



**Terminale di controllo accessi con
lettore di impronte digitali
serie DS-K1T804**

Manuale dell'utente



Informazioni legali

Manuale dell'utente

©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

Informazioni sul presente manuale

Il presente manuale è protetto da copyright nazionale e internazionale. Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") detiene tutti i diritti sul presente manuale. Il presente manuale non può essere riprodotto, modificato, tradotto o distribuito, parzialmente o totalmente, con qualsiasi mezzo, senza previa autorizzazione scritta di Hikvision.

Utilizzare il presente manuale dell'utente sotto la supervisione di

tecnici professionisti. **Marchi commerciali**

HIKVISION e gli altri marchi Hikvision sono di proprietà di Hikvision e sono marchi registrati o oggetto di richiesta di registrazione da parte di Hikvision e/o delle sue affiliate. Gli altri marchi commerciali citati nel presente manuale sono di proprietà dei rispettivi titolari. Non si concede alcun diritto di licenza all'utilizzo di tali marchi senza espressa autorizzazione.

Esclusione di responsabilità

NELLA MASSIMA MISURA PREVISTA DALLA LEGGE VIGENTE, HIKVISION ESCLUDE OGNI GARANZIA, ESPLICITA O IMPLICITA, COMPRESA, A TITOLO DI ESEMPIO, LE GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ A UNO SCOPO SPECIFICO, IN RELAZIONE AL PRESENTE MANUALE. HIKVISION NON ASSICURA, GARANTISCE NÉ DICHIARA ALCUNCHÉ IN RELAZIONE ALL'USO DEL MANUALE O ALLA CORRETTEZZA, ALLA PRECISIONE O ALL'AFFIDABILITÀ DELLE INFORMAZIONI IVI CONTENUTE. L'UTILIZZO DEL PRESENTE MANUALE E L'EVENTUALE AFFIDAMENTO SU DI ESSO SONO INTERAMENTE A RISCHIO DELL'UTENTE E RIENTRANO NELLA SUA RESPONSABILITÀ. IN RIFERIMENTO AI PRODOTTI CON ACCESSO A INTERNET, L'USO DEL PRODOTTO È DA CONSIDERARSI TOTALMENTE A RISCHIO DELL'UTENTE. HIKVISION NON SI ASSUME ALCUNA RESPONSABILITÀ IN CASO DI FUNZIONAMENTO ANOMALO, VIOLAZIONE DELLA RISERVATEZZA, O ALTRI DANNI DERIVANTI DA ATTACCHI INFORMATICI, ATTACCHI DI HACKER, INFEZIONE DA VIRUS O ALTRI RISCHI LEGATI ALLA SICUREZZA SU INTERNET; HIKVISION FORNIRÀ TUTTAVIA TEMPESTIVO SUPPORTO TECNICO OVE NECESSARIO.

LE NORMATIVE CONCERNENTI LA SORVEGLIANZA VARIANO DA UNA GIURISDIZIONE ALL'ALTRA. VERIFICARE TUTTE LE NORMATIVE APPLICABILI NELLA PROPRIA GIURISDIZIONE PRIMA DI UTILIZZARE IL PRESENTE PRODOTTO IN MODO DA GARANTIRE CHE L'USO SIA CONFORME ALLA LEGGE VIGENTE. HIKVISION NON SARÀ RESPONSABILE NEL CASO IN CUI IL PRESENTE PRODOTTO SIA UTILIZZATO PER FINI ILLECITI.

IN CASO DI CONFLITTO TRA IL PRESENTE MANUALE E LA LEGGE VIGENTE, PREVARRÀ QUEST'ULTIMA.




Protezione dei dati

Durante l'utilizzo del dispositivo, saranno raccolti, archiviati ed elaborati dati personali. Per proteggere i dati, sviluppiamo i dispositivi Hikvision applicando i principi della protezione dei dati fin dalla progettazione. Ad esempio, nel caso dei dispositivi con funzioni di riconoscimento facciale, i dati biometrici memorizzati nel dispositivo dell'utente vengono crittografati, mentre i dispositivi di lettura delle impronte digitali salvano solo il modello dell'impronta digitale, il che rende impossibile la ricostruzione di un'immagine dell'impronta stessa.

Ai responsabili del trattamento dei dati, si richiede di intraprendere azioni per la raccolta, l'archiviazione, l'elaborazione e il trasferimento dei dati in conformità alle leggi e ai regolamenti applicabili in materia di protezione dei dati, inclusi, senza limitazioni, implementazione di controlli di sicurezza per salvaguardare i dati personali, ad es. controlli di sicurezza amministrativi e fisici ragionevoli, nonché condurre revisioni e valutazioni periodiche dell'efficacia dei suddetti controlli di sicurezza.

Significato dei simboli

I simboli contenuti nel presente documento sono definiti di seguito.

Simbolo	Descrizione
 Pericolo	Indica situazioni potenzialmente pericolose che, se non evitate, causano o potrebbero causare lesioni gravi o mortali.
 Attenzione	Indica una potenziale situazione di pericolo che, se non evitata, potrebbe provocare danni all'apparecchiatura, perdite di dati, riduzione delle prestazioni o imprevisti.
 Nota	Fornisce informazioni aggiuntive per evidenziare o integrare punti importanti del testo principale.

Informazioni sulle normative

Informazioni sulle norme FCC

Tenere presente che modifiche o alterazioni non espressamente approvate dalla parte responsabile della conformità potrebbero invalidare l'autorità dell'utente ad utilizzare l'apparecchiatura.

