Face Recognition Access Controller

Guida Rapida

V1.0.0

Avvertenze

Generale

Questo manuale introduce l'installazione ed il funzionamento di base dei Terminali di Face Recognition (di seguito denominati " terminali ").

Istruzioni di Sicurezza

I seguenti segnali, con relative spiegazioni, potrebbero apparire nel manuale.

Signal Words	Meaning
DANGER	Indica un potenziale rischio elevato che, se non evitato, causerà morte o lesioni gravi.
WARNING	Indica un rischio medio o basso potenziale che, se non evitato, potrebbe provocare lesioni lievi o moderate.
CAUTION	Indica un potenziale rischio che, se non evitato, potrebbe provocare danni alla proprietà , perdita di dati, prestazioni inferiori o risultati imprevedibili.
TIPS	Fornisce metodi per aiutarti a risolvere un problema o risparmiare tempo.
NOTE	Fornisce ulteriori informazioni come enfasi e supplemento al testo.

Cronologia delle versioni

Version	Revision Content	Release Time
V1.0.0	Prima release	Aprile 2020

Informazioni sul manuale

- Il manuale è indicativo. In caso di incoerenza tra il manuale e il prodotto reale, prevarrà il prodotto reale.
- Non siamo responsabili per eventuali perdite causate da operazioni non conformi al manuale.
- Il manuale verrà aggiornato secondo le ultime leggi e regolamenti delle regioni correlate. Per informazioni dettagliate, consultare il manuale cartaceo, il CD-ROM, il codice QR o il nostro sito Web ufficiale. In caso di incoerenza tra il manuale cartaceo e la versione elettronica, prevarrà la versione elettronica.

- Tutti i design e il software sono soggetti a modifiche senza preavviso scritto. Gli aggiornamenti del prodotto potrebbero causare alcune differenze tra il prodotto reale e il manuale. Si prega di contattare il servizio clienti per l'ultimo programma e la documentazione supplementare.
- Potrebbero esserci ancora differenze nei dati tecnici, nella descrizione delle funzioni e delle operazioni o errori nella stampa. In caso di dubbi o controversie, fare riferimento alla nostra spiegazione finale.
- Aggiornare il software del lettore o provare altri software del lettore tradizionale se non è possibile aprire il manuale (in formato PDF).
- Tutti i marchi, i marchi registrati e i nomi delle società nel manuale sono di proprietà dei rispettivi proprietari.
- Visitare il nostro sito Web, contattare il fornitore o il servizio clienti in caso di problemi durante l'utilizzo del dispositivo.
- In caso di incertezza o controversia, fare riferimento alla nostra spiegazione finale.

Precauzioni Importanti e avvertenze

Questo capitolo descrive i contenuti riguardanti la corretta gestione del terminale, la prevenzione dei pericoli e la prevenzione di danni materiali. Leggere attentamente questi contenuti prima di utilizzare il terminale, rispettarli durante l'utilizzo e conservare bene il manuale per riferimenti futuri.

Requisiti Operativi

- Non posizionare o installare il terminale in un luogo esposto alla luce solare o vicino a fonti di calore.
- Tenere il terminale lontano da umidità, polvere o fuliggine.
- Mantenere il terminale installato in posizione orizzontale in un luogo stabile per evitare che cada.
- Non far cadere o spruzzare liquidi sul terminale e assicurarsi che non vi siano oggetti riempiti di liquido sul terminale per impedire al liquido di fluire nel terminale.
- Installare il terminale in un luogo ben ventilato e non bloccare la ventilazione del terminale.
- Azionare il terminale entro l'intervallo nominale di ingresso e uscita di potenza.
- Non disassemblare il terminale in modo casuale.
- Per il terminale con un'unità di monitoraggio della temperatura:
  - ◇ Installare l'unità di monitoraggio della temperatura in un ambiente interno senza vento e mantenere la temperatura ambiente interna da 15 ° C a 32 ° C.
  - ◇ Riscaldare il dispositivo per più di 20 minuti dopo l'accensione per consentire ad esso di raggiungere l'equilibrio termico.

Sicurezza Elettrica

- L'uso improprio della batteria può provocare incendi, esplosioni o infiammazioni.
- Quando si sostituisce la batteria, assicurarsi di utilizzare lo stesso modello.
- Utilizzare i cavi di alimentazione raccomandati nella regione e conformi alle specifiche di potenza nominale.
- Utilizzare l'alimentatore fornito con il terminale; in caso contrario, potrebbero verificarsi lesioni alle persone e danni al dispositivo.
- La fonte di alimentazione deve essere conforme ai requisiti della norma SELV (Safety Extra Low Voltage) e fornire energia con tensione nominale conforme ai requisiti della fonte di alimentazione limitata secondo IEC60950-1. Si noti che i requisiti di alimentazione sono soggetti all'etichetta del dispositivo.
- Collegare il dispositivo (struttura di tipo I) alla presa di corrente con messa a terra di protezione.
- L'accoppiatore dell'apparecchio è un dispositivo di disconnessione. Quando si utilizza l'accoppiatore, mantenere l'angolazione per un facile utilizzo.

