bloccare la scheda, dopodiché la scheda non potrà essere utilizzata normalmente.

5.4.3.2 Aggiunta di personale a lotti

Procedura

- Passo 1 Selezionare **Persona** > **Gestione del personale** e poi fai clic **Aggiungi batch**. Selezionare il
- Passo 2 tipo di dispositivo, impostare il numero iniziale e il numero di schede.
- Passo 3 Imposta il reparto, il periodo di validità e la data di scadenza della carta. Fai clic
- Passo 4 **Leggere la carta n..**
- Passo 5 Posizionare le carte sull'emittente o sul lettore di carte.
- Il numero della carta verrà letto automaticamente o inserito automaticamente. Fare
- Passo 6 clic **OK**.

Figura 5-13 Aggiungere il personale a lotti

Batch Add

Device: Card Issuer

Start No.: 5

Quantity: 10

Department: Dropdown list

Validity Time: 2022/11/24 0:00:00

Expiration Time: 2032/11/24 23:59:59

Read C...

Issue Card

ID	Card No.
----	----------

OK Cancel

5.4.4 Assegnazione delle autorizzazioni di accesso

La procedura per configurare le autorizzazioni per reparto e per personale è simile, e qui viene utilizzato il reparto come esempio.

Procedura

Passo 1 Selezionare **Configurazione del controllo degli accessi > Impostazioni delle autorizzazioni**

Passo 2 Fai clic per aggiungere una regola di autorizzazione.

Figura 5-14 Assegnazione delle regole di autorizzazione

Passo 3 Inserisci il nome della regola di autorizzazione, seleziona il piano orario e i metodi di sblocco. Nel

Passo 4 **Informazioni sulla persona**area, clicca **Aggiungere** per selezionare il personale, quindi fare clic **OK**.

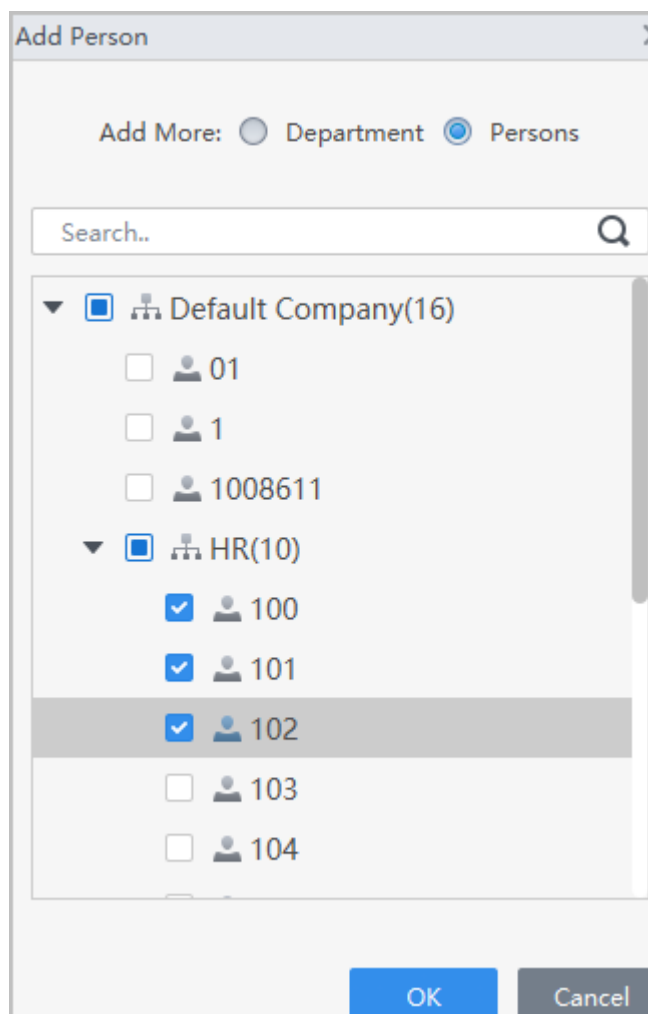
È possibile selezionare il personale a livello di reparto o i singoli utenti.

- Dipartimento: A tutto il personale del dipartimento verranno assegnati i permessi di accesso.
- Utente: Solo agli utenti selezionati verranno assegnate le autorizzazioni di accesso.



