LASFCX

Tastiera touch fingerprint, display LCD.

Guida Rapida

Hiltron Land Srl
Strada Provinciale di Caserta, 218 - 80144 - Napoli t:
+39 081 185 39 000
www.hiltronsecurity.it

V1.0.2

Prefazione

Generale

Questo manuale introduce le funzioni e le operazioni di Fingerprint Access Standalone (di seguito denominato "il Dispositivo").

Istruzioni di sicurezza

Le seguenti parole di segnalazione potrebbero apparire nel manuale.

Avvertenze	Significato
PERICOLO	Indica un rischio potenziale elevato che, se non evitato, provocherà la morte o lesioni gravi.
AVVERTIMENTO	Indica un rischio potenziale medio o basso che, se non evitato, potrebbe causare lesioni lievi o moderate.
ATTENZIONE	Indica un rischio potenziale che, se non evitato, potrebbe causare danni alla proprietà, perdita di dati, riduzione delle prestazioni o risultati imprevedibili.
CONSIGLI	Fornisce metodi per aiutarti a risolvere un problema o risparmiare tempo.
NOTA	Fornisce informazioni aggiuntive come supplemento al testo.

Cronologia delle revisioni

Versione	Contenuto della revisione	Tempo di rilascio
V1.1.2	Schermate aggiornate.	settembre 2021

Informativa sulla tutela della privacy

In qualità di utente del dispositivo o titolare del trattamento dei dati, potresti raccogliere i dati personali di altri come il loro volto, le impronte digitali e il numero di targa. È necessario rispettare le leggi e i regolamenti locali sulla protezione della privacy per proteggere i diritti e gli interessi legittimi di altre persone implementando misure che includono ma non sono limitate: Fornire un'identificazione chiara e visibile per informare le persone dell'esistenza dell'area di sorveglianza e fornire le informazioni di contatto richieste.

Informazioni sul manuale

- Il manuale è solo per riferimento. Potrebbero essere riscontrate lievi differenze tra il manuale e il prodotto.
- Non siamo responsabili per perdite subite a causa dell'uso del prodotto in modi non conformi al manuale.

- Il manuale sarà aggiornato secondo le ultime leggi e regolamenti delle relative giurisdizioni. Per informazioni dettagliate, consultare il manuale utente cartaceo, utilizzare il nostro CD-ROM, scansionare il codice QR o visitare il nostro sito Web ufficiale. Il manuale è solo per riferimento. Leggere differenze potrebbero essere riscontrate tra la versione elettronica e la versione cartacea.
- Tutti i design e il software sono soggetti a modifiche senza preavviso scritto. Gli aggiornamenti del prodotto potrebbero comportare la comparsa di alcune differenze tra il prodotto effettivo e il manuale. Si prega di contattare il servizio clienti per il programma più recente e la documentazione supplementare.
- Potrebbero esserci errori nella stampa o deviazioni nella descrizione delle funzioni, delle operazioni e dei dati tecnici. In caso di dubbi o controversie, ci riserviamo il diritto di spiegazioni finali. Aggiorna il
- software del lettore o prova un altro software di lettura tradizionale se non è possibile aprire il manuale (in formato PDF).
- Tutti i marchi, marchi registrati e nomi di società presenti nel manuale sono di proprietà dei rispettivi proprietari.
- Si prega di visitare il nostro sito Web, contattare il fornitore o il servizio clienti se si verificano problemi durante l'utilizzo del dispositivo.
- In caso di incertezza o controversia, ci riserviamo il diritto di una spiegazione finale.

Importanti misure di salvaguardia e avvertenze

Questa sezione introduce i contenuti riguardanti la corretta gestione del Dispositivo, la prevenzione dei rischi e la prevenzione dei danni alla proprietà. Leggere attentamente prima di utilizzare il dispositivo, attenersi alle linee guida durante l'utilizzo e conservare il manuale in un luogo sicuro per future consultazioni.

Requisiti di trasporto

Trasportare, utilizzare e conservare il Dispositivo in condizioni di umidità e temperatura consentite.

Requisiti di archiviazione

Conservare il dispositivo in condizioni di umidità e temperatura consentite.

Requisiti di installazione

AVVERTIMENTO

- Collegare il dispositivo all'adattatore prima dell'accensione.
- Rispettare rigorosamente gli standard di sicurezza elettrica locali e assicurarsi che la tensione nell'area sia costante e conforme ai requisiti di alimentazione del Dispositivo.
- Non collegare il Dispositivo a più di un alimentatore. In caso contrario, il Dispositivo potrebbe danneggiarsi.

- Osservare tutte le procedure di sicurezza e indossare i dispositivi di protezione richiesti forniti per l'uso durante i lavori in quota.
- Non esporre il Dispositivo alla luce diretta del sole o a fonti di calore.
- Non installare il Dispositivo in luoghi umidi, polverosi o fumosi.
- Installare il Dispositivo in un luogo ben ventilato e non bloccare il ventilatore del Dispositivo. Utilizzare
- l'adattatore di alimentazione o l'alimentatore della custodia forniti dal produttore del dispositivo.
- L'alimentatore deve essere conforme ai requisiti di ES1 nello standard IEC 62368-1 e non essere superiore a PS2. Si noti che i requisiti di alimentazione sono soggetti all'etichetta del dispositivo. Collegare gli apparecchi
- elettrici di classe I a una presa di corrente con messa a terra di protezione.
- Il dispositivo deve essere installato su una superficie solida e piana per garantire la sicurezza sotto carico e sisma. In caso contrario, il dispositivo potrebbe cadere o capovolgersi.

Requisiti operativi

- Assicurarsi che l'alimentazione del dispositivo funzioni correttamente prima dell'uso.

Importanti misure di salvaguardia e avvertenze

- Non estrarre il cavo di alimentazione del dispositivo mentre è acceso. Utilizzare il
- dispositivo solo all'interno della gamma di potenza nominale.
- Utilizzare il dispositivo in condizioni di umidità e temperatura consentite.
- Evitare che i liquidi schizzino o gocciolino sul dispositivo. Assicurarsi che non ci siano oggetti pieni di liquido sopra il Dispositivo per evitare che i liquidi vi penetrino.
- Non smontare il Dispositivo.
- Si prega di utilizzare la batteria correttamente per evitare incendi, esplosioni e altri
- pericoli. Sostituire la batteria usata con una batteria dello stesso tipo.
- Se si utilizza la spina di alimentazione o l'accoppiatore dell'apparecchio come dispositivo di disconnessione, tenere sempre disponibile il dispositivo di disconnessione per essere utilizzato per tutto il tempo.

Sommario

1:PANORAMICO

Fingerprint Access Standalone integra la lettura delle tessere, le configurazioni e altre funzioni. Può essere applicato in molti scenari, come edifici commerciali, società e comunità intelligenti.

Caratteristiche principali

- Tastiera touch + display LCD, protocollo TCP/IP.
- Supporta lo sblocco tramite carta, impronta digitale, password e loro combinazioni.
- Supporta un massimo di 3.000 impronte digitali (per impostazione predefinita) e fino a 4.500 impronte digitali (personalizzate), 30.000 carte valide e 500 password pubbliche.
- Supporta un massimo di 150.000 record di schede e 1024 record di allarme. Supporta allarme timeout
- porta, allarme intrusione, allarme coercizione e allarme sensore porta. Supporta l'ingresso del
- campanello.
- Supporta la carta ospite, la carta coercizione, la lista bloccata/lista consentita e la carta pattuglia, mentre supporta il periodo di validità o i tempi.
- Supporta lettore di schede e controller per porta singola.
- Supporta 128 gruppi di periodo e 128 gruppi di periodo festivo.

⚠

Se questo prodotto richiede alimentazione esterna, utilizzare un adattatore da 12 V CC 0,5 A e il funzionamento la temperatura deve essere compresa tra -5 °C e 55 °C.

