

Manuale utente MA300



Versione: 1.1

Data: Ottobre 2010

Informazioni su questo documento:

Questo documento introduce le operazioni del dispositivo di controllo di accesso. Per l'installazione del prodotto, consultare la guida all'installazione correlato. Per il funzionamento del software, consultare il manuale utente del software.

Simboli convenzionali:

Questo documento include tali simboli convenzionalmente come suggerimenti, avvisi importanti e le precauzioni. Le notazioni contenute in questo manuale sono:



Indica informazioni importanti, comprese le precauzioni, che devono essere lette attentamente per ottenere le prestazioni ottimali attrezzature.



: Indica che il messaggio vocale venga generato dal dispositivo. In caso di discrepanza tra le istruzioni vocali in questo documento e quelli generati dai prodotti reali, prevalgono queste ultime.

Indice dei contenuti

1. Istruzioni per l'uso 1
 1. Finger Placement. 1
 2. Istruzioni per la carta magnetica 2
 3. Precauzioni 2
2. Introduzione del dispositivo 3
 1. Panoramica delle funzioni del dispositivo 3
 2. Aspetto del prodotto 4
 3. L'uso di una tastiera USB esterna 6
 4. Stato di verifica 7
 5. Management Card 7
 6. Password di sistema 8
 7. Timeout operazione. 9
3. Operazioni dispositivo 10
 1. Management Card 10
 1. Iscrivere una scheda di gestione 10
 2. Iscriviti un utente normale 11
 3. Eliminare un singolo utente 17
 2. Operazioni con la tastiera USB 20
 1. Impostare Tastiera password 20
 2. Iscriviti un utente tramite tastiera 21
 3. Eliminare un utente specificato 25
 4. Eliminare tutti gli utenti 27
 5. Ripristina impostazioni predefinite 27
 3. Accesso Funzione di controllo 28
 4. Verifica utente 30
 5. U-disc 33
 6. Interruttore Tamper 35
4. Appendice 36
 1. Lista dei parametri 36
 2. Anti-Passo Indietro ★ 37
 3. Dichiarazione dei diritti dell'uomo e Privacy 40
 4. Environment-Friendly Usa Descrizione 42

1. Istruzioni per l'uso

1. Finger Placement

Dita raccomandati: il dito indice, dito medio e l'anulare, il pollice e il mignolo non sono raccomandati (perché di solito sono goffi sulla schermata di raccolta delle impronte digitali).

1. Una corretta posizione delle dita:
2. Posizione delle dita improprio:

Slanting

: Il numero utente. ** Cancellazione è successo.

%: Il sistema ritorna allo stato di verifica.

Non opaca sulla superficie

Off-center

: Registrazione utente. Si prega di inserire il numero utente.

%: La registrazione è riuscita.

Il dito è piatto in superficie e centrato nella guida dita.

Off-center

Backspace

ase si riferiscono alla



Si prega di iscriversi e verificare le impronte digitali utilizzando la modalità di posizionamento corretto delle dita. Noi non potrà essere ritenuta responsabile per eventuali conseguenze derivanti dal degrado delle prestazioni di verifica a causa di operazioni di utilizzo improprio. Ci riserviamo il diritto di interpretazione finale e revisione di questo documento.

2. Istruzioni per la carta magnetica

Integrato con un modulo senza contatto RF lettore di schede, questo dispositivo supporta le carte d'identità e carte MIFARE (opzionale e viene usato solo come carte d'identità). Con l'offerta di molteplici modalità di verifica, come le impronte digitali, carta di RF e di impronte digitali + verifica della carta di RF, questo dispositivo può soddisfare le esigenze degli utenti diversificate.

Strisciare la carta in tutta l'area del sensore dopo il prompt di voce e rimuovere la scheda dopo che il dispositivo ha intuito. Per la zona magnetica, vedere [2.2 Prodotto](#) Aspetto.

3. Precauzioni

Proteggere l'apparecchio dall'esposizione alla luce solare diretta oa forte fascio di luce forte influenza notevolmente la raccolta di impronte digitali e porta al fallimento verifica delle impronte digitali.

Si raccomanda di utilizzare il dispositivo in una temperatura di 0-50 ° C in modo da ottenere le prestazioni ottimali. In caso di esposizione del dispositivo verso l'esterno per lunghi periodi di tempo, si consiglia di adottare ombrellone e strutture dissipazione di calore poiché la temperatura troppo alta o troppo bassa può rallentare il funzionamento del dispositivo e di conseguenza in alta percentuale di scarto falso (FRR) e tasso di accettazione falso (FAR).

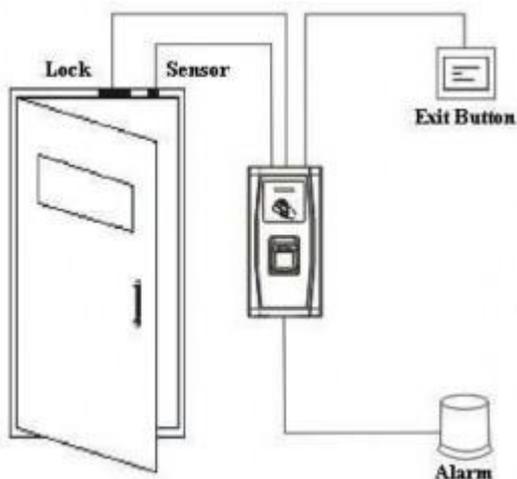
Durante l'installazione del dispositivo, collegare il cavo di alimentazione **dopo aver collegato** gli altri cavi. Se il dispositivo non funziona correttamente, assicurarsi di spegnere l'alimentazione **prima** di eseguire la manutenzione. Si noti che qualsiasi lavoro vivo-linea può danneggiare il dispositivo e il dispositivo di danni derivanti da lavorazioni dal vivo linea cade al di là della portata della nostra garanzia normale. Per le materie che non sono contemplate nel presente documento, si prega di fare riferimento ai materiali connesse, compresi la guida all'installazione, il controllo manuale del software di accesso.

2. Introduzione del dispositivo

1. Panoramica delle funzioni dello strumento

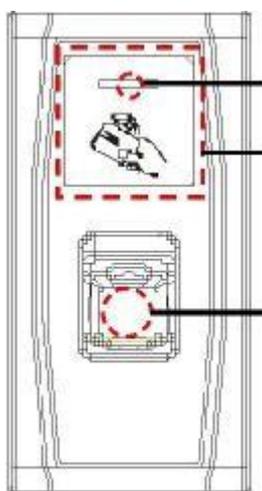
Come un'impronta digitale integrato e dispositivo di controllo di accesso, il nostro prodotto può essere collegato sia con una chiave elettronica o un controller di accesso. Questo dispositivo offre operazioni semplici e flessibili e supporta l'uso di schede di gestione. Con una scheda di gestione, è possibile eseguire tali funzioni come linea di iscrizione, la cancellazione e la gestione del U-disc. Il vocale guideranno l'utente attraverso tutte le operazioni senza visualizzazione su schermo. Questo dispositivo permette di collegare una tastiera esterna e offre molteplici modalità di funzionamento. Supporta la funzione di controllo di accesso per una gestione della sicurezza. E supporta diverse modalità di comunicazione. L'U-disco comprende operazioni semplici e convenienti. Il design impermeabile e cassa in metallo del dispositivo consentono di sopportare un impatto pesante senza danni.

Caratterizzato da un design semplice e compatto, questo dispositivo consente agli utenti di connettere più dispositivi attraverso un PC e di eseguire il monitoraggio in tempo reale.



2. Aspetto del prodotto

Vista frontale:



isultati e situazioni eccezionali, che sono definite come segue:

Regole comuni: se una operazione riesce, l'indicatore verde

Indicatore LED

un secondo; altrimenti, l'indicatore rosso è solida su per un secondo.

Stato Iscrizione: Il LED verde lampeggia tre volte ogni oth

secondo.

Singolo u

secondo. **verificat i**

- **Zona swipe card:** si riferisce alla zona della linea tratteggiata rossa bo

hown nella figura sopra. ☒

Sensore di impronte digitali: U

SERS.

: Eliminare gli utenti. Si prega di inserire il numero utente.

Reg: strazione è successo. Il sistema ritorna allo stato di verifica.

: Conferma password è successo.

%: User intorpidisce e w r ipe scheda Errore di area.

: Il numero utente. ** Cancellazione è successo.

: Verificare gli utenti. Si prega di premere il dito o perforare la carta.

%: Si prega di perforare nuovamente la scheda.

%: Si prega di riprovare.

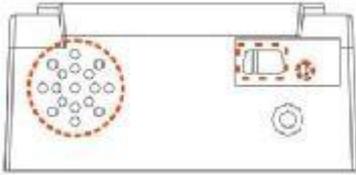
FP Sensore %: il numero utente **, Grazie.

%: Si prega di perforare nuovamente la scheda.