Quando si desidera assegnare le autorizzazioni a una nuova persona o modificare le autorizzazioni di accesso per una persona esistente, è sufficiente aggiungere l'utente a un reparto esistente o collegarlo a un ruolo esistente; in questo modo, le autorizzazioni di accesso impostate per il reparto o il ruolo verranno assegnate automaticamente.

Figura 5-15 Aggiungi utenti



Add Person

Add More: ☐ Department ☒ Persons

Search..

▼ ☒  Default Company(16)

- ☐  01
- ☐  1
- ☐  1008611
- ▼ ☒  HR(10)
 - ☒  100
 - ☒  101
 - ☒  102
 - ☐  103
 - ☐  104

OK Cancel

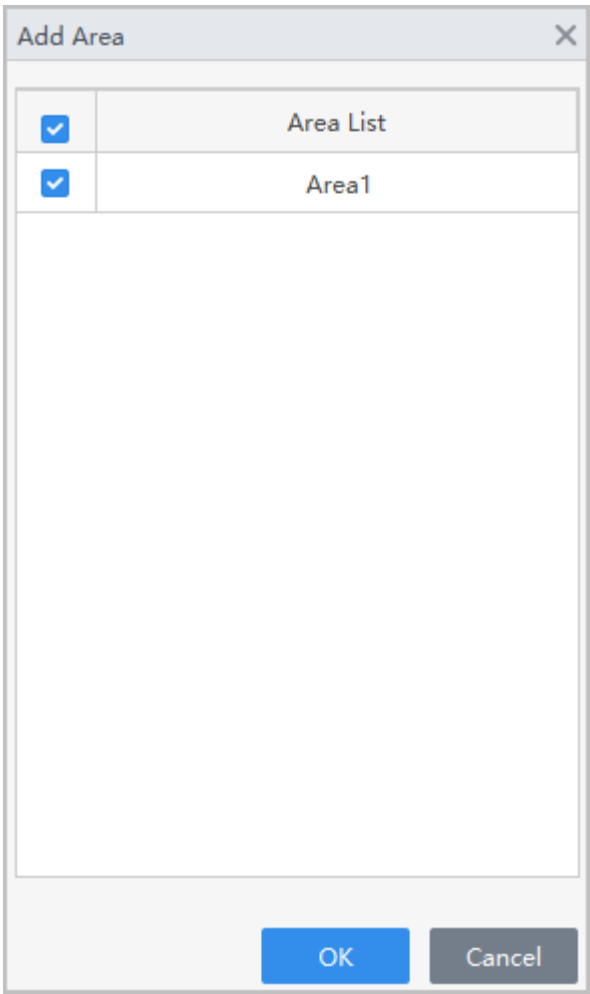


Puoi cliccare  per creare nuove aree di autorizzazione. Per informazioni dettagliate sulla creazione di aree di autorizzazione, consultare il relativo manuale utente.

Passo 5

Nel**Informazioni sulla zona**, clic**Aggiungere** per selezionare un'area e quindi fare clic**OK**.

Figura 5-16 Aggiungi area



Passo 6 **ClicOK.**

Passo 7 Se l'autorizzazione non è riuscita, fai clic  nell'elenco per visualizzare la possibile causa.

Figura 5-17 Stato di avanzamento dell'autorizzazione

Permission Group	Device Name	Progress	Status	Result of Issuing	Operation
Permission Group3		1/1	Finished issuing	Successful: 1, Failed: 0	

5.4.5 Assegnazione delle autorizzazioni di presenza

La procedura per configurare le autorizzazioni per reparto e per personale è simile, e qui viene utilizzato il reparto come esempio.

Procedura

Passo 1 Selezionare**Configurazione del controllo degli accessi>Impostazioni delle autorizzazioni**

Passo 2 Fai clic per  aggiungere una regola di autorizzazione.

Figura 5-18 Assegnazione delle regole di autorizzazione

Add Permission Rule

1 You can only create up to 128 permission rules.

2

Name: Permission Rule1 Remarks:

Weekly Plan: Full-day Time Template Holiday Plan: Disabled

Select Data to be Sent: ☒ Card ☒ Fingerprint ☒ Password ☒ Face

Person Info Area Info

3 4

5

OK Cancel

Passo 3 Inserisci il nome della regola di autorizzazione, seleziona il piano orario e i metodi di sblocco. Nel

Passo 4 **Informazioni sulla persona**area, clicca **Aggiungere** per selezionare il personale, quindi fare clic **OK**.