2:Guida all'installazione

2.1Dimensione del dispositivo

Figura 2-1 Vista frontale

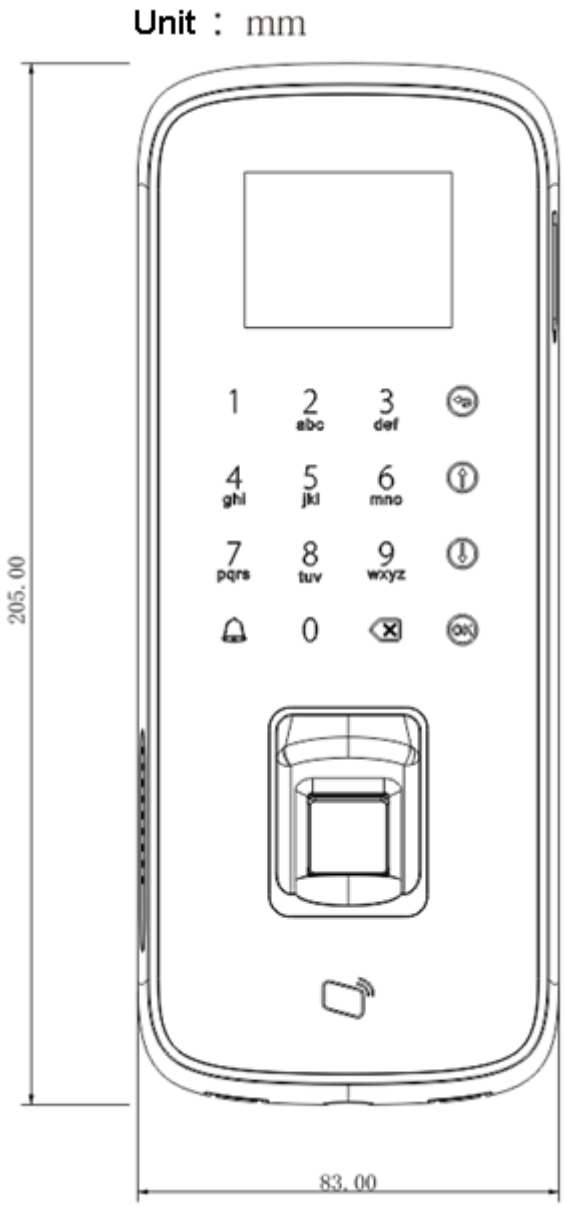
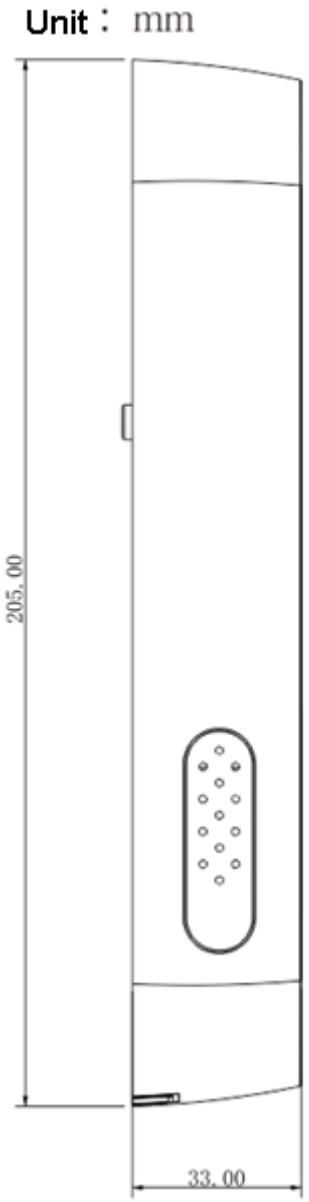


Figura 2-2 Vista laterale



2.2 Installazione del dispositivo

Figura 2-3 Fili del dispositivo

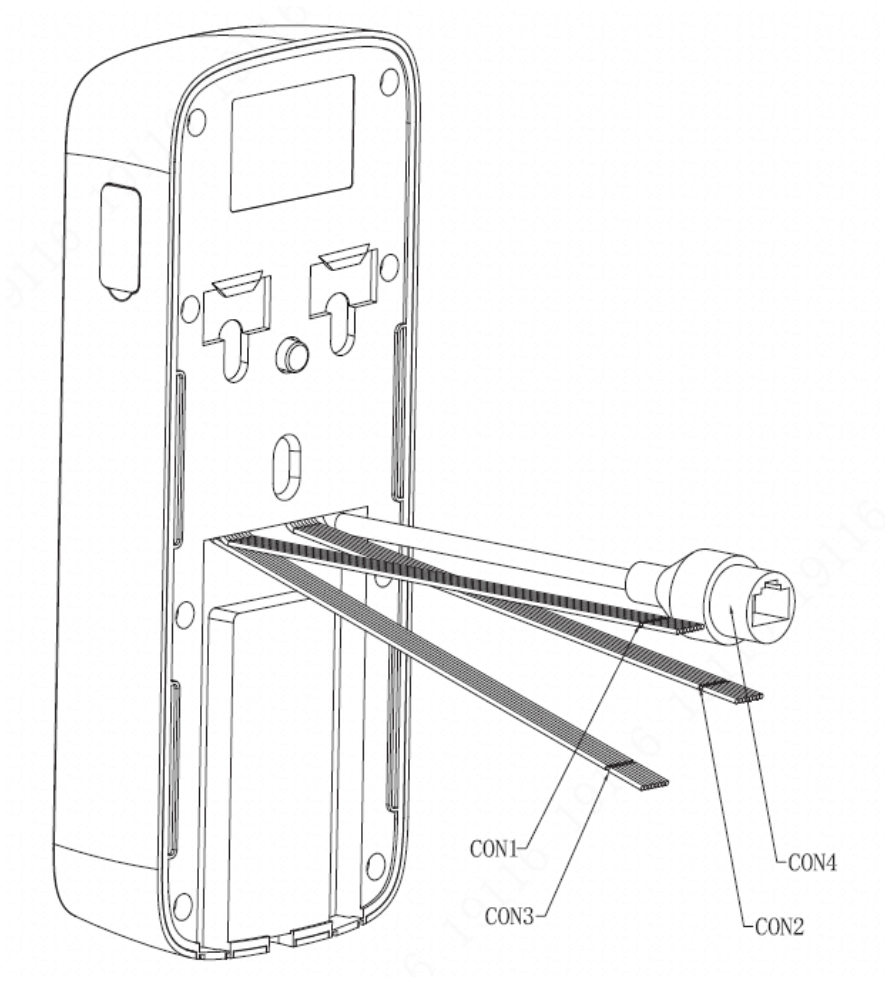


Tabella 2-1 Descrizione delle porte

Porta	Colore	Interfaccia	Nota	Protocollo
CON1	Rosso	+ 12 VI	Ingresso alimentazione 12 V CC	—
	Nero	GND	GND	
	Blu	COM	Blocca COM	
	Bianco	NC	Blocca NC	
	Verde	NO	Serratura n	
	Marrone	SR	Sensore porta	
	Giallo	GND	GND	
	Porpora	SPINGERE	Pulsante di sblocco	
CON2	Rosso	+ 12vo	Uscita alimentazione 12 V CC	—
	Nero	GND	GND	—
	Blu	ASTUCCIO	Lettore di schede	Weigand protocollo
	Bianco	D1	Linea Weigand 1	
	Verde	D0	Linea 0 di Weigand	
	Marrone	GUIDATO	Linea indicatrice della carta Weigand	
	Giallo	B1	RS485B	Protocollo RS485
	Porpora	A1	RS485A	