W



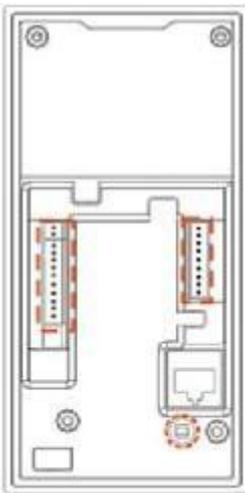
B



Pulsante Reset: Serve per riavviare il dispositivo.

Speaker: Usato per riprodurre il segnale acustico e la voce

asini della verifica, viene emesso un segnale diffusori una volta che, se l'utente non riesce a passare la verifica, i segnali acustici dei diffusori due volte. L'impostazione predefinita indicazioni durante l'uso: bip + vocali **Vista posteriore.:**



n

bili.

- **TC**

Interruttore Tamper: Usato per generare un allarme manomissione. Per dettagli, vedere [3.6](#) ☒

Interruttore Tamper: Usato per generare un allarme manomissione. Per dettagli, vedere [3.6 Tamper Switch](#).

DIP switch: Il DIP switch è dotato di quattro perni numerati 1, 2, 3 e 4. Nella

RS485 comm

numero di dispositivo hardware e il quarto pin è usato per selezionare lo stato di resistenza del terminale. Per le impostazioni dettagliate, vedere la guida per l'installazione. **2.3 Utilizzo di una tastiera USB esterna**

T

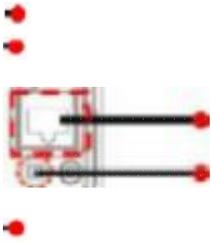
NPloetaicsee: non aggiornare il firmware a vostra discrezione, perché può portare problemi e pregiudicare il normale utilizzo del dispositivo. Contatta i nostri distributori per supporto tecnico o la notifica di aggiornamento.

Pulsante Reset Speaker

Interruttore Tamper DIP switch

through ply

%o:



Per facilitare le operazioni di dispositivi, è possibile collegare la tastiera devicUSB (acquistati dagli utenti) e

Spostare le operazioni fondamentali come l'iscrizione dell'utente, la cancellazione e il ripristino impostazioni di fabbrica, soprattutto quando si specificano gli ID utente durante la registrazione degli utenti e la cancellazione.



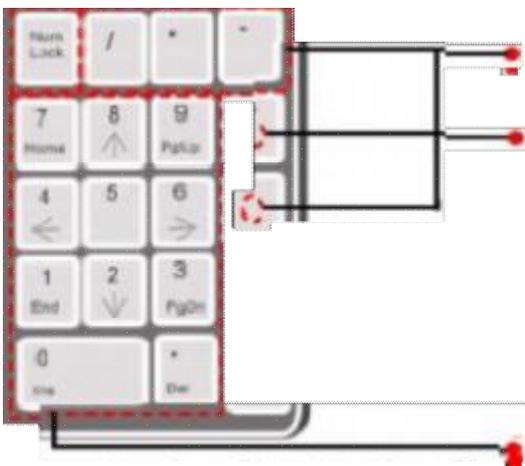
p

BLOC NUM è un tasto di commutazione tastierino numerico. Si è attivata di default. Se è

attivato,

OPERATIVO

2. In modalità di iscrizione basata tastiera con un ID utente specificato, quando si preme **ESC**, il sistema ritorna allo stato di iscrizione e genera un prompt alla voce "%o: gli utenti Registrati. Si prega di inserire il numero utente. "Si può registrare un ID utente e premere il tasto **ESC**. Poi, il sistema genera un prompt alla voce "%o: Il sistema ritorna allo stato di verifica."



e (ple

1. No U-disk o tastiera esterna sono collegati:

- Strisciando il Management

tastiera esterna, è possibile utilizzare solo i tasti numerici, il tasto backspace e

Inserisci chiave nello stato attivato NumLock. **2.4 Stato di Verifica**

Stato di verifica: stato di verification Dopo se si ha

carta o in caso di timeout di qualsiasi operazione. Nello stato di verifica, tutti gli utenti sono autorizzati a verificare la loro identità e sbloccare (l'amministratore recante una scheda di gestione e

impronte digitali (s) precedentemente iscritto), l'amministratore può eseguire operazioni come utente di iscrizione / cancellazione, gestione di U-disk e il funzionamento della tastiera **2.5 scheda di gestione.**

Gli utenti dei dispositivi sono classificati **amministratori**: un amministratore tra utente iscrizione / cancellazione (cancellazione di tutti gli altri utenti, tranne lui / h

e U-disk gestione. I privilegi degli amministratori del dispositivo sono attuate attraverso le schede di gestione **degli utenti ordinari**.. Gli utenti ordinari sono solo permesso di verificare la loro identità e sbloccare.

Una scheda di gestione è una scheda appositamente assegnato per un super amministratore.

Ciascun de

carta è iscritto, non è possibile eseguire alcuna operazione e il sistema genererà un messaggio vocale "%o: registrare la scheda di gestione prega". **È possibile implementare funzioni diverse da strisciata una scheda di gestione per tempi diversi in una riga:**

stato di iscrizione.

Facendo scorrere la scheda di gestione per cinque volte di fila, è possibile immettere il singolo utente

. U-disk è collegato: Con strisciare la gestione

stato di gestione.

. Una tastiera esterna sia collegata: Strisciando il m

tastiera.

fendenti onsecutive: swipes consecutivi significano l'intervallo tra due colpi in un

Le schede di gestione possono essere eliminati attraverso il "Clear All" funzione della tastiera, o hanno la loro amministrazione priv

prima di essere eliminati come carte di identità comune. Per i dettagli, consultare il manuale utente del software di controllo di accesso. Le impronte digitali dell'utente che ha una scheda di gestione possono essere iscritti tramite software o tastiera Enro

Un dispositivo senza carta di gestione, se ha la password tastiera, è possibile attivare la tastiera esterna e enro

Nota: utenti che portano le schede di gestione può solo Verif e u **2.6 Sistema**

Parola d'ordine

Una password di sistema è un padata in TCP / IP o RS485 com

 **Nota:**  La password di sistema può essere modificata tramite il controllo degli accessi 

software. Per i dettagli, consultare il manuale utente del software di controllo di accesso.

2.7 Timeout Operazione

Il tempo di timeout di funzionamento di default è 30 secondi. Quando ci si iscrive una scheda di gestione o di eliminare / iscriversi a un utente (anche nella iscrizione tastiera esterna e cancellazione stati utente), il sistema richiede automaticamente una volta ogni 10 secondi se non vi è alcuna operazione e ritorna al

Stato di verifica dopo che richiede tre volte. Il sistema di navigazione è "%: timeout operazione. Il sistema ritorna allo stato di verifica".

 **Nota:**  È possibile impostare il tempo di timeout attraverso il software di controllo di accesso. 

1. Operazioni dispositivo

1. Scheda di gestione

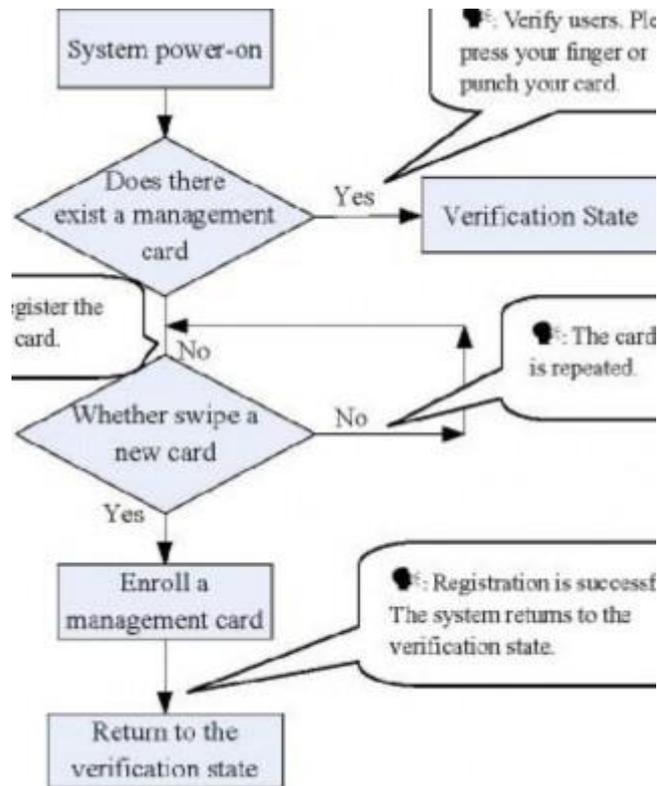
1. Iscrivere una scheda di gestione

Per iscrivere una scheda di gestione, procedere come segue:

1. Il dispositivo rileva automaticamente se esiste una scheda di gestione.
2. Se il dispositivo non riesce a rilevare la presenza di una scheda di gestione, esso entra nello stato di registrazione scheda di gestione. Quindi procedere con il passo 3, altrimenti il sistema genera un prompt alla voce "%: Verificare gli utenti. Si prega di premere il dito o perforare la carta".
3. Dopo che il sistema genera il messaggio vocale "%: registrare la scheda di gestione prega", è possibile strisciare la carta in tutta l'area del sensore.
4. Se l'iscrizione non riesce, il sistema genera un prompt alla voce "%: il numero della carta si ripete" e torna al punto 3, se l'iscrizione ha successo, il sistema genera un prompt alla voce "%: La registrazione è riuscita. Il sistema ritorna allo stato di verifica".

