

Videocitofono con Terminale di Riconoscimento Volti - Manuale d'Uso II

Versione del documento: V1.00

Grazie per aver acquistato il nostro prodotto. In caso di domande o richieste, rivolgersi al rivenditore.

Esclusione di responsabilità

Sono vietate la copia, la riproduzione, la traduzione e la distribuzione di qualsiasi parte del presente manuale, in qualsiasi forma e con qualsiasi mezzo, senza previo consenso scritto del produttore.

Il manuale può essere periodicamente aggiornato a seguito di un aggiornamento della versione o per altri motivi.

Il manuale è a solo scopo di riferimento. Tutte le affermazioni, informazioni e i suggerimenti contenuti in esso non costituiscono garanzie di alcun tipo, esplicite o implicite.

In nessun caso saremo responsabili per danni speciali, consequenziali, accidentali o indiretti derivanti dall'uso di questo manuale o del nostro prodotto, inclusi, a titolo esemplificativo ma non esaustivo, perdite di profitti commerciali, perdite causate da dati o documenti mancanti e anomalie durante il funzionamento del prodotto o fughe di informazioni dovute ad attacchi informatici, attacchi di hacker o attacchi di virus.

Precauzioni per la sicurezza



ATTENZIONE.

La password predefinita viene utilizzata per il primo accesso. Per garantire la sicurezza dell'account, modificare la password dopo il primo accesso. Si consiglia di impostare una password sicura (di almeno otto caratteri).

Prima di eseguire qualsiasi operazione, assicurarsi di leggere attentamente e osservare le disposizioni per la sicurezza contenute nel presente manuale.

- Le schermate fornite nel presente documento sono utilizzate solo a titolo di esempio e il layout dell'interfaccia utente varia a seconda delle versioni.
- Questo manuale si applica a più modelli, ma i modelli non sono tutti elencati nel presente documento. Fare riferimento ai prodotti reali durante la lettura del presente manuale.
- Ci riserviamo il diritto di modificare il contenuto di questo manuale senza preavviso o tempestività, ma non garantiamo che esso sia completamente privo di errori.
- A causa di fattori incerti quali l'ambiente fisico, i valori reali dei dati possono differire dai valori di riferimento qui descritti. In caso di domande o controversie, il diritto all'interpretazione finale spetta a noi.
- Seguire le istruzioni per l'uso riportate nel presente manuale quando si utilizza il prodotto. Decliniamo ogni responsabilità per eventuali problemi causati dal mancato rispetto delle istruzioni. Grazie per la collaborazione.

Protezione ambientale

Questo prodotto è stato progettato per essere conforme ai requisiti sulla protezione ambientale. Per il corretto stoccaggio, uso e smaltimento di questo prodotto, occorre attenersi alle leggi e normative nazionali.




Convenzioni

- Le figure, i grafici e le foto contenuti in questo manuale sono utilizzati a titolo puramente illustrativo e possono differire dal prodotto reale.

- Questo manuale si applica a più modelli, ma i modelli non sono tutti elencati nel presente documento. Fare riferimento ai prodotti reali durante la lettura del presente manuale.
- A causa di fattori incerti quali l'ambiente fisico, i valori reali di alcuni dati possono differire dai valori di riferimento qui descritti. In caso di domande o controversie, il diritto all'interpretazione finale spetta a noi.
- Seguire questo manuale quando si utilizza il prodotto. Si consiglia una guida professionale.
- Le convenzioni notazionali utilizzate nel presente documento sono descritte di seguito:

Formato	Descrizione
Grassetto	Indica pulsanti, menu, schede, nomi di finestre, nomi di finestre di dialogo e nomi di parametri. Ad esempio, fare clic su OK o selezionare Device Management .
“ ”	Indicano messaggi. Ad esempio, sull'interfaccia viene visualizzato “Hanging Up”.
>	Indirizza verso un menu a più livelli. Ad esempio, vai a Device Management > Add Device . In questo esempio, Add Device è un sottomenu di Device Management .

- I simboli riportati nella tabella seguente compaiono nel presente manuale. Seguire accuratamente le istruzioni indicate accanto al simbolo per evitare situazioni di pericolo e garantire un corretto uso del prodotto.

Simbolo	Descrizione
 AVVERTENZA!	Contiene importanti istruzioni per la sicurezza e indica situazioni che potrebbero provocare lesioni personali.
 ATTENZIONE!	Indica di prestare attenzione e che un uso improprio potrebbe provocare danni o guasti al prodotto.
 NOTA!	Indica ulteriori informazioni utili per l'uso del prodotto.

Indice

1	Ambito di applicazione del manuale	1
2	Panoramica del prodotto	1
3	Aspetto del prodotto	1
4	Installazione del prodotto	4
5	Operazioni Locali	4
5.1	Interfaccia iniziale	4
5.2	Interfaccia principale	5
5.3	Modalità annuncio	7
5.4	Interfaccia misurazione della temperatura/maschera	8
5.5	Configurazione Attivazione	13
5.5.1	Informazioni di base	14
5.5.2	Posizione del dispositivo	15
5.5.3	Impostazioni di rete	16
5.5.4	Gestione utenti	17
5.5.5	Password di attivazione	20
5.5.6	Password Amministratore	21
5.5.7	Scenario di autenticazione	21
5.6	Operazioni di chiamata sul videocitofono con terminale di riconoscimento volti	23
5.6.1	Chiamare un inquilino	23
5.6.2	Chiama il centro di gestione	26
5.7	Metodo di apertura della porta	27
5.7.1	Apertura della porta tramite scansione del volto	27
5.7.2	Apertura della porta tramite password	28
5.7.3	Apertura della porta tramite passaggio della scheda	30
5.7.4	Apertura porta con codice QR	31
5.7.5	Apertura da remoto	31
6	Gestione del personale	32
6.1	Inserimento delle informazioni sul personale	32
6.1.1	Importazione di informazioni nel terminale	32
6.2	Eliminazione del personale	32
7	Operazioni sul Web	32
7.1	Accesso	32
7.1.1	Operazioni preliminari	32

7.1.2 Accesso all'Interfaccia Web	34
7.2 Configurazione dei parametri	36
7.2.1 Funzioni comuni.....	36
7.2.2 Intelligente.....	49
7.2.3 Eventi	64
7.2.4 Archiviazione	68
7.2.5 Sicurezza	68
7.2.6 Sistema	70
8 Domande Frequenti	73

1 Ambito di applicazione del manuale

Tabella 1-1 Ambito di applicazione del manuale

Modello	Nome
OET-213H-NB	Terminale di Controllo degli Accessi con Riconoscimento Volti
OET-523L-NB	Terminale di Riconoscimento Volti

2 Panoramica del prodotto

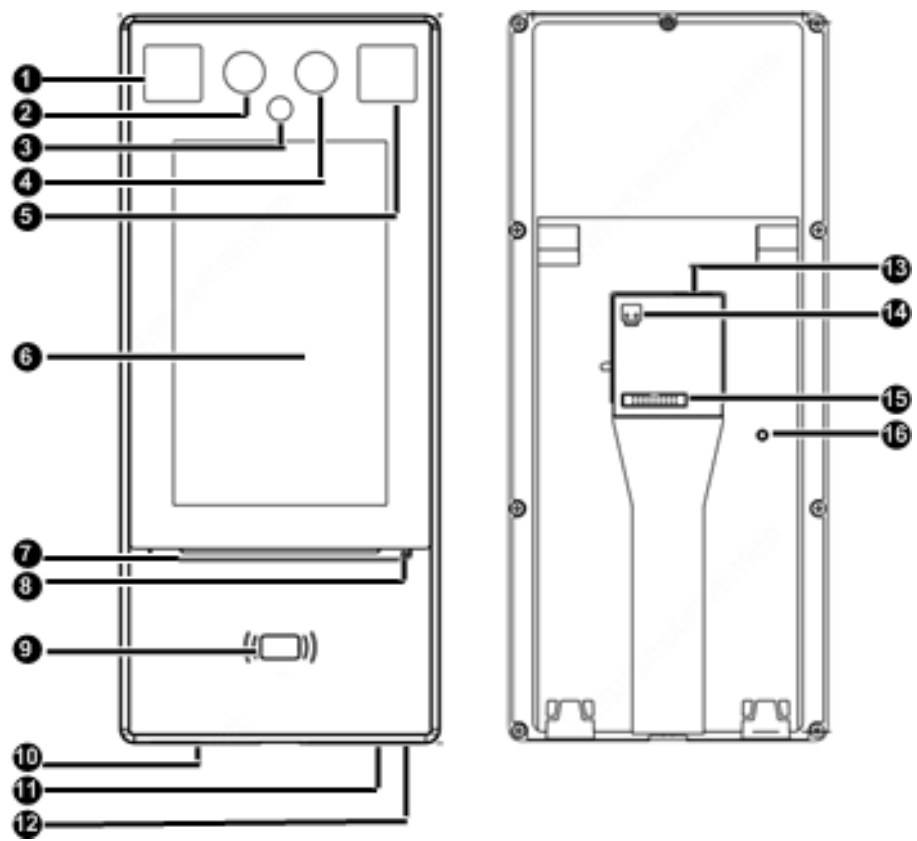
Il videocitofono con terminale di riconoscimento volti (in breve “il terminale di riconoscimento volti”) è un dispositivo per il controllo degli accessi tramite riconoscimento dei volti che offre prestazioni e affidabilità elevate. La tecnologia di riconoscimento dei volti è perfettamente integrata nel dispositivo di controllo degli accessi, che si avvale di un algoritmo di apprendimento profondo per supportare l'autenticazione dei volti per aprire la porta e ottenere un controllo preciso delle persone. Inoltre, viene supportato anche l'utilizzo del telecomando per l'apertura della porta tramite monitor interno. Questa soluzione può essere inoltre ampiamente applicata a scenari di sistemi di edilizia, come comunità intelligenti, sicurezza pubblica, parchi e altre aree di interesse.

3 Aspetto del prodotto

La figura qui sotto mostra la struttura del dispositivo. Prevarrà il dispositivo effettivo.

- OET-213H-NB

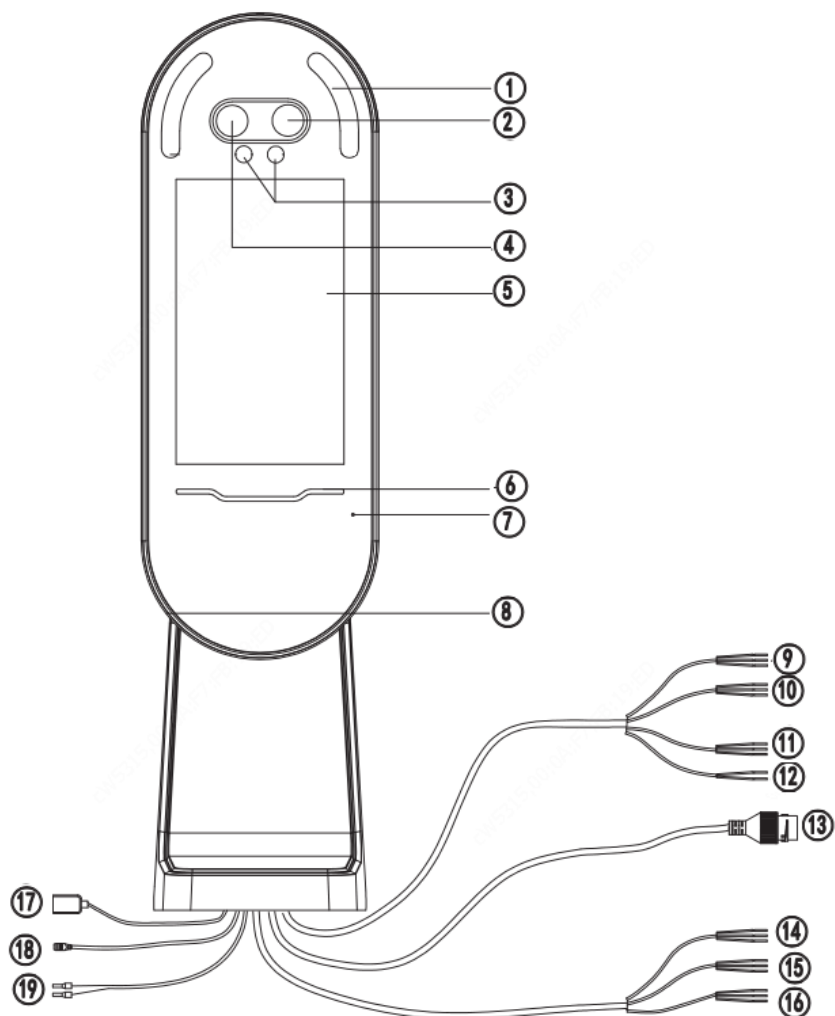
Figura 3-1 Struttura del dispositivo



1. Lampada illuminazione supplementare 1	2. Telecamera 1
3. Lampada a infrarossi supplementare	4. Telecamera 2
5. Lampada illuminazione supplementare 2	6. Schermo
7. Indicatore di transito	8. Microfono
9. Area di lettura schede	10. Altoparlante
11. Reset	12. USB 2.0
13. Interfaccia di rete	14. Ingresso di alimentazione (12 V CC ±25%)
15. Interfaccia a 20 pin	16. Pulsante antimanomissione

- OET-523L-NB

Figura 3-2 Struttura del dispositivo



1. Lampada illuminazione supplementare x2	2. Telecamera 1
3. Lampada a infrarossi supplementare	4. Telecamera 2
5. Schermo	6. Indicatore di transito
7. Microfono	8. Altoparlante
9. Uscita WIEGAND_OUT	10. Ingresso WIEGAND_IN
11. RS232	12. RS485
13. Interfaccia di rete	14. Ingresso ALARM_IN
15. IO-1	16. IO-2
17. USB	18. Uscita di alimentazione (5 V CC)
19. Ingresso di alimentazione (12 V CC ±25%)	

4 Installazione del prodotto

- Installazione dell'unità OET-213H-NB

Per il cablaggio e l'installazione del dispositivo, fare riferimento alla *Guida Rapida per il Terminale di Controllo degli Accessi con Riconoscimento Volti*.

- Installazione dell'unità OET-523L-NB

Per il cablaggio e l'installazione del dispositivo, fare riferimento alla *Guida Rapida per il Terminale di Riconoscimento Volti*.

5 Operazioni Locali

5.1 Interfaccia iniziale

Quando il terminale di riconoscimento volti viene utilizzato per la prima volta o vengono ripristinate le impostazioni predefinite di fabbrica, gli utenti devono impostare la password di attivazione, che viene utilizzata per accedere all'interfaccia [Configurazione Attivazione](#).



NOTA!

La password deve contenere almeno otto caratteri (con almeno due dei seguenti tipi: lettere maiuscole, lettere minuscole, cifre, caratteri di sottolineatura e trattini).

La password di attivazione corrisponde a quella che consente all'**admin** di accedere all'interfaccia web. Se la password di attivazione viene modificata, utilizzare la nuova password per l'[Accesso all'Interfaccia Web](#)

Dopo aver configurato la password di attivazione, apparirà l'[interfaccia principale del vicecitofono con terminale di riconoscimento volti](#). Se in seguito è necessario modificare la password di attivazione, fare riferimento alla sezione "[Password di attivazione](#)" per modificarla.

Figura 5-1 Interfaccia di Configurazione della Password di Attivazione

Wellcome

Please set an activation password first.

admin




OK

5.2 Interfaccia principale

L'interfaccia principale visualizzata sul terminale di riconoscimento volti varia a seconda del tipo di dispositivo. Fare riferimento alla sezione [Info Dispositivo](#).

Figura 5-2 Interfaccia Principale (Modalità Videocitofono)



N.	Descrizione
1	<p>Visualizza la data, l'ora e lo stato di connessione correnti dei vari servizi.</p>  <p>indica i seguenti elementi da sinistra a destra:</p> <ul style="list-style-type: none"> • Se abilitare o meno la modalità di scansione volti • Se un lettore di carte d'identità è connesso correttamente • Se il server 1 è online • Se il server 2 è online <p> NOTA!</p> <p>Un'icona contrassegnata con  indica "No".</p>
2	<ul style="list-style-type: none"> • Totale: numero totale di persone rilevate. • Normale: numero di persone con temperatura normale. <p>Quest'interfaccia viene visualizzata solo quando la funzione di misurazione della temperatura è abilitata. Per una descrizione dettagliata del funzionamento, fare riferimento alla sezione "Impostazioni avanzate".</p>
3	<p>Qui vengono visualizzati la foto e il nome di una persona identificata nella libreria. Fare riferimento alla sezione Visualizzazione dei risultati del riconoscimento per consentire al terminale di riconoscimento volti di visualizzare una o più immagini di volti registrati.</p>

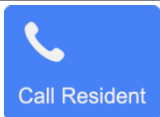



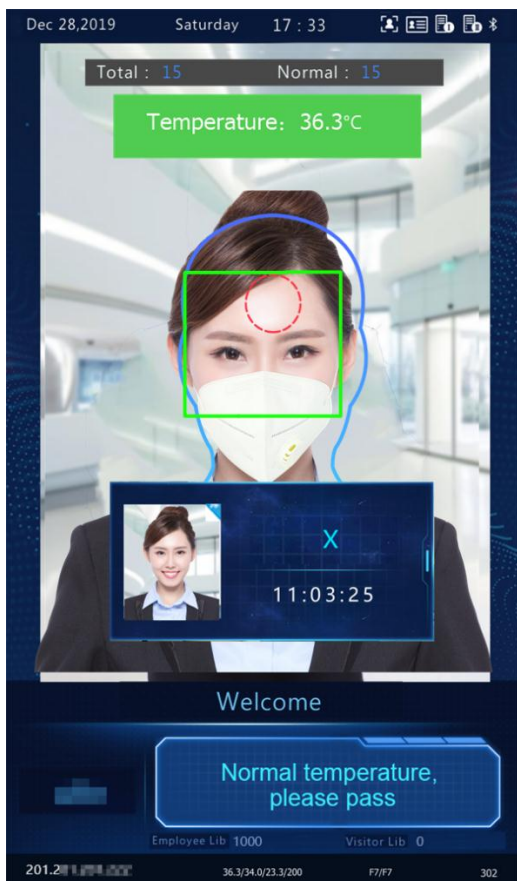
	Quando si seleziona Multiple Faces , a sinistra dello schermo vengono visualizzate le informazioni sull'ultima persona identificata correttamente. L'interfaccia consente di visualizzare le informazioni relative a un massimo di cinque persone identificate con successo di recente.	
4		Chiama un inquilino. Per una descrizione dettagliata della funzione, fare riferimento alla sezione " Chiama un inquilino ".
		Inserire una password per aprire la porta. Per una descrizione dettagliata della funzione, fare riferimento alla sezione Apertura porta con password .
		Chiama il centro di gestione. Per una descrizione dettagliata della funzione, fare riferimento alla sezione " Chiama il centro di gestione ".
		Codice QR utilizzato per l'apertura della porta. Per una descrizione dettagliata, fare riferimento alla sezione " Apertura porta con codice QR ".
5	Barra del titolo, configurabile dall'utente. Per informazioni dettagliate, fare riferimento alla sezione " Avviso e logo personalizzati ".	
6	Barra del logo, configurabile dall'utente. Per informazioni dettagliate, fare riferimento alla sezione " Avviso e logo personalizzati ".	
7	Mostra il risultato dell'identificazione (ad esempio, persona identificata correttamente o non registrata), la modalità di autenticazione (ad esempio scansione del volto o passaggio della scheda) e altre informazioni.	
8	Mostra il numero di persone nella libreria dei dipendenti e quello nella libreria dei visitatori.	
9	Barra di stato inferiore Mostra l'indirizzo IP del dispositivo, la temperatura in tempo reale, la temperatura minima predefinita, la temperatura ambiente, l'ora di rilevamento della temperatura, le informazioni sulla versione software e hardware del modulo di misurazione della temperatura e l'ora delle corrispondenze.	

Figura 5-3 Interfaccia principale (Modalità di controllo degli accessi comune)



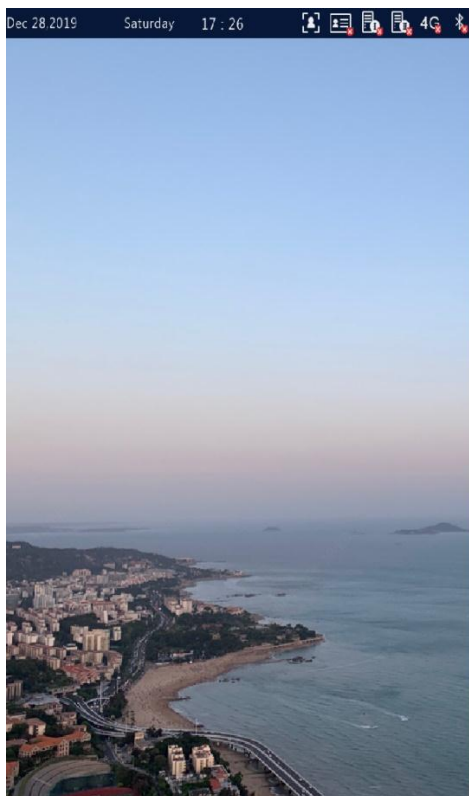
NOTA!

In modalità di controllo degli accessi comune, l'interfaccia principale non supporta le chiamate e l'apertura di porte con codice QR o password. L'interfaccia grafica mostra il risultato del riconoscimento di una sola persona.

5.3 Modalità annuncio

Il terminale di riconoscimento volti supporta gli annunci (fino a un massimo tre immagini). Per la configurazione degli annunci, fare riferimento alla sezione "[Modalità annuncio](#)".

Figura 5-4 Interfaccia annuncio



In modalità annuncio, il sistema non esce da tale modalità se una persona effettua con successo l'autenticazione (tramite scansione del volto o passaggio della scheda). Se la scansione del volto non va a buon fine o se la persona tocca lo schermo, il sistema esce dalla modalità annuncio e il terminale di riconoscimento volti mostra l'[Interfaccia principale](#).

5.4 Interfaccia misurazione della temperatura/maschera

Per contrastare l'epidemia in corso, le aziende, i parchi e le comunità rilevano la temperatura e controllano che le persone che varcano gli ingressi e le uscite indossino una mascherina. Il personale addetto esegue manualmente questo lavoro, il che consuma risorse e aumenta il rischio di infezioni incrociate. Il terminale di controllo degli accessi con riconoscimento volti è in grado di controllare se le persone indossano le mascherine e di rilevare la loro temperatura (a tal scopo è necessario un modulo di rilevamento digitale intelligente in grado di misurare la temperatura della fronte o quella del polso). Nel caso di persone con una temperatura anomala (che supera la soglia di temperatura massima preimpostata) o senza mascherina, il terminale di controllo degli accessi con riconoscimento volti mostra un allarme sull'interfaccia grafica, emette un segnale acustico di avvertimento e determina se aprire la porta sulla base di scene di applicazione reali, in modo da garantire la prevenzione e il controllo epidemico. Per informazioni dettagliate sulla configurazione, fare riferimento a [Impostazioni avanzate intelligenti](#) e [Scenario di autenticazione](#).



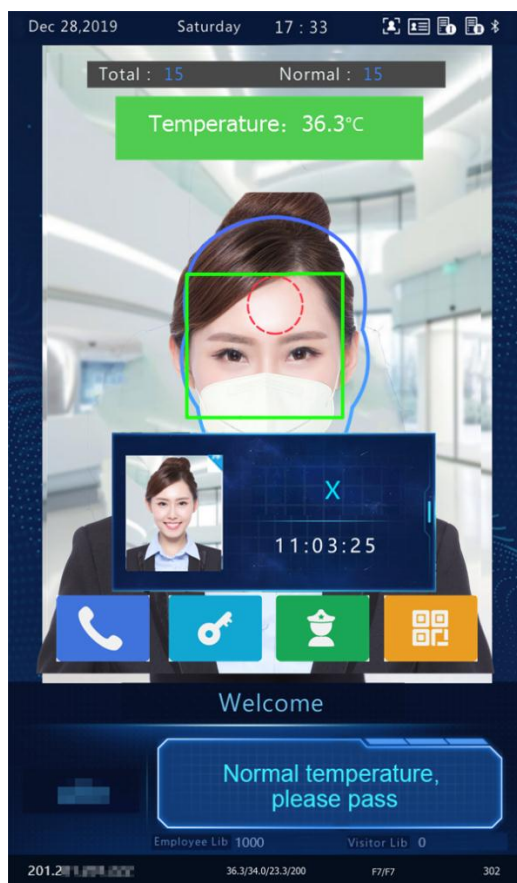
NOTA!

- Quando la funzione di misurazione della temperatura è abilitata per rilevare la temperatura della fronte, la persona deve avvicinarsi in corrispondenza della sagoma umana sullo schermo e puntare il centro della fronte in direzione del cerchio rosso, come mostrato nella [Figura 5-5](#). Quando occorre rilevare la temperatura del polso, la persona deve puntare il polso verso il punto di misurazione della temperatura del modulo di rilevamento digitale.
- Assicurarsi che la fronte o il polso si trovino ad una distanza adeguata dal modulo di rilevamento digitale intelligente. Per il modello OEP-BTM32-NB, la distanza consigliata è di 0,5–0,7 metri. Per il modello OEP-BTS1-NB, la distanza consigliata è di 1–2,5 cm.
- Durante il rilevamento della temperatura della fronte, questa non deve essere coperta da frange, capelli, occhiali da sole o altri oggetti. Durante la misurazione della temperatura del polso, il polso non può essere coperto da maniche, orologi, braccialetti o altri oggetti. Suddetti oggetti, se presenti, devono essere rimossi dalla fronte o dal polso da 0,5 a 1 minuto prima che la temperatura possa essere rilevata.
- La funzione di misurazione della temperatura richiede un modulo di rilevamento digitale intelligente, che può essere collegato al terminale di riconoscimento volti del videocitofono tramite RS485. Per la configurazione, fare riferimento alla sezione [Porta seriale](#).
- Non utilizzare la funzione di misurazione della temperatura in combinazione con la funzione casco di sicurezza/modulo di sicurezza.

