Controller di accesso con riconoscimento volti

Manuale dell'utente

V1.0.0

Introduzione

Generale

Il presente manuale descrive l'installazione e il funzionamento di base del controller di accesso con riconoscimento dei volti (di seguito denominato "controller di accesso").

Istruzioni di sicurezza

All’interno del manuale possono comparire i seguenti indicatori di pericolo, il cui significato è definito qui sotto.

Indicatori di pericolo	Significato
NOTA	Fornisce informazioni aggiuntive che completano quelle riportate nel testo.

Cronologia delle revisioni

Versione	Contenuto della revisione	Data di rilascio
V1.0.0	Prima versione	Agosto 2019

Indicazioni sul manuale

- Questo manuale serve solo come riferimento. In caso di discrepanza fra il manuale e il prodotto, quest’ultimo prevarrà.
- Non ci riteniamo responsabili per eventuali perdite causate da un utilizzo non conforme a quanto esposto nel manuale.
- Il manuale deve essere aggiornato sulla base delle più recenti leggi e normative in vigore nelle regioni interessate. Per informazioni dettagliate, consultare il manuale in formato cartaceo, CD-ROM o disponibile scansionando il codice QR o accedendo al nostro sito web ufficiale. In caso di incongruenze tra il manuale cartaceo e la versione elettronica, quest’ultima prevarrà.
- Grafiche e software sono soggetti a modifica senza preavviso. Gli aggiornamenti del prodotto possono generare delle differenze tra il prodotto effettivo e le informazioni contenute nel manuale. Contattare il servizio di assistenza per le procedure più recenti e la documentazione supplementare.
- Potrebbero inoltre esserci delle differenze nei dati tecnici, nelle descrizioni di funzioni e operazioni, o errori di stampa. In caso di incoerenze o incertezze, fare riferimento alla nostra spiegazione finale.
- Se non è possibile aprire il manuale in formato PDF, aggiornare il programma per la lettura dei file PDF o provarne un altro.
- Tutti i marchi commerciali, i marchi registrati e i nomi di società presenti nel manuale sono di proprietà dei rispettivi titolari.
- In caso di problemi durante l'utilizzo del dispositivo, è possibile consultare il nostro sito web o contattare il fornitore o il servizio di assistenza al cliente.
- In caso di incertezze o controversie, fare riferimento alla spiegazione finale.

Norme di sicurezza e avvertenze importanti

Il presente capitolo descrive le procedure per l'uso corretto del controller di accesso, la prevenzione dei rischi e dei danni materiali. Leggere attentamente queste informazioni prima di utilizzare il controller di accesso, durante l'uso attenersi alle istruzioni fornite e conservarle come futuro riferimento.

Requisiti di funzionamento

- Non collocare o installare il controller di accesso in luoghi esposti alla luce solare o in prossimità di fonti di calore.
- Tenere il controller di accesso lontano da umidità, polvere e fuliggine.
- Installare il controller di accesso in posizione orizzontale su una superficie stabile per evitane la caduta.
- Non far cadere il controller di accesso ed evitare di schizzarlo con liquidi, assicurandosi di tenerlo lontano da contenitori di sostanze liquide che potrebbero penetrare nel dispositivo.
- Installare il controller di accesso in un luogo ben ventilato e non bloccarne la ventilazione.
- Utilizzare il controller di accesso rispettando il campo di potenza nominale in ingresso e in uscita.
- Non smontare il controller di accesso.
- Trasportare, utilizzare e conservare il controller di accesso nelle condizioni di umidità e temperatura consentite.

Sicurezza elettrica

- Un uso scorretto della batteria potrebbe causare esplosioni o principi di incendio.
- Sostituire le batterie usate con altre dello stesso modello.
- Usare cavi di alimentazione conformi alle norme locali e alle specifiche di potenza nominali.
- Per evitare il pericolo di lesioni alle persone e danni al dispositivo, utilizzare l'alimentatore fornito con il controller di accesso.
- L'alimentatore deve essere conforme ai requisiti della direttiva di Tensione estremamente bassa di sicurezza (SELV) e ai requisiti di tensione nominale riportati nello standard IEC60950-1 per gli Alimentatori a tensione limitata. I requisiti di alimentazione elettrica sono quelli riportati nell'etichetta del dispositivo.
- Collegare il dispositivo (con spina di tipo I) a una presa di corrente adeguata, dotata di messa a terra di protezione.
- L'accoppiatore dell'unità è un dispositivo di disconnessione. Utilizzare l'accoppiatore con un'angolazione che ne renda agevole l'uso.

Sommario

1 Panoramica

1.1 Introduzione

Il dispositivo è un pannello di controllo degli accessi che supporta lo sblocco tramite volto, password, impronte digitali, scheda o una combinazione di questi.

1.2 Caratteristiche

- Supporto delle seguenti modalità di sblocco: volto, scheda IC, impronta digitale, password, per intervallo temporale.
- Con riquadro per il riconoscimento dei volti; il volto più grande tra i volti che appaiono contemporaneamente viene riconosciuto per primo; la dimensione massima del volto può essere configurata sul web
- Obiettivo WDR grandangolare da 2 MP; con luce di riempimento automatica/manuale
- Distanza volto-telecamera: 0,3 m-2,0 m; altezza persone: 0,9 m-2,4 m
- Grazie a un algoritmo di riconoscimento dei volti, il terminale è in grado di riconoscere più di 360 posizioni sul volto umano
- Accuratezza della verifica del volto>99,5%; bassa percentuale di falsi riconoscimenti
- Supporto riconoscimento del profilo; l'angolo del profilo è di 0°-90°
- Supporto rilevamento volto reale
- Supporto allarme di coercizione e allarme manomissione
- Supporto utenti generici, utenti sotto coercizione, utenti di pattuglia, utenti della lista nera, utenti VIP, utenti ospiti e utenti inattivi.
- Con 4 modalità di visualizzazione dello stato di sblocco e varie modalità di messaggi vocali

1.3 Dimensioni e componenti

Il controllo degli accessi è disponibile in due versioni: 7 pollici e 10 pollici. Fare riferimento dalla Figura 1-1 alla Figura 1-4.

Controllo degli accessi da 7 pollici

Figura 1-1 Dimensioni e componenti (1) (mm [pollici])

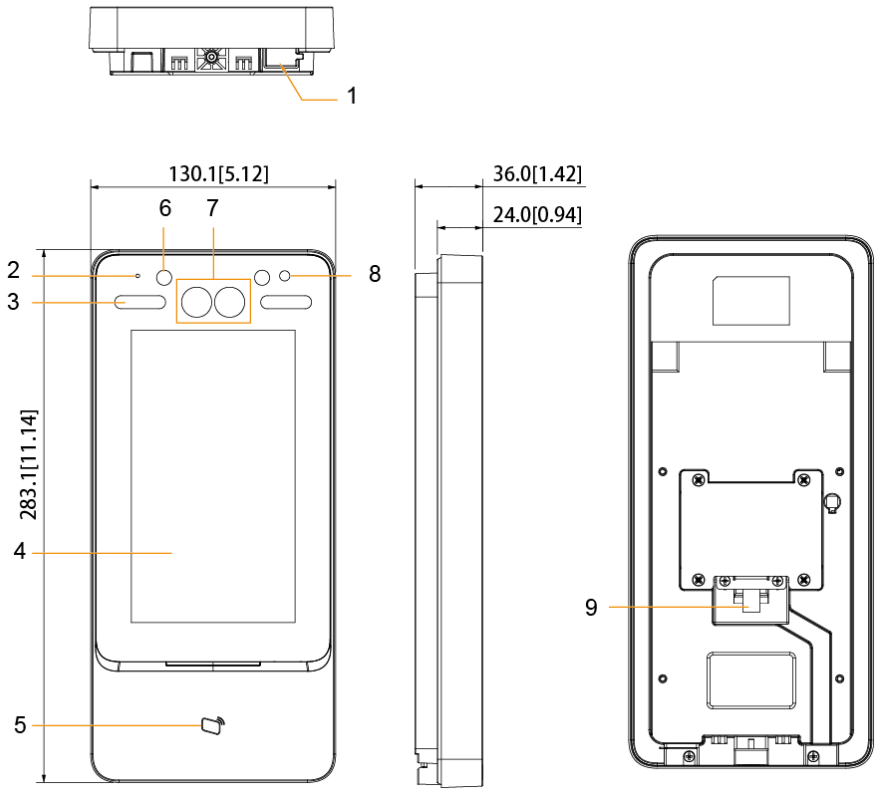


Tabella 1-1 Descrizione dei componenti (1)

N.	Nome	N.	Nome
1	Porta USB	6	Luce IR
2	MIC	7	Doppia telecamera
3	Luce di riempimento bianca	8	Fototransistor
4	Display	9	Ingresso cavo
5	Area di lettura schede	–	–

Figura 1-2 Dimensioni e componenti (2) (mm [pollici])

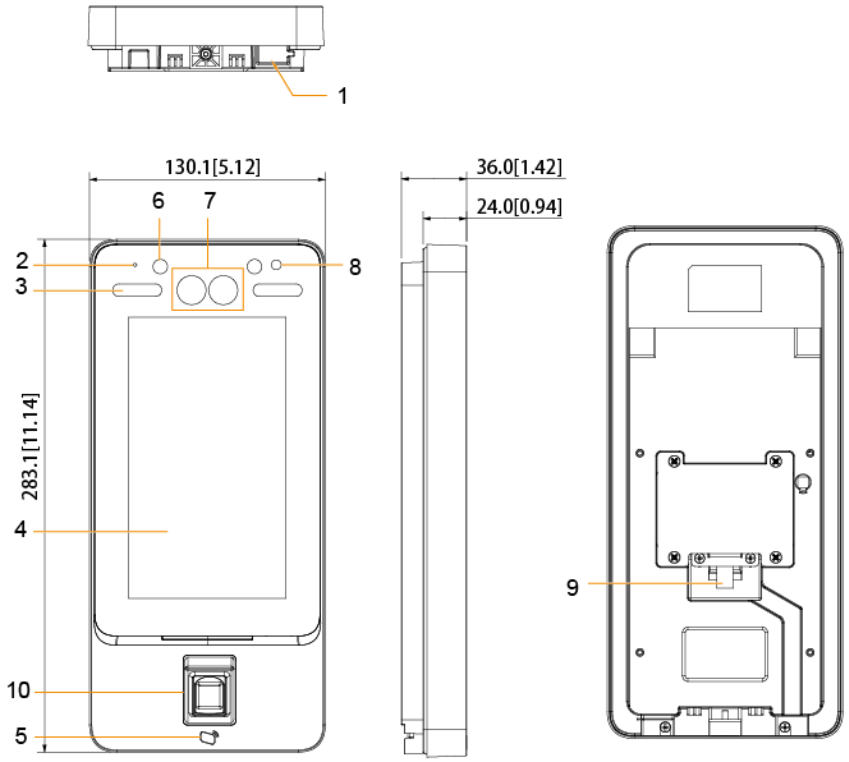


Tabella 1-2 Descrizione dei componenti (2)

N.	Nome	N.	Nome
1	Porta USB	6	Luce IR
2	MIC	7	Doppia telecamera
3	Luce di riempimento bianca	8	Fototransistor
4	Display	9	Ingresso cavo
5	Area di lettura schede	10	Sensore impronte digitali

Figura 1-3 Dimensioni e componenti (3) (mm [pollici])

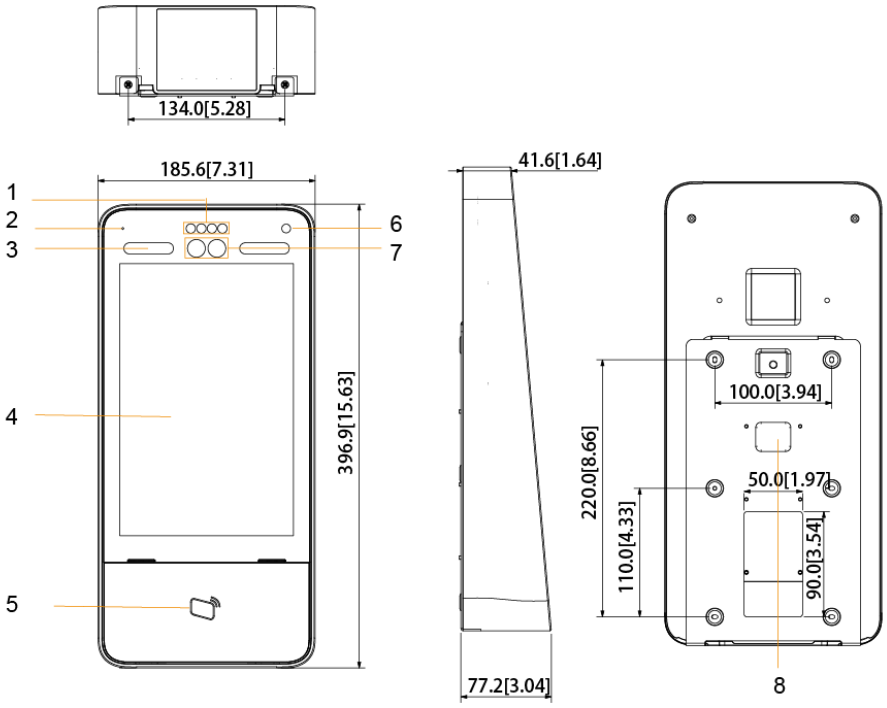


Tabella 1-3 Descrizione dei componenti (3)

N.	Nome	N.	Nome
1	Luce IR	6	Fototransistor
2	MIC	7	Doppia telecamera
3	Luce di riempimento bianca	8	Ingresso cavo
4	Display	9	–
5	Area di lettura schede	10	–

Figura 1-4 Dimensioni e componenti (4) (mm [pollici])

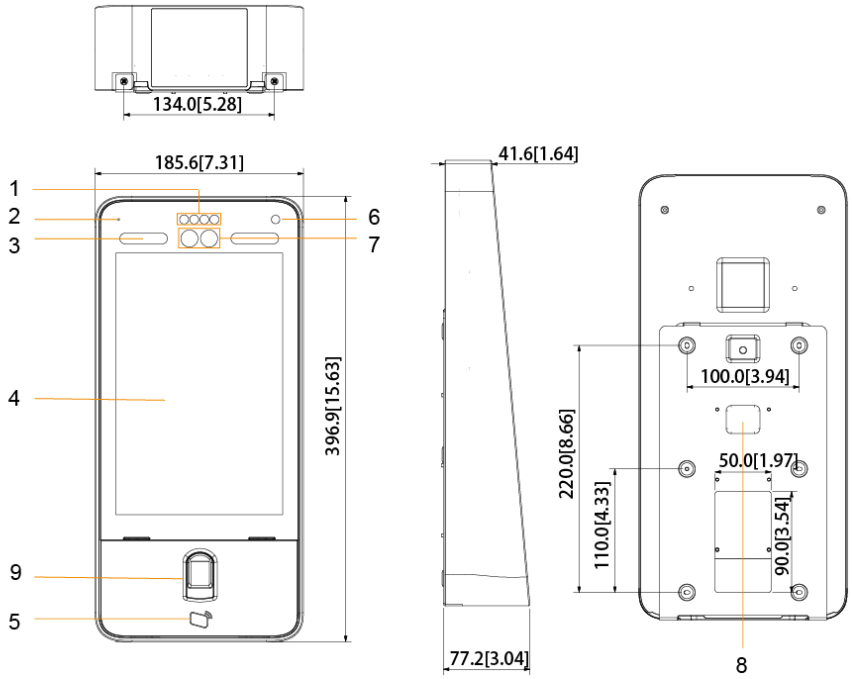


Tabella 1-4 Descrizione dei componenti (4)

N.	Nome	N.	Nome
1	Luce IR	6	Fototransistor
2	MIC	7	Doppia telecamera
3	Luce di riempimento bianca	8	Ingresso cavo
4	Display	9	Sensore impronte digitali
5	Area di lettura schede	10	–

2 Installazione

2.1 Collegamento dei cavi

Il controller di accesso deve essere collegato a dispositivi come sirene, lettori e contatti porta. Per il collegamento dei cavi, fare riferimento alla Tabella 2-1.

Tabella 2-1 Descrizione delle porte

Porta	Colore del cavo	Nome del cavo	Descrizione
CON1	Nero	RD–	Elettrodo negativo dell'alimentazione del lettore di schede esterno.
	Rosso	RD+	Elettrodo positivo dell'alimentazione del lettore di schede esterno.
	Blu	CUSTODIA	Ingresso di allarme manomissione del lettore di schede esterno.
	Bianco	D1	Ingresso (collegato al lettore di schede esterno)/Uscita (collegata al controller) D1 Wiegand.
	Verde	D0	Ingresso (collegato al lettore di schede esterno)/Uscita (collegata al controller) D0 Wiegand.
	Marrone	LED	Collegato alla spia luminosa del lettore di schede esterno
	Giallo	B	Ingresso (collegato al lettore di schede esterno)/Uscita (collegata al controller o al modulo di sicurezza del controllo porta) elettrodo negativo RS-485. ● Se il modulo di sicurezza è abilitato, occorre acquistare separatamente il modulo di sicurezza del controllo degli accessi. Il modulo di sicurezza necessita di un'alimentazione separata per fornire corrente. ● Una volta abilitato il modulo di sicurezza, il pulsante di uscita, il controllo della serratura e il collegamento antincendio non saranno più validi.

Porta	Colore del cavo	Nome del cavo	Descrizione
	Viola	A	Ingresso (collegato al lettore di schede esterno)/Uscita (collegata al controller o al modulo di sicurezza del controllo porta) elettrodo positivo RS-485. ● Se il modulo di sicurezza è abilitato, occorre acquistare separatamente il modulo di sicurezza del controllo degli accessi. Il modulo di sicurezza necessita di un'alimentazione separata per fornire corrente. ● Una volta abilitato il modulo di sicurezza, il pulsante di uscita, il controllo della serratura e il collegamento antincendio non saranno più validi.
CON2	Bianco e rosso	ALARM1_NO	Porta di uscita allarme 1 normalmente aperta.
	Bianco e arancione	ALARM1_COM	Porta di uscita allarme 1 comune.
	Bianco e blu	ALARM2_NO	Porta uscita allarme 2 normalmente aperta.
	Bianco e grigio	ALARM2_COM	Porta di uscita allarme 2 comune.
	Bianco e verde	GND	Connessione alla porta GND comune.
	Bianco Marrone	ALARM1	Porta di ingresso allarme 1.
	Bianco e giallo	GND	Connessione alla porta GND comune.
	Bianco e viola	ALARM2	Porta di ingresso allarme 2.
CON3	Nero e rosso	RIC.	Porta di ricezione RS-232.
	Nero e arancione	TRASM.	Porta di trasmissione RS-232.
	Nero e blu	GND	Connessione alla porta GND comune.
	Nero e grigio	SR1	Utilizzata per il rilevamento dei contatto della porta.
	Nero e verde	PUSH1	Pulsante di apertura porta della porta n. 1
	Nero e marrone	DOOR1_COM	Porta controllo serratura comune.
	Nero e giallo	DOOR1_NO	Porta controllo serratura normalmente aperta.
	Nero e viola	DOOR1_NC	Porta controllo serratura normalmente chiusa.

2.2 Installazione

I metodi di installazione di tutti i controller sono identici. Assicurarsi che la distanza tra l'obiettivo e il suolo sia 1,4 metri. Osservare la Figura 2-1

Figura 2-1 Altezza di installazione

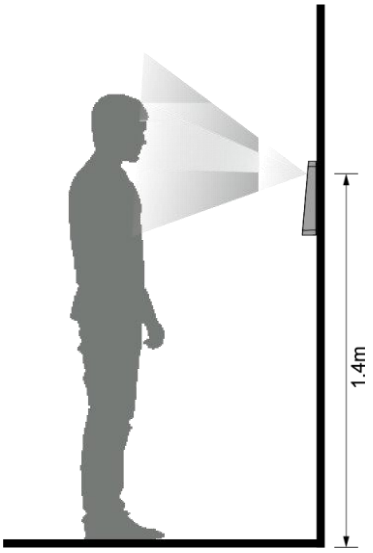
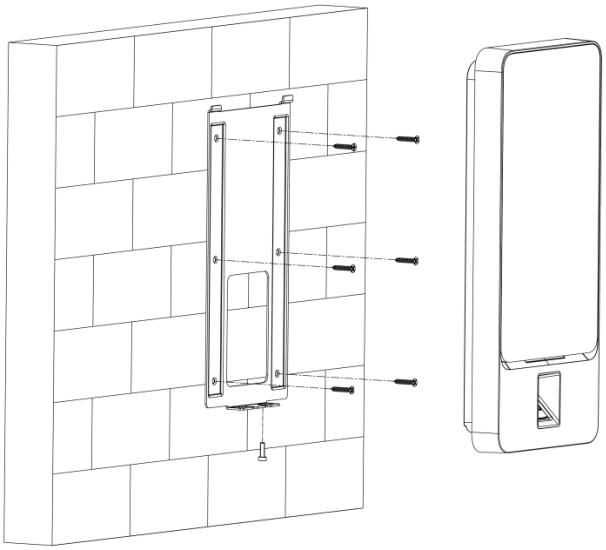


Figura 2-2 Schema di installazione



Procedura di installazione

Fase 1: Praticare sette fori (sei fori per il montaggio della staffa e un foro per il passaggio dei cavi) nella parete secondo i fori della staffa.

Fase 2: Fissare la staffa alla parete inserendo le viti ancoranti nei sei fori di installazione della staffa.

Fase 3: Collegare i cavi per il controller di accesso.

Fare riferimento alla sezione 2.1 Collegamento dei cavi.

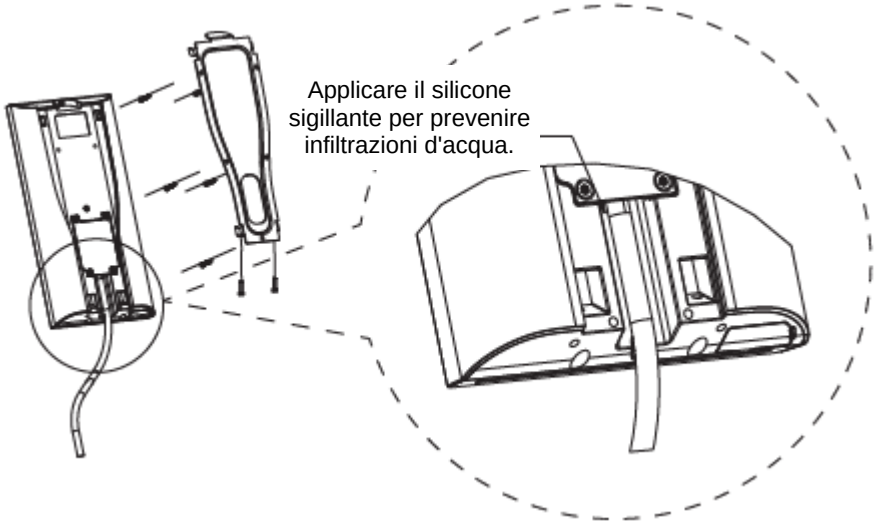
Fase 4: Applicare il silicone sigillante negli spazi tra il dispositivo e la parete.

Fase 5: Appendere il controller di accesso al gancio della staffa.

Fase 6: Stringere le viti sul lato inferiore del controller di accesso.

L'installazione è completata.

Figura 2-3 Applicazione del silicone sigillante

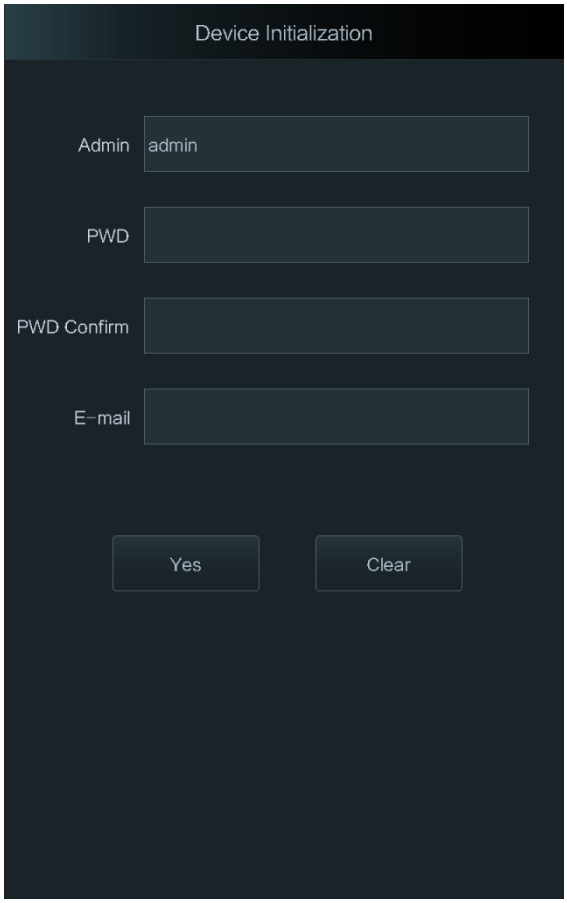


3 Funzionamento del sistema

3.1 Inizializzazione

Alla prima accensione del controller di accesso occorre impostare la password dell'amministratore e un indirizzo e-mail; in caso contrario il controller di accesso non può essere utilizzato.

Figura 3-1 Inizializzazione



L'amministratore e la password impostati in questa schermata vengono utilizzati per accedere alla piattaforma di gestione web.

Qualora l'amministratore dimentichi la propria password, questa può essere reimpostata tramite l'indirizzo e-mail immesso.

La password deve essere composta da 8-32 caratteri non spaziati e deve contenere almeno due tipi di caratteri tra maiuscole, minuscole, numeri e caratteri speciali (esclusi ' " ; : &).

3.2 Schermata di standby

È possibile sbloccare la porta tramite volti, password, schede e impronte digitali. Osservare la Tabella 3-1

Se non viene eseguita alcuna operazione entro 30 secondi, il controller di accesso entra in modalità standby.