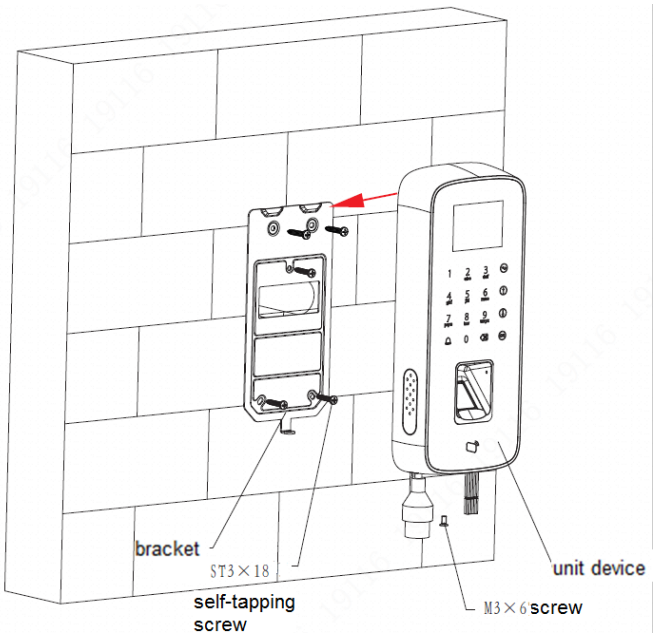
Porta	Colore	Interfaccia	Nota	Protocollo
CON3	Rosso	CAMPANELLO+	Squillo	—
	Nero	CAMPANA-		
	Blu	GND	GND	
	Bianco	AOUT	Uscita allarme	
	Verde	AIN	Ingresso allarme	
	Marrone	GND	GND	
	Giallo	B2	RS485B esterno	Protocollo RS485
	Porpora	A2	RS485A esterna	
CON4	—	RJ45	Rete	—

Procedura d'installazione

Passo 1 Fissare la staffa sulla superficie di installazione con tre viti autofilettanti ST3×18. Collegare i
Passo 2 fili, infilare i fili nelle fessure della staffa e posizionare i fili nella superficie di installazione.

Passaggio 3 Secondo la direzione della freccia, fissare il dispositivo alla staffa.

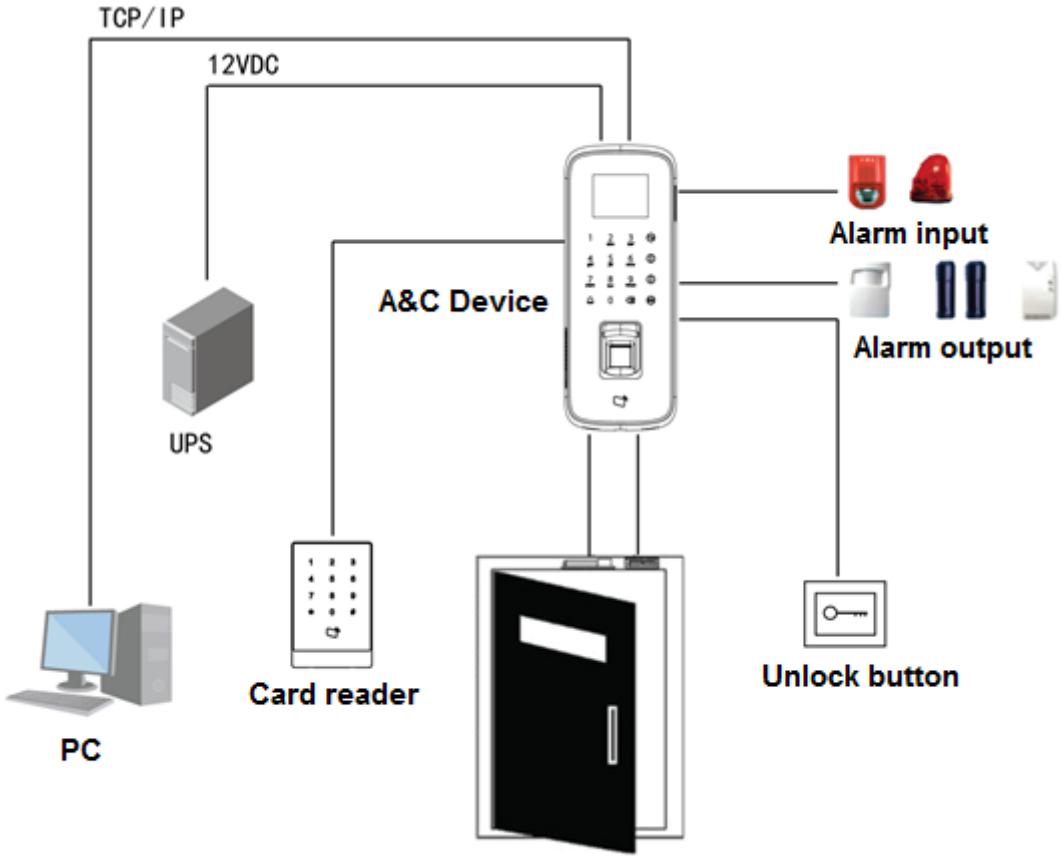
Figura 2-4 Installazione del dispositivo



Passaggio 4 Dal basso verso l'alto e fissare la staffa con una vite M3×6.

3:STRUTTURA DEL SISTEMA

Figura 3-1 Struttura del sistema



4:Impostazioni funzione

4.1 Accesso

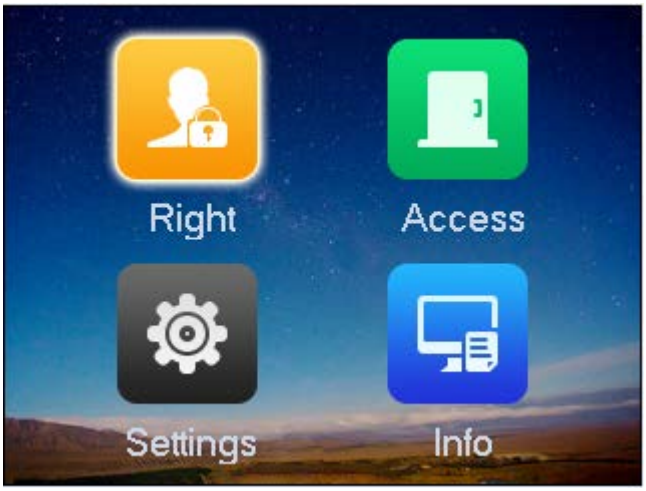
Passo 1 Avvia il dispositivo e tocca**OK**.

Passo 2 Immettere la password dell'amministratore e toccare**OK**per entrare nel**Menu principale**.

La password predefinita è "88888888". Si prega di cambiare la password dell'amministratore.

- Rubinetto↑pulsante per salire. Rubinetto↓
- pulsante per spostarsi verso il basso. Rubinetto
- **OK**per entrare o confermare. Rubinetto
- tornare o uscire.
- Rubinetto tornare indietro.
- Rubinetto suonare.

Figura 4-1 Menu principale



4.2 Gestione utenti

Puoi aggiungere o eliminare utenti.

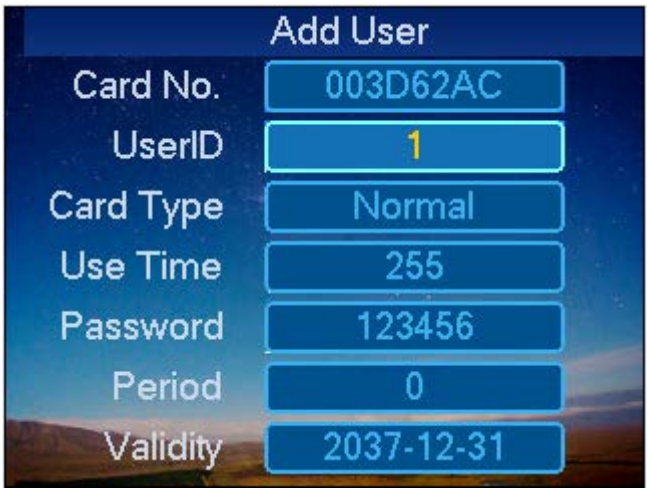
4.2.1 Aggiunta di utenti

Aggiungi utenti per associare il numero della carta con le loro impronte digitali.