Conformità alle norme FCC: la presente apparecchiatura è stata sottoposta a test e dichiarata conforme ai limiti stabiliti per i dispositivi digitali di Classe B, in conformità alla Parte 15 delle Norme FCC. Questi limiti sono pensati per fornire una ragionevole protezione contro le interferenze dannose in installazioni residenziali. Questo dispositivo genera, utilizza e può emettere energia a radiofrequenza e, se non installato e utilizzato in conformità alle istruzioni, può causare interferenze dannose alle comunicazioni radio. Tuttavia, non esistono garanzie che l'interferenza non si verifichi in una particolare installazione. Se l'apparecchio provoca interferenze dannose alle ricezioni radiotelevisive, riscontrabili spegnendo e accendendo l'apparecchio, si consiglia di provare a correggerle adottando uno o più dei seguenti accorgimenti:

- Riorientare o riposizionare l'antenna di ricezione.
- Aumentare la distanza tra l'apparecchio e il ricevitore.
- Collegare il dispositivo a una presa su un circuito diverso da quello a cui è collegato il ricevitore.
- Consultare un rivenditore o un tecnico radio/TV per ricevere assistenza

Installare e utilizzare l'apparecchiatura mantenendo una distanza di almeno 20 cm tra il radiatore e il proprio corpo.

Norme FCC

Questo dispositivo è conforme alla parte 15 delle norme FCC.

L'utilizzo è soggetto alle due condizioni seguenti:

1. Il dispositivo non deve causare interferenze dannose.
2. Il dispositivo deve accettare qualsiasi interferenza ricevuta, incluse le interferenze che possono causare un funzionamento indesiderato.

Dichiarazione di Conformità UE



Questo prodotto e gli eventuali accessori in dotazione sono contrassegnati con il marchio "CE" e sono quindi conformi alle norme europee armonizzate vigenti di cui alla Direttiva CEM 2014/30/UE e alla Direttiva RoHS 2011/65/UE



2012/19/UE (Direttiva RAEE): i prodotti contrassegnati con il presente simbolo non possono essere smaltiti come rifiuti municipali indifferenziati nell'Unione Europea. Per garantire un riciclaggio adeguato, restituire il presente prodotto al proprio rivenditore locale in occasione dell'acquisto di una nuova

apparecchiatura equivalente, oppure smaltirlo nei punti di raccolta designati. Ulteriori informazioni sono disponibili sul sito:

www.recyclethis.info



2006/66/CE (Direttiva sulle batterie): questo prodotto contiene una batteria e non è possibile smaltirlo con i rifiuti municipali indifferenziati nell'Unione Europea. Fare riferimento alla documentazione del prodotto per le informazioni specifiche sulla batteria. La batteria è contrassegnata con il presente simbolo, che potrebbe includere le sigle di cadmio (Cd), piombo (Pb) o mercurio (Hg). Per garantire un riciclaggio adeguato, consegnare la batteria al proprio rivenditore locale oppure

smaltirla nei punti di raccolta designati. Ulteriori informazioni sono disponibili sul sito: www.recyclethis.info

Conformità alla normativa canadese ICES-003

Il presente dispositivo soddisfa i requisiti degli standard CAN ICES-3 (B)/NMB-3(B).

Questo dispositivo è conforme agli standard RSS di Industry Canada per i dispositivi esenti da licenza. L'utilizzo è soggetto alle due condizioni seguenti:

1. Il dispositivo non deve causare interferenze e
2. deve accettare qualsiasi interferenza, incluse le interferenze che possono causare un funzionamento indesiderato del dispositivo.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Ai sensi delle normative di Industry Canada, questo trasmettitore radio può funzionare solo utilizzando un'antenna di tipo e guadagno massimo (o inferiore) approvati per il trasmettitore da Industry Canada. Per ridurre le potenziali interferenze radio nei confronti di altri utenti, il tipo di antenna e il relativo guadagno devono essere scelti in modo che la potenza isotropica irradiata equivalente (EIRP) non sia superiore a quella necessaria per una comunicazione corretta.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Installare e utilizzare l'apparecchiatura mantenendo una distanza di almeno 20 cm tra il radiatore e il proprio corpo.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.



Istruzioni di sicurezza

Le presenti istruzioni servono a garantire che l'utente possa utilizzare il prodotto correttamente, evitando pericoli e danni alla proprietà.

Le misure precauzionali sono indicate con le diciture "Pericolo" e "Attenzione":

Pericolo: ignorare le avvertenze può causare lesioni gravi o mortali.

Attenzione: ignorare le precauzioni può causare lesioni alle persone o danni all'apparecchiatura.

	
Pericolo: seguire queste misure di sicurezza per evitare lesioni gravi o mortali.	Attenzione: seguire queste precauzioni per evitare lesioni alle persone o danni materiali.

Pericolo

- Tutte le operazioni elettroniche devono essere rigorosamente conformi alle disposizioni sulla sicurezza elettrica e sulla prevenzione degli incendi e a qualsiasi altra disposizione locale in materia.
- Utilizzare solo alimentatori forniti da produttori affidabili. La potenza nominale non può essere inferiore al valore indicato.
- Non collegare più dispositivi ad un unico adattatore di corrente, in quanto il sovraccarico potrebbe provocarne il surriscaldamento o causare un incendio.
- Accertarsi che la corrente sia stata scollegata prima di effettuare il cablaggio, installare o smontare il dispositivo.
- Fissare saldamente il prodotto se lo si installa su una parete o al soffitto.
- Se il dispositivo emana fumo, odori o rumori, spegnere l'alimentazione e scollegare il cavo di alimentazione, quindi rivolgersi al centro assistenza.
- Non ingerire la batteria. Pericolo di ustioni chimiche. Questo prodotto contiene una batteria a bottone. Se la batteria a bottone viene ingerita, può causare gravi ustioni interne in sole 2 ore e portare alla morte. Tenere le batterie nuove e usate lontano dalla portata dei bambini. Se il vano batteria non si chiude in modo sicuro, interrompere l'uso del prodotto e tenerlo lontano dalla portata dei bambini. Se si ritiene che le batterie siano state ingerite o poste all'interno di una qualsiasi parte del corpo, rivolgersi immediatamente a un medico.
- Se il prodotto non funziona correttamente, rivolgersi al rivenditore o al centro di assistenza più vicino. Non cercare di smontare il dispositivo da soli. Non ci assumiamo alcuna responsabilità in relazione a problemi causati da interventi non autorizzati di riparazione o manutenzione.