Sommario

1 Dimensioni e Componenti

Figure 1-1 Dimensioni e componenti (mm [inch])

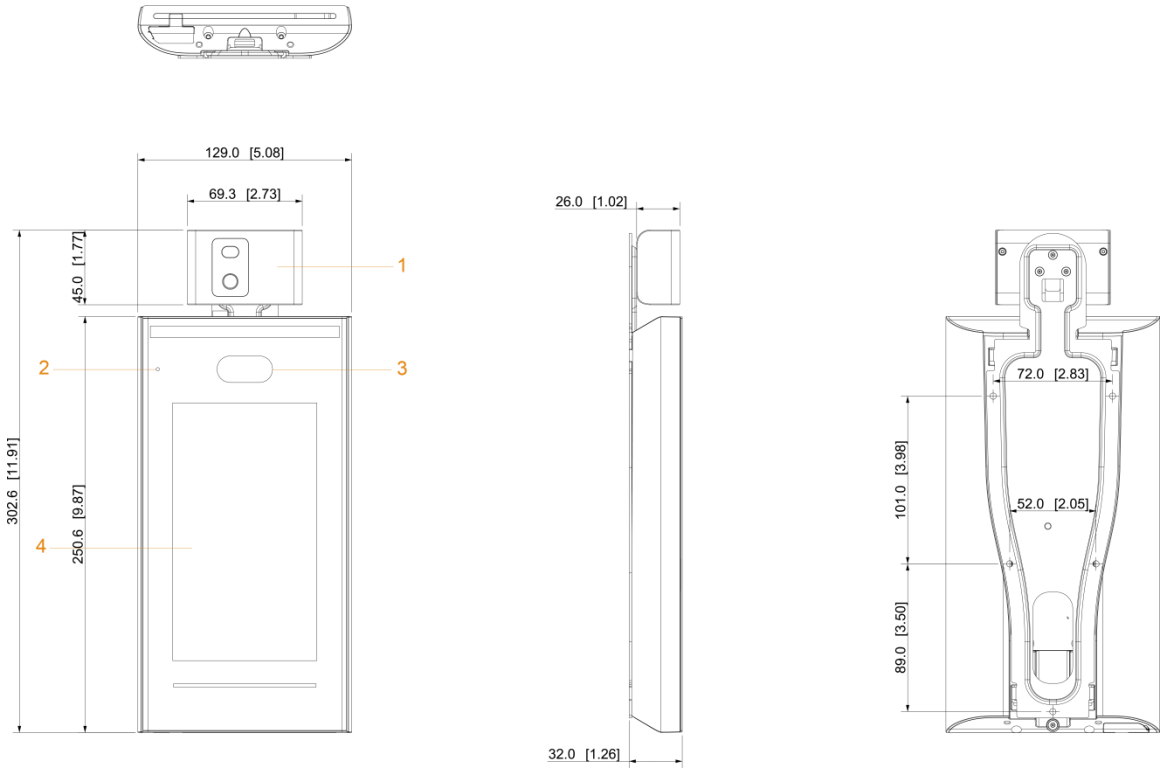


Table 1-1 Descrizione Componenti

No.	Nome	No.	Nome
1	Unità di monitoraggio della temperatura	3	Doppia fotocamera
2	MIC	4	Display

2 Collegamento ed Installazione

2.1 Collegamento Cavi

- Controllare se il modulo di sicurezza del controllo accessi è abilitato in **Funzione> Modulo di sicurezza**. Se abilitato, è necessario acquistare il modulo di sicurezza separatamente. Il modulo di sicurezza necessita di un alimentatore separato.
- Una volta abilitato il modulo di sicurezza, il pulsante di uscita, il controllo del tornello e il collegamento antincendio non saranno più validi.