Figura 3-2 Pagina iniziale

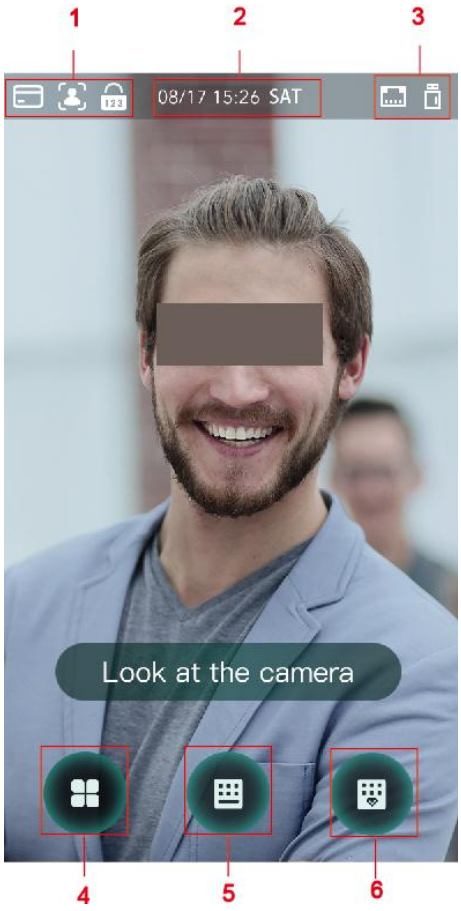


Tabella 3-1 Descrizione della pagina iniziale

N.	Descrizione
1	Modalità di sblocco: scheda, volto, impronta digitale e password. Quando scheda, volto, impronta digitale 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 e ora: la data e l'ora attuale sono mostrati qui.
3	Lo stato della rete e lo stato USB sono visualizzati qui.
4	Icona del menu principale. Solo l'amministratore può accedere al menu principale.
5	Icona di sblocco con password.
6	Icona di sblocco con password amministratore.

3.3 Modalità di sblocco

È possibile sbloccare la porta tramite volto, password, impronta digitale e scheda.

3.3.1 Schede

Strisciare la scheda sull'apposita area per sbloccare la porta.

3.3.2 Volto

Assicurarsi che il viso sia al centro della cornice per il riconoscimento del viso per sbloccare la porta.

3.3.3 Impronte digitali

Posizionare il dito sul sensore di impronte digitali per sbloccare la porta.

3.3.4 Password utente

Immettere la password utente per sbloccare la porta.

Fase 1: Toccare  sulla pagina iniziale.

Fase 2: Digitare l’ID utente, quindi toccare  .

Fase 3: Immettere la password utente, quindi toccare  .

La porta è ora sbloccata.

3.3.5 Password amministratore

Immettere la password dell'amministratore per sbloccare la porta. Esiste solo una password amministratore per un controller di accesso. La password amministratore può sbloccare la porta senza essere soggetta a livelli utente, modalità di sblocco, periodi, piani di vacanza e anti-passback.

La password amministratore non puòessere utilizzata se NC è stato selezionato in "3.6.1.5 Periodo NC".

Fase 1: Toccare  sulla pagina iniziale.

Fase 2: Toccare **Immettere la password amministratore** (Please Enter Administrator PWD).

Fase 3: Immettere la password amministratore, quindi toccare  .

La porta è ora sbloccata.

3.4 Menu principale

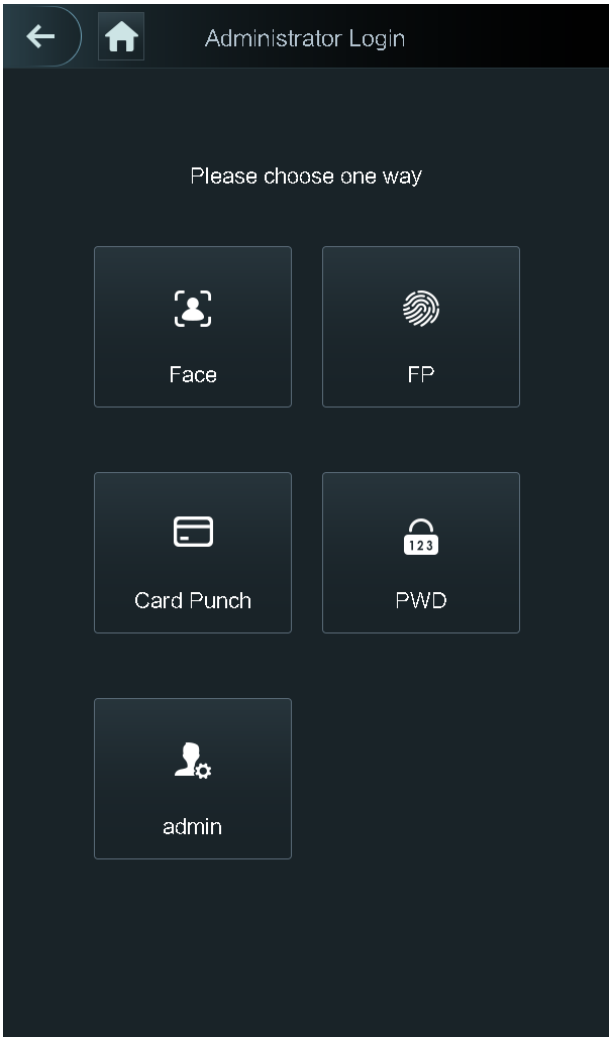
Gli amministratori possono aggiungere utenti di diversi livelli, impostare parametri relativi all'accesso, configurare la rete, visualizzare i record di accesso e le informazioni di sistema e altro ancora nel menu principale.

Fase 1: Toccare  sulla schermata di standby.

Appare la schermata **Accesso amministratore** (Administrator Login).

Modalità diverse supportano metodi di sblocco diversi, pertanto prevarrà l'interfaccia corrente.

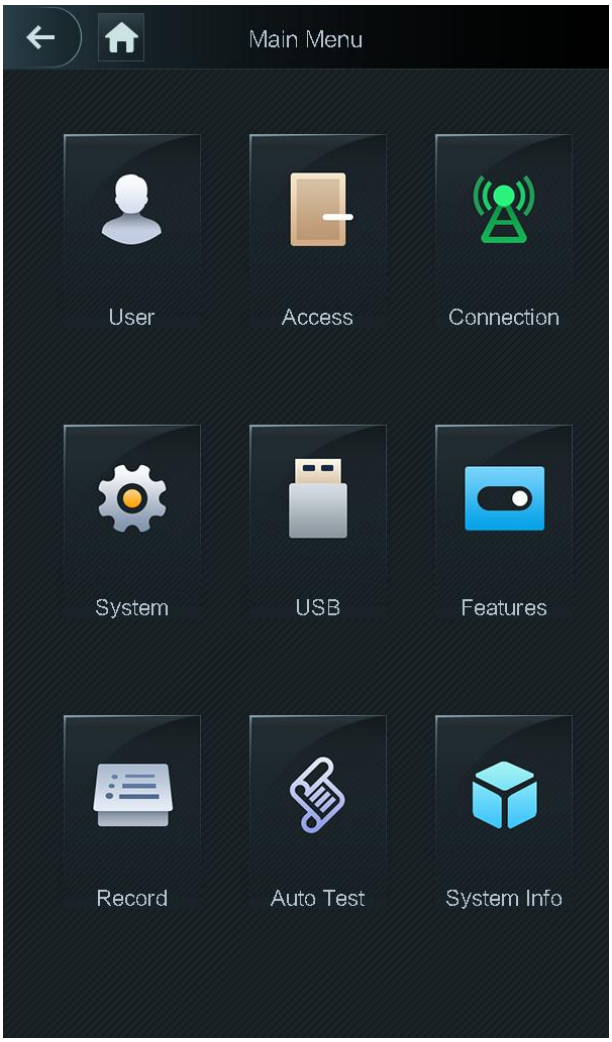
Figura 3-3 Accesso amministratore



Fase 2: Scegliere un metodo di accesso al menu principale.

Apparirà la schermata del menu principale.

Figura 3-4 Menu principale



3.5 Gestione utenti

Nella schermata **Utente** (User) è possibile aggiungere nuovi utenti, visualizzare elenchi di utenti e di amministratori e modificare la password dell'amministratore.

3.5.1 Aggiunta di un nuovo utente

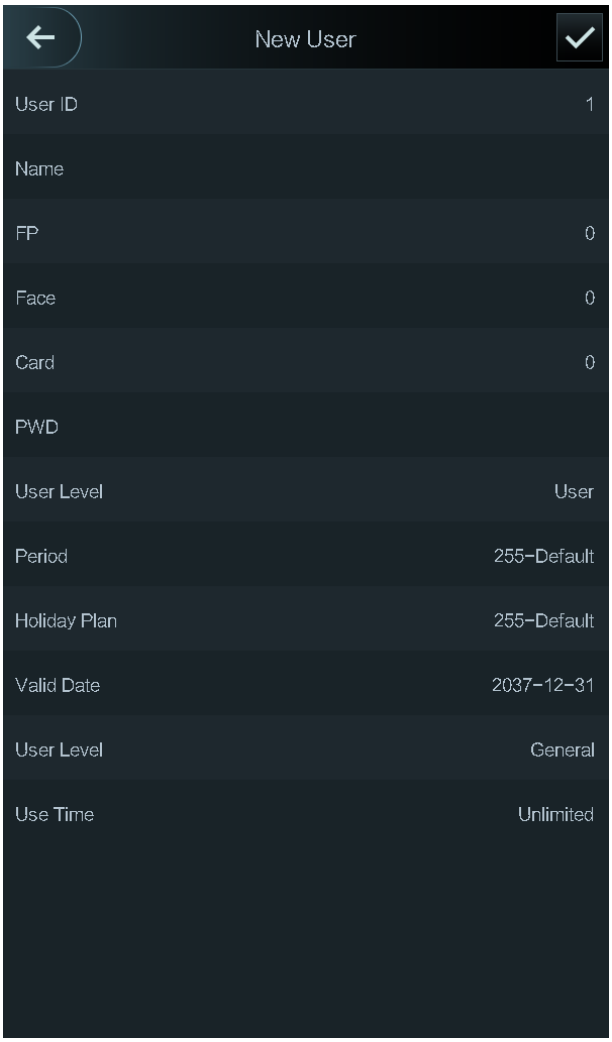
È possibile aggiungere un nuovo utente inserendo l'ID o il nome utente, importando le impronte digitali, l'immagine del volto, la schede, la password, selezionando il livello utente e altro ancora.

Le seguenti illustrazioni sono solo a titolo di riferimento e l'interfaccia effettiva prevale.

Fase 1: Selezionare **Utente > Nuovo Utente** (User > New User).

Apparirà la schermata **Info nuovo utente** (New User Info). Osservare la Figura 3-5

Figura 3-5 Info nuovo utente



Fase 2: Configurare i parametri di configurazione sulla schermata. Osservare la Tabella 3-2

Tabella 3-2 Descrittore dei parametri del nuovo utente

Parametro	Descrizione
ID utente	Qui è possibile inserire l'ID utente. L'ID può contenere numeri, lettere e relative combinazioni, con una lunghezza massima di 32 caratteri.
Nome	È possibile inserire nomi con un massimo di 32 caratteri (compresi numeri, simboli e lettere).
Impronta digitale	È possibile registrare fino a tre impronte digitali di un utente e ogni impronta digitale deve essere verificata tre volte. A una delle tre impronte digitali può essere assegnata la funzione di impronta coercizione. Gli allarmi si attivano se un'impronta di coercizione viene utilizzata per sbloccare la porta. Si sconsiglia di selezionare la prima impronta digitale come impronta di coercizione.
Volto	Assicurarsi che il viso si trovi al centro della cornice di acquisizione dell'immagine; in questo modo il controller di accesso scatterà automaticamente una foto del viso del nuovo utente. Per i dettagli, fare riferimento alla *Guida introduttiva*.

Parametro	Descrizione
Scheda	Per ciascun utente è possibile registrare fino a cinque schede. Sull'interfaccia di registrazione scheda, strisciare la scheda o digitarne il numero; in questo modo il controller di accesso leggerà le informazione della scheda. La funzione di **Scheda coercizione** (Duress Card) può essere abilitata sulla schermata di registrazione scheda. Gli allarmi si attivano se una scheda coercizione viene utilizzata per sbloccare la porta. Solo determinati modelli supportano lo sblocco con scheda.
Password	La password di sblocco della porta. Può contenere fino a 8 caratteri.
Livello utente	È possibile impostare un livello utente per i nuovi utenti. Sono disponibili due opzioni: ● Utente: gli utenti hanno solo l'autorizzazione per lo sblocco delle porte. ● Amministratore: oltre allo sblocco delle porte, gli amministratori possiedono l'autorizzazione per la configurazione dei parametri. Indipendentemente dalla presenza o meno di un amministratore nel controller di accesso, occorre l'autenticazione dell'identità dell'amministratore.
Periodo	È possibile impostare un intervallo temporale entro cui l'utente può sbloccare la porta.
Piano vacanza	È possibile impostare un piano vacanza durante il quale l'utente può sbloccare la porta.
Data validità	È possibile impostare un periodo di validità delle informazioni di sblocco dell'utente.
Livello utente	Sono disponibili sei livelli: ● Generale: utenti generici possono sbloccare normalmente la porta. ● Lista nera: quando gli utenti della lista nera aprono la porta, il personale di servizio riceve una notifica. ● Ospite: gli ospiti possono sbloccare la porta in determinati orari. Una volta superati i tempi massimi, non possono più sbloccare la porta. ● Pattuglia: gli utenti di pattuglia possono far monitorare le loro presenze, ma non hanno l'autorizzazione a sbloccare le porte. ● VIP: quando gli utenti VIP sbloccano la porta, il personale di servizio riceve una notifica. ● Persone disabili: quando una persona disabile sblocca la porta, c'è un ritardo di 5 secondi prima che la porta venga chiusa.
Frequenza di utilizzo	Quando il livello utente è Ospite, è possibile impostare il numero massimo di volte che l'utente può sbloccare la porta.

Fase 3: Dopo aver configurato tutti i parametri, toccare per salvare la configurazione.

3.5.2 Visualizzazione delle informazioni sull'utente

Nella schermata Utente (User) è possibile visualizzare elenchi di utenti e di amministratori e abilitare la password dell'amministratore.

3.6 Gestione degli accessi

È possibile gestire i seguenti aspetti dell'accesso: intervallo di tempo, modalità di sblocco, allarme, stato della porta e durata di sblocco.
Toccare **Accesso** (Access) per accedere alla schermata di gestione degli accessi.

3.6.1 Gestione periodo

È possibile impostare i seguenti periodi: vacanze, pianificazione vacanze, porta normalmente aperta, porta normalmente chiusa, verifica da remoto.

3.6.1.1 Config. periodo

È possibile configurare 128 periodi (settimane) con un intervallo di 0-127. Per ciascun giorno di un periodo (settimana), possono essere impostati quattro periodi. Gli utenti possono sbloccare la porta solo nei periodi impostati.

3.6.1.2 Gruppi di vacanze

L'utente può impostare gruppi di vacanza e i relativi piani. È possibile configurare 128 Gruppi con un intervallo di 0-127. In ogni gruppo possono essere aggiunte 16 vacanze. Dopo aver configurato l'ora di inizio e l'ora di fine di un gruppo di vacanze, gli utenti possono sbloccare la porta solo nei periodi impostati.

È possibile inserire nomi con un massimo di 32 caratteri (numeri, simboli e lettere). Toccare per salvare il nome del gruppo vacanze.

3.6.1.3 Piano vacanza

È possibile aggiungere gruppi di vacanza in piani vacanza. I piani vacanza possono essere utilizzati per gestire le autorizzazioni di accesso degli utenti in diversi gruppi vacanza. Gli utenti possono sbloccare la porta solo nel periodo impostato.

3.6.1.4 Periodo NA

Se al periodo NA viene aggiunto un periodo, la porta resterà normalmente aperta in suddetto periodo.

Le autorizzazioni per il periodo NA/NC hanno la precedenza sulle autorizzazioni di altri periodi.

3.6.1.5 Periodo NC

Se al periodo NC viene aggiunto un periodo, la porta resterà normalmente chiusa in suddetto periodo. In tale periodo gli utenti non possono sbloccare la porta.

3.6.1.6 Periodo di verifica remota

Se è stato configurato il periodo di verifica da remoto, quando si sbloccano le porte durante tale periodo è necessaria la verifica da remoto. Per sbloccare la porta in questo periodo, è necessario un comando di sblocco della porta inviata dalla piattaforma di gestione.

Occorre abilitare il periodo di verifica remota.

indica che l'opzione è attivava.

indica che l'opzione è disattivata.

3.6.2 Sblocco

Ci sono tre modalità di sblocco: modalità di sblocco, sblocco per periodo e combinazione di gruppi. Le modalità di sblocco variano a seconda dei modelli di controller di accesso e prevale il modello effettivamente in uso.

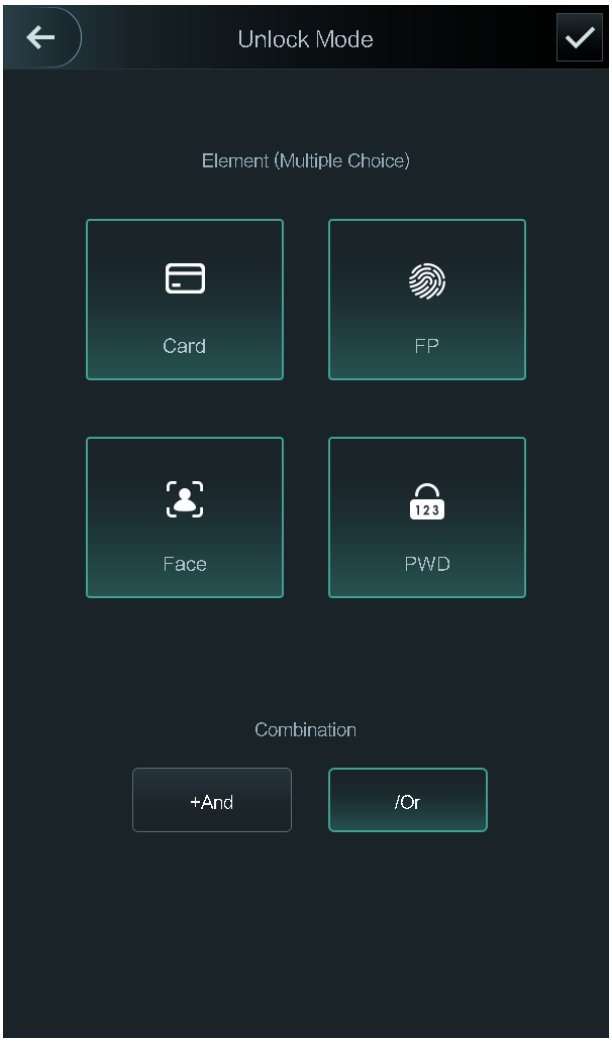
3.6.2.1 Modalità sblocco

Quando la modalità di sblocco è attiva, sono possibili i seguenti **metodi di sblocco** (Unlock Mode): scheda, impronta digitali, volto, password o uno qualsiasi dei suddetti metodi.

Fase 1: Selezionare **Valutazione > Modalità di sblocco > Modalità di sblocco** (Assess > Unlock Mode > Unlock Mode).

Appare la schermata **Elemento (scelta multipla)** [Element (Multiple Choice)]. Osservare la Figura 3-6

Figura 3-6 Elemento (scelta multipla)



Fase 2: Selezionare la modalità di sblocco.

Toccando ancora una volta la modalità di sblocco selezionata, questa verrà eliminata.

Fase 3: Selezionare una modalità di combinazione.

- **+ And** significa "e". Ad esempio, se si seleziona scheda + impronta (card + FP), significa che per sbloccare la porta è necessario prima strisciare la scheda e poi eseguire la scansione delle impronte digitali.
- **/ Or** significa "oppure". Ad esempio, se si seleziona scheda/impronta (card/FP), significa che per sbloccare la porta è necessario strisciare la scheda o eseguire la scansione delle impronte digitali.

Fase 4: Toccare per salvare le impostazioni.

Si aprirà la schermata **Modalità di sblocco** (Unlock Mode).

Fase 5: Abilitare la modalità di sblocco (Unlock Mode).

- ON indica che l'opzione è attivava.
- OFF indica che l'opzione è disattivata.

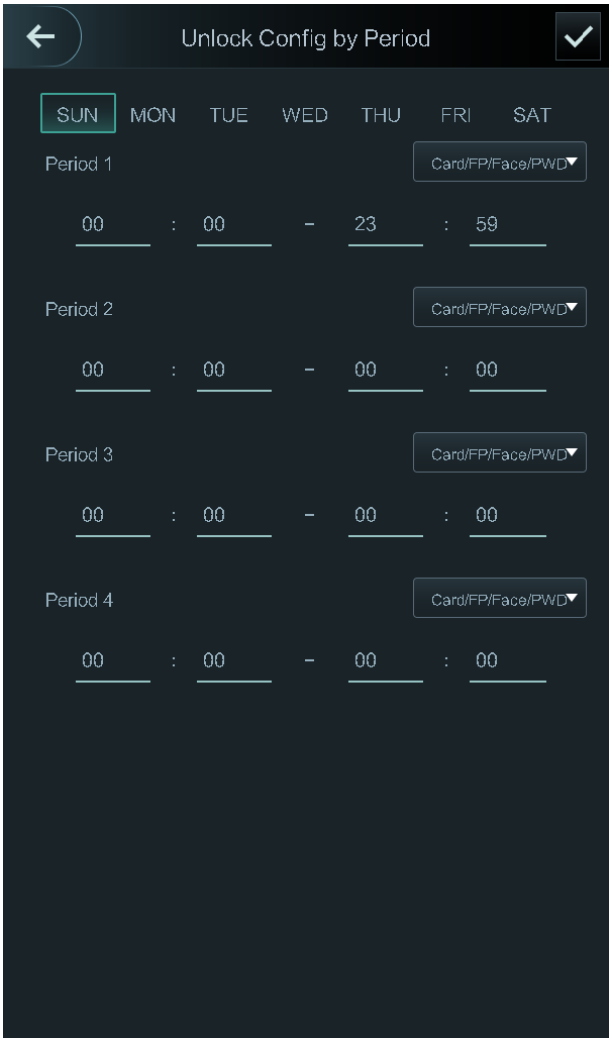
3.6.2.2 Blocco per periodo

Le porte possono essere sbloccate con modalità di sblocco differenti in periodi differenti. Ad esempio, nel periodo 1 la porta può essere sbloccata solo con la scheda, mentre nel periodo 2 solo con le impronte digitali.

Fase 1: Selezionare Valutazione > Modalità di sblocco > Modalità di sblocco > Sblocco per periodo (Assess > Unlock Mode > Unlock by Period).

Si aprirà la schermata **Config. sblocco per periodo** (Unlock Config by Period). Osservare la Figura 3-7

Figura 3-7 Blocco per periodo



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

Fase 3: Toccare  per salvare le impostazioni.

Si aprirà la schermata **Modalità di sblocco** (Unlock Mode).

Fase 4: Abilitare la funzione di sblocco per periodo.

-  indica che l'opzione è attivava.
-  indica che l'opzione è disattivata.

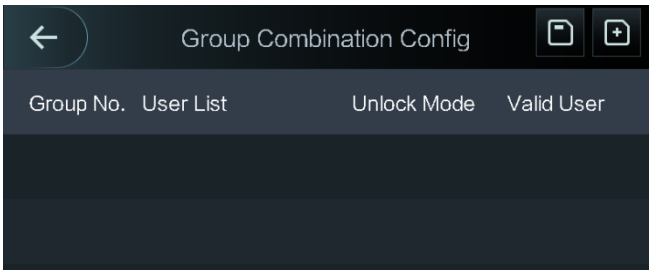
3.6.2.3 Combinazione gruppo

Se Combinazione gruppo (Group Combination) è abilitato, le porte possono essere sbloccate da uno o più gruppi formati da più di due utenti.

Fase 1: Selezionare **Valutazione > Modalità di sblocco > Combinazione gruppo** (Assess > Unlock Mode > Group Combination).

Si aprirà la schermata **Config. combinazione gruppo** (Group Combination Config). Osservare la Figura 3-8

Figura 3-8 Combinazione gruppo



Fase 2: Toccare  per creare un gruppo.

Il sistema mostra l'interfaccia di **Aggiunta gruppo** (Add group). Osservare la Figura 3-9

Figura 3-9 Aggiungi un gruppo

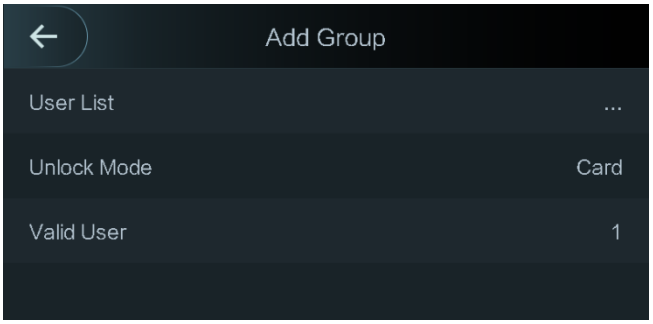


Tabella 3-3 Parametri del gruppo

Parametro	Descrizione
Elenco utenti	Aggiungere utenti nel nuovo gruppo creato. 1. Toccare **Elenco utenti** (User List). Si aprirà la schermata **Elenco utenti** (User List). 2. Toccare  , quindi digitare un ID utente. 3. Toccare  per salvare le impostazioni.
Modalità sblocco	Sono disponibili quattro opzioni: **Scheda** (Card), **Impronta** (FP)**, Password** (PWD) **e Volto** (Face).

Parametro	Descrizione
Utente valido	Utenti in possesso dell'autorizzazione per lo sblocco sono considerati utenti validi. Le porte possono essere sbloccate solo quando il numero di utenti autorizzati a sbloccare le porte è uguale al numero di utenti validi. ● Utenti validi non possono superare il numero totale di utenti in un gruppo. ● Se gli utenti validi equivalgono al numero totale di utenti di un gruppo, le porte possono essere sbloccate da tutti gli utenti del gruppo. ● Se il numero di utenti validi è inferiore al numero totale di utenti di un gruppo, le porte possono essere sbloccate da tutti gli utenti il cui numero è uguale al numero di utenti validi.

Fase 3: Toccare  per tornare alla schermata precedente.

Fase 4: Toccare  per salvare le impostazioni.

Fase 5: Abilitare la **Combinazione gruppo** (Group Combination).

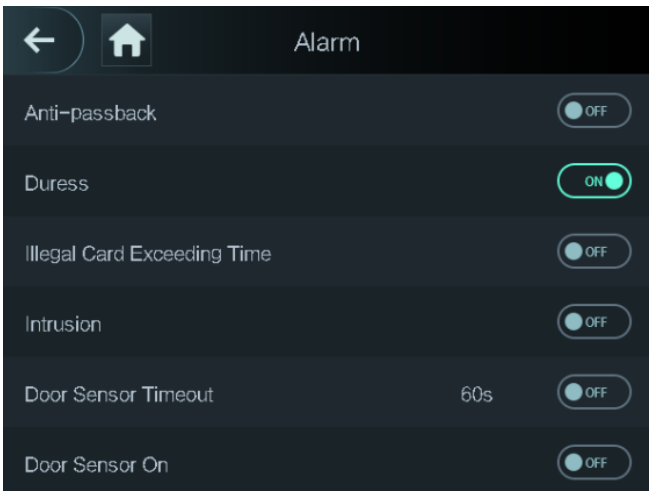
-  indica che l'opzione è attivava.
-  indica che l'opzione è disattivata.