Passo 1 Nella pagina principale selezionare**Destra > OK**.

Passo 2 Rubinetto**Aggiungi utente**>**OK**.

Figura 4-2 Aggiungi utente



Passaggio 3 Utilizzare la tastiera per inserire il numero della carta o posizionare la carta sull'area di strisciamento.

Passaggio 4 Seleziona un tipo di carta.

Tabella 4-1 Tipi di scheda

Tipo di carta	Descrizione
Normale	Le persone possono accedere alla porta entro il tempo configurato e il periodo di validità.
Tessera VIP	Il personale di servizio riceve notifiche quando il titolare della carta VIP entra.
Carta degli ospiti	Gli ospiti possono sbloccare la porta per tempi limitati. Quando i tempi di sblocco si esaurisce, non possono aprire la porta.
Carta di pattuglia	Gli utenti di pattuglia avranno la loro presenza monitorata, ma non hanno permessi di sblocco.
Lista di Bloccati	Quando gli utenti nella lista bloccata sbloccano la porta, il personale di servizio riceverà una notifica.
Carta di coercizione	La carta di coercizione diventa valida dopo aver impostato l'allarme di coercizione. Puoi scorrere questo card da sbloccare, ma verrà inviato un allarme al centro.

Passaggio 5 Configura altri parametri utente.

Passaggio 6 Rubinetto**OK**e il sistema richiede se registrare l'impronta digitale.

- Selezionare**SÌ**e seguire le istruzioni per registrare l'impronta digitale.
- Selezionare**NO**per completare l'aggiunta.

4.2.2 Aggiunta di una password pubblica

Sblocca la porta inserendo solo la password pubblica.

Prima di utilizzare la password pubblica per sbloccare la porta, impostare la modalità di sblocco su sblocco tramite password, o sblocco tramite carta o password o impronta digitale.

Passo 1 Sul**Destra**schermo, selezionare**Aggiungi password pubblica**, quindi toccare**OK**.

Figura 4-3 Password pubblica

Passo 2 Inserisci la password pubblica n. e tocca↓.

Passaggio 3 Inserisci la password pubblica e la password di conferma. Rubinetto

Passaggio 4 **OK**.

4.2.3 Eliminazione di utenti

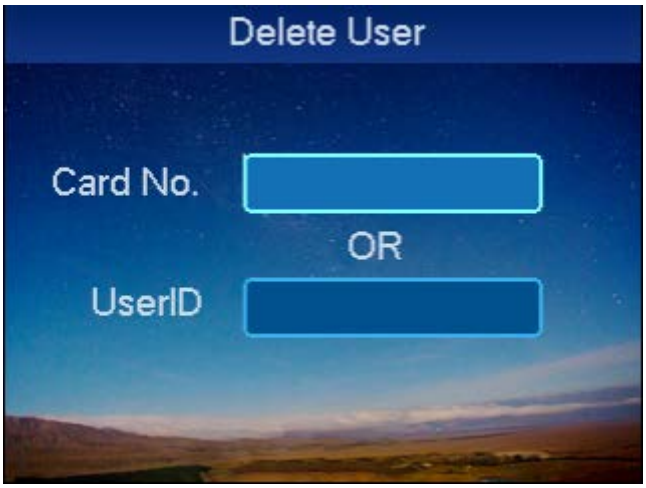
Puoi eliminare un singolo utente o tutti gli utenti.

4.2.3.1 Eliminazione di un singolo utente

Passo 1 Sul**Destra**schermo, selezionare**Elimina utente**e tocca**OK**.

Passo 2 Selezionare**Elimina utente singolo**e tocca**OK**.

Figura 4-4 Elimina utente



Passaggio 3 Elimina utente.

- Inserisci il numero della carta che desideri eliminare e tocca**OK**.
- Eseguire la scansione della carta che si desidera eliminare nell'area di scorrimento della carta, quindi toccare**OK**.
- Immettere il numero utente che si desidera eliminare, quindi toccare**OK**.

Passaggio 4 Selezionare**OK**e tocca**OK**.

4.2.3.2 Eliminazione di tutti gli utenti

Passo 1 Nella schermata Elimina utente, seleziona tutti gli utenti e tocca**OK**

Passo 2 . Selezionare**OK**e tocca**OK**.

4.2.4 Cancellazione password

È possibile eliminare una singola password pubblica o eliminare tutte le password pubbliche.

4.2.4.1 Eliminazione di una singola password pubblica

Passo 1 Sul**Elimina utente**schermo, selezionare**Elimina password pubblica**e tocca**OK**.

Passo 2 Selezionare**Elimina password pubblica singola**e tocca**OK**.

Figura 4-5 Elimina password pubblica

Passaggio 3 Immettere il numero della password pubblica e toccare**OK**.

Passaggio 4 Selezionare**OK**e tocca**OK**.

4.2.4.2 Eliminazione di tutte le password pubbliche

Passo 1 Su**Elimina password pubblica**schermo, selezionare**Elimina tutte le password pubbliche**e tocca**OK**.

Passo 2 Selezionare**OK**e tocca**OK**.

4.2.5 Aggiunta di carte principali

Puoi aggiungere rapidamente gli utenti della carta tramite la carta principale. Prima di aggiungere gli utenti della carta, devi prima aggiungere una carta principale.

Passo 1 Sul**Destra**schermata, selezionare aggiungi altra carta principale e toccare**OK**.

Passo 2 Posiziona la carta principale sull'area di scorrimento e scansiona.

Passaggio 3 Posiziona la carta aggiunta nell'area di scorrimento per eseguire la scansione.

4.3Configurazione del controllo degli accessi

4.3.1 Periodo di impostazione

È possibile impostare il periodo di sblocco, incluso il periodo di scorrimento della carta, il periodo di vacanza, il periodo di modalità e il periodo NO.

4.3.1.1 Impostazione del periodo di strisciamento della carta

Il periodo di scorrimento della carta può essere compreso tra 0 e 127, per un totale di 128 periodi. In ogni periodo, è necessario impostare programmi per una settimana. Quando viene aggiunta una nuova carta e si imposta il periodo di scorrimento della carta, l'utente fa scorrere la carta per sbloccarla. Il controllo degli accessi giudicherà se l'ora corrente rientra nel periodo impostato.

Tabella 4-2 Periodo di strisciamento della carta

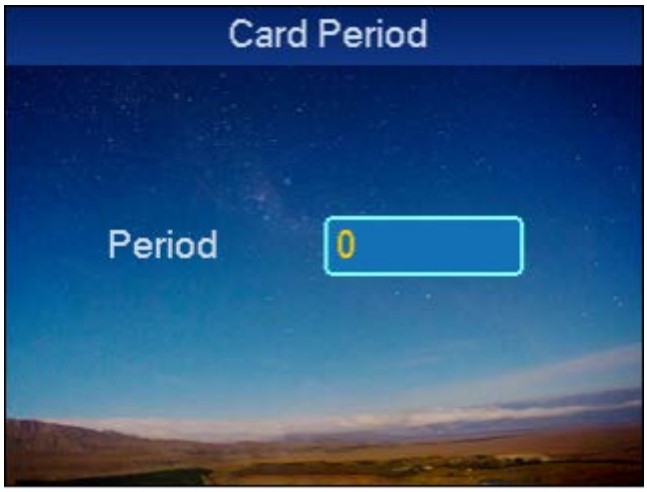
Giorno	Periodo
Lunedi	0800-2200 (periodo valido: dalle 08:00 alle 22:00)
Martedì	0800-2200 (periodo valido: dalle 08:00 alle 22:00)
Mercoledì	0800-2200 (periodo valido: dalle 08:00 alle 22:00)
Giovedì	0800-2200 (periodo valido: dalle 08:00 alle 22:00)
Venerdì	0800-2200 (periodo valido: dalle 08:00 alle 22:00)
Sabato	0800-2200 (periodo valido: dalle 08:00 alle 22:00)
Domenica	0800-2200 (periodo valido: dalle 08:00 alle 22:00)