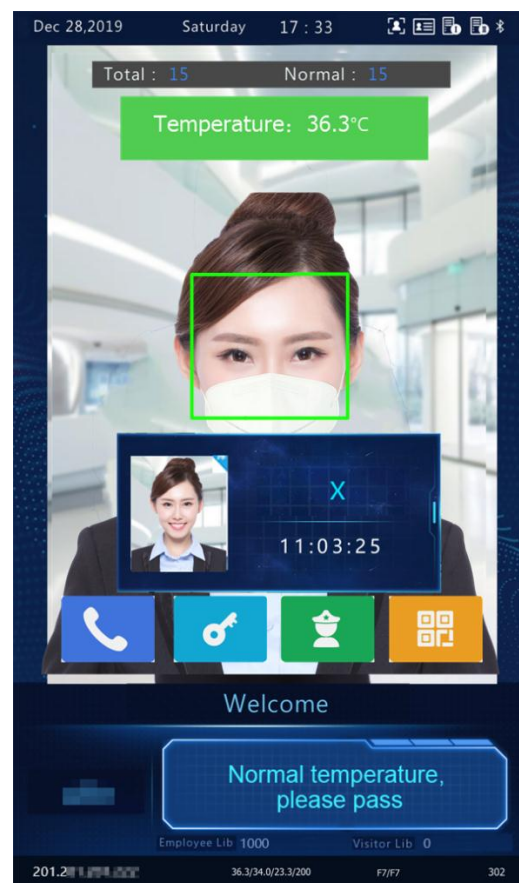
1. Rilevamento della mascherina e misurazione della temperatura

Attivare sia la funzione di rilevamento della mascherina sia quella di misurazione della temperatura sul terminale di riconoscimento facciale del videocitofono. Quando una persona (le cui informazioni sono memorizzate nella libreria) passa attraverso il terminale, l'interfaccia grafica mostra il risultato del rilevamento.

Figura 5-5 Temperatura normale e mascherina indossata

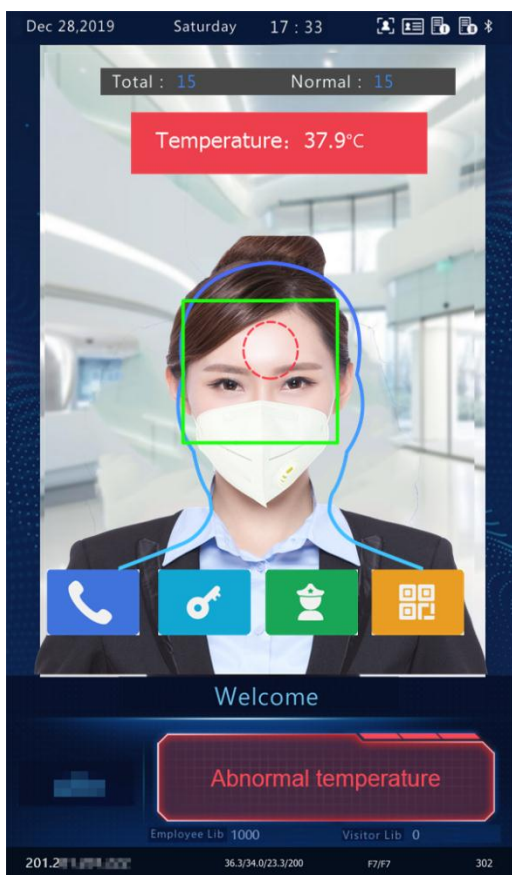


Misurazione della temperatura della fronte

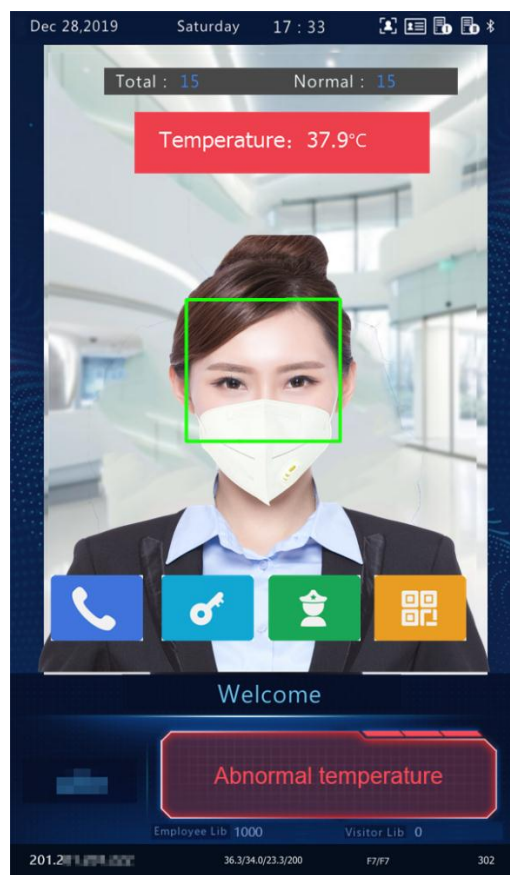


Misurazione della temperatura del polso

Figura 5-6 Mascherina indossata ma temperatura anomala



Misurazione della temperatura della fronte



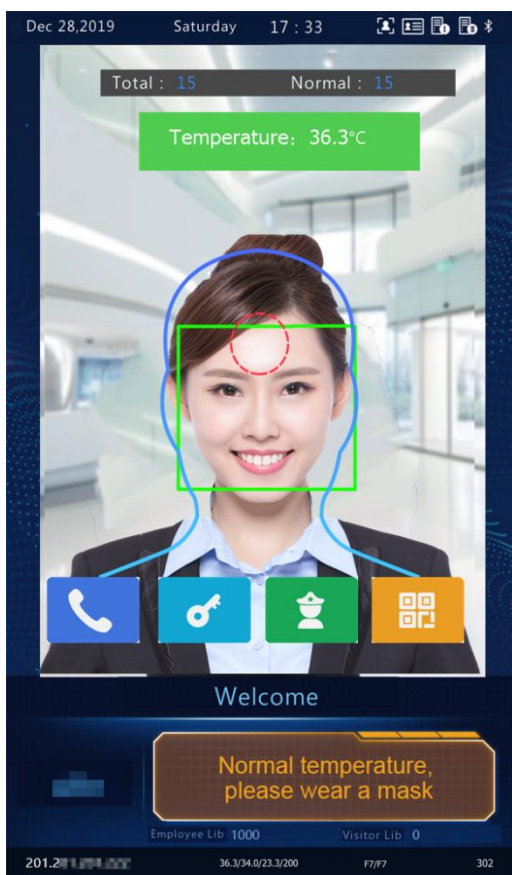
Misurazione della temperatura del polso



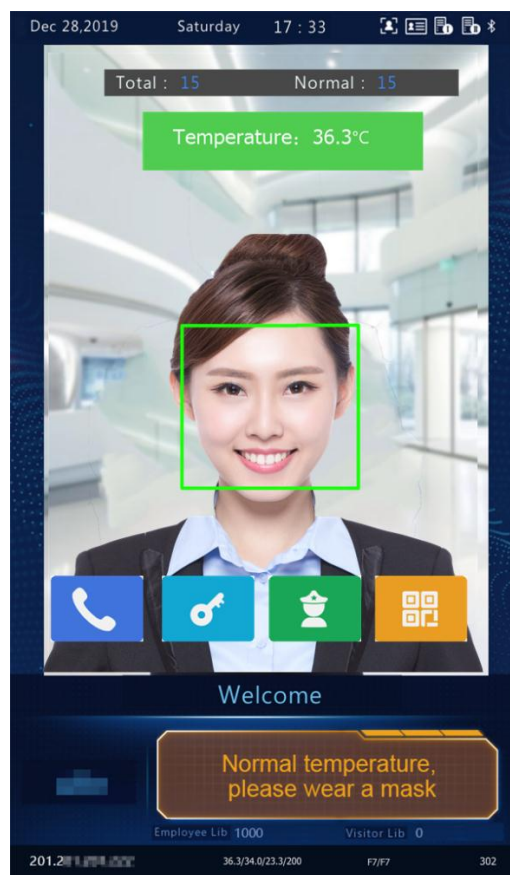
NOTA!

Quando sono abilitate sia la misurazione della temperatura sia il rilevamento della mascherina, la misurazione della temperatura ha priorità rispetto al rilevamento della mascherina. Quando viene rilevata una temperatura anomala, sull'interfaccia grafica viene segnalato un allarme di "temperatura anomala" e viene emesso un segnale acustico di avvertimento, a prescindere dal fatto che la persona indossi o meno una mascherina.

Figura 5-7 Temperatura normale ma mascherina non indossata



Misurazione della temperatura della fronte

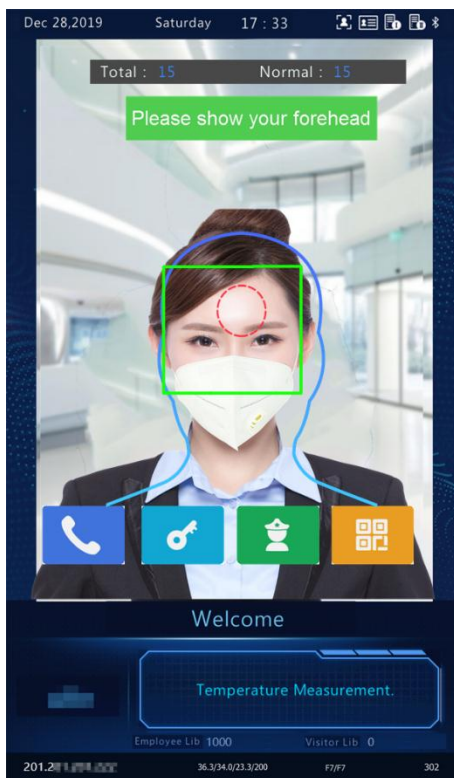


Misurazione della temperatura del polso

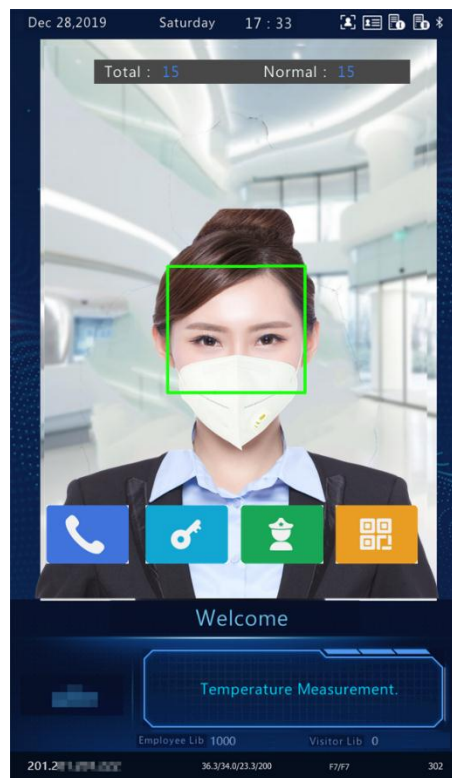
2. Modalità di misurazione della temperatura

Il terminale di riconoscimento dei volti del videocitofono supporta anche la modalità di sola misurazione della temperatura; in questo scenario, la funzione di misurazione della temperatura è abilitata, ma non è stata configurata alcuna modalità di autenticazione nella libreria dei volti (per i dettagli, fare riferimento alla sezione [Gestione libreria volti](#)). In questa modalità, il terminale di riconoscimento volti del videocitofono determina se aprire la porta o meno sulla base di scene reali per persone con temperatura anomala. Per informazioni dettagliate sulla configurazione, fare riferimento a [Impostazioni avanzate intelligenti](#).

Figura 5-8 Modalità di misurazione della temperatura



Misurazione della temperatura della fronte



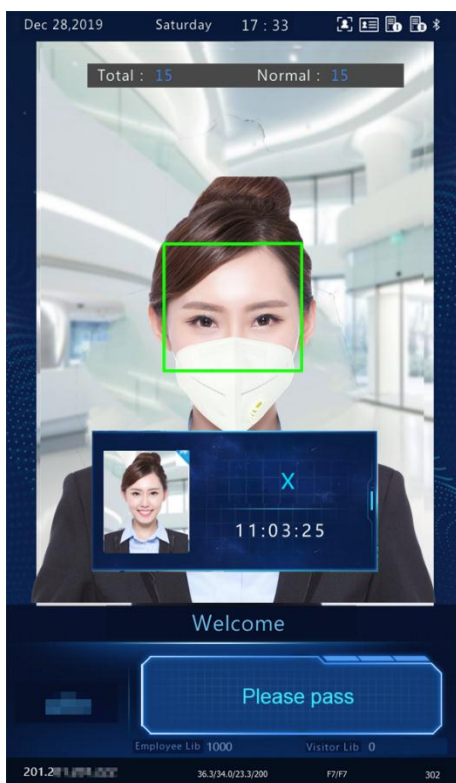
Misurazione della temperatura del polso

- Temperatura normale: la temperatura di una persona rilevata è normale. Per la notifica sull'interfaccia grafica e il messaggio vocale, fare riferimento alla [Figura 5-5](#).
- Temperatura anomala: la temperatura di una persona rilevata è anomala. Per la notifica sull'interfaccia grafica e il messaggio vocale, fare riferimento alla [Figura 5-6](#).

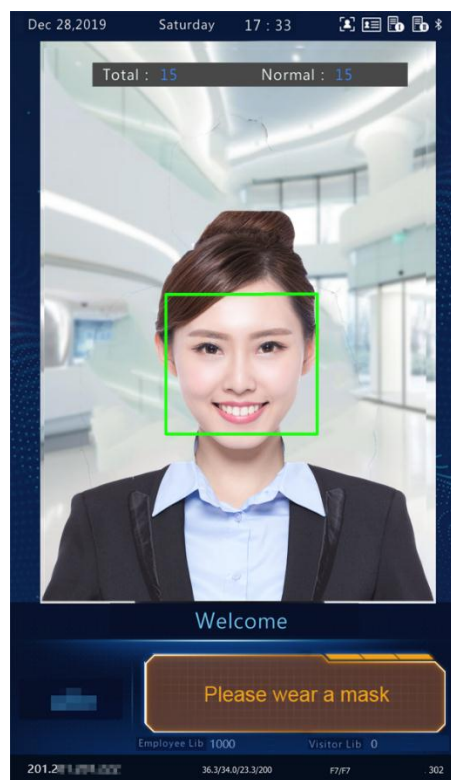
3. Rilevamento mascherina

Il terminale di riconoscimento volti del videocitofono supporta il rilevamento delle mascherine. Quando una persona (le cui informazioni sono memorizzate nella libreria) non indossa una mascherina, sull'interfaccia grafica appare un allarme e viene emesso un segnale acustico di avvertimento. Per coloro che non indossano una mascherina, il terminale determina se aprire la porta sulla base di scenari reali. Per informazioni dettagliate sulla configurazione, fare riferimento a [Impostazioni avanzate intelligenti](#).

Figura 5-9 Rilevamento mascherina



Mascherina indossata



Mascherina non indossata

5.5 Configurazione Attivazione

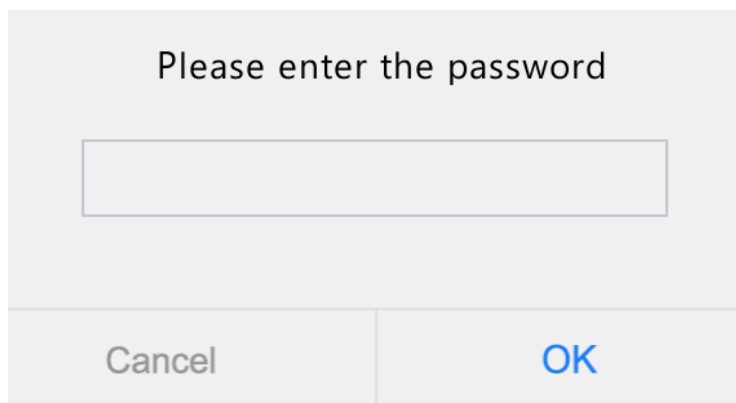
Tenere premuta per più di 3 secondi l'interfaccia principale del terminale di riconoscimento volti. Nell'interfaccia di immissione della password che appare, immettere la password di attivazione configurata per accedere all'interfaccia **Activation Config**. Se si dimentica la password, contattare il rappresentante locale per richiedere assistenza.



NOTA!

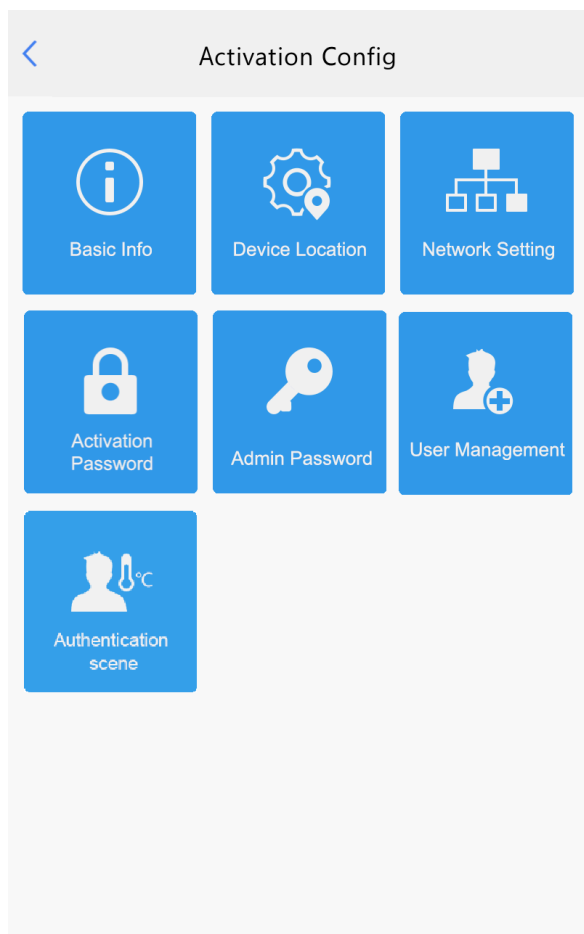
La password di attivazione iniziale è configurata sull'[interfaccia iniziale](#). Se viene modificata (sul [dispositivo locale](#) o sull'[Interfaccia Web](#)), immettere la nuova password di attivazione.

Figura 5-10 Interfaccia di immissione della password di attivazione



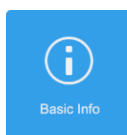
Nell'interfaccia **Activation Config** è possibile visualizzare le informazioni di base relative al terminale per il riconoscimento dei volti, configurare la posizione del dispositivo, la rete e la password, inserire le informazioni sul personale e lo scenario di autenticazione.

Figura 5-11 Interfaccia di Configurazione dell'attivazione



5.5.1 Informazioni di base

L'interfaccia **Basic Info** permette di visualizzare lo stato del dispositivo corrente in tempo reale, in modo da conoscere rapidamente le condizioni del dispositivo e migliorarne la manutenzione.



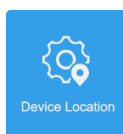
(1) Nell'interfaccia **Activation Config**, toccare  per accedere all'interfaccia **Basic Info**.

Figura 5-12 Interfaccia Basic Info

Basic Info	
Model	OET-525H
Firmware Version	PTS_Q2101-800000011_0007
Hardware Version	A
Boot Version	V1.2
Serial No.	210235C3VC4821600063
Network	204.41.100.101/255.255.255.0/24-4.1.1
MAC Address	480600000000
System Time	2019/9/27 17:09:18
Operation Time	0Day(s)0Hour(s)53Minute(s)
Management Server	Offline(0.0.0.0:5060)
Edge Storage	Normal

5.5.2 Posizione del dispositivo

Nell'interfaccia **Device Location**, è possibile configurare la comunità, l'unità e il centro di gestione a cui appartiene il dispositivo.




(1) Nell'interfaccia **Activation Config**, toccare **Device Location** per accedere all'interfaccia **Device Location**.

Figura 5-13 Interfaccia Device Location

Device Location	
Management Center IP	0 . 0 . 0 . 0
Community	
Building	1
Configurable Units	1
Unit	1 Unit
Save	

(2) Configurare le informazioni sulla posizione del dispositivo facendo riferimento alla tabella qui sotto.

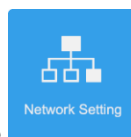
Tabella 5-1 Descrizione e configurazione dei parametri

Parametro	Descrizione e configurazione dei parametri
Indirizzo IP centro di gestione	Digitare qui l'indirizzo IP del centro di gestione. Una volta effettuata la configurazione, un utente può toccare Call Management Center sull'interfaccia grafica per chiamare il centro di gestione.  NOTA! L'indirizzo IP del centro di gestione deve trovarsi nello stesso segmento di rete del dispositivo e non può iniziare con 127.
Comunità	Immettere il nome della comunità a cui appartiene il dispositivo. È possibile inserire da 1 a 35 caratteri (da 1 a 11 caratteri cinesi).
Edificio	<ul style="list-style-type: none"> • Inserire il numero dell'edificio in cui si trova il dispositivo. • Il valore deve essere un numero intero compreso tra 1 e 99.
Unità configurabili	Selezionare il numero di unità che possono essere servite dal dispositivo dall'elenco a discesa. Le opzioni possibili sono 1, 2 e 3 .
Unità	Inserire il numero dell'unità in cui si trova il dispositivo. Il valore deve essere un numero intero compreso tra 1 e 9.

(3) Toccare **Save** per completare la configurazione delle informazioni sulla posizione del dispositivo.

5.5.3 Impostazioni di rete

Nell'interfaccia **Network Setting** è possibile modificare l'indirizzo IP del dispositivo e altri parametri di comunicazione, in modo che il dispositivo possa comunicare con dispositivi esterni.




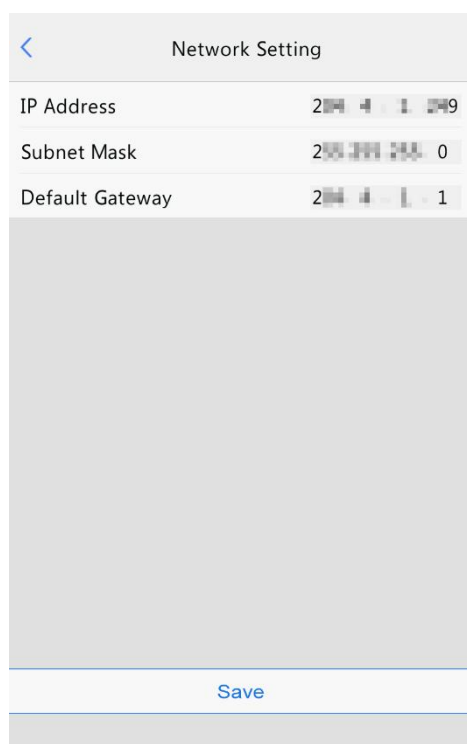
(1) Nell'interfaccia **Activation Config**, toccare  per accedere all'interfaccia **Network Setting**.

Figura 5-14 Interfaccia Network Setting



(2) Impostare i parametri di rete facendo riferimento alla tabella qui sotto.

Tabella 5-2 Descrizione e configurazione dei parametri

Parametro	Descrizione e configurazione dei parametri
Indirizzo IP	Digitare qui l'indirizzo IP del dispositivo. L'indirizzo IP del dispositivo deve essere unico in rete.
Subnet Mask	Immettere la subnet mask del dispositivo.
Gateway predefinito	Immettere il gateway predefinito del dispositivo.

(3) Toccare **Save** per completare l'impostazione di rete.

5.5.4 Gestione utenti

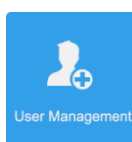
Il terminale di riconoscimento dei volti consente di inserire informazioni sul personale. Gli addetti, le cui informazioni sono state inserite con successo nel dispositivo, possono passare le schede o le credenziali, o sottoporsi alla scansione dei volti per l'accesso.

1. Requisiti per l'acquisizione delle immagini dei volti

Quando si aggiunge una persona all'elenco delle persone consentite, acquisire la foto del volto osservando rigorosamente i seguenti requisiti:

- Requisito generale: foto a tutto volto senza coprire il capo. Durante il processo di acquisizione, sullo schermo del terminale viene visualizzata solo la foto del volto della persona interessata e i volti di altre persone non possono essere inclusi.
- Requisiti di estensione: la foto deve mostrare il contorno di entrambe le orecchie di una persona e comprendere lo spazio che va dalla sommità della testa (compresi tutti i capelli) alla base del collo.
- Requisiti di posizione: durante l'acquisizione, il volto deve essere posizionato all'interno del riquadro visibile sull'interfaccia del terminale.
- Requisiti di trucco: durante l'acquisizione delle immagini, non utilizzare prodotti cosmetici che modificano il colore e influiscono sull'aspetto reale, come il mascara per le ciglia e il make-up per le sopracciglia.
- Requisiti di sfondo: è accettabile uno sfondo bianco, blu o di altro colore a tinta unica.
- Requisiti di illuminazione: Durante l'acquisizione è necessaria un'illuminazione con una luminosità adeguata. Evitare foto troppo scure, troppo luminose e i volti dai toni chiarscuri.