Figure 2-1 Collegamento Cavi

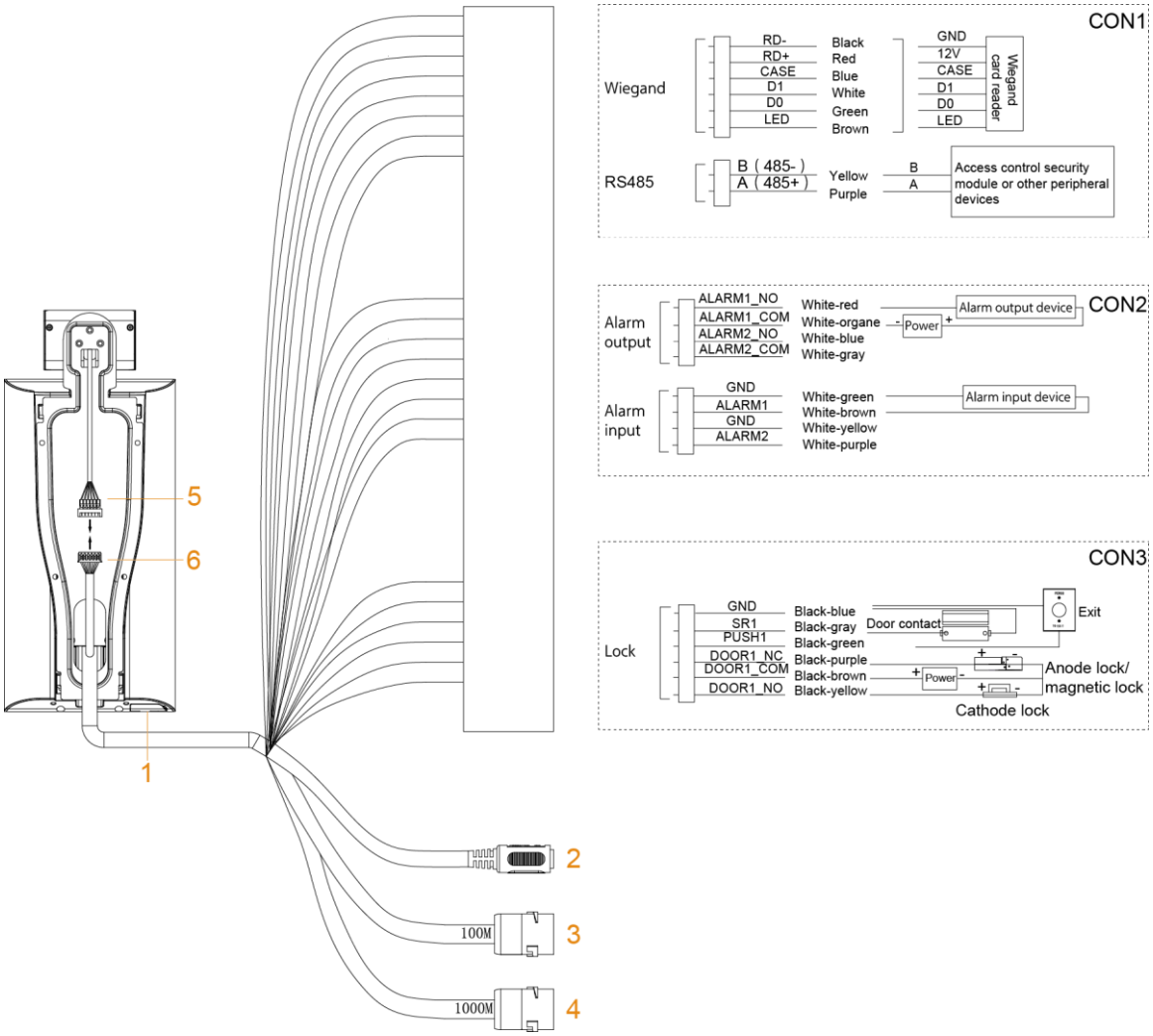


Table 2-1 Descrizione Componenti

No.	Nome
1	Porta USB
2	Porta di aliementazione
3	100M Porta Ethernet
4	1000M Porta Ethernet

No.	Nome
5, 6	Porte per il collegamento dell'unità di monitoraggio della temperatura

2.2 Note sull'Installazione

- Se è presente una fonte di luce a 0,5 metri dal terminale, l'illuminazione minima non deve essere inferiore a 100 Lux.
- Si consiglia di installare il terminale in ambienti chiusi, ad almeno 3 metri da finestre e porte e 2 metri dalle luci.
- Evitare retroilluminazioni e la luce solare diretta.

Requisiti di illuminazione ambientale

Figure 2-2 Requisiti di illuminazione ambientale

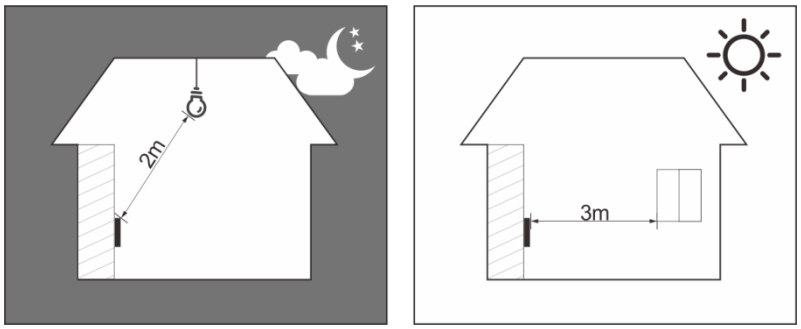
Requisiti di monitoraggio della temperatura

- Si consiglia di installare il dispositivo in un ambiente interno senza vento (un'area relativamente isolata dall'esterno) e mantenere la temperatura ambiente compresa tra 15 ° C e 32 ° C.
- Far riscaldare il dispositivo per più di 20 minuti dopo l'accensione per consentire all'unità di monitoraggio della temperatura di raggiungere l'equilibrio termico.
- Se non esiste un ambiente interno adatto (comprese le zone che si affacciano direttamente su aree interne ed esterne, e porte esterne), impostare un passaggio temporaneo con temperatura ambiente stabile per il monitoraggio della temperatura.
- Fattori quali luce solare, vento, aria fredda e aria condizionata (aria fredda e calda) possono facilmente influenzare la temperatura superficiale del corpo umano e lo stato di funzionamento del dispositivo, causando una differenza tra la temperatura monitorata e quella effettiva.
- Fattori che influenzano il monitoraggio della temperatura
  - ◇ **Vento:** il vento toglierà il calore dalla fronte, il che influenzerà l'accuratezza del monitoraggio della temperatura.
  - ◇ **Sudorazione**: la sudorazione è un modo per il corpo di raffreddarsi automaticamente e dissipare il calore. Quando il corpo suda, anche la temperatura diminuisce.
  - ◇ **Temperatura ambiente**: se la temperatura ambiente è bassa, la temperatura superficiale del corpo umano diminuirà. Se la temperatura della stanza è troppo alta, il corpo umano inizierà a sudare, il che influenzerà l'accuratezza del monitoraggio della temperatura.

◇ L'unità di monitoraggio della temperatura è sensibile alle onde luminose con una lunghezza d'onda compresa tra 10um e 15um. Evitare di usarlo al sole, vicino a fonti di luce fluorescente, prese di aria condizionata, riscaldamento, prese di aria fredda e superfici di vetro.

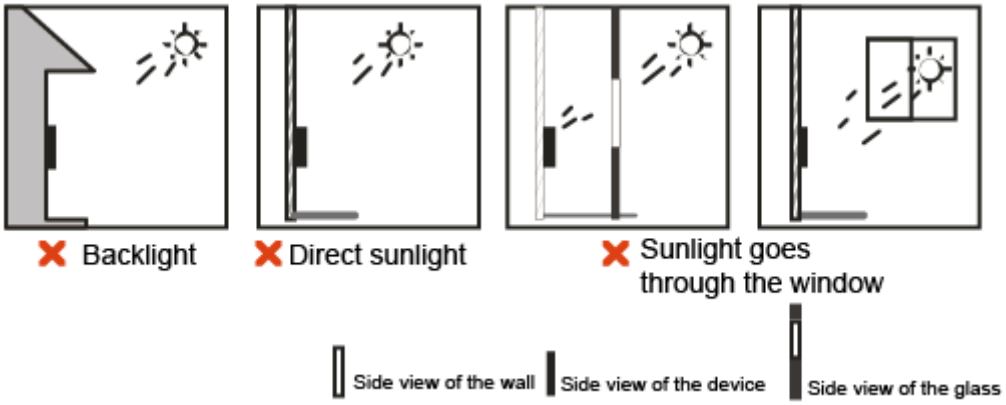
Luoghi Consigliati

Figure 2-3 Luoghi Consigliati



Luoghi Non Consigliati

Figure 2-4 Luoghi Non Consigliati



2.3 Installazione

Assicurarsi che la distanza tra l'obiettivo ed il pavimento sia di 1,4 metri.