 **Nota:**  Il sistema ritorna allo stato di verifica se ogni operazione nella fase 3 volte fuori e  chiede solo di registrare nuovamente la scheda di gestione dopo aver riavviato il dispositivo. 

Si riporta il flusso di iscrizione scheda di gestione:



2. Iscriviti un utente normale

Il modo per voi di entrare nello stato di iscrizione utilizzando il
 m. In un ennesimo a i s e g m o d n e t, c y una o r dum i c s aa k nn n aogn w ely n me un
 en s nrt t o h CLL e aordneenursoelrlm. Wenhten si registra un
 nuovo utente, il sysmtemodeautomatically assegna un ID di minimo per l'utente. Inoltre, è

può anche usare
 iscrizione tastiera esterna
 (Per i dettagli,

t) 3 h. t e 2o.2imEpnleromlleantU m usse o rono d rT e ehnrrooullgmhent di ID specificato.

Tastiera
 vedere

Ve: utenti rify. Si prega di premere il dito o perforare la carta.

: Il numero di record è pieno / Il numero di carta è ripetuta / La scheda è stato registrato /
 L'impronta digitale è ripetuto.

PI: facilità registrare la scheda di gestione.

: Il numero utente. ** Registrati. Si prega di premere il dito o perforare la carta. (Si prega di
 premere il dito.)

%o: Registrati. Si prega di premere il tuo
 dito o pugno la carta / Si prega di premere il dito / Si prega di perforare la carta.

L': numero della carta è ripetuto.

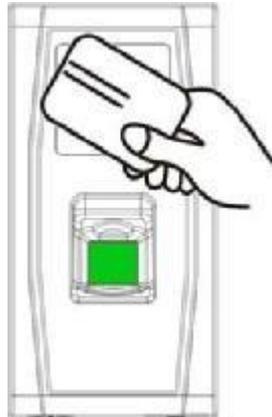
: Errore di password

In entrambe queste due modalità di iscrizione, è possibile iscrivere nuovi utenti. Ogni utente
 è consentito di iscriversi 10 impronte digitali e una carta ID al massimo.

Per iscriversi a un utente, procedere come segue:

1. Nello stato di verifica, il sistema va in ordinario stato di iscrizione utente dopo strisciare una carta di gestione una volta (Nello stato di iscrizione, strisciare una carta di gestione una volta che si ritorna allo stato di verifica).

2. Dopo che il sistema genera un prompt alla voce "%o: Registra gli utenti. Si prega di premere il dito o perforare la carta ", è possibile avviare la registrazione dell'utente. Ci sono due casi seguenti:



3. Swipe carta d'identità prima

1. Quando si striscia la nuova carta d'identità e riuscire a iscriversi a un utente, il dispositivo genera un messaggio vocale " : Il numero utente. ** La registrazione è successo! "(** Si riferisce alla ID assegnato automaticamente l'utente dal sistema; stessa di seguito) e si può passare alla fase b, se si passa il dito un

e: nUrsoellr ndulmDbcearrd **, Rtheegissytesrte.
mPlegaesneerparteesstyhoevroficnegepr! o "manpdt" inserire il especificied stato di registrazione dell'utente.

"Registrazione utenti. Si prega di premere il dito o strisciare la carta.

1. Se si inserisce una password errata per sei volte consecutive, la tastiera verrà bloccata e sarà necessario per alimentare la tastiera di nuovo per sbloccarla.

2. Se non ci sono combinazioni di tasti entro 3 secondi dopo l'attivazione della tastiera, le funzioni della tastiera viene automaticamente disattivata e sarà necessario riattivarla.

2. Dopo che il dispositivo genera un prompt alla voce "%o: Registrati. Si prega di premere il dito ", il sistema entra nello stato di registrazione delle impronte digitali specificato. Premere lo stesso dito sul sensore per tre volte seguendo le istruzioni vocali.

3. Se registrazione delle impronte digitali ha successo, il sistema genera un prompt alla voce "%o: La registrazione è riuscita. Registrati. Si prega di premere il dito "ed entra direttamente lo stato successivo registrazione delle impronte digitali, impronte digitali, se l'iscrizione non riesce, il sistema genera un prompt alla voce" %o: L'impronta digitale viene ripetuto "e ripete il passo b.

4. Il sistema ritorna automaticamente allo stato di verifica quando entrambe le 10 dita e carta ID sono iscritti, o la scheda di gestione è fregato una volta o il funzionamento timeout.

4. Dito premere prima

5. Premere lo stesso dito sul sensore per tre volte seguendo le istruzioni vocali, adottando il corretto posizionamento delle impronte digitali. Se registrazione delle impronte digitali ha successo, il sistema genera un prompt alla voce "%: il numero utente. ** La registrazione è successo "e si può passare alla fase B; se registrata l'impronta digitale prima, il sistema genera un prompt alla voce "%: il numero utente **; Registrazione, premere il dito o perforare la carta" ed entrare nello stato di iscrizione utente specificato.

6. Dopo aver generato il prompt la voce "%: Registrati. Si prega di premere il dito o perforare la carta ", il sistema inserisce le informazioni dell'utente stato iscrizione specificato, in attesa di strisciare la nuova carta d'identità o di premere il dito.

7. Se l'iscrizione carta d'identità ha successo, il sistema genera il messaggio vocale ": La registrazione è riuscita. Si prega di premere il dito "e

passa allo stato registrazione delle impronte digitali direttamente, se si preme un dito che non è iscritto prima e riesce a iscrizione di questo dito, il sistema genera il messaggio vocale: "

: La registrazione è riuscita. Si prega di premere il dito o perforare la carta "e si può continuare ad iscrivere nuove impronte digitali e di carte. Dopo aver registrato 10 impronte digitali, il sistema genererà il messaggio vocale "

: Si prega di perforare la carta "per iscrivere la vostra carta d'identità se la carta d'identità non è iscritto.

8. Il sistema ritorna automaticamente allo stato di verifica quando entrambe le 10 dita e carta ID sono iscritti, o la scheda di gestione è fregato una volta o il funzionamento timeout.

3. Se sei già assegnato con un numero utente, poi ci sono i due casi seguenti:

9. Iscrivere impronte digitali (s) quando si è già iscritto scheda

1. Dopo aver strisciare la carta iscritti, il sistema genererà il messaggio vocale "%: il numero utente. ** Registrati. Si prega di premere il dito "(** indica l'ID assegnato a te, sotto lo stesso) e di entrare nello stato di registrazione delle impronte digitali ..

2. Premere lo stesso dito sul sensore per tre volte seguendo le istruzioni vocali, adottando il corretto posizionamento delle impronte digitali. Se registrazione delle impronte digitali ha successo, il sistema genera un prompt alla voce "%: il numero utente. ** La registrazione è successo ", e si prepara per l'iscrizione di successiva impronte digitali.

3. Il sistema ritorna automaticamente allo stato di verifica quando entrambe le 10 dita e carta ID sono iscritti, o la scheda di gestione è fregato una volta o il funzionamento timeout.



4. Se l'utente registrazione di un'impronta digitale che è ripetuta con la propria impronta digitale, il nuovo sovrascrive l'impronta digitale precedentemente iscritti.

5. In questa modalità, l'impronta digitale dell'utente che porta la scheda di gestione non può essere iscritto perché strisciando la carta gestione restituirà il sistema allo stato di verifica automaticamente.

10. Iscrivere carta e impronte digitali (s) quando si è già iscritti impronte digitali (s)

11. Premere il dito con impronte digitali già iscritti tre volte seguendo le istruzioni vocali. Se sei identificato come la stessa persona in ogni tentativo di verifica, il sistema entra nello stato di registrazione delle impronte digitali.