2. Procedura di immissione delle informazioni sul personale



(1) Nell'interfaccia **Activation Config**, toccare  per accedere all'interfaccia **User Management**.

Figura 5-15 Interfaccia di gestione utente


(2) Configurare l'immissione delle informazioni sul personale facendo riferimento alla tabella qui sotto.

Tabella 5-3 Descrizione e configurazione dei parametri

Parametro	Descrizione e configurazione dei parametri	Note
Nome	Obbligatorio. Inserire il nome di una persona.	/
Sesso	Inserire il sesso della persona. Selezionare Male o Female dall'elenco a discesa. Il valore predefinito è Male .	/
N. scheda	Inserire il numero della scheda della persona. Una volta inserito il numero, la persona può passare la scheda per accedere.	È necessario impostare almeno uno dei parametri in modo che le informazioni sul personale possano essere immesse correttamente.
N. ID	Inserire il numero della carta d'identità della persona. Una volta inserito il numero, la persona può passare la carta d'identità per accedere.	
Immagine volto	Per informazioni su come acquisire e salvare le foto dei volti, fare riferimento alla procedura di acquisizione delle foto dei volti . Dopo aver inserito correttamente i dati, il volto della persona può essere sottoposto alla scansione ai fini dell'accesso.	

(3) Eseguire le seguenti operazioni per acquisire e salvare la foto del volto di una persona.

- a Seguire le istruzioni sull'interfaccia e chiedere alla persona di guardare verso la fotocamera.
- b Quando la foto visualizzata sull'interfaccia grafica soddisfa i [requisiti per l'acquisizione delle immagini](#)


[dei volti](#), toccare  per acquisire l'istantanea del volto. Vedere la figura sotto.



è il pulsante Indietro.

Figura 5-16 Acquisizione e salvataggio di una foto del volto



- c Sull'interfaccia di conferma della foto, toccare  per confermare la foto acquisita.


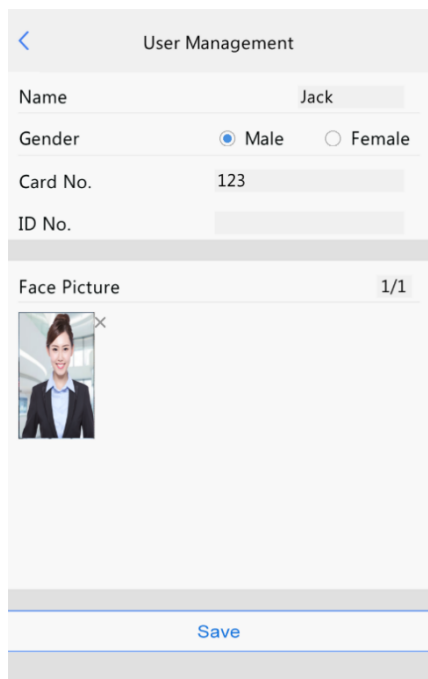
 è il pulsante Indietro.

Figura 5-17 Interfaccia di conferma foto



- (4) Nell'interfaccia **User Management**, toccare **Save** per completare l'immissione delle informazioni sul personale.

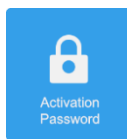
Figura 5-18 Interfaccia di salvataggio



The screenshot shows a mobile application interface titled "User Management". It contains a form with the following fields: "Name" with the value "Jack", "Gender" with radio buttons for "Male" (selected) and "Female", "Card No." with the value "123", and "ID No." which is empty. Below these fields is a "Face Picture" section showing a photo of a woman, with a "1/1" indicator. At the bottom of the screen is a blue "Save" button.

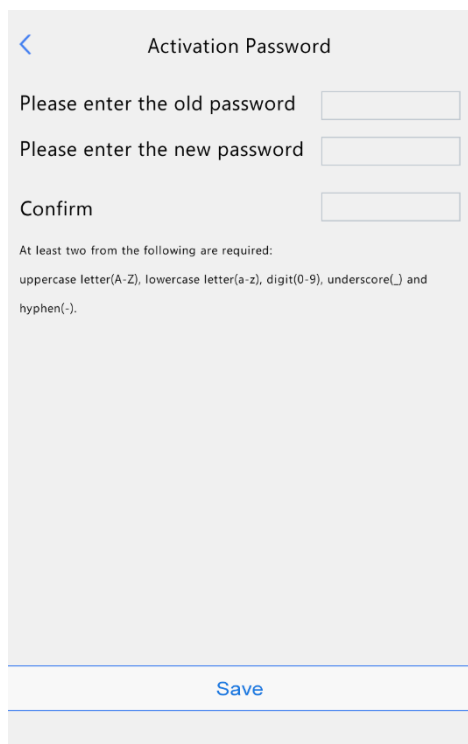
5.5.5 Password di attivazione

Per modificare la password di attivazione configurata, procedere come segue:



(1) Nell'interfaccia **Activation Config**, toccare **Activation Password** per accedere all'interfaccia **Activation Password**.

Figura 5-19 Interfaccia della password di attivazione



The screenshot shows a mobile application interface titled "Activation Password". It contains three input fields: "Please enter the old password", "Please enter the new password", and "Confirm". Below the fields is a list of requirements: "At least two from the following are required: uppercase letter(A-Z), lowercase letter(a-z), digit(0-9), underscore(_) and hyphen(-)". At the bottom of the screen is a blue "Save" button.

(2) Inserire la vecchia password, quindi inserire la nuova password e confermarla come richiesto.



NOTA!

- La password deve contenere almeno otto caratteri (con almeno due dei seguenti tipi: lettere maiuscole, lettere minuscole, cifre, caratteri di sottolineatura e trattini).
- La password di conferma deve coincidere con la nuova password.
- La password di attivazione corrisponde a quella che consente all'**admin** di accedere all'interfaccia web. Se la password di attivazione viene modificata, utilizzare la nuova password per [accedere all'interfaccia Web](#).

(3) Toccare **Save** per completare la modifica della password di attivazione.

5.5.6 Password Amministratore

Nell'[Apertura porta con password](#), gli utenti possono immettere una password Amministratore per aprire la porta. La password di amministratore è applicabile al personale addetto alla gestione dei dispositivi (come le persone del centro di gestione).

La password di amministratore è disattivata per impostazione predefinita. Se occorre attivare la password di amministratore, toccare **Yes** e immettere la password nel campo **Password**, quindi toccare **Confirm**.



NOTA!

- La password deve essere una stringa di otto caratteri.
- La password di conferma deve coincidere con la password.

Figura 5-20 Interfaccia di configurazione della password di amministratore

Password Configuration

Enable Yes No

Password

Confirm

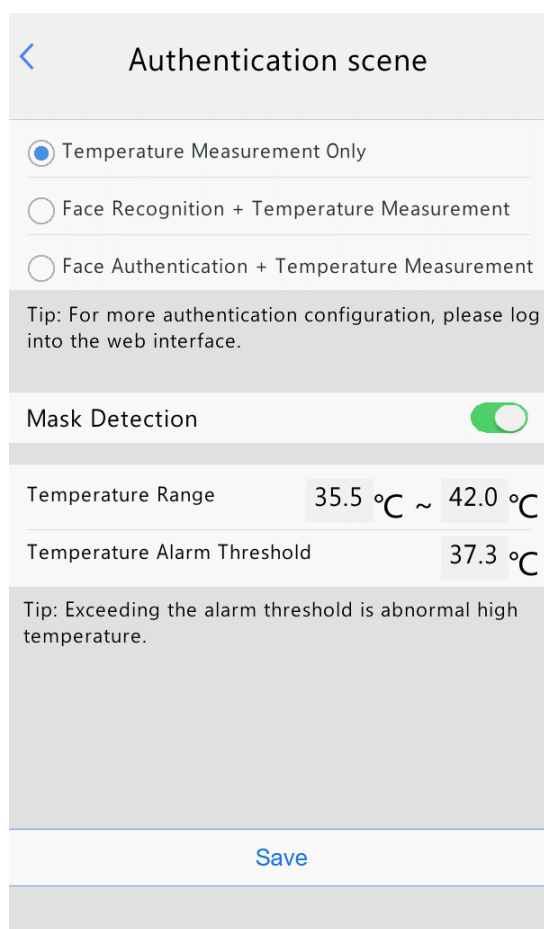
Tip: Please enter a 8-character password.

Save

5.5.7 Scenario di autenticazione

Quest'interfaccia consente di configurare gli scenari di autenticazione del terminale, l'intervallo di misurazione della temperatura, il valore di allarme della temperatura e altri dati. La tabella riportata di seguito descrive i dettagli della configurazione.

Figura 5-21 Interfaccia dello Scenario di autenticazione



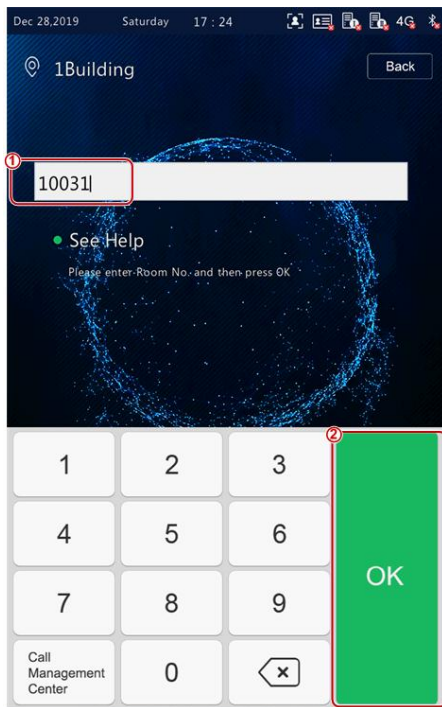
Parametro		Descrizione e configurazione
Scenario di autenticazione	Solo misurazione della temperatura	Il terminale di riconoscimento dei volti del videocitofono misura solo la temperatura delle persone e non effettua altre operazioni di autenticazione. Per le indicazioni sull'interfaccia grafica, fare riferimento alla sezione Modalità di misurazione della temperatura . Nota: In questo scenario, le modalità di autenticazione di tutte le librerie configurate nel terminale di riconoscimento volti del videocitofono saranno cancellate.
	Scansione volto + Misurazione temperatura	Una persona può passare solo dopo che l'autenticazione del volto è riuscita e la temperatura è normale. Per le indicazioni sull'interfaccia grafica, fare riferimento alla sezione Rilevamento della mascherina e misurazione della temperatura .
	Autenticazione volto + Misurazione temperatura	Vengono adottate modalità elenco volti consentiti + modalità misurazione temperatura. Una persona (le cui informazioni sono memorizzate nella libreria) può passare solo dopo che l'autenticazione del volto è riuscita e la temperatura è normale. Per le indicazioni sull'interfaccia grafica, fare riferimento alla sezione Rilevamento della mascherina e misurazione della temperatura . Nota: Questo scenario può essere configurato solo quando la libreria dipendenti predefinita esiste in Gestione libreria volti .
Rilevamento mascherina		Abilitarlo o disabilitarlo in base agli scenari di applicazione reali.
Configurazione della temperatura	Intervallo di misurazione della temperatura	Intervallo di valori: [30–45]; intervallo predefinito: [34-42] Configurare l'intervallo in base agli scenari di applicazione reali.
	Soglia di allarme temperatura	Quando il modulo di rilevamento digitale rileva una temperatura superiore alla soglia qui configurata, l'allarme "temperatura anomala" appare sull'interfaccia grafica e viene emesso il segnale acustico di avvertimento. Intervallo di valori: [30–45]; valore predefinito: 37,3

5.6 Operazioni di chiamata sul videocitofono con terminale di riconoscimento volti

5.6.1 Chiamare un inquilino

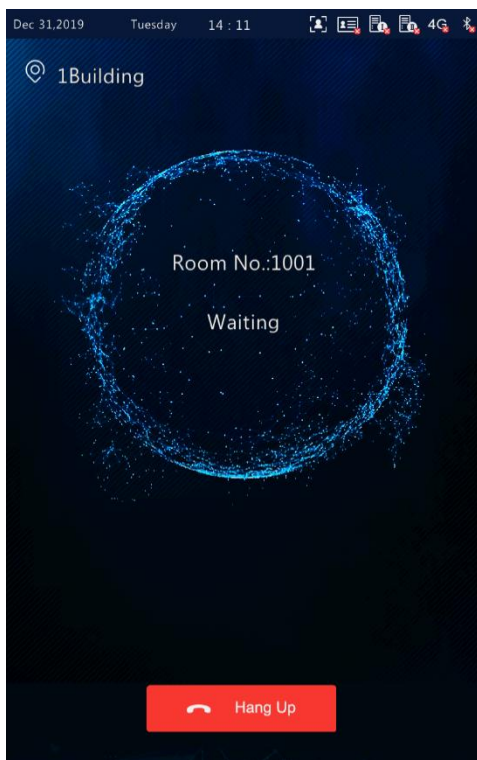
- (1) Toccare **Call Resident** sull'interfaccia principale.
- (2) Nell'interfaccia visualizzata, immettere il numero della stanza come richiesto, quindi toccare **OK**.

Figura 5-22 Interfaccia di composizione per una chiamata



- (3) L'interfaccia di avviso di chiamata viene visualizzata sul terminale di riconoscimento volti, come mostrato nella figura sottostante.

Figura 5-23 Interfaccia di avviso di chiamata

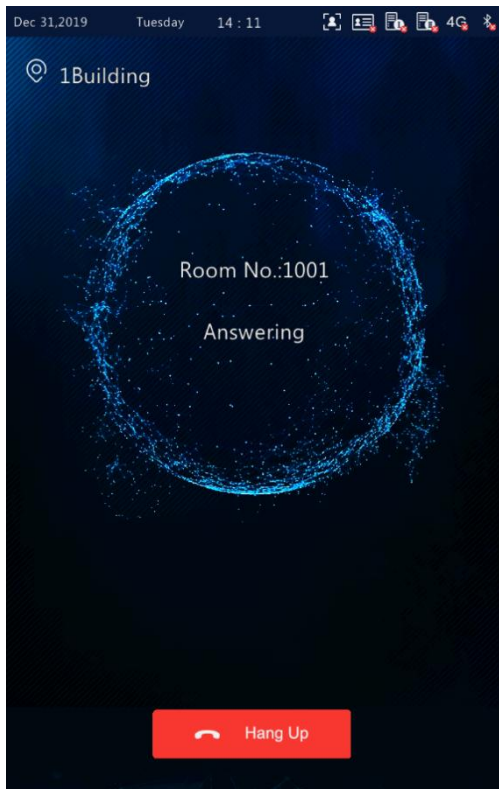


(4) Il terminale di riconoscimento volti presenta diverse interfacce, a seconda che il monitor interno risponda o meno alla chiamata.

- Rispondi

Quando il monitor interno risponde alla chiamata dal terminale di riconoscimento volti, viene visualizzata un'interfaccia come quella mostrata nella figura sottostante.

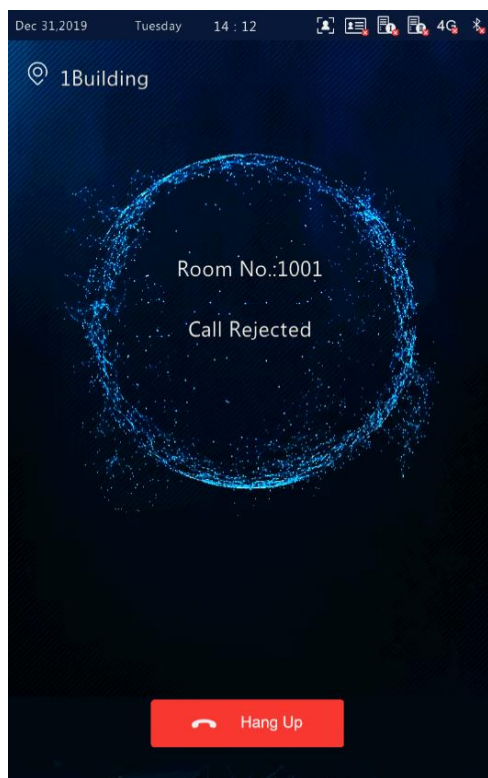
Figura 5-24 Interfaccia visualizzata dopo che il monitor interno ha risposto alla chiamata



- Rifiuta

Quando il monitor interno rifiuta la chiamata dal terminale di riconoscimento volti, viene visualizzata un'interfaccia come quella mostrata nella figura sottostante e il terminale torna all'interfaccia principale.

Figura 5-25 Interfaccia visualizzata dopo che il monitor interno ha rifiutato la chiamata



- Timeout chiamata

Quando il monitor interno non risponde alla chiamata entro un intervallo di tempo prestabilito (60 secondi), il terminale di riconoscimento dei volti termina automaticamente la chiamata e ritorna all'interfaccia principale.

- Altri casi

Quando il terminale di riconoscimento dei volti chiama un monitor interno, sull'interfaccia del terminale vengono fornite diverse indicazioni in base alla configurazione e alle operazioni. Vedere la tabella sottostante.

Tabella 5-4 Descrizione delle indicazioni visualizzate sull'interfaccia

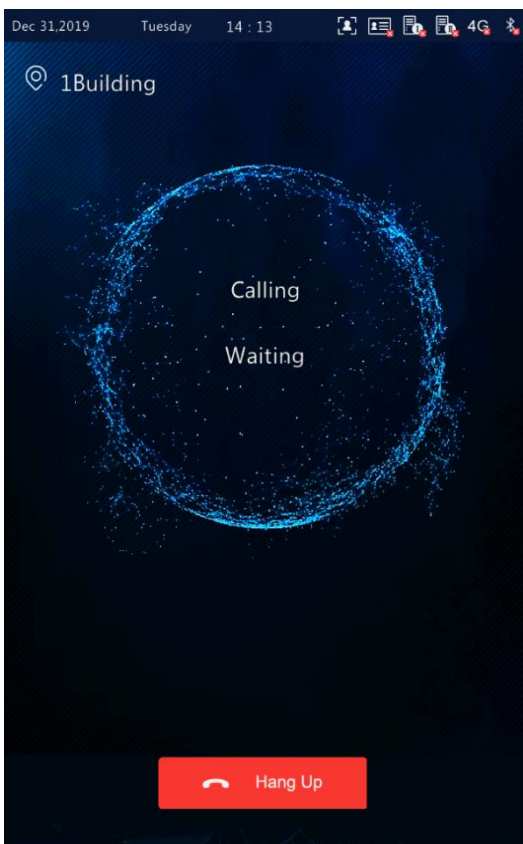
Indicazione visualizzata sull'interfaccia del terminale di riconoscimento dei volti	Descrizione
Riaggancia	Quando si tocca Hang up sull'interfaccia del terminale di riconoscimento dei volti prima che un utente risponda alla chiamata, viene visualizzato "Hanging Up" sull'interfaccia, e dopo 2 secondi il terminale termina la chiamata e ritorna all'interfaccia principale.
Impossibile connettersi	Quando l'inquilino chiamato dal terminale di riconoscimento dei volti non esiste, sull'interfaccia viene visualizzato "Unable to Connect", quindi il terminale termina la chiamata e dopo 2 secondi ritorna all'interfaccia principale.
L'utente chiamato è occupato	Quando il terminale di riconoscimento dei volti chiama un monitor interno che si trova in modalità Non disturbare, sull'interfaccia viene visualizzato "L'utente chiamato è occupato", quindi il terminale termina la chiamata e dopo 2 secondi torna all'interfaccia principale.
Nessuna risposta	Quando il terminale di riconoscimento dei volti chiama un monitor interno configurato con risposta automatica, sull'interfaccia viene visualizzato "No Answer", quindi il terminale termina la chiamata e dopo 2 secondi torna all'interfaccia principale.
Errore di rete	Se la rete del terminale per il riconoscimento dei volti o un monitor interno chiamato è disconnesso, sull'interfaccia viene visualizzato "Network Failure", quindi il terminale termina la chiamata e dopo 2 secondi torna all'interfaccia principale.

<p>Password errata configurata per la postazione esterna.</p>	<p>Se il monitor interno chiamato configura una password errata per il monitor esterno, sull'interfaccia viene visualizzato "Incorrect password configured for the outdoor station", quindi il terminale termina la chiamata e dopo 2 secondi torna all'interfaccia principale.</p>
---	---

5.6.2 Chiama il centro di gestione

- (1) Toccare **Call Management Center** sull'interfaccia principale.
- (2) La seguente immagine mostra l'interfaccia di chiamata visualizzata quando il terminale di riconoscimento dei volti chiama il centro di gestione.
- (3) Per la configurazione del centro di gestione, fare riferimento alla sezione [Configurazione del centro di gestione](#).

Figura 5-26 Interfaccia di chiamata del centro di gestione



- (4) Il terminale di riconoscimento volti presenta diverse interfacce a seconda che il centro di gestione risponda o meno alla chiamata.

- Rispondi

Una persona nel centro di gestione risponde alla chiamata dal terminale di riconoscimento dei volti. Per la schermata dell'interfaccia, fare riferimento a [Rispondi](#).

- Rifiuta

Una persona nel centro di gestione rifiuta la chiamata dal terminale di riconoscimento dei volti. Per la schermata dell'interfaccia, fare riferimento a [Rifiuta](#).

- Timeout chiamata

Quando nessuna persona del centro di gestione risponde alla chiamata entro l'intervallo impostato (60 secondi), il terminale di riconoscimento dei volti termina automaticamente la chiamata e torna all'interfaccia principale.

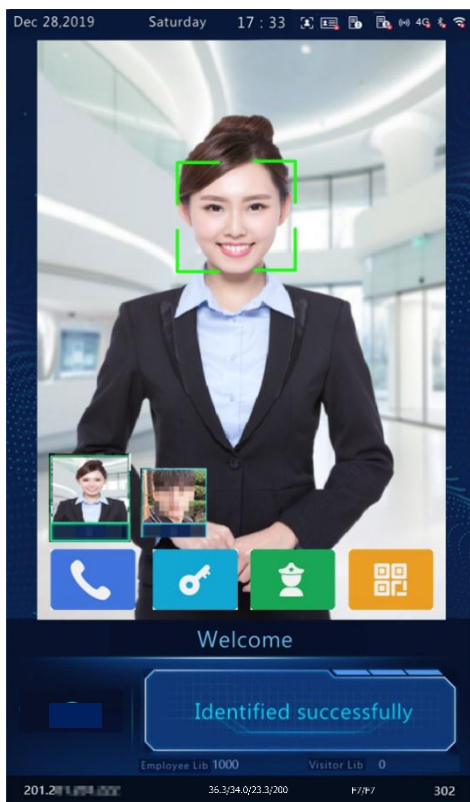
5.7 Metodo di apertura della porta

5.7.1 Apertura della porta tramite scansione del volto

Il terminale di riconoscimento dei volti abbina la foto di un volto precedentemente acquisita con le immagini memorizzate nella libreria di foto dei volti.

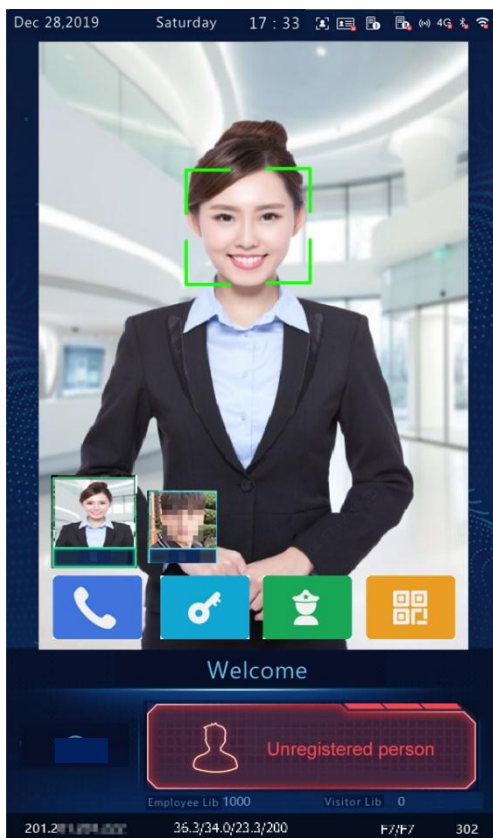
- Se la corrispondenza ha esito positivo, viene visualizzata un'interfaccia come quella illustrata nella figura sottostante, viene riprodotto il messaggio audio "Recognized successfully" e la porta viene aperta.

Figura 5-27 Interfaccia di riconoscimento riuscito



- Se la corrispondenza non riesce, appare un'interfaccia come quella della figura sottostante e viene riprodotto il messaggio audio "Unregistered person". È possibile provare altri metodi di apertura della porta.

Figura 5-28 Interfaccia di persona non registrata



- Altri errori durante l'apertura della porta tramite scansione del volto
Durante l'apertura della porta basata sulla scansione del volto possono verificarsi degli errori. Le indicazioni visualizzate sull'interfaccia sono le seguenti e l'effetto è simile a quello dell'interfaccia [Persona non registrata](#).
 - Non una persona reale.
 - Accesso non programmato.
 - Guardare verso la fotocamera.

5.7.2 Apertura della porta tramite password

Quando l'autenticazione tramite password è abilitata sul monitor esterno (per la configurazione, fare riferimento a [Modello di controllo](#)), una persona può inserire la password della stanza o la password dell'amministratore per aprire la porta.