Figure 2-5 Altezza Installazione

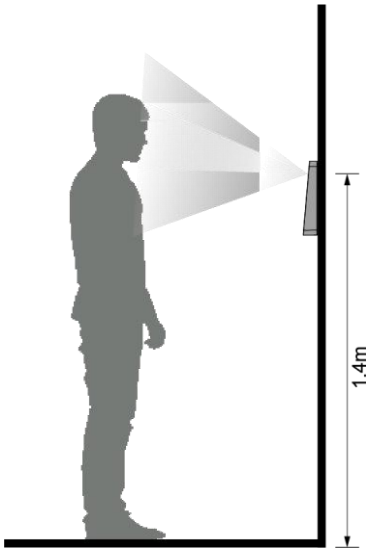
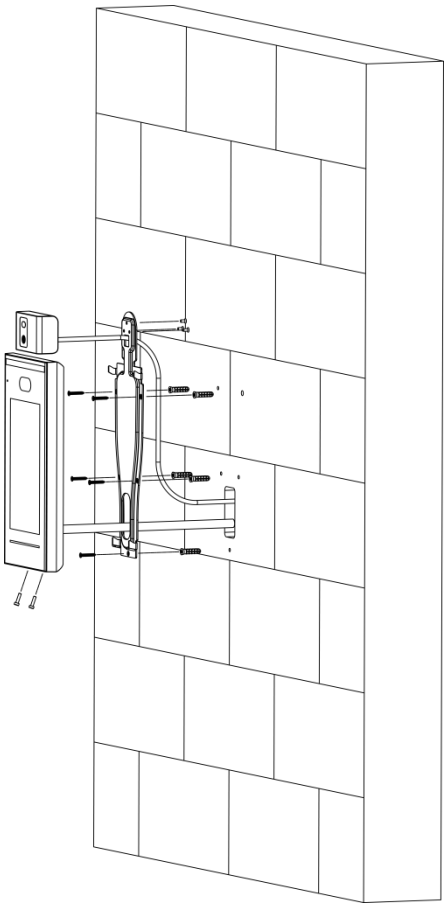


Figure 2-6 Diagramma Installazione



Procedura d’installazione

Step 1 Fissare l'unità di monitoraggio della temperatura sulla staffa con 3 viti.

Step 2 Praticare sei fori (cinque fori di installazione della staffa e un ingresso cavo) nella parete in base ai fori nella staffa.

Step 3 Fissare la staffa sulla parete installando le viti di espansione nei cinque fori di installazione della staffa.

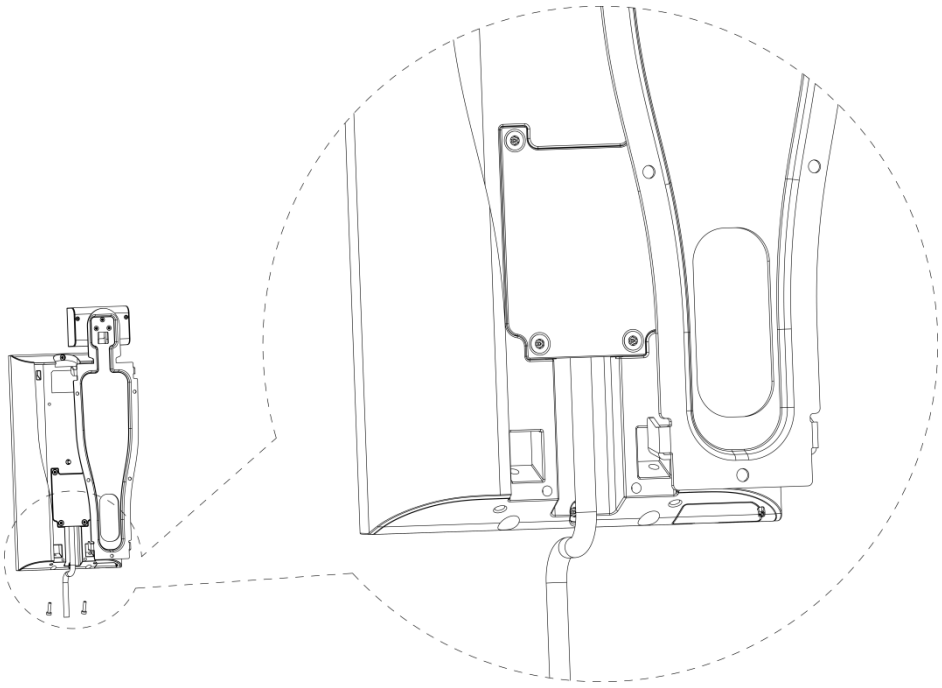
Step 4 Collegare i cavi per il controller di accesso. Vedere "2.2 Collegamenti dei cavi".

Step 5 Appendere il dispositivo sul gancio della staffa.

Step 6 Stringere le viti nella parte inferiore del dispositivo.

Step 7 Applicare sigillante siliconico all'uscita del cavo del dispositivo.

Figure 2-7 Applicazione sigillante siliconico



3 Operazioni di Sistema

3.1 Inizializzazione

La password di amministratore ed un'e-mail devono essere impostate la prima volta che si accende al dispositivo; in caso contrario non è possibile utilizzare prodotto.

