Face Recognition Access Controller

Manuale Utente

V1.0.0

Avvertenze

Generale

Questo manuale introduce l'installazione e le operazioni di base del controller di accesso al riconoscimento facciale (di seguito denominato "controller di accesso").

Istruzioni di Sicurezza

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

Signal Words	Meaning
NOTE	Fornisce ulteriori informazioni come enfasi e supplemento al testo.

Cronologia delle versioni

Version	Revision Content	Release Date
V1.0.0	Prima Release.	May 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 Panoramica

1.1 Introduzione

Il dispositivo è un controllo accessi che supporta lo sblocco tramite volti, password, tessere e supporta lo sblocco tramite le loro combinazioni.

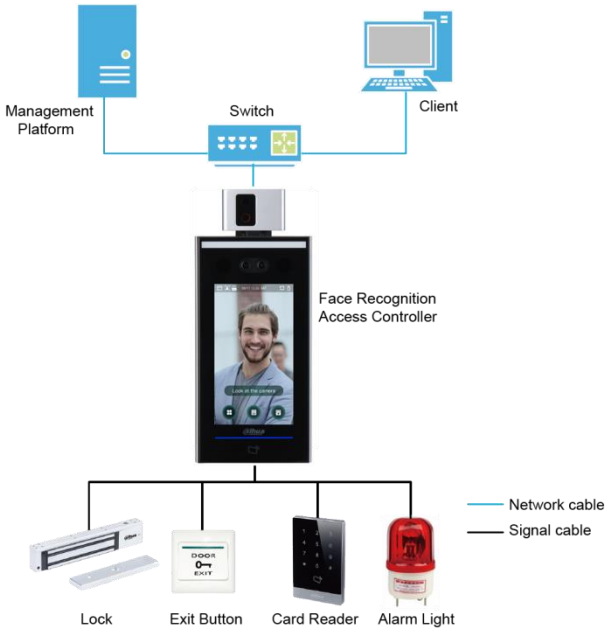
1.2 Caratteristiche

- Display LCD da 7 pollici con risoluzione 1024 × 600.
- Supporto sblocco tramite riconoscimento del volto, scheda IC e password; sblocco in fascia oraria.
- Con riquadro di rilevazione volti; il volto più grande tra i volti che appaiono contemporaneamente viene riconosciuto per primo; la dimensione massima del viso può essere configurata sul web.
- obbiettivo WDR grandangolare da 2 MP; con illuminatore automatico/manuale
- Con Algoritmo di riconoscimento volti, il controller di accesso è in grado di riconoscere più di 360 posizioni sul volto umano
- Precisione della verifica del viso> 99,5%; basso tasso di errori
- Supporto per il riconoscimento del profilo; l'angolo del profilo è 0 ° -90 °
- Supporta il rilevamento di volti reali.
- Supporta allarme coercizione, allarme manomissione, allarme intrusione, allarme timeout contatto porta e allarme soglia superamento carta illegale
- Supportare utenti generici, utenti di pattuglia, utenti nella lista nera, utenti VIP, utenti ospiti e utenti speciali
- Diverse modalità di visualizzazione dello stato di sblocco proteggono la privacy dell'utente
- Supporta il monitoraggio della temperatura corporea attraverso l'unità di monitoraggio della temperatura periferica

1.3 Applicazione

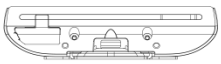
Il controller di accesso è utilizzabile in per parchi, uffici, scuole, fabbriche, aree residenziali e altri luoghi. L'identità viene verificata attraverso il riconoscimento facciale per ottenere il passaggio senza percezione.

Figure 1-1 Networking



1.4 Dimensioni e Componenti

Figure 1-1 Dimensioni e Componenti modello X con lettore di temperatura (mm [inch])



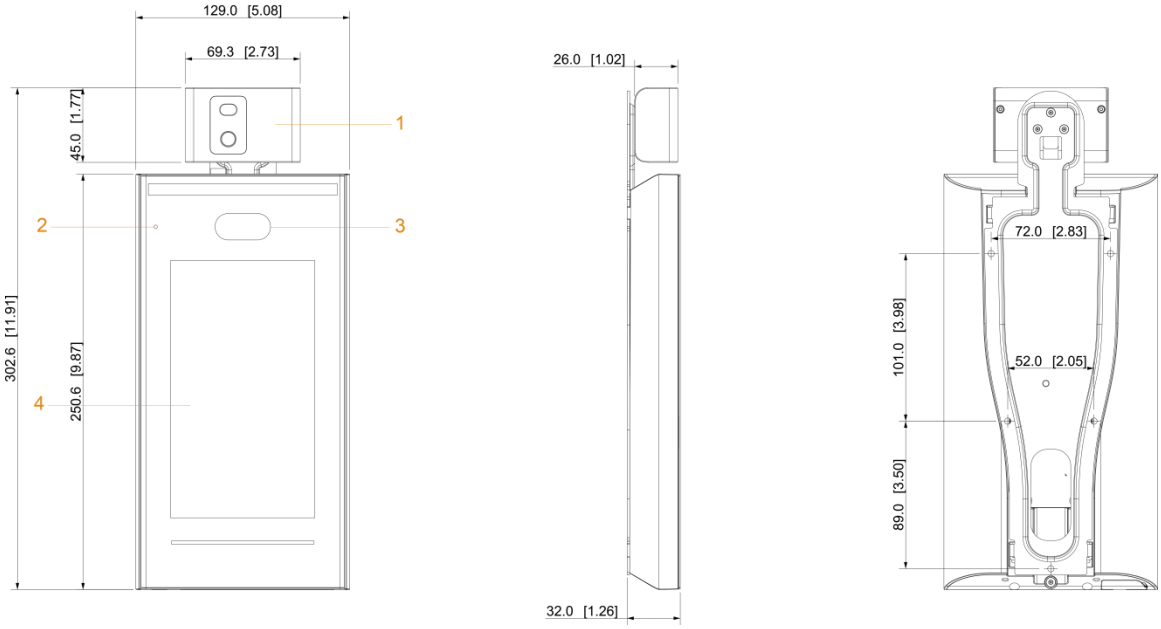


Table 1-1 Descrizione componenti (3)

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

2 Connessione ed Installazione

2.1 Connessione Cavi

Il controller deve essere collegato a dispositivi come sirene, lettori e contatti porta. Per il collegamento dei cavi, vedere, **Error! Reference source not found.**.

Table 2-1 Descrizione Collegamenti

Port	Cable color	Cable name	Description
CON1	Nero	RD–	Negativo lettore di schede esterno.
	Rosso	RD+	Positivo lettore di schede esterno.
	Blu	CASE	Tamper lettore di schede esterno
	Bianco	D1	Wiegand D1 Input (collegato al lettore di schede esterno) / uscita (collegato al controller).
	Verde	D0	Wiegand D0 input (collegato al lettore di schede esterno) / uscita (collegato al controller).
	Marrone	LED	Collegato all'indicatore del lettore esterno
	Giallo	B	Ingresso/elettrodo negativo RS-485 (collegato al lettore di schede esterno) / uscita (collegato al controller o al modulo di sicurezza del controllo della porta). ● Se il modulo di sicurezza è abilitato, è necessario acquistare separatamente il modulo di sicurezza del dispositivo. Il modulo di sicurezza necessita di un alimentatore separato per fornire energia. ● Una volta abilitato il modulo di sicurezza, il pulsante di uscita, il controllo di blocco e il collegamento antincendio non saranno più validi.
	Viola	A	Ingresso/elettrodo Positivo RS-485 (collegato al lettore di schede esterno) / uscita (collegato al controller o al modulo di sicurezza del controllo della porta). ● Se il modulo di sicurezza è abilitato, è necessario acquistare separatamente il modulo di sicurezza del dispositivo. Il modulo di sicurezza necessita di un alimentatore separato per fornire energia. ● Una volta abilitato il modulo di sicurezza, il pulsante di uscita, il controllo di blocco e il collegamento antincendio non saranno più validi.

Port	Cable color	Cable name	Description
CON2	Bianco % Rosso	ALARM1_NO	Allarme 1,contatto di uscita Normalmente Aperto
	Bianco e Arancio	ALARM1_COM	Allarme 1,Comune contatto di uscita
	Bianco e Blu	ALARM2_NO	Allarme 2,contatto di uscita Normalmente Aperto
	Bianco e Grigio	ALARM2_COM	Allarme 2,Comune contatto di uscita
	Bianco e Verde	GND	Collegato alla porta GND comune.
	Bianco Marrone	ALARM1	Allarme 1 Ingresso.
	Bianco e Giallo	GND	Collegato alla porta GND comune.
	Bianco e Viola	ALARM2	Allarme 2 Ingresso.
CON3	Rosso e Nero	RX	RS-232 RX
	Nero e Arancio	TX	RS-232 TX.
	Nero e BLu	GND	Collegato alla porta GND comune.
	Nero e Grigio	SR1	Utilizzato per il contatto stato porta.
	Nero e Verde	PUSH1	Pulsante di apertura della porta n. 1
	Nero e Marrone	DOOR1_COM	Comune controllo blocco porta.
	Nero e Giallo	DOOR1_NO	Controllo porta normalmente aperta..
	Nero e Viola	DOOR1_NC	Controllo porta normalmente chiusa.

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

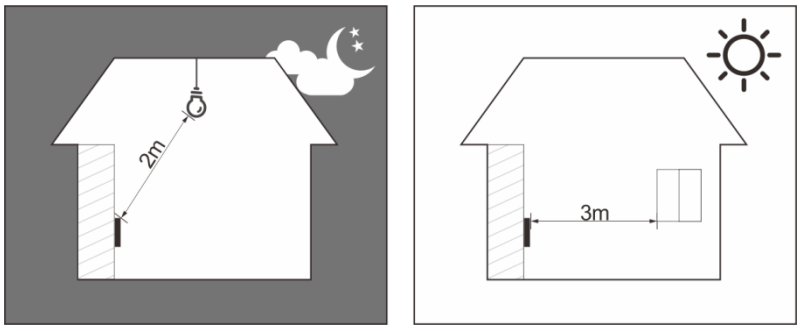
Figure 2-1 Requisiti di illuminazione ambientale

Requisiti di illuminazione ambientale

- 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.

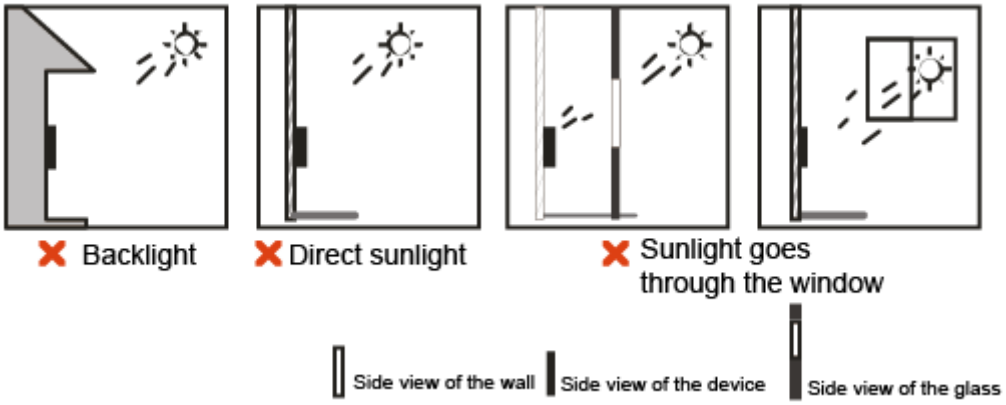
Luoghi Consigliati

Figure 2-2 Luoghi Consigliati



Luoghi Non Consigliati

Figure 2-3 Luoghi Non Consigliati



2.3 Installazione

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

Figure 2-4 Altezza Installazione

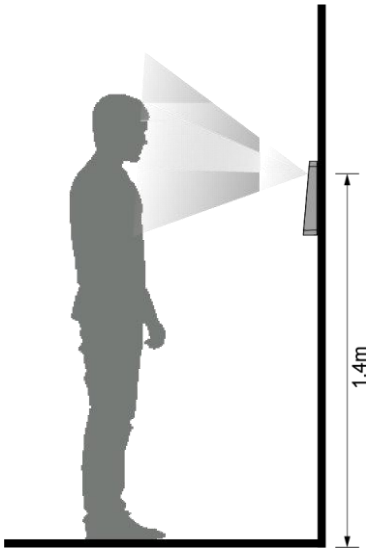
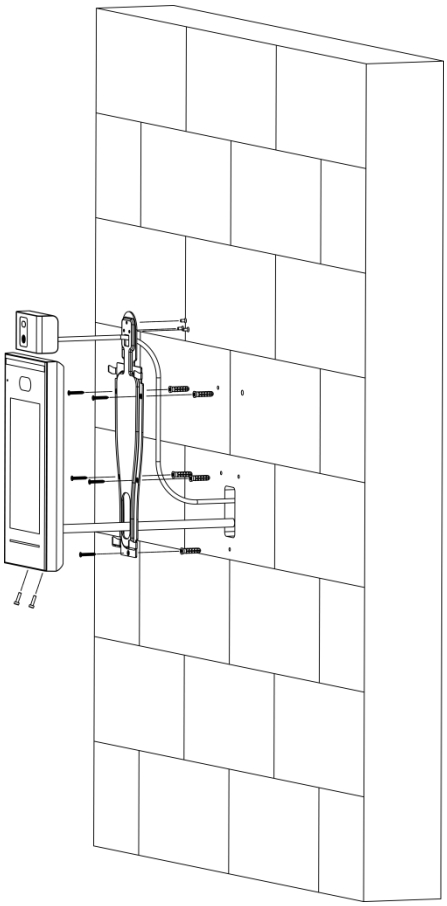


Figure 2-5 Diagramma Installazione



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.

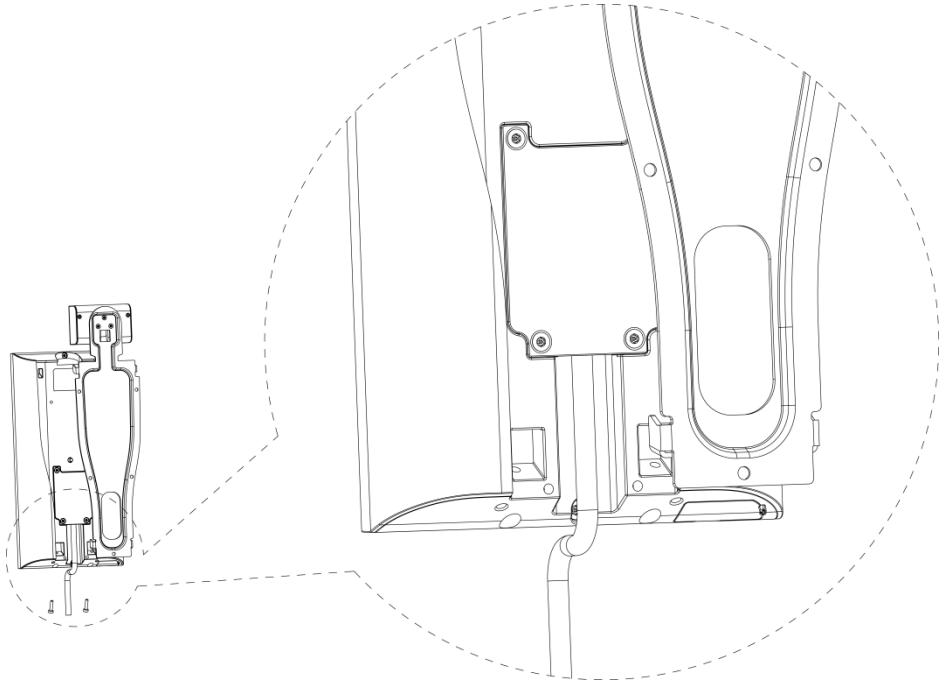
Step 4 Collegare i cavi per il controller di accesso. Vedere "2.2 Collegamenti dei cavi".

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.

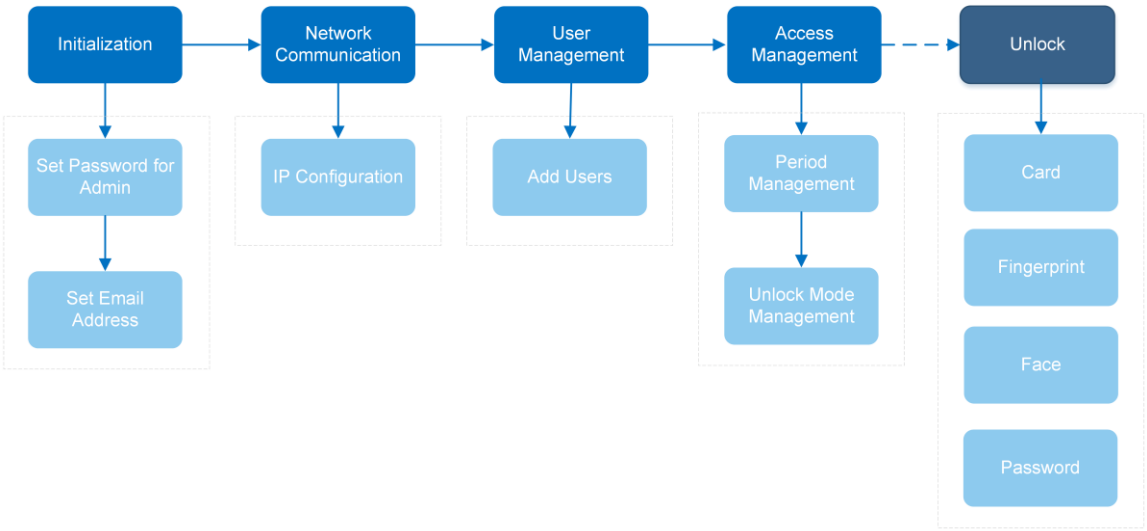
Figure 2-6 Applicazione Sigillante Siliconico



3 Operazioni di Sistema

3.1 Procedura configurazione di base

Figure 3-1 Procedura configurazioen di bas3



3.2 Icone Comuni

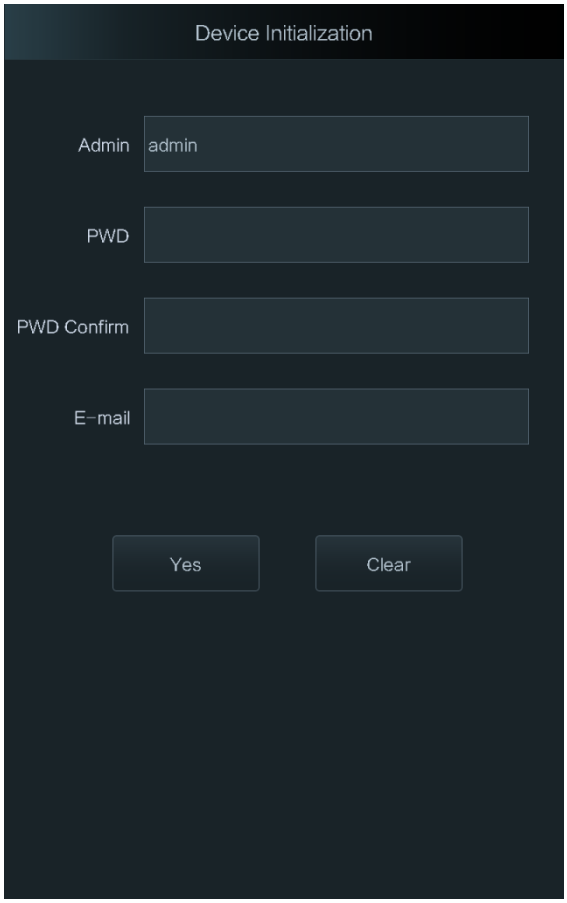
Table 3-1 Descrizione Icone

Icon	Description
	Icona del menu principale.
	Icona di conferma
	Passa alla prima pagina dell'elenco.
	Passa all'ultima pagina dell'elenco.
	Passa alla pagina precedente dell'elenco.
	Passa alla pagina successiva dell'elenco.
	Ritorna al menù precedente.
	Abilita.
	Disabilita.

3.3 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 3-2 Inizializzazione



- Utente Admin e password impostati su questa interfaccia saranno utilizzati per accedere alla piattaforma di gestione Web.
- 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 '";: &).

3.4 Interfaccia Standby

È possibile sbloccare la porta tramite volti, password e carte. Vedi Table 3-2.

- Se non vengono eseguite operazioni entro 30 secondi, il controller passa alla modalità standby.
- L'interfaccia di standby può variare a seconda delle versioni e deve prevalere l'interfaccia effettiva.

Figure 3-3 Homepage

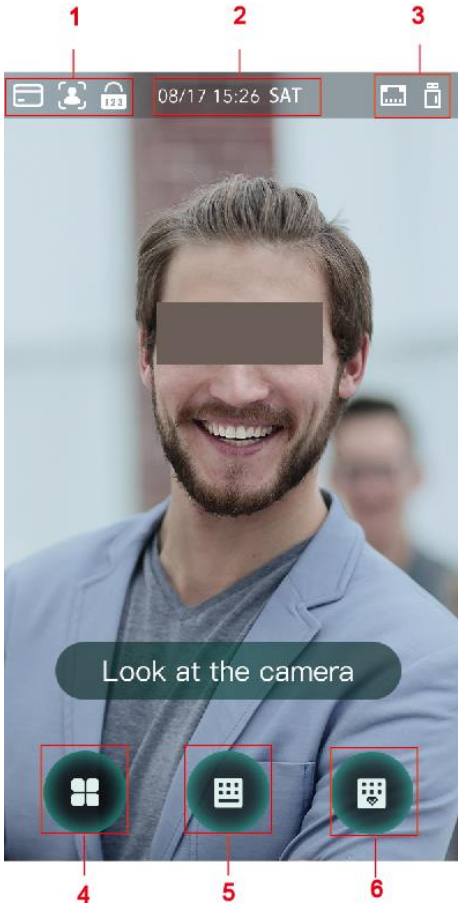


Table 3-2 Descrizione Homepage

No.	Description
1	Metodi di sblocco: Tessera, Volto e password. Quando Tessera, Volto e password sono tutti impostati come modalità di sblocco, l'icona della password non verrà visualizzata nell'angolo in alto a sinistra del controller di accesso.
2	Data & ora: Visualizza la data e l'ora correnti.
3	visualizza lo stato della rete e lo stato USB.
4	Icona del menu principale. Solo gli utenti con il permesso di amministratore possono accedere al menu principale.
5	Icona di sblocco password.
6	Icona di sblocco password amministratore.