3.6.3 Configurazione di allarme

Gli amministratori possono gestire le autorizzazioni di sblocco dei visitatori tramite la configurazione degli allarmi.

Selezionare **Accesso > Allarme** (Access > Alarm). Si aprirà la schermata degli allarmi. Osservare la Figura 3-10

Figura 3-10 Allarme



-  indica che l'opzione è attivava.
-  indica che l'opzione è disattivata.

Tabella 3-4 Parametri sulla schermata degli allarmi

Parametro	Descrizione
Anti-passback	● Una persona sblocca la porta e la sua identità viene verificata dal controller di accesso; se la stessa persona esce senza far verificare l'identità dal controller di accesso, scatta un allarme e perderà l'autorizzazione per sbloccare la porta. ● Se una persona entra in un edificio o in una stanza senza strisciare la scheda, ma esce strisciandola, tale persona non avrà più l'autorizzazione per sbloccare la porta.
Coercizione	Un allarme si attiva se una scheda, una password o un'impronta coercizione viene utilizzata per sbloccare la porta.
Numero massimo di passaggi di una scheda non autorizzata	Se una scheda non autorizzata viene utilizzata per sbloccare la porta più di 5 volte in 50 secondi, scatta un allarme.
Intrusione	Un allarme anti-intrusione scatta se una porta viene aperta senza che il contatto della porta venga sbloccato.
Timeout sensore porta	Un allarme di timeout si attiva se il tempo che un utente impiega per sbloccare la porta supera il tempo di timeout del sensore della porta. L'intervallo di timeout del sensore porta è 1-9999 secondi.
Sensore porta attivo	L'allarme anti-intrusione e l'allarme di timeout del sensore porta possono essere attivati solo se l'opzione **Sensore porta attivo** (Door Sensor On) è abilitata.

3.6.4 Stato porta

Sono disponibili tre opzioni: **NA**, **NC** e **Normale** (NO, NC, Normal).

- NA: selezionando **NA** (NO), lo stato della porta è normalmente aperto e la porta non sarà mai chiusa.
- NC: selezionando **NC**, lo stato della porta è normalmente chiuso e la porta non sarà mai sbloccata.
- Normale: selezionando **Normale** (Normal), la porta sarà sbloccata o bloccata a seconda delle impostazioni.

3.6.5 Durata di sblocco

La **Durata di sblocco serratura** (Lock Holding Time) indica l'intervallo di tempo in cui la serratura resta sbloccata. La serratura viene automaticamente bloccata se è stata sbloccata per un periodo superiore alla durata impostata.

3.7 Comunicazione di rete

Per il corretto funzionamento del controller di accesso occorre configurare i parametri di rete, delle porte seriali e delle porte Wiegand.

3.7.1 Indirizzo IP

3.7.1.1 Configurazione IP

Configurare l'indirizzo IP del controller di accesso per la connessione di rete. Fare riferimento alla Figura 3-11 e alla Tabella 3-5.

Figura 3-11 Configurazione dell'indirizzo IP

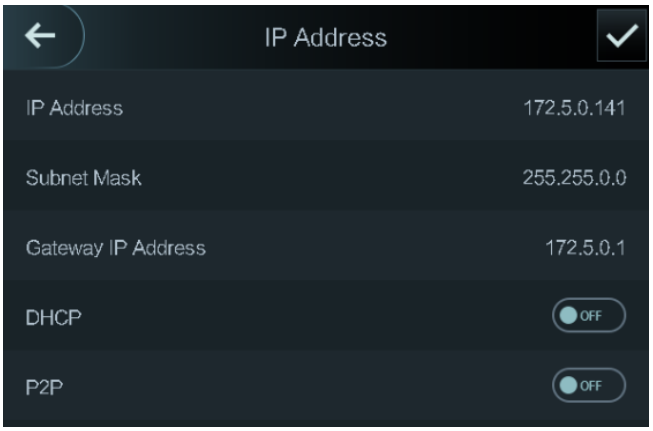


Tabella 3-5 Parametri di configurazione IP

Parametro	Descrizione
Indirizzo IP/Subnet mask/Indirizzo IP Gateway	L'indirizzo IP, la subnet mask e l'indirizzo IP del gateway devono essere nello stesso segmento di rete. Al termine della configurazione, toccare per salvare i valori.
DHCP	DHCP (protocollo di configurazione host dinamico). Quando il DHCP è abilitato, l'indirizzo IP viene acquisito automaticamente; l'indirizzo IP, la subnet mask e l'indirizzo IP del gateway non possono essere configurati manualmente.
P2P	P2P è una tecnologia di rete privata che consente all'utente di gestire i dispositivi senza richiedere il DDNS, la mappatura delle porte o il server di transito.

3.7.1.2 Registrazione attiva

La registrazione attiva consente di collegare il controller di accesso alla piattaforma di gestione.

Le configurazioni effettuate possono essere cancellate sulla piattaforma di gestione e il controller di accesso può essere inizializzato; pertanto è necessario proteggere il controllo della gestione della piattaforma in caso di perdita di dati causata da un cattivo funzionamento.

Per i parametri di registrazione attiva, fare riferimento alla Tabella 3-6.

Tabella 3-6 Registrazione attiva

Nome	Parametro
Indirizzo IP del server	Indirizzo IP della piattaforma di gestione.
Porta	Numero di porta della piattaforma di gestione.
ID dispositivo	Numero di dispositivo subordinato sulla piattaforma di gestione.

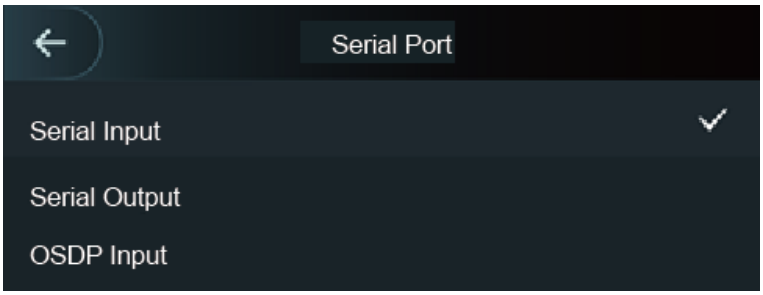
3.7.1.3 Wi-Fi

Se il controller di accesso è dotato di funzione Wi-Fi è possibile collegarlo alla rete.

3.7.2 Impostazioni della porta seriale

Selezionare l'ingresso o l'uscita seriale in base alla direzione di entrata e di uscita.
Selezionare **Connessione > Porta seriale** (Connection > Serial Port) per aprire la schermata **Porta seriale** (Serial Port). Osservare la Figura 3-12

Figura 3-12 Porta seriale



- Selezionare **Ingresso seriale** (Serial Input) quando al controller di accesso sono collegati dispositivi esterni con funzioni di lettura e scrittura scheda. **Ingresso seriale** (Serial Input) viene selezionato per consentire l'invio delle informazioni della scheda di accesso al controller di accesso e alla piattaforma di gestione.
- Nel caso di controller di accesso con funzioni di riconoscimento del volto, riconoscimento delle impronte digitali, lettura e scrittura della scheda, selezionando **l'Uscita Seriale** (Serial Output), le informazioni di blocco/sblocco verranno inviate a tali controller di accesso. Esistono due tipi di informazioni di blocco/sblocco:
  - ◇ ID utente
  - ◇ N. scheda
- Selezionare Ingresso OSDP (OSDP Input) se il lettore di schede del protocollo OSDP è collegato al controller di accesso. Il controller di accesso invia le informazioni della scheda alla piattaforma di gestione.

3.7.3 Configurazione Wiegand

Selezionare **Ingresso Wiegand** (Wiegand Input) o **Uscita Wiegand** (Wiegand Output) in base alla direzione di entrata e di uscita.
Selezionare **Connessione > Wiegand** (Connection > Wiegand) per aprire la schermata Wiegand. Osservare la Figura 3-13

Figura 3-13 Wiegand

- Selezionare **Ingresso Wiegand** (Wiegand Input) quando un meccanismo di scorrimento scheda esterno è collegato al controller di accesso.
- Selezionare **Uscita Wiegand** (Wiegand Output) quando il controller di accesso funge da lettore collegabile al controller. Osservare la Tabella 3-7

Tabella 3-7 Uscita Wiegand

Parametro	Descrizione
Tipo di uscita Wiegand	Il tipo di uscita Wiegand determina il numero della scheda o la cifra del numero riconoscibile dal controller di accesso. ● Weigand26, tre byte, sei cifre. ● Weigand34, quattro byte, otto cifre. ● Weigand66, otto byte, sedici cifre.
Ampiezza impulso	L'utente può impostare l'ampiezza e l'intervallo dell'impulso.
Intervallo impulso	
Tipo di dati in uscita	Qui è possibile selezionare i tipi di dati in uscita. ● ID utente: selezionando questa opzione, il tipo di dati in uscita sarà ID utente. ● N. scheda: selezionando questa opzione, il tipo di dati in uscita sarà N. scheda.

3.8 Sistema

3.8.1 Ora

Qui è possibile configurare la data e il formato della data, l'ora, l'ora legale, la verifica NTP e il fuso orario.

Se si seleziona il Network Time Protocol (NTP), occorre abilitare prima la funzione di verifica NTP. Indirizzo IP del server: inserendo l'indirizzo IP del server di riferimento dell'ora, l'ora del controller di accesso sarà sincronizzata con il suddetto server.
Porta: immettere qui il numero della porta del server di riferimento dell'ora.
Intervallo (minuti): Intervallo della verifica NTP. Per salvare, toccare l'icona di salvataggio delle impostazioni.

3.8.2 Parametro volto

Figura 3-14 Parametro volto

Toccare un parametro, eseguire la configurazione, quindi toccare .

Tabella 3-8 Parametro volto

Nome	Descrizione
Soglia di riconoscimento volti	L'utente può regolare la precisione del riconoscimento dei volti. Più alto è il valore, più elevata sarà la precisione.
Angolo max. di riconoscimento volti	Qui è possibile impostare l'angolo di inquadratura dei profili del pannello di controllo. Più grande è il valore, più ampia è la gamma di profili che verrà riconosciuta.
Distanza pupille	La distanza pupillare è il valore in pixel dell'immagine tra il centro delle pupille di ciascun occhio. Occorre impostare un valore appropriato in modo che il controller di accesso possa riconoscere i volti. Il valore cambia a seconda delle dimensioni del volto e della distanza tra i volti e l'obiettivo. Più il volto è vicino all'obiettivo, maggiore deve essere il valore. Se un adulto si trova a 1,5 metri di distanza dall'obiettivo, il valore della distanza pupillare può essere compreso tra 50 e 70.
Timeout riconoscimento	Quando una persona che non possiede l'autorizzazione all'accesso si trova di fronte al controller di accesso per il riconoscimento del volto, il controller segnalerà che il riconoscimento non è riuscito. L'intervallo fino alla segnalazione è chiamato timeout di riconoscimento.
Intervallo di riconoscimento	Quando una persona che possiede l'autorizzazione all'accesso si trova di fronte al controller di accesso per il riconoscimento del volto, il controller segnalerà che il riconoscimento è riuscito. L'intervallo fino alla segnalazione è chiamato intervallo di riconoscimento.
Soglia anti-falsificazione	Questa funzione impedisce alle persone di sbloccare la porta con immagini o modelli di volti. Più grande è il valore, più difficile sarà che l'immagine del volto possa sbloccare la porta. Si consiglia un valore superiore a 80.

3.8.3 Impostazioni della modalità luce di riempimento

Scegliere la modalità di luce di riempimento in base alle proprie esigenze. Sono disponibili tre modalità:

- Automatica: quando il sensore fotografico rileva che l'ambiente circostante non è buio, la luce di riempimento è normalmente spenta; in caso contrario, la luce di riempimento sarà accesa.
- NA: la luce di riempimento è normalmente accesa.
- NC: la luce di riempimento è normalmente spenta.

3.8.4 Impostazioni di luminosità della luce di riempimento

Scegliere la luminosità della luce di riempimento in base alle proprie esigenze.

3.8.5 Regolazione del volume

Toccare  o  per regolare il volume.

3.8.6 Regolazione di luminosità della luce IR

Più grande è il valore, più chiare saranno le immagini.

3.8.7 Parametro impronta digitale

Qui è possibile impostare il livello di precisione dell'impronta digitale. Più alto è il livello, più basso sarà il tasso di riconoscimenti errati.

3.8.8 Ripristino delle impostazioni di fabbrica

Ripristinando le impostazioni di fabbrica del controller di accesso tutti i dati andranno persi.
Una volta ripristinate le impostazioni di fabbrica del controller di accesso, l'indirizzo IP non verrà modificato.
L'utente può decidere se conservare le informazioni utente e i registri.

- È possibile selezionare di ripristinare le impostazioni di fabbrica del controller di accesso con tutte le informazioni dell'utente e le informazioni sul dispositivo cancellate.
- Oppure di ripristinare le impostazioni di fabbrica del controller di accesso senza cancellare le informazioni dell'utente e le informazioni sul dispositivo.

3.8.9 Riavvia

Selezionare **Impostazioni > Riavvio** (Setting > Reboot), quindi toccare **Riavvia** (Reboot) per riavviare il controller di accesso.

3.9 Unità USB

Assicurarsi che l'unità USB sia inserita prima di esportare le informazioni dell'utente e di effettuare l'aggiornamento. Durante l'esportazione o l'aggiornamento, non rimuovere l'unità USB e non effettuare altre operazioni, altrimenti l'esportazione o l'aggiornamento non andranno a buon fine.

È necessario esportare le informazioni da un controller di accesso all'unità USB prima di utilizzare quest'ultima per importare le informazioni su un altro controller di accesso.

L'unità USB può essere utilizzata anche per aggiornare il programma.

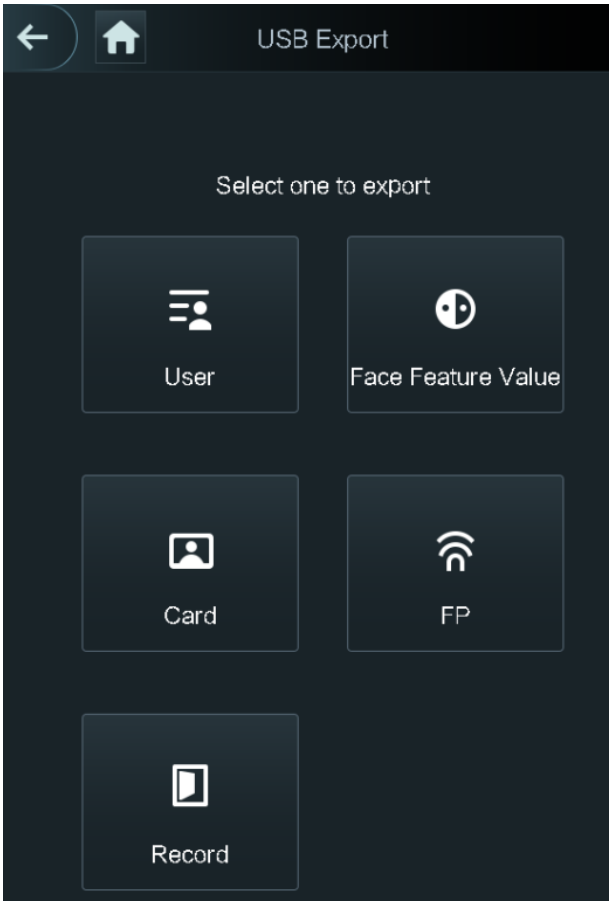
3.9.1 Esportazione verso l'unità USB

Dopo aver inserito l'unità USB è possibile esportarvi i dati dal controller di accesso. I dati esportati sono crittografati e non è possibile modificarli.

Fase 1: Selezionare **USB > Esporta USB** (USB > USB Export).

Si aprirà la schermata **Esporta USB** (USB Export). Osservare la Figura 3-15

Figura 3-15 Esportazione verso l'unità USB



Fase 2: Selezionare i tipi di dati che si desidera esportare.

Viene visualizzato il messaggio Conferma per esportare (Confirm to export).

Fase 3: Toccare **OK**.

I dati esportati vengono salvato sull'unità USB.

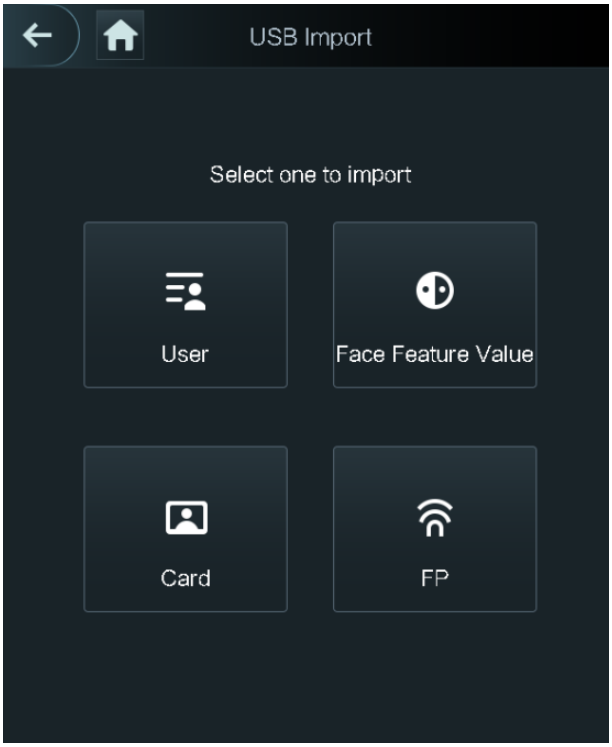
3.9.2 Importazione USB

Solo i dati contenuti nell'unità USB che sono stati esportati da un controller di accesso possono essere importati in un altro controller di accesso.

Fase 1: Selezionare **USB > Importazione USB** (USB > USB Import).

Si aprirà la schermata **Importazione USB** (USB Import). Osservare la Figura 3-16

Figura 3-16 Importazione USB



Fase 2: Selezionare i tipi di dati che si desidera importare.

Viene visualizzato il messaggio **Conferma per importare** (Confirm to import).

Fase 3: Toccare **OK**.

I dati contenuti nell'unità USB verranno importati nel controller di accesso.

3.9.3 Aggiornamento USB

L'unità USB può essere utilizzata anche per aggiornare il sistema.

Fase 1: Modificare il nome del file di aggiornamento in "update.bin" e salvarlo nella directory radice dell'unità USB.

Fase 2: Selezionare **USB > Aggiornamento tramite USB** (USB > USB Update).

Viene visualizzato il messaggio **Conferma per aggiornare** (Confirm to Update).

Fase 3: Toccare **OK**.

Il processo di aggiornamento si avvia e una volta terminato il controller di accesso verrà riavviato.

3.9.4 Funzionalità

L'utente può configurare le impostazione della privacy, invertire il numero della scheda, configurare il modulo di sicurezza, il tipo di sensore porta e ottenere un feedback del risultato. Per dettagli sulle funzioni citate, fare riferimento alla Figura 3-17 e alla Tabella 3-9.

Figura 3-17 Caratteristiche

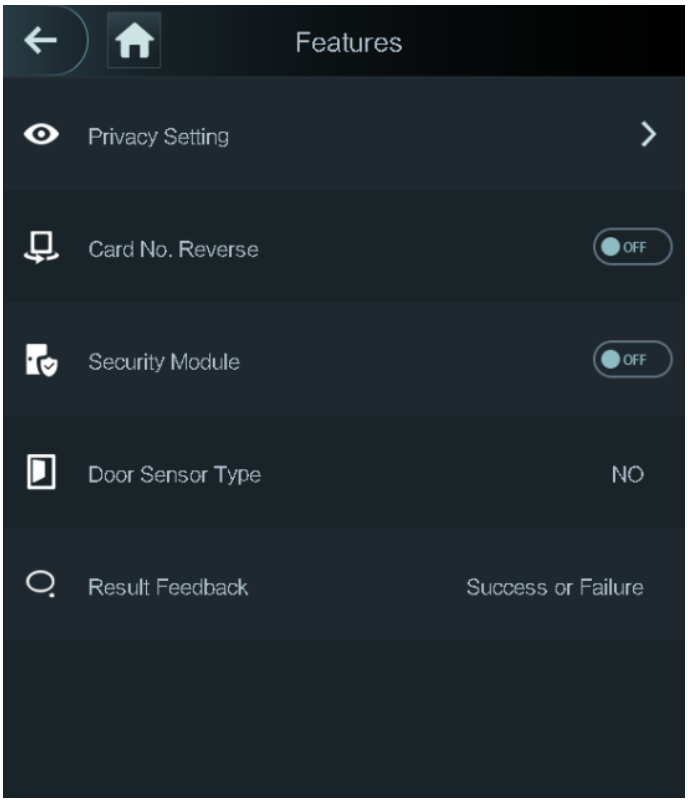


Tabella 3-9 Descrizione delle funzioni

Parametro	Descrizione
Impostazioni di privacy	Fare riferimento a "3.9.5 Impostazioni di privacy" per i dettagli.
Inversione numero scheda	Se il lettore di schede di terze parti deve essere collegato al controller di accesso attraverso la porta di uscita Wiegand, è necessario abilitare la funzione di inversione del numero di scheda; altrimenti la comunicazione tra il controller di accesso e il lettore di schede di terze parti potrebbe non funzionare a causa di una discrepanza di protocollo.
Modulo di sicurezza	• Se il modulo di sicurezza è abilitato, occorre acquistare separatamente il modulo di sicurezza del controllo degli accessi. Il modulo di sicurezza necessita di un'alimentazione separata per fornire corrente. • Una volta abilitato il modulo di sicurezza, il pulsante di uscita, il controllo della serratura e il collegamento antincendio non saranno più validi.
Tipo di sensore porta	Sono disponibili due opzioni: **NA** (NO) e **NC**.
Feedback risultato	Mostra se lo sblocco è andato o meno a buon fine.

3.9.5 Impostazioni di privacy

Figura 3-18 Impostazioni di privacy

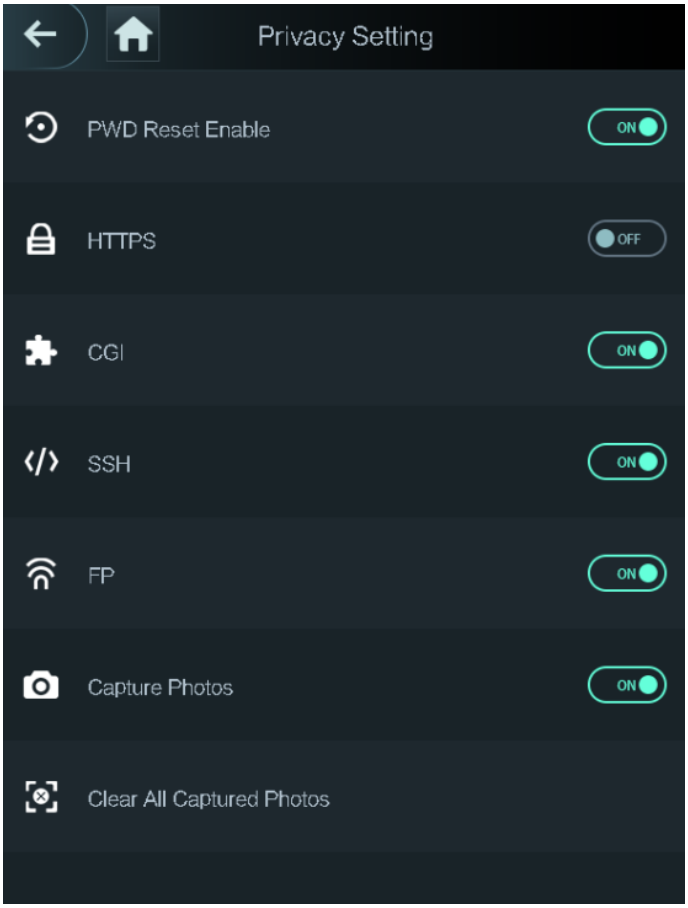


Tabella 3-10 Caratteristiche

Parametro	Descrizione
Abilita la reimpostazione della password	Se la funzione **Abilita la reimpostazione della password** (PWD Reset Enable) è stata abilitata, sarà possibile reimpostare la password. La funzione di reimpostazione della password è abilitata per impostazione predefinita.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) è un protocollo che garantisce la sicurezza della comunicazione su una rete di computer. Se abilitato, HTTPS verrà utilizzato per accedere ai comandi CGI; altrimenti verrà utilizzato il protocollo HTTP. Quando HTTPS viene abilitato, il controller di accesso si riavvia automaticamente.
CGI	Common Gateway Interface (CGI) offre un protocollo standard per i server web che consente di eseguire programmi come applicazioni di console in esecuzione su un server che genera pagine web in modo dinamico. Quando la funzione CGI è abilitata, è possibile utilizzare i comandi CGI. CGI è abilitato per impostazione predefinita.