Figure 3-1 Inizializzazione

- La password dell'amministratore può essere reimpostata tramite l'indirizzo e-mail inserito se la password è stata dimenticata.
- La password deve contenere da 8 a 32 caratteri non vuoti e contenere almeno due tipi di caratteri tra maiuscolo, minuscolo, numero e carattere speciale (escluso '";: &).
- Per dispositivi senza touchscreen, inizializzare tramite l'interfaccia Web. Vedere il manuale utente per i dettagli..

3.2 Aggiunta di nuovi utenti

Puoi aggiungere nuovi utenti inserendo ID utente, nomi, importando impronte digitali, immagini di volti, password e selezionando i livelli utente.

Le figure seguenti sono solo di riferimento e prevarrà l'interfaccia effettiva.

Step 1 Seleziona **Utente > Nuovo Utente**.

Figure 3-2 Nuovo Utente

Step 2 Configurare i parametri sull'interfaccia.

Table 3-1 Descrizione Parametri

Parameter	Description
User ID	Inserisci gli ID utente. Gli ID sono composti da 32 caratteri (inclusi numeri e lettere) e ogni ID è unico.
Nome	Inserire nomi con al massimo 32 caratteri (inclusi numeri, simboli e lettere).
Volto	Assicurati che il viso sia centrato nel riquadro di acquisizione delle immagini, verrà automaticamente catturata un'immagine del viso. Per i dettagli sulla registrazione delle immagini dei volti, vedere " Appendice 2 Note sulla registrazione/confotrno dei Volti".
Tessera	Puoi registrare al massimo cinque tessere per ogni utente. Nell'interfaccia di registrazione tessere, inserisci il numero della tessera o passala sul lettore, le informazioni verranno lette dal dispositivo. È possibile abilitare la funzione Tessera di Coercizione nell'interfaccia di registrazione della tessera. Gli allarmi verranno attivati se si utilizza una tessera di coercizione per sbloccare la porta. Se il controller di accesso è senza lettore di tessere, è necessario collegare il dispositivo ad un lettore periferico.

Parameter	Description
Password	Password di sblocco porta. La lunghezza massima della password è di 8 cifre. Se il terminale è senza touch-screen, è necessario collegarlo a un lettore di schede periferico. Ci sono pulsanti sul lettore di schede che permetteranno l'inserimento della password
Livelli	È possibile selezionare un livello utente per i nuovi utenti. Vi sono due opzioni. ● Utente: gli utenti hanno solo il permesso di sblocco della porta. ● Amministratore: gli amministratori possono sbloccare la porta e disporre anche dell'autorizzazione alla configurazione dei parametri. E' consigliato creare più di un amministratore così da poter accedere al sistema nel caso in cui smarrite la password di amministratore,
Periodo	Il periodo in cui l'utente può sbloccare la porta. Per le impostazioni dettagliate del periodo consultare il manuale dell'utente.
Piano Vacanze	È possibile impostare un piano vacanze in cui l'utente può sbloccare la porta. Per le impostazioni dettagliate del piano ferie, consultare il manuale dell'utente.
Validità Data	È possibile impostare un periodo durante il quale è possibile sbloccare la porta.
Livello Utenti	Ci sono sei livelli:: ● **Generale**: gli utenti generici possono sbloccare normalmente la porta. ● **Blacklist**: quando gli utenti in Blacklist aprono la porta, il personale di servizio riceverà una notifica. ● **Ospite**: gli ospiti sono autorizzati a sbloccare la porta in determinati orari o in determinati periodi. Quando superano i tempi o i periodi massimi non potranno aprire la porta. ● **Ronda**: gli utenti di pattugliamento possono tenere traccia della loro presenza, ma non dispongono dell'autorizzazione di sblocco. ● **VIP**: quando VIP apre la porta, il personale di servizio riceverà un messaggio. ● **Speciale**: quando utenti speciali aprono la porta, ci sarà un ritardo di 5 secondi prima che la porta venga chiusa.
N. utilizzi	è possibile impostare il numero massimo di volte in cui l'utente Ospite può sbloccare la porta.

Step 3 Premi to per salvare la configurazione.

4 Operazioni WEB

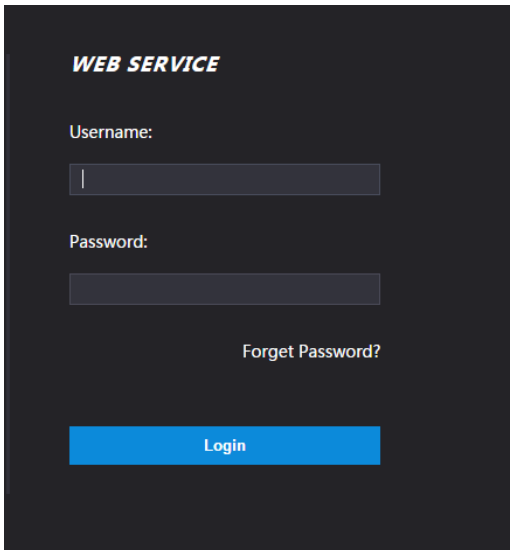
Il terminale può essere configurato e gestito tramite interfaccia web. Da Web è possibile impostare parametri tra cui parametri di rete, parametri video e parametri del terminale; e possibile anche aggiornare il sistema. Per i dettagli, consultare il manuale dell'utente. Qui verranno descritte solamente le operazione di accesso.

È necessario impostare una password e un indirizzo e-mail prima di accedere all'interfaccia Web per la prima volta. La password impostata viene utilizzata per accedere al Web e l'e-mail viene utilizzata per reimpostare le password.