È possibile selezionare il personale a livello di reparto o i singoli utenti.

- Dipartimento: A tutto il personale del dipartimento verranno assegnati i permessi di accesso.
- Utente: Solo agli utenti selezionati verranno assegnate le autorizzazioni di accesso.



Quando si desidera assegnare le autorizzazioni a una nuova persona o modificare le autorizzazioni di accesso per una persona esistente, è sufficiente aggiungere l'utente a un reparto esistente o collegarlo a un ruolo esistente; in questo modo, le autorizzazioni di accesso impostate per il reparto o il ruolo verranno assegnate automaticamente.

Figura 5-19 Aggiungi utenti

Add Person

Add More: ☐ Department ☒ Persons

Search..

▼ ☒ Default Company(16)

☐ 01

☐ 1

☐ 1008611

▼ ☒ HR(10)

☒ 100

☒ 101

☒ 102

☐ 103

☐ 104

OK Cancel



Puoi cliccare per creare nuove aree di autorizzazione. Per informazioni dettagliate sulla creazione di aree di autorizzazione, consultare il relativo manuale utente.

Passo 5

Nel **Informazioni sulla zona**, clic **Aggiungere** per selezionare un'area e quindi fare clic **OK**.

Figura 5-20 Aggiungi area

Add Area

Area List

Area1

OK

Cancel

Passo 6 **ClicOK.**

Passo 7 Se l'autorizzazione non è riuscita, fai clic  nell'elenco per visualizzare la possibile causa.

Figura 5-21 Stato di avanzamento dell'autorizzazione

Permission Group	Device Name	Progress	Status	Result of Issuing	Operation
Permission Group3		1/1	Finished issuing	Successful: 1, Failed: 0	

5.5 Monitoraggio del controllo degli accessi

Procedura

Passo 1 Clic**Monitoraggio del controllo degli accessi**sulla pagina iniziale.

Passo 2 Gestisci la porta.