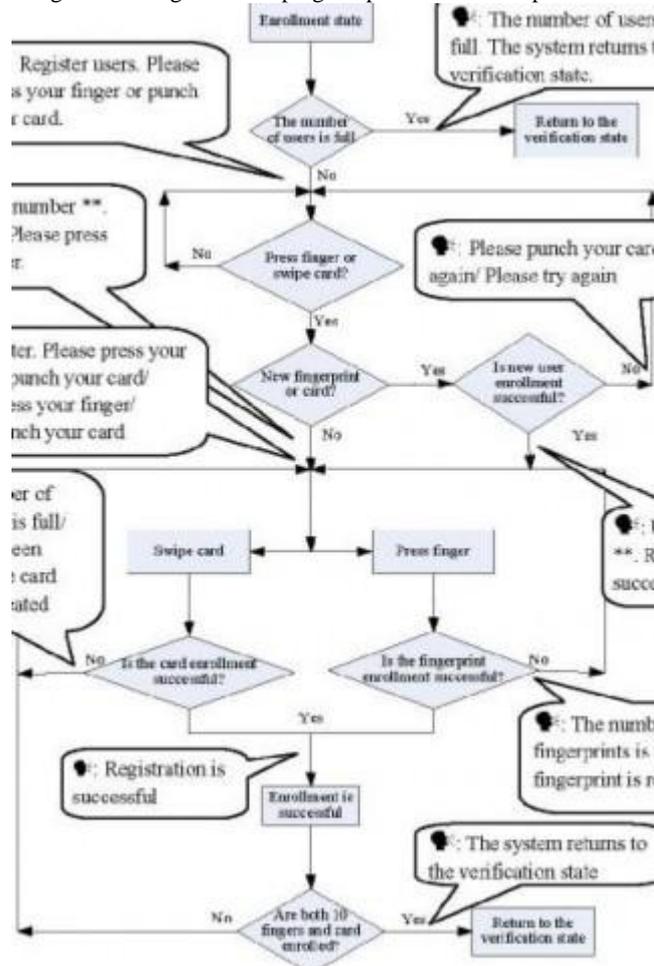
12. Dopo aver generato il prompt la voce "%: il numero utente. ** Registrati. Si prega di premere il dito o perforare la carta ", il sistema inizia a registrare le impronte digitali.

13. Se l'iscrizione carta d'identità ha successo, il sistema genera un prompt alla voce "%: La registrazione è riuscita. Registrati. Si prega di premere il dito "ed entra direttamente lo stato registrazione delle impronte digitali, se si preme un dito che non si sono iscritti prima e riesce a iscrizione di questo dito, il sistema genera il messaggio vocale:" "%: La registrazione è riuscita. Si prega di premere il dito o perforare la carta "e si può continuare ad iscrivere nuove impronte digitali e di carte. Dopo aver registrato 10 impronte digitali, il sistema genererà un prompt alla voce "%: Si prega di perforare la carta" per iscrivere la tua carta d'identità se la carta d'identità non è iscritto.

14. Il sistema ritorna automaticamente allo stato di verifica quando entrambe le 10 dita e carta ID sono iscritti, o la scheda di gestione è fregato una volta o il funzionamento timeout.

Il diagramma di flusso è la seguente:

%: gli utenti Registrati. Si prega di premere il dito o perforare la carta.



%: Il numero di utenti è piena. Il sistema ritorna allo stato di verifica.

%: il numero utente. ** Registrati. Si prega di premere il dito.

% Registrati. Si prega di premere il dito o perforare la carta / Si prega di premere il dito / Si prega di perforare la carta

: Il numero di carte laminate è pieno / scheda e 'stato gistrati / mber La scheda è ripetuta

%: Si prega di perforare la carta di nuovo / Riprova

%: il numero utente

** La registrazione è riuscita

%: La registrazione è riuscita

%: il numero di iscritti impronte digitali è pieno / L'impronta digitale è ripetuto

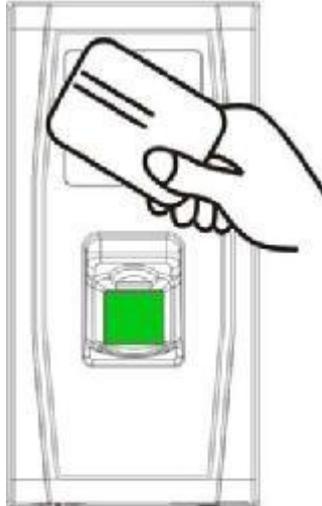
%: il sistema ritorna allo stato di verifica

3. Eliminare un singolo utente

Eliminazione di un utente utilizzando una scheda di gestione è chiamato il **semplice modo di eliminazione del singolo utente**. Eliminazione di un utente mediante una tastiera esterna viene chiamata la **modalità di cancellazione dell'account utente specificato**. (Vedi [3.2.3 Eliminazione di un utente specificato](#)).

Gli step operativi per la semplice cancellazione singolo utente:

1. Nella verifica dello stato, strisciare la carta di gestione per cinque volte consecutive per entrare nel semplice stato di delezione singolo utente (strisciare la carta ancora una volta per tornare allo stato di verifica).



2. Il sistema genererà la voce Prompt "%: eliminare utenti. Si prega di premere il dito o perforare la carta. "

3. Premere il dito sul sensore di impronte digitali o di strisciare la carta nel lettore di schede.

4. Premere il dito sul sensore per eliminare un utente.

Premere una delle dita registrate correttamente sul sensore. Se l'

: VeUrsifeicrantiuomn bseurc * c * e. eDdesl, etihoensistuecmcewsisllfugle.
 nDeeraletteetuhseevrso.icPeleparosme prte "ss il dito o un pugno la vostra carta."
 (** indica il numero ID dell'utente) e ritornare automaticamente allo stato di
 eliminazione. Se la verifica ha esito negativo, il sistema genererà il messaggio
 vocale "

: Si prega di riprovare. "

%o

1. La tastiera deve essere inserita o rimossa in un intervallo di più di 15 secondi, altrimenti il sistema non può identificare il suo stato.



Strisciare la carta di gestione per cinque volte consecutive

"Elimina gli utenti. Si prega di premere il dito o scheda punchyour. "

5. Strisciare la carta sul lettore per eliminare un utente.

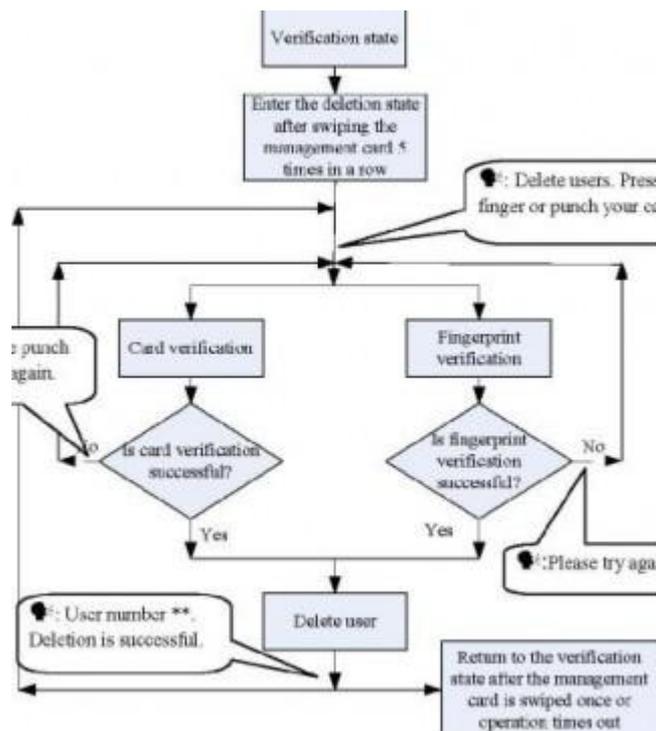
Strisciare una carta di credito registrata sul lettore. Se la verifica ha esito positivo, il sistema genererà un prompt alla voce "%o: il numero utente. ** Cancellazione è successo. Cancellare utenti. Si prega di premere il dito o strisciare la carta. "E ritorna automaticamente allo stato di eliminazione. Se la verifica ha esito negativo, il sistema genererà un prompt alla voce "%o:. Si prega di perforare nuovamente la scheda"

6. Se si strisciare la carta di una gestione più tempo o le timeout dell'operazione, il sistema ritorna allo stato di verifica.



Nota: In semplice modalità di eliminazione single-user, utenti della carta di gestione non possono essere eliminati perché strisciando la carta gestione restituirà il sistema allo stato di verifica.

Semplice procedura di cancellazione utente singolo:

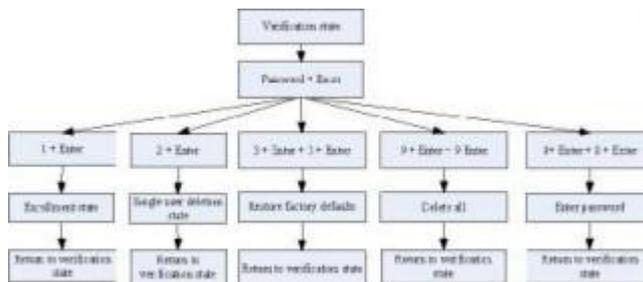


%: Elimina utenti. Premere il dito o perforare la carta.

%: Si prega di riprovare.

2. Operazioni con la tastiera USB

Le operazioni di tastiera diagramma di flusso è la seguente:



1. Impostare Tastiera password

Se l'utente ha bisogno di una tastiera esterna, lui / lei può collegare la tastiera al dispositivo e poi strisciare la carta di gestione per attivare la tastiera esterna.

Il sistema consente all'utente di impostare una password dedicata per la tastiera esterna.