1. Apertura della porta tramite password

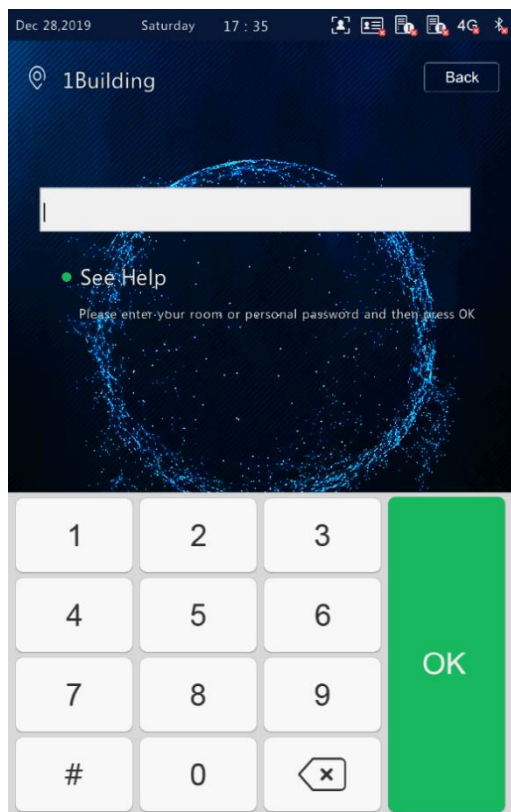
- (1) Toccare **Password** sull'interfaccia principale.
- (2) Nell'interfaccia visualizzata, immettere la password come richiesto, quindi toccare **OK**.



NOTA!

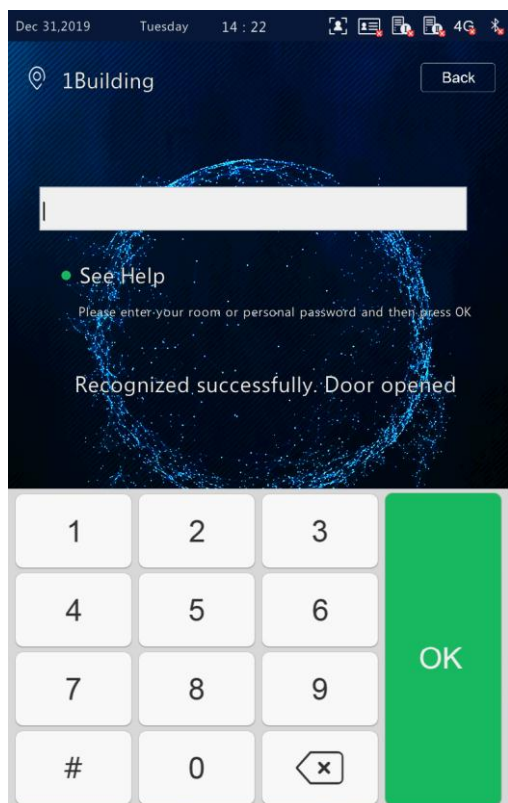
- Le password di apertura delle porte sono configurate sul monitor interno. Per i dettagli, consultare il *Manuale d'uso del monitor interno montato a parete*.

Figura 5-29 Interfaccia di apertura della porta tramite password



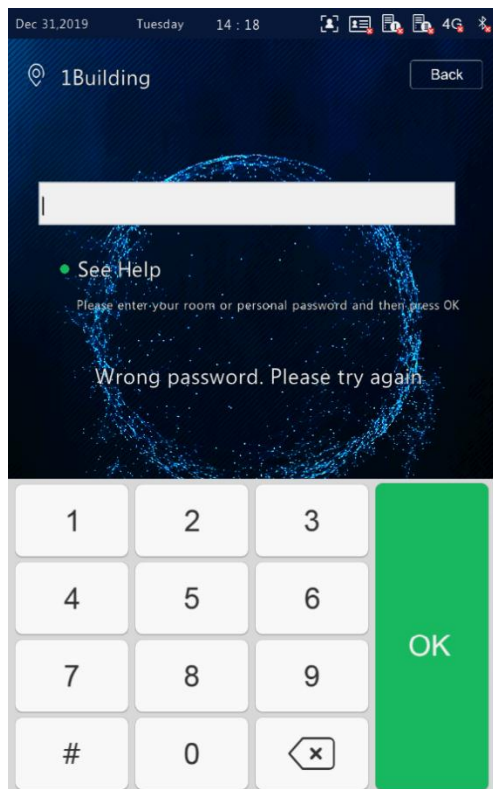
- La password è corretta e la porta è stata aperta con successo.
Dopo aver inserito una password corretta per la stanza, appare un'interfaccia come quella della figura sottostante e viene riprodotto il messaggio audio "Recognized Successfully".

Figura 5-30 Interfaccia di riconoscimento riuscito



- La password è errata e non è stato possibile aprire la porta.
Dopo aver inserito una password errata per la stanza, appare un'interfaccia come quella della figura sottostante e viene riprodotto il messaggio audio "Password authentication failed".

Figura 5-31 Interfaccia di password errata



2. Apertura della porta tramite password di amministratore

- (1) Toccare **Password** sull'interfaccia principale.
- (2) Nell'interfaccia visualizzata, immettere la password di amministratore come richiesto, quindi toccare **OK**.



NOTA!

Per le impostazioni della password amministratore, fare riferimento alla sezione [Password amministratore](#).

- La password amministratore è corretta e la porta è stata aperta con successo.
Per l'interfaccia e le indicazioni vocali, fare riferimento a [La password è corretta e la porta è stata aperta con successo](#).
- La password amministratore è errata e non è stato possibile aprire la porta.
Per l'interfaccia e le indicazioni vocali, fare riferimento a [La password è errata e non è stato possibile aprire la porta](#).

5.7.3 Apertura della porta tramite passaggio della scheda

- Le persone possono strisciare le loro schede sul terminale di controllo degli accessi con riconoscimento dei volti ET-B31H-M@B per aprire la porta.
- Quando un lettore di schede è connesso al terminale di riconoscimento volti, le persone possono strisciare le loro schede nell'apposita area di scansione per aprire la porta.



NOTA!

Le informazioni della scheda delle persone devono essere inviate in anticipo al terminale di riconoscimento dei volti.

5.7.4 Apertura porta con codice QR

Il terminale di riconoscimento volti supporta l'apertura della porta tramite codice QR.



- (1) Toccare sull'interfaccia principale per accedere all'interfaccia di scansione del codice QR.
- (2) Puntare il codice QR generato verso la fotocamera del terminale di riconoscimento dei volti o verso un dispositivo di scansione del codice QR collegato. Il riconoscimento andrà a buon fine e la porta si aprirà.



NOTA!

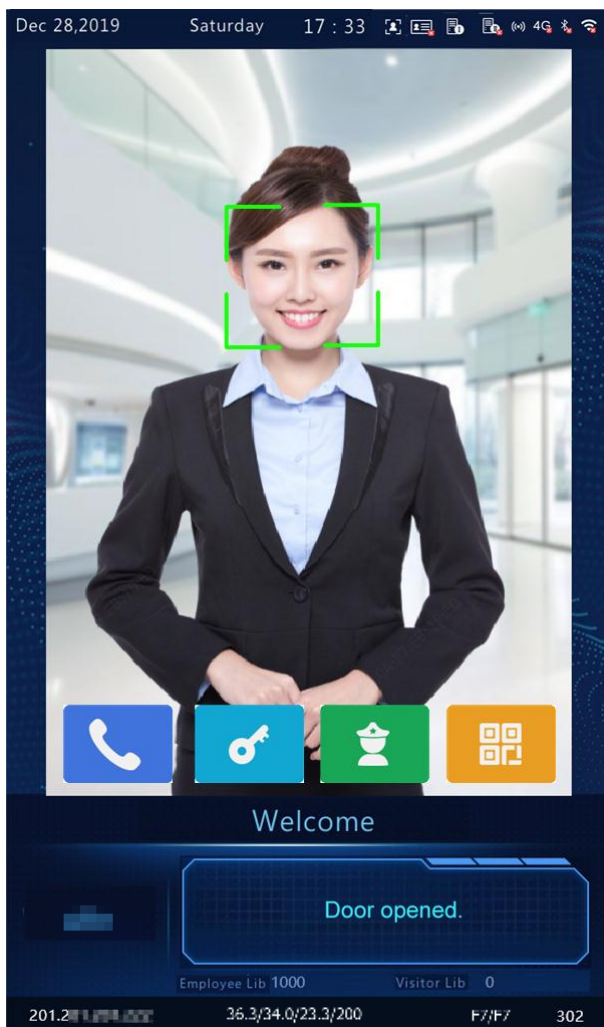
Se entro 30 secondi non viene eseguita alcuna operazione sull'interfaccia del codice QR, il terminale di riconoscimento dei volti passa automaticamente all'interfaccia di visualizzazione dal vivo.

5.7.5 Apertura da remoto

Dopo che la porta è stata aperta da remoto, il terminale di riconoscimento dei volti informa l'utente dell'apertura della porta mostrando e riproducendo un avviso.

Dopo che il terminale di riconoscimento dei volti è stato collegato ad un monitor interno e la configurazione è stata completata, è possibile eseguire operazioni sul monitor interno per aprire la porta da remoto. Per i dettagli, consultare il *Manuale d'uso del monitor interno montato a parete*.

Figura 5-32 Interfaccia di apertura della porta riuscita



6 Gestione del personale

6.1 Inserimento delle informazioni sul personale

Il terminale di riconoscimento dei volti supporta diversi metodi di immissione delle informazioni sul personale. Gli utenti possono selezionare un metodo appropriato in base agli scenari applicativi reali.

6.1.1 Importazione di informazioni nel terminale

È possibile importare informazioni utilizzando lo Strumento di importazione persone o inserendo le informazioni a livello locale.

1. Immissione locale

Il terminale di riconoscimento dei volti consente di inserire informazioni sul personale a livello locale. Per i dettagli, fare riferimento a [Gestione utenti](#).

2. Immissione nell'interfaccia Web

È possibile importare le informazioni sul personale nell'interfaccia Web del terminale di riconoscimento dei volti del videocitofono. Per i dettagli, fare riferimento a [Gestione del personale](#).

3. Importazione utilizzando lo strumento di importazione persone

Decomprimere **People Import Tool.7z** e importare le informazioni sul personale facendo riferimento al *Manuale operativo dello strumento di importazione delle persone (versione dettagliata)* e al *Manuale operativo dello strumento di importazione delle persone (versione semplificata)*.

6.2 Eliminazione del personale

1. Eliminazione tramite interfaccia Web

È possibile eliminare le informazioni sul personale nell'interfaccia Web del terminale di riconoscimento dei volti del videocitofono. Per i dettagli, fare riferimento a [Gestione del personale](#).

2. Eliminazione utilizzando lo strumento di importazione delle persone

Per i dettagli, fare riferimento a [Importazione utilizzando lo strumento di importazione persone](#).

7 Operazioni sul Web

7.1 Accesso

7.1.1 Operazioni preliminari

Installare il dispositivo facendo riferimento alla guida rapida del prodotto (inclusa nella fornitura). Collegare il dispositivo ad una fonte di alimentazione e avviarlo. La gestione e la manutenzione del videocitofono con terminale di riconoscimento dei volti possono essere eseguite in modalità visiva tramite il browser Web.

Di seguito viene utilizzato a titolo di esempio Internet Explorer 10.0 in esecuzione su Windows 7.0.

1. Prima di effettuare l'accesso, verificare quanto segue

- La connessione di rete tra il PC client e il terminale di riconoscimento dei volti è perfettamente funzionante.

- Sul computer in uso è installata la versione di Internet Explorer 10.0 o successive.
- La risoluzione è impostata su 1440 × 900 (Opzionale).

2. Aggiunta dell'indirizzo IP come sito attendibile

Figura 7-1 Impostazioni Internet

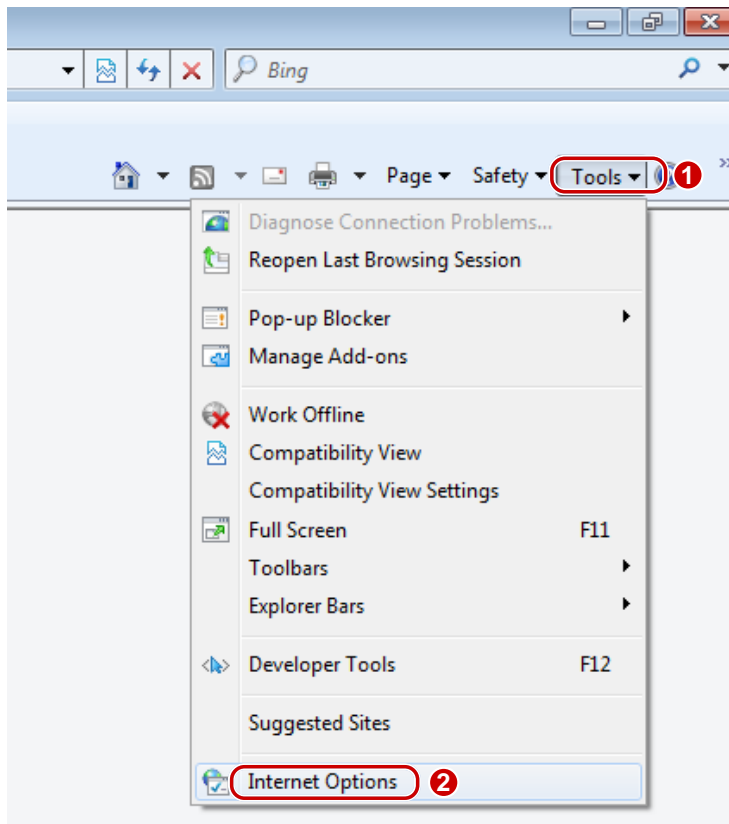
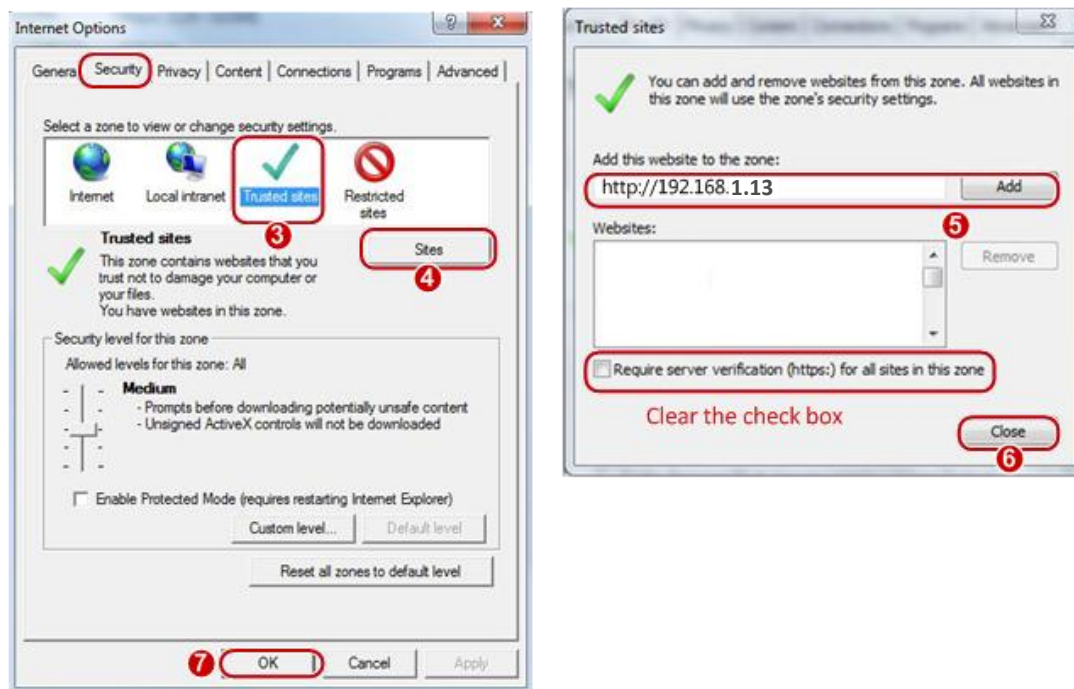


Figura 7-2 Aggiunta dell'indirizzo IP come sito attendibile





NOTA!

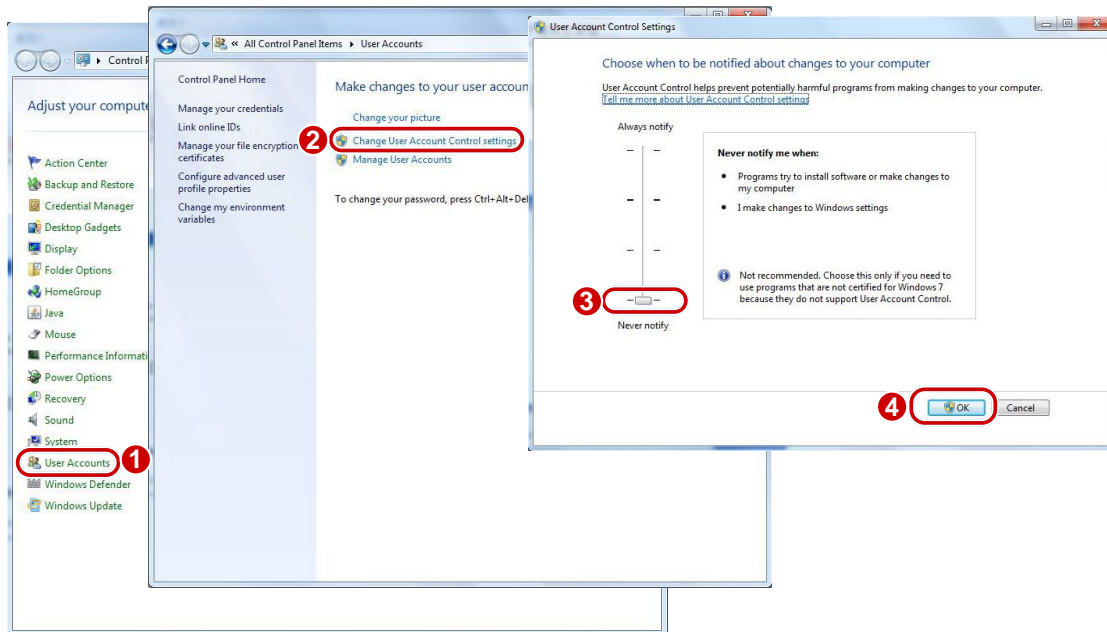
L'indirizzo IP 192.168.1.13 in questo esempio è l'indirizzo IP predefinito. Se è stato modificato, sostituirlo con l'indirizzo effettivo del terminale di riconoscimento dei volti.

3. Modifica delle impostazioni di controllo di accesso dell'utente (Opzionale)

Si consiglia di impostare l'autorizzazione di controllo utente al livello minimo prima di accedere al dispositivo.

Selezionare **Start > Pannello di controllo**. Nella schermata del **Pannello di controllo**, procedere come indicato di seguito per impostare al minimo l'autorizzazione di controllo utente.

Figura 7-3 Impostazione dell'autorizzazione di controllo



7.1.2 Accesso all'Interfaccia Web

L'indirizzo IP statico predefinito del dispositivo è 192.168.1.13. Il dispositivo supporta anche il login semplice utilizzando l'indirizzo IP 192.168.0.13 e la subnet mask 255.255.255.0.

Il protocollo di configurazione host dinamico (DHCP) è abilitato per impostazione predefinita sul dispositivo. Se nella rete viene utilizzato un server DHCP, l'indirizzo IP può essere assegnato dinamicamente. In questo caso, utilizzare l'indirizzo IP effettivo per l'accesso. Per le operazioni da eseguire quando viene assegnato un indirizzo IP dinamico, fare clic [qui](#) per un riferimento.

I passaggi per accedere all'interfaccia Web (Internet Explorer 10 a titolo esemplificativo) sono i seguenti:

- (1) Inserire l'indirizzo IP nella barra degli indirizzi del browser e premere **Invio**.
- (2) Quando si accede per la prima volta all'interfaccia Web viene visualizzata una richiesta di installazione del plug-in, come mostrato nella figura sottostante. Seguire le istruzioni sull'interfaccia per completare l'installazione del plug-in (tutti i browser devono essere chiusi a tal fine), riavviare Internet Explorer e accedere nuovamente al sistema.





NOTA!

- Per caricare manualmente ActiveX, digitare `http://IP address/ActiveX/Setup.exe` nella barra degli indirizzi e premere **Invio**.
- La password predefinita viene utilizzata per il primo accesso. Per garantire la sicurezza dell'account, modificare la password dopo il primo accesso. Si consiglia di impostare una password sicura (di almeno otto caratteri).
- Il dispositivo limita il numero di tentativi di accesso non riusciti per proteggere dall'accesso illegale. Dopo sei tentativi di accesso consecutivi non riusciti, il dispositivo si blocca automaticamente per 10 minuti.

(3) Inserire nome utente e password e quindi fare clic su **Login**.

Figura 7-4 Interfaccia di accesso

La tabella qui sotto descrive i parametri e i plug-in sull'interfaccia e la loro configurazione.

Tabella 7-1 Descrizione e configurazione dei parametri

Parametro/Plug-in	Descrizione	Configurazione
Nome utente/Password	<p>Nome utente e password per l'accesso all'Interfaccia Web.</p> <p>Al primo accesso: Il nome utente predefinito è admin e la password predefinita è 123456.</p> <p>La password per l'accesso dell'amministratore all'interfaccia Web è uguale a quella di attivazione. Se la password di attivazione è stata modificata, inserire la nuova password qui.</p>	Inserire il nome utente e la password in base alle condizioni reali.
Visualizzazione live	<ul style="list-style-type: none"> • Se selezionato, i video dal vivo vengono visualizzati su tutte le schermate di visualizzazione live dopo aver effettuato il login all'interfaccia Web. • Se deselezionato, i video in tempo reale vengono visualizzati solo dopo che la visualizzazione live è stata abilitata manualmente. Per informazioni dettagliate. 	<p>Impostare i parametri basandosi sulla situazione effettiva.</p> <p>In questo esempio è stato selezionato.</p>
Password dimenticata	/	/

Salva la password	Selezionando quest'opzione, al prossimo login è possibile effettuare il login direttamente senza inserire la password. Se la password viene modificata, non sarà possibile effettuare il login senza inserire la password. Si consiglia di non selezionare questa opzione per motivi di sicurezza.	In questo esempio non è stata selezionata.
Reset	Facendo clic su Reset , le caselle Username , Password e Save Password saranno cancellate. Altre caselle, ad es. quella della lingua e Live View non saranno reimpostate o cancellate.	/

7.2 Configurazione dei parametri

7.2.1 Funzioni comuni

1. Utenti

Il dispositivo supporta non più di un amministratore e un massimo di 32 utenti ordinari. Per impostazione predefinita, l'amministratore è **admin** (il nome dell'amministratore non può essere modificato) e dispone di tutte le autorizzazioni di gestione e funzionamento per il dispositivo e gli utenti. Gli utenti ordinari dispongono solo dell'autorizzazione di visualizzazione live per il dispositivo.

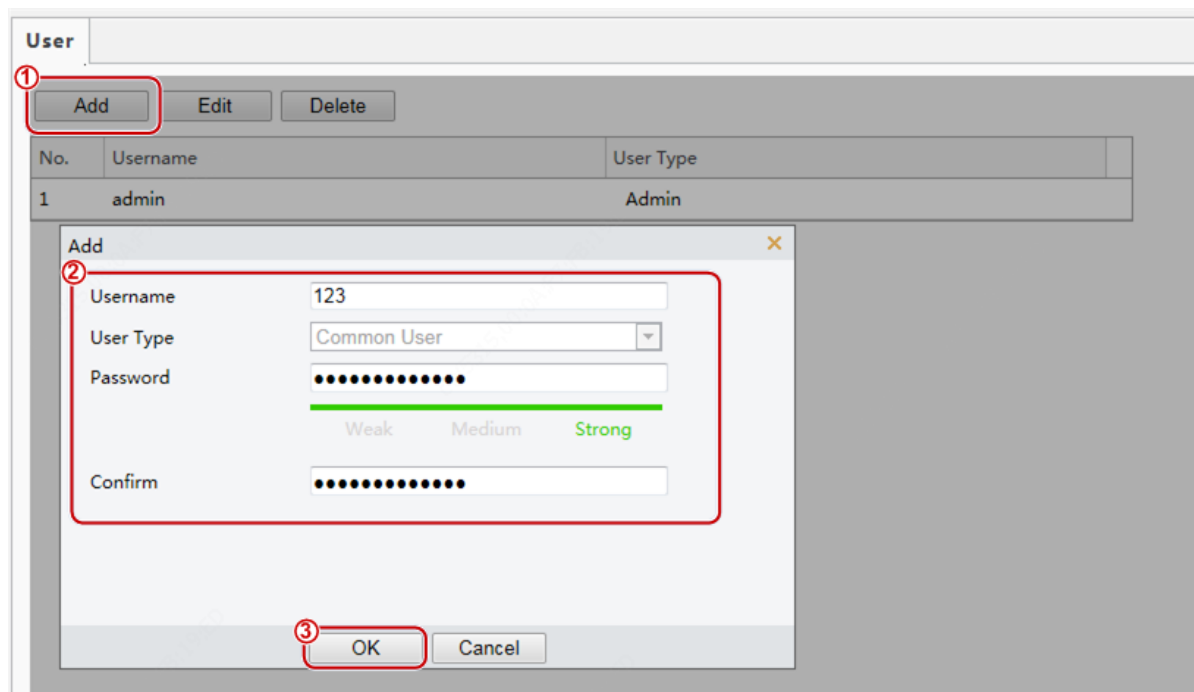
(1) Aggiunta di un utente ordinario

(1) Accedere all'interfaccia del terminale come **admin**.