⚠ **Attenzione**

- Non far cadere il dispositivo, non sottoporlo a urti e non esporlo a forti radiazioni elettromagnetiche. Evitare di installare il dispositivo su superfici vibranti o in luoghi a rischio di impatti (ignorare questa precauzione può causare danni all'apparecchiatura).
- Non mettere il dispositivo in luoghi troppo caldi (fare riferimento alle specifiche tecniche per informazioni dettagliate sulle temperature di funzionamento), freddi, polverosi o umidi e non esporlo a forti radiazioni elettromagnetiche.
- Tenere il coperchio del dispositivo per l'uso in ambienti chiusi lontano da pioggia e umidità.
- Per evitare il pericolo di incendio, non collocare l'apparecchio alla luce diretta del sole, in luoghi poco ventilati o vicino a fonti di calore.
- Non collocare il dispositivo al sole o in luoghi molto luminosi. Ciò potrebbe causare uno sbiadimento o la formazione di macchie (che tuttavia non sono segni di malfunzionamento) e avere effetti sulla durata del sensore.
- Utilizzare il guanto in dotazione per aprire il coperchio del dispositivo ed evitare il contatto diretto con il coperchio, in quanto l'acido contenuto nel sudore delle dita può corroderne il rivestimento.
- Pulire le superfici interne ed esterne del coperchio con un panno morbido e asciutto. Non utilizzare detergenti alcalini.
- Conservare il materiale d'imballaggio per un eventuale uso futuro. In caso di guasti, sarà necessario inviare il dispositivo al sito di produzione con l'imballaggio originale. Il trasporto senza l'imballaggio originale potrebbe causare danni al dispositivo e ulteriori costi.
- L'uso improprio o la sostituzione della batteria eseguita in modo non corretto possono provocare esplosioni. Sostituirla soltanto con una batteria dello stesso tipo o equivalente. Smaltire le batterie esaurite conformemente alle istruzioni fornite dal produttore della batteria.
- È possibile visualizzare la licenza del dispositivo tramite il sito Web: <http://opensource.hikvision.com/Home/List?id=46>.

Modelli disponibili

Il terminale di controllo accessi con lettore di impronte digitali comprende i seguenti modelli:

Nome del prodotto	Modello	Descrizione
Terminale di controllo accessi con lettore di impronte digitali	DS-K1T804F	Supporta solo impronte digitali.
	DS-K1T804MF	Supporta il passaggio di tessere M1.
	DS-K1T804EF	Supporta il passaggio di tessere EM.

Utilizzare solo gli alimentatori indicati nel presente manuale:

Modello	Produttore	Standard
DSA-12PFT-12FUK 120100	Dee Van Enterprise Co., Ltd.	BS
DSA-12PFT-12FAU 120100	Dee Van Enterprise Co., Ltd.	AS
DSA-12PFT-12FIN 120100	Dee Van Enterprise Co., Ltd.	IS
DSA-12PFT-12FUS 120100	Dee Van Enterprise Co., Ltd.	IEC
DSA-12PFT-12 FBZ 120100	Dee Van Enterprise Co., Ltd.	NBR
ADS-12B-12 12012E	Shenzhen Honor Electronics Co., Ltd.	IEC
ADS-12B-12 12012E	Shenzhen Honor Electronics Co., Ltd.	NEMA
ADS-12B-12 12012E	Shenzhen Honor Electronics Co., Ltd.	NBR
ADS-12B-12 12012E	Shenzhen Honor Electronics Co., Ltd.	BS

Indice

1	Panoramica	1
2	Funzioni	1
3	Descrizione dell'aspetto	2
4	Cablaggio del dispositivo	4
4.1	Descrizione dei terminali	4
4.2	Cablaggio del dispositivo esterno	6
4.3	Cablaggio dell'unità di controllo porta protetta DS-K2M060.....	6
5	Installazione	6
6	Attivazione.....	8
6.1	Attivazione tramite dispositivo	8
6.2	Attivazione tramite SADP.....	9
6.3	Attivazione del dispositivo tramite il software client.....	10
7	Impostazioni locali.....	10
7.1	Selezione della lingua.....	10
7.2	Aggiunta di amministratori	11
7.3	Accesso locale	13
7.4	Impostazioni di comunicazione.....	13
7.4.1	Impostazione della rete.....	13
7.4.2	Impostazione dei parametri Wi-Fi	13
7.4.3	Impostazione dei parametri EHome	14
7.5	Gestione delle persone	15
7.5.1	Aggiunta di persone	15
7.5.2	Gestione delle persone (Ricerca/Modifica/Eliminazione).....	18
7.6	Stato di presenza	18
7.6.1	Impostazione della presenza automatica....	18
7.6.2	Impostazione della presenza manuale	19

7.6.3	Impostazione della presenza manuale e automatica.....	20
7.6.4	Disattivazione della modalità di presenza .	21
7.7	Gestione di orari e presenze	22
7.7.1	Gestione dei reparti (Modifica/Ricerca/Ripristino).....	22
7.7.2	Gestione dei turni.....	23
7.7.3	Gestione delle ferie (Aggiunta/Ricerca/Modifica/Eliminazione)	25
7.7.4	Pianificazione dei turni	26
7.7.5	Esportazione del report delle presenze	28
7.7.6	Trasferimento dei dati.....	29
7.8	Impostazioni di sistema	29
7.8.1	Impostazione dell'ora	29
7.8.2	Gestione dei dati di sistema	30
7.8.3	Impostazione dei parametri di sistema	31
7.8.4	Aggiornamento del sistema.....	32
7.8.5	Ripristino delle impostazioni	33
7.8.6	Visualizzazione delle informazioni di sistema.....	33
8	Configurazione del software client.....	34
8.1	Aggiunta di un dispositivo	34
8.1.1	Aggiunta di dispositivi online.....	34
8.1.2	Aggiunta di un dispositivo tramite l'indirizzo IP o il nome dominio	37
8.1.3	Aggiunta di dispositivi tramite segmento IP.....	38
8.1.4	Aggiunta di dispositivi tramite account EHome	39
8.1.5	Importazione di dispositivi in batch.....	40
8.2	Gestione delle persone	41
8.2.1	Aggiunta di organizzazioni.....	42
8.2.2	Configurazione delle informazioni di base...	42