Step 1 Aprire il Browser IE, inserire l'indirizzo IP del terminale nella barra degli indirizzi, quindi premere il tasto Invio.

- Assicurarsi che l'indirizzo IP del computer utilizzato per accedere al Web sia nella stessa LAN con il terminale.
- Il terminale ha due schede di rete. L'indirizzo IP predefinito per la porta di rete 1000M è 192.168.1.108 e per la porta di rete 100M è 192.168.2.108

Figure 4-1 Login



Step 2 Inserire username e password.

- Il nome utente predefinito dell'amministratore è admin e la password è la password di accesso impostata dopo l'inizializzazione del terminale. Modifica regolarmente la password di admin e conservala correttamente per motivi di sicurezza.
- Se si dimentica la password di accesso dell'amministratore, è possibile fare clic su **Password dimenticata?** per resettarlo. Vedi il manual utente.

Step 3 Click **Login**.

Viene visualizzata la pagina iniziale dell'interfaccia Web.

.

Appendix 1 Note sul monitoraggio della temperatura

- Riscaldare l'unità di monitoraggio della temperatura per 20 minuti dopo l'accensione per consentire al dispositivo di raggiungere l'equilibrio termico.
- Installare l'unità di monitoraggio della temperatura in un ambiente interno senza vento e mantenere la temperatura ambiente interna da 15 ° C a 32 ° C.
- Evitare la luce solare diretta sull'unità.
- Evitare di installare l'unità di monitoraggio della temperatura rivolta verso fonti di luce e vetro.
- Tenere il dispositivo lontano da fonti di interferenza termica.
- Fattori quali luce solare, vento, aria fredda e aria condizionata (aria fredda e calda) influenzeranno la temperatura superficiale del corpo umano, causando la differenza tra la temperatura monitorata e la temperatura effettiva.
- La sudorazione è un modo per il corpo di raffreddarsi automaticamente e dissipare il calore, causando anche la differenza tra la temperatura monitorata e la temperatura effettiva.
- Pulire regolarmente l'unità di monitoraggio della temperatura (ogni 2 settimane). Utilizzare un panno morbido per rimuovere delicatamente la polvere sulla superficie del sensore di temperatura e del sensore di distanza.

Appendix 2 Note sulla registrazione/confronto dei Volti

Prima della Registrazione

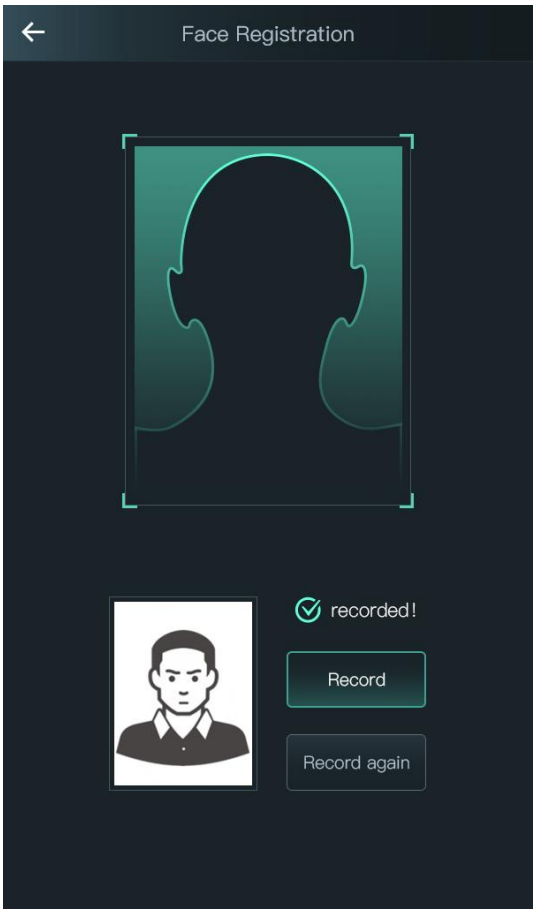
- Occhiali, cappelli e barbe potrebbero influenzare le prestazioni del riconoscimento facciale.
- Non coprire le sopracciglia quando si indossano i cappelli.
- Non cambiare notevolmente lo stile della barba se utilizzerai il dispositivo; altrimenti il riconoscimento facciale potrebbe non riuscire.
- Mantieni il viso pulito.
- Tenere il dispositivo ad almeno due metri dalla fonte di luce e ad almeno tre metri da finestre o porte; in caso contrario, la retroilluminazione e la luce solare diretta potrebbero influenzare le prestazioni di riconoscimento del volto del dispositivo.

Durante la Registrazione

È possibile registrare i volti attraverso il terminale o attraverso la piattaforma. Per la registrazione attraverso la piattaforma, consultare il manuale utente della piattaforma.

Posiziona la testa al centro della cornice di acquisizione delle foto. Una foto del tuo viso verrà catturata automaticamente.