3.5 Menu Principale

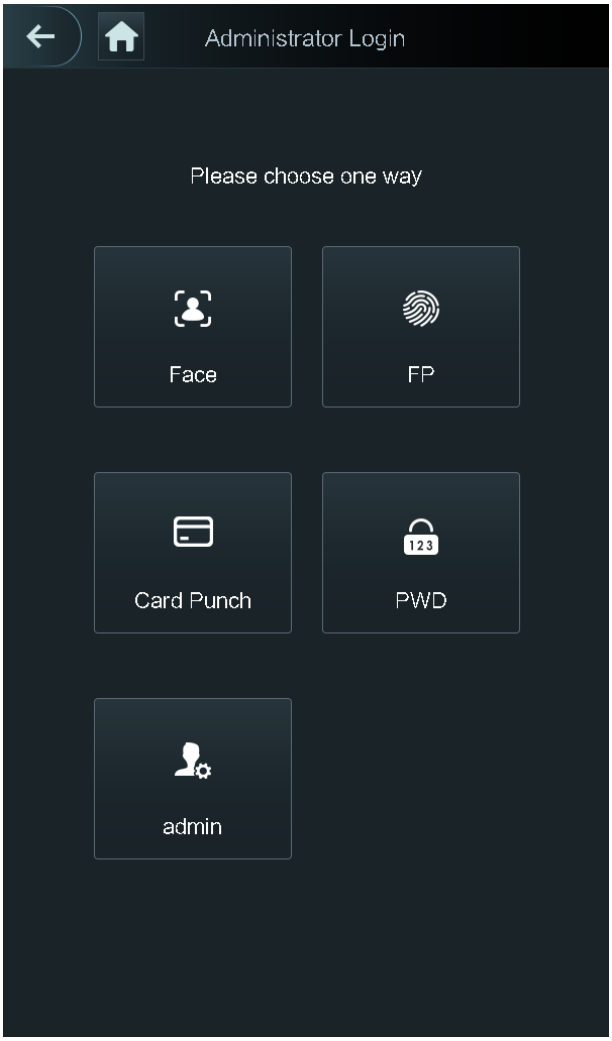
Gli amministratori possono aggiungere utenti di diversi livelli, impostare parametri relativi all'accesso, eseguire la configurazione di rete, visualizzare i record di accesso e le informazioni di sistema e altro.

Step 1 Premi  sull'interfaccia di standby.

Step 2 Selezionare un metodo di accesso al menu principale.

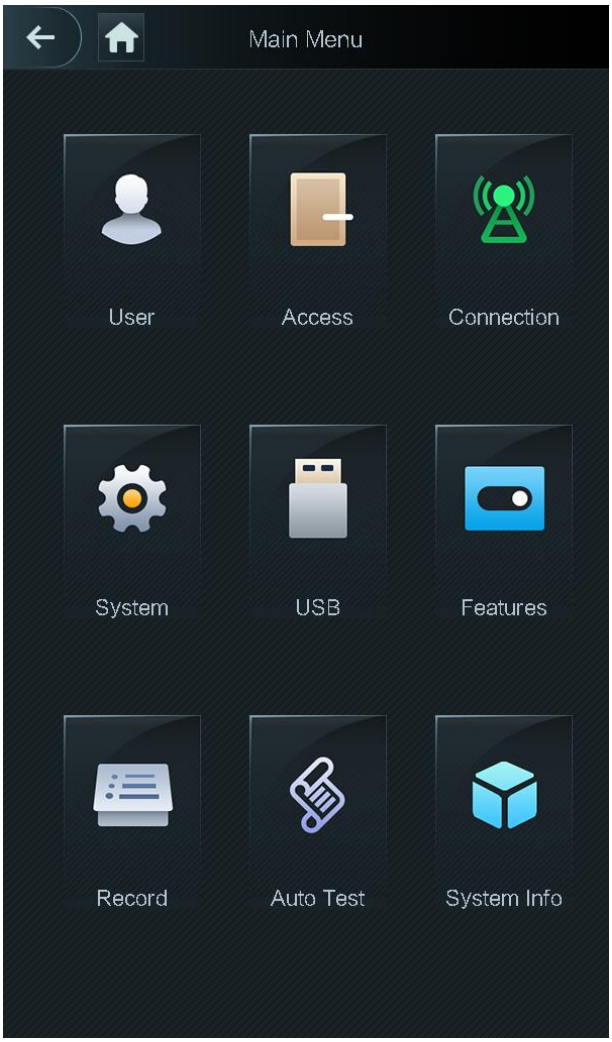
Sono supportati diversi metodi di sblocco, prevarrà l'interfaccia effettiva..

Figure 3-4 Administrator login



Viene visualizzata l'interfaccia del menu principale.

Figure 3-5 Menu Principale



3.6 Metodi di sblocco

È possibile sbloccare la porta tramite volti, password e tessere.

3.6.1 Tessere

Passa la tessera sul lettore per sbloccare la porta.

3.6.2 Volti

Assicurati che il tuo viso sia centrato nel riquadro di riconoscimento per sbloccare la porta.

3.6.3 Password Utente

Inserire la password utente per sbloccare la porta.

Step 1 Premere  nella homepage.

Step 2 Inserire ID utente, e poi premere ☑.

Step 3 Inserire la password utente, e poi premere ☑.

La porta è aperta.

3.6.4 Password Amministratore

Inserire la password di amministratore per sbloccare la porta. Esiste una sola password amministratore. La password può sbloccare la porta senza essere soggetta a livelli utente, modalità di sblocco, periodi, pianificazioni vacanze e anti-passback.

La password amministratore non può essere utilizzata quando NC è selezionato in "3.8.1.5 Periodo NC".

Step 1 premere  nella homepage.

Step 2 premere **Inserire PWD amministratore**.

Step 3 Inserire la password amministratore, e poi premere ☑.

La porta è aperta.

3.7 Gestione Utenti

È possibile aggiungere nuovi utenti, visualizzare l'elenco utenti, elenco amministratori e modificare la password dell'amministratore sull'interfaccia utente.

3.7.1 Inserimento nuovi utenti

E' possibile aggiungere nuovi utenti inserendo ID utente, nomi, immagini dei volti, tessere, password, selezionare i livelli utente e altro.

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

Step 1 Seleziona **Utenti > Nuovi Utenti**.

Figure 3-6 Info Nuovi Utenti

Step 2 Configurare i parametri sull'interfaccia.

Table 3-3 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 e che il dispositivo scatti automaticamente una foto del viso del nuovo utente.
Tessera	Puoi registrare al massimo cinque tessere per ogni utente. Nell'interfaccia di registrazione tessere, inserisci il numero della tessera o passal 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. Solo alcuni modelli supportano lo sblocco con tessera

Parameter	Description
Password	Password di sblocco porta. La lunghezza massima della password è di 8 cifre. Se il terminale è senza touchscreen, 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 per salvare la configurazione.

3.7.2 Visualizzare Informazioni utente

È possibile visualizzare l'elenco degli utenti, l'elenco degli amministratori e abilitare la password dell'amministratore tramite l'interfaccia utente.

3.8 Gestione degli Accessi

È possibile eseguire la gestione degli accessi in base a periodo, modalità di sblocco, allarme, stato della porta e tempo di blocco.

Premi **Accesso** per accedere all'interfaccia di gestione degli accessi.

3.8.1 Gestione Periodi

È possibile impostare periodi, periodi festivi, periodi del piano ferie, periodi normalmente aperti, periodi normalmente chiusi e periodi con verifica remota.

3.8.1.1 Configurazione Periodi

È possibile configurare 128 periodi (settimane) il cui intervallo di numeri è compreso tra 0 e 127. È possibile impostare quattro periodi per ogni giorno di un periodo (settimana). Gli utenti possono sbloccare la porta solo nei periodi impostati.

3.8.1.2 Gruppo Vacanze

È possibile impostare i gruppi Vacanze, quindi è possibile impostare i piani per le festività. È possibile configurare 128 gruppi il cui intervallo di numeri è compreso tra 0 e 127. Puoi aggiungere 16 festività in un gruppo. Configurare l'ora di inizio e l'ora di fine di un gruppo festivo, quindi gli utenti possono sbloccare la porta solo nei periodi impostati.

Puoi inserire nomi con 32 caratteri (inclusi numeri, simboli e lettere). Premere Per salvare il nome del Gruppo Vacanze.

3.8.1.3 Piano Vacanze

È possibile aggiungere gruppi di ferie nei piani di ferie. È possibile utilizzare i piani ferie per gestire l'autorizzazione di accesso dell'utente in diversi gruppi festivi. Gli utenti possono sbloccare la porta solo nel periodo impostato.

3.8.1.4 Periodo NO

Se un periodo viene aggiunto al periodo NO, la porta sarà normalmente aperta.

Le autorizzazioni per periodi NO / NC sono superiori alle autorizzazioni in altri periodi..

3.8.1.5 Periodo NC

Se un periodo viene aggiunto al periodo NC, la porta sarà normalmente chiusa. Gli utenti non potranno aprire la porta in questo periodo.

3.8.1.6 Periodo con verifica remota

Se è stato configurato il periodo di verifica remota, quando si sblocca la porte durante verrà richiesta la verifica remota. Per sbloccare la porta in questo periodo, è necessaria una conferma di sblocco tramite la piattaforma di gestione.

È necessario abilitare il Periodo di verifica remota.

- 

significa Abilitato.
- 

significa Disabilitato.

3.8.2 Sblocco

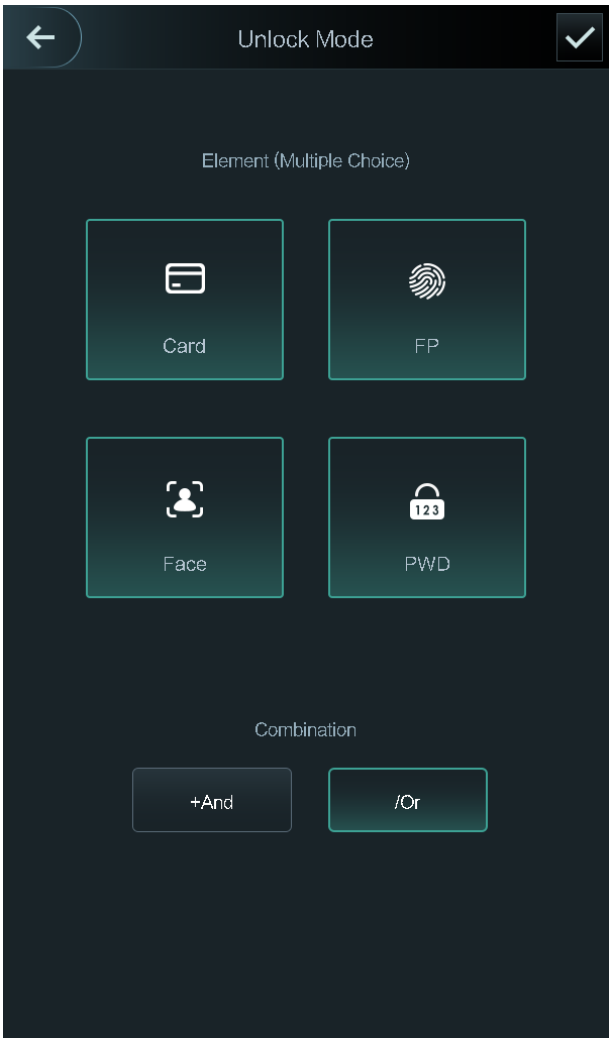
Esistono tre modalità di sblocco: modalità di sblocco, sblocco per periodo e combinazione di gruppi. Le modalità di sblocco variano in base ai modelli di dispositivo e prevarrà l'accesso effettivo al controller.

3.8.2.1 Modalità di Sblocco

Quando la modalità di sblocco è attiva, gli utenti possono sbloccare con: tessere, volti, password o uno di tutti i metodi di sblocco.

Step 1 Seleziona **Accesso > Modalità Sblocco > Modalità Sblocco**.

Figure 3-7 Elemento (scelta multipla)



Step 2 Selezionare le modalità di sblocco.

Toccando nuovo una modalità di sblocco selezionata, la modalità di sblocco verrà eliminata..

Step 3 Selezionare una combinazione.

- **+ And** significa "and". Ad esempio, se selezioni la scheda + PWD, significa che per sbloccare la porta, devi prima scorrere la scheda, quindi inserire la password.
- **/ Or** significa "or". Ad esempio, se si seleziona la scheda / PWD, significa che per sbloccare la porta, è possibile scorrere la scheda o inserire la password.

Step 4 Seleziona per salvare la configurazione.

Verrà visualizzata l'interfaccia della **modalità di sblocco**.

Step 5 Abilitare la modalità di sblocco.

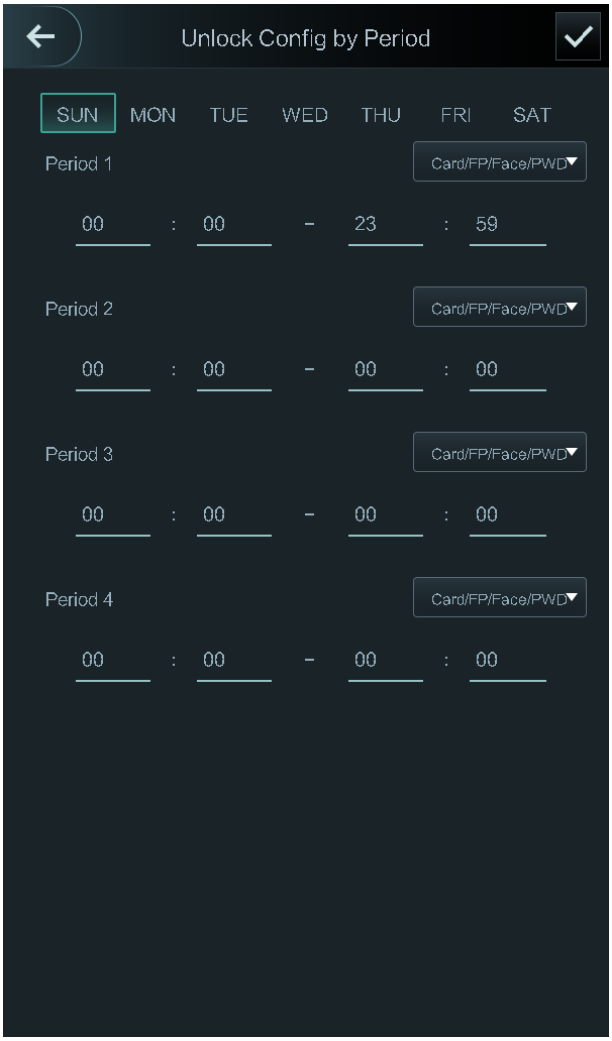
- ON significa abilitato.
- OFF significa non abilitato.

3.8.2.2 Sblocco per periodo

Le porte possono essere sbloccate attraverso diverse modalità di sblocco in periodi diversi. Ad esempio, nel periodo 1, la porta può essere aperta solo attraverso le carte; e nel periodo 2, le porte possono essere bloccate solo attraverso le facce.

Step 1 Seleziona **Accesso > Modalità di Sblocco > Sblocco per Periodo**.

Figure 3-8 Sblocco per Periodo



Step 2 Impostare l'ora di inizio e l'ora di fine per un periodo, quindi selezionare una modalità di sblocco.

Step 3 Selezion per salvare la configurazione.

Verrà visualizzata l'interfaccia della **modalità di sblocco**.

Step 4 Abilitare la modalità di sblocco.

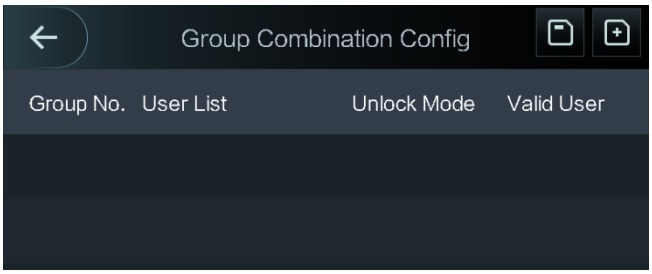
- ON significa abilitato.
- OFF significa non abilitato.

3.8.2.3 Combinazione Gruppi

Le porte possono essere sbloccate da un gruppo o gruppi costituiti da più di due utenti se la combinazione di gruppi è abilitata.

Step 1 Seleziona **Accesso > Modalità di Sblocco > Combinazione Gruppi**.

Figure 3-9 Combinazione Gruppi



Step 2 Seleziona  per creare un gruppo.

Figure 3-10 Aggiungere un gruppo

Table 3-4 Parametri Gruppo

Parameter	Description
Lista Utenti	Aggiungi utenti al gruppo appena creato. 1. Seleziona **Elenco utenti**. Viene visualizzata l'interfaccia **Elenco utenti**. 2. Seleziona  , ed inserisci user ID. 3. Seleziona  per salvare la configurazione.
Modalità di sblocco	Sono disponibili tre opzioni: **Tessera**, **Password** e **Volto**.
Utente valido	Gli utenti validi sono quelli che dispongono dell'autorizzazione di sblocco. Le porte possono essere sbloccate solo quando il numero di utenti per sbloccare le porte è uguale al numero utente valido. ● Gli utenti validi non possono superare il numero totale di utenti in un gruppo. ● Se gli utenti validi equivalgono al numero totale di utenti in un gruppo, le porte possono essere sbloccate solo da tutti gli utenti del gruppo. ● Se gli utenti validi sono inferiori al numero totale di utenti in un gruppo, le porte possono essere sbloccate da qualsiasi utente il cui numero sia uguale al numero utente valido.

Step 3 Seleziona per tornare all'interfaccia precedent.

Step 4 Selezion Per Salvare la configurazione.

Step 5 Abilita la **Combinazione di gruppi**.

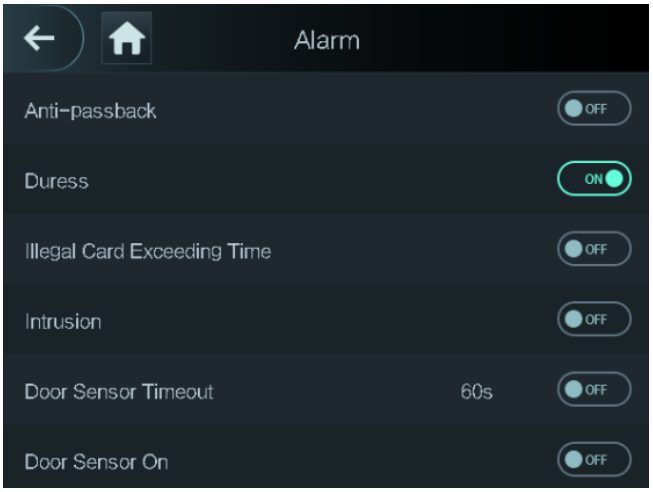
- significa abilitato.
- significa disabilitato.

3.8.3 Configurazione Allarme

Gli amministratori possono gestire l'autorizzazione di sblocco dei visitatori attraverso la configurazione degli allarmi.

Seleziona **Accesso > Allarme**. Viene visualizzata l'interfaccia di allarme.

Figure 3-11 Allarme



- significa abilitato.
- significa disabilitato.

Table 3-5 Parametri interfaccia di allarme

Parameter	Description
Anti-passback	Dopo aver abilitato l'anti-passback, gli utenti devono verificare l'identità sia per l'ingresso che per l'uscita; altrimenti verrà attivato un allarme.. ● Se una persona entra con l'identità verificata ed esce senza l'identità verificata, verrà attivato un allarme quando la persona tenta di entrare nuovamente e la persona non avrà più il permesso di sbloccare la porta. ● Se una persona entra senza l'identità controllata, verrà attivato un allarme quando la persona tenta di uscire con l'identità controllata e la persona non avrà più il permesso di sbloccare la porta.
Costrizione	Verrà attivato un allarme quando si utilizza una carta coercizione o una password coercizione per sbloccare la porta.

Parameter	Description
Tempo superamento carta illegale	Dopo che una carta non autorizzata viene utilizzata per sbloccare la porta più di 5 volte in 50 secondi, verrà attivato un allarme.
Intrusione	Un allarme antintrusione verrà attivato se una porta viene sbloccata senza che il contatto della porta venga rilasciato.
Timeout sensore porta	Un allarme di timeout verrà attivato se il tempo impiegato da un utente per sbloccare la porta supera il tempo di timeout del sensore della porta. L'intervallo di timeout del sensore porta è compreso tra 1 e 9999 secondi.
Sensore porta On	Solo quando è **attivato il sensore porta** è possibile attivare l'allarme di intrusione e il timeout del sensore porta.

3.8.4 Stato Porta

Sono disponibili tre opzioni: NO, NC e Normale.

- NO: se si seleziona **NO**, lo stato della porta è normalmente aperto, il che significa che la porta non verrà mai chiusa.NC:
- NC: se si seleziona **NC**, lo stato della porta è normalmente chiuso, il che significa che la porta non verrà sbloccata
- Normale: se si seleziona **Normale**, la porta verrà sbloccata e bloccata a seconda delle impostazioni.

3.8.5 Tempo di Blocco

Il **tempo di blocco** è la durata in cui la serratura è sbloccata. Se la serratura è stata sbloccata per un periodo superiore alla durata, la serratura verrà automaticamente bloccata.

3.9 Network

E' necessario configurare i parametri di rete, le porte seriali e le porte Wiegand per far funzionare normalmente il dispositivo.

3.9.1 Indirizzo IP

3.9.1.1 Configurazione IP

Configurare un indirizzo IP per il controller in modo che sia collegato alla rete. Vedi **Error! Reference source not found.** e **Error! Reference source not found.**.