Punti di funzionamento:

1. In stato di verifica, collegare una tastiera esterna con il dispositivo attraverso l'interfaccia USB.

2. Strisciare la carta di gestione, una volta per attivare la tastiera. Il sistema genera un prompt alla voce "%: Si prega di premere il tasto della tastiera"

3 bis. gTayipne. Tinhe "8s" yasntedmprgeesnsereantetesrt.hTehveonictypperoinm "p8t" "e premere Invio

.. Si prega di impostare la password "Digitare la password desiderata e premere

. Il sistema genera la voce promEpt t "er

: L'operazione è riuscita. Il sistema torna

stato di verifica. "Se non ci sono combinazioni di tasti entro 30 secondi, il sistema genera il messaggio vocale"

: Timeout operazione. Il sistema ritorna allo stato di verifica. "(
La password deve avere una lunghezza compresa tra 4 e 6 cifre.

)

L'utente può inserire questa password per attivare le funzioni della tastiera esterna al successivo utilizzo, o strisciare una carta di gestione una volta (che è obbligatorio per il primo utilizzo della tastiera esterna).

2. Iscriviti un utente tramite tastiera

Iscrivere un utente utilizzando una tastiera USB è chiamata **modalità di iscrizione basata tastiera**. In questa modalità, l'utente può registrare un utente con l'ID utente specificato.

Punti di funzionamento:

1. Come mostrato in [3.2 USB Keyboard](#) diagramma di flusso [Operations](#), digitare "1" e premere **Invio** per entrare nello stato di iscrizione.
2. Quando il sistema genera un prompt alla voce "%o: Registra gli utenti. Si prega di inserire il numero utente. ", Immettere un ID utente.
3. UTsheer nsuymstbemer g ** e.nReeragtiestsetrhuesveorsic.ePpleraosmeppt r "WorldSofting il dito o perforare la carta". (** Indica l'ID numero dell'utente; stessa di seguito) Il sistema entra nello stato di iscrizione ID specificato.

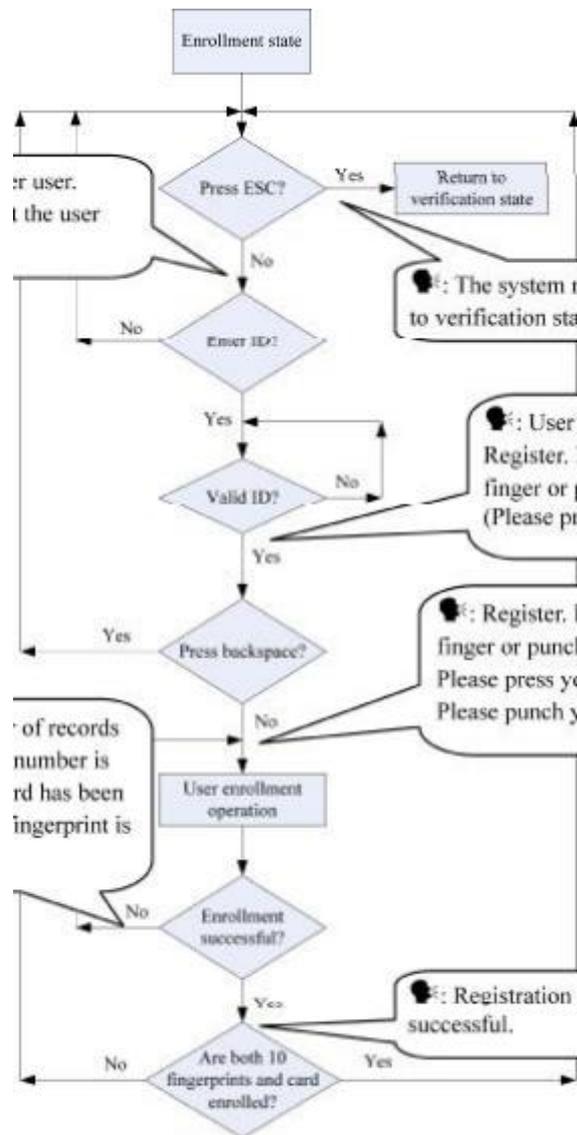


3. Se un utente si è iscritto al sistema con una scheda di gestione, il sistema genererà il messaggio vocale "%o: il numero utente. ** Si prega di premere il dito. "
4. Se un utente si è iscritto al sistema con un ID utente e 10 impronte digitali, il sistema genererà il messaggio vocale "%o: il numero utente. ** Si prega di perforare la carta. "
5. L'utente iscriversi funzionamento nello stato di iscrizione ID specificato è simile alla ID specificato iscriversi funzionamento nella modalità di iscrizione scheda di gestione. Per dettagli, vedere [3.1.2 Enroll un utente normale](#).
6. Nel ID utente standby iscritti, premere **ESC** per tornare allo stato di verifica. Nello stato di iscrizione ID utente specificato, premere **ESC** due volte per tornare allo stato di verifica.



Nota: In modalità di iscrizione basata su tastiera, è possibile registrare gli utenti consecutivamente. In caso di superamento iscriversi, il sistema torna automaticamente allo stato di iscrizione.

La base di diagramma di flusso iscrizione tastiera è la seguente:



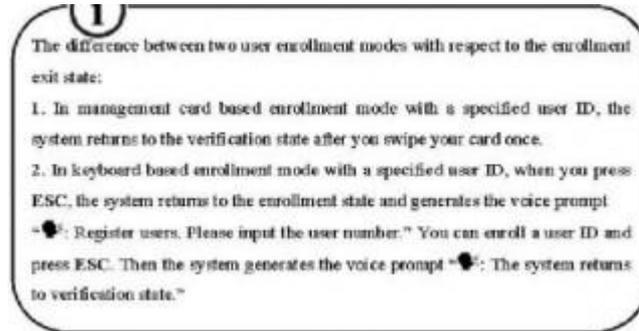
Dichiarazione importante:

1. In modalità di iscrizione a base della tastiera, se i tempi di qualsiasi operazione, il sistema richiede automaticamente di questa operazione una volta ogni 10 secondi e torna allo stato di verifica dopo che richiede tre volte.
2. Impronte digitali nuovi iscritti sovrascrivono quelli originali in carta di modalità di iscrizione Based Management, e la modalità di iscrizione basata tastiera allo stesso modo.
3. Un utente può registrare una sola scheda. Quando l'utente con una scheda iscritti iscrive nel sistema, il sistema genera un prompt alla voce "%: Registrati. . Si prega di premere il dito "Quando l'utente fa scorrere la carta, il sistema genera un prompt alla voce" %:. La scheda è stato registrato "

La differenza tra le due modalità di registrazione degli utenti per quanto riguarda lo Stato di uscita di iscrizione:

1. Nella scheda Modalità di iscrizione a base di gestione con un ID utente specificato, il sistema ritorna allo stato di verifica dopo che strisciare la carta di una volta.

- Una carta non può essere iscritto ripetutamente, altrimenti il sistema genererà un prompt alla voce "%o: il numero della carta si ripete". Durante la strisciata della carta. Diversi utenti non possono iscriversi la stessa impronta digitale, altrimenti il sistema genererà un prompt alla voce "%o: L'impronta digitale è ripetuto." Durante la registrazione delle impronte digitali. Nuove impronte digitali di un utente sovrascrivono quelle esistenti.



3. Eliminazione di un utente specificato

Eliminazione di un utente mediante una tastiera esterna viene chiamata la **modalità di cancellazione dell'account utente specificato**.

Punti di funzionamento:

- Collegare una tastiera USB al dispositivo, e strisciare la carta di gestione, una volta o immettere la password per attivare la tastiera.
- Premere il tasto "2" e **Invio** per accedere alla modalità di cancellazione dell'account utente specificato. il sistema genererà la voce Prompt "%o: eliminare utenti. Si prega di inserire il numero utente. "E si può procedere con il passo 3.

? **Avviso:** Caso particolare: se non ci sono utenti (includere utente scheda di gestione) iscritti, e si ha la password tastiera, è possibile utilizzare la password per attivare la tastiera e premere il tasto 2 e **Invio** per entrare nello stato di cancellazione dell'account utente, il sistema si generare la richiesta di voce "%o: No utente registrato. Il sistema ritorna allo stato di verifica ".

- Immettere un ID utente e il sistema verifica se l'ID utente valido.
- Se l'ID utente è valido, il sistema genera il messaggio vocale "%o: il numero utente. ** Cancellazione è successo. Cancellare utenti. Si prega di inserire il numero utente. "E ritorna automaticamente allo stato di eliminazione. Se l'ID utente non è valido, il sistema genererà un prompt alla voce "%o: ID utente non valido"

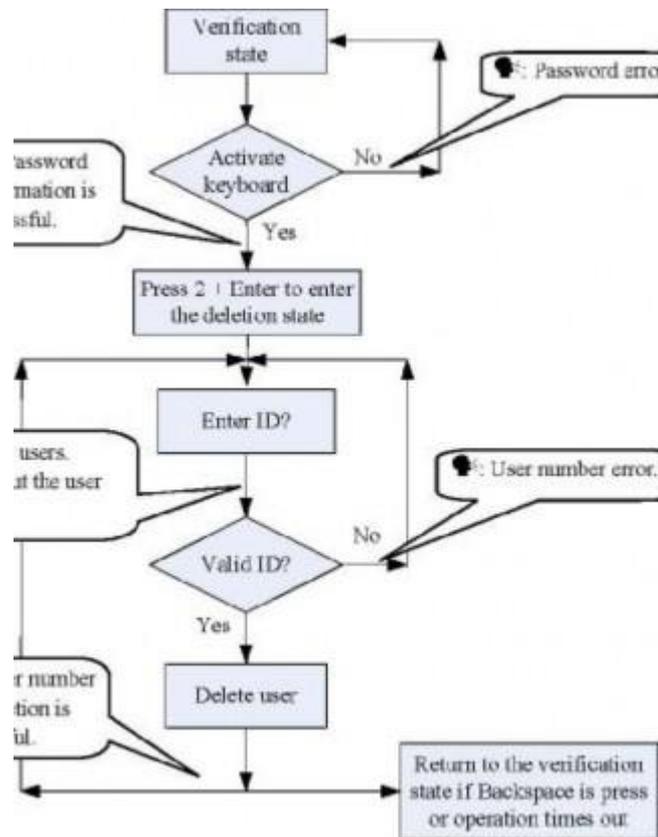
6. Se si preme **ESC** o vostri tempi di funzionamento, il sistema ritorna allo stato di verifica.