Appendix Figure 2-1 Registrazione

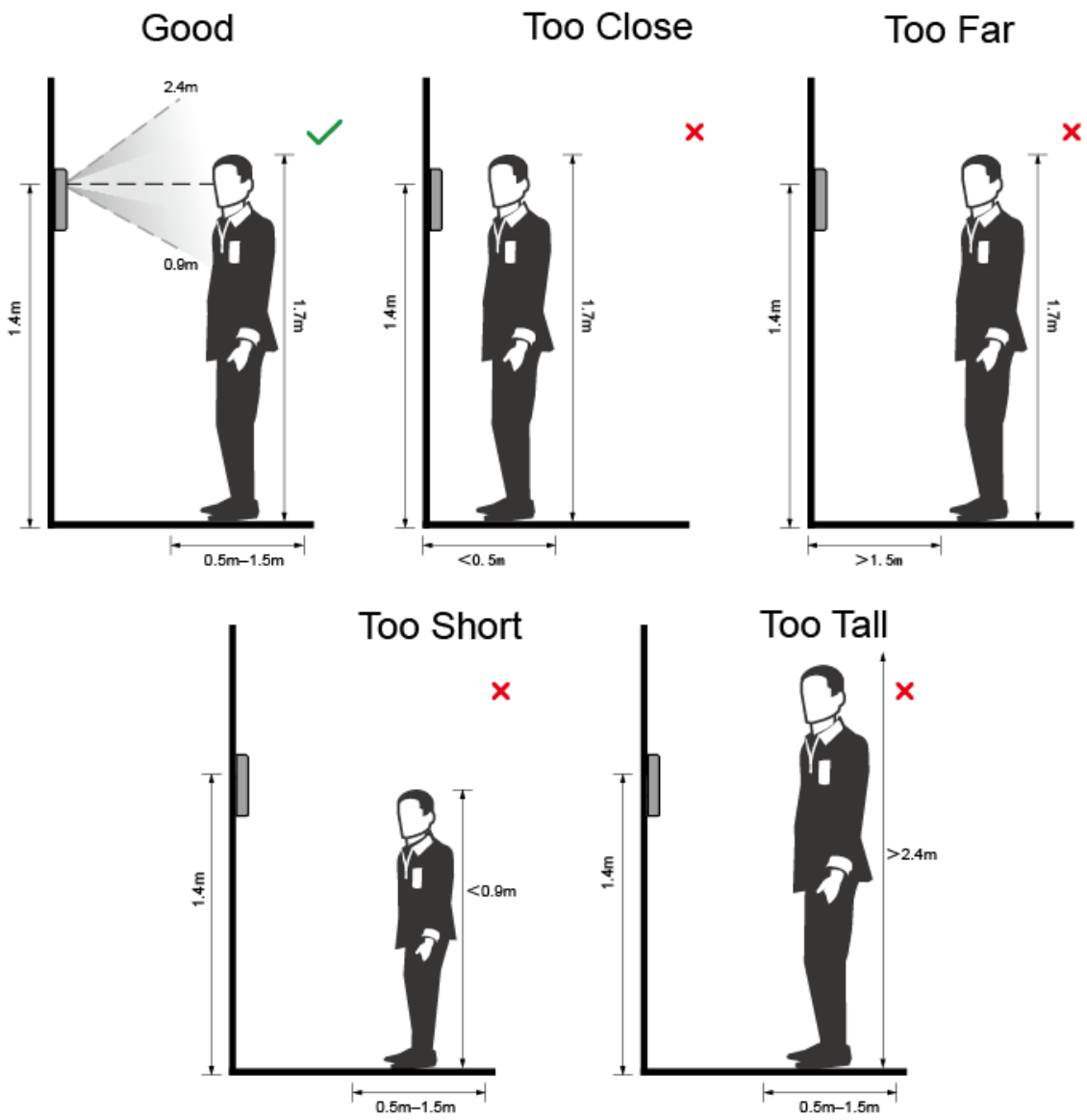


- Non scuotere la testa o il corpo, altrimenti la registrazione potrebbe non riuscire.
- Evitare che due volti compaiano nel riquadro di acquisizione contemporaneamente.

Posizione Viso

Se il viso non si trova nella posizione appropriata, il riconoscimento potrebbe essere influenzato.

Appendix Figure 2-2 Posizione appropriata



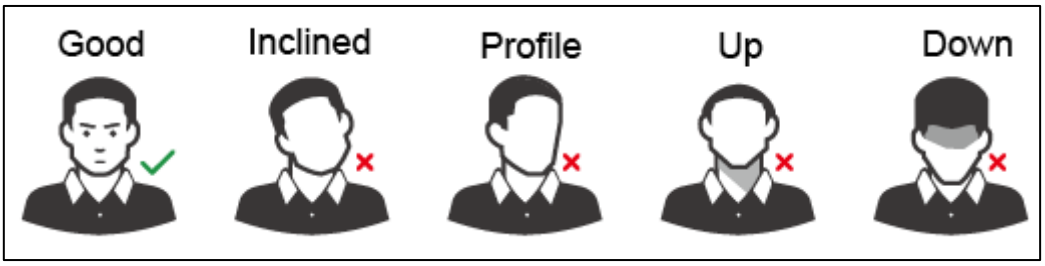
Requisiti dei Volti

- Assicurarsi che il viso sia pulito e la fronte non sia coperta dai capelli.
- Non indossare occhiali, cappelli, barbe pesanti o altri ornamenti per il viso che influenzano la registrazione delle immagini del viso.
- Con gli occhi aperti, senza espressioni facciali, e inclina il viso verso il centro della fotocamera
- Durante la registrazione del viso o durante il riconoscimento del volto, non tenere il viso

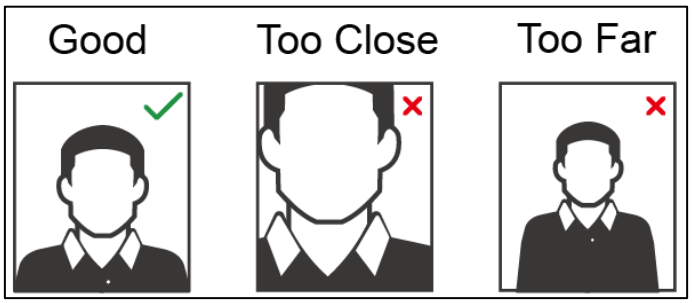
troppo vicino o troppo lontano dalla fotocamera.

.