(2) Selezionare **Setup > Common > User** per accedere all'interfaccia **User**.

(3) Seguire i passaggi illustrati nella figura qui sotto per aggiungere un utente ordinario.

Figura 7-5 Interfaccia di aggiunta utente ordinario



(2) Modifica di un utente ordinario

Di seguito viene utilizzato un utente ordinario a titolo di esempio. I passaggi per la modifica di utente **admin** sono gli stessi di quelli per la modifica di un utente ordinario.

- (1) Accedere all'interfaccia del terminale come **admin**.
- (2) Selezionare **Setup > Common > User** per accedere all'interfaccia **User**.
- (3) Selezionare l'utente ordinario che si desidera modificare e seguire i passaggi illustrati nella figura sottostante per modificare le informazioni sull'utente.

Figura 7-6 Interfaccia di modifica delle informazioni su un utente ordinario

The screenshot shows a 'User' management window with three buttons: 'Add', 'Edit', and 'Delete'. The 'Edit' button is circled with a red circle containing the number '2'. Below the buttons is a table with two columns: 'No.' and 'User Type'. The table contains two rows: row 1 with 'admin' and 'Admin', and row 2 with '123' and 'Common User'. Row 2 is highlighted with a red box and a red circle containing the number '1'. Below the table is an 'Edit' dialog box with the following fields: 'Username' (containing '123'), 'User Type' (a dropdown menu set to 'Common User'), 'Password' (with a strength indicator showing 'Weak', 'Medium', and 'Strong'), and 'Confirm'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

- (4) Dopo aver modificato le informazioni, fare clic su **OK** per salvare le informazioni sull'utente.

(3) Eliminazione di un utente ordinario

- (1) Accedere all'interfaccia del terminale come **admin**.
- (2) Selezionare **Setup > Common > User** per accedere all'interfaccia **User**.
- (3) Selezionare l'utente ordinario che si desidera eliminare e seguire i passaggi illustrati nella figura sottostante per eliminarlo.

Figura 7-7 Interfaccia di eliminazione utente ordinario

The screenshot shows the 'User' management window with three buttons: 'Add', 'Edit', and 'Delete'. The 'Delete' button is circled with a red circle containing the number '2'. Below the buttons is a table with two columns: 'No.' and 'User Type'. The table contains two rows: row 1 with 'admin' and 'Admin', and row 2 with '123' and 'Common User'. Row 2 is highlighted with a red box and a red circle containing the number '1'.



NOTA!

- Solo l'utente **admin** può modificare le password. Quando si modifica il nome o la password di un utente, se l'utente ha effettuato l'accesso al sistema, sarà costretto a disconnettersi e dovrà inserire il nuovo nome o la nuova password per effettuare l'accesso la prossima volta.
- Solo l'utente **admin** può eliminare gli utenti esistenti. Dopo che un utente è stato eliminato, non può più effettuare l'accesso. Se l'utente ha effettuato l'accesso al sistema prima dell'eliminazione, sarà costretto a disconnettersi.
- La password di accesso all'interfaccia Web dell'utente **admin** è identica alla password di attivazione. Se la password di accesso di **admin** è stata modificata, utilizzare la nuova password per accedere all'interfaccia [Configurazione Attivazione](#).

2. Porte e dispositivi

(1) Porta Seriale

Quando il terminale per il riconoscimento dei volti esegue la gestione O&M su una macchina di controllo attraverso una porta seriale o si collega ad un lettore di carte d'identità, è necessario configurare le informazioni della porta seriale. Attenersi alla procedura seguente per configurare una porta seriale:



NOTA!

L'interfaccia di configurazione della porta seriale varia a seconda del tipo di dispositivo.

(1) Selezionare **Setup > Common > Ports & Devices**, quindi fare clic sulla scheda **Serial Port**.

Figura 7-8 Interfaccia di configurazione della porta seriale

Serial Port	Wiegand Interface	IO Configuration	Volume Control	Illumination	USB
RS485_1					
Port Mode	Security/Temperature ▾				
RS485_1	<input type="checkbox"/> Enable Security Module				
RS485 Address	0 ▾				
Baud Rate	115200 ▾				
Data Bits	8 ▾				
Stop Bits	1 ▾				
Parity	None ▾				
Flow Control	None ▾				
<input type="checkbox"/> Enable Trans-Channel					
<input type="button" value="Save"/>					
RS232_1					
Port Mode	IC Card Mode ▾				
Baud Rate	19200 ▾				
Data Bits	8 ▾				
Stop Bits	1 ▾				
Parity	None ▾				
Flow Control	None ▾				
<input type="checkbox"/> Enable Trans-Channel					

Tabella 7-2 Descrizione e configurazione dei parametri

Parametro	RS485_1	RS232_1
Modalità porta	<ul style="list-style-type: none"> Modulo di sicurezza: Selezionare questa opzione quando il terminale di riconoscimento dei volti si connette a un modulo di rilevamento digitale tramite la porta seriale RS485. Modalità Controllo C: selezionare questa opzione quando è richiesta la gestione O&M per macchine di controllo collegate al terminale di riconoscimento dei volti tramite la porta seriale RS485. Solo la macchina di controllo FG8223 supporta questa opzione. Modalità Controllo B: le correnti macchine di controllo non supportano questa opzione. Nessuno: Selezionare quest'opzione quando nessun dispositivo esterno è collegato o i dispositivi esterni non necessitano di gestione O&M. Modalità magnete porta: selezionare quest'opzione quando il terminale di riconoscimento dei volti si collega a un magnete porta attraverso la porta seriale RS485. <p>Impostare i parametri basandosi sullo scenario effettivo.</p> <p>Nota: La funzione del modulo di sicurezza non è attualmente applicabile.</p>	<ul style="list-style-type: none"> Modalità carta d'identità: selezionare quest'opzione quando il terminale di riconoscimento dei volti si connette a un lettore di carte d'identità. Modalità codice QR: selezionare quest'opzione quando il terminale di riconoscimento dei volti si connette a un lettore codice QR. Modalità IC Card: quest'opzione viene visualizzata quando il terminale di riconoscimento dei volti dispone di un lettore di schede integrato. Modalità Two-to-One: selezionare quest'opzione quando il terminale di riconoscimento dei volti si connette a un lettore di IC Card (Modello: EG121@ID). Modalità Controllo A: selezionare questa opzione quando è richiesta la gestione O&M per macchine di controllo collegate al terminale di riconoscimento dei volti tramite la porta seriale RS232. Le macchine di controllo FG6221, FG8221 e FG8222 supportano questa modalità. Modalità Controllo D: selezionare questa opzione quando è richiesta la gestione O&M per macchine di controllo collegate al terminale di riconoscimento dei volti tramite la porta seriale RS232. (le macchine di controllo EL-S802, EL-S801, EL-S601, EL-B602, EL-B501, DEL-811, DEL-611 e DEL-511 supportano questa modalità.) Non configurato: Selezionare quest'opzione quando nessun dispositivo esterno è collegato o i dispositivi esterni non necessitano di gestione O&M. Modalità Bluetooth: quest'opzione viene visualizzata quando il terminale di riconoscimento dei volti viene utilizzato con una serratura smart tramite Bluetooth. Modalità IC Card Wiegand: selezionare quest'opzione quando il terminale di riconoscimento dei volti è collegato a un lettore di schede tramite RS232. <p>Impostare i parametri basandosi sullo scenario effettivo.</p>
	NOTA! Per le porta seriali RS485 e RS232, la Modalità Porta non può essere impostata contemporaneamente su una modalità controllo.	
Abilita Modulo di Sicurezza	La configurazione non è supportata.	/
Indirizzo RS485	La configurazione non è supportata.	/
Velocità in baud	La configurazione non è supportata. Utilizzare il valore predefinito.	

Bit di dati/Bit di stop/Parità/Controllo di flusso	Mantenere i valori predefiniti come segue: Bit di Dati: 8 Bit di stop: 1 Parità: Nessuna Controllo di flusso: Nessuna NOTA! I parametri non possono essere impostati quando Port Mode è impostato su IC Card Mode .
Abilita Trans-Canale	Viene utilizzato per il debug interno. Ignorarlo.

(2) Configurare le informazioni della porta seriale in base alla configurazione della scena reale.

(3) Fare clic su **Save** per completare la configurazione della porta seriale.

(2) Interfaccia Wiegand

Quando il terminale di riconoscimento dei volti è collegato a un lettore di schede IC, è necessario configurare le informazioni dell'interfaccia Wiegand. Eseguire le seguenti operazioni per completare la configurazione:

(1) Selezionare **Setup > Common > Ports & Devices** e fare clic sulla scheda **Wiegand Interface**.



NOTA!

- Alcuni dispositivi supportano l'ingresso attraverso una sola interfaccia Wiegand o zero interfacce Wiegand; inoltre, la schermata di configurazione per l'interfaccia di ingresso Wiegand varia a seconda dei dispositivi.
- Alcuni dispositivi non supportano l'uscita attraverso l'interfaccia Wiegand. In questo caso la schermata di configurazione dell'interfaccia di uscita di Wiegand non viene visualizzata.
- La schermata di configurazione dell'interfaccia Wiegand non è disponibile per ET-B31H-M@B con un lettore di schede IC integrato.

Figura 7-9 Schermata di configurazione dell'interfaccia Wiegand

Wiegand Input_1		Wiegand Output_1	
Protocol	Wiegand 26	Protocol	None
Format	Ascending O	Format	Ascending O

(2) Configurare le informazioni dell'interfaccia Wiegand facendo riferimento alla tabella qui sotto.

Tabella 7-3 Descrizione e configurazione dei parametri

Parametro	Configurazione
Protocollo	Impostarlo su Wiegand 26 o Wiegand 34 in base agli scenari attuali.
Formato	<p>Le opzioni sono le seguenti:</p> <ul style="list-style-type: none"> Ordine ascendente La sequenza del numero di scheda letta dal lettore di schede (EG121@IC) è la sequenza positiva. Quando la sequenza è identica a quella del numero di scheda letta dal lettore di schede, selezionare Ascending Order nell'ingresso/uscita. Ordine decrescente Quando la sequenza è opposta alla sequenza del numero della scheda letta dal lettore di schede, selezionare Descending Order nell'ingresso/uscita. <p>Il valore predefinito è Ascending Order. Impostare i parametri basandosi sullo scenario effettivo.</p>

(3) Fare clic su **Save** per completare la configurazione dell'interfaccia Wiegand.

(3) Configurazione IO

Il terminale di riconoscimento dei volti si collega alle macchine di controllo, alle serrature delle porte o ai pulsanti di controllo degli accessi e invia loro il segnale di apertura della porta. Eseguire le seguenti operazioni per completare la configurazione:

(1) Selezionare **Setup > Common > Ports & Devices** e fare clic sulla scheda **IO Configuration**.



NOTA!

- Alcuni dispositivi supportano l'uscita da una sola porta IO o da zero porte IO; l'interfaccia di configurazione della porta IO varia a seconda dei dispositivi.
- Alcuni dispositivi non supportano le serrature delle porte o i pulsanti di controllo dell'accesso; l'interfaccia di configurazione della porta IO varia a seconda dei dispositivi.

Figura 7-10 Interfaccia di configurazione IO

ID	Enable	Type	Level Value	Pulse Width
F1	<input checked="" type="checkbox"/>	Door Lock	Low Level	30 s
F2	<input checked="" type="checkbox"/>	Door Button	Low Level	500 ms

Access Control

Unlock Interval s

Door Opening Timeout s

Auto Door Lock Upon C... On Off


Check Door Magnet Sta... On Off

Door Magnet Check Time Before Door Closing After Door Closing

Save

(2) Configurare le informazioni della porta IO facendo riferimento alla tabella qui sotto.

Tabella 7-4 Descrizione e configurazione dei parametri

Parametro	Descrizione e configurazione dei parametri
F1/F2	<p>F1/F2 indica la porta IO del terminale di riconoscimento dei volti. Selezionare la casella di controllo nella parte anteriore. In questo modo, la configurazione della porta IO diventerà effettiva.</p> <p>Le porte IO supportano i seguenti tipi di dispositivi esterni:</p> <ul style="list-style-type: none"> Serratura porta: Il terminale di riconoscimento dei volti emette segnali di apertura porta alle serrature delle porte attraverso una porta IO. Pulse Width si riferisce qui alla durata dell'apertura di una porta. Quando la durata di apertura della porta supera questo valore, il magnete della porta attiva un allarme. Intervallo di valori: [1–300] s; Valore predefinito: 5 s Pulsante porta: Il terminale di riconoscimento dei volti può ricevere il segnale di apertura porta dal pulsante di controllo degli accessi attraverso una porta IO e invia il segnale di apertura porta alla serratura della medesima. Il valore di ampiezza dell'impulso indica che un segnale di apertura porta valido viene generato solo quando il tempo in cui il pulsante di apertura porta viene tenuto premuto raggiunge il valore qui indicato. Intervallo di valori: [0–20000] ms; Valore predefinito: 100 ms <p>Level Value può essere impostato su Low Level o High Level. Il valore deve essere coerente con il livello del segnale di ingresso e di uscita supportato da dispositivi esterni.</p>
Intervallo di sblocco	<p>Indica l'intervallo tra due operazioni di sblocco. Una volta sbloccata, la porta non verrà sbloccata nuovamente entro l'intervallo di sblocco, anche se viene ricevuto un nuovo segnale di sblocco. Inoltre, la durata di apertura della porta della serratura non sarà ricalcolata. Se impostato su 0, lo sblocco della porta viene attivato ogni volta che viene ricevuto il segnale di sblocco e la durata di apertura della porta della serratura viene ricalcolata.</p> <p>Intervallo di valori: [0–300] s; Valore predefinito: 0 s</p>
Timeout apertura porta	<p>Dopo aver abilitato il Blocco porta automatico alla chiusura, se il tempo di chiusura della porta supera il valore qui indicato e il magnete della porta rileva che quest'ultima si trova in posizione chiusa, il terminale di riconoscimento dei volti blocca automaticamente la porta.</p> <p>Intervallo di valori: [1–300] s; Valore predefinito: 10 s</p> <p> NOTA!</p> <ul style="list-style-type: none"> Non è consigliabile impostarlo su un valore molto basso. In caso contrario, la normale apertura della porta risulterà compromessa. La creazione di un allarme magnete porta dipende dal timeout di apertura della porta.
Blocco porta automatico alla chiusura	<p>Selezionare se abilitare o meno il blocco porta automatico al momento della chiusura della porta.</p> <p>Le opzioni sono le seguenti:</p> <ul style="list-style-type: none"> On: quando il magnete della porta rileva che la porta è chiusa e il tempo di chiusura della porta supera il valore Timeout apertura porta, la porta verrà automaticamente bloccata. Non attiva: il blocco porta automatico alla chiusura è disattivato e il tempo di chiusura della porta è la durata di apertura della porta.
Verificare lo stato del magnete della porta prima della chiusura	<p>Le opzioni sono le seguenti:</p> <ul style="list-style-type: none"> On: Lo stato del magnete della porta viene controllato prima della chiusura. Non attiva: Lo stato del magnete della porta non viene controllato prima della chiusura.
Tempo di verifica magnete porta	<p>Questo parametro è disponibile solo dopo che Verificare lo stato del magnete della porta prima della chiusura è stato impostato su On. Impostare questo parametro in base al tipo di serratura.</p> <ul style="list-style-type: none"> Prima della chiusura della porta: selezionare quest'opzione per serrature elettroniche. Dopo la chiusura della porta: selezionare quest'opzione per serrature elettromagnetiche.

(3) Fare clic su **Save** per completare la configurazione della porta IO.

(4) Audio

Se il terminale di riconoscimento dei volti è collegato a un dispositivo audio, configurare le informazioni pertinenti nella scheda **Audio**.

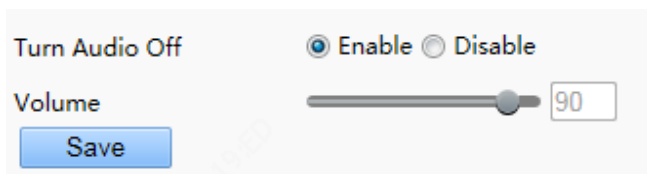
(1) Selezionare **Setup > Common > Ports & Devices** e fare clic sulla scheda **Audio**.



NOTA!

Questa funzione non è supportata da alcuni modelli. Fare riferimento al modello effettivo per i dettagli.

Figura 7-11 Interfaccia di configurazione audio



(2) Impostare se disattivare l'audio. In caso negativo, impostare il volume di riproduzione.

(3) Fare clic su **Save** per completare la configurazione audio.

(5) Illuminazione



NOTA!

Questa funzione non è supportata da alcuni modelli. Fare riferimento al modello effettivo per i dettagli.

(1.1) Luce LCD

Configurare la luce LCD per il terminale di riconoscimento dei volti nella scheda **Illumination**.



NOTA!

dispositivi non supportano la configurazione della luce LCD; in tal caso, l'area **LCDLight** non verrà visualizzata.

(1) Selezionare **Setup > Common > Ports & Devices** e fare clic sulla scheda **Illumination**.

(2) Impostare la luce LCD come desiderato.

Figura 7-12 Interfaccia di configurazione della luce LCD



Spia di stato	Operazioni
Luce bianca	<p>Quando il terminale di riconoscimento dei volti è in modalità standby, la luce LCD è bianca.</p> <ul style="list-style-type: none"> On: La luce LCD è bianca quando il terminale di riconoscimento volti è in modalità standby. Non attiva: La luce LCD non si illumina di bianco quando il terminale di riconoscimento volti è in modalità standby.
Luce verde	<p>La luce LCD del terminale di riconoscimento volti è verde in caso di passaggio normale.</p> <ul style="list-style-type: none"> On: La luce LCD del terminale di riconoscimento volti è verde in caso di passaggio normale. Non attiva: La luce LCD del terminale di riconoscimento volti non si illumina di verde in caso di passaggio normale.
Luce rossa	<p>La luce LCD del terminale di riconoscimento volti si illumina di rosso quando si verifica un'eccezione durante il passaggio del personale.</p> <ul style="list-style-type: none"> On: La luce LCD del terminale di riconoscimento volti si illumina di rosso quando si verifica un'eccezione durante il passaggio del personale. Non attiva: La luce LCD del terminale di riconoscimento volti non si illumina di rosso quando si verifica un'eccezione durante il passaggio del personale.

(3) Fare clic su **Save** per completare la configurazione della luce LCD.

(1.2) Risparmio energetico

Il terminale di riconoscimento volti supporta la configurazione di risparmio energetico della luce.

(1) Selezionare **Setup > Common > Ports & Devices** e fare clic sulla scheda **Illumination**.

(2) Impostare i parametri di risparmio energetico in base ai requisiti effettivi.

Figura 7-13 Interfaccia di configurazione del risparmio energetico

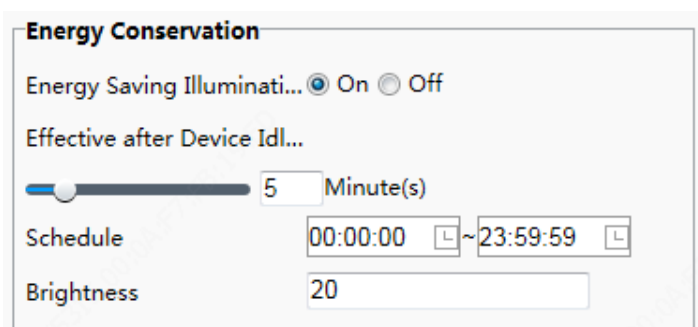



Tabella 7-5 Descrizione e configurazione dei parametri

Parametro	Descrizione	Configurazione
Illuminazione con risparmio energetico	<ul style="list-style-type: none"> On: Quando il terminale di riconoscimento volti rileva un volto durante l'intervallo di tempo impostato in Programma, tutte le luci (inclusa la luce LCD, la schermata del display e la lampada di illuminazione supplementare) sono accese (solo quando la luminosità della luce ambientale corrente non raggiunge la soglia minima di luminosità del dispositivo). Quando non viene rilevato alcun volto all'interno del valore preimpostato Effettivo dopo che il dispositivo è rimasto inattivo per, le luci si spengono gradualmente (solo quando la luminosità della luce ambientale corrente supera la soglia di luminosità massima del dispositivo). Le luci restano accese al di fuori dell'intervallo impostato in Programma a prescindere dal rilevamento di un volto da parte del terminale di riconoscimento volti. Non attiva: le luci sono accese in modo fisso indipendentemente dal fatto che il terminale di riconoscimento facciale rilevi o meno un volto. Il risparmio energetico per le luci è disattivato. 	Impostare i parametri basandosi sullo scenario effettivo.

	L'illuminazione con risparmio energetico è disattivato per impostazione predefinita.	
Effettivo dopo che il dispositivo è rimasto inattivo per	Tempo in cui il terminale di riconoscimento facciale non rileva un volto. Se il tempo supera questo valore, le luci del terminale di riconoscimento volti si spegneranno gradualmente. Intervallo di valori: [1–30] min; valore predefinito: 5 min	Impostare i parametri basandosi sullo scenario effettivo.
Programma	Quando l'opzione Illuminazione con risparmio energetico viene impostata su On, il terminale di riconoscimento volti applica l'illuminazione a risparmio energetico all'interno del programma. L'illuminazione a risparmio energetico non viene impiegata al di fuori del programma. Il valore varia da 00:00:00 a 23:59:59 e l'unità può essere impostata con una precisione al secondo.  NOTA! Quando l'opzione Illuminazione con risparmio energetico viene impostata su On, il valore predefinito di Schedule è [00:00:00~23:59:59]. Quando l'opzione Illuminazione con risparmio energetico viene impostata su Off, la voce Schedule non è disponibile.	Impostare i parametri basandosi sullo scenario effettivo.
Luminosità	Questo parametro viene utilizzato per regolare la luminosità della lampada di illuminazione supplementare quando lo schermo è spento. Un valore più elevato indica un aumento nella luminosità della lampada di illuminazione supplementare e viceversa. Intervallo di valori: [0-200]; valore predefinito: 20 Se il parametro è impostato su 0 , la lampada di illuminazione supplementare viene spenta. Le modifiche della luminosità avranno effetto solamente quando lo schermo si spegnerà nuovamente.	Impostare i parametri basandosi sullo scenario effettivo.

(3) Fare clic su **Save** per completare la configurazione del risparmio energetico.

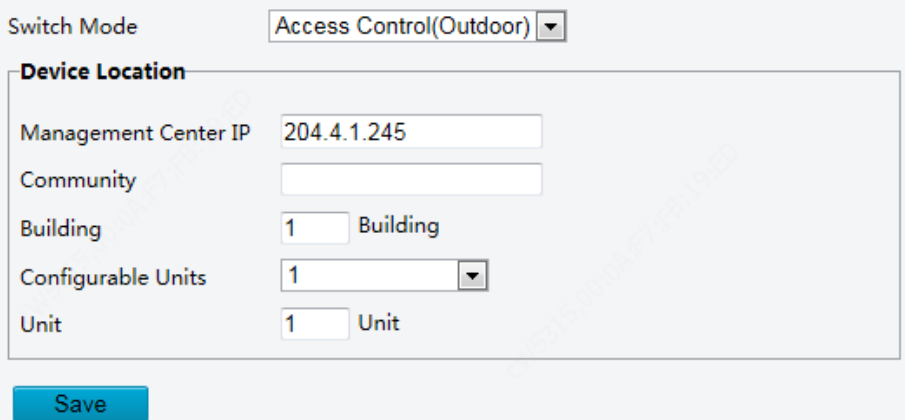
3. Info Dispositivo

L'interfaccia **Device Info** consente di configurare la posizione attuale del dispositivo.

(1) Accedere all'interfaccia del terminale come **admin**.

(2) Selezionare **Setup > Common > Device Info** per accedere all'interfaccia **Device Info**.

Figura 7-14 Interfaccia Configurazione Informazioni Dispositivo



Switch Mode: Access Control(Outdoor) ▼

Device Location

Management Center IP: 204.4.1.245

Community:


Building: 1 Building

Configurable Units: 1 ▼

Unit: 1 Unit

Save

Tabella 7-6 Descrizione e configurazione dei parametri

Parametro	Descrizione e configurazione dei parametri
Cambia modalità	<p>Impostare la modalità di lavoro per il terminale di controllo degli accessi. Sono incluse le seguenti opzioni:</p> <ul style="list-style-type: none"> Controllo degli accessi (esterno): dispositivo di controllo degli accessi normale, che prevede la chiamata, l'apertura della porta tramite password, l'apertura della porta tramite scansione del volto e altre funzionalità. Controllo degli accessi normale: il terminale di controllo degli accessi è un normale dispositivo di controllo degli accessi che non supporta le funzioni di chiamata e di apertura della porta tramite password. Per informazioni dettagliate, consultare il <i>Manuale d'Uso del Terminale di Riconoscimento Volti</i>. <p>Impostare questo parametro in base agli scenari applicativi reali.</p>
Indirizzo IP centro di gestione	<p>Digitare qui l'indirizzo IP del centro di gestione.</p> <p>Una volta effettuata la configurazione, un utente può toccare Call Management Center sull'interfaccia grafica per chiamare il centro di gestione.</p> <p> NOTA!</p> <p>L'indirizzo IP del centro di gestione deve trovarsi nello stesso segmento di rete del dispositivo.</p>
Comunità	<p>Immettere il nome della comunità a cui appartiene il dispositivo.</p> <p>È possibile inserire da 1 a 36 caratteri (da 1 a 12 caratteri cinesi).</p>
Edificio	<ul style="list-style-type: none"> Inserire il numero dell'edificio in cui si trova il dispositivo. Il valore deve essere un numero intero compreso tra 1 e 99.
Unità configurabili	<p>Selezionare il numero di unità che possono essere servite dal dispositivo dall'elenco a discesa.</p> <p>Le opzioni possibili sono 0, 1, 2 e 3.</p>
Unità	<p>Inserire il numero dell'unità in cui si trova il dispositivo.</p> <p>Il valore è un numero intero compreso tra 0 e 9.</p>



NOTA!