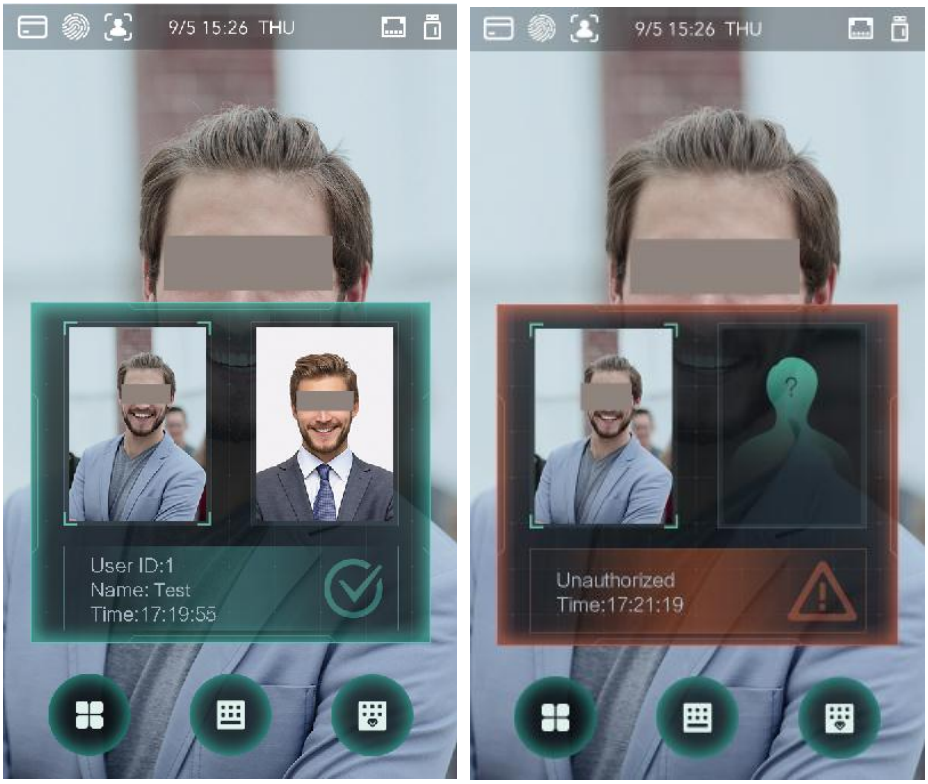
Parametro	Descrizione
SSH	Secure Shell (SSH) è un protocollo di rete crittografico per il funzionamento sicuro dei servizi di rete su una rete non protetta. Se abilitato, SSH fornisce un servizio di crittografia per la trasmissione dei dati.
Impronta digitale	Se si seleziona DISATTIVA (OFF) per Impronte digitale (FP), le informazioni sulle impronte digitali degli utenti non vengono visualizzate durante il loro rilevamento o quando si utilizzano le impronte digitali per sbloccare la porta.
Acquisizione foto	Selezionando ATTIVA (ON), quando una persona sblocca la porta, verrà automaticamente acquisita una sua fotografia. Questa funzione è attiva per impostazione predefinita.
Cancellare tutte le foto acquisite	Toccare questa icona per eliminare tutte le foto acquisite.

3.9.6 Feedback risultato

L'utente può scegliere una modalità di feedback in base alle proprie esigenze.

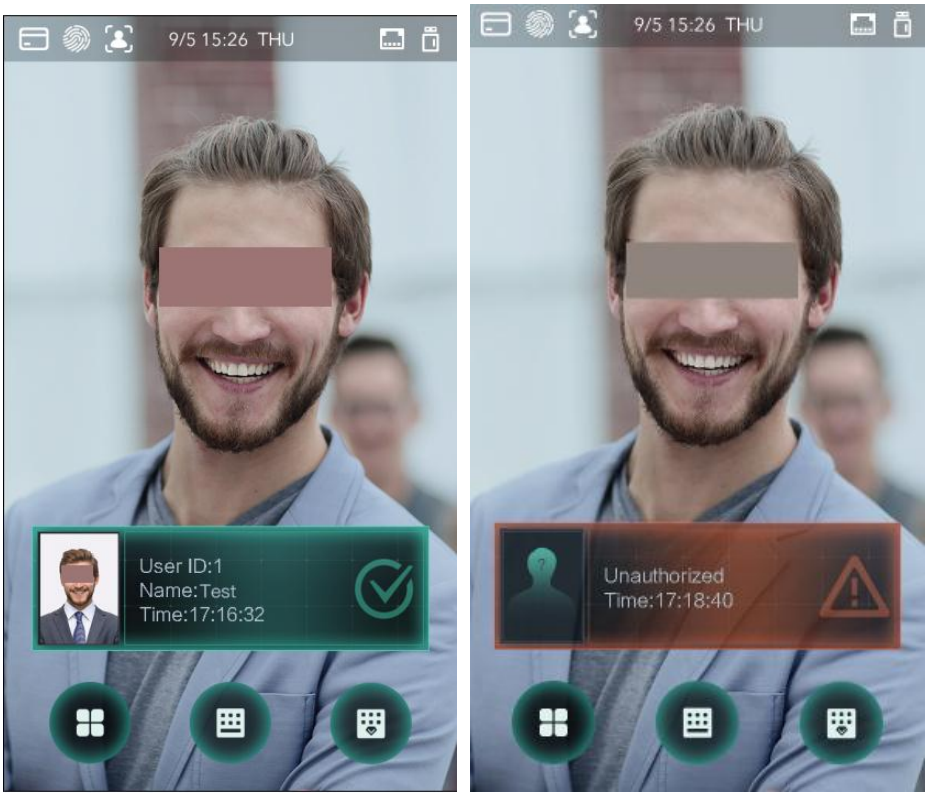
Modalità 1

Figura 3-19 Modalità 1



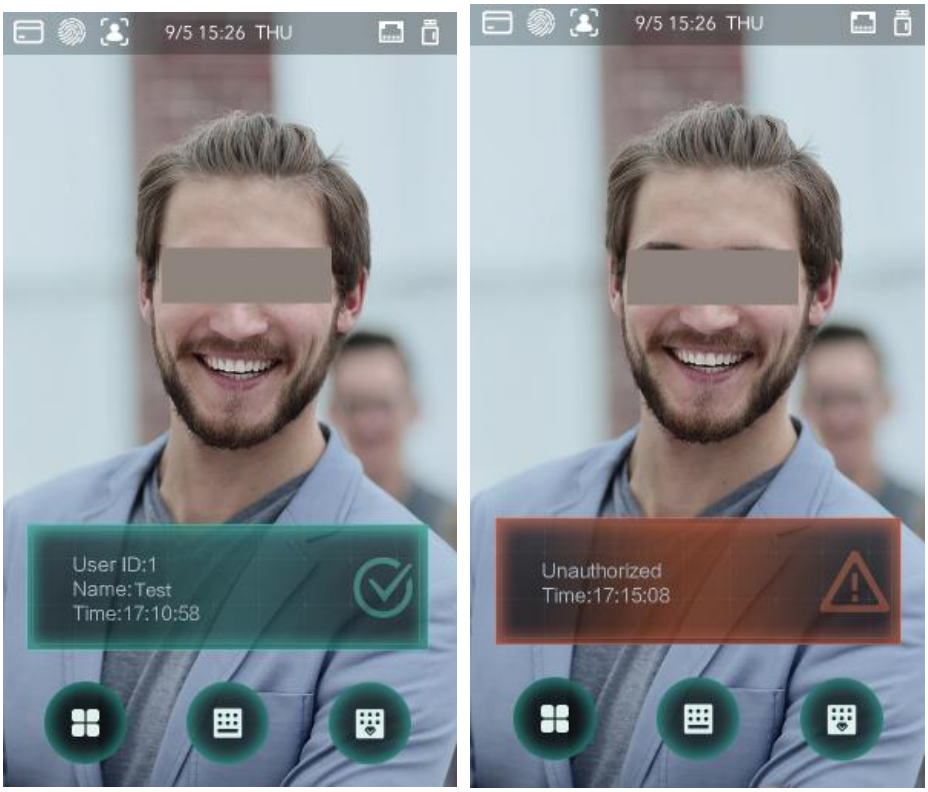
Modalità 2

Figura 3-20 Modalità 2



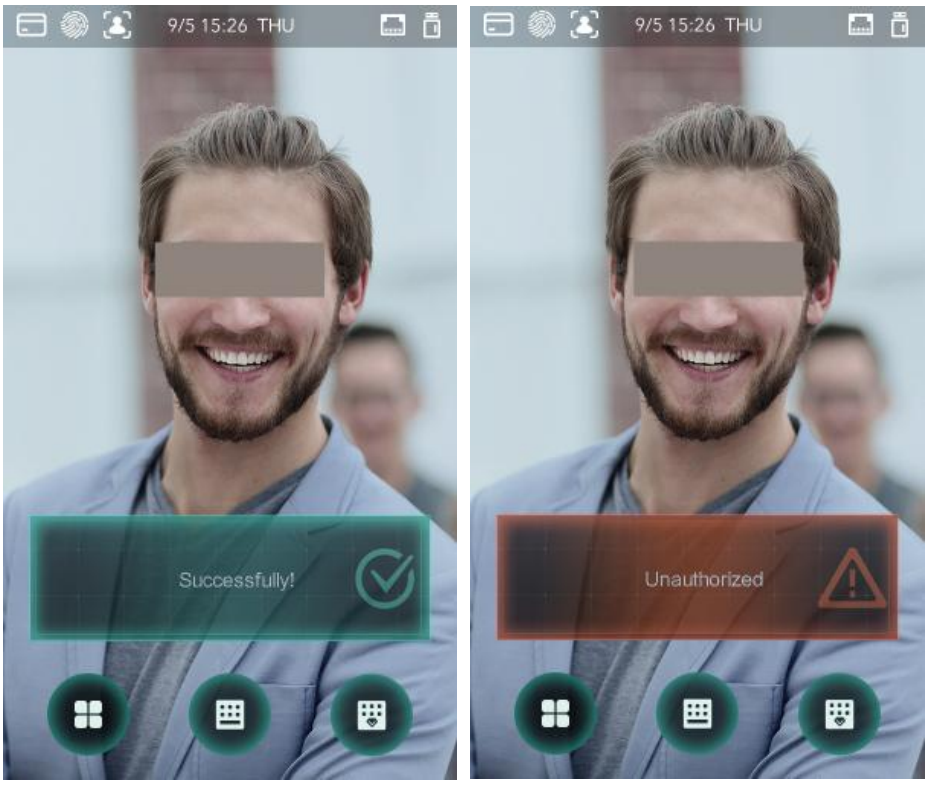
Modalità 3

Figura 3-21 Modalità 3



Modalità 4

Figura 3-22 Modalità 4



3.10 Registra

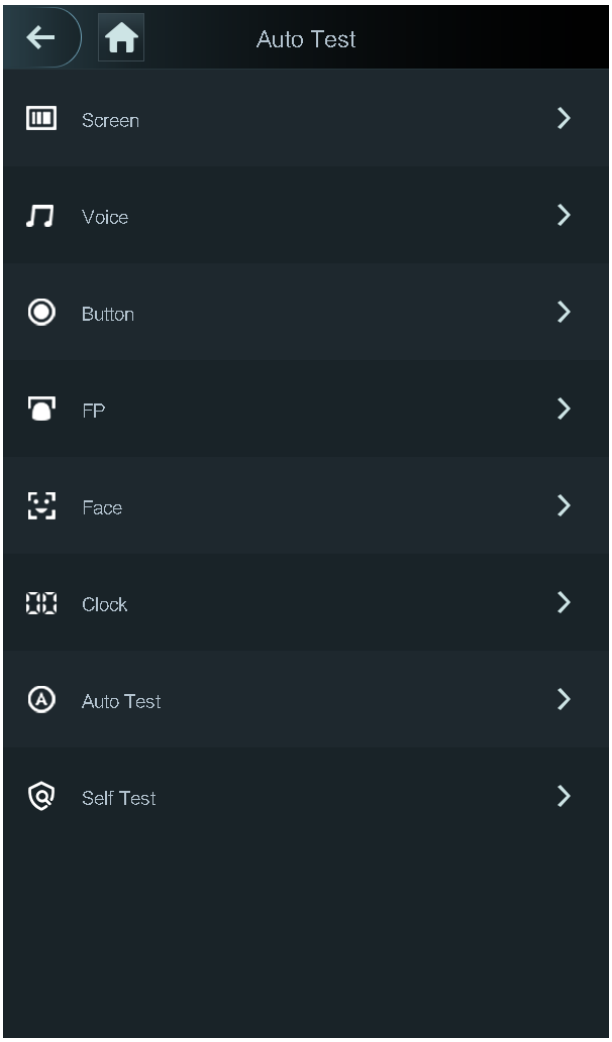
È possibile consultare tutti i record di sblocco.

Figura 3-23 Ricerca record di timbro cartellino

3.11 Test automatico

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 può funzionare normalmente. Procedere in base alle indicazioni.

Figura 3-24 Test automatico



Quando si seleziona **Test automatico** (Auto Test), il controller di accesso guiderà l'utente attraverso l'esecuzione di tutti i test automatici.

3.12 Informazioni sul sistema

Sulla schermata **Informazioni di sistema** (System Info) è possibile visualizzare la capacità di dati, la versione del dispositivo e le informazioni sul firmware del controller di accesso.

4 Operazioni su Web

L'utente può configurare e utilizzare il controller di accesso tramite interfaccia web. Tramite interfaccia web è possibile impostare i parametri di rete, i parametri video e i parametri del controller di accesso; inoltre l'utente può effettuare la manutenzione e l'aggiornamento del sistema.

4.1 Inizializzazione

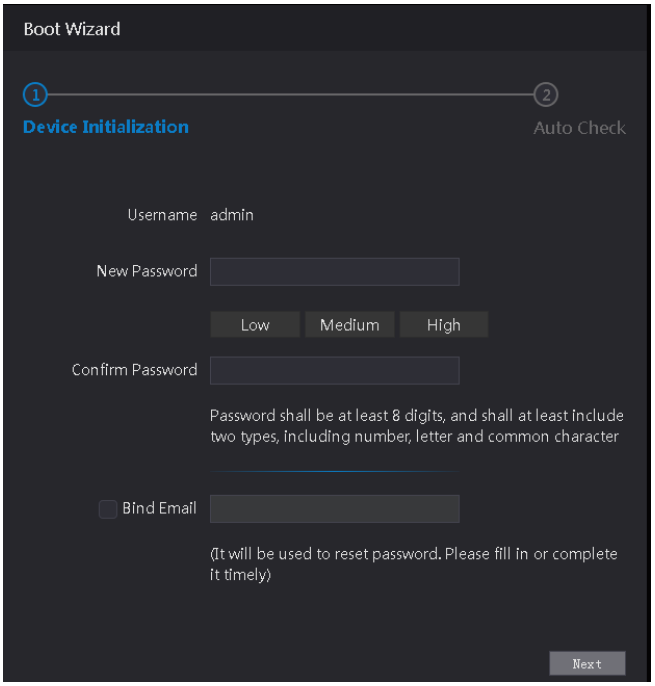
Prima di effettuare il primo login sul web è necessario impostare una password e un indirizzo e-mail.

Fase 1: Aprire il Web browser IE e digitare l'indirizzo IP del controller di accesso (l'indirizzo predefinito è 192.168.1.108) nella barra degli indirizzi, quindi premere Invia.

Il sistema mostra la schermata **Inizializzazione** (initialization). Osservare la Figura 4-1

Utilizzare un browser più recente di IE 8, altrimenti potrebbe non essere possibile effettuare l'accesso sul web.

Figura 4-1 Inizializzazione



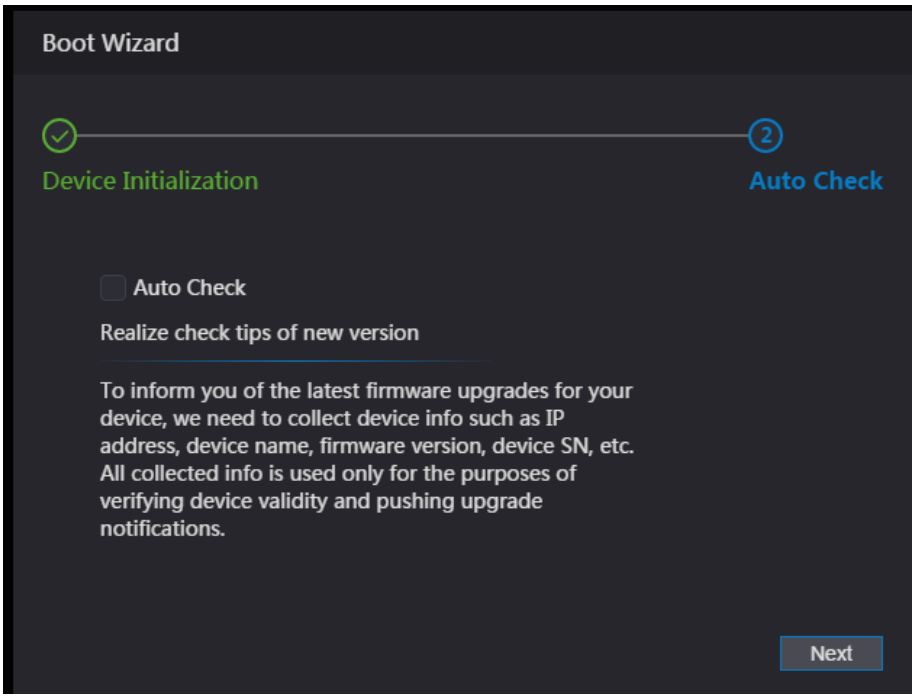
Fase 2: Immettere la nuova password e confermarla, quindi immettere un indirizzo e-mail e toccare **Avanti** (Next).

- Per motivi di sicurezza, conservare la password in modo appropriato dopo l'inizializzazione e modificarla regolarmente.
- La password deve essere composta da 8-32 caratteri non spaziati e deve contenere almeno due tipi di caratteri tra maiuscole, minuscole, numeri e caratteri speciali (esclusi ' " ; : &). Impostare una password con un livello di sicurezza elevato in base alle istruzioni visualizzate.
- Se occorre reimpostare la password dell'amministratore tramite la scansione del codice QR, è necessario un indirizzo e-mail per ricevere il codice di sicurezza.

Fase 3: Fare clic su “**Avanti**” (Next).

Si aprirà la schermata **Verifica automatica** (Auto Check). Osservare la Figura 4-2

Figura 4-2 Test automatico



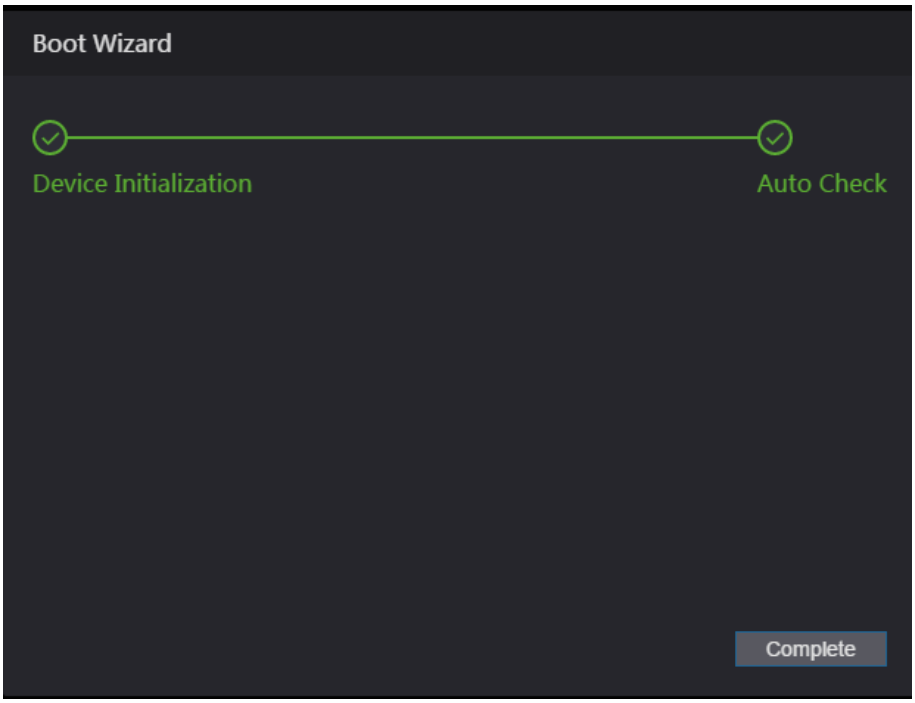
Fase 4: Qui è possibile decidere se selezionare o meno la **verifica automatica** (Auto Check).

Si consiglia di selezionare **Verifica automatica** (Auto Check) per ricevere gli aggiornamenti più recenti quando diventano disponibili.

Fase 5: Fare clic su “Avanti” (Next).

La configurazione è completata. Osservare la Figura 4-3

Figura 4-3 Configurazione completata



Fase 6: Fare clic su **Completa** (Complete) per completare l'inizializzazione.

Si aprirà la schermata di accesso amministratore.

4.2 Accesso

Fase 1: Aprire il Web browser IE e digitare l'indirizzo IP del controller di accesso nella barra degli indirizzi, quindi premere **Invia** (Enter).

Figura 4-4 Accesso

Fase 4: Inserire il nome utente e la password.

- Il nome amministratore predefinito è admin, mentre la password è la password di accesso dopo l'inizializzazione del controller di accesso. Modificare regolarmente la password amministratore e conservarla in modo appropriato per garantire la sicurezza.
- Se si dimentica la password di accesso dell'amministratore, fare clic su **Password dimenticata?** (Forgot password?) per reimpostarla. Fare riferimento alla sezione 4.3 Reimpostazione della password.

Fase 3: Fare clic su **Accedi** (Login).

Ora l'utente ha effettuato l'accesso all'interfaccia web.

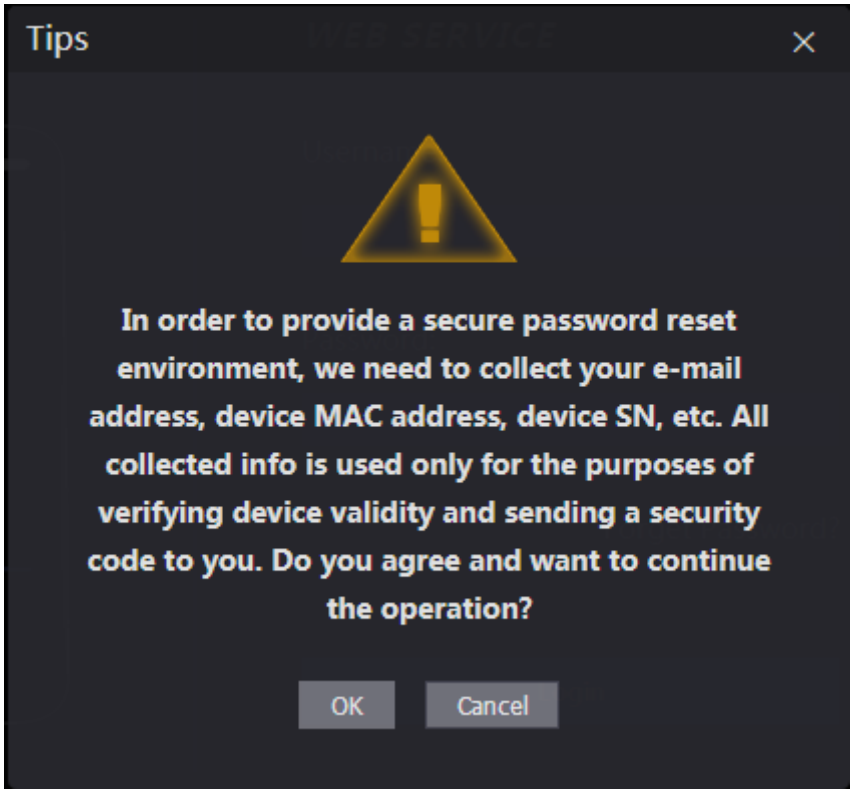
4.3 Reimpostazione della password

Per reimpostare la password dell'account amministratore occorre l'indirizzo e-mail dell'utente.

Fase 1: Fare clic su **Password dimenticata?** (Forgot password?) nella schermata di accesso.

Si aprirà la schermata **Suggerimenti** (Tips).

Figura 4-5 Suggerimenti

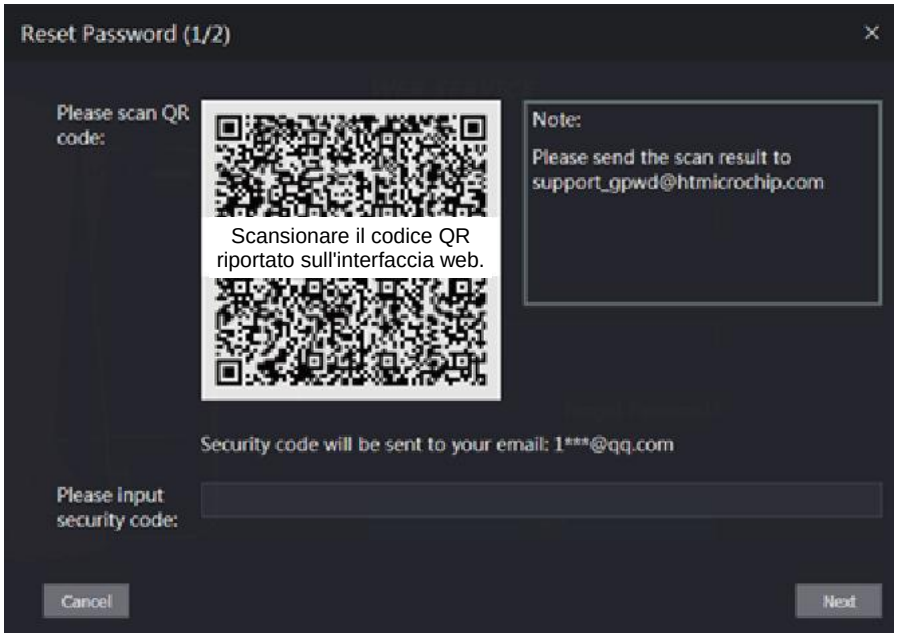


Fase 2: Leggere i suggerimenti.

Fase 3: Fare clic su OK.

Si aprirà la schermata di **reimpostazione della password** (Reset Password).

Figura 4-6 Reimpostazione della password



Fase 4: Scansionare il codice QR riportato sulla schermata per ottenere il codice di sicurezza.

- È possibile ricevere fino a due codici di sicurezza mediante la scansione dello stesso codice QR. Se i codici di sicurezza non sono più validi, aggiornare il codice QR per ottenerne altri.

- È necessario inviare il contenuto ottenuto dopo aver scansionato il codice QR all'indirizzo e-mail designato per ottenere il codice di sicurezza.
- Utilizzare il codice di sicurezza entro 24 ore dal suo ricevimento. Trascorso questo intervallo di tempo, non sarà più valido.
- Se si inserisce un codice di sicurezza errato per cinque volte consecutive, l'amministratore sarà bloccato per cinque minuti.

Fase 5: Digitare il codice di sicurezza ricevuto.

Fase 6: Fare clic su “**Avanti**” (Next).

Si aprirà la schermata di **reimpostazione della password** (Reset Password).

Fase 7: Reimpostare la password e confermarla.

La password deve essere composta da 8-32 caratteri non spaziati e deve contenere almeno due tipi di caratteri tra maiuscole, minuscole, numeri e caratteri speciali (esclusi ' " ; : &).

Fase 8: Fare clic su **OK** per completare la reimpostazione.