Figure 3-12 Configurazione indirizzo IP

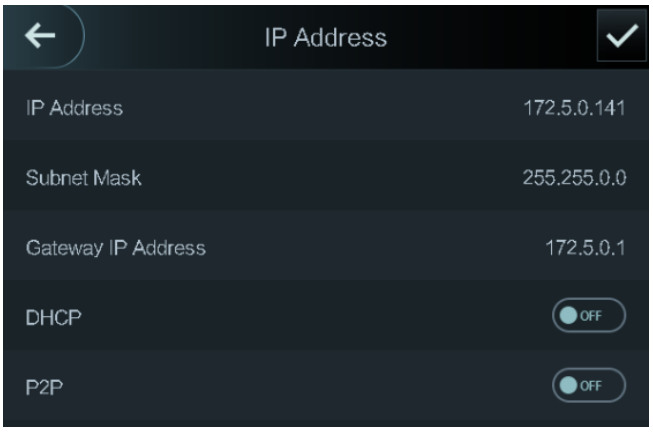


Table 3-6 Parametri configurazione IP

Parameter	Description
IP Address/Subnet Mask/Gateway IP Address	L'indirizzo IP, subnet mask, and gateway IP devono trovarsi sullo stesso segmento di rete. Dopo la configurazione, selezionare per salvare.
DHCP	DHCP (Dynamic Host Configuration Protocol). Quando il DHCP è abilitato, l'indirizzo IP può essere acquisito automaticamente e l'indirizzo IP, la subnet mask e l'indirizzo IP del gateway non possono essere configurati manualmente.
P2P	P2P è una tecnologia di attraversamento della rete privata che consente all'utente di gestire i dispositivi senza richiedere DDNS, mappatura delle porte o server di transito.

- Assicurarsi che il computer utilizzato per accedere al Web si trovi nella stessa LAN con il dispositivo.
- I controller di accesso modello X da 7 pollici hanno due schede NIC. L'indirizzo di gestione predefinito per la porta di rete 1000M è 192.168.1.108 e per la porta di rete 100M è 192.168.2.108.

3.9.1.2 Auto Register

Con l'auto register, è possibile connettere il controller di accesso alla piattaforma di gestione, quindi è possibile gestire il controller di accesso tramite la piattaforma di gestione.

Le configurazioni effettuate possono essere cancellate sulla piattaforma di gestione e il controller di accesso può essere inizializzato, è necessario proteggere l'autorizzazione di gestione della piattaforma in caso di perdita di dati causata da un funzionamento improprio.

Per I parametri, vedi Table 3-7.

Table 3-7 Active register

Name	Parameter
Server IP Address	Indirizzo IP della piattaforma di gestione.

Port	Numero di porta della piattaforma di gestione.
Device ID	Numero di dispositivo secondario sulla piattaforma di gestione.

3.9.1.3 Wi-Fi

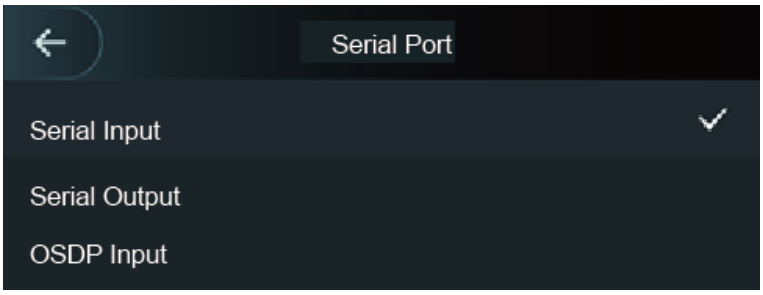
È possibile connettere il controller di accesso alla rete tramite Wi-Fi se il controller di accesso ha la funzione Wi-Fi..

3.9.2 Impostazioni Porta Seriale

Selezionare l'ingresso seriale o l'uscita seriale in base all'uso dei dispositivi esterni.

Seleziona **Connessioni > Serial Port**, verrà visualizzata l'interfaccia della **Serial Port**.

Figure 3-13 Serial port



- Selezionare **Ingresso seriale** quando dispositivi esterni dotati di funzioni di lettura e scrittura delle carte sono collegati al controller di accesso. **L'ingresso seriale** è selezionato per consentire l'invio delle informazioni della carta di accesso al controller di accesso e alla piattaforma di gestione.
- Per i controller di accesso con funzioni di riconoscimento facciale, lettura e scrittura delle carte, se si seleziona **Uscita seriale**, il controller di accesso invierà informazioni di blocco / sblocco al controller di accesso. Esistono due tipi di informazioni di blocco / sblocco:
  - ◇ User ID
  - ◇ Card No.
- Selezionare Ingresso OSDP quando il lettore di schede del protocollo OSDP è collegato al controller di accesso. Il controller di accesso può inviare le informazioni sulla carta alla piattaforma di gestione.

3.9.3 Configurazioen Wiegand

Seleziona **Wiegand Input** or **Wiegand Output**.

Selezioan **Connessioni > Wiegand**, l'interfaccia Wiegand verrà visualizzata.

Figure 3-14 Wiegand

- Selezionare **Wiegand Input** quando un meccanismo di scorrimento della scheda esterno è collegato al controller di accesso.
- Selezionare **Wiegand Output** quando il controller di accesso funziona come un lettore che può essere collegato al controller. See Table 3-8.

Table 3-8 Wiegand output

Parameter	Description
Wiegand Output Type	Il tipo di uscita Wiegand determina il numero della carta o la cifra del numero che può essere riconosciuto dal controller di accesso.. ● Wiegand26, 3 bytes, 6 digits. ● Wiegand34, 4 bytes, 8 digits. ● Wiegand66, 8 bytes, 16 digits.
Pulse Width	È possibile impostare la larghezza e l'intervallo degli impulsi.
Pulse Interval	
Output Data Type	È possibile selezionare i tipi di dati di output.. ● ID utente: se si seleziona ID utente, quindi verrà emesso l'ID utente. ● N. scheda: se si seleziona N. scheda, verrà emesso il numero della scheda.

3.10 Sistema

3.10.1 Time

È possibile eseguire le impostazioni del formato della data, dell'impostazione della data, dell'impostazione dell'ora, dell'ora legale, del controllo NTP e delle impostazioni del fuso orario.

- Quando si seleziona Network Time Protocol (NTP), è necessario prima abilitare la funzione di controllo NTP. Indirizzo IP del server: inserire l'indirizzo IP del time server, l'ora del controller di accesso verrà sincronizzata con il time server.
- Porta: immettere il numero di porta del time server.
- Intervallo (Intervallo (min): intervallo di controllo NPT. Tocca l'icona di salvataggio per salvare.

3.10.2 Parametri Volti

Figure 3-15 Face parameter

Seleziona un parametro ed esegui la configurazione, poi premi .

Table 3-9 Parametri Volti

Name	Description
Soglia di riconoscimento Volti	È possibile regolare la precisione del riconoscimento Volti. Maggiore è il valore, maggiore sarà l'accuratezza.

Name	Description
Angolo Max Riconoscimento Volti	Imposta l'angolo di ripresa dei profili sul pannello di controllo. Maggiore è il valore, verrà riconosciuta la gamma più ampia di profili.
Distanza pupillare	La distanza pupillare è il valore in pixel dell'immagine tra i centri delle pupille di ciascun occhio. È necessario impostare un valore appropriato in modo che il controller di accesso possa riconoscere i volti secondo necessità. Il valore cambia in base alle dimensioni del viso e alla distanza tra i volti e l'obiettivo. Più il viso è vicino all'obiettivo, maggiore dovrebbe essere il valore. Se un adulto si trova a 1,5 metri dall'obiettivo, il valore della distanza pupillare può essere compreso tra 50 e 70.
Timeout Riconoscimento	Quando una persona che non dispone dell'autorizzazione di accesso si trova di fronte al controller di accesso e ottiene il volto riconosciuto, il controller chiederà che il riconoscimento del volto non sia riuscito. L'intervallo di prompt si chiama timeout del riconoscimento.
Intervallo Riconoscimento	Quando una persona che dispone dell'autorizzazione di accesso si trova di fronte al controller di accesso e ottiene il volto riconosciuto, il controller chiederà che il riconoscimento del volto abbia avuto esito positivo. L'intervallo di prompt è l'intervallo di riconoscimento.
Invalid Messaggio Volto invalido	Quando una Volto senza l'autorizzazione di accesso si trova di fronte al controller di accesso, il controller Mostrerà un avviso.
Soglia Anti-fake	Questa funzione impedisce alle persone di sbloccarsi con immagini di volti umani o modelli di volti. Maggiore è il valore, più difficili sono le immagini dei volti che possono sbloccare la porta. L'intervallo di valori consigliato è superiore a 80.

Name	Description
Monitoraggio della temperatura	Set whether to enable the body temperature monitoring. ● Temp Unit: selezionare un'unità di temperatura. ● Temp Rect: Impostare se abilitare o meno la casella di monitoraggio della temperatura. ● Distanza Monitoraggio Temp (cm): Il valore è 0 per impostazione predefinita. Impostare altri valori per abilitare il monitoraggio della temperatura entro una distanza definita. 80 cm è raccomandato. ● Soglia Temp (°C): Imposta la soglia di temperatura. La temperatura corporea monitorata verrà giudicata come temperatura elevata se è maggiore o uguale al valore impostato. ● Valore Correzione Temp: Questo parametro serve per il test. La differenza dell'ambiente di monitoraggio della temperatura potrebbe causare una differenza tra la temperatura monitorata e la temperatura effettiva. È possibile selezionare più campioni monitorati per il test, quindi correggere la differenza della temperatura con questo parametro in base al confronto tra la temperatura monitorata e la temperatura effettiva. Ad esempio, se la temperatura monitorata è inferiore di 0,5 ° C rispetto alla temperatura effettiva, il valore di correzione è impostato su 0,5 ° C; se la temperatura monitorata è superiore di 0,5 ° C rispetto alla temperatura effettiva, il valore di correzione è impostato su -0,5 ° C. Solo il controller con un'unità di monitoraggio della temperatura supporta questo parametro.
Modalità Maschera	● Nessun rilevamento: la maschera non viene rilevata durante il riconoscimento facciale. ● Promemoria maschera: la maschera viene rilevata durante il riconoscimento facciale. Se la persona viene rilevata senza indossare una mascherina, il sistema richiederà il promemoria della maschera e il passaggio è consentito. ● Intercettazione maschera: la maschera viene rilevata durante il riconoscimento facciale. Se la persona viene rilevata senza indossare una maschera, il sistema richiederà il promemoria della maschera e il passaggio non è consentito.

3.10.3 Modalità Immagine

Ci sono tre opzioni:

- Interno: selezionare **Interno** quando il controller di accesso è installato all'interno;
- Esterno: selezionare **Esterno** quando il controller di accesso è installato all'aperto;
- Altro: selezionare **Altro** quando il controller di accesso è installato in luoghi con retroilluminazione come corridoi e corridoi.

3.10.4 Impostazione modalità luce di cortesia

È possibile selezionare le modalità di riempimento della luce in base alle proprie esigenze. Esistono tre modalità:

- Auto: quando il sensore fotografico rileva che l'ambiente circostante non è buio, la luce di cortesia è normalmente spenta; altrimenti, la luce di cortesia sarà accesa.
- NO: la luce di cortesia è normalmente accesa.
- NC: la luce di cortesia è normalmente spenta.

3.10.5 Impostazione Luminosità luce di cortesia

È possibile selezionare la luminosità della luce di Cortesia in base alle proprie esigenze.

3.10.6 Regolazione Volume

Premere  o  per regolare il volume.

3.10.7 Regolazione Luminosità IR

Maggiore è il valore, più chiare saranno le immagini; altrimenti le immagini saranno poco chiare.

3.10.8 Ripristino impostazioni di fabbrica

- I dati andranno persi se si ripristina il controller di accesso alle impostazioni di fabbrica.
- Dopo aver ripristinato le impostazioni di fabbrica del controller di accesso, l'indirizzo IP non verrà modificato.

È possibile selezionare se conservare le informazioni e i registri dell'utente.

- È possibile selezionare per ripristinare il controller di accesso alle impostazioni di fabbrica con tutte le informazioni sull'utente e sul dispositivo eliminate.
- E' possibile selezionare per ripristinare il controller di accesso alle impostazioni di fabbrica con le informazioni utente e le informazioni sul dispositivo conservate..

3.10.9 Riavvio

Selziona **Impostazioni > Reboot**, seleziona **Reboot**, il dispositivo si riavvierà.

3.11 USB

- Assicurarsi che l'USB sia inserito prima di esportare le informazioni utente e l'aggiornamento. Durante l'esportazione o l'aggiornamento, non estrarre l'USB né eseguire altre operazioni; altrimenti l'esportazione o l'aggiornamento falliranno.
- È necessario importare informazioni da un controller di accesso a USB prima di utilizzare USB per importare informazioni in un altro controller di accesso.
- USB può essere utilizzato anche per aggiornare il programma.

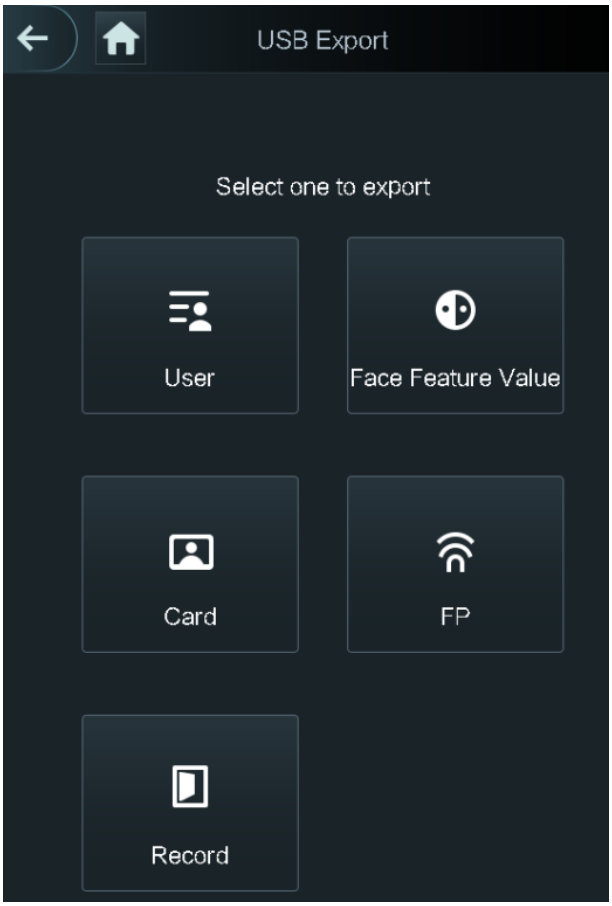
3.11.1 Esportazione USB

È possibile esportare i dati dal controller di accesso all'USB dopo aver inserito l'USB. I dati esportati sono crittografati e non possono essere modificati.

Step 1 Seleziona **USB > USB Export**.

L'interfaccia **USB Export** verrà mostrata See Figure 3-16.

Figure 3-16 USB export



Step 2 Selezionare il tipo di dati che si desidera esportare.

Viene visualizzato il messaggio Conferma di esportazione.

Step 3 seleziona **OK**.

I dati esportati saranno salvati sulla chiavetta USB.

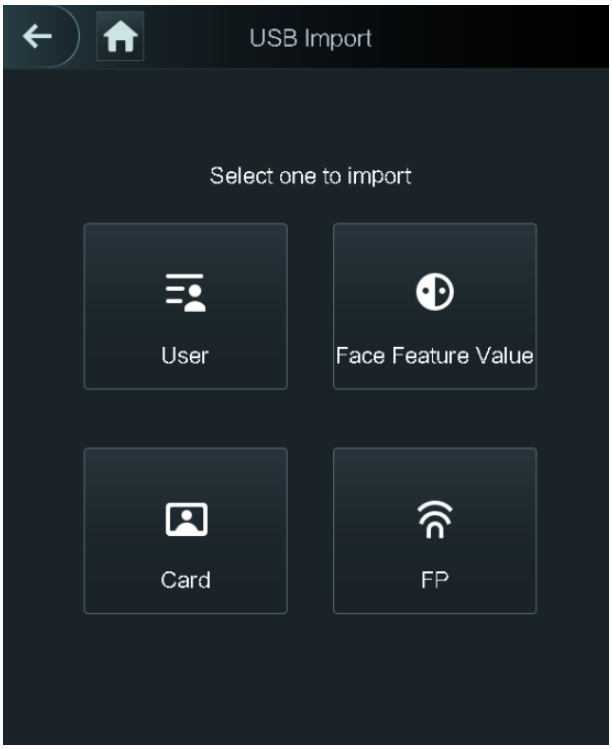
3.11.2 USB Import

Solo i dati nell'USB esportati da un controller di accesso possono essere importati in un altro controller di accesso.

Step 1 Seleziona **USB > USB Import.**

L'interfaccia **USB Import** verrà mostrata sul display. See Figure 3-17.

Figure 3-17 USB Import



Step 2 Selezionare il tipo di dati che si desidera importare.

Viene visualizzato il messaggio **Conferma importazione**.

Step 3 seleziona **OK**.

I dati verranno importati dalla chiavetta USB.

3.11.3 USB Update

La chiavetta USB può essere utilizzata per aggiornare il sistema.

Step 1 Rinominare il file di aggiornamento in "update.bin" e salvare il file "update.bin" nella directory principale dell'unità flash USB.

- Assicurarsi che il computer utilizzato per accedere al Web si trovi nella stessa LAN con il dispositivo.
- I controller di accesso modello X da 7 pollici hanno due schede NIC. L'indirizzo di gestione predefinito per la porta di rete 1000M è 192.168.1.108 e per la porta di rete 100M è 192.168.2.108.

Step 2 Seleziona **USB > USB Update**.

Il messaggio **Conferma aggiornamento** verrà visualizzato.

Step 3 Seleziona **OK**.

L'aggiornamento si avvia e il controller di accesso si riavvia al termine dell'aggiornamento.

3.12 Caratteristiche

È possibile eseguire impostazioni relative alla privacy, inversione del numero di carta, modulo di sicurezza, tipo di sensore porta e feedback dei risultati. Per i dettagli delle funzioni menzionate, vedi Figure 3-18 e Table 3-10.

Figure 3-18 Caratteristiche

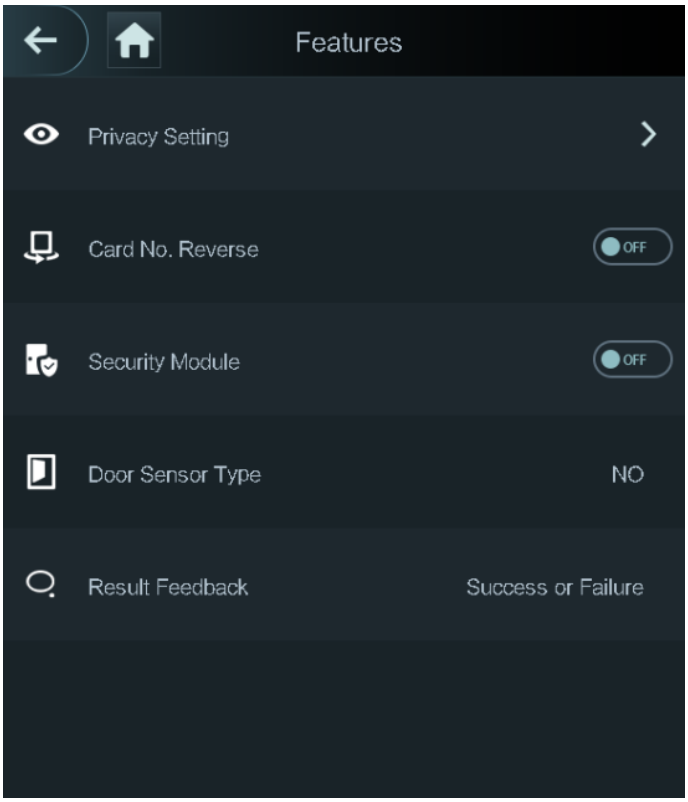


Table 3-10 Descrizione

Parameter	Description
Privacy Setting	Vedi "3.12.1 Privacy Setting" per dettagli.
Card No. Reverse	Se il lettore di schede di terze parti deve essere collegato al controller di accesso tramite la porta di uscita wiegand, è necessario abilitare la funzione Reverse No. scheda; in caso contrario, la comunicazione tra il controller di accesso e il lettore di schede di terze parti potrebbe non riuscire a causa della discrepanza del protocollo.
Security Module	• Se il modulo di sicurezza è abilitato, è necessario acquistare separatamente il modulo di sicurezza del controllo di accesso. Il modulo di sicurezza necessita di un alimentatore separato per fornire energia. • Una volta abilitato il modulo di sicurezza, il pulsante di uscita, il controllo di blocco e il collegamento antincendio non saranno più validi.
Tipo di sensore porta	Esistono due opzioni: **NO** e **NC**.
Result Feedback	Mostra se lo sblocco è riuscito o meno.

3.12.1 Privacy Setting

Figure 3-19 Privacy setting

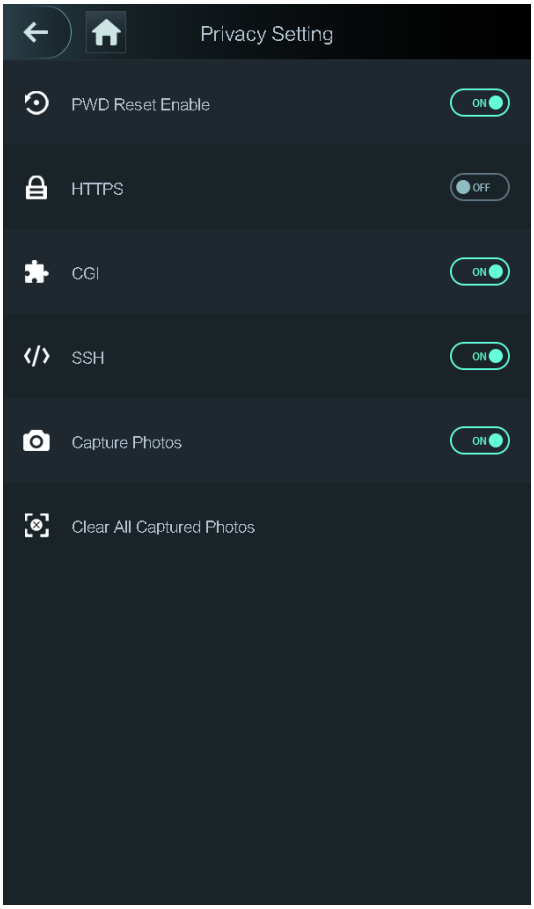


Table 3-11 Features

Parameter	Description
Abilita PWD Reset	Se la funzione Abilita ripristino PWD è abilitata, è possibile ripristinare la password. La funzione di ripristino PWD è abilitata per impostazione predefinita.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) è un protocollo per la comunicazione sicura su una rete di computer. Quando HTTPS è abilitato, HTTPS verrà utilizzato per accedere ai comandi CGI; altrimenti verrà utilizzato HTTP. Quando HTTPS è abilitato, il controller di accesso si riavvierà automaticamente.
CGI	Common Gateway Interface (CGI) offre un protocollo standard per i server Web per eseguire programmi che eseguono come applicazioni console in esecuzione su un server che genera pagine Web in modo dinamico. Quando CGI è abilitato, è possibile utilizzare i comandi CGI. Il CGI è abilitato per impostazione predefinita.