8.2.3 Emissione di una tessera per una persona	43
8.2.4 Raccolta delle impronte digitali tramite il client	44
8.2.5 Raccolta di impronte digitali tramite dispositivo di controllo accessi.....	45
8.2.6 Configurazione delle informazioni sul controllo degli accessi	46
8.2.7 Personalizzazione delle informazioni personali	47
8.2.8 Configurazione di ulteriori informazioni....	48
8.2.9 Importazione ed esportazione di informazioni di identificazione personali	48
8.2.10 Importazione delle informazioni delle persone	48
8.2.11 Esportazione di informazioni delle persone	49
8.2.12 Recupero delle informazioni delle persone dal dispositivo di controllo accessi	49
8.2.13 Trasferimento di persone a un'altra organizzazione	50
8.2.14 Rilascio di tessere a persone in batch.....	50
8.2.15 Segnalazione di smarrimento della tessera	51
8.2.16 Impostazione dei parametri di emissione delle tessere.....	51
8.3 Configurazione di pianificazioni e modelli	52
8.3.1 Aggiunta di ferie	53
8.3.2 Aggiunta di modelli	53
8.4 Impostazione di un gruppo di accesso per l'assegnazione di autorizzazioni di accesso alle persone	55
8.5 Configurazione delle funzioni avanzate	56
8.5.1 Configurazione dei parametri del dispositivo.....	56
8.5.2 Configurazione per mantenere aperta/chiusa una porta	60

8.5.3 Configurazione della regola Wiegand personalizzata	62
8.5.4 Configurazione della modalità di autenticazione e di pianificazione del lettore di tessere	63
8.5.5 Configurazione dei parametri del dispositivo.....	64
8.6 Configurazione delle azioni di collegamento per il controllo accessi.....	69
8.6.1 Configurazione delle azioni del client per gli eventi di accesso	69
8.6.2 Configurazione delle azioni del dispositivo per gli eventi di accesso	70
8.6.3 Configurazione delle azioni del dispositivo per il passaggio della tessera	72
8.6.4 Configurazione delle azioni del dispositivo per ID della persona.....	73
8.7 Controllo delle porte.....	74
8.7.1 Controllo dello stato della porta.....	75
8.7.2 Controllo dei record di accesso in tempo reale	76
8.8 Modulo Event Center	76
8.8.1 Attivazione della ricezione di notifiche degli eventi dai dispositivi.....	76
8.8.2 Visualizzazione degli eventi in tempo reale ...	77
8.8.3 Ricerca di eventi nella cronologia.....	78
8.9 Orari e presenze.....	81
8.9.1 Configurazione dei parametri di presenza...	81
8.9.2 Aggiunta di tabelle di orari	86
8.9.3 Aggiunta di turni.....	87
8.9.4 Gestione della pianificazione dei turni	88
8.9.5 Correzione manuale del record di check-in/check-out	92
8.9.6 Aggiunta di congedi, permessi e viaggi di lavoro	93

8.9.7 Calcolo dei dati sulle presenze	94
8.9.8 Statistiche delle presenze.....	95
9 Configurazione remota (Web).....	98
9.1 Gestione dell'ora.....	98
9.2 Impostazione delle informazioni di rete	98
9.2.1 Impostazioni dei parametri di rete	98
9.2.2 Impostazioni dei parametri del centro di rete	99
9.3 Modifica della password del dispositivo	99
9.4 Impostazioni della modalità di sicurezza.....	100
9.5 Manutenzione del sistema.....	100
9.6 Visualizzazione delle informazioni del dispositivo	101
A. Suggerimenti per la scansione delle impronte digitali	102
B. Capacità di controllo accessi.....	103
C. Regola di eliminazione dei record delle presenze ...	105
D. Tabella dei report delle presenze	105
E. Descrizioni delle regole Wiegand personalizzate	110

1 Panoramica

Il terminale di controllo accessi con lettore di impronte digitali serie DS-K1T804 è dotato di uno schermo LCD da 2,4 pollici. Sono supportate anche le modalità di trasmissione con funzionamento offline, rete cablata (TCP/IP) e rete wireless. I modelli con -1 non supportano la funzione di rete wireless.

2 Funzioni

- Design del pulsante del campanello fisico, supporta il collegamento del campanello esterno
- Gestione integrata del controllo degli accessi e delle presenze
- Schermo LCD da 2,4 pollici per visualizzare l'ora, la data e i risultati dell'autenticazione tramite il passaggio della tessera/impronta digitale
- Modalità di trasmissione con rete cablata (TCP/IP) e rete wireless
- Massimo 3000 utenti, massimo 3000 impronte digitali, massimo 100.000 record di eventi e massimo 150.000 record di presenze
- È possibile configurare diversi tipi di autenticazione in base alle diverse situazioni
- Funzionamento indipendente: consente di aggiungere a livello locale informazioni su persone, tessere e impronte digitali
- Consente di esportare i dati dei passaggi delle tessere e il report delle presenze sull'unità flash USB
- È possibile configurare fino a 32 turni normali, 32 turni ore-uomo e 32 pianificazioni per le ferie
- Genera automaticamente il report delle presenze
- Autenticazione del terminale e dell'utente
- Lettura della tessera EM (per DS-K1T804EF)
- Lettura della tessera Mifare, inclusa la lettura del numero di tessera (per DSK1T804MF)
- Unità di controllo porta protetta DS-K2M060 con collegamento RS-485
- Rilevamento delle manomissioni, allarme durata eccessiva sblocco, allarme numero eccessivo di passaggi di tessera non valida, allarme tessera di coercizione, ecc.
- Supporta più lingue: inglese, vietnamita, portoghese brasiliano, spagnolo, francese, italiano, arabo e thailandese
- Visualizzazione accurata dei dati e dell'ora grazie all'orologio elettronico incorporato
- Controllo dello stato di funzionamento del dispositivo tramite watchdog. Quando si verifica uno stato di eccezione, il sistema si riavvia automaticamente
- I dati possono essere salvati in modo permanente dopo lo spegnimento

- Controllo da remoto tramite il software client
- Supporta l'attivazione da parte di dispositivi esterni
- Supporta la trasmissione dei dati tramite EHome per realizzare la trasmissione dell'intera rete
- Funziona tramite client mobile Hik-Connect
- Anticlonazione di tag NFC

3 Descrizione dell'aspetto

Di seguito sono riportati l'aspetto del dispositivo e la descrizione della tastiera.