4.4 Collegamento allarme

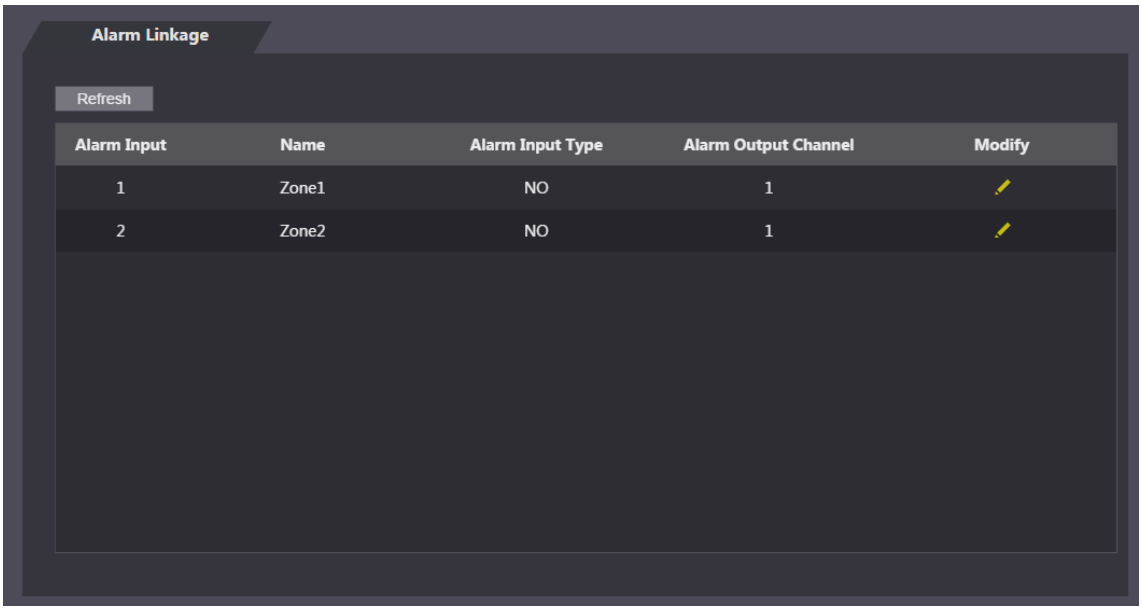
4.4.1 Impostazione del collegamento dell'allarme

I dispositivi di ingresso allarme possono essere collegati al controller di accesso; l'utente può modificare il parametro di collegamento dell'allarme in base alle proprie esigenze.

Fase 1: Selezionare **Collegamento allarme** (Alarm Linkage) sulla barra di navigazione.

Si aprirà la schermata di **collegamento dell'allarme** (Alarm Linkage). Osservare la Figura 4-7

Figura 4-7 Collegamento allarme



Fase 2: Fare clic su  per modificare i parametri del collegamento dell'allarme. Osservare la Figura 4-8

Figura 4-8 Modifica dei parametri del collegamento dell'allarme

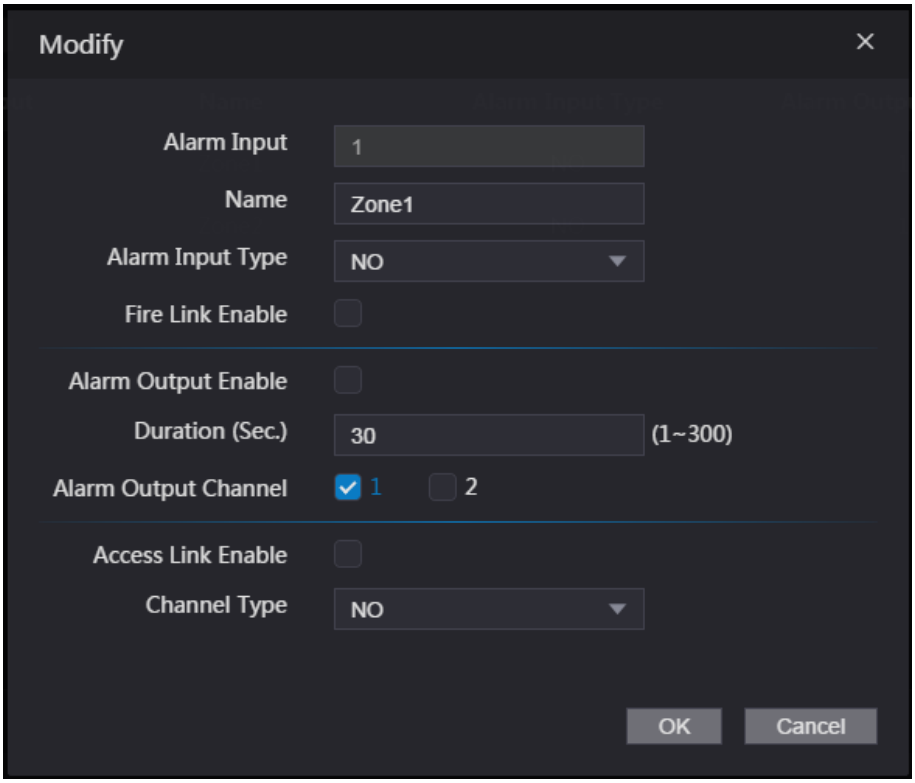


Tabella 4-1 Descrizione dei parametri del collegamento dell'allarme

Parametro	Descrizione
Ingresso allarme	Il valore non può essere modificato. Utilizzare il valore predefinito.
Nome	Inserire il nome di zona.
Tipi di ingresso allarme	Sono disponibili due opzioni: NA (NO) e NC. Selezionare Normalmente aperto (NA) se il tipo di ingresso di allarme del dispositivo di allarme acquistato è NA; altrimenti, selezionare NC.
Attiva collegamento antincendio	Se il collegamento antincendio è abilitato, il controller di accesso emette un allarme quando scatta l'allarme antincendio. I dettagli sull'allarme vengono visualizzati nel registri allarmi. L'uscita allarme e il collegamento accesso sono normalmente aperti per impostazione predefinita.
Attiva uscita allarme	Il relè può fornire in uscita le informazioni sugli allarmi (saranno inviate alla piattaforma di gestione) se l'**uscita di allarme** (Alarm Output) è abilitata.
Durata (in secondi)	Indica la durata dell'allarme (con un intervallo di 1-300 secondi).
Canale di uscita allarme	L'utente può selezionare un canale di uscita di allarme in base al dispositivo di allarme installato. Ciascun dispositivo di allarme può essere considerato con un canale.
Attiva collegamento accesso	Dopo aver abilitato il Collegamento Accesso (Access Link), il controller di accesso sarà normalmente aperto o normalmente chiuso quando ci sono segnali di allarme in ingresso.
Tipo di canale	Sono disponibili due opzioni: NA (NO) e NC.

Fase 3: Fare clic su **OK** per completare la configurazione.

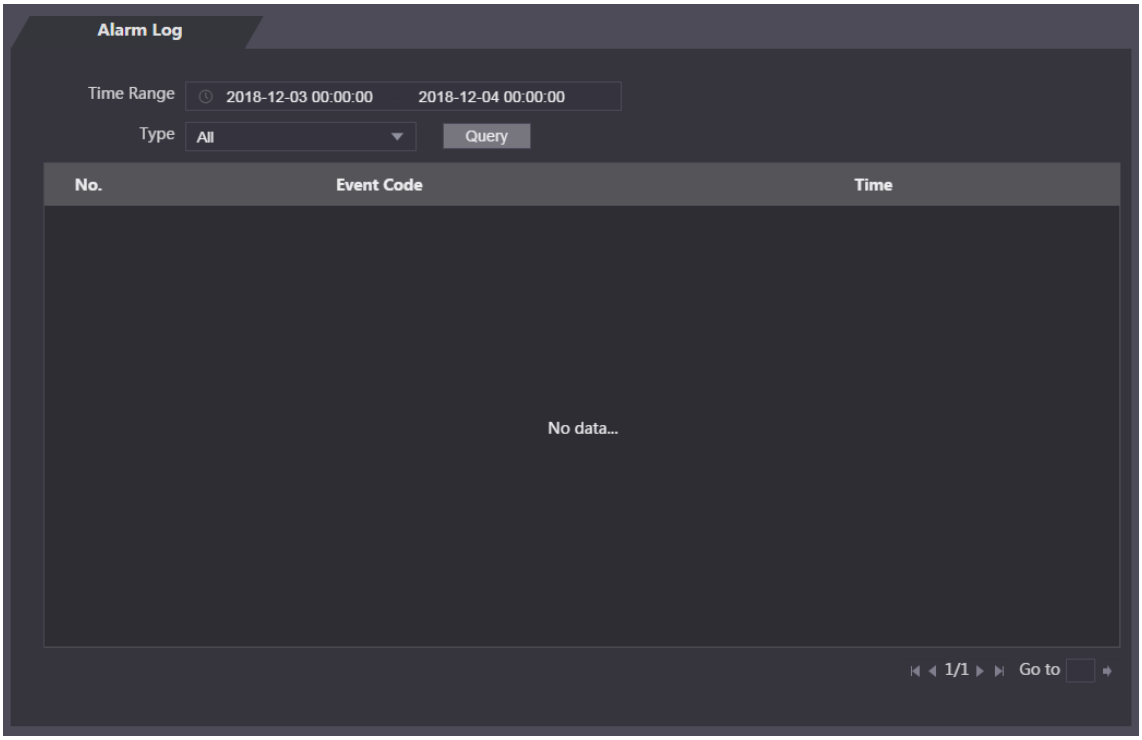
La configurazione sul web sarà sincronizzata con la configurazione sul client se il controller di accesso viene aggiunto ad un client.

4.4.2 Registro allarmi

Nella schermata del **registro degli allarmi** (Alarm Log) è possibile visualizzare il tipo di allarme e l'intervallo di tempo.

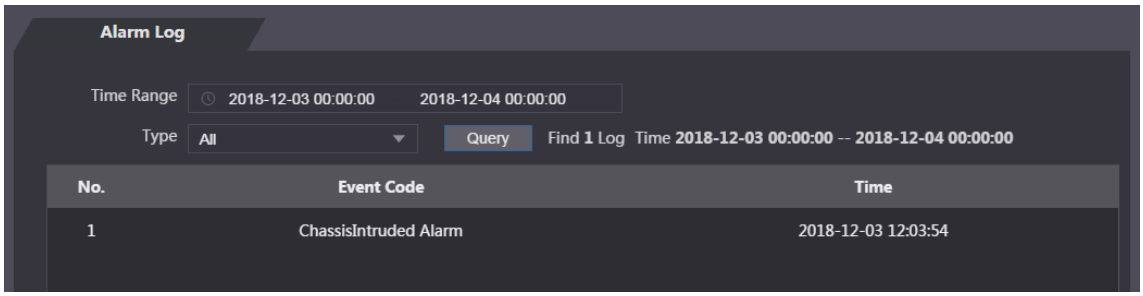
Fase 1: Selezionare **Collegamento allarme > Registri allarmi** (Alarm Linkage > Alarm Log). Si aprirà la schermata del **registri allarmi** (Alarm Log). Osservare la Figura 4-9

Figura 4-9 Registro allarmi



Fase 2: Selezionare un intervallo di tempo e un tipo di allarme, quindi fare clic su **Query**. Appariranno i risultati della query. Osservare la Figura 4-10

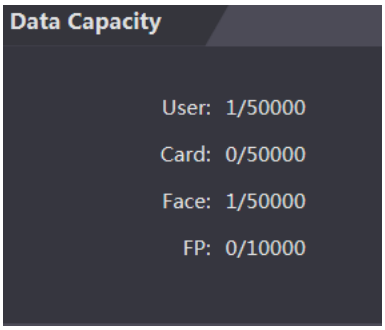
Figura 4-10 Risultati della query



4.5 Capacità dati

La schermata **Capacità Dati** (Data Capacity) mostra quanti utenti, schede, immagini di volti e impronte digitali il controller di accesso può contenere.

Figura 4-11 Capacità dati



4.6 Impostazioni video

La schermata **Impostazioni Video** (Video Setting) consente di impostare i parametri, tra cui la velocità dei dati, i parametri dell'immagine (luminosità, contrasto, tonalità, saturazione e altro ancora) e l'esposizione.

4.6.1 Velocità dati

Fare riferimento alla Tabella 4-2 per la descrizione della velocità dati.

Figura 4-12 Velocità dati

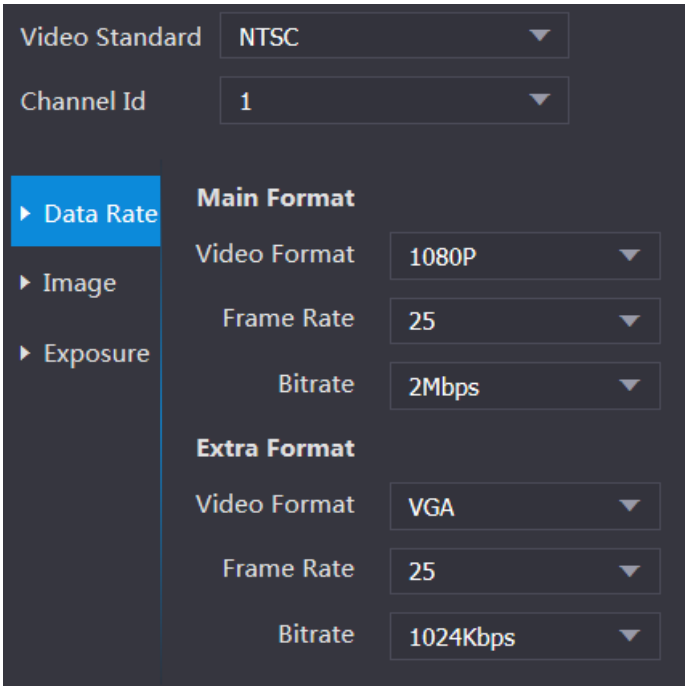


Tabella 4-2 Descrizione dei parametri della velocità dati

Parametro	Descrizione
Standard video	Sono disponibili due opzioni: NTSC e PAL. Selezionare uno standard a seconda dello standard video utilizzato nel proprio Paese.

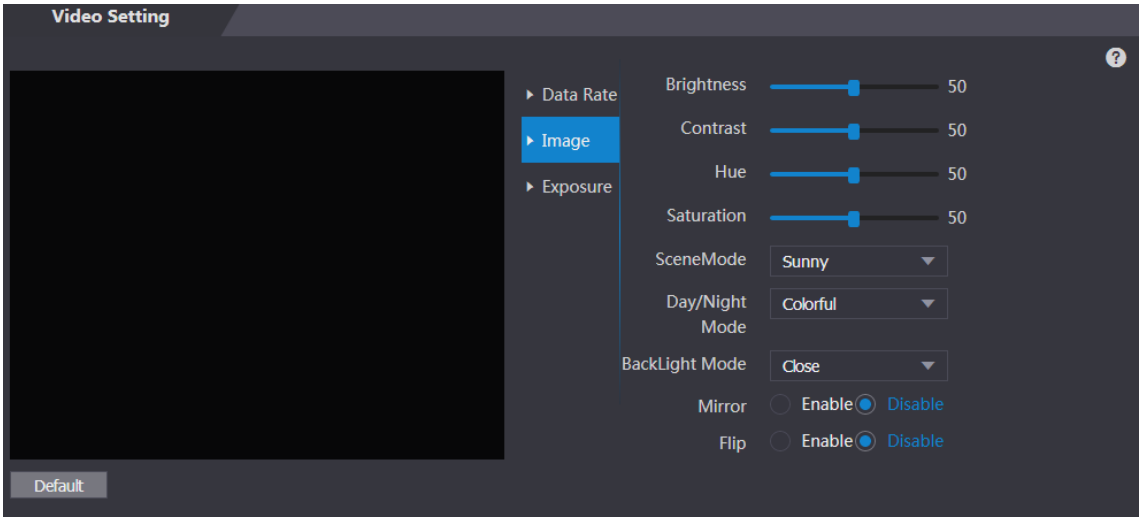
Parametro		Descrizione
Canale		Sono disponibili due opzioni: 1 e 2. 1 è la telecamera a luce bianca e 2 è la telecamera a infrarossi.
Formato principale	Formato video	Sono disponibili quattro opzioni: D1, VGA, 720p e 1080p. Selezionare un'opzione a seconda della qualità video desiderata.
	Frequenza fotogrammi	La velocità con cui fotogrammi consecutivi appaiono su un display. L'intervallo della frequenza fotogrammi è 1-25 fps.
	Velocità in bit	Il numero di bit che vengono trasportati o elaborati per unità di tempo. Sono disponibili cinque opzioni: 1,75 Mbps, 2 Mbps, 4 Mbps, 6 Mbps e 8 Mbps.
Formato extra	Formato video	Sono disponibili tre opzioni: D1, VGA e QVGA.
	Frequenza fotogrammi	La velocità con cui fotogrammi consecutivi appaiono su un display. L'intervallo della frequenza fotogrammi è 1-25 fps.
	Velocità in bit	Il numero di bit che vengono trasportati o elaborati per unità di tempo. Queste sono le opzioni: 256 Kbps, 320 Kbps, 384 Kbps, 448 Kbps, 512 Kbps, 640 Kbps, 768 Kbps, 896 Kbps, 1024 Kbps, 1,25 Mbps, 1,5 Mbps e 1,75 Mbps.

4.6.2 Immagine

Ci sono due canali e occorre configurare i parametri per ciascun canale.

Fase 1: Selezionare **Impostazioni Video > Impostazioni Video > Immagine** (Video Setting > Video Setting > Image).

Figura 4-13 Immagine



Fase 2: Alla voce Modalità retroilluminazione (Backlight Mode), selezionare Gamma dinamica estesa (Wide Dynamic).

Tabella 4-3 Descrizione dei parametri dell’immagine

Parametro	Descrizione
Luminosità	Quanto più grande è il valore, tanto più luminose saranno le immagini.
Contrasto	Il contrasto è la differenza di luminanza o di colore che rende un oggetto distinguibile. Quanto maggiore è il valore di contrasto, tanto maggiori saranno la luminosità e il contrasto del colore.
Tonalità	Quanto più grande è il valore, tanto più profondi saranno i colori.
Saturazione	Quanto più grande è il valore, tanto più luminosi saranno i colori.  Il valore non modifica la luminosità dell'immagine.
Modalità scena	● Chiuso: senza modalità. ● Automatica: il sistema regola automaticamente le modalità della scena. ● Soleggiato: in questa modalità, la tonalità dell'immagine viene ridotta. ● Notte: in questa modalità, la tonalità dell'immagine viene aumentata.  **Soleggiato** (Sunny) è selezionato per impostazione predefinita.
Modalità giorno/notte	La modalità giorno/notte determina lo stato operativo della luce di riempimento. ● Automatica: il sistema regola automaticamente le modalità giorno/notte. ● A colori: in questa modalità, le immagini sono a colori. ● Bianco e nero: in questa modalità, le immagini sono in bianco e nero.
Modalità controluce	● Chiuso: senza controluce. ● BLC: la compensazione del controluce corregge le regioni con livelli di luce estremamente alti o bassi, in modo da mantenere un livello di luce normale e utilizzabile per l'oggetto a fuoco. ● WDR: nella modalità ad ampia gamma dinamica, il sistema attenua le aree chiare e compensa le aree scure per garantire la definizione degli oggetti in entrambe le aree.  Quando i volti delle persone sono in controluce, occorre attivare la gamma dinamica ampia. ● HLC: la compensazione delle luminosità elevate è necessaria per compensare la sovraesposizione di luci intense o di forti sorgenti luminose come riflettori, fari, luci di veranda, ecc. per creare un'immagine utilizzabile e non sovraccaricata da una luce brillante.
Specchio	Quando la funzione è abilitata, le immagini vengono visualizzate con i lati destro e sinistro invertiti.
Capovolgimento	Quando questa funzione è abilitata, i video possono essere capovolti.

4.6.3 Esposizione

Fare riferimento alla Tabella 4-4 per la descrizione dei parametri dell'esposizione.

Tabella 4-4 Descrizione dei parametri dell'esposizione

Parametro	Descrizione
Anti-sfarfallio	● 50 Hz: Quando la frequenza di esercizio della corrente alternata è di 50 Hz, l'esposizione viene regolata automaticamente per garantire che non ci siano strisce sulle immagini. ● 60 Hz: Quando la frequenza di esercizio della corrente alternata è di 60 Hz, l'esposizione viene regolata automaticamente per garantire che non ci siano strisce sulle immagini. ● Esterni: selezionando **Esterni** (Outdoor), è possibile commutare la modalità di esposizione.
Modalità di esposizione	 ● Selezionando **Esterni** (Outdoor) nell'elenco a discesa Anti sfarfallio (Anti-flicker), è possibile selezionare **Priorità otturatore** (Shutter Priority) come modalità di esposizione. ● Le modalità di esposizione dei diversi dispositivi possono variare e prevarrà il prodotto effettivamente utilizzato. L'utente può selezionare: ● Automatica: il controller di accesso regola automaticamente la luminosità delle immagini. ● Priorità otturatore: Il controller di accesso regola la luminosità dell'immagine in base alla gamma di valori 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 di guadagno per ottenere la luminosità ideale. ● Manuale: l'utente può configurare manualmente il guadagno e il valore dell'otturatore per regolare la luminosità dell'immagine.
Otturatore	Quanto maggiore è il valore dell'otturatore e quanto più breve è il tempo di esposizione, tanto più scure saranno le immagini.
Intervallo dei valori dell'otturatore	Se si seleziona **Intervallo personalizzato** (Customized Range), è possibile personalizzare l'intervallo dei valori dell'otturatore.
Intervallo dei valori del guadagno	La qualità video risulterà migliore tramite l'impostazione dell'intervallo dei valori del guadagno.
Compensazione dell'esposizione	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 livello di rumore video può essere ridotto e verranno prodotti video ad alta definizione.
Grado	Se l'opzione 3D NR è attiva, l'utente può regolare il valore della riduzione del rumore 3D. Quanto maggiore è il valore, tanto minore sarà il rumore.

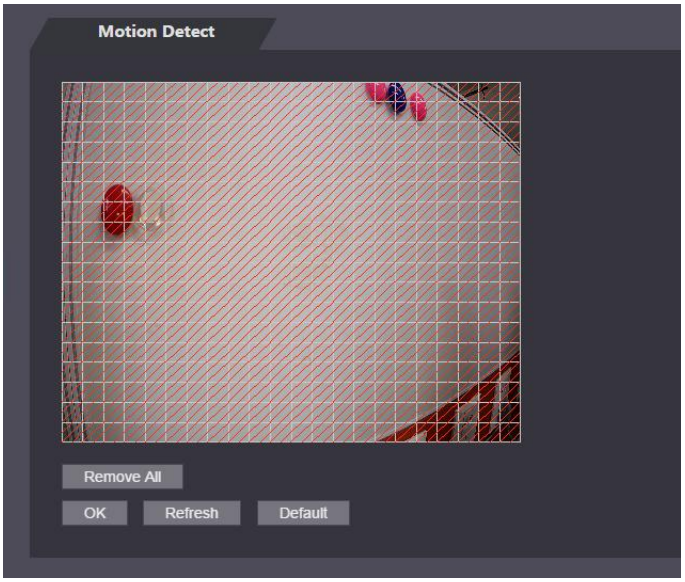
4.6.4 Rilevamento dei movimenti

Qui è possibile Impostare un intervallo entro il quale gli oggetti in movimento possono essere rilevati.

Fase 1: Selezionare **Impostazioni Video > Impostazioni Video > Rilevamento del movimento** (Video Setting > Video Setting > Motion Detection).

Si aprirà la schermata **Rilevamento del movimento** (Motion Detection). Osservare la Figura 4-14

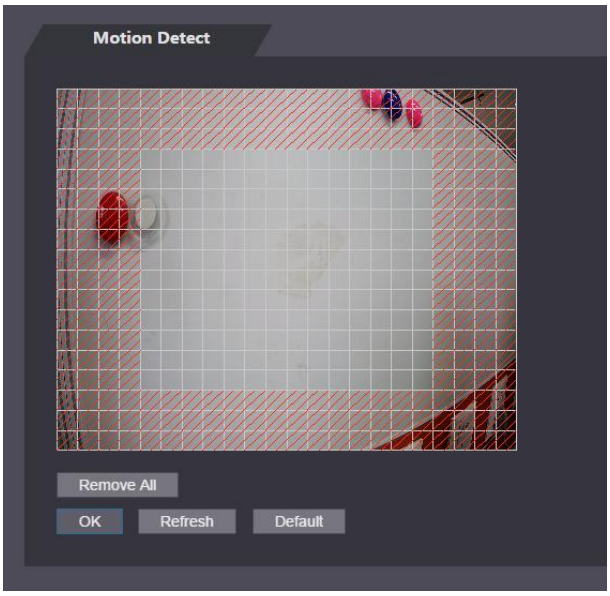
Figura 4-14 Rilevamento dei movimenti



Fase 2: Tenere premuto il tasto sinistro del mouse e trascinare il mouse nell'area rossa. Verrà visualizzata l'area di rilevamento del movimento. Osservare la Figura 4-15

- I quadratini rossi indicano l'area di rilevamento del movimento. L'insieme dei quadratini rossi corrisponde a tutto l'intervallo di rilevamento del movimento predefinito.
- Per disegnare un'area di rilevamento del movimento occorre prima fare clic su **Elimina tutti** (Remove All).
- L'area di rilevamento del movimento disegnata sarà un'area di non rilevamento del movimento se si disegna nell'area predefinita.

Figura 4-15 Area di rilevamento del movimento

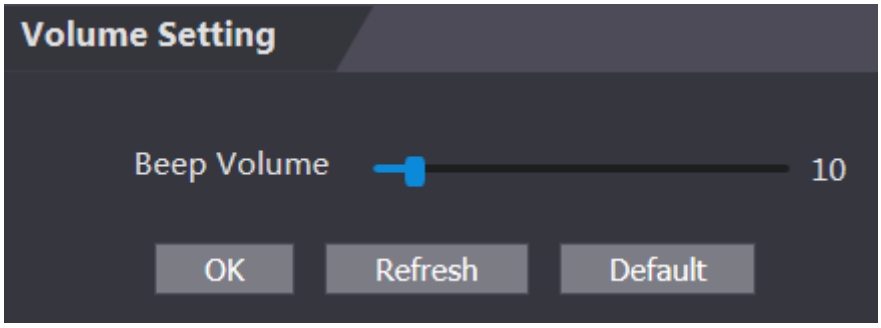


Fase 3: Fare clic su **OK** per completare l'impostazione.

4.6.5 Impostazione del volume

Qui è possibile regolare il volume dello speaker del controller di accesso.