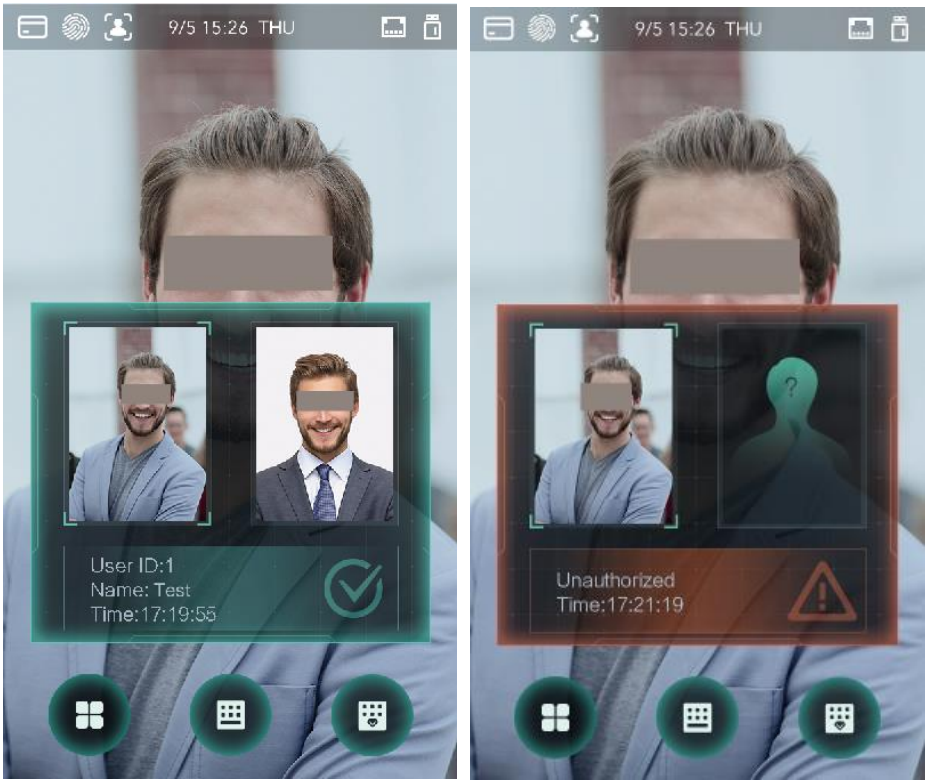
Parameter	Description
SSH	Secure Shell (SSH) è un protocollo di rete crittografica per il funzionamento sicuro dei servizi di rete su una rete non protetta. Quando SSH è abilitato, SSH fornisce un servizio crittografico per la trasmissione dei dati.
Scatta foto	Se si seleziona ON, quando un utente apre la porta, la foto dell'utente verrà automaticamente scattata. Questa funzione è attivata per impostazione predefinita.
Cancella tutte le foto catturate	Tocca l'icona e puoi eliminare tutte le foto catturate.

3.12.2 Result Feedback

È possibile selezionare una modalità di feedback dei risultati secondo necessità.

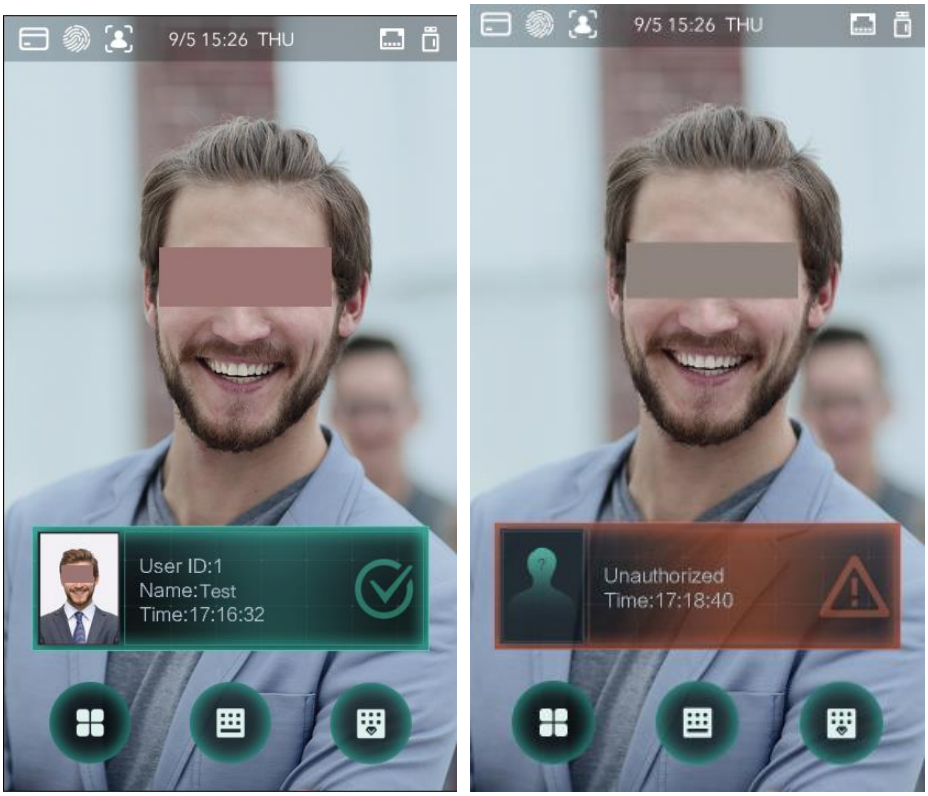
Mode 1

Figure 3-20 Mode 1



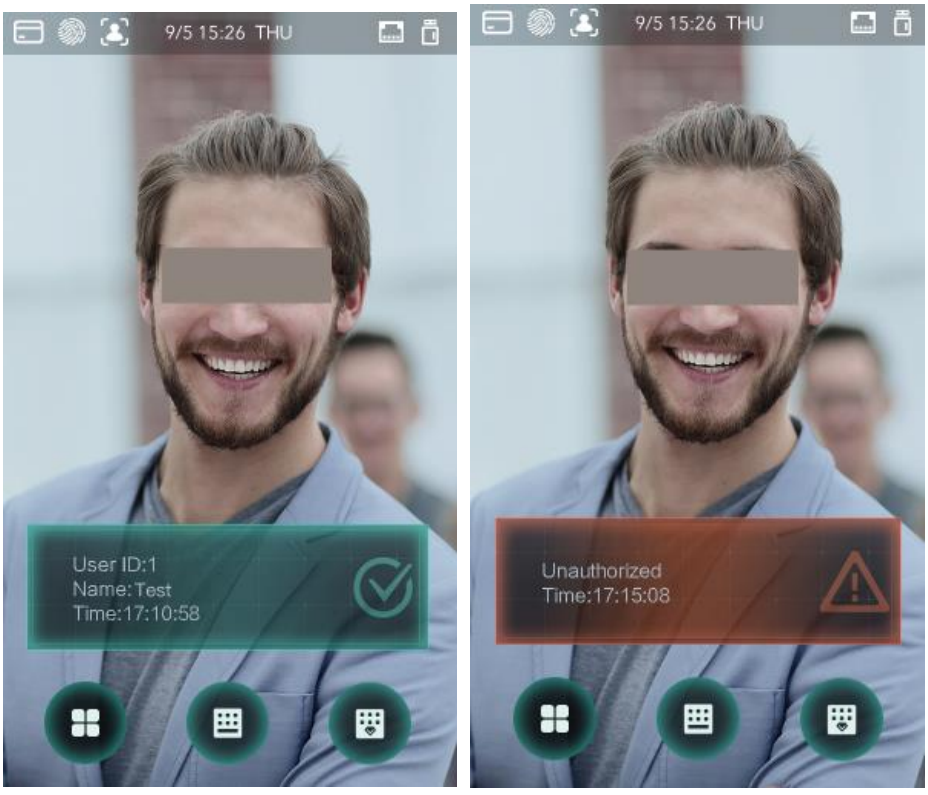
Mode 2

Figure 3-21 Mode 2



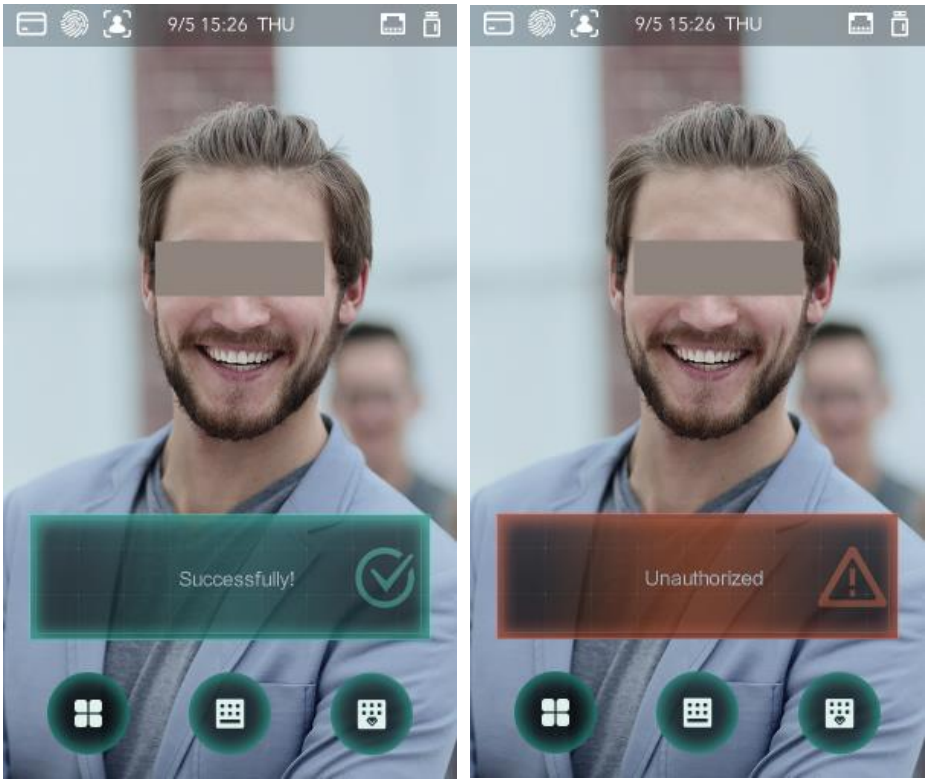
Mode 3

Figure 3-22 Mode 3



Mode 4

Figure 3-23 Mode 4



3.13 Record

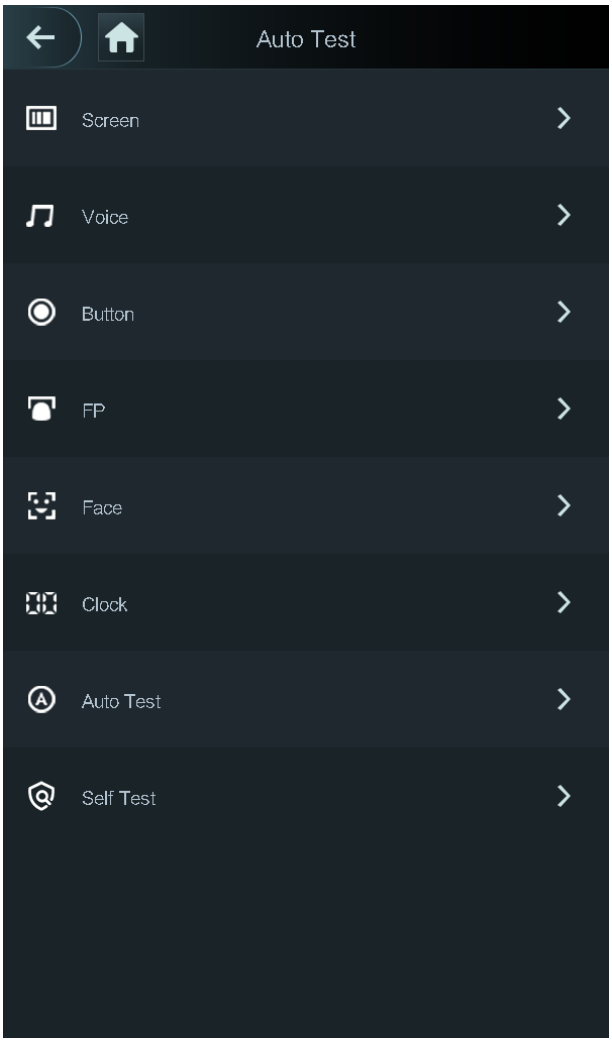
È possibile eseguire una query su tutti i record di sblocco.

Figure 3-24 Search punch records

3.14 Auto Test

Quando si utilizza il controller di accesso per la prima volta o quando il controller di accesso non funziona correttamente, è possibile utilizzare la funzione di test automatico per verificare se il controller di accesso può funzionare normalmente. Fare azioni secondo le istruzioni.

Figure 3-25 Auto test



Quando si seleziona Test automatico, il controller di accesso guida l'utente a eseguire tutti i test automatici..

3.15 System Info

È possibile visualizzare la capacità dei dati, la versione del dispositivo e le informazioni sul firmware del controller di accesso nell'interfaccia Informazioni di sistema.

4 Operazioni Web

Il controller di accesso può essere configurato e gestito sul Web. Tramite il Web è possibile impostare parametri di rete, parametri video e parametri del controller di accesso; e puoi anche mantenere e aggiornare il sistema.

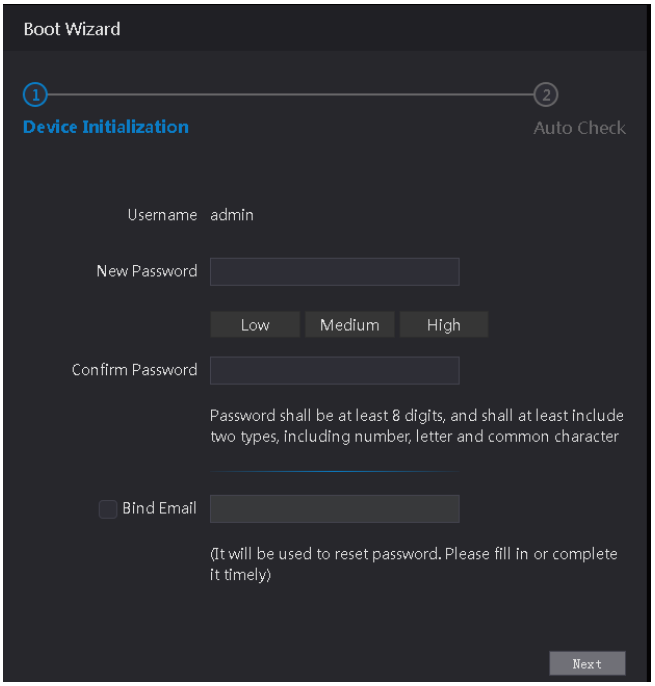
4.1 Inizializzazione

È necessario impostare una password e un indirizzo e-mail prima di accedere al Web per la prima volta.

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

- Utilizzare un browser più recente di Internet Explorer 8, altrimenti non è possibile accedere al Web.
- Assicurarsi che il computer utilizzato per accedere al Web si trovi nella stessa LAN con il dispositivo.
- I controller di accesso modello X da 7 pollici hanno due schede NIC. 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 Initialization



Step 2 Inserire la nuova password, confermare la password, immettere un indirizzo e-mail, quindi fare clic su **Avanti**.

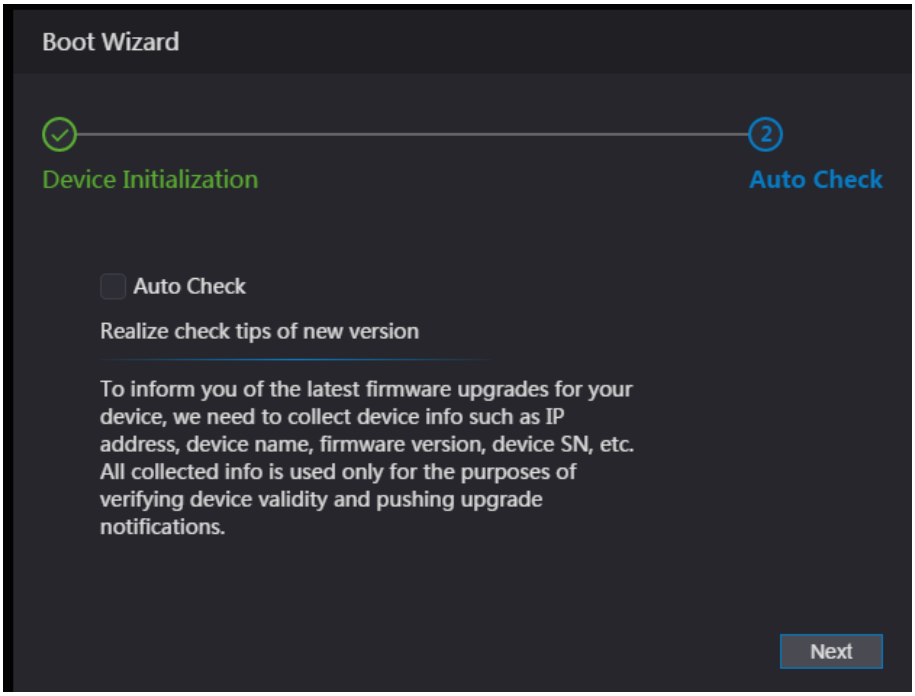
- La password deve contenere da 8 a 32 caratteri non vuoti e contenere almeno due tipi di caratteri tra maiuscolo, minuscolo, numero e carattere speciale (escluso

'";: &). Impostare una password di livello di sicurezza elevato in base al prompt di sicurezza della password.

- Per motivi di sicurezza, conservare correttamente la password dopo l'inizializzazione e cambiarla regolarmente.
- Quando è necessario reimpostare la password dell'amministratore tramite la scansione del codice QR, è necessario un indirizzo e-mail per ricevere il codice di sicurezza..

Step 3 Premere **Next**.

Figure 4-2 Auto check

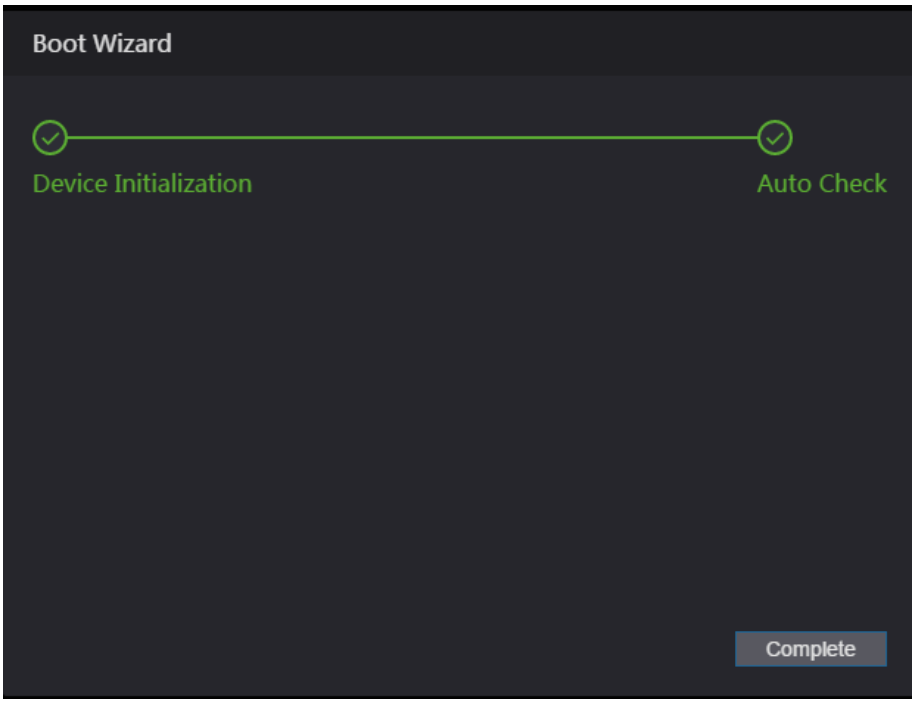


Step 4 È possibile decidere se selezionare Verifica automatica o meno.

Si consiglia di selezionare Auto Check per ottenere il programma più recente in tempo..

Step 5 premere **Next**.

Figure 4-3 Finished configuration



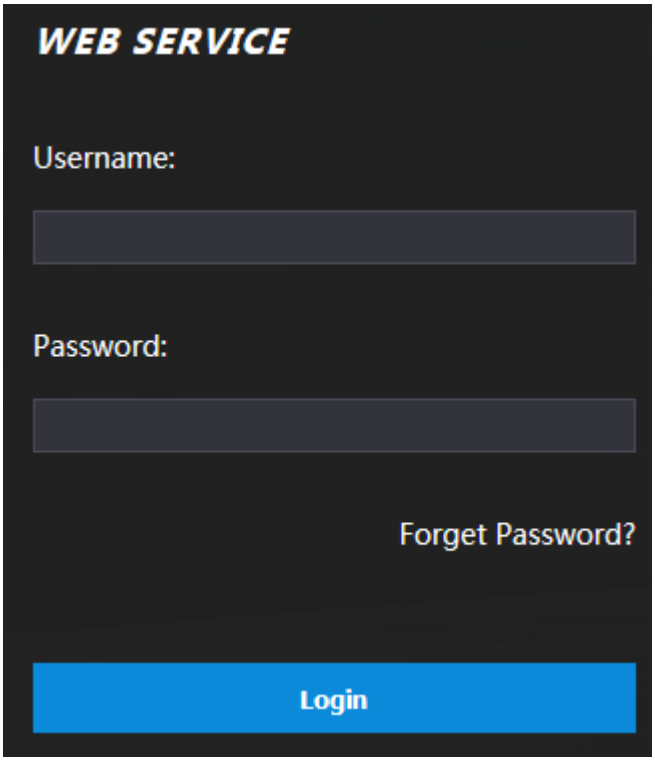
Step 1 Fare clic su **Completa** e l'inizializzazione è completata.
Viene visualizzata l'interfaccia di accesso Web.

4.2 Login

Step 2 Aprire il browser Web IE, inserire l'indirizzo IP del controller di accesso nella barra degli indirizzi e premere **Invio**.

- Utilizzare un browser più recente di Internet Explorer 8, altrimenti non è possibile accedere al Web.
- Assicurarsi che il computer utilizzato per accedere al Web si trovi nella stessa LAN con il dispositivo.
- I controller di accesso modello X da 7 pollici hanno due schede NIC. 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 4-4 Login



Step 3 Inserire username e password.