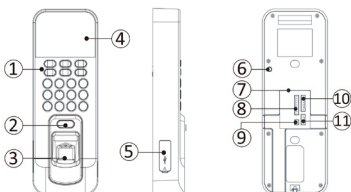


Figura 3-1 Aspetto del dispositivo



Nota

Le immagini che seguono servono solo come riferimento. Alcuni modelli non supportano la funzione di passaggio delle tessere. Per dettagli, fare riferimento al prodotto in uso.

Tabella 3-1 Descrizione dell'aspetto

N.	Descrizione
1	Tastierino
2	Tasto campanello
3	Modulo di lettura delle impronte digitali
4	Schermata con display LCD da 2,4 pollici
5	Pulsante Reset/Interfaccia USB (all'interno del coperchio)
6	Pulsante antimanomissione
7	Porta Ethernet
8	Morsettiera RS-485/ Wiegand
9	Interfaccia di alimentazione da 12 V
10	Morsettiera serratura porta
11	Morsettiera allarme

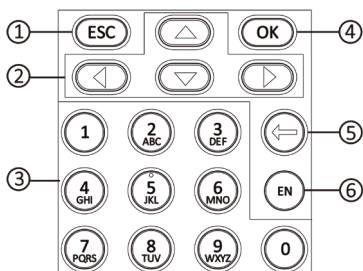






Figura 3-2 Descrizione della tastiera

Tabella 3-2 Descrizione della tastiera

N.	Descrizione
1	<p>Tasto di uscita: premere il tasto per uscire dal menu.</p> <p> Nota</p> <p>Se si attiva la funzione di stato di presenza, il tasto di uscita può essere programmato come il tasto di scelta rapida dello stato di presenza.</p>
2	<p>Tasti freccia: utilizzare i tasti freccia per spostare il cursore nel menu.</p> <p> Nota</p> <ul style="list-style-type: none"> • Se si attiva la funzione di stato di presenza, i tasti freccia possono essere tasti di scelta rapida dello stato di presenza. • Nella pagina di inserimento dati, utilizzare il tasto freccia per modificare il metodo di immissione.
3	<p>Tasti alfanumerici: premere per immettere numeri o lettere.</p> <p> Nota</p> <p>Il tasto 0 può anche permettere di aggiungere uno spazio, eccetto quando si utilizza il metodo di immissione di numeri.</p>
4	<p>Tasto OK: premere il tasto OK per confermare le operazioni. Tenere premuto il tasto per 2 secondi per accedere all'interfaccia di accesso.</p> <p> Nota</p> <p>Se si attiva la funzione di stato di presenza, il tasto OK può essere il tasto di scelta rapida dello stato di presenza.</p>

N.	Descrizione
5	Tasto di eliminazione: premere il tasto per eliminare le lettere o i numeri uno alla volta nella casella di testo.
6	Tasto di modifica: tenere premuto il tasto per spostarsi tra numeri/lettere minuscole, numeri/lettere maiuscole e simboli.

4 Cablaggio del dispositivo

4.1 Descrizione dei terminali

Lo schema dei terminali è il seguente.