Modificare il tipo di dispositivo causerà il riavvio del dispositivo e il ripristino della configurazione predefinita per la modalità di autenticazione.

4. Personalizzazione

(1) Modalità annuncio

Il terminale di riconoscimento volti supporta gli annunci (solamente immagini). Seguire la procedura che segue per la configurazione:

- Selezionare **Setup > Common > Personalization** e fare clic sulla scheda **Ad Mode**.
- Impostare la modalità annuncio facendo riferimento alla tabella qui in basso.

Figura 7-15 Interfaccia Impostazione modalità annuncio

Tabella 7-7 Configurazione dei parametri

Parametro	Descrizione e configurazione
Modalità annuncio	<ul style="list-style-type: none"> • Attiva • Non attiva Selezionare se attivare la modalità annuncio in base alla situazione effettiva.
Intervallo Riproduzione Immagine Annuncio (s)	Impostare l'intervallo per la riproduzione delle immagini. Il valore è un numero intero compreso tra 1 e 3600 s. Il valore predefinito è 10 s.
Tempo Standby (s)	Il terminale di riconoscimento volti entrerà in modalità annuncio quando non rileva un volto per il tempo impostato in questa sezione. Il valore è un numero intero compreso tra 10 e 3600 s. Il valore predefinito è 10 s. Il terminale di riconoscimento volti uscirà dalla modalità annuncio quando la scansione di un volto non riesce o un utente tocca lo schermo.
Importa File Immagine	Gli utenti possono scegliere le immagini degli annunci. Le immagini devono rispondere a questi requisiti: <ul style="list-style-type: none"> • Il file da importare deve avere estensione .zip. Il file può contenere un massimo di tre immagini .bmp, il cui nome deve essere 1.bmp, 2.bmp e 3.bmp. • Formato delle immagini: le immagini devono essere file .bmp a 32-bit, con dimensioni pari a 480 x 800.

(3) Fare clic su **Save** per completare la configurazione della modalità annuncio.

(2) Avviso e logo personalizzati

Il terminale di riconoscimento volti supporta avvisi e loghi personalizzati. Seguire la procedura che segue per la configurazione:

(1) Selezionare **Setup > Common > Personalization** e fare clic sulla scheda **Custom Logo and Prompt**.

(1) Impostare il logo e l'avviso personalizzati facendo riferimento alla tabella qui in basso.

Figura 7-16 Interfaccia Avviso e logo personalizzati

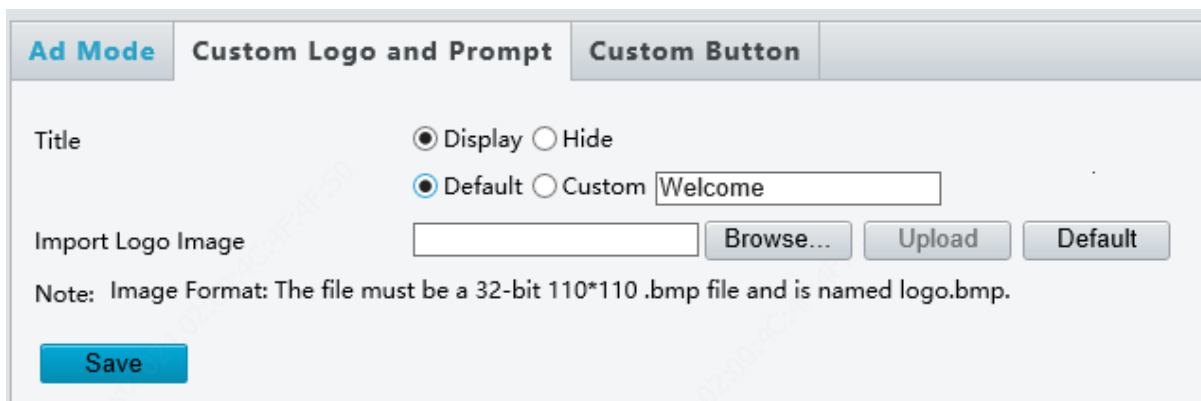


Tabella 7-8 Configurazione dei parametri

Parametro	Descrizione e configurazione
Titolo	<ul style="list-style-type: none"> • Display: la barra del titolo viene visualizzata. Il titolo può essere impostato nel modo seguente: <ul style="list-style-type: none"> ➤ Predefinito: la barra del titolo mostra la scritta "Benvenuto". ➤ Personalizzato: è possibile scegliere il titolo. Inserire una stringa contenente da 0 a 14 caratteri. • Nascondi: la barra del titolo non viene visualizzata.
Importa Immagine Logo	<p>Gli utenti possono scegliere l'immagine del logo. L'immagine del logo deve rispondere ai seguenti requisiti: deve trattarsi di un'immagine .bmp a 32-bit, con dimensioni pari a 110 x 110 e il nome logo.bmp.</p>

(2) Fare clic su **Save** per completare la configurazione del logo e dell'avviso personalizzati.

(3) Pulsanti personalizzati

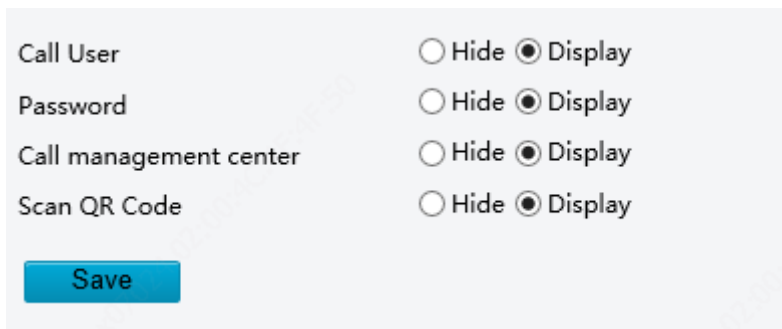
Il terminale di riconoscimento volti supporta la personalizzazione dei pulsanti. Seguire la procedura che segue per la configurazione:

(1) Selezionare **Setup > Common > Ports & Devices** e fare clic sulla scheda **Custom Button**.

(2) Definire i pulsanti in base agli scenari applicativi.

- Display: il pulsante viene visualizzato sull'interfaccia grafica.
- Nascondi: il pulsante non viene visualizzato sull'interfaccia grafica.

Figura 7-17 Interfaccia Pulsanti personalizzati



(3) Fare clic su **Save** per completare la configurazione della personalizzazione dei pulsanti.

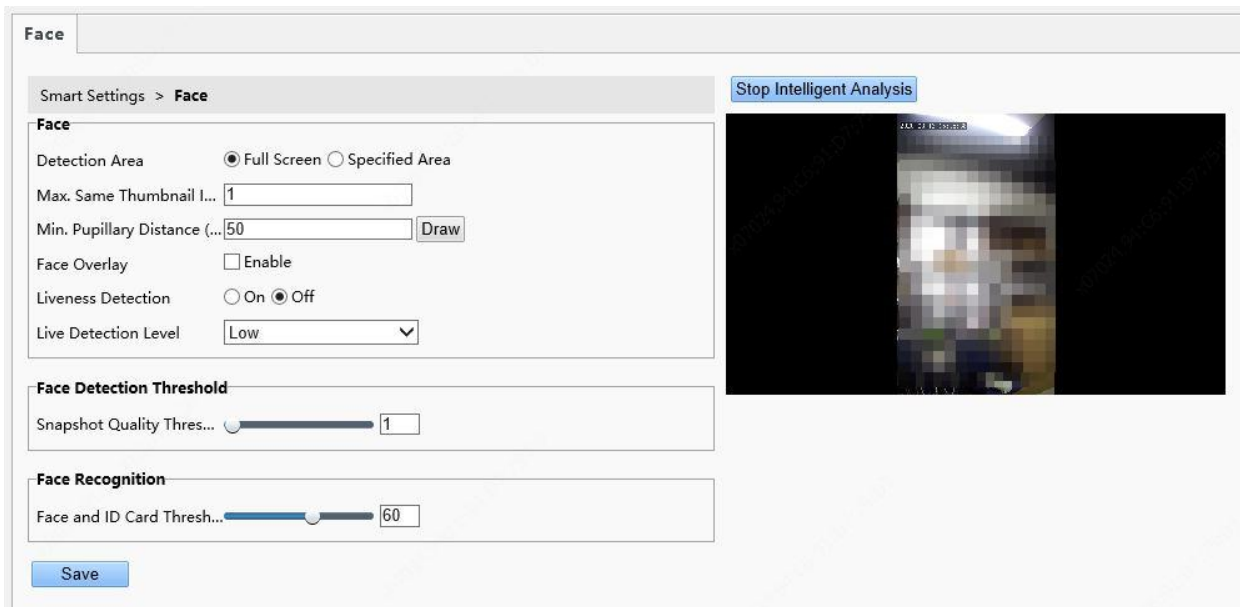
7.2.2 Intelligente

1. Istantanea volto

La configurazione della funzione istantanea volto comprende vari parametri, tra cui il rilevamento dei volti, la soglia di rilevamento dei volti, filtra per dimensioni oggetto (px) e altri. La corretta configurazione di questi parametri è essenziale per rilevare e riconoscere i volti.

(1) Selezionare **Setup > Intelligente > Face** e fare clic sulla scheda **Face**.

Figura 7-18 Interfaccia Configurazione istantanea volto



(2) Impostare i parametri facendo riferimento alla tabella qui sotto.

L'analisi intelligente è attiva per impostazione predefinita. Per cambiare i parametri dell'interfaccia, fare clic su **Stop Intelligent Analysis** per interrompere l'analisi intelligente e procedere con le modifiche.

Tabella 7-9 Descrizione e configurazione dei parametri

Pannello	Parametro	Descrizione e configurazione
Volto	Area di rilevamento	<ul style="list-style-type: none"> Fare clic su Full Screen per far sì che venga rilevata la foto del volto a schermo intero. Fare clic su Specified Area per far sì che i volti vengano rilevati all'interno di un'area selezionata.
	Max. Same	Il parametro non è al momento disponibile.
	Distanza pupillare min. (px)	È possibile tracciare la distanza pupillare utilizzando il mouse nella visualizzazione live sul lato destro dell'interfaccia. Verrà acquisita una foto solamente se il valore di Min. Pupillary Distance(px) è all'interno dell'intervallo preimpostato. L'intervallo va da 20 a 150 px.
	Sovrapposizione volto	La configurazione non è supportata.
	Rilevamento contraffazioni	Fare clic su On per attivare la funzione di rilevamento contraffazioni. Questa funzionalità è in grado di prevenire in modo efficace la contraffazione di foto e video. L'opzione è attiva per impostazione predefinita.
	Livello di rilevamento persone reali	L'opzione ha tre livelli di impostazione: High , Medium e Low . Un livello più elevato aumenta la precisione con la quale vengono rilevate le persone non reali. Il valore predefinito è Low .

Soglia di rilevamento volti	Soglia qualitativa istantanea	<p>Soglia per la corrispondenza 1:N delle istantanee dei volti.</p> <p>Quando la somiglianza di un volto raggiunge il valore preimpostato, la corrispondenza risulta positiva.</p> <p>Intervallo di valori: [1-100]; valore predefinito: 1</p> <p>Nota: Quando l'opzione Rilevamento mascherina viene attivata, il parametro Snapshot Quality Threshold deve essere impostato su 1.</p>
Riconoscimento di volti	Soglia volti e carta d'identità	<p>Soglia per la corrispondenza 1:1 delle carte d'identità.</p> <p>Quando la somiglianza fra l'istantanea di un volto e la foto sulla carta d'identità raggiunge il valore preimpostato, la corrispondenza risulta positiva.</p> <p>Intervallo di valori: [1-100]; valore predefinito: 60</p>

- (1) Fare clic su **Save** per completare la configurazione.
- (2) Fare clic su **Start Intelligent Analysis** per attivare l'analisi intelligente.

2. Schemi temporali

È possibile impostare uno schema temporale per limitare l'orario in cui le persone possono entrare o uscire. Quando una persona viene autenticata al di fuori dello schema temporale (intervallo di inserimento), apparirà la scritta "non-specified time". Lo schema temporale può essere impostato su base settimanale, inoltre possono essere configurati un massimo di otto intervalli di inserimento per ogni giorno. Le eccezioni possono essere impostate separatamente, ma solo su base giornaliera.

Figura 7-19 Schemi temporali

- Aggiunta di uno schema temporale



NOTA!

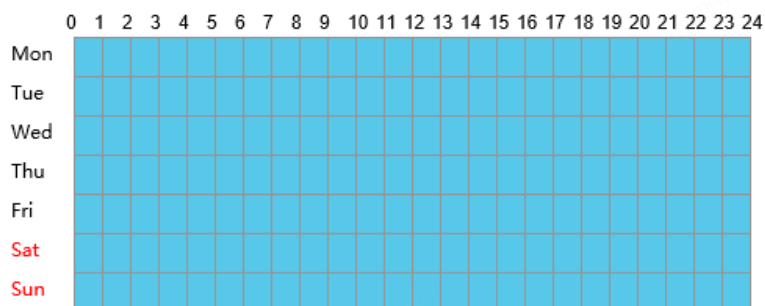
È possibile impostare un massimo di 16 schemi temporali.

- (1) Selezionare **Setup > Intelligent > Time Template** e fare clic su **Add**.
- (2) Impostare i parametri nel pannello sulla parte destra dell'interfaccia.

- **Nome schema:** inserire il nome dello schema temporale. Requisiti: da 1 a 20 caratteri, scelti fra lettere maiuscole e minuscole dell'alfabeto inglese, cifre, trattini e trattini bassi.
- **Abilita pianificazioni:** Selezionare la casella di controllo per abilitare il piano di inserimento.
- Impostare l'intervallo di inserimento.

- ◆ Fare clic su Armed Unarmed e trascinare il mouse sull'orario per impostare l'intervallo di inserimento. La precisione minima è di un'ora.

Figura 7-20 Orario su cui impostare l'intervallo di inserimento trascinando il mouse



- ◆ Facendo clic su si accede all'interfaccia **Edit**, nella quale è possibile impostare l'intervallo di inserimento per una settimana.

È consentito impostare un massimo di otto intervalli di inserimento per ogni giorno. Gli intervalli di inserimento non possono sovrapporsi. L'avviso di avvenuto riconoscimento viene visualizzato solo quando un'autenticazione positiva avviene all'interno degli intervalli di inserimento preimpostati. Quando un'autenticazione positiva avviene al di fuori degli intervalli di inserimento, viene visualizzato l'avviso "non-specified time".

Una volta configurato l'intervallo di inserimento per un giorno, è possibile copiare l'impostazione anche per gli altri giorni.

Figura 7-21 Modifica interfaccia

No.	Start Time	End Time
1	00:00:00	23:59:59
2		
3		
4		
5		
6		
7		
8		

Copy To Select All
 Mon Tue Wed Thu Fri Sat Sun

- **Abilitazione della data di eccezione:** selezionare la casella di controllo per abilitare le eccezioni.
- Impostare un'eccezione.
Le eccezioni sono su base giornaliera e non sono basate sugli intervalli di inserimento orari.

Un'eccezione può essere aggiunta, eliminata o modificata. Quando un'autenticazione positiva avviene in una data impostata come eccezione, viene visualizzato l'avviso "non-specified time".

Figura 7-22 Abilitazione della data di eccezione

No.	Date	Time Interval	Operation
1	2020-03-10	00:00:00--23:59:59	

(3) Fare clic su **Save** per salvare lo schema temporale aggiunto.

- Modifica di uno schema temporale
Per modificare uno schema temporale esistente, selezionarlo, modificare i parametri desiderati e fare clic su **Save** per completarne la modifica.
- Eliminazione di uno schema temporale

(1) Selezionare **Setup > Intelligent > Time Template** e selezionare lo schema temporale da eliminare.

(2) Fare clic su **Delete**.

(3) Nella casella di conferma visualizzata, fare clic su **OK** per eliminarlo.



NOTA!

Se una persona è associata a uno schema temporale, è necessario rimuovere l'associazione prima di eliminare lo schema temporale. In caso contrario, al momento dell'eliminazione sarà visualizzato un messaggio indicante la mancata operazione e sarà per prima cosa necessario rimuovere l'associazione della persona.

3. Modello di controllo

Un modello di controllo supporta le modalità di autenticazione basate su fasce orarie ed è possibile impostarne fino a un massimo di otto al giorno (le fasce orarie non possono sovrapporsi). La modalità di autenticazione può essere impostata separatamente per ciascun giorno o copiata su tutti i giorni.

Figura 7-23 Modello di controllo

	Mon	Tue	Wed	Thu
Time Interval1	00:00:00	23:59:59	Face X	
Time Interval2				
Time Interval3				
Time Interval4				
Time Interval5				
Time Interval6				
Time Interval7				
Time Interval8				

Copy To Select All
 Mon Tue Wed Thu Fri Sat Sun

- Aggiunta di un modello di controllo



NOTA!

È possibile impostare fino a un massimo di 16 modelli di controllo.

(1) Selezionare **Setup > Intelligent > Check Template** e fare clic su **Add**.

(2) Impostare i parametri nel pannello sulla parte destra dell'interfaccia.

- **Nome schema:** Inserire il nome del modello di controllo. Il valore è una stringa con un numero di caratteri compreso tra 1 e 63.
- Fascia oraria e modalità di autenticazione
 Impostare la modalità di autenticazione per ciascuna fascia oraria in una settimana in base alle condizioni effettive. Sono disponibili quattro modalità di autenticazione:
 - ◆ Scheda IC: il terminale di riconoscimento dei volti esegue una corrispondenza 1:N sul numero della scheda acquisita (numero della scheda IC o numero della scheda ID) e sui numeri delle schede nella libreria.
 - ◆ Volto: il terminale di riconoscimento dei volti esegue una corrispondenza 1:N sull'istantanea del volto e sulle foto dei volti nella libreria.
 - ◆ Scheda IC + Volto: il terminale di riconoscimento dei volti esegue una corrispondenza 1:N sul numero della scheda acquisita (numero della scheda IC) e sui numeri delle schede nella libreria, quindi esegue una corrispondenza 1:1 sulla foto del volto corrispondente al numero della scheda e all'istantanea del volto.
 - ◆ Password: il terminale consente di inserire "unit No.#room No.#room password" per aprire la porta.

Viene utilizzata una modalità di autenticazione per configurare il metodo con il quale le persone passano attraverso il terminale. Sono disponibili cinque modalità di autenticazione in totale: È possibile selezionarne almeno una ma non più di tre in base alle necessità effettive. Quando si utilizzano più modalità di autenticazione, queste si trovano in un rapporto "OR" che consente l'apertura della porta quando una persona supera l'autenticazione in una qualsiasi delle modalità.

- Copia di fasce orarie e modalità di autenticazione
 - ◆ Una volta impostate le fasce orarie e le modalità di autenticazione di lunedì, se sono necessarie le stesse identiche impostazioni da giovedì a sabato selezionare la casella davanti a **Select All** per copiarle su tutti i giorni.
 - ◆ Se le stesse fasce orarie e modalità di autenticazione sono necessarie solo per alcuni giorni, selezionare le giornate specifiche e fare clic su **Copy**.

(3) Fare clic su **Save** per salvare il modello di controllo aggiunto.

- Modifica di un modello di controllo
 Per modificare un modello di controllo esistente, selezionarlo, modificare i parametri desiderati e fare clic su **Save** per completarne la modifica.
- Eliminazione di un modello di controllo

(1) Selezionare **Setup > Intelligent > Check Template** e selezionare il modello di controllo da eliminare.

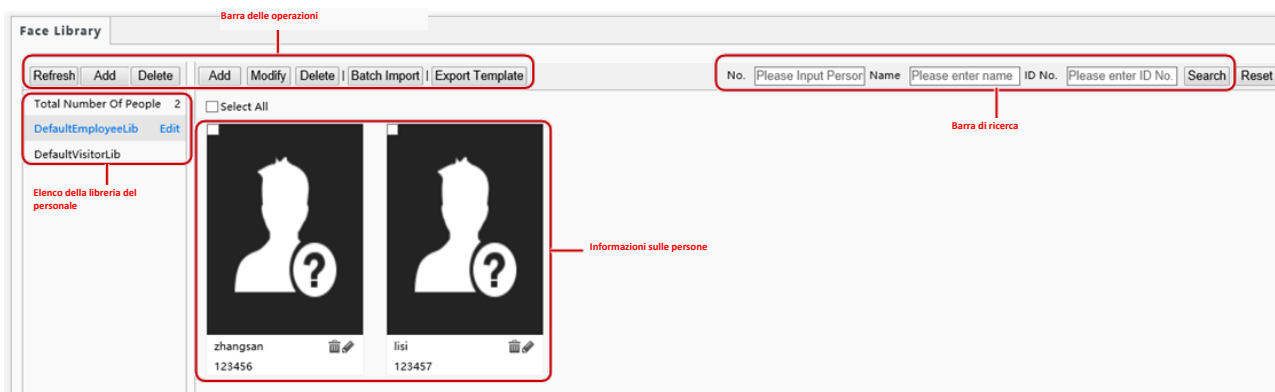
(2) Fare clic su **Delete**.

(3) Nella casella di conferma visualizzata, fare clic su **OK** per eliminarlo.

4. Libreria di volti

Selezionare **Setup > Intelligent > Face Library**. Sull'interfaccia **Face Library**, è possibile aggiungere una libreria di volti e quindi aggiungervi le persone.

Figura 7-24 Interfaccia della libreria di volti



(1) Gestione di librerie di volti

- Aggiunta di una libreria di volti



NOTA!

È possibile impostare fino a un massimo di 16 librerie di volti.

- (1) Fare clic su **Add** nell’elenco della libreria del personale.
- (2) Sull’interfaccia **Add Face Library** visualizzata, configurare le informazioni sulla libreria di volti facendo riferimento alla tabella seguente.

Figura 7-25 Aggiunta dell’interfaccia della libreria di volti

Add Face Library ✕

Face Library Type:

Face Library Name:

Check Template:

1:N Match Threshold:

Verify Success Linkage Configuration

Open door Voice Prompt HMI Prompt Wiegand Output

Verify Failure Linkage Configuration

Voice Prompt HMI Prompt

Tabella 7-10 Configurazione dei parametri

Parametro	Descrizione e configurazione
Tipo di libreria di volti	Impostare il parametro su una delle seguenti opzioni in base alle condizioni effettive: <ul style="list-style-type: none"> • Libreria dei dipendenti • Libreria dei visitatori
Nome libreria di volti	Inserire il nome della libreria. È possibile inserire da 1 a 63 caratteri.
Modello di controllo	Selezionare modello di controllo dall’elenco a discesa. Verificare i modelli di controllo aggiunti

	sull'interfaccia Modello di controllo .
Soglia di corrispondenza 1:N	La corrispondenza 1:N viene utilizzata nel riconoscimento di volti. Quando la somiglianza della corrispondenza raggiunge la soglia impostata qui, viene effettuata l'autenticazione.
Verifica riuscita della configurazione del collegamento	Le opzioni sono le seguenti: <ul style="list-style-type: none"> • Apertura porta: quando l'autenticazione riesce, viene inviato un segnale di apertura della porta per attivarne l'apertura. • Messaggio vocale: quando l'autenticazione riesce viene riprodotto un messaggio vocale. • Messaggio HMI: quando l'autenticazione riesce viene visualizzato un messaggio sull'interfaccia grafica utente. • Uscita Wiegand: se l'autenticazione riesce vengono inviati i dati attraverso l'interfaccia Wiegand.
Verifica fallimento della configurazione del collegamento	Le opzioni sono le seguenti: <ul style="list-style-type: none"> • Messaggio vocale: quando l'autenticazione non riesce viene riprodotto un messaggio vocale. • Messaggio HMI: quando l'autenticazione non riesce viene visualizzato un messaggio sull'interfaccia grafica utente.

- Modifica di una libreria di volti

(1) Selezionare la libreria di volti da modificare e fare clic su **Edit**.

(2) Nell'interfaccia **Edit Face Library** visualizzata, modificare i parametri facendo riferimento alla descrizione indicata in [Aggiunta di una libreria di volti](#).

Figura 7-26 Modifica dell'interfaccia della libreria di volti

(3) Fare clic su **OK** per completare la modifica.

- Eliminazione di una libreria di volti

(1) Selezionare la libreria di volti da eliminare e fare clic su **Delete**.

(2) Nella casella di conferma visualizzata, fare clic su **OK** per eliminare la libreria di volti.

L'eliminazione di una libreria di volti rimuoverà le persone in essa contenute.

(1) Gestione del personale

- Aggiunta di persone

È possibile aggiungere persone singolarmente o in gruppi.

- Aggiunta di una persona
 - (1) Selezionare **Setup > Intelligent > Face Library** e selezionare la libreria di volti alla quale aggiungere le persone.
 - (2) Fare clic su **Add** nella barra dell'elenco del personale.
 - (3) Sull'interfaccia **Add Face Info** visualizzata, configurare le informazioni sulle persone facendo riferimento alla tabella seguente.