- Il nome amministratore predefinito è admin e la password è la password di accesso dopo l'inizializzazione del controller di accesso. Modifica l'amministratore regolarmente e conservalo correttamente per motivi di sicurezza.
- Se si dimentica la password di accesso dell'amministratore, è possibile fare clic su **Password dimenticata?** per resettarlo. Vedi "4.3 Reimpostazione della password."

Step 4 Selezionare **Login**.

Il login alla pagina web è avvenuto.

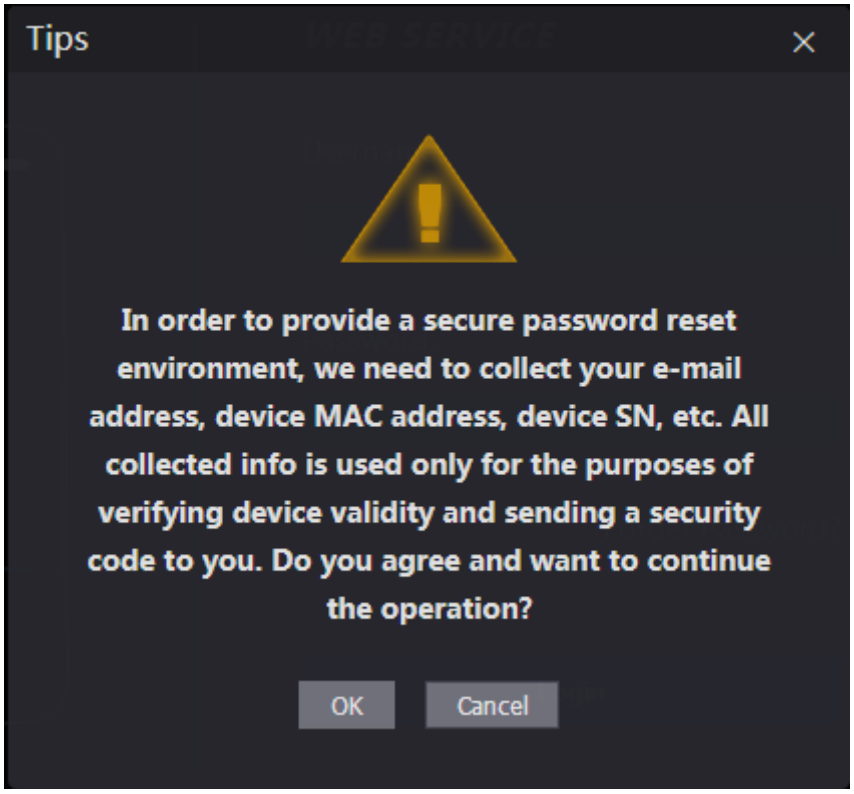
4.3 Reset Password

Quando si reimposta la password dell'account amministratore, sarà necessario il proprio indirizzo e-mail.

Step 1 Seleziona **Password Dimenticata?** Nella pagina di login.

La pagina dei suggerimenti verrà visualizzata.

Figure 4-5 Tips

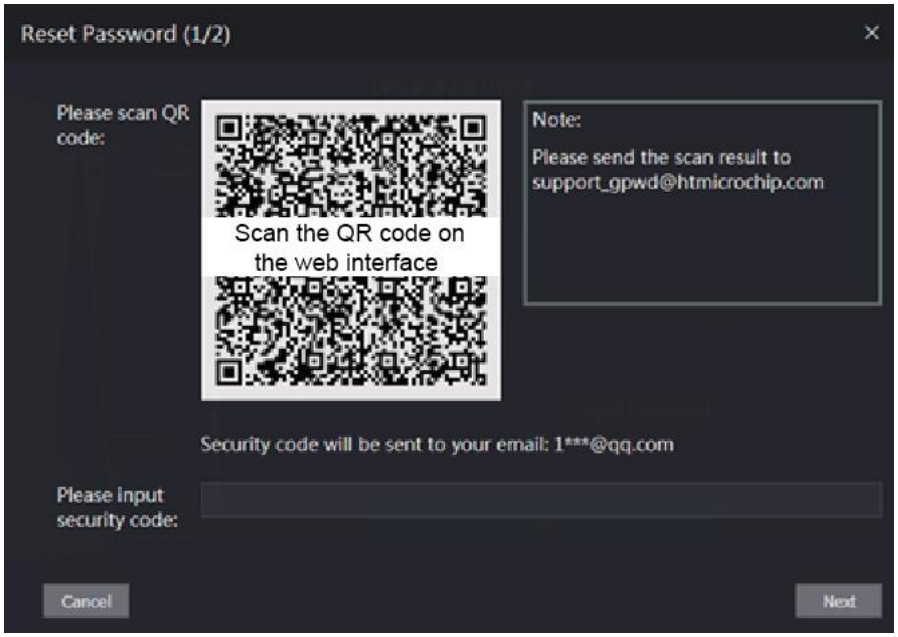


Step 2 Leggere I suggerimenti.

Step 3 premere **OK**.

L'interfaccia di **Reset Password** verrà visualizzata.

Figure 4-6 Reset Password



Step 4 Scansiona il codice QR e otterrai il codice di sicurezza.

- Al massimo due codici di sicurezza verranno generati scansionando lo stesso codice QR. Se i codici di sicurezza diventano non validi, per ottenere più codici di sicurezza, aggiornare il codice QR.

- Inviare il contenuto che ottieni dopo aver scansionato il codice QR all'indirizzo di posta elettronica designato, quindi otterrai il codice di sicurezza.
- Utilizzare il codice di sicurezza entro 24 ore dalla ricezione. Altrimenti, non sarà più valido.
- Se vengono immessi codici di sicurezza errati per cinque volte consecutive, l'amministratore verrà bloccato per cinque minuti.

Step 5 Inserire il codice di sicurezza ricevuto.

Step 6 selezionare **Next**.

L'interfacia **Reset Password** verrà visualizzata.

Step 7 Reset e conferma la buova password.

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 '";: &).

Step 8 Selezionare **OK**, il reset password è completato.

4.4 Alarm Linkage

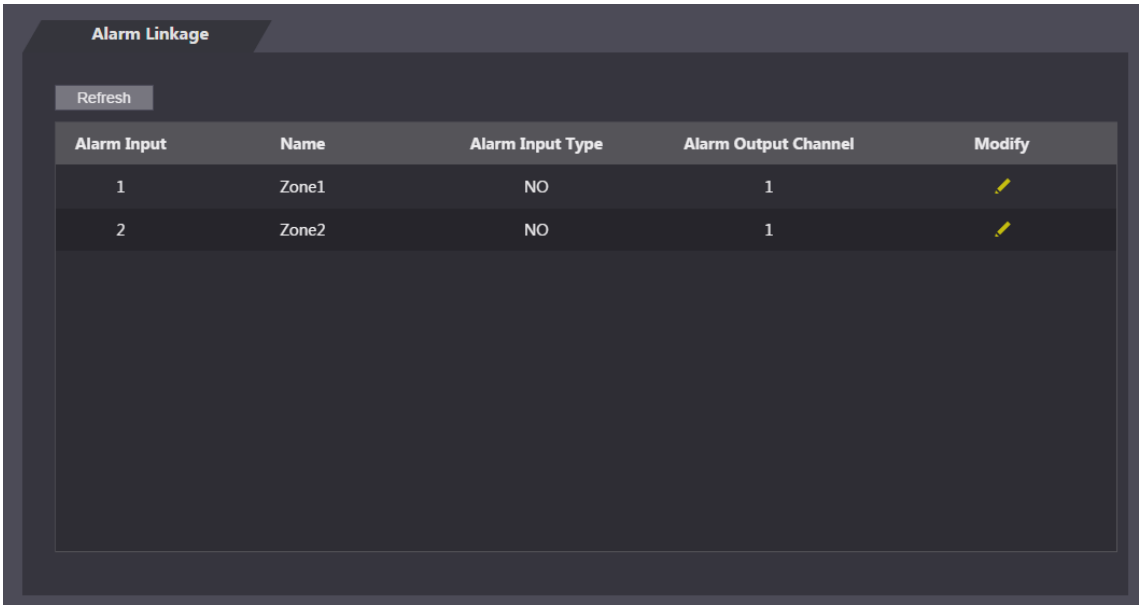
4.4.1 Impostazione Alarm Linkage

I dispositivi di ingresso allarme possono essere collegati al controller di accesso e, se necessario, è possibile modificare il parametro di collegamento allarme.

Step 1 Seleziona **Alarm Linkage** nella barra di navigazione.

L'interfaccia **Alarm Linkage** verrà visualizzata. See Figure 4-7.

Figure 4-7 Alarm linkage



Step 2 Seleziona  , ora potrai modificare I parametri. See **Error! Reference source not found.**

Figure 4-8 Modifica Parametri Alarm Linkage

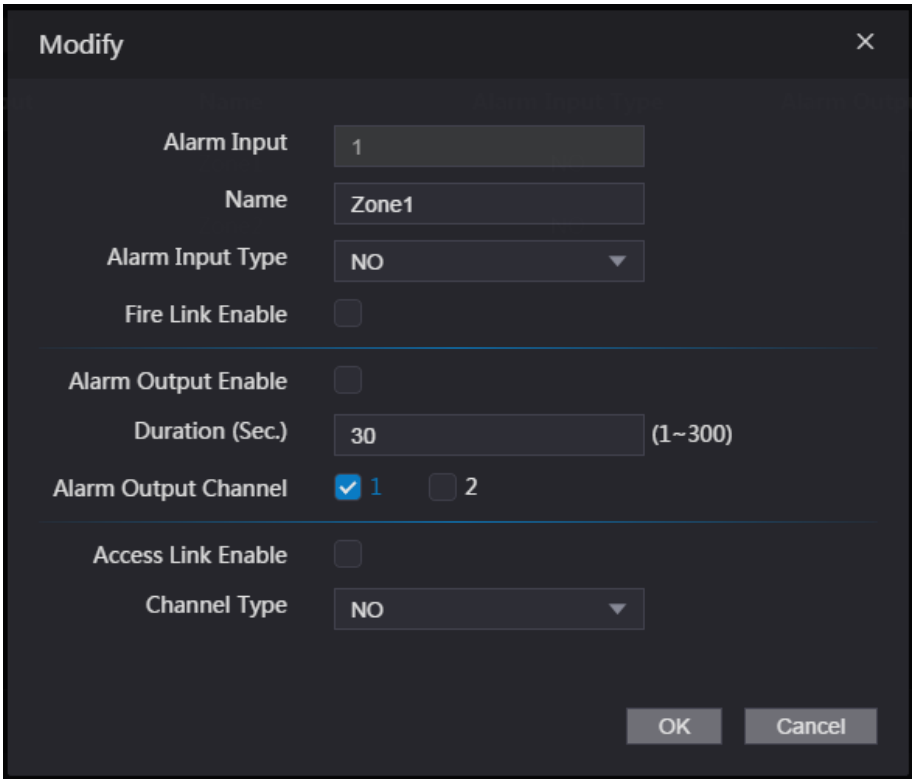


Table 4-1 Alarm linkage parameter description

Parameter	Description
Ingresso di allarme	Non è possibile modificare il valore.
Nome	Inserire il nome zona.
Tipo di ingresso allarme	Esistono due opzioni: NO e NC. Se il tipo di ingresso allarme del dispositivo di allarme acquistato è NO, selezionare NO; altrimenti dovresti selezionare NC.
Allarme incendio Abilitato	Se il collegamento antincendio è abilitato, il controller di accesso emetterà allarmi quando vengono attivati gli allarmi antincendio. I dettagli dell'allarme verranno visualizzati nel registro degli allarmi. L'uscita allarme e il collegamento d'accesso sono NO per impostazione predefinita se il collegamento incendio è abilitato.
Abilitazione uscita allarme	Il relè può emettere informazioni di allarme (verranno inviate alla piattaforma di gestione) se **l'uscita di allarme** è abilitata.
Durata (Sec.)	durata dell'allarme, l'intervallo è compreso tra 1 e 300 secondi.
Canale di uscita dell'allarme	È possibile selezionare un canale di uscita dell'allarme in base al dispositivo di allarme installato. Ogni dispositivo di allarme può essere considerato come un canale.
Access Link Enable	Dopo aver abilitato il collegamento di accesso, il controller di accesso sarà normalmente acceso o normalmente chiuso quando sono presenti segnali di allarme in ingresso.
Tipo Canale	Esistono due opzioni: NO e NC.

Step 3 Seleziona **OK**, la configurazione è eseguita.

La configurazione sul Web verrà sincronizzata con la configurazione nel client se il controller di accesso viene aggiunto a un client.

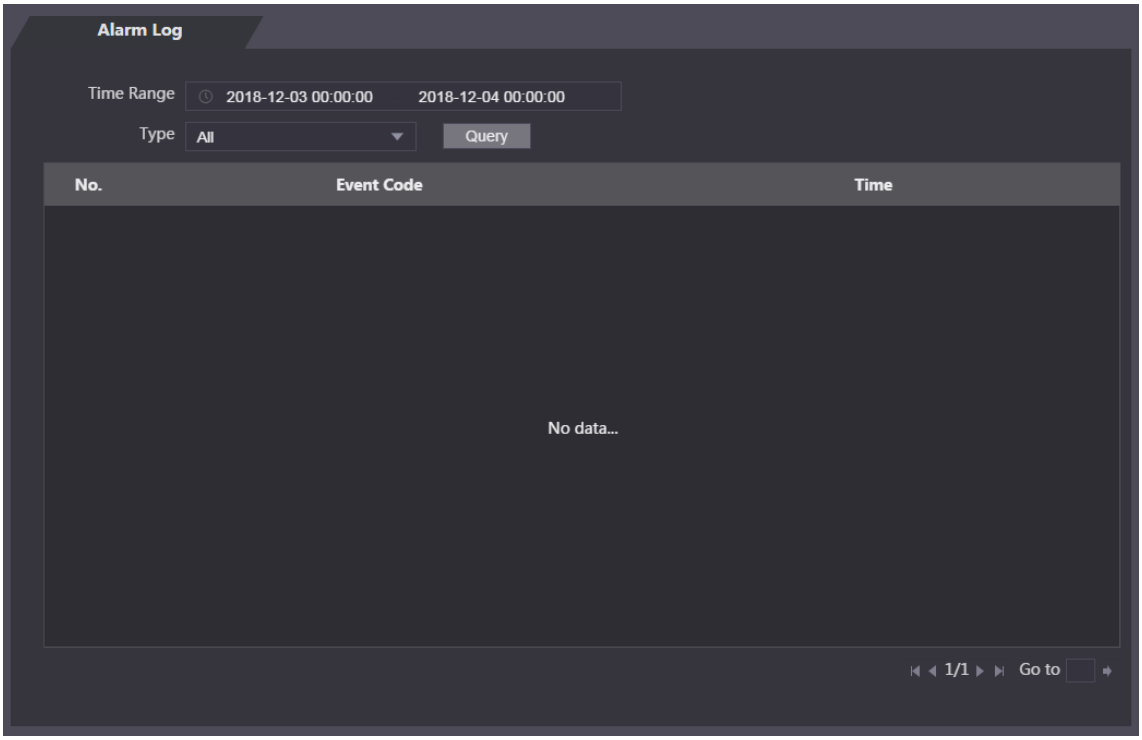
4.4.2 Log Allarme

È possibile visualizzare il tipo di allarme e l'intervallo di tempo nell'interfaccia Registro allarmi.

Step 1 Seleziona **Alarm Linkage > Alarm Log**.

L'interfaccia **Alarm Log** viene visualizzata sul display. See Figure 4-9.

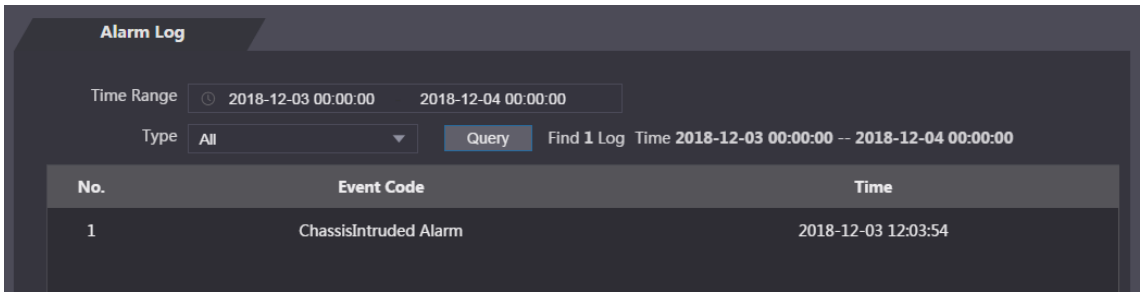
Figure 4-9 Alarm log



Step 2 Selezionare un intervallo di tempo e un tipo di allarme, quindi fare clic su **Query**.

Vengono visualizzati i risultati della query. See Figure 4-10.

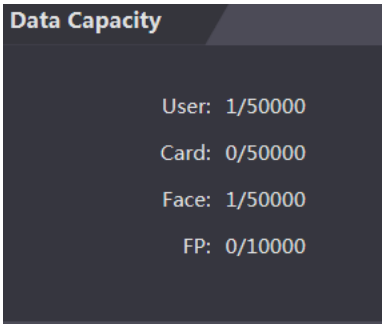
Figure 4-10 Query results



4.5 Capacità Dati

Puoi vedere quanti utenti, schede e immagini di volti possono essere conservati dal controller di accesso nell'interfaccia Capacità dati.

Figure 4-11 Data capacity



4.6 Impostazioni Video

È possibile impostare parametri tra cui velocità dati, parametri immagine (luminosità, contrasto, tonalità, saturazione e altro) ed esposizione nell'interfaccia Impostazioni video.

4.6.1 Data Rate

Figure 4-12 Data rate

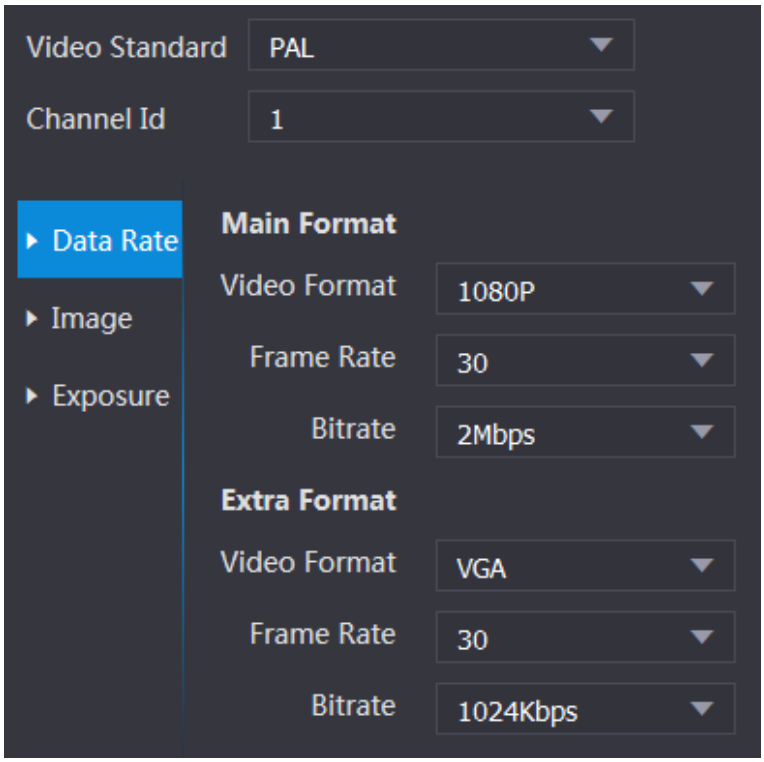


Table 4-2 Data rate parameter description

Parameter	Description
Video Standard	Esistono due opzioni: NTSC e PAL. Seleziona uno standard in base allo standard video della tua regione.
Canale	Sono disponibili due opzioni: 1 e 2. 1 è la fotocamera a luce bianca e 2 è la fotocamera a luce IR.

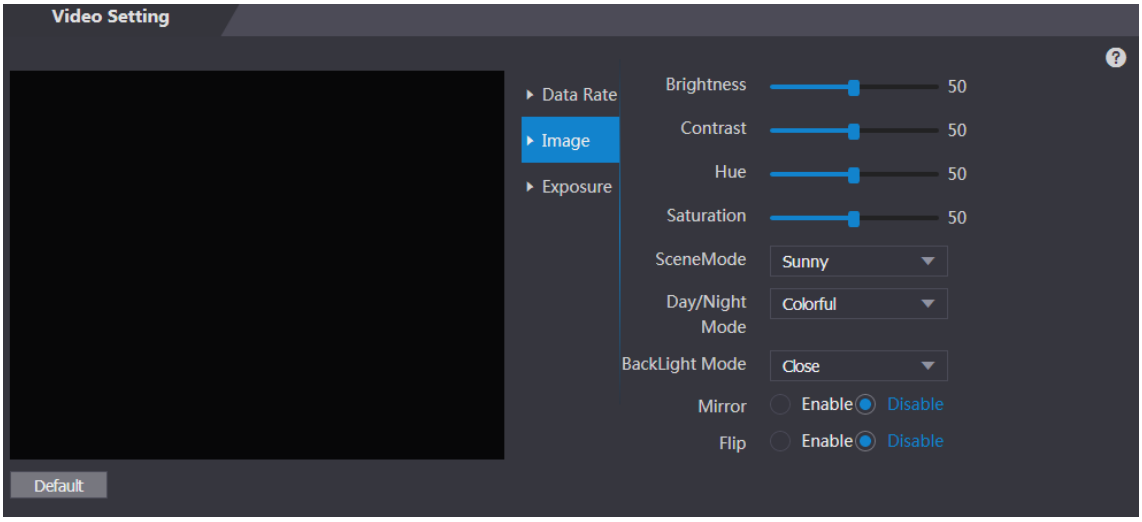
Parameter		Description
Main Format	Video Format	Sono disponibili quattro opzioni: D1, VGA, 720p e 1080p. Seleziona un'opzione in base alla qualità video che desideri.
	Frame Rate	La velocità con cui i fotogrammi consecutivi vengono visualizzati su un display. L'intervallo della frequenza dei fotogrammi è compreso tra 1 e 30 fps.
	Bit Rate	Il numero di bit che vengono convogliati o elaborati per unità di tempo. Sono disponibili cinque opzioni: 2 Mbps, 4 Mbps, 6 Mbps, 8 Mbps e 10 Mbps.
Extra Format	Video Format	Sono disponibili tre opzioni: D1, VGA e QVGA.
	Frame Rate	La velocità con cui i fotogrammi consecutivi vengono visualizzati su un display. L'intervallo della frequenza dei fotogrammi è compreso tra 1 e 30 fps.
	Bit Rate	Il numero di bit che vengono convogliati o elaborati per unità di tempo. Sono disponibili opzioni: 512 Kbps, 640 Kbps, 768 Kbps, 896 Kbps, 1024 Kbps, 1,25 Mbps, 1,5 Mbps, 1,75 Mbps e 2 Mbps.