Passo 1 Nel menu principale selezionare**Accesso**e tocca**OK**. Seleziona

Passo 2 il periodo di tempo e tocca**OK**. Seleziona il periodo di

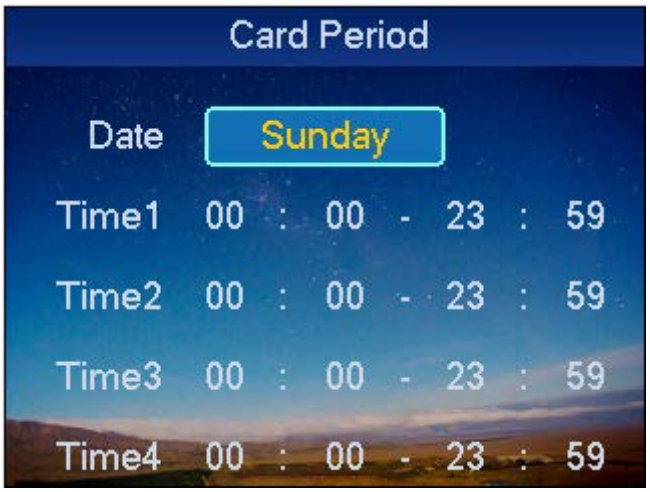
Passaggio 3 scorrimento della carta e tocca**OK**.

Figura 4-6 Periodo di strisciamento della carta (1)



Passaggio 4 Immettere il periodo di tempo e toccare**OK**. Inserisci qualsiasi numero compreso tra 0 e 127.

Figura 4-7 Periodo di strisciamento della carta (2)



Passaggio 5 Selezionare un giorno per impostare i periodi e toccare**OK**.

Passaggio 6 Impostare i periodi per il resto della settimana. Rubinetto**OK**

Passaggio 7 .

Passaggio 8 Selezionare**SÌ**e tocca**OK**.

4.3.1.2 Impostazione del periodo di ferie

È possibile impostare fino a 128 periodi di vacanza (da 0 a 127). Passo

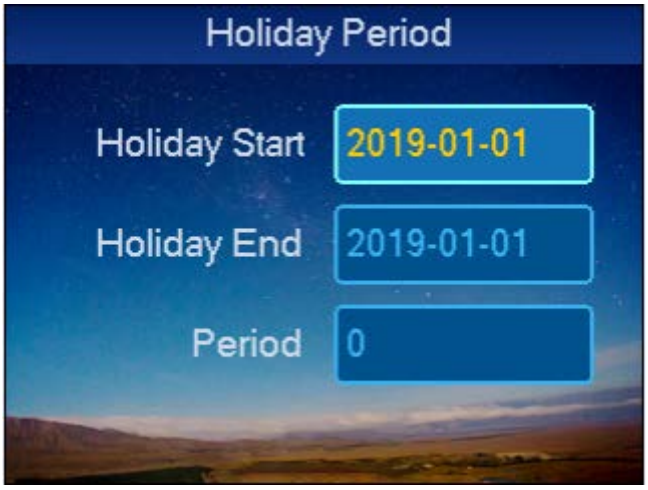
1 Nella schermata di impostazione del periodo di tempo, selezionare il periodo delle vacanze, quindi toccare**OK**.

Passo 2 Immettere il numero del periodo (0–127).

Passaggio 3 Immettere l'ora di inizio della vacanza, l'ora di fine della vacanza e il periodo, quindi toccare**OK**.

Il periodo è il numero del periodo impostato nella schermata del periodo della carta.

Figura 4-8 Periodo festivo

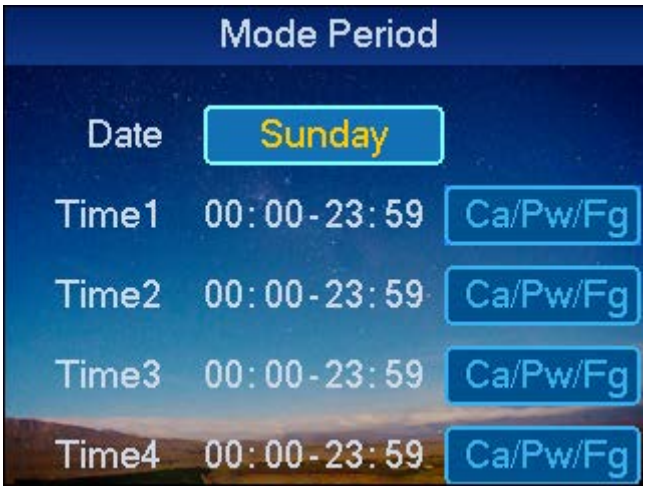


Passaggio 4 Selezionare**SÌ**e tocca**OK**.

4.3.1.3 Periodo modalità di impostazione

Il periodo di modalità ha quattro periodi al giorno dal lunedì alla domenica. Passo 1 Nella schermata di impostazione del periodo di tempo, selezionare il periodo della modalità e toccare**OK**.

Figura 4-9 Periodo della modalità



Passo 2 Selezionare**Lunedì**e tocca**OK**.

Passaggio 3 Configura il periodo, tocca**OK**per selezionare la modalità di sblocco del

Passaggio 4 periodo. Configura i periodi dal martedì alla domenica.

Passaggio 5 Rubinetto**OK**.

Passaggio 6 Selezionare**SÌ**e tocca**OK**.

Dopo il completamento, le modalità di sblocco vengono gestite secondo i quattro periodi.

4.3.1.4 Impostazione NO periodo

Dopo aver impostato il periodo NO, la porta rimarrà sbloccata durante questo periodo. Passo 1

Nella schermata di impostazione dell'ora, selezionare**NO Periodo**e tocca**OK**.

Figura 4-10 Periodo NO

Il numero del periodo è il numero impostato nella schermata del periodo di strisciamento della carta.

Passo 2 Rubinetto per eliminare i vecchi dati, inserire il numero del periodo, quindi toccare**OK**.

4.3.2 Impostazione della scheda principale

Puoi modificare o aggiungere la carta principale.

Passo 1 Sul**Accesso**schermo, selezionare la configurazione della scheda principale e toccare**OK**.

Figura 4-11 Impostazione della scheda principale

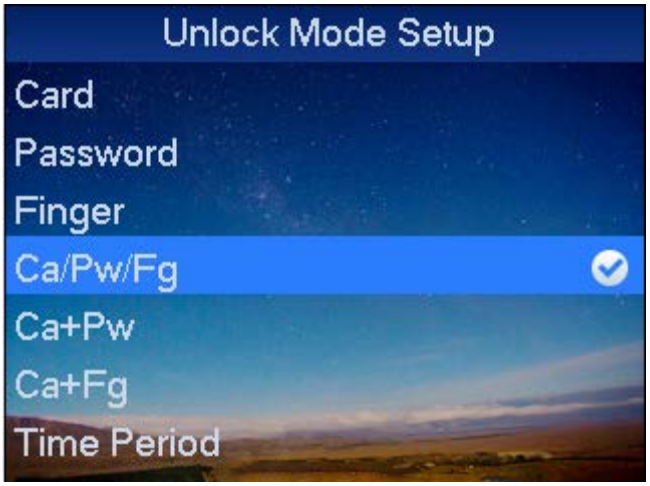
Passo 2 Rubinetto per eliminare il vecchio numero di carta e inserire il nuovo numero di carta o posizionare la carta su area di scorrimento per la scansione, quindi toccare**OK**.

4.3.3 Impostazione della modalità di sblocco

Le modalità di sblocco includono carta, password, impronta digitale, carta e password, carta e impronta digitale, carta o password o impronta digitale.

Passo 1 Sul**Accesso**schermo, selezionare la modalità di sblocco, quindi toccare**OK**.