5. In modalità di eliminazione specificata utente, ID utente e la scheda di gestione ID utente che sono iscritti nel sistema sono tutti considerata non valida.

6. In modalità di eliminazione basata sulla tastiera, il sistema disattiva il sensore di impronte digitali e lettore di schede e quindi qualsiasi operazione su di essi non è valido.

L'utente diagramma di flusso eliminazione specificato di seguito è riportato:



4. Eliminare tutti gli utenti

Punti di funzionamento:

1. Collegare una tastiera USB al dispositivo, e strisciare la carta di gestione, una volta o immettere la password per attivare la tastiera.
2. Premere il tasto "9" e premere **Invio**. Quindi premere "9" e di nuovo **Invio**. Il sistema elimina tutti gli utenti.
3. Se l'operazione ha esito positivo, il sistema genererà un prompt alla voce "%: Elimina tutti gli utenti. L'operazione è riuscita. Il sistema ritorna allo stato di verifica. Si prega di registrare la scheda di gestione. "



Nota:

4. È possibile eliminare una scheda di gestione utilizzando la funzione All Elimina.
 5. È possibile utilizzare la funzione All Elimina per eliminare tutti gli utenti iscritti, le impronte digitali e le registrazioni.
- 3). Estrema cautela deve essere esercitata durante l'esecuzione di questa operazione, come una volta cancellati, i dati non possono essere recuperati.

5. Ripristina impostazioni predefinite di fabbrica

Punti di funzionamento:

1. Collegare una tastiera USB al dispositivo, e strisciare la carta di gestione, una volta o immettere la password per attivare la tastiera.
2. Premere il tasto "3" e premere **Invio**. Quindi premere "3" e di nuovo **Invio**. Il sistema ripristina le impostazioni di fabbrica.
3. Dopo l'operazione ha esito positivo, il sistema genera un prompt alla voce "%o: ripristinare le impostazioni predefinite. L'operazione è riuscita. Il sistema ritorna allo stato di verifica".

È inoltre possibile ripristinare le impostazioni predefinite di fabbrica reimpostando l'interruttore antimanomissione. Vedere [3.6 Interruttore antimanomissione](#).

Dopo che il dispositivo è stato ripristinato alle impostazioni di fabbrica, le informazioni sul dispositivo viene ripristinato alle impostazioni di fabbrica, compreso il numero del dispositivo, password di sistema, l'indirizzo IP, indirizzo 485, e la password tastiera.



Nota: Le informazioni utente memorizzate sul dispositivo non viene cancellato dopo che il dispositivo viene ripristinato alle impostazioni di fabbrica. 

1. L'accesso alle funzioni di controllo

Impostazione di controllo di accesso è quella di impostare il fuso orario aperto la porta di utente, blocco di controllo e parametri del dispositivo relativo.

Per sbloccare l'utente registrato deve essere conforme alle seguenti condizioni:

1. Il periodo di sblocco corrente dovrebbe essere nel tempo effettivo di fuso orario dell'utente o gruppo.
2. Il gruppo dove utente è necessario essere in controllo di accesso (o nello stesso controllo di accesso con altro gruppo, per aprire la porta insieme).

Il default del sistema il nuovo utente si iscrive, come il gruppo di prima, ora locale gruppo di default come 1, il controllo di accesso come il primo gruppo, e il nuovo utente registrato è in unlock (L'utente può modificare la relativa impostazione del controllo di accesso, attraverso il software di controllo di accesso).



Avviso: Il bisogno della funzione di controllo di accesso del dispositivo per impostare e modificare attraverso il software di controllo accessi, per i dettagli, si prega di fare riferimento al manuale utente del software. 

Accesso alle funzioni di controllo:

3. Access Control Time Zone:

Fuso orario è l'unità minima possibilità di controllo di accesso di. L'intero sistema può definire 50 fusi orari. Ogni volta zone definisce sette sezioni di tempo (vale a dire, una settimana). Ogni sezione di tempo è il fuso orario effettivo entro 24 ore tutti i giorni. Ogni utente può impostare tre fusi orari. "O" esiste

un **E m r r o r g t i m l u i e s t h r o e e u n a z l a o r n m e s**. Dlteifsineffteh cetimveaixf oenrrloyrotrnime eis allarme stoattisrifgiegde.r. Non è attraverso, e superare questi tempi definiti, il segnale di allarme quando la verifica

4. Accedere vacanze Ambito:

verrà attivato automaticamente.

Tempo di controllo di accesso speciale può avere bisogno durante il soggiorno. E' diverso per modificare il tempo di controllo di accesso di tutti. Così una vacanza di tempo di controllo di accesso può essere impostata, che è applicabile a tutti i dipendenti.

5. Accedere Gruppo Time Zone:

Raggruppamento è quello di gestire i dipendenti in gruppi. Impiegato in gruppi utilizzano il fuso orario di gruppo per impostazione predefinita. I membri del gruppo possono anche impostare il fuso orario dell'utente. Ogni gruppo può contenere i fusi orari. Il nuovo utente registrato appartiene al gruppo 1 di default e può anche essere assegnato ad altri gruppi.

6. Sblocca Combinazione Ambito:

Fai vari gruppi in accesso diversi controlli per raggiungere multi-verifica e migliorare la sicurezza. Un controllo di accesso può essere costituito da 5 gruppi al massimo.

7. Accedere ai parametri di controllo:

Bloccare Control Delay: applicare per determinare ora di sblocco, i min is20ms dell'unità misurata, in condizioni normali è di 100-200ms.

Modalità Anti-Pass: Può essere impostato su "Nessuno", "Out", "A", "InOut".

Lo stato di registrazione del Maestro: Può essere impostato su "Nessuno", "Out", "In".

Modalità Sensore: Set Mode Sensore porta. Può essere impostato su "Nessuno", "NOpen", stato "nChiudere".

Ritardo sensore: Impostare il tempo di ritardo del sensore quando la porta è aperta. Dopo questo tempo definito il sensore rileva lo stato della porta. Se lo stato della porta non è coerente verrà attivato l'allarme. Gamma dispositivo schermo in bianco e nero è 0-254. Colore gamma dispositivo dello schermo è 0-99.

Sensore di allarme: impostare il tempo di ritardo allarme dopo che l'allarme è attivato. L'intervallo è 0-999 secondi.

8. Impostazione indietro Anti-Pass:

Funzione di back Anti-Passo consultare [4.2 Anti-Pass indietro](#).

7. Disattivare l'allarme:

Quando il dispositivo è in stato di allarme, la verifica di utente può disattivare l'allarme, e il dispositivo si riprenderà stato normale. In caso contrario, si sveglia tutto il tempo.

Tipo di allarme: Allarme porta sensore e allarme manomissione.

2. Verifica utente

La verifica di default del dispositivo è FP / RF di verifica, l'utente può utilizzare il software di controllo di accesso per modificare la modalità di verifica per RF, FP o RF & verifica FP. Per i dettagli si prega di fare riferimento al manuale utente del software.