4.6.2 Immagine

Esistono due canali ed è necessario configurare i parametri per ciascun canale.

Step 1 Seleziona **Video Setting > Video Setting > Image**.

Figure 4-13 Image



Step 2 Seleziona **Wide Dynamic** In Modalità di retroilluminazione.

Table 4-3 Image parameter description

Parameter	Description
Luminosità	Maggiore è il valore, più luminose saranno le immagini.

Parameter	Description
Contrasto	Il contrasto è la differenza di luminanza o colore che rende distinguibile un oggetto. Maggiore è il valore del contrasto, maggiore sarà la luminosità e il contrasto del colore.
Colore	Maggiore è il valore, più profondo sarà il colore.
Saturazione	Maggiore è il valore, più brillanti saranno i colori. Il valore non cambia la luminosità dell'immagine.
Scene Mode	● Chiudi: senza modalità. ● Auto: il sistema regola automaticamente le modalità scena. ● Soleggiato: in questa modalità, la tonalità dell'immagine verrà ridotta. ● Notte: in questa modalità, la tonalità dell'immagine verrà aumentata. **Soelggiato** è selezionato di Default.
Day/Night Mode	Day/Night mode decides the working status of the fill light. ● Auto: il sistema regola automaticamente le modalità giorno / notte. ● Colore: in questa modalità, le immagini sono a colori. ● Bianco e nero: in questa modalità, le immagini sono in bianco e nero.
Back Light Mode	● Close: Senza compensazione backlight. ● BLC: La compensazione del controluce corregge le regioni con livelli di luce estremamente alti o bassi per mantenere un livello di luce normale e utilizzabile per l'oggetto a fuoco. ● WDR: Nella modalità WDR, il sistema attenua le aree luminose e compensa le aree scure per garantire la definizione di oggetti nelle aree chiare e scure. Quando i volti umani sono in controluce, è necessario abilitare WDR. ● HLC: la compensazione dell'evidenziazione è necessaria per compensare la sovraesposizione di luci o fonti luminose intense come faretti, fari, luci del portico, ecc. Per creare un'immagine utilizzabile e non superata da una luce intensa.
Mirror	Quando la funzione è abilitata, le immagini verranno visualizzate con i lati sinistro e destro invertiti.
Flip	Quando questa funzione è abilitata, è possibile capovolgere le immagini.

4.6.3 Esposizione

Table 4-4 Exposure parameter description

Parameter	Description
Anti-flicker	● □ 50Hz: quando la frequenza di servizio della corrente alternata è 50Hz, l'esposizione viene regolata automaticamente per assicurarsi che non vi siano strisce sulle immagini. ● □ 60Hz: quando la frequenza di utilizzo della corrente alternata è 60Hz, l'esposizione viene regolata automaticamente per assicurarsi che non vi siano strisce sulle immagini. ● □ Esterno: quando si seleziona **Esterno**, è possibile cambiare la modalità di esposizione.
Exposure Mode	🕮 ● Quando si seleziona Esterno nell'elenco a discesa Anti-sfarfallio, è possibile selezionare Priorità otturatore come modalità di esposizione. ● Le modalità di esposizione di diversi dispositivi possono variare e il prodotto reale prevarrà. Puoi selezionare da: ● Auto: il controller di accesso regola automaticamente la luminosità delle immagini. ● Priorità dell'otturatore: il controller di accesso regola la luminosità dell'immagine in base all'intervallo del valore di esposizione dell'otturatore. Se la luminosità dell'immagine non è sufficiente e il valore dell'otturatore ha raggiunto il limite superiore o inferiore, il controller di accesso regolerà automaticamente il valore del guadagno per ottenere la luminosità ideale. ● Manuale: è possibile configurare manualmente il guadagno e il valore dell'otturatore per regolare la luminosità dell'immagine.
Shutter	Maggiore è il valore dell'otturatore e minore è il tempo di esposizione, più scure saranno le immagini.
Shutter Value Range	Se si seleziona Intervallo personalizzato, è possibile personalizzare l'intervallo di valori dell'otturatore.
Gain Value Range	Quando viene impostato l'intervallo del valore di guadagno, la qualità video verrà migliorata.
Exposure Compensation	È possibile aumentare la luminosità del video regolando il valore di compensazione dell'esposizione.
3D NR	Quando la riduzione del rumore 3D (RD) è abilitata, il rumore video può essere ridotto e verranno prodotti video ad alta definizione.
Grade	È possibile regolare il valore di NR 3D quando 3D NR è abilitato. Maggiore è il valore, minore sarà il rumore.

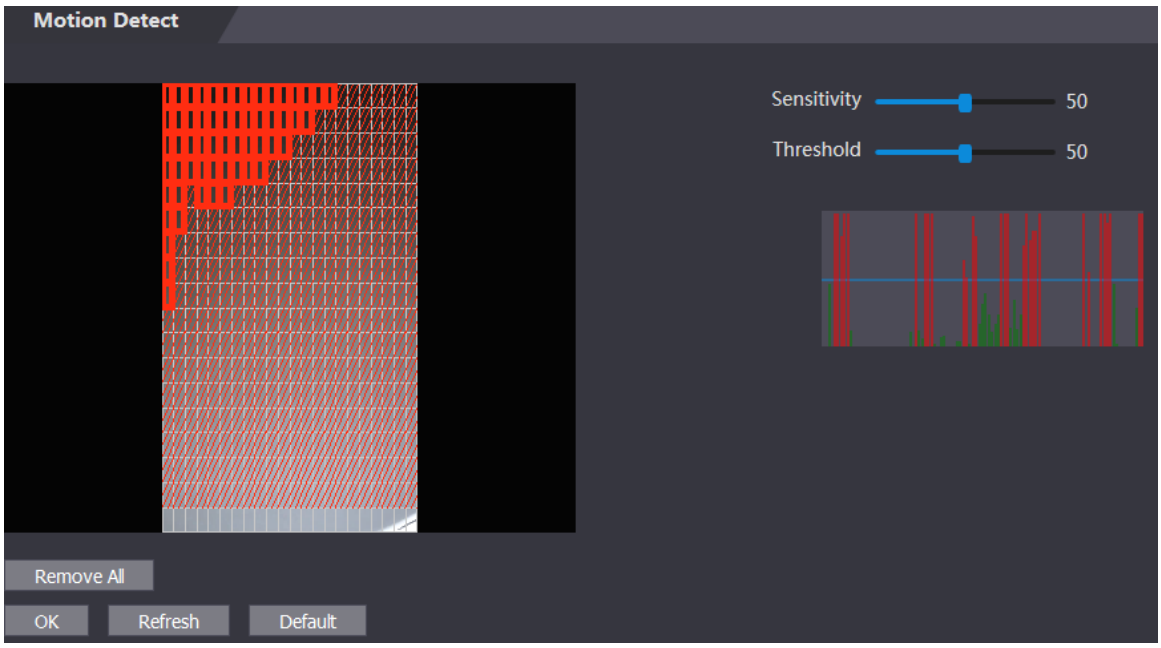
4.6.4 Motion Detection

Imposta un intervallo in cui è possibile rilevare oggetti in movimento.

Step 1 Seleziona **Video Setting > Video Setting > Motion Detection**.

L'interfaccia **Motion Detection** verrà visualizzata. See Figure 4-14.

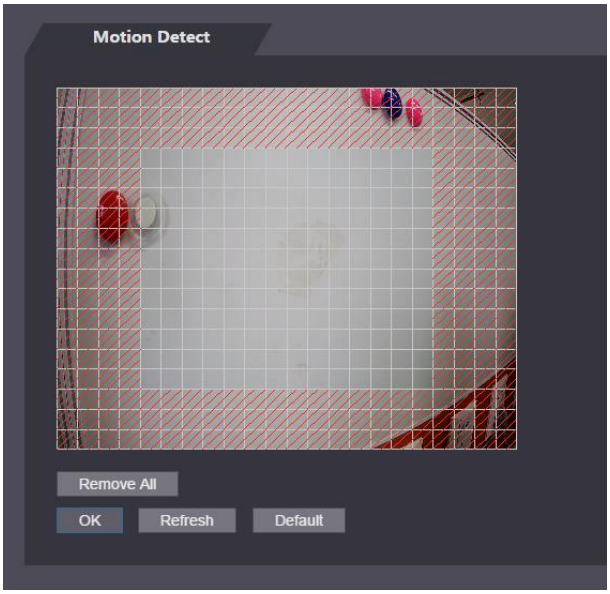
Figure 4-14 Motion detection



Step 2 Tenere premuto il pulsante sinistro del mouse, quindi trascinare il mouse nell'area rossa. Viene visualizzata l'area Rilevazione movimento. See Figure 4-15.

- I rettangoli rossi sono un'area di rilevamento del movimento. L'intervallo di rilevamento del movimento predefinito è tutti i rettangoli.
- Per disegnare un'area di rilevamento del movimento, è necessario prima fare clic su Rimuovi tutto.
- L'area di rilevamento del movimento che si disegna sarà un'area di rilevamento del non movimento se si disegna nell'area di rilevamento del movimento predefinita.

Figure 4-15 Motion detection area



Step 3 Impostare la sensibilità e la soglia.

- La sensibilità rappresenta la capacità di ciascuna griglia di rilevare il movimento. Maggiore è il valore, maggiore è la sensibilità.

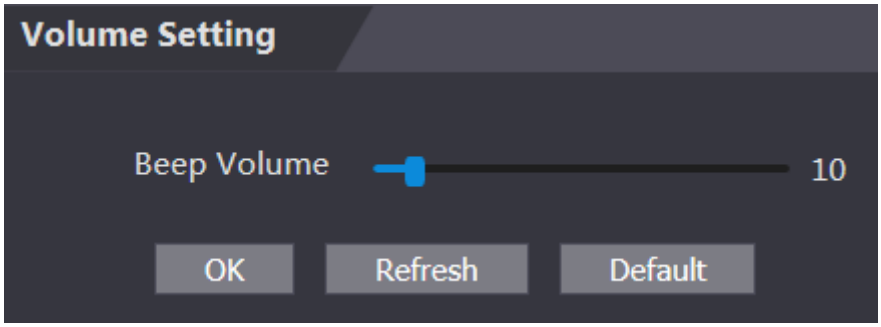
- La soglia è la condizione del rilevamento del movimento. Quando il numero della griglia raggiunge la soglia, verrà attivato il rilevamento del movimento. Più piccolo è il valore, più è probabile che venga attivato il rilevamento del movimento.
- Quando il numero della griglia è inferiore alla soglia, apparirà una linea verde; quando il numero della griglia è superiore alla soglia, apparirà una linea rossa. Vedi Figure 4-14.

Step 4 Seleziona **OK** per finire il settaggio.

4.6.5 Impostazioni Volume

È possibile regolare il volume dell'altoparlante del controller di accesso.

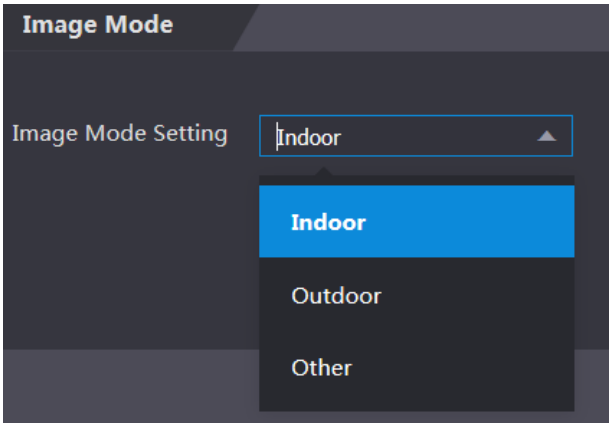
Figure 4-16 Volume setting



4.6.6 Modalità immagine

Esistono tre opzioni: indoor, outdoor e altro. Selezionare **Indoor** quando il controller di accesso è installato all'interno; selezionare **Outdoor** quando il controller di accesso è installato all'aperto; e selezionare Altro quando il controller di accesso è installato in luoghi con retroilluminazione come corridoi e corridoi.

Figure 4-17 Image mode

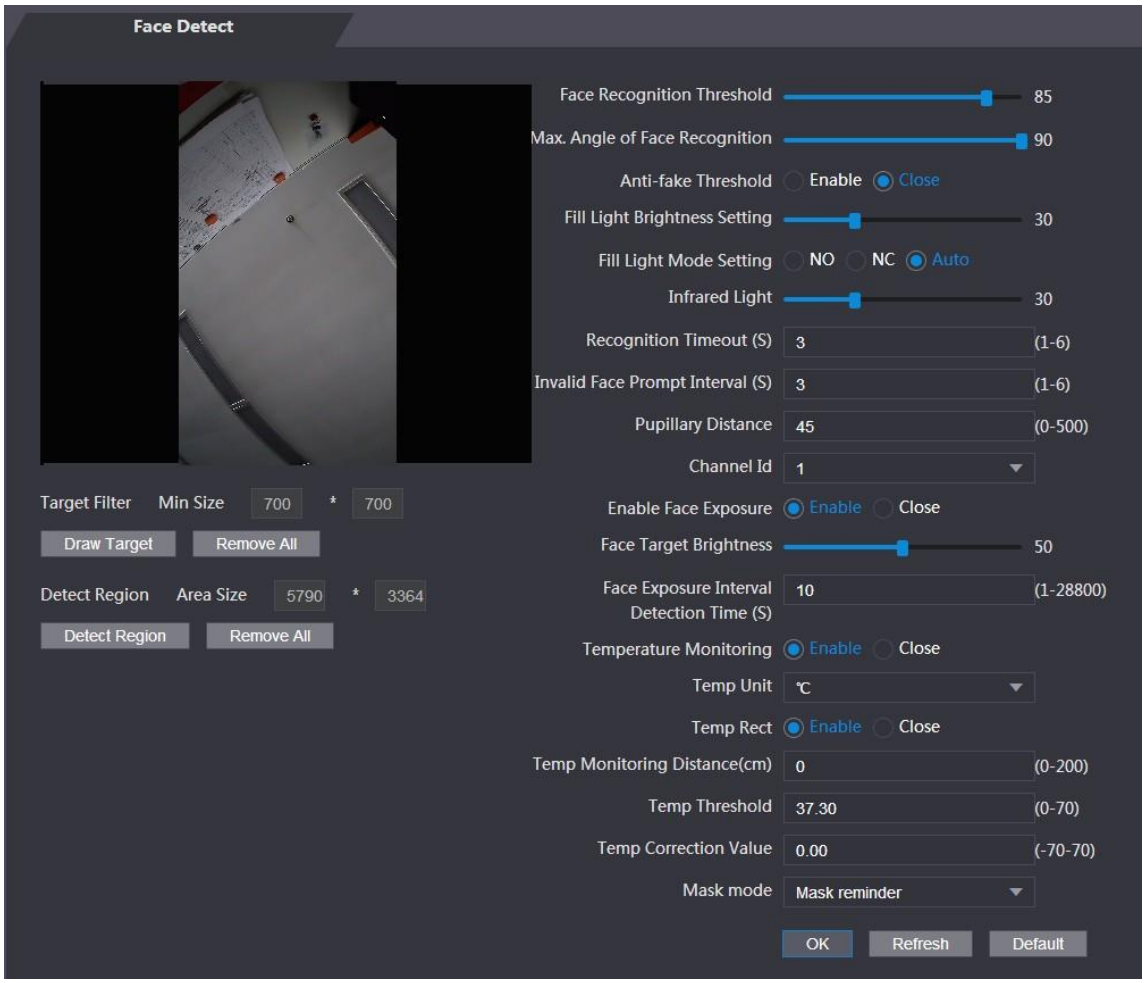


4.7 Face Detect

È possibile configurare i parametri relativi al volto umano su questa interfaccia per aumentare l'accuratezza del riconoscimento del volto..

Step 1 Seleziona **Face Detect**.

Figure 4-18 Face detect



Step 2 Configurazione Parametri.

Table 4-5 Face detect parameter description

Parameter	Description
Soglia di riconoscimento facciale	Maggiore è il valore, maggiore sarà l'accuratezza.
Max. Angle of Face Recognition	Maggiore è l'angolo, verrà riconosciuta la gamma più ampia dei profili.
Anti-fake Threshold	Questa funzione impedisce alle persone di aprire la porta con immagini di volti umani o modelli di volti. Sono disponibili due opzioni: **Abilita** e **Chiudi**.
Fill Light Brightness Setting	È possibile impostare la luminosità della luce di riempimento.
Fill Light Mode Setting	Esistono tre modalità di luce di cortesia. NO: la luce di cortesia è normalmente accesa. NC: la luce di cortesia è normalmente chiusa. ● Auto: la luce di cortesia si accenderà automaticamente quando viene attivato un evento di rilevamento del movimento.

Parameter	Description
	Quando si seleziona Auto, la luce di cortesia non sarà accesa anche se il valore della luce infrarossa è maggiore di 19.
Infrared Light	Regola la luminosità degli IR.
Recognition Timeout	Quando una persona che non dispone dell'autorizzazione di accesso si trova di fronte al controller di accesso, il dispositivo avviserà che il riconoscimento del volto è riuscito. L'intervallo di prompt si chiama timeout Recognition.
Invalid Face Prompt Interval	Quando una volto non ha i permessi di accesso di fronte al controller, il dispositivo indicherà che il volto non è valido. L'intervallo di prompt non è valido.
Pupillary Distance	La distanza pupillare è il valore in pixel dell'immagine tra i centri delle pupille di ciascun occhio. È necessario impostare un valore appropriato in modo che il controller di accesso possa riconoscere i volti secondo necessità. Il valore cambia in base alle dimensioni del viso e alla distanza tra i volti e l'obiettivo. Più il viso è vicino all'obiettivo, maggiore dovrebbe essere il valore. Se un adulto si trova a 1,5 metri dall'obiettivo, il valore della distanza pupillare può essere compreso tra 50 e 70.
Enable Face Exposure	Dopo aver abilitato l'esposizione del viso, il viso umano sarà più chiaro quando il controller di accesso è installato all'aperto.
Channel Id	Sono disponibili due opzioni: 1 e 2. 1 è la fotocamera a luce bianca e 2 è la fotocamera a luce IR.
Draw Target	Fare clic su **Disegna** bersaglio, quindi è possibile disegnare il riquadro di rilevamento minimo del volto. • Fai clic su **Rimuovi** tutto e puoi rimuovere tutti i frame disegnati.
Detect Region	Fai clic su **Detect Region**, sposta il mouse e puoi regolare la regione di rilevamento volto. • Fare clic su **Rimuovi tutto** ed è possibile rimuovere tutte le aree di rilevamento.
Face Target Brightness	Il valore predefinito è 50. Regolare la luminosità secondo necessità.
Face Exposure Interval	Dopo il rilevamento di un volto, il controller di accesso emetterà luce per illuminare il viso e il controller di accesso non emetterà più luce fino a quando non sarà trascorso l'intervallo impostato.
Temperature Monitoring	Impostare se abilitare il monitoraggio della temperatura corporea. ● Unità temporanea: selezionare un'unità di temperatura. ● Temp Rect: imposta se abilitare o meno la finestra di monitoraggio della temperatura. ● Distanza monitoraggio temp (cm): il valore è 0 per impostazione predefinita. Impostare altri valori per abilitare il monitoraggio della temperatura entro una distanza definita. 80 cm è raccomandato. ● Soglia di temperatura (° C): imposta la soglia di temperatura. La temperatura corporea monitorata verrà giudicata come temperatura elevata se è maggiore o uguale al valore impostato.

Parameter	Description
	● Valore correzione temp: questo parametro è per il test. La differenza dell'ambiente di monitoraggio della temperatura potrebbe causare la deviazione della temperatura tra la temperatura monitorata e la temperatura effettiva. È possibile selezionare più campioni monitorati per il test. In base al confronto tra la temperatura monitorata e la temperatura effettiva, è possibile correggere la deviazione della temperatura con questo parametro. Ad esempio, se la temperatura monitorata è inferiore di 0,5 ° C rispetto alla temperatura effettiva, il valore di correzione è impostato su 0,5 ° C; se la temperatura monitorata è superiore di 0,5 ° C rispetto alla temperatura effettiva, il valore di correzione è impostato su -0,5 ° C. Solo il controller di accesso con un'unità di monitoraggio della temperatura supporta questo parametro.
Mask Mode	● Nessun rilevamento: la maschera non viene rilevata durante il riconoscimento facciale. ● Promemoria maschera: la maschera viene rilevata durante il riconoscimento facciale. Se la persona viene rilevata senza indossare una maschera, il sistema richiederà il promemoria della maschera e il passaggio è consentito. ● Intercettazione maschera: la maschera viene rilevata durante il riconoscimento facciale. Se la persona viene rilevata senza indossare una maschera, il sistema richiederà il promemoria della maschera e il passaggio non è consentito.

Step 3 premi **OK** per terminare le impostazioni.