Figura 7-27 Aggiunta all'interfaccia delle informazioni sui volti

Add Face Info

Basic Info

*No.

*Name

CardType1

CardNo.1

CardType2

CardNo.2

Comment

Photo

+
Local Upload

Note: Only JPG format supported. Please select pictures of 10-512K size.The maximum number of pictures is 6.

Time Template

EffectiveTime

ExpirationTime

default

OK Cancel

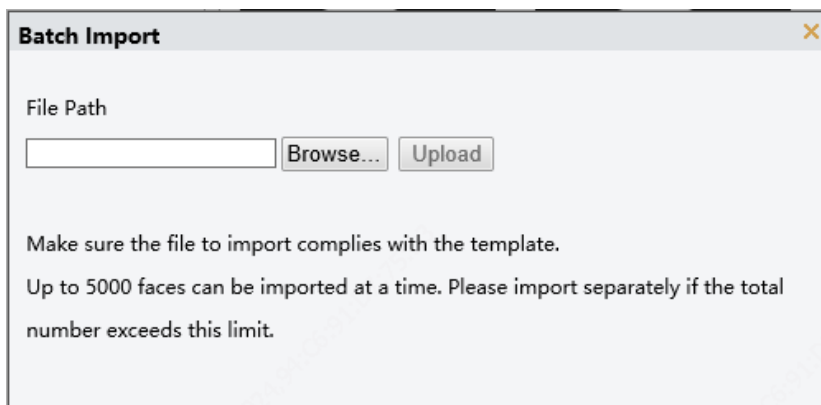
Tabella 7-11 Configurazione dei parametri

Pannello	Parametro	Descrizione e configurazione
Informazioni di base	N.	È obbligatorio. Inserire il numero di una persona. Requisiti: possibilità di scelta da 1 a 15 caratteri fra lettere alfabetiche maiuscole e minuscole, cifre, trattino e trattino basso.
	Nome	È obbligatorio. Inserire il nome della persona. Requisiti: una stringa di lunghezza compresa tra 1 e 63 caratteri.
	Tipo scheda 1/ Tipo scheda 2 N. scheda 1/ N. scheda 2	Selezionare il tipo di scheda e quindi inserirne il numero. Le opzioni riguardanti il tipo di scheda includono Scheda IC, Scheda ID e Nessuna. Requisiti per il numero di scheda: possibilità di scelta da 1 a 20 caratteri fra lettere alfabetiche maiuscole e minuscole trattino e trattino basso.
	Commento	Inserire una nota per la persona.
Foto	/	Fare clic Local Upload . Sull'interfaccia visualizzata, selezionare una foto del volto locale da caricare.

		ET-S51H@B consente di caricare fino a sei foto a persona e ET-B31H-M@B supporta tre foto al massimo per persona. Requisiti delle foto: sono supportate solo immagini .jpg di dimensioni comprese tra 10 KB e 512 KB.
Schemi temporali	Ora di entrata in vigore	Selezionare uno schema temporale e quindi impostare l'ora di entrata in vigore e l'ora di scadenza dello schema temporale.
	Ora di scadenza	Selezionare la casella davanti allo schema temporale in base alla situazione effettiva.
	Schemi temporali	NOTA! <ul style="list-style-type: none"> • Quando si associano più schemi temporali, viene assunta l'unione di questi durante l'autenticazione. • Se uno schema temporale non si trova entro l'intervallo tra l'ora di entrata in vigore o l'ora di scadenza, all'autenticazione viene visualizzato il messaggio "orario non specificato".

- (4) Fare clic su **OK** per completare l'aggiunta.
- Importazione delle informazioni sul personale in gruppo
- (1) Selezionare **Setup > Intelligent > Face Library** e selezionare la libreria di volti alla quale aggiungere le persone.
 - (2) Fare clic su **Export Template** per scaricare un modello da importare sul dispositivo locale.
 - (3) Scompattare il modello. Nella tabella di importazione, inserire le informazioni in base ai requisiti.
 - (4) Fare clic su **Batch Import** per caricare la tabella da importare.

Figura 7-28 Importazione in gruppo



La figura qui sotto mostra lo stato dell'importazione.

Se non è possibile importare le informazioni su una persona, verificarne il motivo nella colonna della descrizione, modificare l'informazione e quindi importare di nuovo le informazioni sulla persona.



NOTA!

- OET-515H è in grado di memorizzare le informazioni su 50.000 persone al massimo.
- OET-213H è in grado di memorizzare le informazioni su 10.000 persone al massimo.

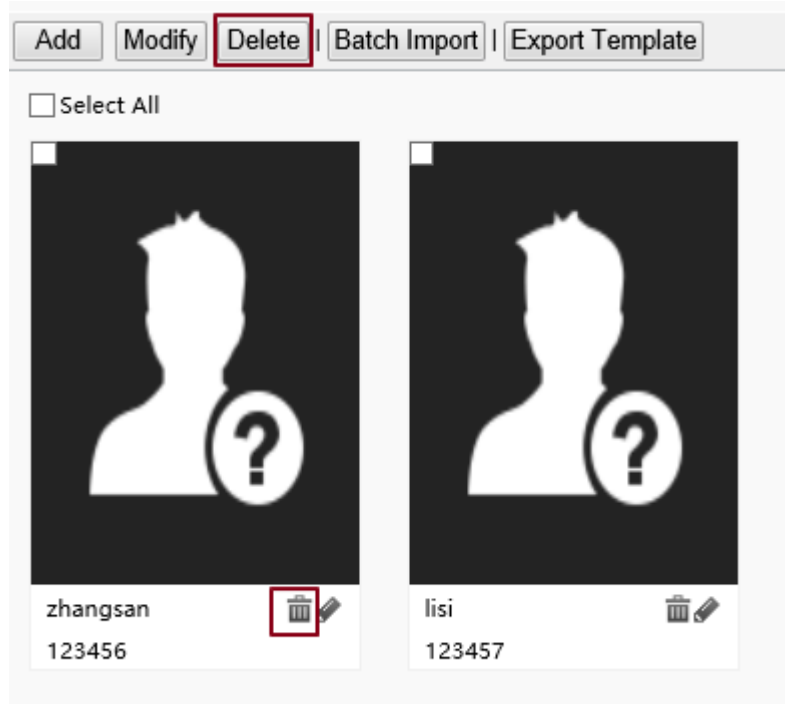
- Modifica delle informazioni su una persona
 - (1) Selezionare la casella nell'angolo in alto a sinistra di una persona della quale occorre modificarne le informazioni.
 - (2) Fare clic sul tasto di modifica come mostrato nella figura di seguito.

Figura 7-29 Modifica interfaccia



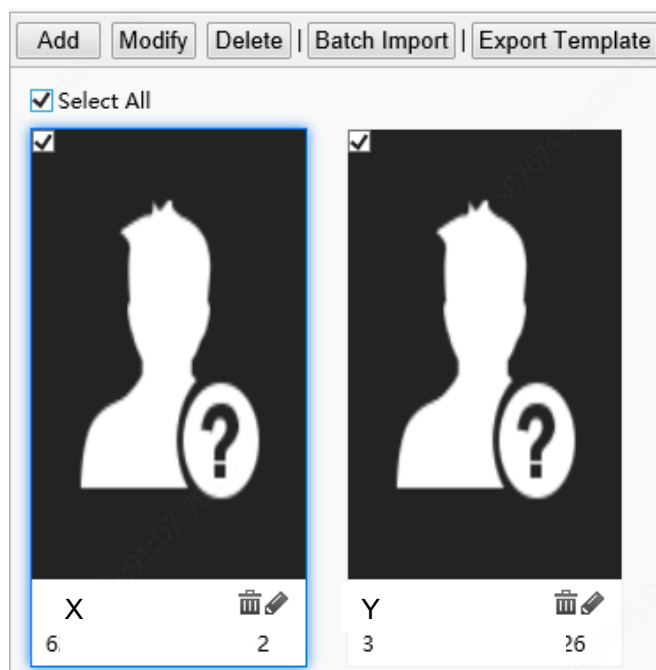
- (3) Sull'interfaccia di modifica visualizzata, modificare le informazioni su una persona facendo riferimento a [Aggiunta di una persona](#).
 - (4) Fare clic su **OK** per completare la modifica.
- Eliminazione di persone
 - È possibile eliminare persone singolarmente o in gruppi.
 - Eliminazione di una persona
 - (1) Selezionare la casella nell'angolo in alto a sinistra di una persona da eliminare.
 - (2) Fare clic sul tasto di eliminazione come mostrato nella figura di seguito.

Figura 7-30 Interfaccia di eliminazione



- (3) Nella casella di conferma visualizzata, fare clic su **OK** per completare l'eliminazione.
- Eliminazione di tutte le persone
 - (1) Selezionare tutte le caselle davanti a **Select All**.

Figura 7-31 Selezione di tutte le persone




- (2) Fare clic su **Delete** o .
- (3) Nella casella di conferma visualizzata, fare clic su **OK** per completare l'eliminazione.
- Ricerca di una persona
 - È possibile cercare le informazioni sul personale per numero, nome o numero di scheda identificativa.

Figura 7-32 Casella di Ricerca

No.	<input type="text" value="Please Input Person"/>	Name	<input type="text" value="Please enter name"/>	ID No.	<input type="text" value="Please enter ID No."/>	<input type="button" value="Search"/>	<input type="button" value="Reset"/>
-----	--	------	--	--------	--	---------------------------------------	--------------------------------------

5. Impostazioni Avanzate

Selezionare **Setup > Intelligent > Advanced Setting**.

Impostare i parametri facendo riferimento alla tabella qui sotto.

Figura 7-33 Interfaccia Impostazioni Avanzate

Advanced Setting

QR Code Detection Off On (Note: Require card authentication)

QR Code Protocol Private Third Party

Call Mode

Upload Setting

Image Reporting Mode

Record Reporting Type

Local Storage Settings

Local Storage On Off

Image Storage Mode

Record Storage Type

Attribute Rule Configuration

Safety Helmet

Authentication Failed A... Off On

Mask

Authentication Failed A... Off On

Temperature Measurement

Temperature Measurem... Measure Forehead Temperature Measure Wrist Temperature

Authentication Failed A... Off On

Temperature Measurem... ~

Temperature Alarm Thr...

Temperature Alert Off On

Temperature Alert Offset (Temperature Alert Threshold = Temperature Alarm Threshold - Temperature Alert Offset)

Alarm Output Configuration

High Temperature Alarm Off On

Not Wearing Mask Alarm Off On

Blacklist Alarm Off On

Authentication Failure A... Off On

Tabella 7-12 Descrizione e configurazione dei parametri

Componente	Descrizione	
Modalità di Apertura Porta	<ul style="list-style-type: none"> • Autenticazione: Quando l'opzione Door Opening Mode è impostata su Authentication, il terminale genera il segnale di apertura porta solo dopo che la persona in ingresso ha superato l'autenticazione in Modello di controllo. • Volto: Quando l'opzione Door Opening Mode è impostata su Face, Il terminale di riconoscimento facciale genera il segnale di apertura porta dopo aver riconosciuto la foto di un volto. In caso di configurazione di una libreria whitelist, il riconoscimento facciale sarà effettuato sul personale incluso in whitelist e il sistema fornirà una segnalazione in caso di successo. L'interfaccia utente del sistema non darà alcuna segnalazione in caso di scansione di volti di personale non incluso in whitelist. <p>Impostare questo parametro in base agli scenari applicativi reali.</p>	
Rilevamento Codice QR	<ul style="list-style-type: none"> • Non attiva: Quando l'opzione è impostata su Off, la telecamera del terminale di riconoscimento facciale non raccoglierà i dati del codice QR. • On: Quando l'opzione è impostata su On e la scheda IC è contenuta in Modello di controllo, la telecamera del terminale di riconoscimento facciale raccoglierà i dati del codice QR ed effettuerà l'autenticazione. Per i dettagli di tale operazione, consultare la sezione Apertura porta con codice QR. <p>Impostare questo parametro in base agli scenari applicativi reali.</p>	
Protocollo Codice QR	<ul style="list-style-type: none"> • Certificati privati Quando l'opzione è impostata su Private, il terminale di riconoscimento facciale analizzerà localmente i dati del codice QR (questo protocollo è applicabile se il sistema fa uso di una telecamera o di uno scanner per il codice QR). • Soggetto esterno La configurazione non è supportata. 	
Modalità Chiamata	<ul style="list-style-type: none"> • Chiamata Community: Quando l'opzione Call Mode è impostata su Community Call, la chiamata avviata nel terminale di riconoscimento facciale del videocitofono sarà normale (chiamata al monitor interno). • Chiamata Cloud: Quando l'opzione Call Mode è impostata su Cloud Call, la chiamata avviata nel terminale di riconoscimento facciale del videocitofono sarà su cloud (chiamata sull'APP mobile). <p>Impostare questo parametro in base agli scenari applicativi reali.</p>	
Impostazioni di Caricamento	Modalità Report di Immagini	<ul style="list-style-type: none"> • Report Senza Immagini: I report dei registri di accesso da inviare alla piattaforma di livello superiore non contengono immagini. • Report Solo Immagini Grandi: I report dei registri di accesso da inviare alla piattaforma di livello superiore contengono solo immagini grandi (cioè immagini panoramiche). • Report Solo Immagini Piccole: I report dei registri di accesso da inviare alla piattaforma di livello superiore contengono solo immagini piccole (cioè immagini ritagliate su dettagli specifici). • Report Completo: I report dei registri di accesso contengono immagini grande e piccole. Il valore predefinito è Report All.
	Modalità di Report Registri	<ul style="list-style-type: none"> • Carica Tutto: Il terminale di riconoscimento facciale carica tutti i registri del personale in transito. • Carica Registri con autenticazione riuscita: Il terminale di riconoscimento facciale carica solo i registri del personale in transito con autenticazione riuscita. <p>Impostare questo parametro in base agli scenari applicativi reali.</p>

Impostazioni Archivio Locale	Archivio locale		Le opzioni sono On e Off . Impostare i parametri basandosi sulla situazione effettiva. Il valore predefinito è Off .	
	Modalità Archiviazione Immagini		Salva Tutte le Immagini: Il sistema archiverà tutte le immagini, grandi e piccole.	
	Tipo Archivio di Registrazione		Salva Tutti i Registri: Il sistema archiverà tutti i registri di accesso (relativi ad autenticazioni riuscite e non).	
Configurazione Regola Attributi	Casco di Sicurezza	Apertura Porta in caso di Rilevamento non Riuscito	<p>Le opzioni sono On e Off. Impostare i parametri basandosi sulla situazione effettiva. Il valore predefinito è Off.</p> <p>Facendo clic su On per questa opzione, quando il terminale di riconoscimento facciale rileva una persona che non indossa il casco di sicurezza, il sistema mostra un avviso sull'interfaccia utente e riproduce un annuncio vocale (si prega di indossare il casco di sicurezza), ma il processo di autenticazione (scansione volto, scheda IC, carta d'identità) e il risultato dell'operazione di apertura porta non saranno influenzati.</p> <p>Facendo clic su Off per questa opzione, quando il terminale di riconoscimento facciale rileva una persona che non indossa il casco di sicurezza, il sistema mostra un avviso sull'interfaccia utente e riproduce un annuncio vocale (si prega di indossare il casco di sicurezza), ma la porta non si apre.</p>	
	Maschera	Apertura Porta in caso di Rilevamento non Riuscito	<p>Le opzioni sono On e Off. Impostare i parametri basandosi sulla situazione effettiva. Il valore predefinito è Off.</p> <p>Facendo clic su On per questa opzione, quando il terminale di riconoscimento facciale rileva una persona che non indossa la maschera, il sistema mostra un avviso sull'interfaccia utente e riproduce un annuncio vocale (si prega di indossare la maschera), ma il processo di autenticazione (scansione volto, scheda IC, carta d'identità) e il risultato dell'operazione di apertura porta non saranno influenzati.</p> <p>Facendo clic su Off per questa opzione, quando il terminale di riconoscimento facciale rileva una persona che non indossa la maschera, il sistema mostra un avviso sull'interfaccia utente e riproduce un annuncio vocale (si prega di indossare la maschera), ma la porta non si apre.</p>	
	Temperatura Misurazione	Misurazione della Temperatura		<ul style="list-style-type: none"> Misurazione della Temperatura della Fronte: Il sistema misura la temperatura della fronte. Misurazione della Temperatura del Polso: Il sistema misura la temperatura del polso. <p>Non è richiesta alcuna configurazione. Una volta collegato al modulo di rilevamento digitale, il terminale passerà automaticamente alla modalità di misurazione delle temperatura corrispondente.</p>
			Autenticazione non Riuscita e Apertura della Porta	<p>Le opzioni sono On e Off. Impostare i parametri basandosi sulla situazione effettiva. Il valore predefinito è Off.</p> <p>Facendo clic su On per questa opzione, quando il modulo di rilevamento digitale individua una persona la cui temperatura supera la soglia di allarme predefinita, il sistema mostra un avviso sull'interfaccia utente e riproduce un annuncio vocale (anomalia di temperatura), ma il processo di autenticazione (scansione volto, scheda IC, carta d'identità) e il risultato dell'operazione di apertura porta non saranno influenzati.</p> <p>Facendo clic su Off per questa opzione, quando il modulo di rilevamento digitale individua una persona la cui temperatura supera la soglia di allarme predefinita, il sistema mostra un avviso sull'interfaccia utente e riproduce un annuncio vocale (anomalia di temperatura), ma la porta non sarà aperta.</p>
			Intervallo di misurazione della temperatura	Intervallo di valori: [30–45]; intervallo predefinito: [34-42] Configurare l'intervallo in base agli scenari di applicazione reali.
			Soglia di allarme	Quando il modulo di rilevamento digitale rileva una temperatura superiore alla soglia qui configurata, l'allarme "temperatura anomala"

	temperatura	appare sull'interfaccia grafica e viene emesso il segnale acustico di avvertimento. Intervallo di valori: [30-45]; valore predefinito: 37,3
	Avviso Temperatura	Le opzioni sono On e Off . Impostare i parametri basandosi sulla situazione effettiva. Il valore predefinito è Off . Attivando l'opzione di avviso temperatura, quando la temperatura corporea è compresa tra la soglia di avviso e quella di allarme, il sistema genera un allarme di temperatura elevata, segnalando alle persone di effettuare un nuovo rilevamento di temperatura.
	Offset avviso temperatura	Soglia di Avviso Temperatura = Soglia di Allarme Temperatura - Offset di Avviso Temperatura
Configurazione Uscita Allarme	Allarme Temperatura Elevata	Le opzioni sono On e Off . Impostare i parametri basandosi sulla situazione effettiva. Il valore predefinito è Off . Dopo aver attivato l'allarme di temperatura elevata, il terminale segnalerà tale allarme quando il modulo di rilevamento digitale individua persone con temperatura alta.
	Allarme di Maschera non Indossata	Le opzioni sono On e Off . Impostare i parametri basandosi sulla situazione effettiva. Il valore predefinito è Off . Dopo aver attivato l'allarme di maschera non indossata, il terminale segnalerà tale allarme quando individua persone che non indossano la maschera.
	Allarme blacklist	Le opzioni sono On e Off . Impostare i parametri basandosi sulla situazione effettiva. Il valore predefinito è Off . Dopo aver attivato l'allarme blacklist, il terminale segnalerà tale allarme quando individua persone che sono incluse in blacklist.
	Allarme di Autenticazione non Riuscita	Le opzioni sono On e Off . Impostare i parametri basandosi sulla situazione effettiva. Il valore predefinito è Off . Dopo aver attivato l'allarme di autenticazione non riuscita, il terminale segnalerà tale allarme quando l'autenticazione di volti o schede non riesce.

6. Visualizzazione Risultato del Riconoscimento

L'interfaccia **Recognition Result Display** permette di stabilire se il nome e la foto registrata di una persona dovranno essere visualizzati sull'interfaccia del terminale dopo un riconoscimento facciale riuscito.

(1) Selezionare la voce **Setup > Common > Smart Snapshot** e fare clic sulla scheda **Recognition Result Display**.

Figura 7-34 Interfaccia di Visualizzazione Risultato del Riconoscimento

(2) È possibile configurare la visualizzazione dei risultati del riconoscimento, facendo riferimento alla tabella qui sotto.

Tabella 7-13 Descrizione e configurazione dei parametri

Parametro	Descrizione e configurazione
Foto della Libreria di Volti	<ul style="list-style-type: none"> Display: Il terminale di riconoscimento facciale mostra la foto registrata di una persona in caso di riconoscimento riuscito.

	<ul style="list-style-type: none"> Nascondi: Il terminale di riconoscimento facciale non mostra la foto registrata di una persona in caso di riconoscimento riuscito. <p>Questo parametro deve essere impostato in base ai requisiti dell'applicazione reale.</p>
Riconoscimento Riuscito	<ul style="list-style-type: none"> Impostazione predefinita: Il terminale di riconoscimento facciale mostra la scritta "Riconoscimento Riuscito" in caso di riconoscimento di un volto. Personalizzato: In caso di riconoscimento riuscito, il terminale mostra le informazioni definite qui al posto del nome della persona riconosciuta. È possibile inserire una stringa di 0–10 caratteri nella casella personalizzata. <p>Questo parametro deve essere impostato in base ai requisiti dell'applicazione reale.</p>
Data e ora	<ul style="list-style-type: none"> Display: Il terminale di riconoscimento facciale mostra l'ora attuale di sistema. Nascondi: Il terminale di riconoscimento facciale non mostra l'ora attuale di sistema. <p>Questo parametro deve essere impostato in base ai requisiti dell'applicazione reale.</p> <p>Nota: Questo parametro è disponibile solo se l'opzione Base Image Display è impostata su Single Face.</p>
Visualizzazione Immagini di Base	<ul style="list-style-type: none"> Volto Singolo: L'interfaccia utente mostra solo le informazioni della persona individuata dopo il riconoscimento facciale riuscito. Volti Multipli: L'interfaccia utente mostra le informazioni di più persone individuate dopo il riconoscimento facciale riuscito. È possibile mostrare al massimo le informazioni relative alle ultime cinque persone riconosciute. Le informazioni sull'ultima persona riconosciuta sono mostrate sulla sinistra dello schermo. <p>Questo parametro deve essere impostato in base ai requisiti dell'applicazione reale. L'impostazione predefinita di tale opzione è Single Face.</p>

(3) Fare clic su **Save** per completare la configurazione.

7.2.3 Eventi

È possibile definire l'inserimento di allarme in modo da implementare la segnalazione dell'allarme. Definendo le azioni di attivazione di altri dispositivi, è possibile che un allarme attivi uno o più tipi di azione, in modo che l'utente sia in grado di gestire in tempo l'allarme e le relative azioni.

Gli allarmi che possono essere inseriti comprendono allarmi incendio, allarmi antismontaggio e allarmi di magneti porta.

1. Allarmi incendio

Se il terminale di riconoscimento facciale è collegato a un dispositivo di allarme incendio, il terminale sarà in grado di segnalare un allarme incendio quando si verifica.

(1) Selezionare **Setup > Events > Events** e fare clic su **Fire Alarm**.

Figura 7-35 Interfaccia di Configurazione Allarmi Incendio

Alarm Name: 1

Alarm ID:

Alarm Type: N.O.

Alarm Input: On Off

Trigger Actions

Snapshot Open door

Enable Plan

Armed Unarmed Edit

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Mon																									
Tue																									
Wed																									
Thu																									
Fri																									
Sat																									
Sun																									

Save

(2) Impostare le informazioni dell'allarme incendio.

- 1) Selezionare l'allarme e impostare il nome dell'allarme.
- 2) Selezionare **N.O.** o **N.C.** a seconda del tipo di ingresso allarme di terze parti. Ad esempio, se il dispositivo dell'ingresso allarme di terze parti è normalmente aperto, occorre selezionare **N.O.**, in modo che la telecamera possa ricevere le informazioni sull'allarme dal dispositivo dell'ingresso allarme di terze parti.
- 3) Permette di abilitare l'Ingresso Allarme. Se l'opzione **Alarm Input** è impostata su **On**, il terminale riceverà gli allarmi del dispositivo antincendio. Se l'opzione è impostata su **Off**, il terminale non riceverà gli allarmi del dispositivo antincendio.

(3) Imposta le azioni associate agli allarmi incendio.

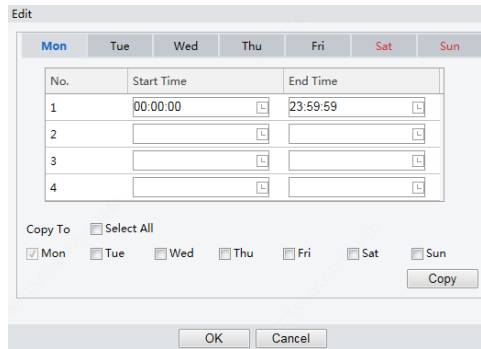
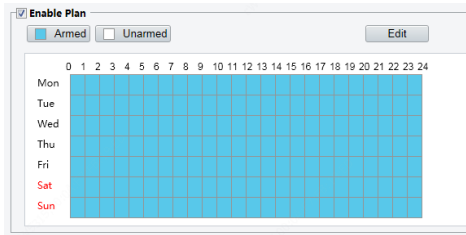
Gli allarmi incendio possono essere associati ad azioni di acquisizione istantanee e di apertura porte del terminale. Le due funzioni potranno essere abilitate in base allo scenario effettivo di applicazione.