Punti di funzionamento:

1. Quando il dispositivo è in stato di verifica, il sistema genera un prompt alla voce "%: Verificare gli utenti. Si prega di premere il dito o perforare la carta. "
2. Avviare verifica utente. Il dispositivo supporta quattro modalità di verifiche: FP / RF, FP, RF e FP & RF verifica.
3. Verifica delle impronte digitali
Premere il dito sul sensore di impronte digitali in modo corretto. Se la verifica ha esito positivo, il sistema genera un prompt alla voce "%: il numero utente. ** Grazie. "E contemporaneamente attiva un segnale di sblocco. Se la verifica ha esito negativo, il sistema genera un prompt alla voce "%:. Riprova"
4. Verifica della carta
Strisciare la carta nel lettore di schede. Se la verifica ha esito positivo, il sistema genera un prompt alla voce "%: il numero utente. ** Grazie. "E contemporaneamente attiva un segnale di sblocco. Se la verifica ha esito negativo, il sistema genera un prompt alla voce "%:. Si prega di perforare nuovamente la scheda"
5. Fingerprint verifica + Card
Impostare la modalità di verifica utente per FP & RF attraverso il software di controllo accessi, l'operazione di verifica come segue:

Premere il dito prima:

Premere il dito sul sensore di impronte digitali in modo corretto. Se la verifica ha esito positivo, il sistema genera un prompt alla voce "%:. Numero utente **, Si prega di perforare la carta", dopo verifica della carta di successo, e contemporaneamente attiva un segnale di sblocco. Se la verifica ha esito negativo, il sistema genera un prompt alla voce "%:. Si prega di perforare nuovamente la scheda"

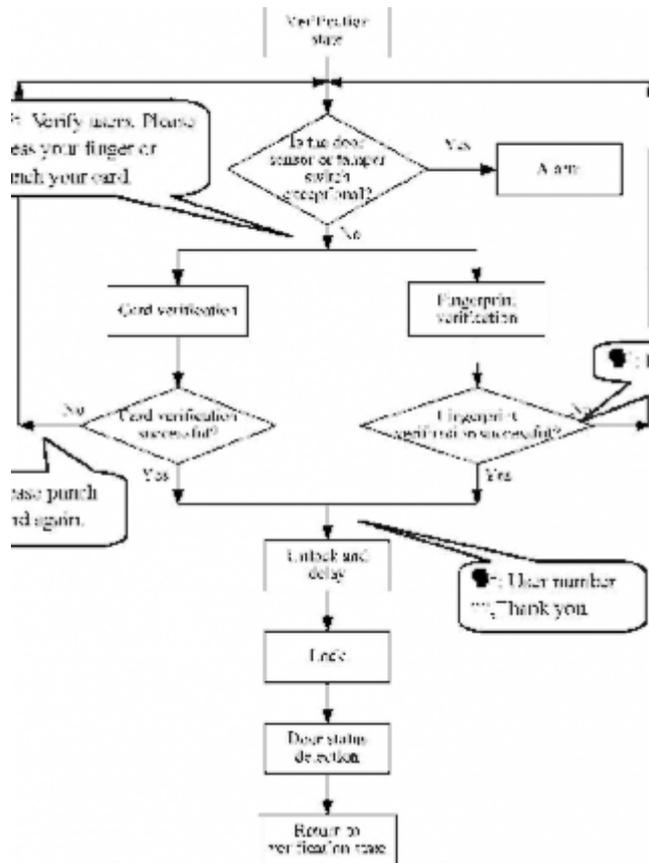
Swipe della carta prima:

Strisciare la carta nel lettore di schede. Se la verifica ha esito positivo, il sistema genera un prompt alla voce "%:. Numero utente **, Si prega di premere il dito" Dopo la verifica delle impronte digitali successo, e contemporaneamente attiva un segnale di sblocco. Se la verifica ha esito negativo, il sistema genera un prompt alla voce "%:. Riprova"

6. Verifica delle impronte digitali o scheda

Cioè, l'operazione di verifica di (1) o (2) sia efficaci.

L'utente diagramma di flusso di verifica è spettacolo, come di seguito:



⊠ Suggerimento: ⊠

7. Se l'utente non è nel fuso orario di controllo di accesso effettivo, non può verificare e sbloccare la porta, il sistema genera un prompt alla voce "%o: Time Zone valida"
8. Se l'utente non è utilizzare la modalità di verifica impostata per verificare, non può verificare e sbloccare la porta, il sistema genera un prompt alla voce "%o: Modalità di verifica non valido"

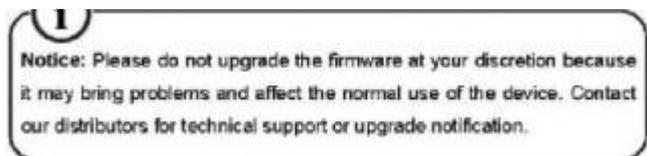
3. U-disc

L'utente può eseguire **download registrazioni**, **scaricare utente**, **utente di upload** e **aggiornamento del firmware** attraverso un U-disk.

1. **Record Scarica**: Scarica la partecipazione alle riunioni di tutti gli utenti dal dispositivo a un U-disk.
2. **SCARICA**: Scarica tutte le informazioni utente, come le impronte digitali e numeri di carta dal dispositivo a un U-disk.
3. **Caricare Utente**: Carica le informazioni utente da un U-disk al dispositivo.

4. Aggiornamento firmware: Aggiornare il firmware del dispositivo tramite un U-disk. I file di configurazione nella U-disk possono essere creati e modificati utilizzando

il software di controllo di accesso. L'operazione si prega di fare riferimento al manuale utente del software.



Operazioni di U-disk includono i seguenti due casi:

1. Se si collega un U-disk, senza file di configurazione per il dispositivo, il sistema richiede automaticamente le operazioni in sequenza.
 1. Dopo aver collegato un U-disk per il dispositivo, è possibile strisciare la carta una volta per entrare nello stato di gestione del U-disk.
 2. Il sistema genera un prompt alla voce "%: ****". Si prega di perforare la scheda di gestione per la conferma ". (**** Indica le quattro posizioni di lavoro da A a D in sequenza, sotto lo stesso)
 3. Se si desidera eseguire la gestione del U-disk, strisciare la carta per la conferma. Se l'operazione riesce, il sistema genererà un prompt alla voce "%: l'operazione è riuscita." E chiede di procedere alla fase successiva. Dopo aver completato i quattro elementi, il sistema genera un prompt alla voce "%: Il sistema ritorna allo stato di verifica." Se l'operazione non riesce, il sistema genererà un prompt alla voce "%: L'operazione non riesce. Il sistema ritorna allo stato di verifica".
 4. Se non lo fai strisciare la carta di gestione, il sistema salterà automaticamente questo passaggio su di 5 secondi e richiederà del passo successivo. Dopo aver completato i quattro elementi, il sistema ritorna allo stato di verifica automaticamente.
2. Se si collega un U-disk con il file di configurazione per il dispositivo, il sistema effettuerà operazioni in base alle impostazioni del file di configurazione.
 1. Dopo aver collegato un U-disk per il dispositivo, è possibile strisciare la carta una volta per entrare nello stato di gestione del U-disk.
 2. Il sistema ottiene comandi operativi leggendo il file di configurazione sul U-disk e genera un prompt alla voce "%: eseguire i file di configurazione del U-disk. Si prega di strisciare la carta di gestione per la conferma".
 3. Dopo aver strisciare la carta e di eseguire tutte le operazioni con successo, il sistema genererà il messaggio vocale "
: ****. L'operazione è riuscita. "In sequenza per ogni fase di funzionamento. Se
qualsiasi delle operazioni

f:.. A * I * Is **, thTehesyosptemratwioinll fgaeilnse "tasso messaggio vocale"
 4. Dopo aver terminato tutte le operazioni, il sistema genera un prompt alla voce "%: Il sistema ritorna allo stato di verifica."

? Avviso: Si prega di attendere 8 secondi dopo aver inserito il U-disk nel dispositivo, in caso contrario, il sistema può non rilevare l'U-disk probabilmente.

3.6 Interruttore antimanomissione

Viene premuto l'interruttore antimanomissione e tenuto premuto con un coperchio posteriore. Quando il dispositivo viene smontato, l'interruttore antimanomissione sarà sollevato e poi si invia un segnale di allarme per attivare un allarme.

Cancellare l'allarme: L'utente può cancellare l'allarme antifurto aprendo la porta su di abbinamento di successo.

Ripristinare le impostazioni predefinite: Le impostazioni di fabbrica possono essere ripristinate tramite l'interruttore antimanomissione.

Quando il sistema genera un allarme per 30-60 secondi, l'utente può premere l'interruttore antimanomissione per tre volte (finché i suoni degli altoparlanti) per ripristinare le impostazioni predefinite, tra cui il numero del dispositivo, password di sistema, l'indirizzo IP, indirizzo 485, e la password tastiera.



1. Le informazioni utente memorizzate sul dispositivo non viene cancellato dopo che il dispositivo viene ripristinato alle impostazioni di fabbrica.
2. Le impostazioni di fabbrica possono essere ripristinate attraverso la tastiera USB. Per dettagli, vedere [3.2.5 ripristinare le impostazioni predefinite](#).

1. Appendice

1. Elenco dei parametri

La seguente tabella elenca i parametri funzionali di base del dispositivo.