Appendix Figure 2-3 Posizione Testa



Appendix Figure 2-4 Face distance



- Quando si importano immagini di volti attraverso la piattaforma di gestione, assicurarsi che la risoluzione dell'immagine sia compresa nell'intervallo 150 × 300–600 × 1200; i pixel dell'immagine sono più di 500 × 500; la dimensione dell'immagine è inferiore a 75 KB ed il nome dell'immagine e l'ID utenti siano gli stessi.
- Accertarsi che il viso non occupi 2/3 dell'intera area dell'immagine e che le proporzioni non superino 1: 2.

Appendix 3 Raccomandazioni Cybersecurity

La sicurezza informatica non è solo una parola d'ordine: è qualcosa che riguarda tutti i dispositivi connessi a Internet. La videosorveglianza IP non è immune ai rischi informatici, ma adottare misure di base per proteggere e rafforzare le reti e gli apparecchi in rete li renderà meno suscettibili agli attacchi. Di seguito sono riportati alcuni suggerimenti e raccomandazioni su come creare un sistema di sicurezza più sicuro.

Azioni obbligatorie da adottare per la sicurezza della rete delle apparecchiature di base:
Use Strong Passwords

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 .;

1. **Aggiorna il Firmware e Client Software**
   - Secondo la procedura standard nell'industria tecnologica, si consiglia di mantenere aggiornato il firmware delle apparecchiature (come NVR, DVR, telecamera IP, ecc.) Per garantire che il sistema sia dotato delle ultime patch e correzioni di sicurezza. Quando l'apparecchiatura è connessa alla rete pubblica, si consiglia di abilitare la funzione di "controllo automatico degli aggiornamenti" per ottenere informazioni tempestive sugli aggiornamenti del firmware rilasciati dal produttore.
   - Ti consigliamo di scaricare e utilizzare la versione più recente del software client.

"Nice to have" raccomandazioni per migliorare la sicurezza della tua rete di apparecchiature:

1. **Protezione fisica**
   Ti consigliamo di installare i dispositivi in ambienti protetti, particolare attenzione verso i dispositivi di archiviazione. Ad esempio, posizionare l'apparecchiatura in una sala computer e un armadio, implementare l'autorizzazione di controllo accessi e la gestione delle chiavi per impedire a personale non autorizzato di danneggiare l'hardware, o di poter operare su supporti rigidi (come disco flash USB , porta seriale), ecc..
2. **Cambia password regolarmente**
   Ti consigliamo di cambiare regolarmente le password.
3. **Impostare ed aggiornare le password e le informazioni tempestivamente**
   L'apparecchiatura 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 protezione della password e l'indirizzo email dell'utente finale. Se le informazioni cambiano, si prega di modificarle in tempo. Quando si impostano domande sulla protezione della password, si consiglia di non utilizzare quelle che possono essere facilmente indovinate.
4. **Abilita Blocco 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 di accedere più volte con la password errata, l'account corrispondente e l'indirizzo IP di origine verranno bloccati.

5. **Modifica le porte HTTP e di altri servizi**
   Ti consigliamo di modificare le porte HTTP e di altri servizi predefinite in qualsiasi set di numeri compreso tra 1024 e 65535, riducendo il rischio che gli estranei siano in grado di indovinare quali porte stai utilizzando.
6. **Abilita HTTPS**
   Ti consigliamo di abilitare HTTPS.
7. **Abilita Whitelist**
   Ti consigliamo di abilitare la funzione whitelist per impedire a tutti, tranne quelli con indirizzi IP specificati, di accedere al sistema. Pertanto, assicurati di aggiungere l'indirizzo IP del tuo computer e l'indirizzo IP dell'apparecchiatura di accompagnamento alla lista bianca.
8. **MAC Address Binding**
   Si consiglia di associare l'indirizzo IP e MAC del gateway all'apparecchiatura, riducendo così il rischio di spoofing ARP.
9. **Assegnare Accounts e Privilegi Ragionevolmente**
   In base ai requisiti aziendali e di gestione, aggiungere ragionevolmente utenti e assegnare loro un set minimo di autorizzazioni.
10. **Disabilitare i servizi non necessari e scegliere 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 ma non limitati ai seguenti servizi::
    - SNMP: Scegli SNMP v3 e imposta password di crittografia complesse e password di autenticazione.
    - SMTP: Scegli TLS per accedere al server.
    - FTP: Scegli SFTP e imposta password complesse.
    - AP hotspot: Scegli la modalità di crittografia WPA2-PSK e imposta password complesse.
11. **Trasmissione crittografata audio e video**
    If Se i contenuti dei tuoi 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 dell'efficienza della trasmissione.
12. **Auditing Sicuro**
    - Controlla utenti online: ti consigliamo di controllare regolarmente gli utenti online per vedere se il dispositivo è connesso senza autorizzazione.
    - Controlla il registro delle apparecchiature: visualizzando i registri, puoi conoscere gli indirizzi IP utilizzati per accedere ai tuoi dispositivi e le loro operazioni chiave.
13. **Network Log**
    A causa della limitata capacità di archiviazione dell'apparecchiatura, il registro archiviato è limitato. Se è necessario salvare il registro per molto tempo, si consiglia di abilitare la funzione di registro di rete per garantire che i registri critici siano sincronizzati con il server di registro di rete per la traccia.

14. Costruire un ambiente di rete sicuro

Per garantire una migliore sicurezza delle attrezzature e ridurre i potenziali rischi informatici, si consiglia:

- Disabilitare la funzione di mappatura delle porte del router per evitare l'accesso diretto ai dispositivi Intranet dalla rete esterna.
- La rete deve essere suddivisa e isolata in base alle effettive esigenze della rete. Se non vi 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.
- Istituire il sistema di autenticazione dell'accesso 802.1x per ridurre il rischio di accesso non autorizzato alle reti private.
- Si consiglia di abilitare il firewall del dispositivo o la lista nera e la funzione di whitelist per ridurre il rischio che il dispositivo possa essere attaccato.