(4) Imposta l'attivazione del programma di inserimento.

Selezionare la casella di controllo **Enable Plan** e inserire l'orario iniziale e finale di allarme (facendo clic su **Edit**). Gli intervalli di inserimento non possono sovrapporsi. Il dispositivo attiverà i segnali di allarme solo nell'intervallo orario impostato.

Le opzioni disponibili includono la definizione dei giorni da lunedì a domenica e la definizione di quattro fasce orarie per ogni giorno.

Dopo aver definito il programma orario di un giorno, è possibile fare clic su **Copy** e quindi su **Paste** in un altro giorno per copiare il piano ad altri giorni.



Definizione Orari di Inserimento tramite Mouse

Modifica di Tabelle per Impostazione Orari di Inserimento

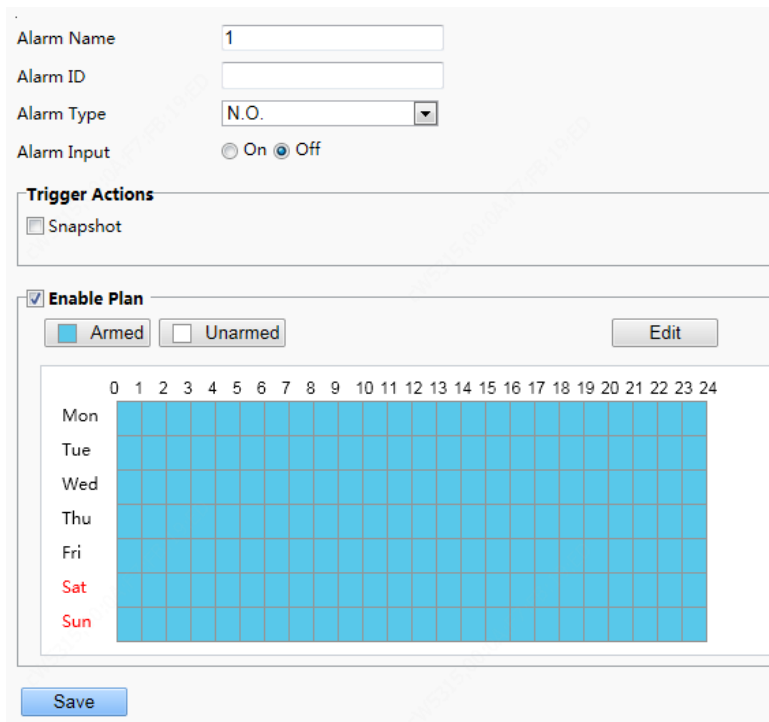
(5) Fare clic su **Save**.

2. Allarme Antimanomissione

Il terminale di riconoscimento facciale è dotato di un pulsante antimanomissione, che permette di inviare l'allarme manomissione al terminale.

(1) Selezionare **Setup > Events > Events** e poi fare clic su **Tamper Alarm**.

Figura 7-36 Interfaccia di Configurazione Allarme Antimanomissione



(2) Impostare le informazioni base degli allarmi manomissione.

- 1) Selezionare l'allarme e impostare il nome dell'allarme.
- 2) Selezionare il tipo di allarme. Impostare **Alarm Type** su **N.O.** o **N.C.** a seconda che l'ingresso allarme di manomissione sia normalmente aperto o chiuso.
- 3) Permette di abilitare l'Ingresso Allarme. Se l'opzione **Alarm Input** è impostata su **On**, il terminale riceverà gli allarmi antismontaggio. Se l'opzione è impostata su **Off**, il terminale non riceverà gli allarmi antismontaggio.

(3) Impostare le azioni associate agli allarmi antimanomissione.

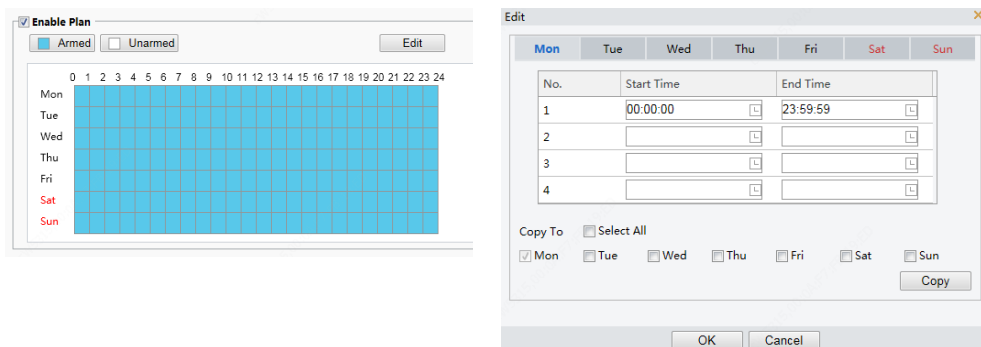
(4) Gli allarmi antimanomissione possono essere associati all'azione di acquisizione di istantanee del terminale. La funzione potrà essere abilitata in base allo scenario effettivo di applicazione.

Imposta l'attivazione del programma di inserimento.

Selezionare la casella di controllo **Enable Plan** e inserire l'orario iniziale e finale di allarme (facendo clic su **Edit**). Gli intervalli di inserimento non possono sovrapporsi. Il dispositivo attiverà i segnali di allarme solo nell'intervallo orario impostato.

Le opzioni disponibili includono la definizione dei giorni da lunedì a domenica e la definizione di quattro fasce orarie per ogni giorno.

Dopo aver definito il programma orario di un giorno, è possibile fare clic su Copy e quindi su Paste in un altro giorno per copiare il piano ad altri giorni.



Definizione Orari di Inserimento tramite Mouse

Modifica di Tabelle per Impostazione Orari di Inserimento

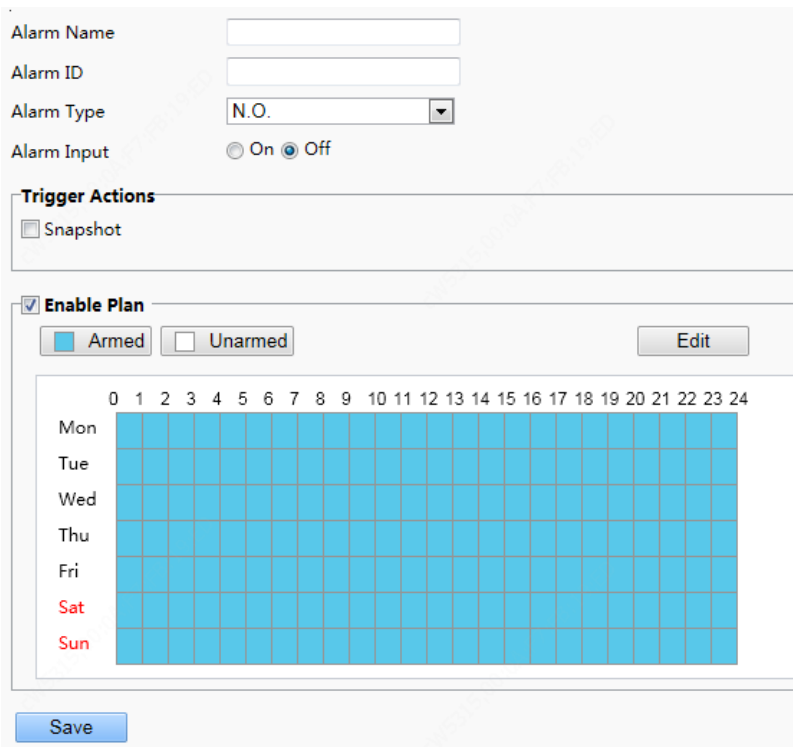
(5) Fare clic su **Save**.

3. Allarmi magnete porta

Se il terminale di riconoscimento facciale è collegato a un magnete porta, può ricevere i relativi allarmi.

(1) Selezionare **Setup > Events > Events** e poi fare clic su **Door Magnet Alarm**.

Figura 7-37 Interfaccia di Configurazione di Allarme Magnete Porta



(2) Impostare le informazioni base degli allarmi di magnete porta.

- 1) Selezionare l'allarme e impostare il nome dell'allarme.
- 2) Selezionare il tipo di allarme. Impostare **Alarm Type** su **N.O.** or **N.C.** a seconda che il dispositivo di ingresso allarme collegato sia normalmente aperto o chiuso. Ad esempio, per dispositivi di ingresso

allarme normalmente aperti, l'opzione **Alarm Type** deve essere impostata su **N.O.** per consentire al terminale di riconoscimento facciale di ricevere gli allarmi dal dispositivo collegato.

- 3) Permette di abilitare l'Ingresso Allarme. Se l'opzione **Alarm Input** è impostata su **On**, il terminale riceverà gli allarmi del magnete porta. Se l'opzione è impostata su **Off**, il terminale non riceverà gli allarmi del magnete porta.

- (3) Impostare le azioni associate agli allarmi del magnete porta.

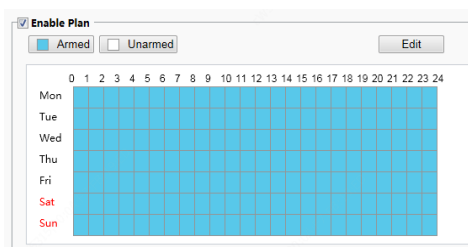
Gli allarmi del magnete porta possono essere associati all'azione di acquisizione di istantanee del terminale. La funzione potrà essere abilitata in base allo scenario effettivo di applicazione.

- (4) Imposta l'attivazione del programma di inserimento.

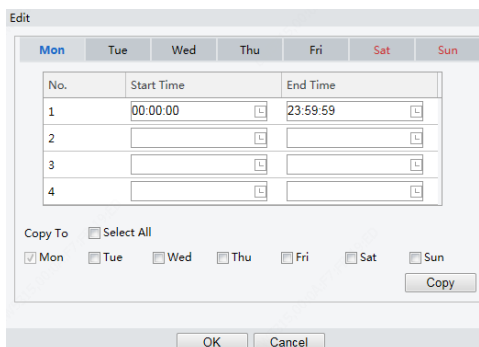
Selezionare la casella di controllo **Enable Plan** e inserire l'orario iniziale e finale di allarme (facendo clic su **Edit**). Gli intervalli di inserimento non possono sovrapporsi. Il dispositivo attiverà i segnali di allarme solo nell'intervallo orario impostato.

Le opzioni disponibili includono la definizione dei giorni da lunedì a domenica e la definizione di quattro fasce orarie per ogni giorno.

Dopo aver definito il programma orario di un giorno, è possibile fare clic su Copy e quindi su Paste in un altro giorno per copiare il piano ad altri giorni.



Definizione Orari di Inserimento tramite Mouse



Modifica di Tabelle per Impostazione Orari di Inserimento

- (5) Fare clic su **Save**.

7.2.4 Archiviazione

1. Archiviazione

- (1) Fare clic su **Setup > Storage > Storage**.



NOTA!

- Mantenere i valori predefiniti sull'interfaccia **Storage**. La configurazione non è consentita.
- La formattazione non è consentita.

7.2.5 Sicurezza

1. Utenti

Per i dettagli sulla configurazione dell'utente, consultare [Utenti](#).

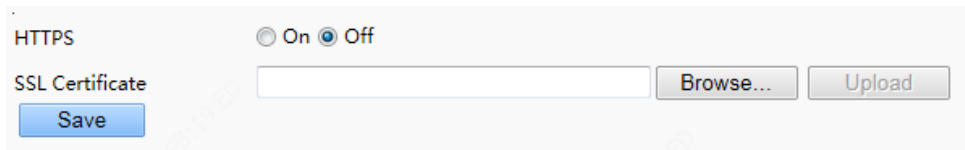
2. Sicurezza di Rete

Dopo aver impostato le opzioni di trasmissione sicura delle informazioni, sarà possibile definire un canale per la trasmissione sicura dei dati.

(1) HTTPS

(1) Fare clic su **Setup > Security > Network Security > HTTPS**.

Figura 7-38 Interfaccia Impostazioni HTTPS



(2) Selezionare **On** per **HTTPS**. È possibile importare un certificato SSL personalizzato se necessario.

(3) Fare clic su **Save**.

Quando si effettua l'accesso la volta successiva, inserire nel formato `https://IP:HTTPS` numero di porta, ad esempio `https://192.168.1.13:443` per garantire la modalità di canale sicuro. Se si utilizza la porta HTTPS predefinita, inserire `https://IP`.

(2) Autenticazione RTSP

L'RTSP (Protocollo di streaming in tempo reale) è un protocollo di livello applicativo. Per trasmettere e controllare l'audio e il video, impostare l'autenticazione RTSP sull'interfaccia web.

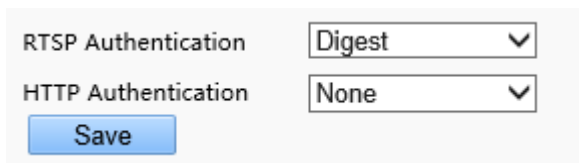
(1) Fare clic su **Setup > Security > Network Security > RTSP Authentication**.

(2) Selezionare una modalità di autenticazione.

Tabella 7-14 Descrizione e configurazione dei parametri

Parametro	Descrizione e configurazione
Autenticazione RSTP	Le opzioni sono Basic , Digest e None . Il valore predefinito è Digest .
Autenticazione HTTP	Le opzioni sono Digest e None . Il valore predefinito è None .

Figura 7-39 Interfaccia di Autenticazione Impostazioni RTSP



(3) Fare clic su **Save**.



NOTA!

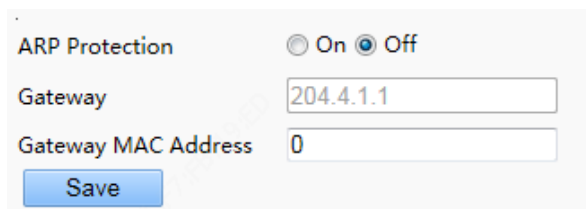
Se il terminale di riconoscimento facciale del videocitofono è usato in combinazione con i monitor interni, occorre impostare la modalità di autenticazione su **None**.

(3) Protezione ARP

Questa funzione protegge la telecamera da attacchi ARP. Il gateway e l'indirizzo MAC devono essere impostati adeguatamente prima che un computer possa accedere alla telecamera da un'altra rete; se si imposta un indirizzo MAC, solo i computer sulla stessa LAN possono accedere.

(1) Fare clic su **Setup > Security > Network Security > ARP Protection**.

Figura 7-40 Interfaccia di Impostazione Protezione ARP



(2) Selezionare la casella di controllo per abilitare la funzione di associazione ARP e impostare l'indirizzo MAC del gateway.

(3) Fare clic su **Save**.

(4) **Filtro Indirizzi IP**

Utilizzare il filtro indirizzi IP per consentire o negare l'accesso da indirizzi IP specifici.

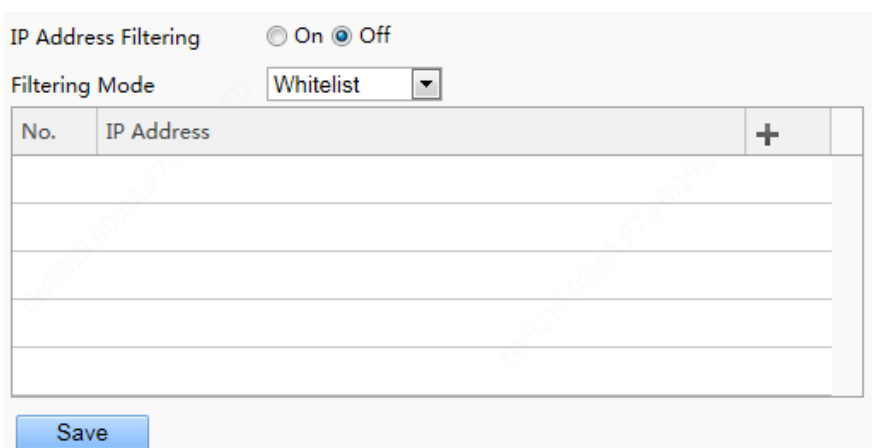


NOTA!

Questa funzione non è supportata da alcuni modelli. Fare riferimento al modello effettivo per i dettagli.

(1) Fare clic su **Setup > Security > Network Security > IP Address Filtering**.

Figura 7-41 Interfaccia Impostazioni di Filtro Indirizzi IP



(2) Selezionare **On** per abilitare il Filtro indirizzi IP.

(3) Selezionare una modalità filtro, quindi aggiungere gli indirizzi IP.

(4) Fare clic su **Save**.



NOTA!

- Se Filtering Mode è impostato su Whitelist, allora solo gli indirizzi IP aggiunti possono accedere alla telecamera. Se Filtering Mode è impostato su Deny Access, allora solo gli indirizzi IP aggiunti non possono accedere alla telecamera.
- Sono consentiti fino a 32 indirizzi IP. Ciascun indirizzo IP può essere aggiunto solo una volta.
- Il primo byte di ciascun indirizzo IP deve essere compreso tra 1 e 223 e il quarto non può essere 0. Ad esempio, i seguenti indirizzi IP non sono consentiti e non possono essere aggiunti: 0.0.0.0, 127.0.0.1, 255.255.255.255, 224.0.0.1.

7.2.6 Sistema

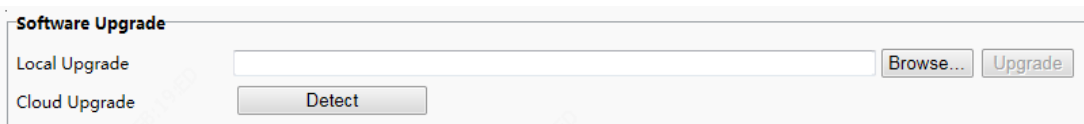
1. Porte e dispositivi

Per la configurazione di porte e dispositivi, consultare [Porte e dispositivi](#).

(1) Manutenzione

(1) Fare clic su **Setup > System > Maintenance**.

Figura 7-42 Interfaccia di Aggiornamento Locale



(2) Sotto **Software Upgrade**, fare clic su **Browse** e selezionare il file di aggiornamento corretto.

(3) Fare clic su **Upgrade** e quindi confermare per iniziare. La telecamera si riavvierà in automatico una volta completato l'aggiornamento.



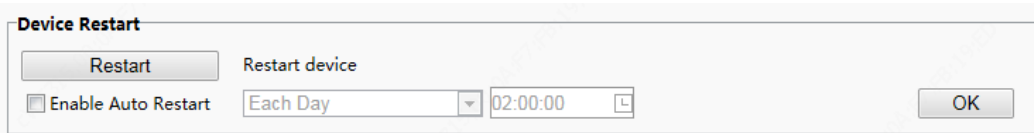
NOTA!

- Occorre utilizzare il file di aggiornamento corretto per la telecamera. In caso contrario, potrebbero verificarsi dei problemi.
- Il file di aggiornamento è un file ZIP e deve includere tutti i file necessari.
- Accertarsi che l'alimentazione funzioni normalmente durante l'aggiornamento. Il dispositivo si riavvierà una volta completato l'aggiornamento.

(2) Riavvio dispositivo

(1) Fare clic su **Setup > System > Maintenance**.

Figura 7-43 Interfaccia di Configurazione Riavvio



(2) Sotto **Device Restart**, fare clic su **Restart**. Il dispositivo si riavvierà una volta confermata l'operazione.

(3) È possibile selezionare **Enable Auto Restart** e poi definire l'orario di riavvio. Il dispositivo si riavvierà automaticamente all'orario impostato.



ATTENZIONE.

Eseguire l'operazione con cautela perché l'avvio del sistema interrompe il servizio in corso.

Si suggerisce di non impostare alcun orario di riavvio automatico del dispositivo se non ci sono servizi in corso.

(3) Configurazione del sistema

(1.1) Ripristino Impostazioni di Fabbrica

- Ripristino impostazioni di fabbrica

Facendo clic su **Default**, tutti i parametri sono reimpostati ai valori predefiniti di fabbrica, ad eccezione della password di accesso amministratore, parametri delle porte di rete, orario di sistema, password di amministratore e di attivazione.



NOTA!

Dopo aver reimpostato i valori predefiniti, l'interfaccia grafica mostra un avviso che chiede di modificare la password di attivazione. Ulteriori informazioni sulla modifica delle password sono disponibili [qui](#).

- Ripristino completo impostazioni di fabbrica

Selezionando **Ripristina tutte le impostazioni ai valori predefiniti senza mantenere le impostazioni di rete e utente correnti**, tutti i parametri sono reimpostati ai valori predefiniti di fabbrica.

(1.2) Importazione e Esportazione del File di Configurazione del Sistema

Esportare le configurazioni correnti della telecamera e salvarle su computer o un supporto di memoria esterno. È inoltre possibile ripristinare rapidamente le configurazioni nella telecamera importando le configurazioni di backup archiviate nel computer o su un supporto di archiviazione esterno.

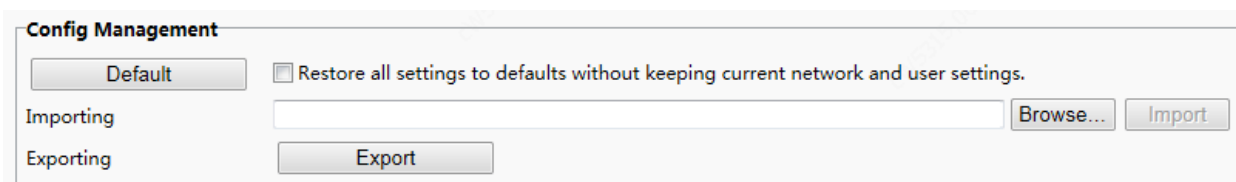


ATTENZIONE.

- Una volta eseguita l'operazione predefinita, tutte le impostazioni vengono ripristinate ai valori predefiniti di fabbrica, tranne i seguenti: password di accesso dell'amministratore di sistema e ora di sistema.
- Accertarsi di importare il file di configurazione corretto della telecamera. In caso contrario, potrebbero verificarsi dei problemi.
- La telecamera si riavvierà quando il file di configurazione è importato correttamente.

(1) Fare clic su **Setup > System > Maintenance**.

Figura 7-44 Interfaccia di Configurazione Importazione/Esportazione



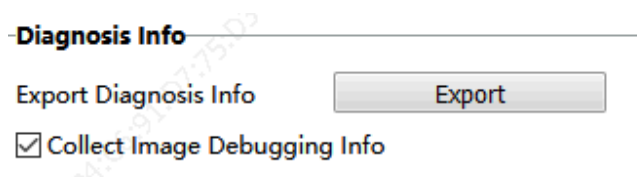
- (2) Per importare le configurazioni di cui è stato eseguito il backup, fare clic su **Browse** vicino al pulsante **Import**, selezionare le configurazioni da importare e quindi fare clic su **Import**. Verranno visualizzati i risultati.
- (3) Per esportare le attuali configurazioni di sistema, fare clic su **Browse** (accanto al campo **Exporting**), definire la destinazione e fare clic su **Export**.
- (4) Per ripristinare le configurazioni predefinite, fare clic su **Default** e quindi confermare l'operazione. Il dispositivo si riavvierà e ripristinerà le configurazioni predefinite. Facendo clic su **Default** quando la casella di controllo è selezionata, tutte le impostazioni del dispositivo saranno ripristinate ai valori predefiniti di fabbrica.

(4) Raccolta di Informazioni Diagnostiche

Le informazioni diagnostiche includono log e configurazioni del sistema. È possibile esportare le informazioni diagnostiche sul computer.

(1) Fare clic su **Setup > System > Maintenance**.

Figura 7-45 Interfaccia di Raccolta Informazioni Diagnostiche



- (2) Fare clic su **Export**. Selezionare la cartella locale per memorizzare le informazioni, nella casella di dialogo visualizzata.



NOTA!

- Le informazioni diagnostiche sono esportate nella cartella locale sotto forma di un file compresso. Occorre decomprimere il file tramite uno strumento come WinRAR e quindi aprirlo con un editor di testo.
 - Selezionando **Collect Image Debugging Info**, è possibile visualizzare video con le informazioni di debug annesse, semplificando la risoluzione dei problemi.
-

8 Domande Frequenti

(1) Cosa devo fare se non viene visualizzato alcun messaggio per l'installazione di ActiveX quando accedo su un computer con Windows 7 per la prima volta?

Risposta: Attenersi ai seguenti passaggi per disattivare UAC e quindi eseguire di nuovo l'accesso:

1. Fare clic sul pulsante **Start**, quindi su **Pannello di controllo**.
2. Nel campo di ricerca, digitare `uac`, quindi fare clic su **Modificare le impostazioni di controllo dell'account**.
3. Spostare il dispositivo di scorrimento su **Never Notify**, quindi fare clic su **OK**.
4. Una volta disattivato il Controllo dell'account utente, effettuare di nuovo l'accesso.

(2) Cosa devo fare se l'installazione di ActiveX non riesce

Risposta: Se l'installazione non riesce, aggiungere l'indirizzo IP della telecamera come sito attendibile: aprire **Opzione Internet** in IE, fare clic sulla scheda **Security**, fare clic su **Trusted sites**, quindi su **Sites** per aggiungere il sito web.

Se si utilizza Windows 7, occorre salvare per prima cosa il file **setup.exe** sul computer, quindi fare clic sul file con il tasto destro del mouse, selezionare **Run as administrator** e quindi installarlo seguendo le istruzioni.

(3) Cosa devo fare se il video live non funziona quando accedo per la prima volta?

Risposta: Chiudere il firewall sul computer e quindi accedere di nuovo all'interfaccia web.