Figura 5-22 Monitorare la porta

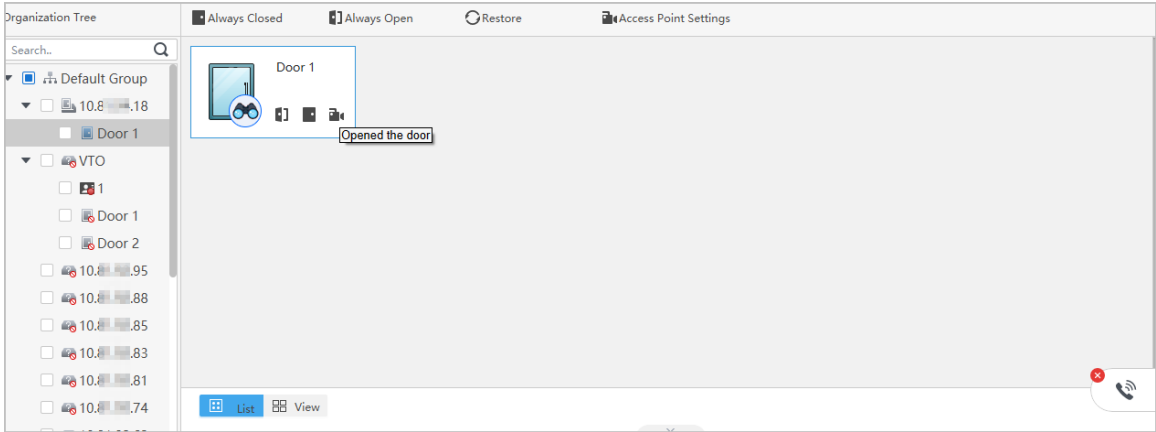


Tabella 5-3 Descrizione dei parametri

Funzione	Descrizione
Controllo remoto della porta	Controllo remoto della porta. ● Metodo 1: Fai clic con il pulsante destro del mouse su una porta e seleziona Aprire o Vicino. ● Metodo 2: Fare clic  per aprire o chiudere la porta.
	Visualizza il video ripreso dalla telecamera del controller di accesso o dalla telecamera esterna collegata.  Se non riesci a visualizzare il video in tempo reale, significa che il dispositivo di controllo accessi non è dotato di telecamera e non è collegato a una telecamera esterna. Configura una telecamera esterna per il controller di accesso. Per maggiori dettagli, consulta il relativo manuale utente. Se desideri visualizzare più video in diretta contemporaneamente, fai clic  e quindi trascinare il dispositivo di controllo accessi nell'organizzazione. Aprire la struttura ad albero in Windows oppure fare doppio clic sul dispositivo di controllo degli accessi nella struttura ad albero dell'organizzazione.
Sempre aperto	Dopo aver impostato "sempre aperto" o "sempre chiuso", la porta rimane aperta o chiusa in modo permanente e non può essere controllata manualmente. Se si desidera controllare nuovamente la porta manualmente, fare clic su Normale per ripristinare lo stato della porta.
Sempre chiuso	
Ripristinare	
Impostazioni del punto di accesso	Configura i dispositivi (NVR, IPC, IVSS e altri) che supportano il riconoscimento dei bersagli come punti di controllo degli accessi. Dopo la configurazione, i registri di sblocco delle porte verranno caricati sulla piattaforma.

Passo 3 Fare clic con il pulsante destro del mouse su un dispositivo di controllo accessi per gestirlo.

Figura 5-23 Gestire il dispositivo

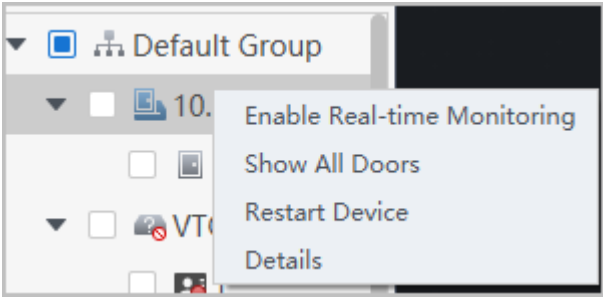


Tabella 5-4 Descrizione dei parametri

Parametro	Descrizione
Abilita il monitoraggio in tempo reale	Avvia il monitoraggio degli eventi in tempo reale.
Mostra tutte le porte	Mostra tutte le porte collegate al dispositivo di controllo accessi.
Riavvia il dispositivo	Riavviare il dispositivo di controllo accessi.
Dettagli	Visualizza le informazioni sul dispositivo, come la versione e altro ancora.

Passo 4 Visualizza lo stato della porta su **Informazioni sull'evento** elenco. Per i dettagli, consultare il relativo manuale utente.

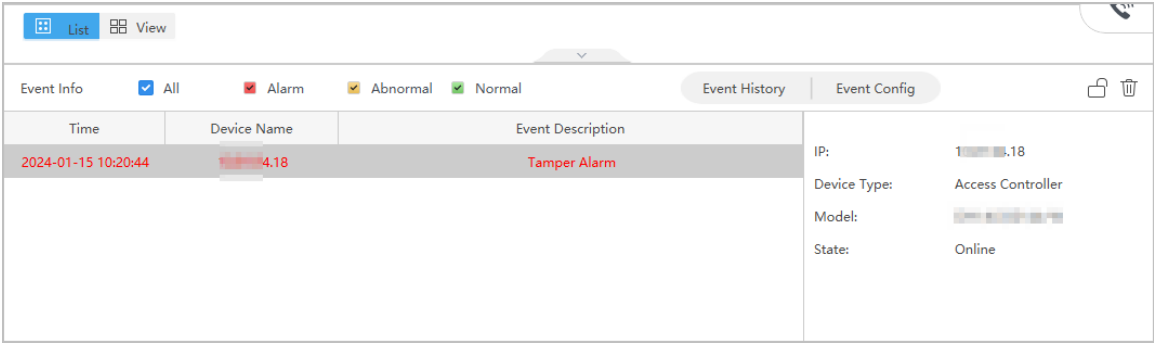
Operazioni correlate

Clic  per aprire il **Informazioni sull'evento** lista.



- Visualizza le informazioni sul controllo degli accessi: puoi visualizzare le informazioni di accesso in tempo reale nel **Informazioni sull'evento** elenco. Le informazioni verranno cancellate al riavvio della piattaforma.
- Filtra gli eventi: Seleziona il tipo di evento in **Informazioni sull'evento**, e l'elenco degli eventi visualizza gli eventi dei tipi selezionati. Ad esempio, seleziona **Allarme** e l'elenco degli eventi visualizza solo gli eventi di allarme.
- Blocca o sblocca l'elenco degli eventi: fai clic sul lato destro di **Informazioni sull'evento** per bloccare o sbloccare l'elenco degli eventi, dopodiché non sarà possibile visualizzare gli eventi in tempo reale.
- Elimina gli eventi: fai clic sul lato destro di **Informazioni sull'evento** per cancellare tutti gli eventi dall'elenco degli eventi.
- Clic **Storia dell'evento** per saltare al **Registro di controllo degli accessi** pagina e clicca **Configurazione evento** per saltare al **Configurazione evento** pagina.