Figura 4-1 Schema dei terminali

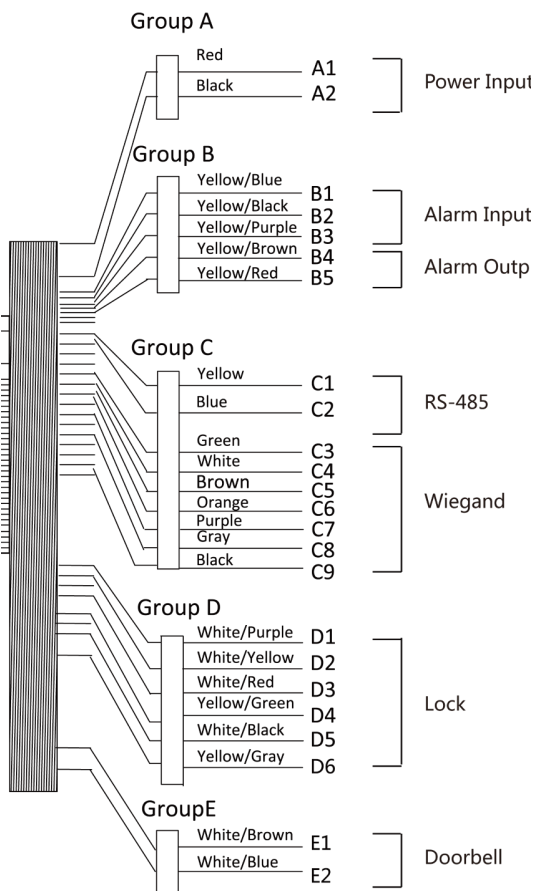


Tabella 4-1 Descrizione del cablaggio con unità di controllo porta protetta

Gruppo di cavi	N.	Funzione	Colore	Nome terminale	Descrizione	
Gruppo A	A1	Ingresso alimentazione	Rosso	+12 V	Alimentazione 12 V CC	
	A2		Nero		GND	GND
Gruppo B	B1	Ingresso allarme	Giallo/Blu		IN1	Ingresso allarme 1
	B2		Giallo/Nero		GND	GND
	B3	Uscita allarme	Giallo/Viola		NC	Cablaggio uscita di allarme
	B4		Giallo/Marrone		COM	
	B5		Giallo/Rosso		NO	
Gruppo C	C1	RS-485 Comunicazione	Giallo		485+	Cablaggio RS-485
	C2		Blu		485-	
	C3	Wiegand	Verde		W0	Cablaggio Wiegand 0
	C4		Bianco		W1	Cablaggio Wiegand 1
	C5		Marrone		WG_OK	Wiegand autenticato
	C6		Arancione		WG_ERR	Autenticazione Wiegand non riuscita
	C7		Viola		WG_BEEP	Cablaggio avvisatore acustico
	C8		Grigio		WG_TAMP	Cablaggio allarme antimanomissione
	C9		Nero		GND	GND
Gruppo D	D1	Blocco	Bianco/Viola		NC	Cablaggio blocco
	D2		Bianco/Giallo		COM	
	D3		Bianco/Rosso		NO	
	D4		Giallo/Verde		SENSOR	Ingresso segnale del contatto porta
	D5		Bianco/Nero		GND	GND
	D6		Giallo/Grigio		BUTTON	Cablaggio porta d'uscita
Gruppo E	E1	Campanello	Bianco/Marrone		BELL+	Campanello Cablaggio
	E2		Bianco/Blu		BELL-	

4.2 Cablaggio del dispositivo esterno

Eseguire il cablaggio del dispositivo esterno.

Lo schema di cablaggio è il seguente.

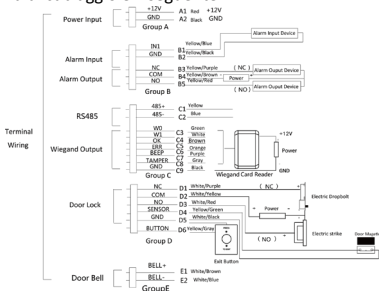


Figura 4-2 Cablaggio del dispositivo esterno



Nota

L'alimentazione esterna e il terminale di controllo accessi devono utilizzare lo stesso cavo GND.

4.3 Cablaggio dell'unità di controllo porta protetta DS-K2M060

Lo schema di cablaggio è il seguente:

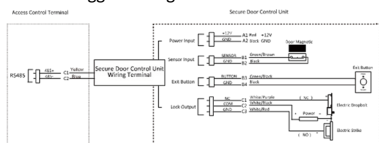


Figura 4-3 Cablaggio dell'unità di controllo porta



Nota

- L'alimentazione esterna e l'unità di controllo porta protetta DS-K2M060 devono utilizzare lo stesso cavo GND.
- Se si desidera collegare un'unità di controllo porta protetta, è necessario impostare la modalità di connessione su **Connect Extension Module** nelle impostazioni RS-485 nel software client.

5 Installazione

Prima di iniziare

- Assicurarsi che il dispositivo nell'imballaggio sia in buone condizioni e che siano presenti tutte le parti necessarie per l'assemblaggio.
- Verificare che la parete sia abbastanza resistente da reggere un peso triplo rispetto a quello del dispositivo.

Passaggi

1. Installare la scatola portafrutti da 120 nella parete.

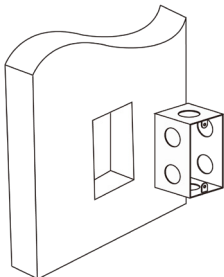


Figura 5-1 Installazione della scatola portafrutti

2. Instradare i cavi facendoli passare attraverso il foro della base di montaggio.
3. Fissare con 2 viti (in dotazione) la piastra di montaggio del dispositivo sulla scatola portafrutti.

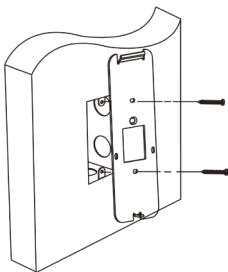


Figura 5-2 Installazione della piastra di montaggio

4. Collegare i cavi corrispondenti.
5. Allineare il dispositivo alla piastra di montaggio. Spingere il terminale nella piastra di montaggio dal basso verso l'alto. Fissare il terminale sulla piastra con i fermi.

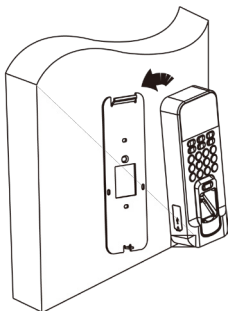


Figura 5-3 Installazione del dispositivo

6. Fissare il dispositivo sulla piastra di montaggio con una vite e completare l'installazione.

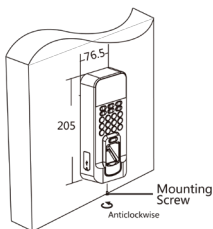


Figura 5-4 Fissaggio



Nota

Le immagini riportate in questo documento servono solo come riferimento. Fare riferimento al prodotto in uso.

6 Attivazione

Attivare il dispositivo prima di effettuare l'accesso per la prima volta. Dopo l'accensione del dispositivo, il sistema passa alla pagina Device Activation.

Sono supportate l'attivazione tramite il dispositivo, lo strumento SADP e il software client.

I valori predefiniti del dispositivo sono i seguenti:

- Indirizzo IP predefinito: 192.0.0.64
- Numero di porta predefinito: 8000
- Nome utente predefinito: admin

6.1 Attivazione tramite dispositivo

Se il dispositivo non viene attivato prima del primo accesso, il sistema accede all'interfaccia Device Activation dopo l'accensione.

Passaggi

1. Creare una password per l'attivazione del dispositivo.
2. Confermare la password.



Nota

Premere il tasto su o giù sulla tastiera per modificare il metodo di immissione.

3. Premere **OK** per attivare il



Nota

Si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.

Come continuare

Dopo l'attivazione del dispositivo, si accede alla pagina di aggiunta degli amministratori. Aggiungere un amministratore prima eseguire altre operazioni.