Figura 4-12 Impostazione della modalità di sblocco



Passo 2 Seleziona la modalità di sblocco e tocca**OK**.

4.3.4 Impostazione del tempo di blocco della porta

Il tempo di blocco della porta include il tempo di mantenimento della serratura e il tempo aggiuntivo.

- Tempo di attesa: dopo aver fatto scorrere la carta, la porta rimane sbloccata per un tempo di attesa definito prima di richiudersi.
- Nel tempo: se la porta rimane sbloccata dopo il tempo definito dopo aver fatto scorrere la carta, viene attivato un allarme.

Passo 1 Sul**Accesso**schermo, selezionare l'impostazione dell'ora di blocco della porta e toccare**OK**.

Figura 4-13 Impostazione del tempo di blocco della porta

Passo 2 Rubinetto per eliminare i dati originali, inserire il tempo di attesa e nel tempo, quindi toccare**OK**.

Il tempo di blocco della porta è il tempo in cui la porta rimane aperta dopo che una persona fa scorrere la carta. Se la porta rimane aperto oltre il "tempo", viene attivato un allarme.

4.3.5 Impostazione degli allarmi

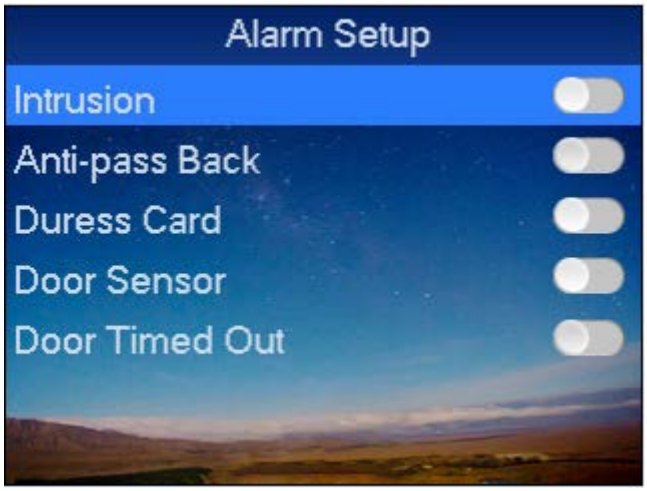
Puoi abilitare o disabilitare gli allarmi. L'allarme di sistema include intrusione, anti-pass back, tessera coercizione, sensore porta e timeout porta.

Tabella 4-3 Tipo di allarme

Tipo di allarme	Nota
Intrusione	Viene attivato un allarme quando le persone entrano senza strisciare una carta valida o una password.
Anti-passback	Se abilitato, gli utenti devono verificare le identità sia per l'ingresso che per l'uscita; in caso contrario verrà attivato un allarme. - Se una persona entra con verifica ed esce senza verifica, verrà attivato un allarme quando tenta di sbloccare nuovamente e l'accesso viene negato allo stesso tempo. - Se una persona entra senza verifica ed esce con verifica, verrà attivato un allarme quando tenta di sbloccare nuovamente e l'accesso viene negato allo stesso tempo.
Carta di coercizione	Un allarme verrà attivato quando una carta di coercizione o una password di coercizione viene utilizzata per sbloccare la porta.
Sensore porta	Quando il dispositivo è danneggiato, verrà attivato un allarme.
Porta scaduta	Se la porta rimane sbloccata per un tempo superiore a quello preimpostato, verrà attivato un allarme di timeout.

Passo 1 Sul**Accesso**schermo, selezionare l'impostazione della sveglia e toccare**OK**.

Figura 4-14 Impostazione allarme



Passo 2 Selezionare il tipo di sveglia per abilitare la funzione sveglia, quindi toccare**OK**.

4.3.6 Impostazione dello stato della porta

È possibile impostare lo stato del controllo accessi su normale, NO o NC.

Passo 1 Sul**Accesso**schermo, selezionare la configurazione dello stato della porta, quindi toccare**OK**.

Passo 2 Utilizzo↑e↓ aselezionare lo stato di controllo dell'accesso e toccare**OK**.

viene visualizzato dopo la selezione.

4.4 Impostazioni di sistema

4.4.1 Configurazione locale

È possibile impostare dati, password amministratore e posta vocale. Puoi anche esportare tutti i dati e ripristinare le impostazioni predefinite.

4.4.1.1 Data impostazione

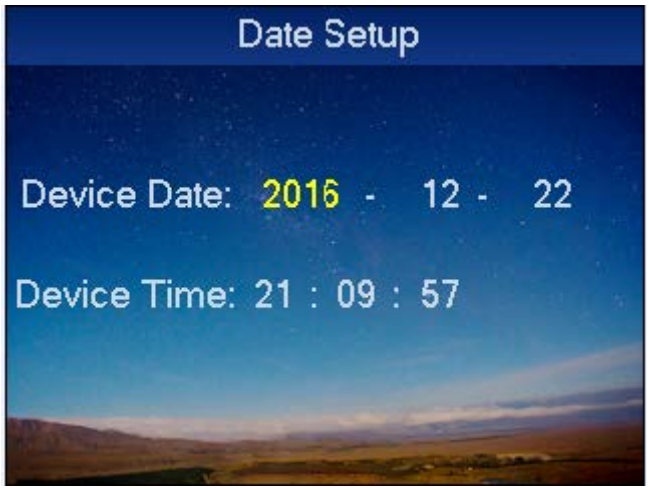
Imposta la data e l'ora del sistema.

Passo 1 Sul**Sistema**schermo, toccare↑o↓per selezionare l'impostazione della data, quindi toccare**OK**.

Passo 2 Seleziona la configurazione locale, quindi tocca**OK**.

Passaggio 3 Selezionare l'impostazione della data, quindi toccare**OK**.

Figura 4-15 Impostazione dati



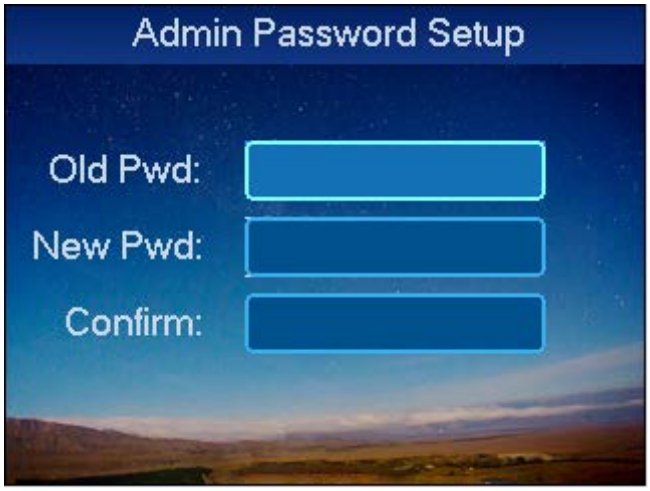
Passaggio 4 Impostare la data e l'ora del dispositivo, quindi toccare**OK**.

4.4.1.2 Modifica della password dell'amministratore

Puoi cambiare la password dell'amministratore.

Passo 1 Nella schermata di configurazione locale, seleziona configurazione password amministratore, quindi tocca**OK**.

Figura 4-16 Impostazione password amministratore

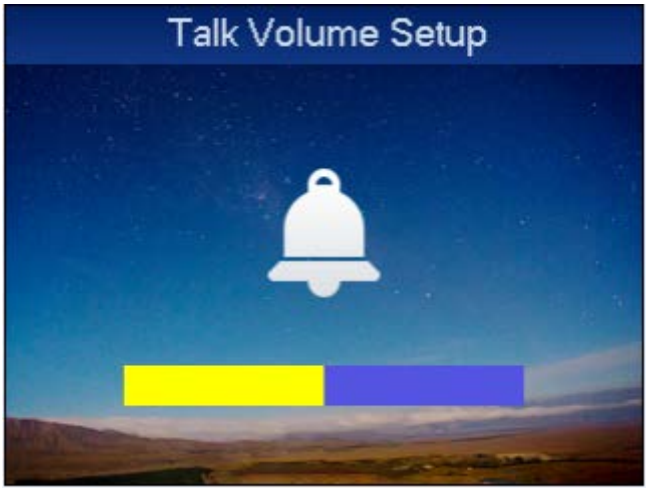


Passo 2 Immettere la vecchia password, la nuova password, la password di conferma, quindi toccare**OK**.