4.8 Network Setting

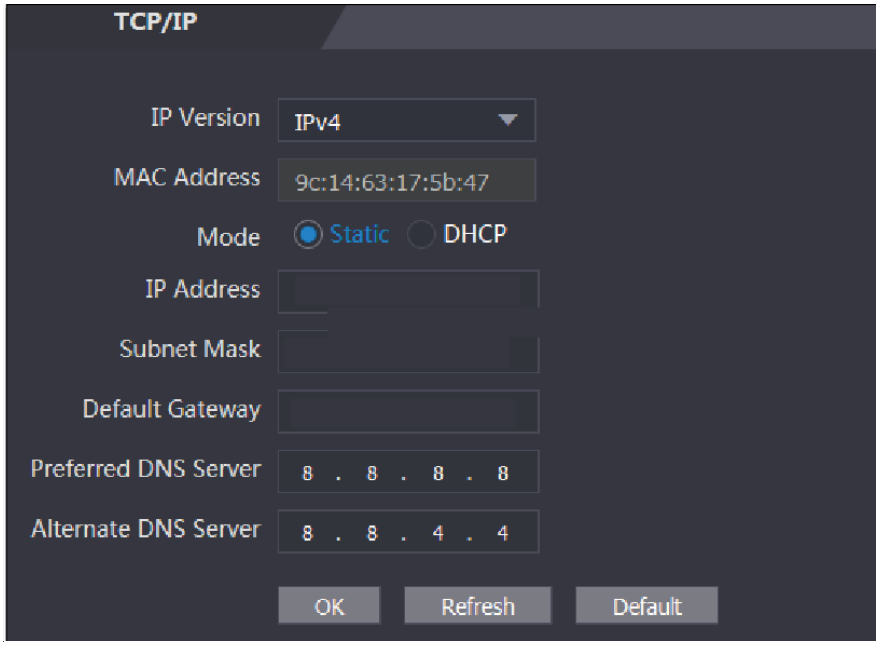
4.8.1 TCP/IP

È necessario configurare l'indirizzo IP e il server DNS per assicurarsi che il controller di accesso possa comunicare con altri dispositivi.

Assicurarsi che il controller di accesso sia collegato correttamente alla rete.

Step 1 Seleziona **Network Setting > TCP/IP**.

Figure 4-19 TCP/IP



Step 2 Configurazione Parametri.

Table 4-6 TCP/IP

Parameter	Description
IP Version	C’è una sola opzione: IPv4.
MAC Address	MAC address of the access controller is displayed.
Mode	● Statico Impostare manualmente l'indirizzo IP, la maschera di sottorete e l'indirizzo gateway. DHCP ◇ Dopo aver abilitato DHCP, l'indirizzo IP, la maschera di sottorete e l'indirizzo gateway non possono essere configurati. ◇ Se DHCP è attivo, l'indirizzo IP, la maschera di sottorete e l'indirizzo gateway verranno visualizzati automaticamente; se DHCP non è efficace, l'indirizzo IP, la maschera di sottorete e l'indirizzo gateway saranno tutti zero. ◇ Se si desidera visualizzare l'IP predefinito quando DHCP è attivo, è necessario disabilitare DHCP.
Link-local address	Se si desidera visualizzare l'IP predefinito quando DHCP è attivo, è necessario disabilitare DHCP • L'indirizzo di collegamento locale è disponibile solo quando IPv6 è selezionato nella versione IP. Gli indirizzi univoci di collegamento locale saranno assegnati al controller dell'interfaccia di rete in ciascuna rete locale per consentire le comunicazioni. L'indirizzo locale del collegamento non può essere modificato.
IP Address	Immettere l'indirizzo IP, quindi configurare la maschera di sottorete e l'indirizzo gateway. 🕮 L'indirizzo IP e l'indirizzo gateway devono trovarsi nello stesso segmento di rete.
Subnet Mask	
Default Gateway	
Preferred DNS Server	Imposta l'indirizzo IP del server DNS preferito.
Alternate DNS Server	Imposta l'indirizzo IP del server DNS alternativo.

Step 3 premi **OK** per completare la configurazione.

4.8.2 Port

Impostare il numeor massimo di client a cui è possibile collegare il controller di accesso e i numeri di porta.

Step 1 Seleziona **Network Setting > Port**.

L’interfaccia **Port** verrà visualizzata.

Step 2 Configurare i numeri di porta. Vedi la tabella seguente.

🕮

Tranne la connessione massima, è necessario riavviare il controller di accesso per rendere effettiva la configurazione dopo aver modificato i valori.

Table 4-7 Port description

Parameter	Description
Max Connection	È possibile impostare le connessioni massime dei client a cui è possibile collegare il controller di accesso. I client della piattaforma come Smart PSS non vengono conteggiati.
TCP Port	Il valore predefinito è 37777.
HTTP Port	Il valore predefinito è 80. Se si utilizza un altro valore come numero di porta, è necessario aggiungere questo valore dietro l'indirizzo quando si accede tramite i browser.
HTTPS Port	Il valore predefinito è 443.
RTSP Port	Il valore predefinito è 554.

Step 3 Premere **OK** per salvare la configurazione.

4.8.3 Register

Quando è collegato a una rete esterna, il controller di accesso segnalerà il proprio indirizzo al server designato dall'utente in modo che i client possano accedere al controller di accesso..

Step 1 Seleziona **Network Setting > Auto Register**.

L'interfaccia **Auto Register** verrà visualizzata.

Step 2 Seleziona **Enable**, inserire IP Host, port, e sub device ID.

Table 4-8 Auto register description

Parameter	Description
Host IP	Indirizzo IP del server o nome dominio del server.
Port	Porta del server utilizzata per la registrazione automatica.
Sub Device ID	Accedere all'ID controller assegnato dal server.

Step 3 Premi **OK** completare il salvataggio.

4.8.4 P2P

peer-to-peer è un'architettura di applicazione distribuita che suddivide le attività o i carichi di lavoro tra peer. Gli utenti possono scaricare l'applicazione mobile tramite la scansione del codice QR e quindi registrare un account in modo che sia possibile gestire più di un controller di accesso sull'app mobile. Non è necessario applicare un nome di dominio dinamico, eseguire il mapping delle porte o non è necessario il server di transito.

Se si desidera utilizzare P2P, è necessario collegare il controller di accesso alla rete esterna; in caso contrario non è possibile utilizzare il controller di accesso.

Figure 4-20 P2P

Step 1 Seleziona **Network Setting > P2P**.

L'interfaccia **P2P** verrà visualizzata.

Step 2 Seleziona **Enable** per abilitare il P2P.

Step 3 seleziona **OK** per completare la configurazione.

Scansiona il codice QR sulla tua interfaccia web per ottenere il numero seriale del controller di accesso.

4.9 Impostazione Data

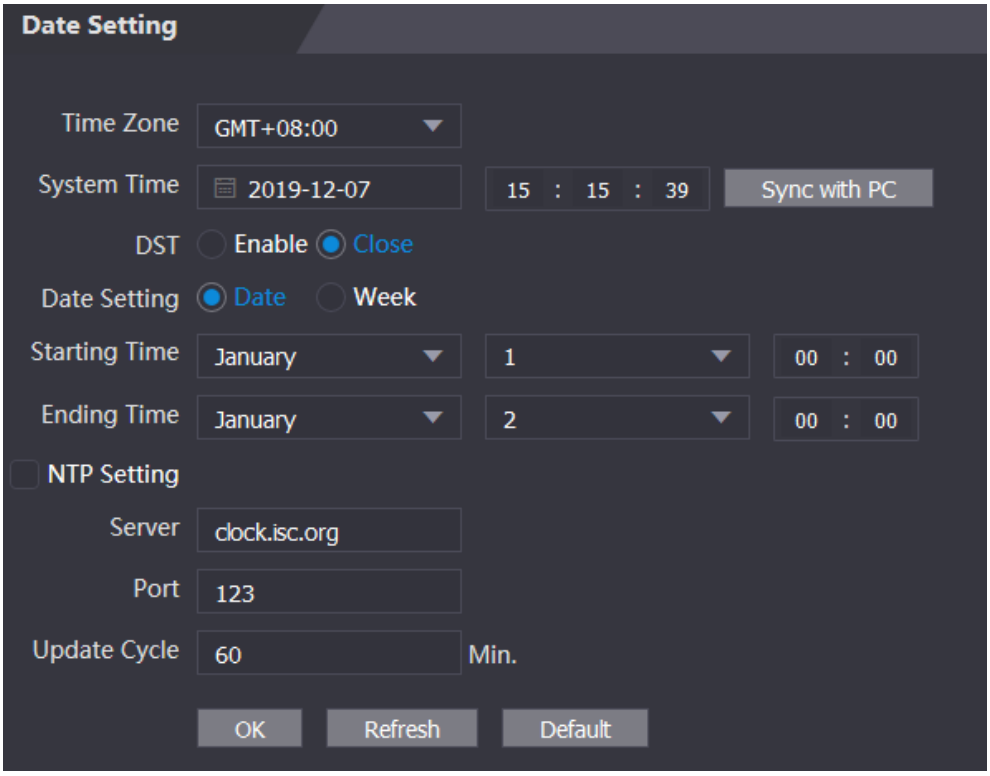
È necessario impostare fuso orario, ora, ora legale e NTP per il controller di accesso.

Solo alcuni modelli supportano questa funzione..

Step 1 Seleziona **Date Setting**.

L'interfaccia **Date Setting** verrà visualizzata. See Figure 4-21

Figure 4-21 Date Setting



Step 2 Impostazione Parametri.

Table 4-9 Date setting

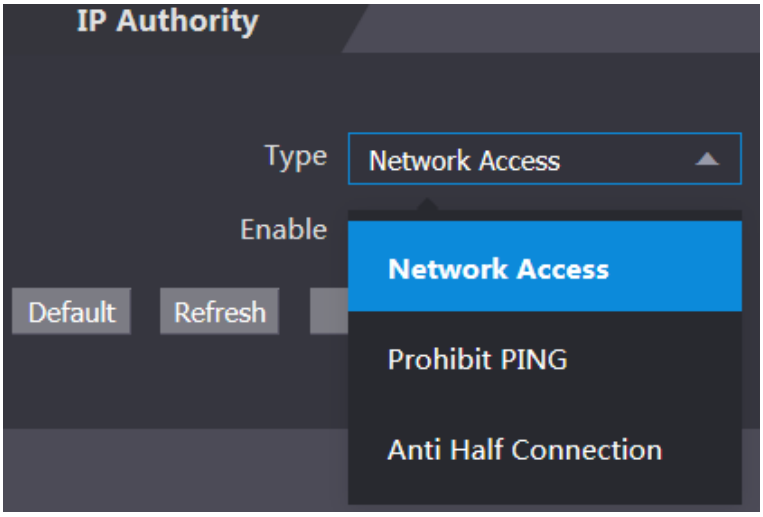
Parameter	Description
Time Zone	Selezionare il fuso orario secondo necessità.
System Time	È possibile impostare l'ora di sistema manualmente oppure fare clic su Sincronizza con PC per sincronizzare l'ora del controller di accesso con l'ora del computer.
DST	• 1. Abilitare l'ora legale. DST • 2. Selezionare Data o Settimana in Impostazione data. • 3. Impostare l'ora di inizio e l'ora di fine.
NTP Setting	• 1. Abilitare le impostazioni **NTP**. • 2. Configurare i parametri. Server: immettere il nome dominio del server NTP. L'ora del controller di accesso verrà sincronizzata con il server NTP. Porta: immettere il numero di porta del server NTP. Ciclo di aggiornamento: impostare un ciclo di aggiornamento, quindi l'ora del controller di accesso verrà aggiornata di conseguenza. 3. Fai clic su **OK**.

4.10 Safety Management

4.10.1 IP Authority

Seleziona una modalità di sicurezza informatica in base alle esigenze.

Figure 4-22 IP authority



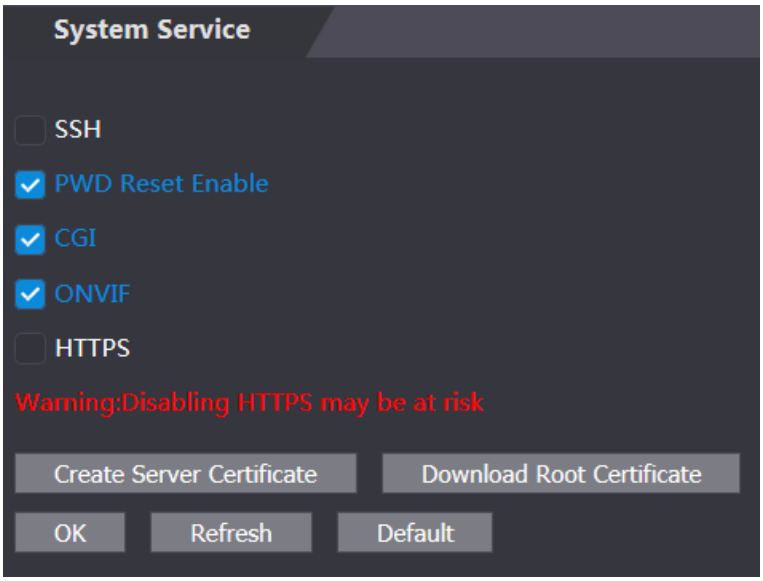
4.10.2 Systems

4.10.2.1 System Service

Sono disponibili quattro opzioni: SSH, Abilita ripristino PWD, CGI e HTTPS. Fare riferimento a "3.12 Funzioni" per selezionare una o più di una di esse.

La configurazione del servizio di sistema eseguita sulla pagina Web e la configurazione sull'interfaccia Funzioni del controller di accesso verranno sincronizzate.

Figure 4-23 System service



4.10.2.2 Creare Certificato

Fare clic su **Crea certificato**, immettere le informazioni necessarie, fare clic su Salva, quindi il controller di accesso verrà riavviato.

4.10.2.3 Downloading Root Certificate

Step 1 Seleziona **Download Root Certificate**.
Selezionare un percorso per salvare il certificato nella finestra di dialogo Salva file.
Step 2 Fare doppio clic sul certificato radice scaricato per installare il certificato. Installa il certificato seguendo le istruzioni sullo schermo.

4.11 Gestione utenti

Puoi aggiungere ed eliminare utenti, modificare le password degli utenti e inserire un indirizzo email per reimpostare la password quando la dimentichi.

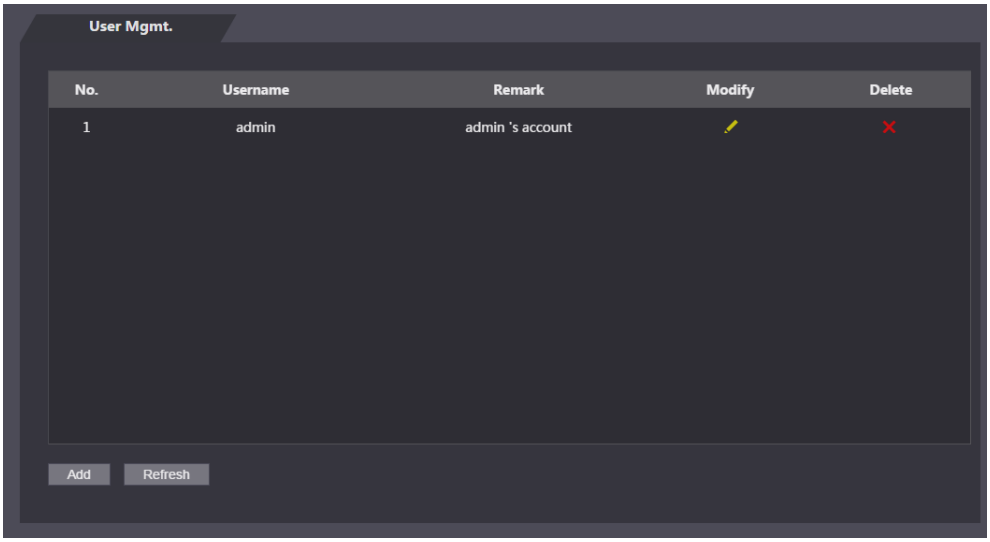
4.11.1 Aggiunta nuovi utenti

Fare clic su **Aggiungi** su **Mgmt utente**. interfaccia per aggiungere utenti, quindi inserire nome utente, password, password confermata e commento. Fare clic su OK per completare l'aggiunta dell'utente.

4.11.2 Modifica Informazione Utenti

Puoi modificare le informazioni dell'utente facendo clic in **User Mgmt.**. Vedi Figure 4-24.

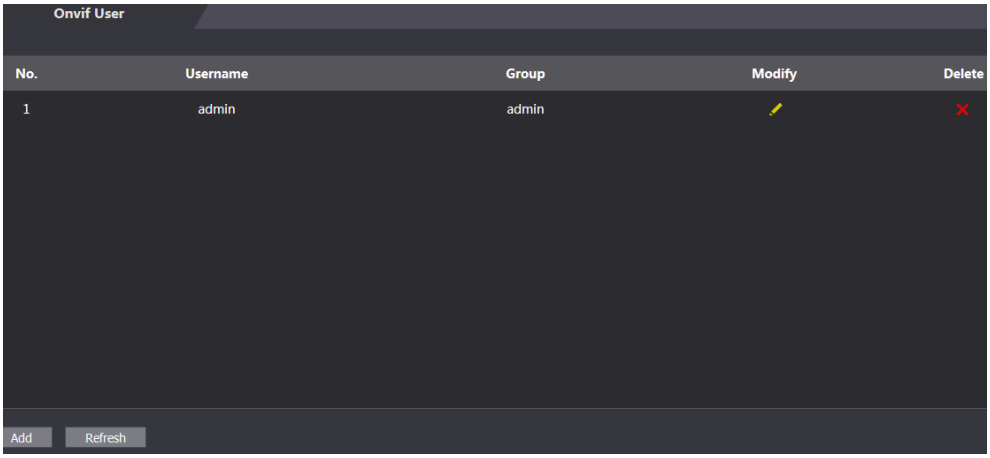
Figure 4-24 User management



4.11.3 Utente Onvif

Open Network Video Interface Forum (ONVIF), un forum di settore globale e aperto con l'obiettivo di facilitare lo sviluppo e l'uso di uno standard aperto globale per l'interfaccia di prodotti di sicurezza fisici basati su IP. Quando si utilizza ONVIF, l'amministratore, l'operatore e l'utente dispongono di autorizzazioni diverse per il server ONVIF. Crea utenti onvif secondo necessità..

Figure 4-25 Onvif user

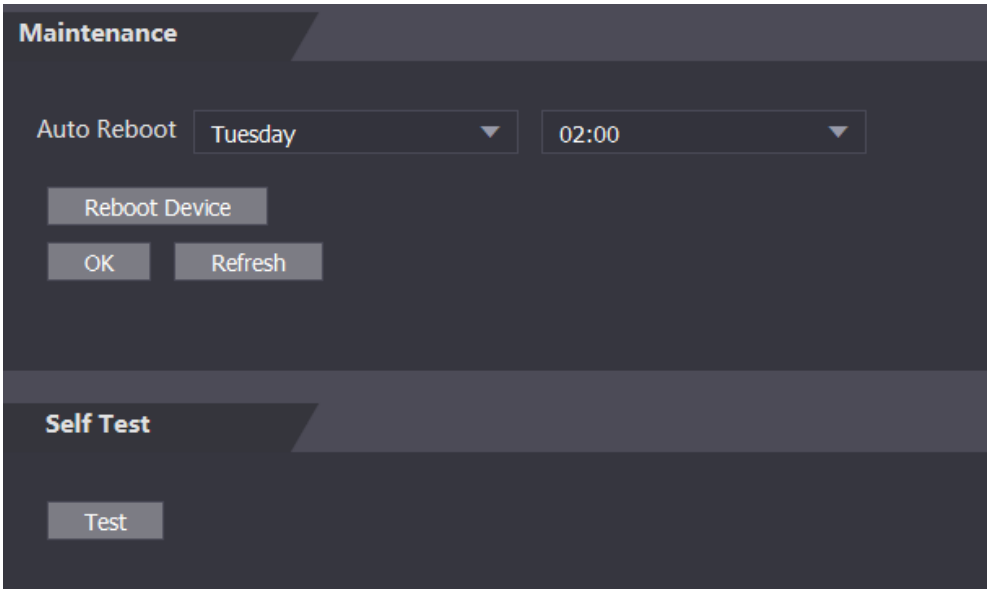


4.12 Manutenzione

È possibile eseguire il riavvio del controller in modalità automatica per migliorare la velocità di esecuzione del dispositivo. È necessario impostare la data e l'ora del riavvio automatico.

L'ora di riavvio predefinita è alle 2 del mattino di martedì. Fai clic su Riavvia dispositivo, il controller di accesso si riavvierà immediatamente. Fai clic su OK, il controller di accesso si riavvierà alle 2 del mattino ogni martedì. Vedi Figure 4-26.

Figure 4-26 Maintenance



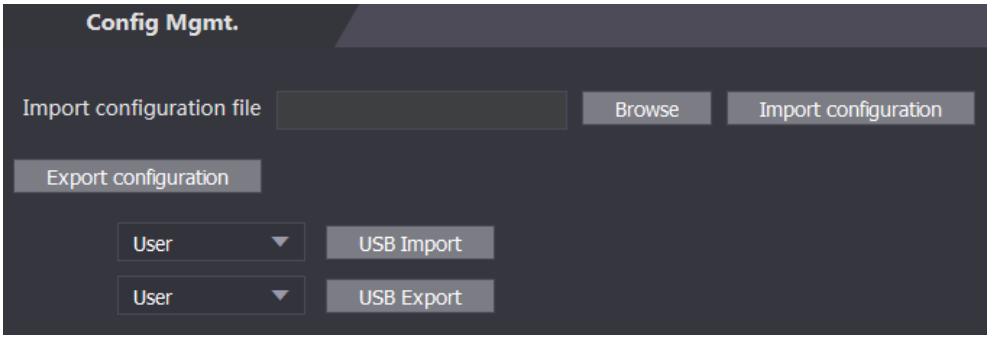
4.13 Gestione Configurazione

È necessario eseguire la gestione della configurazione, selezionare il feedback sui risultati di sblocco, Wiegand e le impostazioni seriali per il controller di accesso.

4.13.1 Config Mgmt.

E’ possibile esportare ed importare la configurazione tra due dispositivi se questi necessitano della stessa configurazione. See Figure 4-27.

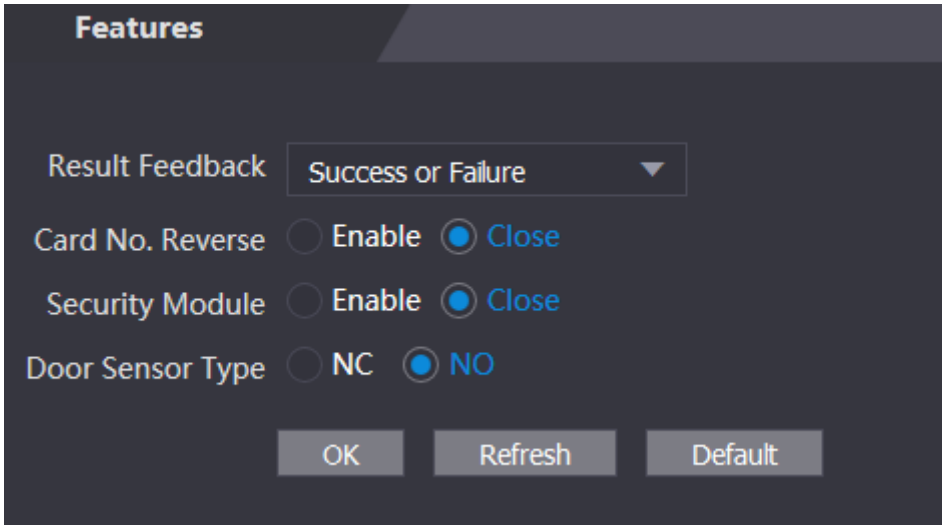
Figure 4-27 Configuration management



4.13.2 Caratteristiche

Selezionare la modalità di feedback dei risultati secondo necessità. Per dettagli, vedi "3.12.2 Result Feedback."