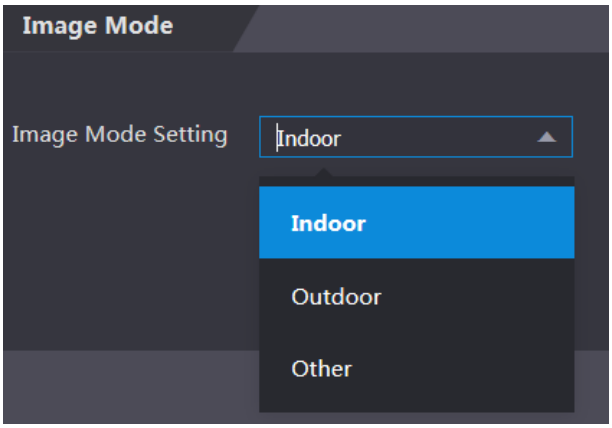
Figura 4-16 Impostazione del volume



4.6.6 Modalità immagine

Sono disponibili tre opzioni: interni, esterni e altro. Selezionare **Interni** (Indoor) quando il controller di accesso è installato in ambienti interni; selezionare **Esterni** (Outdoor) quando il controller di accesso è installato in ambienti esterni; e selezionare **Altro** (Other) quando il controller di accesso è installato in luoghi con controluce come corridoi e androni.

Figura 4-17 Modalità immagine



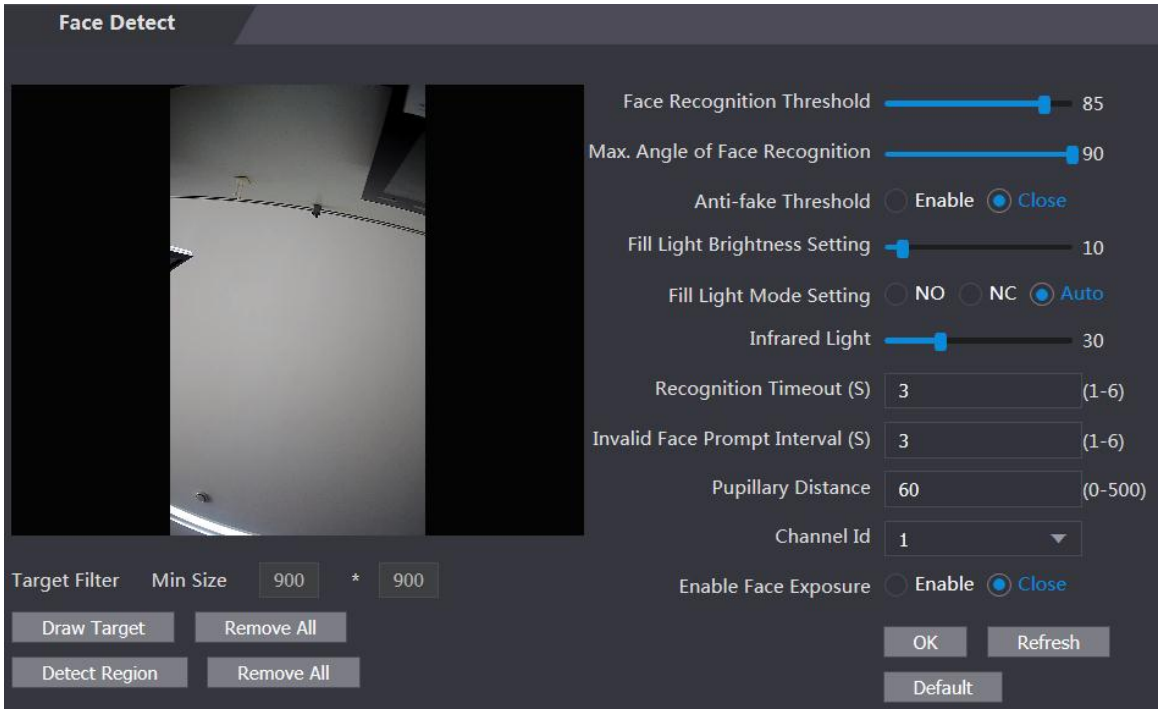
4.7 Rilevamento volto

Su questa schermata è possibile configurare i parametri relativi al volto umano per aumentare la precisione del riconoscimento dei volti.

Fase 1: Selezionare **Rilevamento volto** (Face Detect).

Si aprirà la schermata **Rilevamento volto** (Face Detect). Osservare la Figura 4-18

Figura 4-18 Rilevamento volto



Fase 2: Configura i parametri. Osservare la Tabella 4-5

Tabella 4-5 Descrizione dei parametri del rilevamento volto

Parametro	Descrizione
Soglia di riconoscimento volti	Più alto è il valore, più elevata sarà la precisione.
Angolo max. di riconoscimento volti	Più grande è l'angolo, più ampia è la gamma di profili che verrà riconosciuta.
Soglia anti-falsificazione	Sono disponibili due opzioni: **Abilita** (Enable) e **Chiudi** (Close).
Impostazioni di luminosità della luce di riempimento	Qui è possibile impostare la luminosità della luce di riempimento.
Impostazioni della modalità luce di riempimento	Ci sono tre modalità di luce di riempimento. ● NA: la luce di riempimento è normalmente accesa. ● NC: la luce di riempimento è normalmente spenta. ● Automatica: la luce di riempimento si accende automaticamente quando viene attivato un evento di rilevamento di movimenti. Selezionando **Auto**, la luce di riempimento non si accende neanche se il valore della luce a infrarossi è maggiore di 19.
Luce a infrarossi	Trascinando la barra di scorrimento è possibile regolare la luminosità della luce a infrarossi.
Timeout riconoscimento	Quando una persona che non possiede l'autorizzazione all'accesso si trova di fronte al controller di accesso per il riconoscimento del volto, il controller segnalerà che il riconoscimento non è riuscito. L'intervallo fino alla segnalazione è chiamato timeout di riconoscimento.

Parametro	Descrizione
Intervallo di segnalazione volto non valido	Quando una persona priva di autorizzazione si trova di fronte al controller di accesso, il controller segnalerà che il volto non è valido. L'intervallo fino alla segnalazione è chiamato intervallo di segnalazione di volto non valido.
Distanza pupille	La distanza pupillare è il valore in pixel dell'immagine tra il centro delle pupille di ciascun occhio. Occorre impostare un valore appropriato in modo che il controller di accesso possa riconoscere i volti. Il valore cambia a seconda delle dimensioni del volto e della distanza tra i volti e l'obiettivo. Più il volto è vicino all'obiettivo, maggiore deve essere il valore. Se un adulto si trova a 1,5 metri di distanza dall'obiettivo, il valore della distanza pupillare può essere compreso tra 50 e 70.
Abilita esposizione volti	Dopo aver abilitato l'esposizione del volto, i volti saranno più chiari se il controller di accesso è installato all'esterno.
ID canale	Sono disponibili due opzioni: 1 e 2. 1 è la telecamera a luce bianca e 2 è la telecamera a infrarossi.
Disegna target	Fare clic su **Disegna target** (Draw Target) per definire la cornice minima di rilevamento volti. Fare clic su **Elimina tutti** (Remove All) per eliminare tutte le cornici precedentemente disegnate.
Rilevamento regione	Fare clic su **Rilevamento area** (Detect Region) e trascinare il mouse per regolare l'area di rilevamento volti. Fare clic su **Elimina tutti** (Remove All) per eliminare tutte le aree di rilevamento.

Fase 3: Fare clic su **OK** per completare l'impostazione.

4.8 Impostazioni di rete

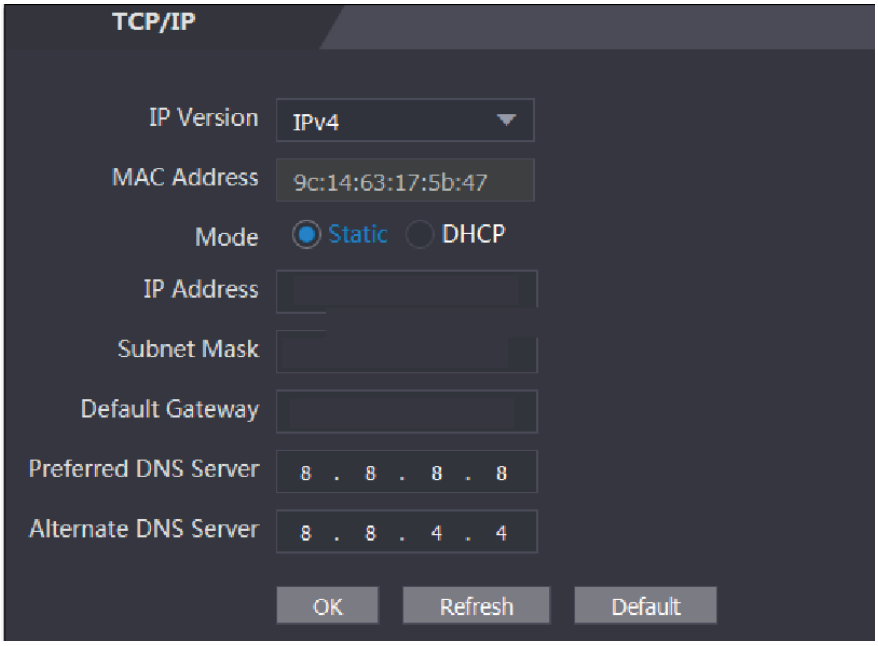
4.8.1 TCP/IP

È necessario configurare l'indirizzo IP e il server DNS affinché il controller di accesso comunichi con altri dispositivi.

Prerequisito

Assicurarsi che il controller di accesso sia collegato correttamente alla rete.
Fase 1: Selezionare **Impostazioni di rete > TCP/IP** (Network Setting > TCP/IP).

Figura 4-19 TCP/IP



Fase 2: Configura i parametri.

Tabella 4-6 TCP/IP

Parametro	Descrizione
Versione IP	Sono disponibili due opzioni: IPv4.
Indirizzo MAC	Viene visualizzato l'indirizzo MAC del controller di accesso.
Modalità	● Statico Qui è possibile configurare manualmente l'indirizzo IP, la subnet mask e l'indirizzo del gateway. ● DHCP ◇ Dopo aver abilitato il protocollo DHCP, non sarà possibile configurare l'indirizzo IP, la subnet mask e l'indirizzo del gateway. ◇ Se il DHCP è in uso, l'indirizzo IP, la subnet mask e l'indirizzo del gateway saranno visualizzati automaticamente; se il DHCP non è in uso, i suddetti parametri saranno tutti pari a zero. ◇ Per visualizzare l'indirizzo IP predefinito quando DHCP è in uso, occorre disattivare quest'ultimo.
Indirizzo link-local	L'indirizzo link-local è disponibile solo quando IPv6 è selezionato nella versione IP. Indirizzi link-local saranno assegnati al controller dell'interfaccia di rete in ogni rete locale per abilitare le comunicazioni. L'indirizzo link-local non può essere modificato.
Indirizzo IP Subnet mask Gateway predefinito	Digitare l'indirizzo IP, quindi configurare la subnet mask e l'indirizzo del gateway. L'indirizzo IP e l'indirizzo del gateway devono trovarsi nello stesso segmento di rete.
Server DNS preferito	Immettere qui l'indirizzo IP del server DNS preferito.
Server DNS alternativo	Immettere qui l'indirizzo IP del server DNS alternativo.

Fase 3: Fare clic su **OK** per completare l'impostazione.

4.8.2 Porta

Qui è possibile impostare il numero massimo di connessioni dei client a cui il controller di accesso può essere collegato e i numeri di porta.

Fase 1: Selezionare **Impostazioni di rete > Porta** (Network Setting > Port).

Si aprirà la schermata **Porta** (Port).

Fase 2: Configurare i numeri di porta. Fare riferimento alla tabella sottostante.

Ad eccezione del numero max. di connessioni, dopo aver modificato i valori è necessario riavviare il controller di accesso per rendere efficace la configurazione.

Tabella 4-7 Descrizione delle porte

Parametro	Descrizione
Connessione max	Qui è possibile impostare il numero massimo di connessioni dei client a cui il controller di accesso può essere collegato. I client di piattaforme come Smartpass non vengono conteggiati.
Porta TCP	Il valore predefinito è 37777.
Porta HTTP	Il valore predefinito è 80. Se come numero di porta viene utilizzato un altro valore, è necessario aggiungerlo dietro l'indirizzo quando si accede tramite browser.
Porta HTTPS	Il valore predefinito è 443.
Porta RTSP	Il valore predefinito è 554.

Fase 3: Fare clic su **OK** per completare l'impostazione.

4.8.2.2 Registrazione

Se connesso a una rete esterna, il controller di accesso comunicherà il suo indirizzo al server designato dall'utente, in modo che i client possano accedervi.

Fase 1: Selezionare **Impostazioni di rete > Registrazione automatica** (Network Setting > Auto Register).

Si aprirà la schermata di **Registrazione automatica** (Auto Register).

Fase 2: Selezionare **Abilita** (Enable), quindi immettere l'indirizzo IP dell'host, la porta e l'ID del dispositivo secondario.

Tabella 4-8 Descrizione della registrazione automatica

Parametro	Descrizione
IP host	Indirizzo IP o nome di dominio del server.
Porta	La porta del server utilizzata per la registrazione automatica.
ID dispositivo secondario	ID del controller di accesso assegnato dal server.

Fase 3: Fare clic su **OK** per completare l'impostazione.

4.8.3 P2P

Il peer-to-peer computing o networking è un'architettura applicativa distribuita che suddivide i compiti o i carichi di lavoro tra nodi paritari (peer). Gli utenti possono scaricare l'applicazione mobile scansionando il codice QR e poi registrare un account in modo che più di un controller di accesso possa essere gestito tramite l'applicazione mobile. Non occorre applicare un nome di dominio dinamico, effettuare la mappatura delle porte o non è necessario alcun server di transito.

Se si sceglie il P2P, è necessario collegare il controller di accesso alla rete esterna, altrimenti non sarà possibile utilizzarlo.

Figura 4-20 P2P

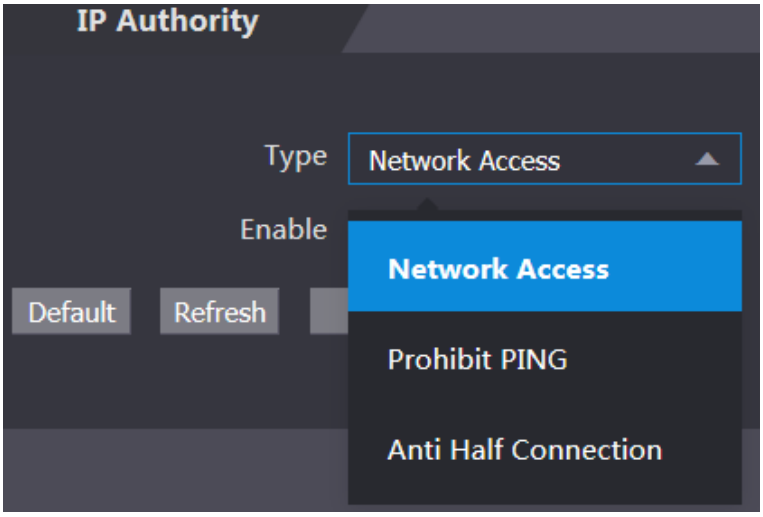
Fase 1: Selezionare **Impostazioni di rete > P2P** (Network Setting > P2P).
Si aprirà la schermata **P2P**.
Fase 2: Selezionare **Abilita** (Enable) per attivare la funzione P2P.
Fase 3: Fare clic su **OK** per completare l'impostazione.

Eseguire la scansione del codice QR sull'interfaccia web per ricevere il numero di serie del controller di accesso.

4.9 Gestione della sicurezza

4.9.1 Autorità IP

Figura 4-21 Autorità IP



Selezionare una modalità di sicurezza informatica in base alle proprie esigenze.

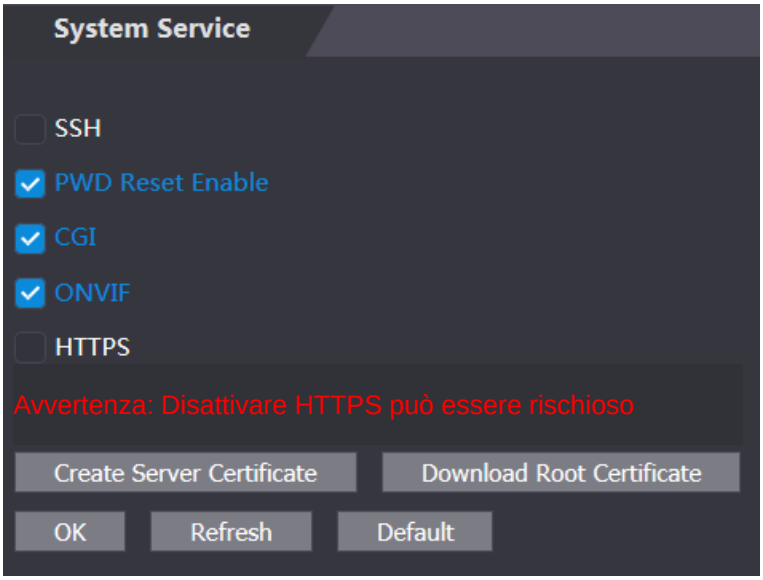
4.9.2 Sistemi

4.9.2.1 Servizio di sistema

Sono disponibili quattro opzioni: SSH, Abilita la reimpostazione della password, CGI e HTTPS. Fare riferimento al paragrafo "3.9.4 Funzionalità" per selezionare uno o più sistemi.

La configurazione del servizio di sistema effettuata sulla pagina web e la configurazione sull'interfaccia **Funzionalità** (Features) del controller di accesso saranno sincronizzate.

Figura 4-22 Servizio di sistema



4.9.2.2 Crea certificato del server

Fare clic su **Crea certificato del server** (Create Server Certificate), inserire le informazioni richieste, quindi fare clic su **Salva** (Save); il controller di accesso verrà riavviato.

4.9.2.3 Scarica certificato radice

Fase 1: Fare clic su **Scarica certificato radice** (Download Root Certificate).
Selezionare un percorso per salvare il certificato nella finestra di dialogo **Salva file** (Save File).
Fase 2: Fare doppio clic sul **certificato radice** (Root Certificate)scaricato per installarlo. Installare il certificato seguendo le istruzioni visualizzate.

4.9.3 Gestione utenti

Qui è possibile aggiungere ed eliminare utenti, modificare le password degli utenti e immettere un indirizzo e-mail per reimpostare una password dimenticata.

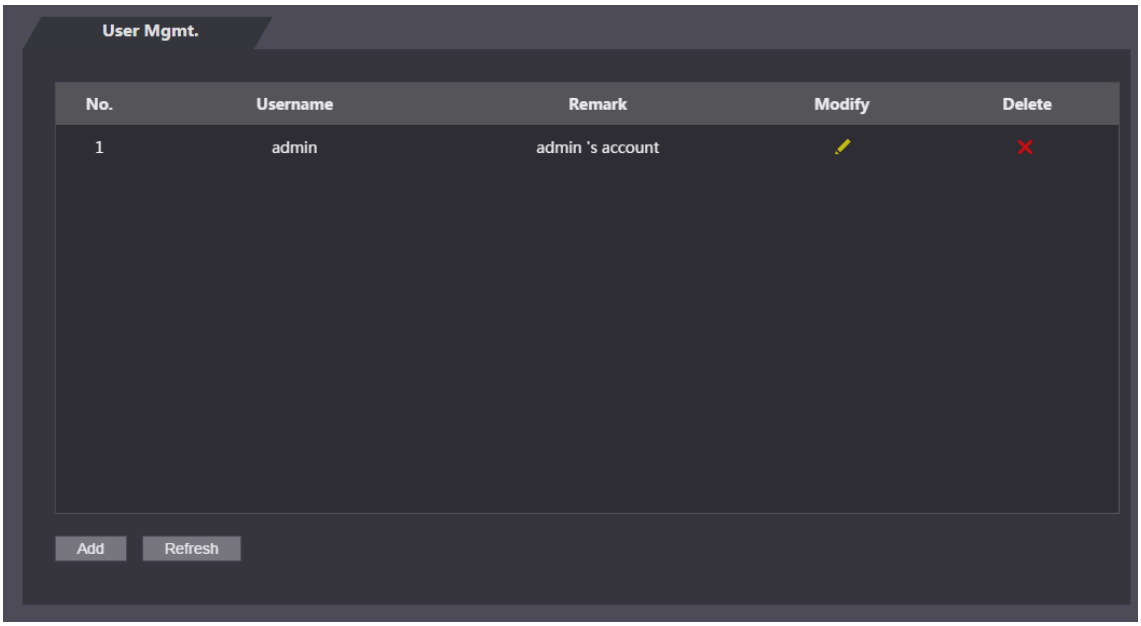
4.9.3.1 Aggiungi utenti

Per aggiungere un utente, fare clic su **Aggiungi** (Add) sulla schermata **Gestione utenti** (User Mgmt.), quindi immettere il nome utente, la password, la conferma della password e il commento. Fare clic su **OK** per completare l'aggiunta dell'utente.

4.9.3.2 Modifica delle informazioni sull'utente

Per modificare le informazioni sull'utente, fare clic su sulla schermata di **Gestione utenti** (User Mgmt.). Osservare la Figura 4-23

Figura 4-23 Gestione utenti

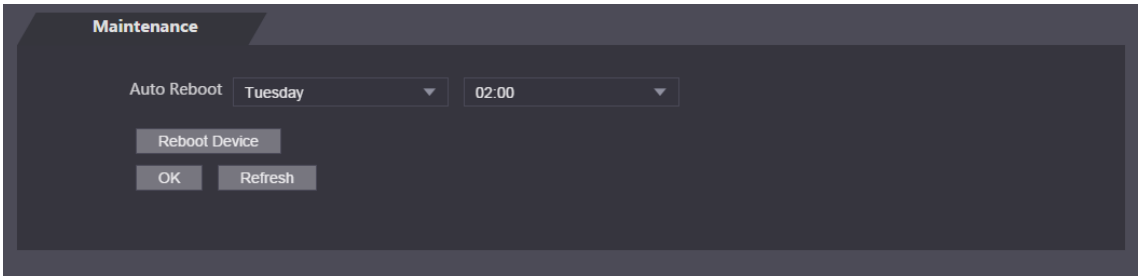


4.9.4 Manutenzione

È possibile fare in modo che il controller di accesso si riavvii da solo nel periodo di inattività per migliorarne la velocità di funzionamento. A tal fine occorre impostare la data e l'ora del riavvio automatico.

L'ora predefinita per il riavvio è alle 2 del mattino di martedì. Facendo clic su **Riavvia dispositivo** (Reboot Device), il controller di accesso si riavvia immediatamente. Fare clic su **OK**; il controller di accesso si riavvierà ogni martedì alle 2 del mattino. Fare riferimento alla Figura 4-24.

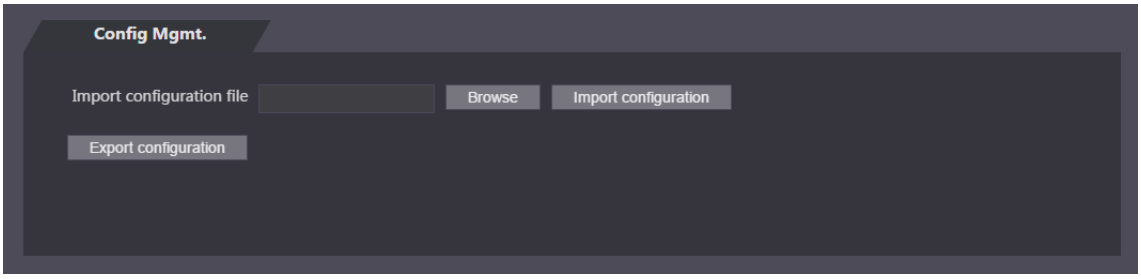
Figura 4-24 Manutenzione



4.9.5 Gestione della configurazione

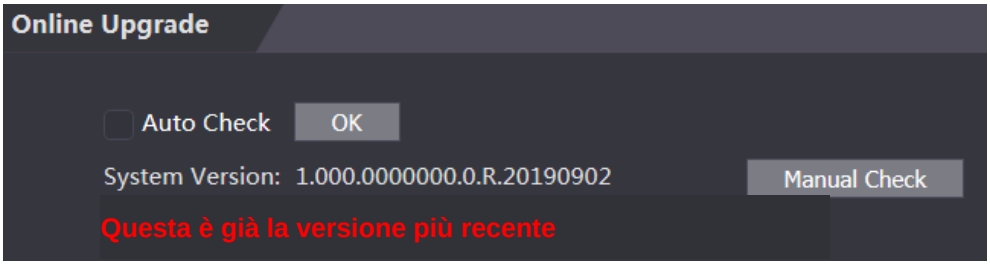
Quando occorre applicare la stessa configurazione a più di un controller di accesso, è possibile configurare i parametri importando o esportando i file di configurazione. Osservare la Figura 4-25

Figura 4-25 Gestione della configurazione



4.9.6 Aggiornamento

Selezionare **Verifica automatica** (Auto Check) per aggiornare automaticamente il sistema. Oppure selezionare **Verifica manuale** (Manual Check) per aggiornare manualmente il sistema.



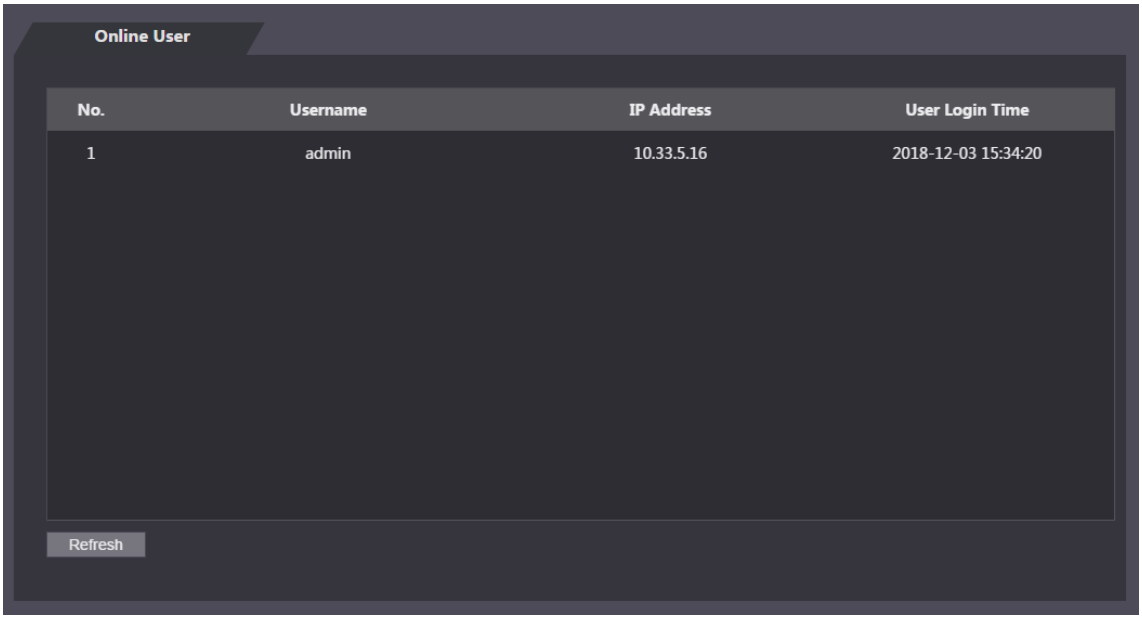
4.9.7 Informazioni sulla versione

È possibile visualizzare informazioni quali l'indirizzo MAC, il numero di serie, la versione MCU, la versione web, la versione della baseline di sicurezza e la versione del sistema.