6.2 Attivazione tramite SADP

SADP è uno strumento che consente di rilevare, attivare e modificare l'indirizzo IP del dispositivo sulla LAN.

Prima di iniziare

- È possibile ottenere il software SADP dal disco in dotazione o sul sito ufficiale <http://www.hikvision.com/en/> e installare SADP seguendo le istruzioni.
- Il dispositivo e il PC su cui è in esecuzione lo strumento SADP devono trovarsi all'interno della stessa subnet.

I seguenti passaggi mostrano come attivare un dispositivo e modificarne l'indirizzo IP. Per i dettagli sull'attivazione in batch e la modifica degli indirizzi IP, fare riferimento al *Manuale dell'utente di SADP*.

Passaggi

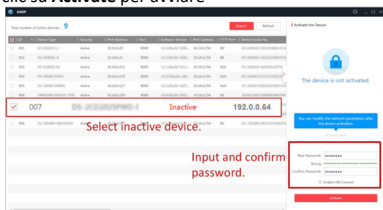
1. Eseguire il software SADP per cercare i dispositivi online.
2. Trovare e selezionare il proprio dispositivo nell'elenco dei dispositivi online.
3. Inserire la nuova password (password amministratore) e confermarla.



Attenzione

PASSWORD COMPLESSA CONSIGLIATA: si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, che comprendano lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.

4. Fare clic su **Attivate** per avviare



Lo stato del dispositivo diventa **Active** dopo l'attivazione.

5. Modificare l'indirizzo IP del dispositivo.

- 1) Selezionare il dispositivo.
- 2) Cambiare l'indirizzo IP del dispositivo con quello della stessa subnet alla quale è connesso il computer modificando l'indirizzo IP manualmente oppure selezionando **Enable DHCP**.

- 3) Inserire la password dell'amministratore e fare clic su **Modify** per applicare la modifica dell'indirizzo IP.

6.3 Attivazione del dispositivo tramite il software client


Alcuni dispositivi richiedono la creazione di una password di attivazione, per poter essere aggiunti al software e funzionare correttamente.

Passaggi



Nota

Questa funzione deve essere supportata dal dispositivo.

1. Accedere alla pagina Device Management.
 2. Fare clic su  sulla destra di **Device Management** e selezionare **Device**.
 3. Fare clic su **Online Device** per visualizzare l'area del dispositivo online.
I dispositivi online cercati vengono visualizzati nell'elenco.
 4. Controllare lo stato del dispositivo (visualizzato nella colonna **Security Level**) e selezionare un dispositivo inattivo.
 5. Fare clic su **Activate** per aprire la finestra di dialogo Activation.
 6. Inserire una password nel relativo campo e confermarla.
-



Attenzione

Il sistema è in grado di valutare automaticamente la complessità della password del dispositivo. Si consiglia vivamente di modificare la password scelta (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.

Rientra nella responsabilità dell'installatore e/o dell'utente finale configurare correttamente tutte le password e altri parametri di sicurezza.

7. Fare clic su **OK** per attivare il dispositivo.

7 Impostazioni locali

7.1 Selezione della lingua

È possibile selezionare una lingua per il sistema del dispositivo.

Dopo l'attivazione del dispositivo, è possibile selezionare una lingua per il sistema del dispositivo.

Per impostazione predefinita, la lingua del sistema è l'inglese.



Nota

Dopo aver modificato la lingua del sistema, il dispositivo sarà riavviato automaticamente.

7.2 Aggiunta di amministratori

Dopo l'attivazione del dispositivo e la selezione della lingua del sistema, è necessario aggiungere un amministratore. È possibile impostare il nome utente dell'amministratore e il numero della tessera. È inoltre possibile aggiungere l'impronta digitale dell'utente, impostare la password, il reparto e la modalità di autenticazione.

Passaggi

1. Spostare il cursore e selezionare **User** → **New** per accedere alla pagina New.

The screenshot shows a terminal-style interface for adding an administrator. The title is 'Add Administrator'. The fields are: ID (1), Name (empty), Card (Set, View Info, 0), FP (Set, 0), PWD (Set, No Configured), Dept. (Set), and Auth. (Controller). At the bottom, there are navigation options: [Esc] Back [OK] Confirm.

Figura 7-1 Aggiunta di amministratori

2. Immettere i parametri del nuovo utente.

ID (ID dipendente)

Per impostazione predefinita, il numero ID aumenterà in sequenza. È possibile modificare l'ID in base alle proprie preferenze.



Nota

- L'ID si riferisce al numero di serie delle presenze dell'utente.
- L'ID deve essere compreso tra 1 e 99999999 e non deve iniziare con 0.
- L'ID deve essere utilizzato una sola volta.

Name

Inserire il nuovo nome utente.



Nota

- Premere il tasto su o giù sulla tastiera per modificare il metodo di immissione.
- Il nome utente può contenere un massimo di 32 caratteri.

Card

Set: passare la tessera nell'area di passaggio delle tessere o immettere manualmente il numero della tessera e selezionare una proprietà per la tessera.

View Info.: visualizzare le informazioni della tessera dell'utente aggiunta.



Nota

- Il numero della tessera è obbligatorio.
 - È possibile inserire fino a 20 cifre nel numero della tessera.
 - Il numero della tessera può essere 0.
 - Il numero della tessera può iniziare con 0 quando contiene più di un numero, ad es. 012345.
 - Il numero della tessera deve essere utilizzato una sola volta.
 - Se il dispositivo non supporta il passaggio delle tessere, è necessario immettere manualmente il numero della tessera. Se è necessario immetterlo manualmente, attivare **Press Key to Input Card No.** Per i dettagli, consultare *Configurazione dei parametri per il dispositivo di controllo accessi.*
-

FP (impronta digitale)

Nella pagina Fingerprint, selezionare un dito e registrarlo in base alle istruzioni vocali.