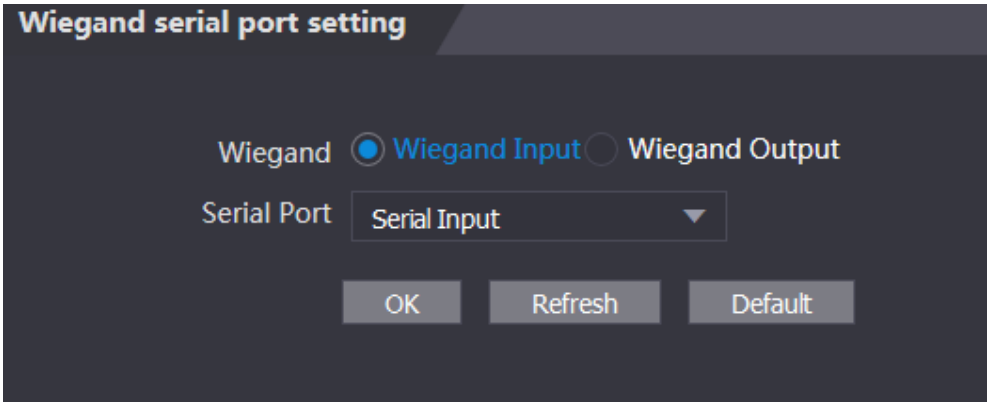
Figure 4-28 Features



4.13.3 Wiegand Serial Port Setting

Selezionare le impostazioni della porta seriale / Wiegand secondo necessità. Per dettagli, vedi "3.9.2 Impostazioni Porta Seriale " e "3.9.3 Configurazioen Wiegand ."

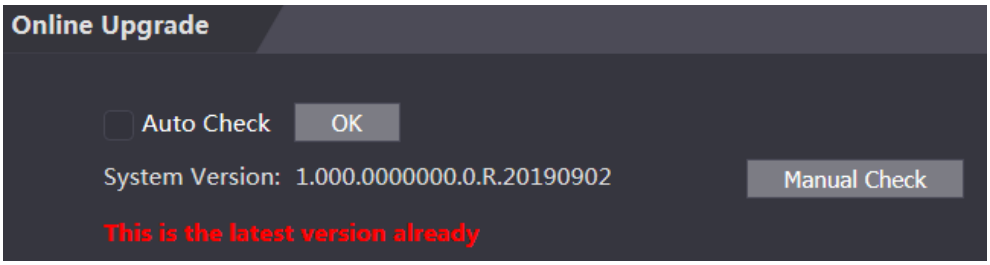
Figure 4-29 Wiegand serial port setting



4.14 Upgrade

È possibile selezionare Auto Check per aggiornare automaticamente il sistema. È inoltre possibile selezionare Controllo manuale per aggiornare manualmente il sistema.

Figure 4-30



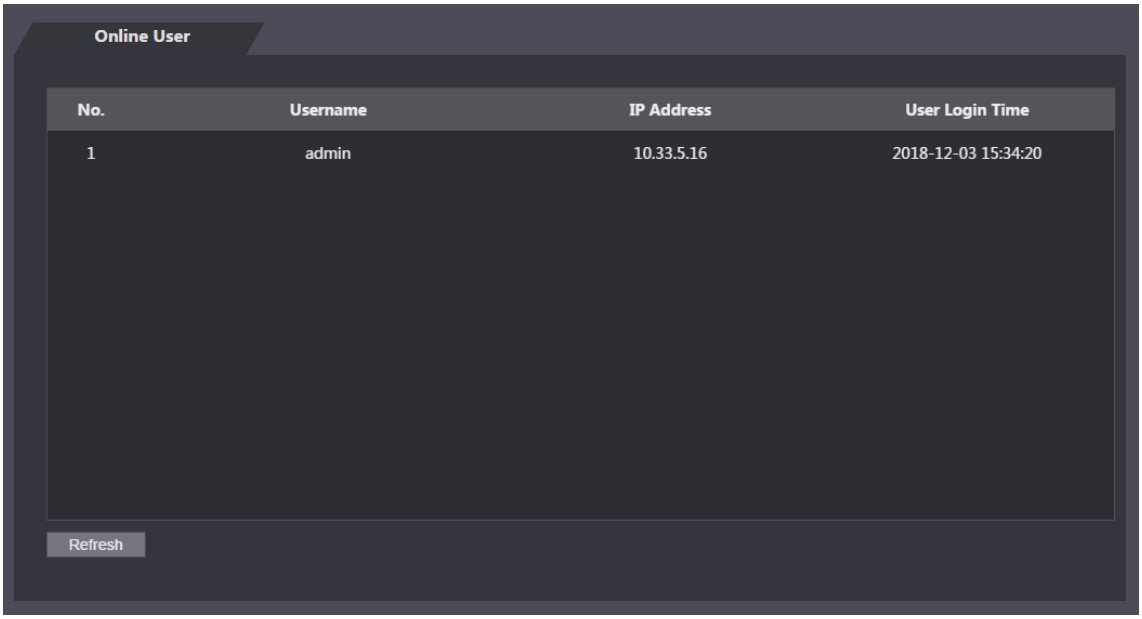
4.15 Info Versione

È possibile visualizzare informazioni tra cui indirizzo MAC, numero di serie, versione MCU, versione Web, versione di base di sicurezza e versione di sistema.

4.16 Online User

È possibile visualizzare nome utente, indirizzo IP e tempo di accesso dell'utente nell'interfaccia utente online. Vedi Figure 4-31.

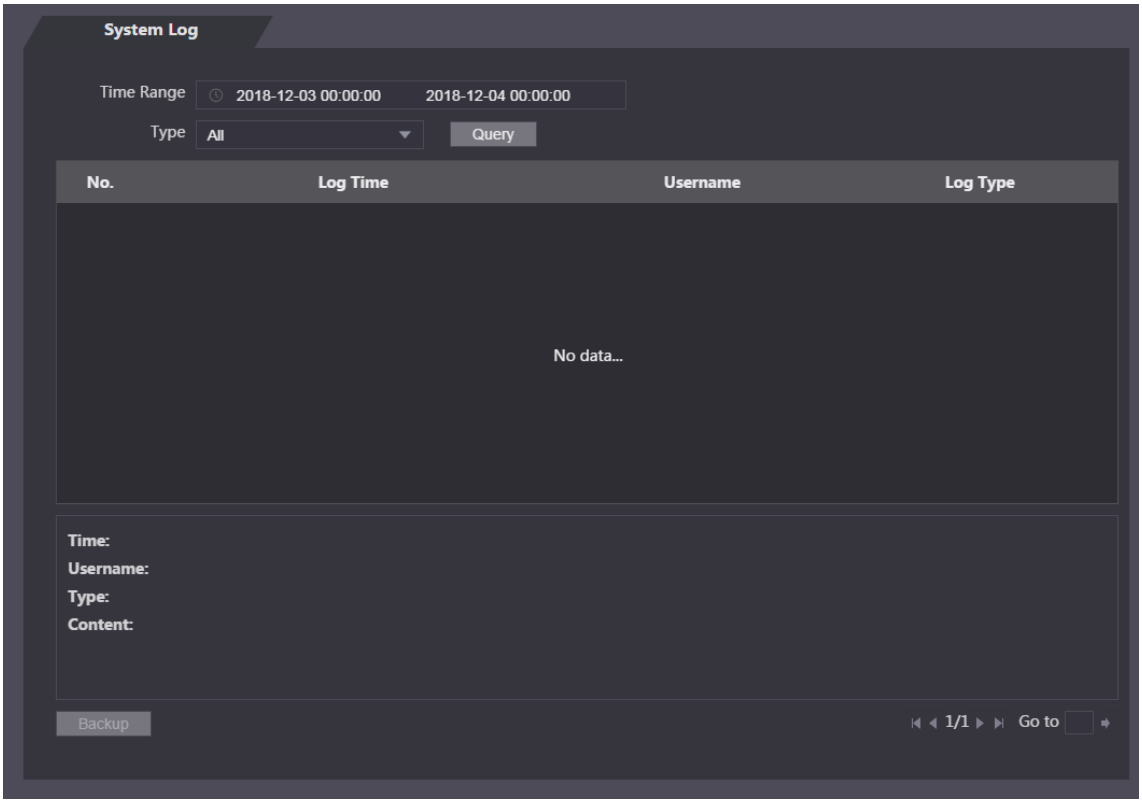
Figure 4-31 Online user



4.17 Log Sistema

È possibile visualizzare ed eseguire il backup del registro di sistema nell'interfaccia log di sistema.

Figure 4-32 System log



4.17.1 Querying Logs

Seleziona un intervallo di tempo e il suo tipo, fai clic su Query e verranno visualizzati i log che soddisfano le condizioni.

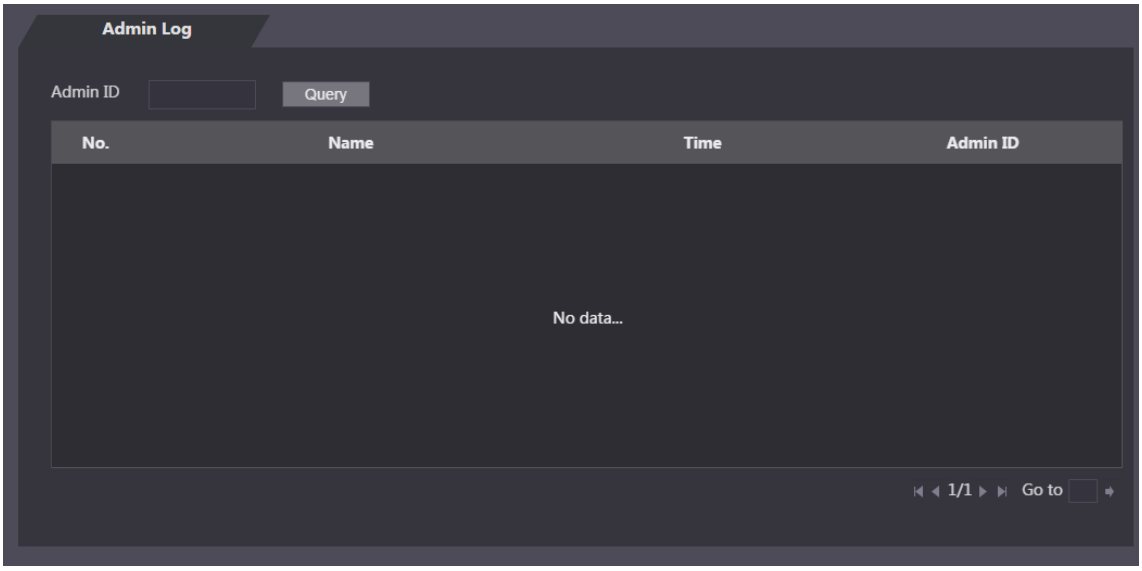
4.17.2 Backup Logs

Fare clic su Backup per eseguire il backup dei registri visualizzati.

4.17.3 Admin Log

Immettere l'ID amministratore nell'interfaccia del registro di amministrazione, fare clic su Query, quindi verranno visualizzati i record delle operazioni dell'amministratore.

Figure 4-33 Admin log



Passa il cursore del mouse sopra , potrai vedere le informazioni dettagliate dell'utente corrente.

Exit

seleziona , premi **OK**, uscirai dalla webpage.

5 FAQ

1 **Il 1 Il controller di accesso non si avvia dopo l'accensione**.
Verificare che l'alimentazione a 12V sia collegata correttamente e che il pulsante di accensione sia premuto.

2 **I volti non possono essere riconosciuti dopo l'accensione del controller di accesso.**
Assicurati che Face sia selezionato nella modalità di sblocco. Vedere "3.8.2 Sblocco".
Assicurati che Face sia selezionato come modalità di sblocco in Accesso> Modalità di sblocco> Combinazione di gruppo. Vedere "3.8.2.3 Combinazione di gruppi".

3 **Non vi è alcun segnale di uscita quando il controller di accesso e il controller esterno sono collegati alla porta Wiegand**.
Controllare se il cavo GND del controller di accesso e il controller esterno sono collegati.

4 **Le configurazioni non possono essere effettuate dopo che l'amministratore e la password sono stati dimenticati.**
Elimina gli amministratori tramite la piattaforma o contatta l'assistenza tecnica per sbloccare il controller di accesso in remoto.

5 **Le informazioni dell'utente e le immagini dei volti non possono essere importate nel controller di accesso**.
Controlla se i nomi dei file XML e i titoli delle tabelle sono stati modificati perché il sistema identificherà i file attraverso i loro titoli.

6 **Quando viene riconosciuto il volto di un utente, ma vengono visualizzate le informazioni di altri utenti**.
Quando si importano volti umani, assicurarsi che non vi siano altre persone in giro. Elimina la faccia originale e importala di nuovo.

Appendix 1 Notes of Temperature Monitoring

- 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 Notes of Face Recording/Comparison

Prima della Registrazione

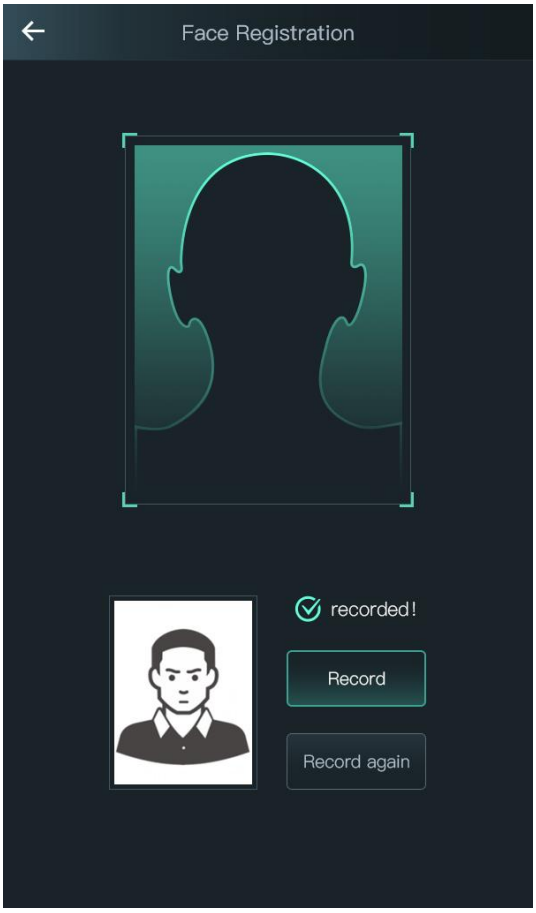
- Occhiali, cappelli e barbe potrebbero influenzare le prestazioni del riconoscimento facciale.
- Non coprire le sopracciglia quando si indossano i cappelli.
- Non cambiare notevolmente lo stile della barba se utilizzerai il dispositivo; altrimenti il riconoscimento facciale potrebbe non riuscire.
- 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

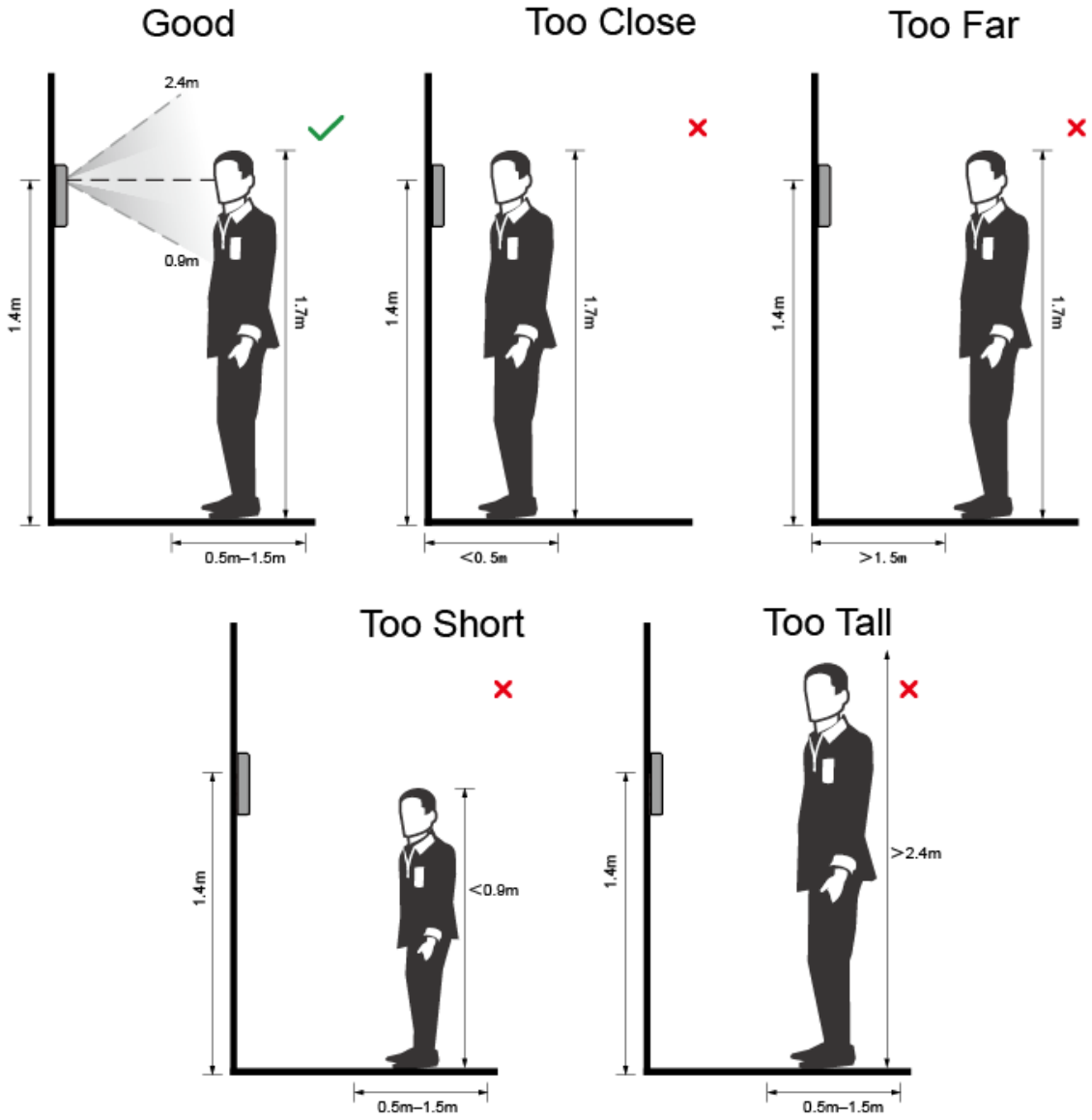


- Non scuotere la testa o il corpo, altrimenti la registrazione potrebbe non riuscire.
- Evitare che due volti compaiano nel riquadro di acquisizione contemporaneamente.

Posizione Viso

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

Appendix Figure 2-2 Posizione appropriata

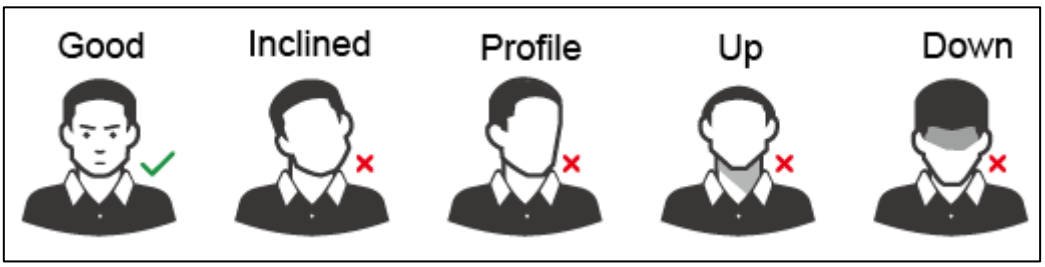


Requisiti dei Volti

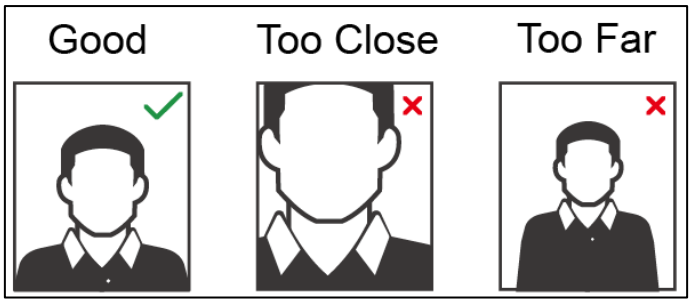
- Assicurarsi che il viso sia pulito e la fronte non sia coperta dai capelli.
- Non indossare occhiali, cappelli, barbe pesanti o altri ornamenti per il viso che influenzano la registrazione delle immagini del viso.
- Con gli occhi aperti, senza espressioni facciali, e inclina il viso verso il centro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

1. Usa Password Sicure

   7 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 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

   8 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..

3. Cambia password regolarmente

   9 Ti consigliamo di cambiare regolarmente le password.

4. Impostare ed aggiornare le password e le informazioni tempestivamente

   10 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.

5. Abilita Blocco account

   11 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.

6. Modifica le porte HTTP e di altri servizi

   12 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.

7. Abilita HTTPS

   13 Ti consigliamo di abilitare HTTPS.

8. Abilita Whitelist

   14 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.

9. MAC Address Binding

   15 Si consiglia di associare l'indirizzo IP e MAC del gateway all'apparecchiatura, riducendo così il rischio di spoofing ARP.

10. Assegnare Accounts e Privilegi Ragionevolmente

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

11. Disabilitare i servizi non necessari e scegliere le modalità sicure

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

    18 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.

12. Trasmissione crittografata audio e video

    19 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.

    20 Promemoria: la trasmissione crittografata causerà una perdita dell'efficienza della trasmissione.

13. 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.

14. Network Log

21 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.

15. Costruire un ambiente di rete sicuro

22 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.