Articolo	Nota
Alimentazione	12V 3A
Funzione	Accesso dispositivo di controllo, sensore / allarme / blocco / uscita butto Uno Wiegand di ingresso e uno di uscita Wiegand
Quantità utente	10000 (impronte digitali e la carta d'identità)
Capacità di registrazione	100000 pezzi di record
Capacità di iscrizione (impronta digitale / scheda)	1500 fingerprints/10000 carte
Modalità di verifica.	ID (Mifare) carta, dito impronta digitale + scheda
Comunicazioni	TCP / IP, RS485, U-disc
Altoparlante	Voce, BEEP
LED	Indicazione bicolore (rosso / verde)
Tastiera	Chiavi valide: 0-9, Enter, ESC
	L'Environment Friendly Usa Periodo (EFUP) ha segnato in questa produzione periodo di sicurezza di tempo in cui il prodotto viene utilizzato nella circostanza le istruzioni del prodotto senza perdite di nociva e dannosa subst La EFUP di questo prodotto non copre le parti di consumo tha

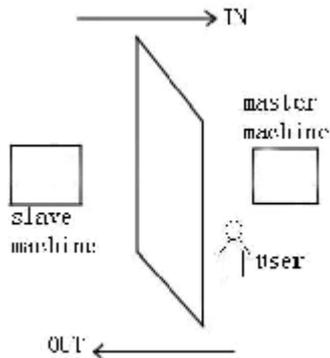
n

2. Anti-Passo Indietro ★

[Presentazione]

Talvolta, qualche persona illegale segue l'altro uno nel cancello, che porterà problema di sicurezza. Per evitare tale rischio, questa funzione è attiva. Nel record deve corrispondere out record o il cancello non sarà aperto.

Questa funzione ha bisogno di due macchine per lavorare insieme. Uno è installato all'interno della porta (macchina master di seguito), l'altro è installato al di fuori della porta (macchina slave di seguito). Comunicazione segnale Wiegand è adottato tra le due macchine.



[Principio di funzionamento] La macchina master è Wiegand A e macchina slave è Wiegand Out. Collegare Wiegand Fuori macchina slave a Wiegand In di macchina master. Wiegand uscita dalla macchina slave non deve possedere ID macchina. Il numero inviato al mas

maestro mach

[Funzione] Giudice se si tratta di anti-pass back secondo dell'utente recente in-out record. Nel registrare e fuori registro m

fuori, in o out-in anti-pass back. Quando macchina master è impostato come "out anti-pass back", se l'utente vuole entrare e uscire normalmente, il suo recente record deve essere "in", o lui non può uscire. Ogni record "fuori" sarà "anti-pass back rifiutato". Ad esempio, recente record di un utente è "in", il suo secondo record può essere "fuori" o "in". Il suo terzo album è basato sul suo secondo album. Fuori di record e nel record deve corrispondere **(Avviso:** Se custo

a ma non può uscire). Quando la macchina master è impostato come "in anti-pass back", se l'utente vuole entrare e uscire normalmente, il suo recente record deve essere "out", o lui non può uscire. Ogni record di fuori sarà "anti-retropassaggio rifiutato" dal sistema (Nota: se il

ma non può venire in). Quando la macchina master è impostato come "out-in anti-pass back", se l'utente vuole entrare e uscire normalmente, se la sua rec

poi la sua prossima rec

【 Operazione

1. Selezione modello

Maestro

lettore.

Macchina slave: Macchina con Wiegand funzione Out.

2. Impostare la direzione indietro anti-pass e st dispositivo

3. Modifica formato di uscita Wiegand del dispositivo

Quando i due dispositivi a
ID del dispositivo sono rec

4. **Iscrivi utente** l'utente deve essere sulla macchina master e macchina slave, allo stesso tempo, e il PIN utente deve essere lo stesso. Pertanto, è necessario

utente sulla macchina master e

5. **Collegamento un'istruzione di** comunicazione Wiegand è adottato per mas

llowing per connessione: Master Slave

IND0 <-----> wd0

IND1 <-----> WD1



Nota:



È possibile impostare solo i parametri posteriori anti-passa attraverso l'accesso c



m

3. Dichiarazione dei diritti dell'uomo e Privacy

Cari clienti:

Grazie per aver scelto i prodotti ibridi biometrici progettati e realizzati da noi. Come un famoso fornitore di tecnologie e servizi biometrici, prestiamo molta attenzione al rispetto delle leggi relative ai diritti umani e la privacy in tutti i paesi, mentre costantemente l'esecuzione di attività di ricerca e sviluppo.

Con la presente facciamo le seguenti dichiarazioni:

1. Tutti i nostri dispositivi di riconoscimento delle impronte digitali per uso civile solo raccogliere i punti caratteristici delle impronte digitali al posto delle immagini delle impronte digitali, e quindi senza problemi di privacy sono coinvolti.
2. I punti caratteristici delle impronte digitali raccolte dai nostri prodotti non possono essere utilizzati per ripristinare le immagini originali delle impronte digitali, e quindi senza problemi di privacy sono coinvolti.
3. Noi, come fornitore di attrezzature, non devono essere ritenuti legalmente responsabili, direttamente o indirettamente, per eventuali conseguenze derivanti dovuto l'uso dei nostri prodotti.
4. Per qualsiasi controversia che coinvolge i diritti umani o la vita privata quando si utilizzano i nostri prodotti, si prega di contattare direttamente il tuo datore di lavoro.

I nostri prodotti di impronte digitali o strumenti di sviluppo per l'uso di polizia sostengono la raccolta delle immagini originali di impronte digitali. Per quanto riguarda se un tale tipo di raccolta di impronte digitali costituisce una violazione della sua privacy, si prega di contattare il governo o il fornitore di attrezzature finale. Noi, come il produttore di apparecchiature originali, non devono essere ritenuti legalmente responsabili per qualsiasi violazione contestazione in merito.

 **Nota:**  La legge della Repubblica popolare cinese ha le seguenti norme per quanto riguarda la libertà personale: 

5. È vietata arresti illegali, la detenzione o la ricerca di cittadini della Repubblica popolare cinese; violazione della privacy individuale è vietata.
6. La dignità personale dei cittadini della Repubblica popolare cinese è inviolabile.
7. La casa dei cittadini della Repubblica popolare cinese è inviolabile.
8. La libertà e la segretezza della corrispondenza dei cittadini della Repubblica popolare cinese sono protetti dalla legge.

Infine sottolineiamo ancora una volta che i dati biometrici, come la tecnologia di riconoscimento avanzato, sarà applicata in molti settori, tra cui l'e-commerce, banche, assicurazioni e affari legali. Ogni anno le persone in tutto il mondo soffrono di gravi perdite a causa della mancanza di sicurezza delle password. Il riconoscimento delle impronte digitali in realtà fornisce una protezione adeguata per la propria identità in un ambiente di massima sicurezza.

4. Environment-Friendly Usa Descrizione

Articolo Nota

Alimentatore 12V 3A Dispositivo di controllo di accesso alle funzioni, sensore / allarme / pulsante di uscita di blocco /

Un ingresso Wiegand e un'uscita Wiegand Quantità utente 10000 (impronte digitali e la carta d'identità Record di capacità 100000 pezzi di record capacità di iscrizione (impronta digitale / scheda) 1500 fingerprints/10000 carte Modalità di verifica. ID (Mifare) carta, impronte delle dita + scheda Comunicazione TCP / IP, RS485, U-disc Speaker Voice, BEEP Indicazione LED bicolore (rosso / verde) Tastiera Tasti validi: 0-9, Enter, ESC L'Environment Friendly Usa Periodo (EFUP) ha segnato in questo periodo di sicurezza produzione di tempo in cui il prodotto viene utilizzato nella circostanza le istruzioni del prodotto senza perdite di nociva e dannosa subst La EFUP di questo prodotto non copre le parti di consumo tha sostituito su un regolarmente come batterie e così via. I EFUP 5 anni.

Nomi e concentrazione di sostanze o elementi tossici e pericolosi

Nome delle parti tossiche e
Sostanze o E
PHC Cr
BGD 6 +

Resistore chip					
Condensatore di circuito integrato	x				
Chip induttore	x				
Chip diodo	x				

DIACHIARAZIONE DI CONFORMITA'



La sottoscritta BETTONI ELISABETTA

in qualità di legale rappresentante della ditta SAISYSTEM DI ELISABETTA BETTONI

con sede in via Torino 12/A 10040 Druento (TORINO)

Partita Iva 09735350010

Dichiara

Che il prodotto: Controllo Accessi con Impronta digitale

Codice: MA300

Anno inizio costruzione: 2010

È stato costruito rispettando le seguenti norme:

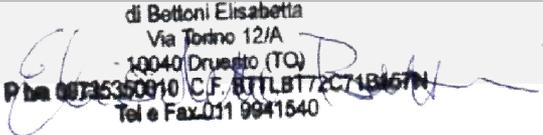
- Direttiva 2006/95 CE nota come Direttiva bassa tensione
- Direttiva 2004/108/CE nota come "Direttiva compatibilità elettromagnetica".
- Direttiva 2011/65/UE restrizione dell'uso dei materiali inquinanti negli AEE
- Norma UNI EN ISO 12100-1:2005 Principi generali di progettazione
- Norma UNI EN ISO 12100-2:2005 Principi generali di progettazione
- Norma UNI EN ISO 13849-1:2007 principi generali per la progettazione

Ed e quindi conforme alle normative vigenti

Data 15-05-2011

Firma

SAISYSTEM
di Bettoni Elisabetta
Via Torino 12/A
10040 Druento (TO)
P. IVA 09735350010 C.F. 811181720718167N
Tel e Fax 011 9941540



Declaration of conformity