4.9.8 Utente in linea

Sulla schermata **Utente in linea** (Online User) è possibile visualizzare il nome utente, l'indirizzo IP e l'ora di accesso dell'utente. Osservare la Figura 4-26

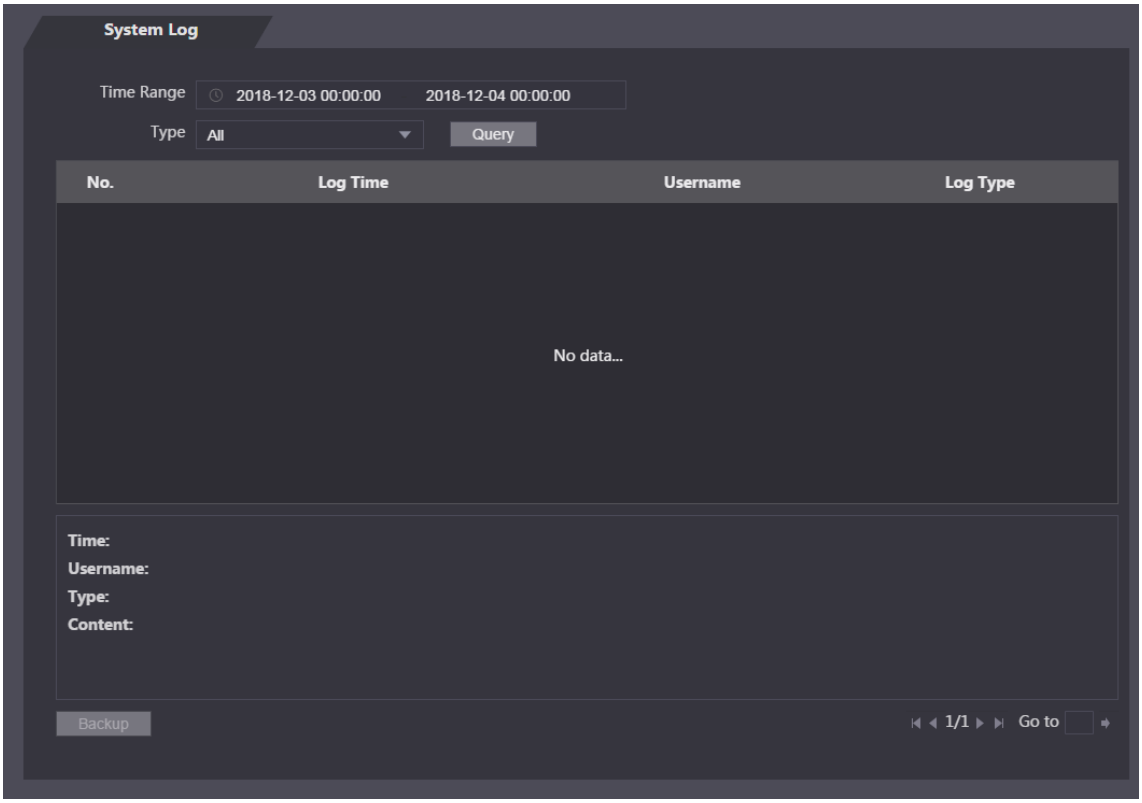
Figura 4-26 Utente in linea



4.10 Registro di sistema

Sulla schermata **Registro di sistema** (System Log) è possibile visualizzare il registro di sistema ed effettuarne il backup. Osservare la Figura 4-27

Figura 4-27 Registro di sistema



4.10.1 Registri di query

Selezionare un intervallo di tempo e il tipo, quindi fare clic su **Query** per visualizzare i registri che soddisfano i requisiti.

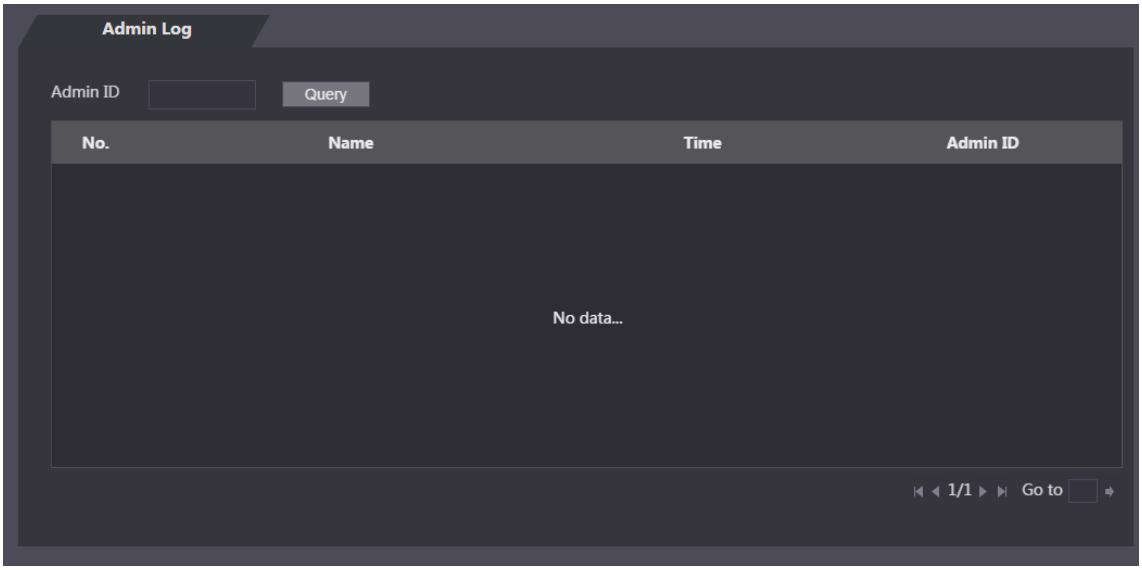
4.10.2 Backup dei registri

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

4.11 Registro amministratore

Inserire l'ID amministratore sull'interfaccia **Registro amministratore** (Admin Log), quindi fare clic su **Query** per visualizzare i record delle operazioni dell'amministratore. Osservare la Figura 4-28

Figura 4-28 Registro amministratore



Passare il cursore del mouse sopra per visualizzare le informazioni dettagliate sull'utente corrente.

4.12 Uscita

Fare clic su , quindi fare clic su **OK** per uscire dall'interfaccia web.

5 Configurazione Smart PSS

Il client Smart PSS consente di configurare le autorizzazioni di accesso a una singola porta o a gruppi di porte. Per maggiori informazioni sulla configurazione, fare riferimento al manuale dell'utente del client Smart PSS.

Le interfacce Smart PSS possono variare a seconda della versione e prevale l'interfaccia attuale.

5.1 Accesso

Installare il client Smart PSS (il nome utente predefinito è admin, la password predefinita è admin123), fare doppio clic su 

per avviarlo. Seguire le istruzioni per terminare l'inizializzazione e accedere.

5.2 Aggiunta dispositivi

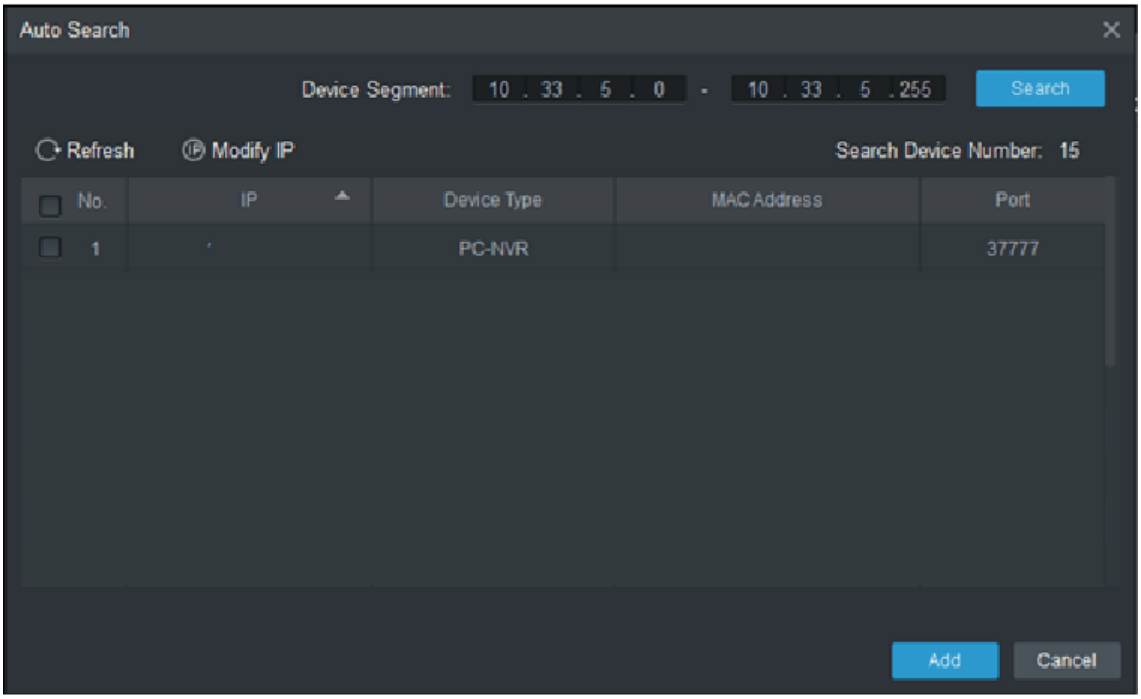
L'utente deve aggiungere controller di accesso allo Smart PSS. A tal fine, fare clic su **Ricerca automatica** (Auto Search), quindi fare clic su **Aggiungi** (Add) per aggiungere manualmente i dispositivi.

5.2.1 Ricerca automatica

L'opzione consente di cercare e aggiungere controller di accesso sullo stesso segmento di rete allo Smart PSS. Fare riferimento alla Figura 5-1 e alla Figura 5-2.

Figura 5-1 Dispositivi

Figura 5-2 Ricerca automatica



Fase 1: Fare clic su **Ricerca automatica** (Auto Search), digitare il segmento di rete, quindi fare clic su Cerca (Search). Verrà visualizzato un elenco di dispositivi.

Fase 2: Selezionare il controllo di accesso che si desidera aggiungere allo Smart PSS, quindi fare clic su Aggiungi (Add). Si aprirà la finestra di dialogo con le informazioni di accesso.

Fase 3: Immettere il nome utente e la password per accedere.

Nella schermata **Dispositivi** (Devices) sono visibili i controller di accesso aggiunti.

Selezionare un controller di accesso e fare clic su **Modifica IP** (Modify IP) per modificare l'indirizzo IP del controller. Per i dettagli su come modificare l'indirizzo IP, fare riferimento al manuale dell'utente dello Smart PSS.

5.2.2 Aggiunta manuale

È necessario conoscere gli indirizzi IP e i nomi di dominio dei controller di accesso che si desidera aggiungere. Fare riferimento alla Figura 5-3 e alla Figura 5-4.

Figura 5-3 Dispositivi

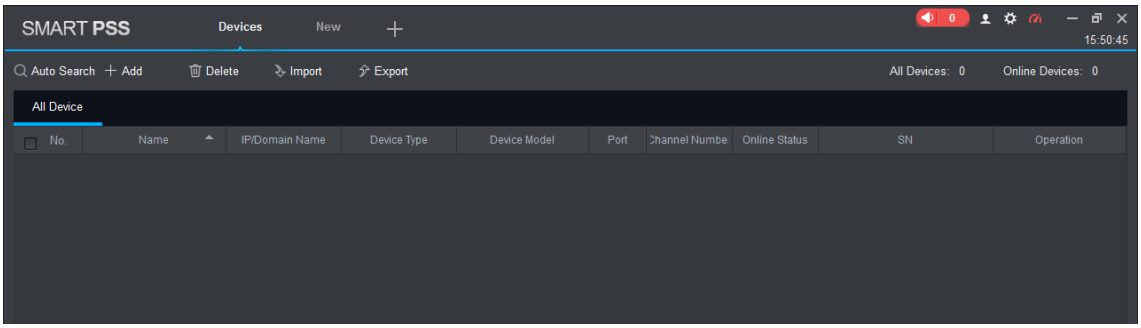
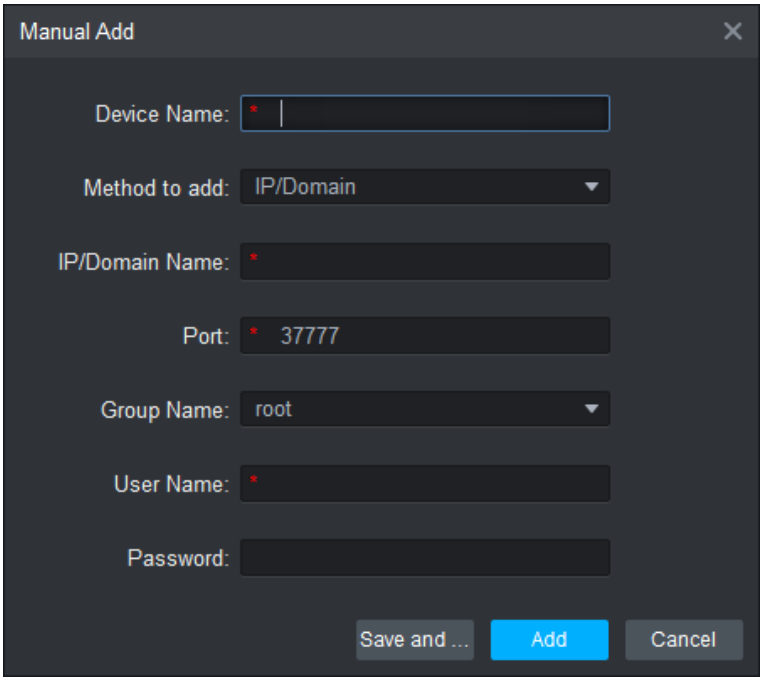


Figura 5-4 Aggiunta manuale



Fase 1: Fare clic su **Aggiungi** (Add) nella schermata dei dispositivi; si aprirà la schermata Aggiunta manuale (Manual Add).

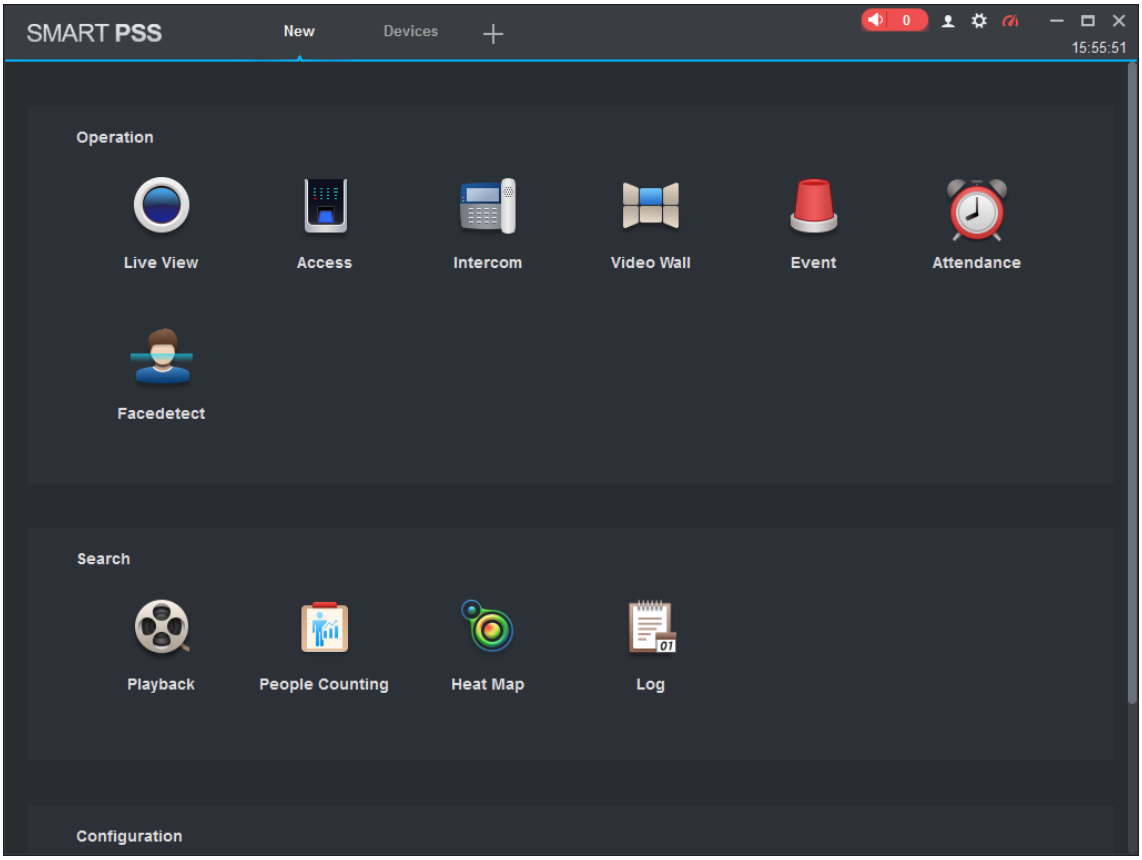
Fase 2: Immettere il nome del dispositivo, selezionare un metodo di aggiunta, immettere l'indirizzo IP/il nome di dominio, il numero di porta (37777 è l'impostazione predefinita), il nome del gruppo, il nome utente e la password.

Fase 3: Fare clic su **Aggiungi** (Add); il controller di accesso aggiunto è ora visibile nella schermata dei dispositivi.

5.3 Aggiungi utenti

Gli utenti sono associati a schede. Dopo aver aggiunti utenti allo Smart PSS, è possibile configurare le autorizzazioni di accesso degli utenti sulla schermata **Nuovo > Accesso** (New > Access). Osservare la Figura 5-5

Figura 5-5 Nuovo



5.3.1 Selezione del tipo di scheda

I tipi di scheda devono corrispondere a quelli dell'emittente della scheda, altrimenti non sarà possibile leggere il numero della scheda.

Sulla schermata **Accesso** (Access), fare clic su  , quindi fare clic sull'icona della scheda IC o ID, infine selezionare il tipo di scheda. Sono disponibili due opzioni: Scheda ID e scheda IC. Fare riferimento alla Figura 5-6 e alla Figura 5-7.

Figura 5-6 Accesso

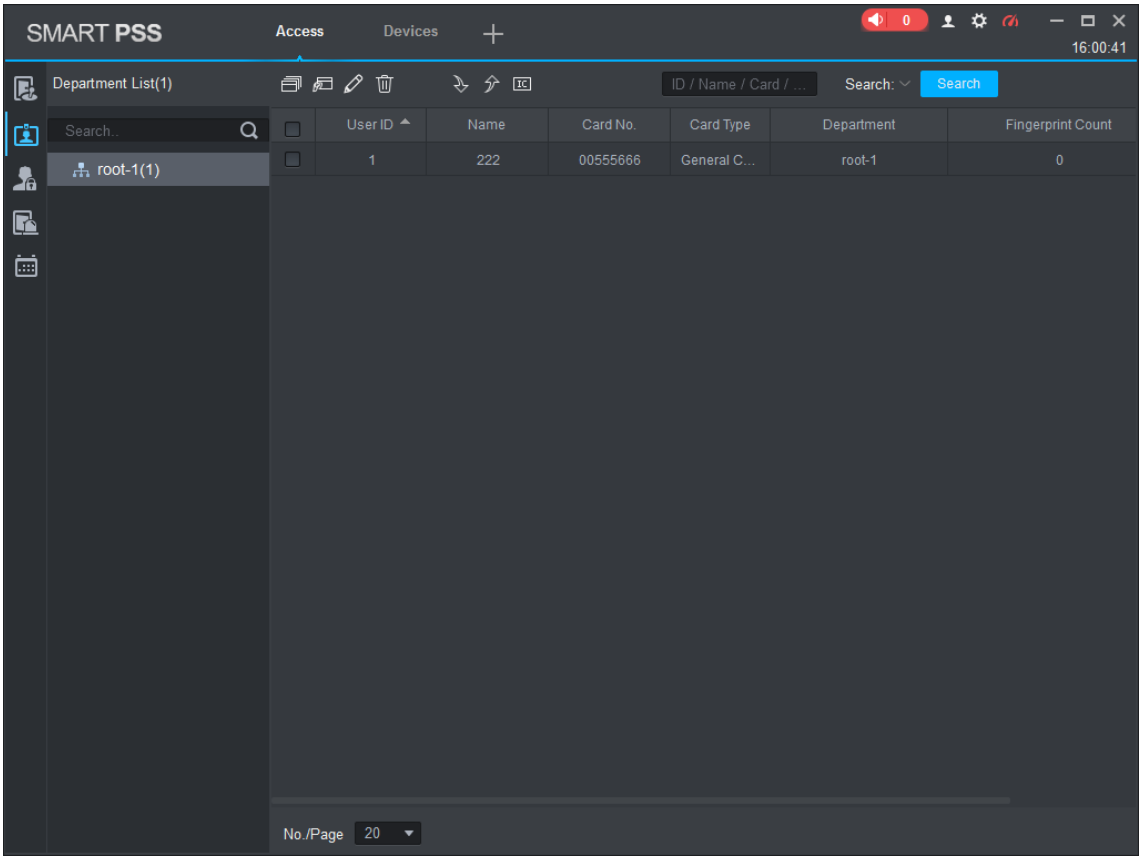
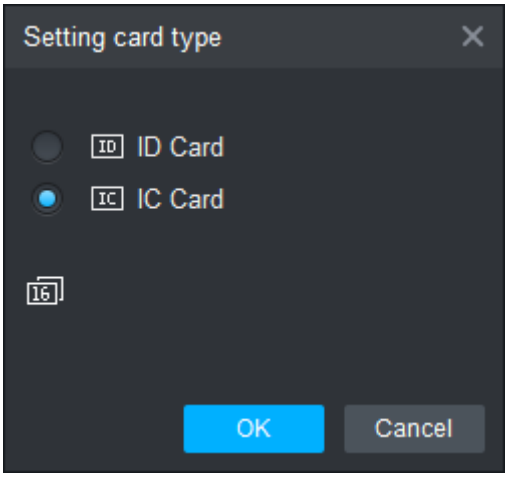


Figura 5-7 Impostazione del tipo di scheda



5.3.2 Aggiunta di un utente

È possibile aggiungere utenti uno per volta,

Sulla schermata **Accesso** (Access), fare clic su  , quindi fare clic su  e immettere le informazioni sull'utente. Fare clic su **Fine** (Finish) per completare l'aggiunta dell'utente. Fare riferimento alla Figura 5-8 e alla Figura 5-9.

Figura 5-8 Accesso

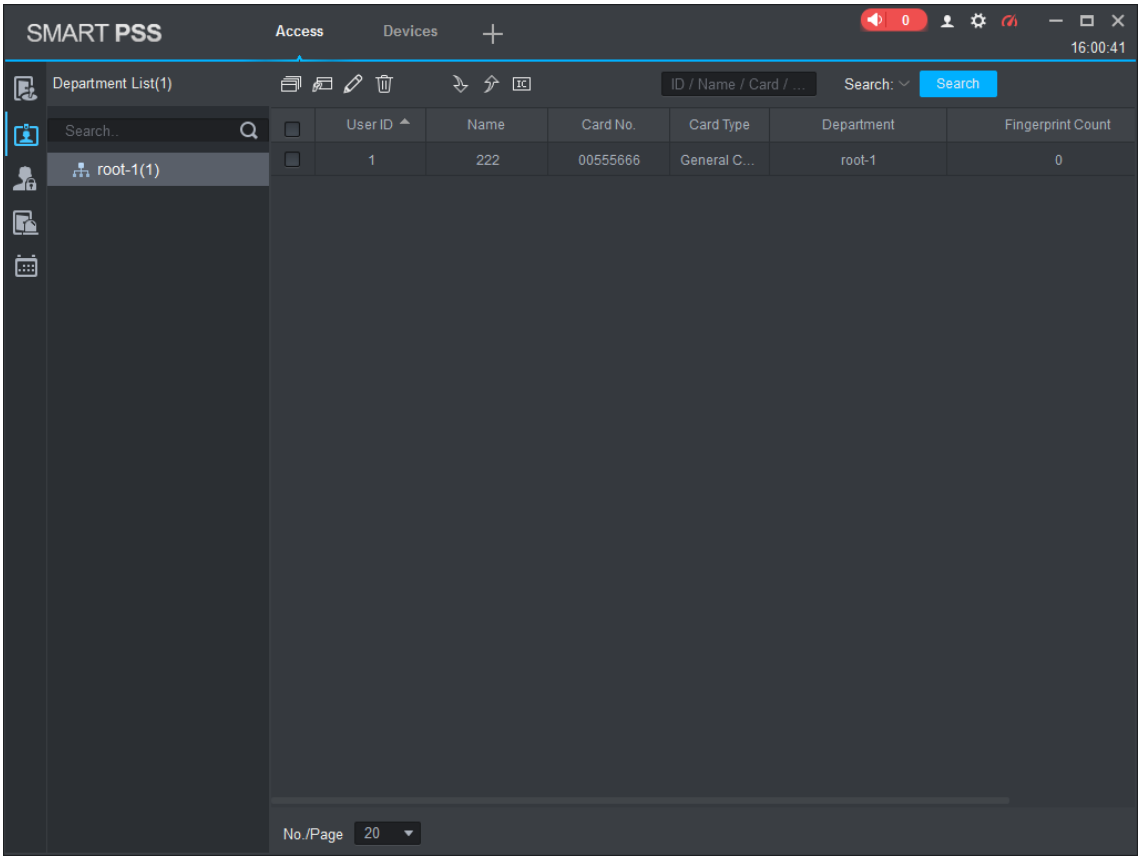
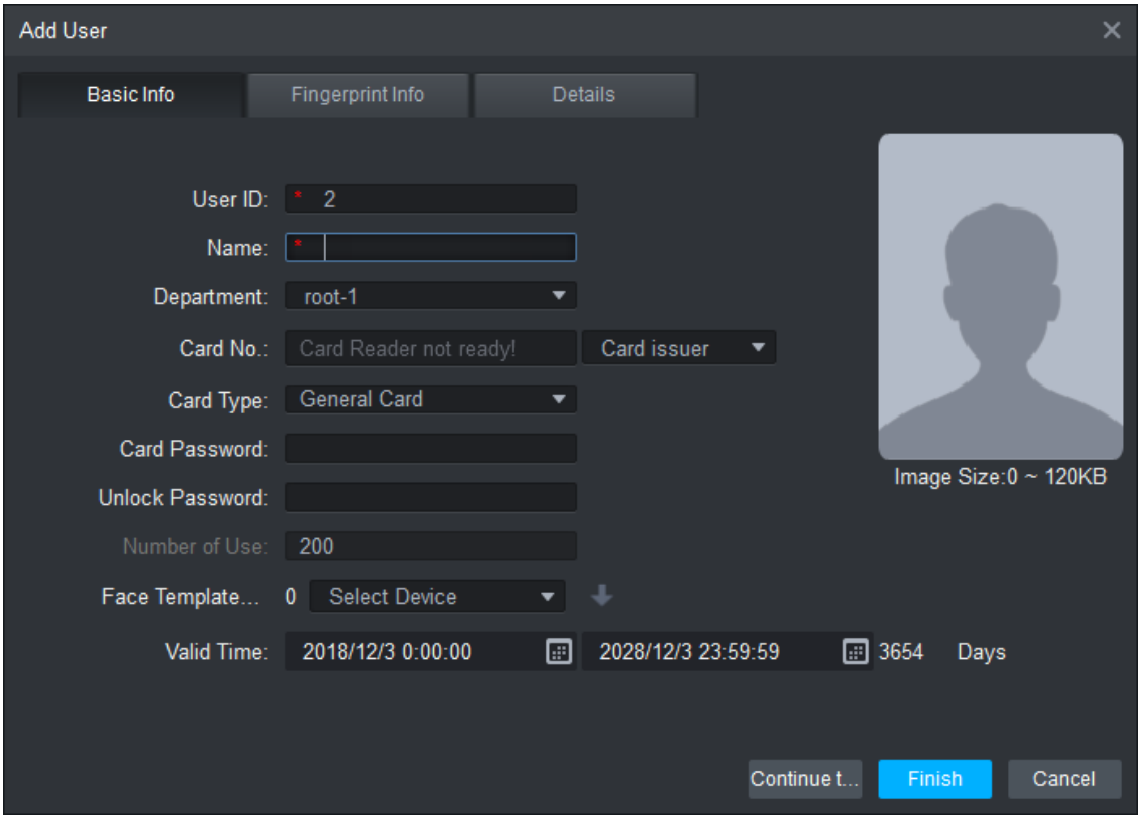


Figura 5-9 Aggiungi utente



5.4 Aggiunta di gruppo porta

È possibile gestire le porte unendole in gruppi.