Figura 5-24 Informazioni sull'evento



Appendice 1 Punti importanti delle impronte digitali

Istruzioni per la registrazione

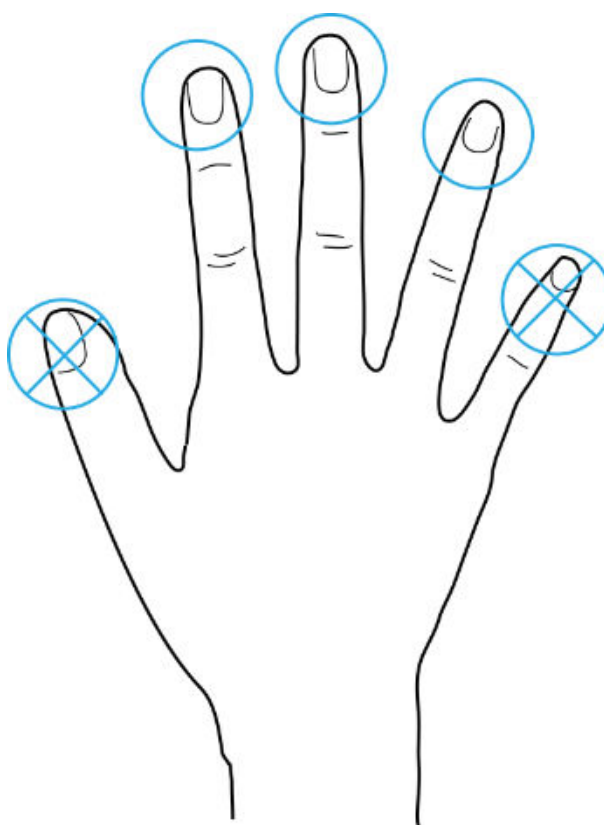
Quando registri l'impronta digitale, presta attenzione ai seguenti punti:

- Assicurati che le tue dita e la superficie dello scanner siano pulite e asciutte.
- Premi il dito al centro dello scanner di impronte digitali.
- Non posizionare il sensore di impronte digitali in un luogo con luce intensa, temperature elevate e umidità elevata.
- Se le tue impronte digitali non sono chiare, utilizza altri metodi di sblocco.

Dita consigliate

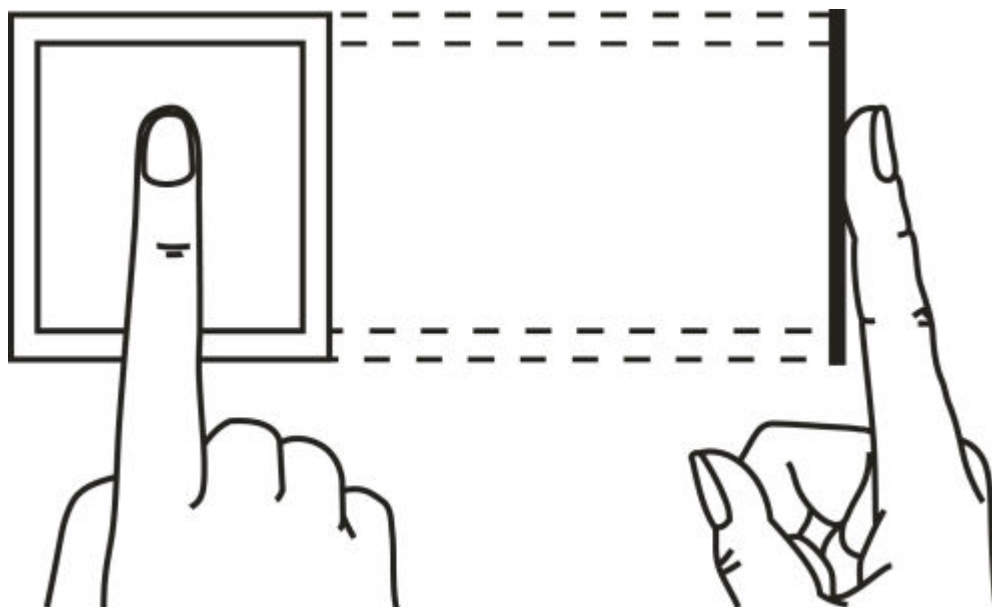
Si consiglia di utilizzare indice, medio e anulare. Il pollice e il mignolo non si adattano facilmente al centro di registrazione.