4.4.1.3 Impostazione del volume

Passo 1 Nella schermata di configurazione locale, selezionare**Configurazione del volume di conversazione**, quindi toccare**OK**.

Figura 4-17 Impostazione del volume



Passo 2 Rubinetto↑o↓,per regolare il volume.

4.4.1.4 Ripristino delle impostazioni predefinite

Passo 1 Nella schermata di configurazione locale, selezionare predefinito, quindi toccare**OK**

Passo 2 . Selezionare**SÌ**e quindi toccare**OK**ripristinare.

4.4.2 Configurazione della rete

4.4.2.1 Impostazione della modalità di rete

Passo 1 Nel menu principale selezionare**Impostazioni**, quindi toccare**OK**.

Passo 2 Selezionare**Configurazione di rete**e tocca**OK**. Selezionare**Configurazione**

Passaggio 3 **della modalità di rete**e tocca**OK**.

Figura 4-18 Impostazione della modalità di rete

Passaggio 4 Rubinetto↑o↓,per selezionare la modalità di rete e abilitarla, quindi toccare**OK**.

Rubinetto**OK**di nuovo per chiudere la modalità di connessione di rete.

Tipo di rete	Nota
DHCP	Auto ottiene la funzione IP. Quando si abilita l'indirizzo IP DHCP, non è possibile impostare subnet mask e gateway predefinito.
Abilitazione P2P	Non è necessario richiedere un dominio dinamico, una porta di mappatura o una distribuzione server.

4.4.2.2 Impostazione IP

Passo 1 Sul**Configurazione di rete**schermo, selezionare**Configurazione dell'IP**, quindi toccare**OK**.

Figura 4-19 Configurazione IP

Passo 2 Modifica IP, subnet mask e gateway, quindi tocca**OK**.

4.4.3 Impostazione della modalità del dispositivo

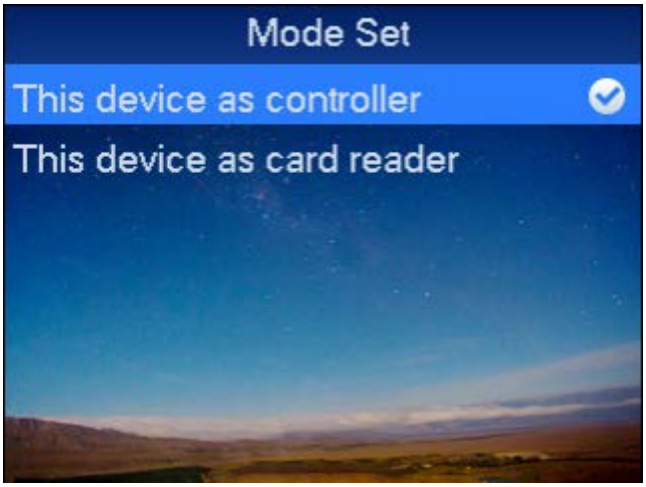
Il dispositivo supporta due modalità del dispositivo, che sono la modalità controller e la modalità lettore di schede.

- **Questo dispositivo come controller**: il dispositivo viene utilizzato come controller per controllare l'accesso.
- **Questo dispositivo come lettore di schede**: il dispositivo viene utilizzato come lettore di schede. Se è necessario controllare l'accesso alla porta, è necessario collegarlo a un controller.

Passo 1 Sul**Impostazioni**schermata, selezionare la configurazione della modalità, quindi

Passo 2 toccare**OK**. Seleziona la modalità di lavoro e tocca**OK.**

Figura 4-20 Impostazione modalità



Passaggio 3 Rubinetto↑o↓per selezionare la modalità di lavoro, quindi toccare**OK**.

Dopo che la selezione è andata a buon fine, a○ √verrà visualizzato accanto alla modalità di lavoro.

4.4.4 Riavvio del dispositivo

Passo 1 Nel menu principale selezionare**Impostazioni**e quindi toccare**OK**.

Passo 2 Selezionare**Riavviare**e quindi toccare**OK**.

Passaggio 3 Selezionare**SÌ**, quindi toccare**OK**per riavviare il dispositivo.

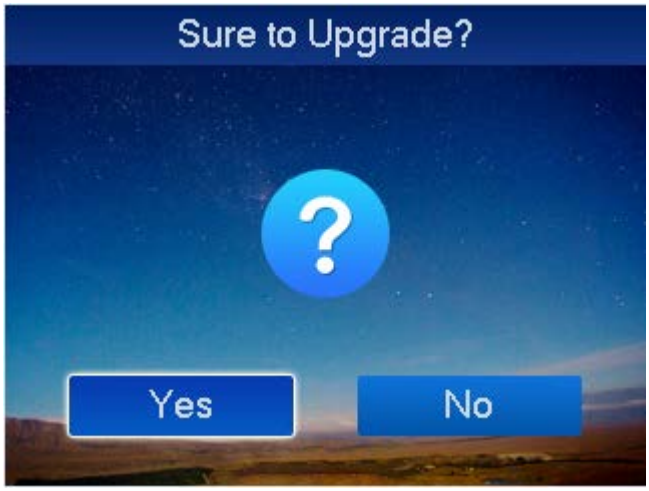
4.4.5 Sistema di aggiornamento

Passo 1 Rinominare il file di aggiornamento come "AutoUpDate.bin", salvarlo nella directory principale USB, quindi inserire l'USB nel dispositivo.

Passo 2 Nel menu principale selezionare**Impostazioni**, quindi toccare**OK**.

Passaggio 3 Selezionare**Aggiornamento USB**e tocca**OK**.

Figura 4-21 Aggiornamento tramite USB



Passaggio 4 Utilizzo↑e↓selezionare**sì**, quindi toccare**OK**.

Il sistema inizia ad aggiornarsi e si riavvierà automaticamente al termine dell'aggiornamento.

4.5 Informazioni di sistema

È possibile visualizzare le informazioni sullo scorrimento della carta, le informazioni sugli allarmi e le informazioni locali.

4.5.1 Visualizzazione dei record di sblocco

Passo 1 Nel menu principale selezionare**Informazioni**, quindi toccare**OK**

Passo 2 . Seleziona Sblocca record, quindi tocca**OK**.

Figura 4-22 Sblocca record

Passaggio 3 Rubinetto↑o↓per selezionare il metodo di visualizzazione.

- Visualizza tutta la cronologia di sblocco

  Selezionare**Visualizza tutti i record di sblocco**, quindi toccare**OK**. È possibile visualizzare le informazioni sui record di sblocco, inclusi ora, numero di carta, modalità e stato.

- Visualizza record per periodo

1) Seleziona**Visualizza record per periodo**, quindi toccare**OK**.

Figura 4-23 Visualizza record per periodo

2) Immettere l'ora di inizio e l'ora di fine, quindi toccare**OK**.

È possibile visualizzare un massimo di 150.000 record.

4.5.2 Visualizzazione dei record di allarme

Passo 1 Sul**Informazioni**schermata, selezionare la registrazione dell'allarme, quindi toccare**OK**.

Figura 4-24 Record di allarme

Passo 2 Rubinetto↑o↓per selezionare il metodo di visualizzazione.

- Visualizza tutti i record di allarme

  Selezionare**Visualizza tutti i record di allarme**, quindi toccare**OK**per visualizzare il tipo di sveglia, l'ora della sveglia e altro.