Nella schermata **Accesso** (Access), fare clic su  , poi fare clic su **Aggiungi** (Add), immettere un nome di gruppo porte, infine selezionare un fuso orario. Fare clic su **Fine** (Finish) per completare l'aggiunta dell'utente. Fare riferimento alla Figura 5-10 e alla Figura 5-11.

Figura 5-10 Accesso

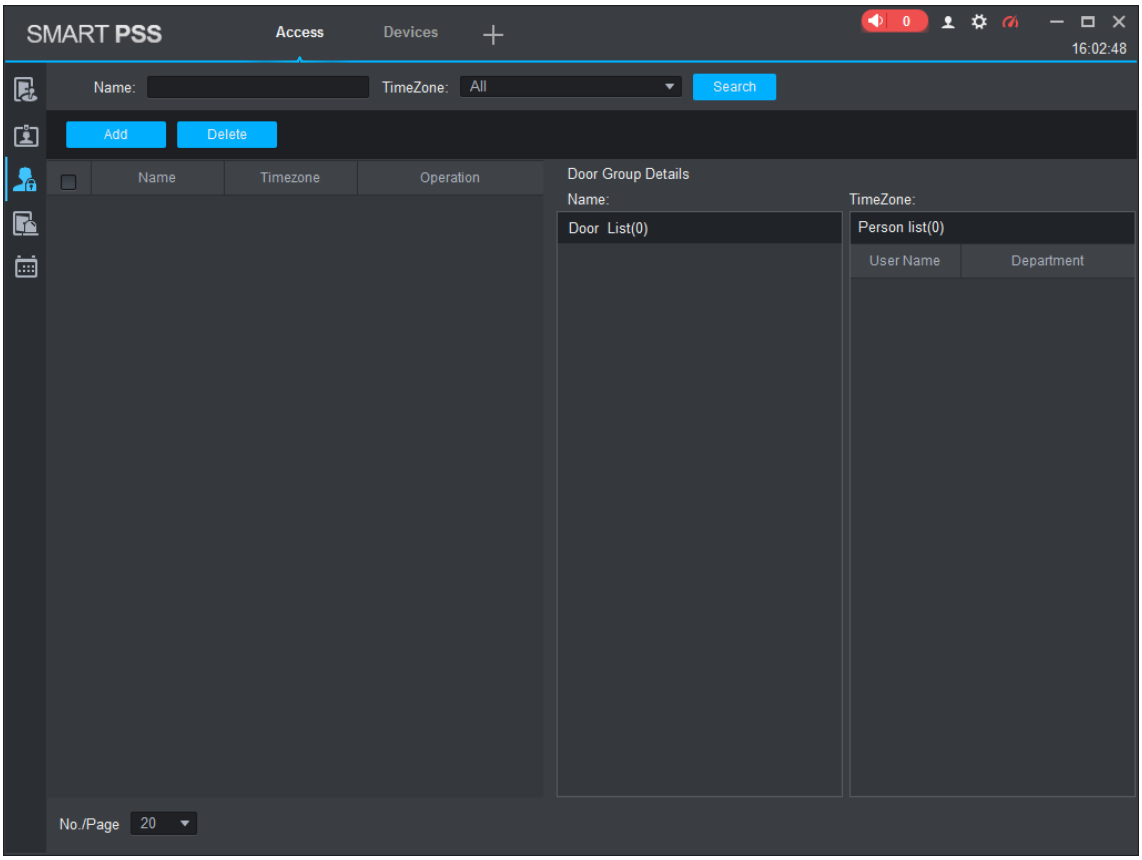
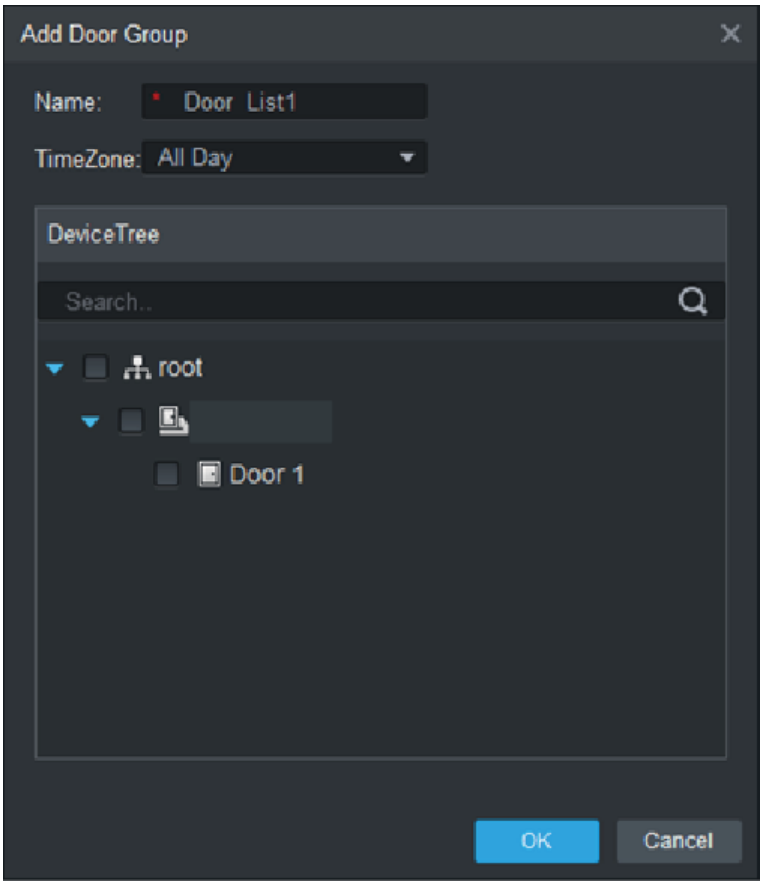


Figura 5-11 Aggiungi gruppo porte



5.5 Configurazione delle autorizzazioni di accesso

L'opzione consente di configurare le autorizzazioni di accesso. Sono disponibili due opzioni: autorizzazione di accesso gruppo porte e autorizzazioni di accesso utente. Le informazioni degli utenti a cui è stata data l'autorizzazione all'accesso nello Smart PSS e nei controller di accesso saranno sincronizzate.

5.5.1 Concessione dell'autorizzazione per gruppo di porte

Selezionare un gruppo di porte e aggiungere utenti all'elenco delle porte. In questo modo, gli utenti aggiunti ottengono le autorizzazioni all'accesso per tutte le porte dell'elenco. Fare riferimento alla Figura 5-12 e alla Figura 5-13.

Figura 5-12 Accesso

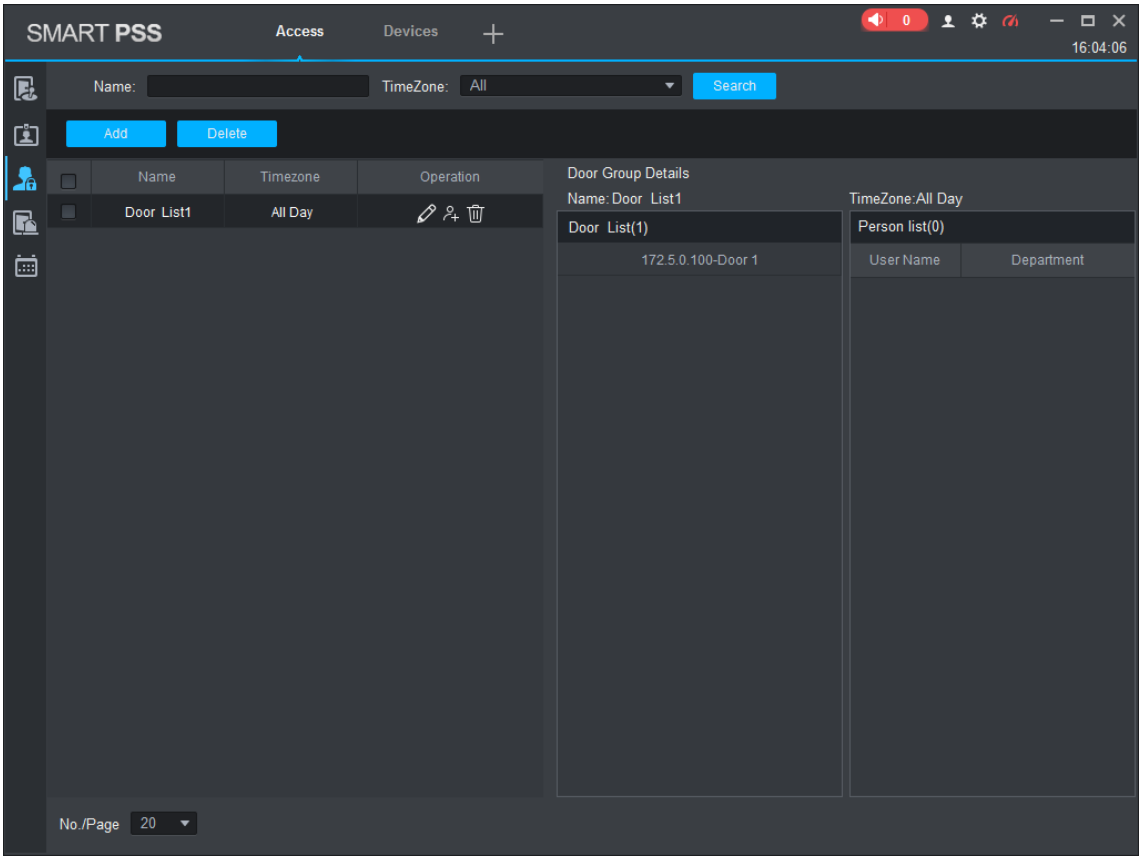
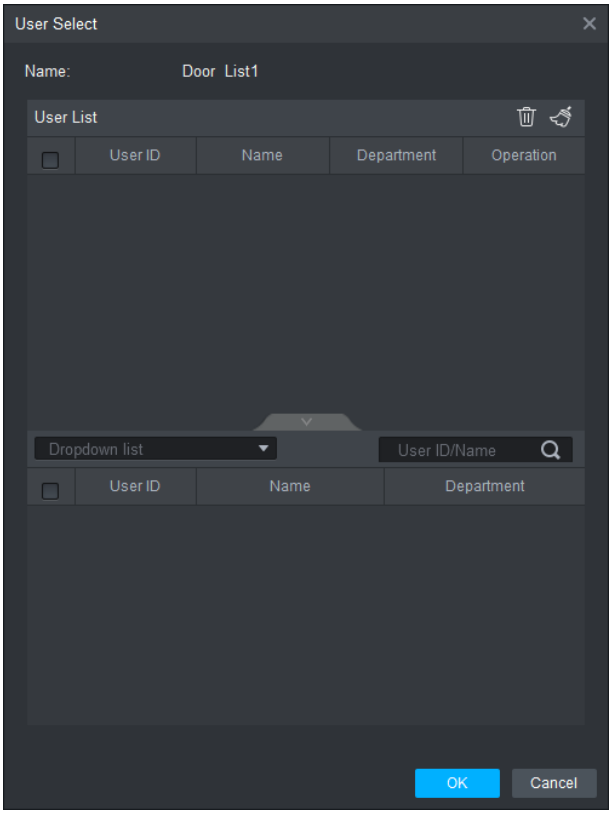


Figura 5-13 Selezione utente



Fase 1: Sulla schermata **Accesso** (Access), fare clic su  , quindi su **Aggiungi** (Add) e infine su **Autorizzazione gruppo porte** (Door Group Permission).

Fase 2: Fare clic su  . Selezionare il reparto utente nell'elenco a discesa oppure immettere **l'ID/il nome** (ID/Name) utente, quindi cercare l'utente. Selezionare utenti tra quelli trovati.

Fase 3: Fare clic su **Fine** (Finish) per completare la configurazione.

Non è possibile trovare utenti privi di ID.

5.5.2 Concessione dell'autorizzazione per ID utente

È possibile concedere l'autorizzazione all'accesso ad un utente selezionando l'utente stesso, e quindi selezionando i gruppi di porte per l'utente. Fare riferimento alla Figura 5-14 e alla Figura 5-15.

Figura 5-14 Accesso

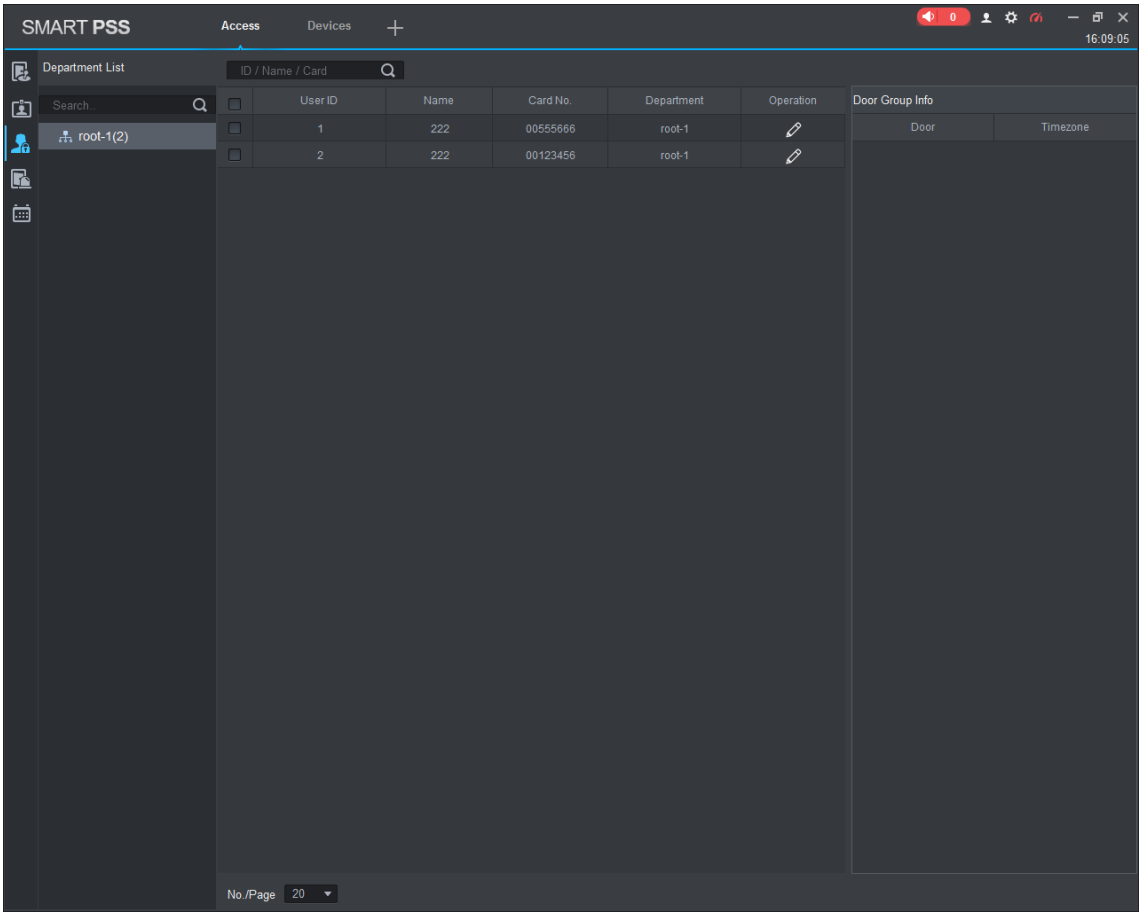
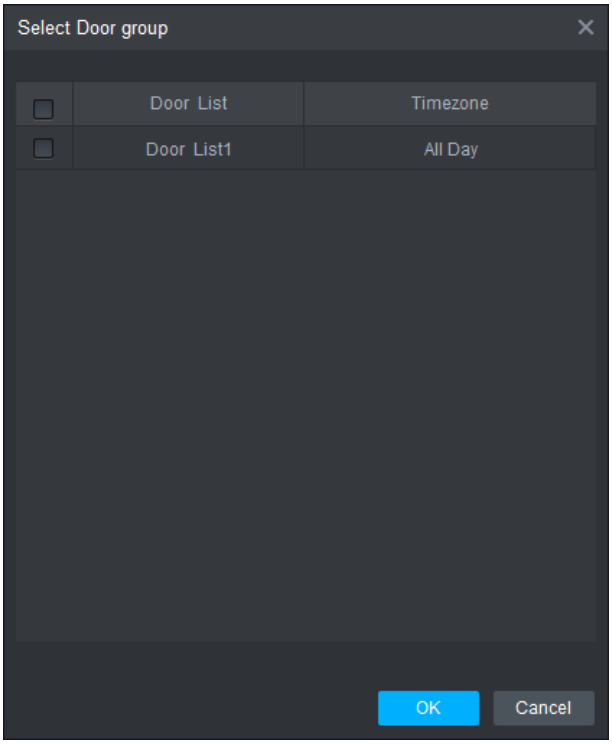


Figura 5-15 Selezione di un gruppo porte



Fase 1: Sulla schermata **Accesso** (Access), fare clic su  .

Fase 2: Fare clic su  . Si aprirà la schermata di Selezione di un gruppo porte (Select Door Group).

Fase 3: Selezionare il reparto utente nell'elenco a discesa oppure immettere l'ID/il nome utente, quindi selezionare un elenco di porte.

Fase 4: Fare clic su Fine (Finish) per completare la configurazione.

Appendice 1 Suggerimenti in materia di sicurezza informatica

La sicurezza informatica non è solamente una parola di moda: è qualcosa che ha a che fare con tutti i dispositivi collegati a Internet. La sorveglianza video IP non è immune ai rischi informatici, ma adottare semplici misure di protezione e rafforzamento delle reti e dei dispositivi di rete rende questi ultimi meno suscettibili agli attacchi. Di seguito sono forniti alcuni consigli e raccomandazioni su come creare un sistema di sorveglianza più sicuro.

Azioni obbligatorie da intraprendere per la sicurezza di rete di base dei dispositivi:

1. **Utilizzare password sicure**

   Seguire queste raccomandazioni quando si impostano le password:

   - la lunghezza non deve essere inferiore a 8 caratteri;
   - utilizzare almeno due tipi di caratteri diversi scelti fra lettere maiuscole e minuscole, numeri e simboli;
   - le password non devono contenere il nome dell'account o il nome dell'account al contrario;
   - non utilizzare caratteri in sequenza, come 123, abc ecc.;
   - non utilizzare caratteri ripetuti, come 111, aaa ecc.;

2. **Aggiornare il firmware e il software del client regolarmente**

   - Per assicurare che il sistema sia sempre protetto dalle patch e dagli aggiornamenti di sicurezza più recenti, è consigliabile mantenere aggiornati i firmware dei propri dispositivi (come NVR, DVR, telecamere IP ecc), come previsto dagli standard del settore tecnologico. Quando i dispositivi sono collegati a una rete pubblica, è consigliabile attivare la funzione Verifica automaticamente la presenza di aggiornamenti (auto-check for updates) per ottenere informazioni regolari sugli aggiornamenti del firmware rilasciati dai produttori.
   - È consigliabile scaricare e utilizzare l'ultima versione del software del client.

Raccomandazioni facoltative ma consigliate per migliorare la sicurezza di rete dei dispositivi:

1. **Protezione fisica**

   È consigliabile proteggere fisicamente le apparecchiature, specialmente i dispositivi di archiviazione. Ad esempio, posizionare le apparecchiature all'interno di un armadio in una stanza dei computer e implementare misure per il controllo degli accessi e la gestione delle chiavi adatte a evitare che il personale non autorizzato possa danneggiare l'hardware, collegare senza permesso dispositivi rimovibili (come chiavette USB e porte seriali) ecc.

2. **Modificare le password con regolarità**

   È consigliabile modificare le password regolarmente per ridurre il rischio che vengano scoperte o violate.

3. **Impostare e aggiornare tempestivamente le informazioni per il ripristino delle password**

   Il dispositivo supporta la funzione di ripristino della password. Configurare per tempo le informazioni relative al ripristino della password, compreso l'indirizzo e-mail dell'utente finale e le domande di sicurezza. Se le informazioni cambiano, modificarle tempestivamente. Quando si impostano le domande di sicurezza per il ripristino della password, è consigliabile non utilizzare domande le cui risposte possono essere facilmente indovinate.

4. **Attivare il blocco dell’account**
   La funzione di blocco dell’account è attiva per impostazione predefinita ed è consigliabile non disattivarla per garantire la sicurezza dell’account. Se un malintenzionato cerca di accedere ripetutamente con una password errata, l’account corrispondente e l’indirizzo IP utilizzato verranno bloccati.
5. **Modificare i valori predefiniti delle porte HTTP e relative agli altri servizi**
   Per ridurre il rischio che venga scoperto il numero di porta utilizzato, è consigliabile modificare i valori predefiniti delle porte HTTP e relative agli altri servizi scegliendo una qualsiasi combinazione di numeri compresa fra 1024 e 65535.
6. **Attivare il protocollo HTTPS**
   È consigliabile attivare il protocollo HTTPS, così da poter accedere al servizio web tramite un canale di comunicazione sicuro.
7. **Attivare la whitelist**
   È consigliabile attivare la whitelist per consentire l’accesso al sistema solo dagli indirizzi IP specificati. Pertanto, assicurarsi di aggiungere alla whitelist l’indirizzo IP del proprio computer e dei propri dispositivi.
8. **Associare l’indirizzo MAC**
   È consigliabile associare gli indirizzi IP e MAC del gateway alle apparecchiature per ridurre il rischio di spoofing ARP.
9. **Assegnare account e autorizzazioni in modo ragionevole**
   Aggiungere gli utenti con ragionevolezza e assegnare loro il minimo set di permessi in base alle esigenze lavorative e di gestione.
10. **Disattivare i servizi non necessari e scegliere modalità sicure**
    Per ridurre i rischi, è consigliabile disattivare servizi come SNMP, SMTP, UPnP ecc quando non sono necessari.
    Se sono necessari, è vivamente consigliato utilizzare le modalità sicure per i servizi che seguono (l’elenco non è esaustivo):
    - SNMP: scegliere SNMPv3 e impostare password crittografiche e di autenticazione sicure.
    - SMTP: scegliere TLS per accedere al server e-mail.
    - FTP: scegliere SFTP e impostare password sicure.
    - Hotspot AP: scegliere la crittografia WPA2-PSK e impostare password sicure.
11. **Utilizzare la trasmissione crittografata di audio e video**
    Se i contenuti audio e video sono molto importanti o sensibili, è consigliabili utilizzare la funzione di trasmissione crittografata per ridurre il rischio che i dati vengano rubati.
    Nota: la trasmissione crittografata rende la trasmissione meno efficiente.
12. **Verifiche di sicurezza**
    - Verifica degli utenti online: è consigliabile verificare regolarmente gli utenti online per vedere se qualcuno ha eseguito l’accesso al dispositivo senza autorizzazione.
    - Verifica dei registri delle apparecchiature: controllando i registri, è possibile conoscere gli indirizzi IP utilizzati per accedere ai propri dispositivi e alle operazioni chiave.
13. **Registro di rete**
    A causa della limitata capacità di archiviazione delle apparecchiature, il registro salvato è limitato. Se è necessario archiviare il registro per un tempo maggiore, è consigliabile attivare il registro di rete per assicurarsi che i registri critici siano sincronizzati con il server del registro di rete, garantendo una tracciatura efficiente.

14. Costruire un ambiente di rete sicuro

Per garantire la sicurezza delle apparecchiature e ridurre i rischi informatici potenziali, è consigliabile:

- disattivare la funzione di mappatura delle porte del router per evitare l'accesso diretto ai dispositivi intranet da una rete esterna;
- la rete deve essere suddivisa e isolata in base alle effettive esigenze di rete. in assenza di requisiti di comunicazione fra due sottoreti, è consigliabile utilizzare tecnologie come VLAN, GAP e altre per suddividere la rete e isolarla.
- Utilizzare il sistema di autenticazione degli accessi 802.1x per ridurre il rischio di accessi non autorizzati alle reti private.