Appendice Figura 1-1 Dita consigliate

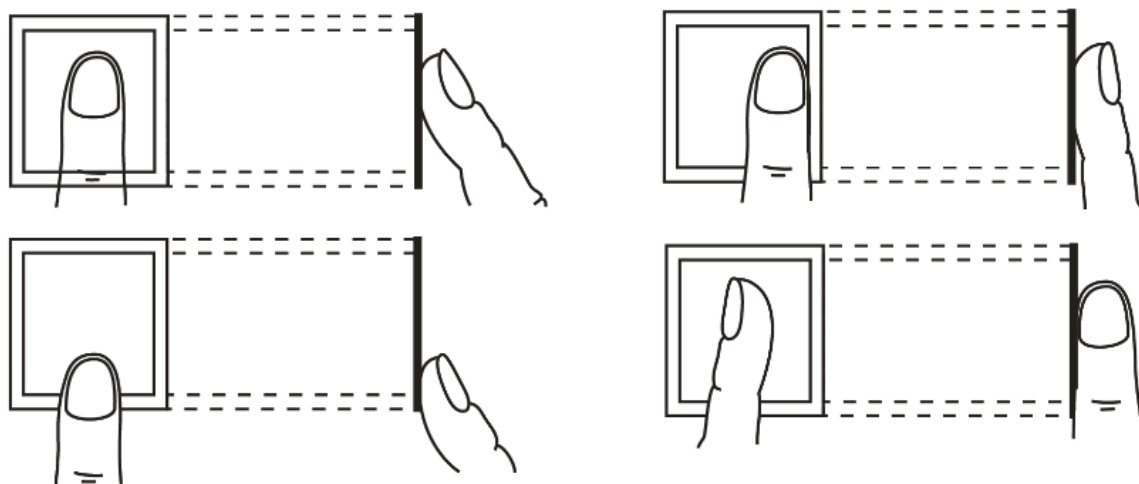


Come imprimere la propria impronta digitale sullo scanner

Appendice Figura 1-2 Posizionamento corretto



Appendice Figura 1-3 Posizionamento errato



Appendice 2 Raccomandazione di sicurezza

Gestione account

1. Utilizzare password complesse

Si prega di fare riferimento ai seguenti suggerimenti per impostare le password:

- La lunghezza non deve essere inferiore a 8 caratteri;
- Includi almeno due tipi di caratteri: lettere maiuscole e minuscole, numeri e simboli;
- Non inserire il nome dell'account né il nome dell'account in ordine inverso;
- Non utilizzare caratteri consecutivi, come 123, abc, ecc.;
- Non utilizzare caratteri ripetuti, come 111, aaa, ecc.

2. Cambiare le password periodicamente

Si raccomanda di cambiare periodicamente la password del dispositivo per ridurre il rischio che venga indovinata o violata.

3. Assegnare account e autorizzazioni in modo appropriato

Aggiungere gli utenti in modo appropriato in base ai requisiti di servizio e di gestione e assegnare a ciascun utente i set minimi di autorizzazioni.

4. Attiva la funzione di blocco dell'account

La funzione di blocco dell'account è abilitata per impostazione predefinita. Si consiglia di mantenerla attiva per proteggere la sicurezza dell'account. Dopo diversi tentativi di accesso errati, l'account e l'indirizzo IP di origine corrispondenti verranno bloccati.

5. Impostare e aggiornare tempestivamente le informazioni per il ripristino della password.

Il dispositivo supporta la funzione di reimpostazione della password. Per ridurre il rischio che questa funzione venga utilizzata da malintenzionati, in caso di modifiche alle informazioni, si prega di aggiornarle tempestivamente. Quando si impostano le domande di sicurezza, si consiglia di non utilizzare risposte facili da indovinare.