- Visualizza record per periodo

1) Seleziona**Visualizza record per periodo**, quindi toccare**OK**.

Figura 4-25 Visualizza record per periodo

2) Immettere l'ora di inizio e l'ora di fine e toccare**OK**.

È possibile visualizzare un massimo di 1024 record.

4.5.3 Visualizzazione delle informazioni sul dispositivo

È possibile visualizzare le informazioni di base sul dispositivo come versione del dispositivo, MAC e IP.

Passo 1 Nel menu principale selezionare**Informazioni**, quindi toccare**OK**.

Passo 2 Selezionare**Informazioni locali**e tocca**OK**.

4.5.4 Esportazione/Importazione

È possibile esportare record di sblocco e record di allarme su USB ed esportare o importare configurazioni tramite USB.

Passo 1 Nel menu principale selezionare**Informazioni**, quindi toccare**OK**.

Passo 2 Selezionare**Esportazione USB**e tocca**OK**.

Figura 4-26 Esportazione USB

Passaggio 3 Rubinetto↑o↓per selezionare l'elemento che si desidera esportare o importare.

Tabella 4-4 Descrizione dell'esportazione USB

Parametro	Descrizione
Esporta tutti i record di sblocco	Selezionare**Esporta tutti i record di sblocco**e tocca**OK**.
Esporta i record di sblocco per periodo	1. Selezionare**Esporta record di sblocco per periodo**e tocca**OK**. 2. Entra**Ora di inizio**e**Tempo scaduto**, rubinetto**OK**.
Esporta tutti i record di allarme	Selezionare**Esporta tutti i record di allarme**, rubinetto**OK**.
Esporta record di allarme per periodo	1. Selezionare**Esporta i record di allarme per periodo**e tocca**OK**. 2. Entra**Ora di inizio**e**Tempo scaduto**, rubinetto**OK**.
Esporta configurazione	Selezionare**Esporta configurazione**e tocca**OK**.
Importa configurazione	Selezionare**Importa configurazione**e tocca**OK**.

Azioni obbligatorie da intraprendere per la sicurezza di base della rete del dispositivo:

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.
- Includere almeno due tipi di caratteri; i tipi di carattere includono lettere maiuscole e minuscole, numeri e simboli.
- Non contenere il nome dell'account o il nome dell'account in ordine inverso.
- Non utilizzare caratteri continui, come 123, abc, ecc.
- Non utilizzare caratteri sovrapposti, come 111, aaa, ecc.

2. Aggiorna il firmware e il software client in tempo

- Secondo la procedura standard nell'industria tecnologica, si consiglia di mantenere aggiornato il firmware del dispositivo (come NVR, DVR, telecamera IP, ecc.) per garantire che il sistema sia dotato delle patch e delle correzioni di sicurezza più recenti. Quando il dispositivo è connesso alla rete pubblica, si consiglia di abilitare la funzione "auto-check for updates" per ottenere informazioni tempestive sugli aggiornamenti firmware rilasciati dal produttore.
- Si consiglia di scaricare e utilizzare l'ultima versione del software client.

Raccomandazioni "bello da avere" per migliorare la sicurezza della rete del dispositivo:

1. Protezione fisica

Ti suggeriamo di eseguire la protezione fisica del dispositivo, in particolare i dispositivi di archiviazione. Ad esempio, posizionare il dispositivo in una sala computer e in un armadietto speciali e implementare un'autorizzazione di controllo degli accessi e una gestione delle chiavi ben fatte per impedire a personale non autorizzato di effettuare contatti fisici come danni all'hardware, connessione non autorizzata di dispositivi rimovibili (come un disco flash USB , porta seriale), ecc.

2. Modifica regolarmente le password

Ti suggeriamo di cambiare regolarmente le password per ridurre il rischio di essere indovinato o violato.

3. Impostare e aggiornare le password Reimpostare le informazioni tempestivamente

Il dispositivo supporta la funzione di reimpostazione della password. Si prega di impostare le informazioni correlate per la reimpostazione della password in tempo, comprese le domande sulla casella di posta dell'utente finale e sulla protezione della password. Se le informazioni cambiano, si prega di modificarle in tempo. Quando si impostano le domande di protezione della password, si consiglia di non utilizzare quelle che possono essere facilmente indovinate.

4. Abilita il blocco dell'account

La funzione di blocco dell'account è abilitata per impostazione predefinita e ti consigliamo di mantenerla attiva per garantire la sicurezza dell'account. Se un utente malintenzionato tenta più volte di accedere con la password errata, l'account corrispondente e l'indirizzo IP di origine verranno bloccati.

5. Modifica HTTP predefinito e altre porte di servizio

Ti consigliamo di modificare HTTP predefinito e altre porte di servizio in qualsiasi set di numeri compreso tra 1024 e 65535, riducendo il rischio che estranei possano indovinare quali porte stai utilizzando.

6. Abilita HTTPS

Ti consigliamo di abilitare HTTPS, in modo da visitare il servizio Web attraverso un canale di comunicazione sicuro.

7. Collegamento indirizzo MAC

Ti consigliamo di associare l'indirizzo IP e MAC del gateway al dispositivo, riducendo così

il rischio di spoofing ARP.

8. Assegna account e privilegi in modo ragionevole

In base ai requisiti aziendali e gestionali, aggiungere ragionevolmente gli utenti e assegnare loro un set minimo di autorizzazioni.

9. Disabilita i servizi non necessari e scegli le modalità sicure

Se non necessario, si consiglia di disattivare alcuni servizi come SNMP, SMTP, UPnP, ecc., per ridurre i rischi.

Se necessario, si consiglia vivamente di utilizzare le modalità sicure, inclusi, a titolo esemplificativo ma non esaustivo, i seguenti servizi:

- SNMP: scegli SNMP v3 e imposta password di crittografia avanzata e password di autenticazione.
- SMTP: scegliere TLS per accedere al server delle cassette
- postali. FTP: scegli SFTP e imposta password complesse.
- Hotspot AP: scegli la modalità di crittografia WPA2-PSK e imposta password complesse.

10. Trasmissione crittografata audio e video

Se i tuoi contenuti di dati audio e video sono molto importanti o sensibili, ti consigliamo di utilizzare la funzione di trasmissione crittografata, per ridurre il rischio di furto di dati audio e video durante la trasmissione.

Promemoria: la trasmissione crittografata causerà una perdita di efficienza della trasmissione.

11. Controllo sicuro

- Controlla gli utenti online: ti suggeriamo di controllare regolarmente gli utenti online per vedere se il dispositivo ha effettuato l'accesso senza autorizzazione.
- Controlla il registro del dispositivo: visualizzando i registri, puoi conoscere gli indirizzi IP che sono stati utilizzati per accedere ai tuoi dispositivi e le loro operazioni chiave.

12. Registro di rete

A causa della limitata capacità di archiviazione del dispositivo, il registro memorizzato è limitato. Se è necessario salvare il registro per un lungo periodo, si consiglia di abilitare la funzione del registro di rete per garantire che i registri critici siano sincronizzati con il server del registro di rete per la traccia.

13. Costruire un ambiente di rete sicuro

Per garantire al meglio la sicurezza del dispositivo e ridurre i potenziali rischi informatici, si consiglia di:

- Disattivare la funzione di mappatura delle porte del router per evitare l'accesso diretto ai dispositivi intranet dalla rete esterna.
- La rete dovrebbe essere partizionata e isolata in base alle effettive esigenze della rete. Se non ci sono requisiti di comunicazione tra due sottoreti, si consiglia di utilizzare VLAN, GAP di rete e altre tecnologie per partizionare la rete, in modo da ottenere l'effetto di isolamento della rete.
- Stabilire il sistema di autenticazione degli accessi 802.1x per ridurre il rischio di accesso non autorizzato alle reti private.
- Abilitare la funzione di filtraggio degli indirizzi IP/MAC per limitare l'intervallo di host autorizzati ad accedere al dispositivo.