Configurazione del servizio

1. Abilita HTTPS

Si raccomanda di abilitare HTTPS per accedere ai servizi web tramite canali sicuri.

2. Trasmissione crittografata di audio e video

Se i contenuti audio e video sono molto importanti o sensibili, si consiglia di utilizzare la funzione di trasmissione crittografata per ridurre il rischio che vengano intercettati durante la trasmissione.

3. Disattiva i servizi non essenziali e utilizza la modalità sicura.

Se non necessari, si consiglia di disattivare alcuni servizi come SSH, SNMP, SMTP, UPnP, hotspot AP ecc., per ridurre le superfici di attacco.

Se necessario, si raccomanda vivamente di scegliere modalità sicure, tra cui, a titolo esemplificativo ma non esaustivo, i seguenti servizi:

- SNMP: scegli SNMP v3 e imposta password di crittografia e autenticazione robuste.
- SMTP: scegli TLS per accedere al server di posta.
- FTP: scegli SFTP e imposta password complesse.
- Hotspot AP: scegli la modalità di crittografia WPA2-PSK e imposta password complesse.

4. Modifica le porte HTTP e altre porte di servizio predefinite

Si consiglia di modificare la porta predefinita di HTTP e di altri servizi, impostandola su una porta compresa tra 1024 e 65535, per ridurre il rischio di essere individuati da malintenzionati.

Configurazione di rete

1. Abilita elenco consentiti

Si consiglia di attivare la funzione "lista di accesso" e di consentire l'accesso al dispositivo solo agli indirizzi IP presenti in tale lista. Pertanto, assicurarsi di aggiungere l'indirizzo IP del computer e l'indirizzo IP del dispositivo di supporto alla lista di accesso.

2. associazione indirizzo MAC

Si raccomanda di associare l'indirizzo IP del gateway all'indirizzo MAC del dispositivo per ridurre il rischio di ARP spoofing.

3. Creare un ambiente di rete sicuro

Al fine di garantire al meglio la sicurezza dei dispositivi e ridurre i potenziali rischi informatici, si raccomanda quanto segue:

- Disabilitare la funzione di port mapping del router per evitare l'accesso diretto ai dispositivi della rete intranet dalla rete esterna;
- In base alle effettive esigenze di rete, partizionare la rete: se non vi è alcuna richiesta di comunicazione tra le due sottoreti, si consiglia di utilizzare VLAN, gateway e altri metodi per partizionare la rete e ottenere l'isolamento della rete;
- Implementare un sistema di autenticazione degli accessi 802.1x per ridurre il rischio di accessi non autorizzati alla rete privata da parte dei terminali.

Audit di sicurezza

1. Controlla gli utenti online

Si raccomanda di controllare regolarmente gli utenti online per identificare quelli che utilizzano metodi illegali.

2. Controlla il registro del dispositivo

Consultando i log, è possibile ottenere informazioni sugli indirizzi IP che tentano di accedere al dispositivo e sulle operazioni principali eseguite dagli utenti connessi.

3. Configurare il registro di rete

A causa della capacità di archiviazione limitata dei dispositivi, la quantità di log memorizzati è limitata. Se è necessario conservare i log per un lungo periodo, si consiglia di abilitare la funzione di registrazione di rete per garantire la sincronizzazione dei log critici con il server di log di rete ai fini della tracciabilità.

Sicurezza del software

1. Aggiornare il firmware in tempo

Secondo le specifiche operative standard del settore, il firmware dei dispositivi deve essere aggiornato tempestivamente all'ultima versione per garantire che il dispositivo disponga delle funzionalità e della sicurezza più recenti. Se il dispositivo è connesso a una rete pubblica, si consiglia di abilitare la funzione di rilevamento automatico degli aggiornamenti online, in modo da ricevere tempestivamente le informazioni sugli aggiornamenti del firmware rilasciate dal produttore.

2. Aggiornare tempestivamente il software client

Si raccomanda di scaricare e utilizzare il software client più recente.

Protezione fisica

Si raccomanda di adottare misure di protezione fisica per i dispositivi (in particolare per i dispositivi di archiviazione), come ad esempio collocarli in una sala macchine e in un armadio dedicati e di disporre di un sistema di controllo degli accessi.

e un sistema di gestione delle chiavi per impedire al personale non autorizzato di danneggiare l'hardware e altre apparecchiature periferiche (ad esempio, unità flash USB, porta seriale).