Nota

- Uno stesso dito non può essere aggiunto più di una volta.
 - È possibile aggiungere fino a 10 impronte digitali per un utente.
 - È inoltre possibile eseguire la scansione delle impronte digitali tramite il registratore di impronte digitali esterno e applicarle al dispositivo tramite il software client.
 - Per informazioni dettagliate sulla scansione dell'impronta digitale, consultare la sezione *Suggerimenti per la scansione delle impronte digitali.*
-

PWD (password)

Creare una password per l'utente e confermarla.



Nota

Sono consentiti fino a 8 caratteri.

Dept. (reparto)

Selezionare un reparto dall'elenco e modificarlo.



Nota

Per informazioni dettagliate sulla modifica del reparto, vedere.

3. Premere **ESC** e selezionare **Yes** per salvare le impostazioni e uscire dalla pagina.

7.3 Accesso locale

Accedere al dispositivo come amministratore per gestire i parametri del dispositivo, tra cui l'utente, il reparto, il turno, le ferie, la pianificazione dei turni, il report, la comunicazione, il sistema, l'ora, ecc.

Tenere premuto **OK** per 3 secondi per accedere alla pagina di accesso. Selezionare FP, Device PWD o Card e autenticarsi per accedere alla home page.



Nota

- Premere il tasto su o giù sulla tastiera per modificare il metodo di immissione.
 - La pagina di accesso varia a seconda del modello di dispositivo. Durante il funzionamento, fare riferimento alla pagina del dispositivo corrente.
-

7.4 Impostazioni di comunicazione

Impostare la rete del dispositivo, i servizi EHome e Hik-Connect.

7.4.1 Impostazione della rete

È possibile impostare i parametri di rete del dispositivo, tra cui l'indirizzo IP, la subnet mask, l'indirizzo del gateway e il DHCP.

Passaggi

1. Spostare il cursore e selezionare **Comm. → Network**.
 2. Premere **OK** per accedere alla pagina Network.
 3. Modificare l'indirizzo IP, la subnet mask e il gateway.
-



Nota

L'indirizzo IP del dispositivo e del PC devono trovarsi nello stesso segmento di rete.

4. **Opzionale:** abilitare il **DHCP**.

Il sistema assegna automaticamente l'indirizzo IP per il dispositivo.

5. Premere **ESC** e selezionare **Yes** per salvare i parametri e tornare al menu precedente.

7.4.2 Impostazione dei parametri Wi-Fi

È possibile attivare la funzione Wi-Fi e trasmettere i dati tramite Wi-Fi.

Passaggi



Nota

La funzione è supportata da alcuni modelli.

1. Spostare il cursore e selezionare **Comm. → Wi-Fi**.
2. Premere **OK** per accedere alla pagina Wi-Fi.

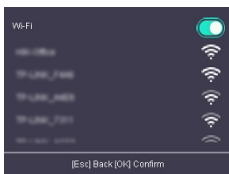


Figura 7-2 Pagina Wi-Fi

3. Attivare la funzione Wi-Fi.
4. Selezionare una rete Wi-Fi dall'elenco e impostare i parametri del Wi-Fi, tra cui la password del Wi-Fi, la modalità IP, l'indirizzo IP, la subnet mask e il gateway.
5. Premere **ESC** e selezionare **Yes** per salvare i parametri.

7.4.3 Impostazione dei parametri EHome

Impostare i parametri EHome e il dispositivo potrà caricare i dati tramite il protocollo EHome.

Prima di iniziare

Assicurarsi che il dispositivo sia connesso a una rete.

Passaggi

1. Spostare il cursore e selezionare **Comm. → EHome**.

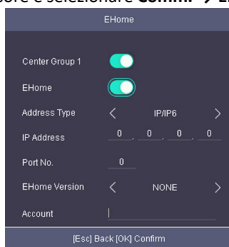


Figura 7-3 Impostazioni EHome

2. Attivare la funzione EHome e impostare i parametri del server EHome.

Center Group 1

Abilitare il gruppo centrale 1 e i dati verranno caricati nel gruppo centrale.

EHome

Abilitare la funzione EHome e i dati verranno caricati tramite il protocollo EHome.

Address Type

Selezionare un tipo di indirizzo in base alle proprie esigenze.

IP Address

Configurare l'indirizzo IP del server EHome.

Port No.

Impostare il numero di porta del server EHome.

EHome Version

Impostare la versione di EHome in base alle proprie esigenze. Se si sceglie V5.0, è necessario creare un account e una chiave EHome. Se si sceglie un'altra versione, è necessario creare solo un account EHome.



Nota

Ricordare l'account EHome e la chiave EHome. È necessario immettere il nome dell'account o la chiave quando il dispositivo deve comunicare con altre piattaforme tramite il protocollo EHome.

7.5 Gestione delle persone

7.5.1 Aggiunta di persone

È possibile aggiungere utenti impostando il numero ID, il nome utente e il numero della tessera. È inoltre possibile registrare l'impronta digitale dell'utente, impostare la password, il reparto, il ruolo e la modalità di autenticazione.

Passaggi

1. Spostare il cursore e selezionare **User** → **New** per accedere alla pagina New.

New			
ID	1		
Name			
Card	Set	View Info.	0
FP	Set		0
PWD	Set	Not Configured	
Dept.	Set		
Auth.	<	Controller	>
Role	<	User	>
[ESC] Back [OK] Confirm			

Figura 7-4 Pagina New

2. Immettere i parametri del nuovo utente.

ID (ID dipendente)

Per impostazione predefinita, il numero ID aumenterà in sequenza. È possibile modificare l'ID in base alle proprie preferenze.



Nota

- L'ID si riferisce al numero di serie delle presenze dell'utente.
 - L'ID deve essere compreso tra 1 e 99999999 e non deve iniziare con 0.
 - L'ID deve essere univoco.
-

Name

Inserire il nuovo nome utente.



Nota

- Premere il tasto su o giù sulla tastiera per modificare il metodo di immissione.
 - Il nome utente può contenere un massimo di 32 caratteri.
-

Card

Set: passare la tessera nell'area di passaggio delle tessere o immettere manualmente il numero della tessera e selezionare una proprietà per la tessera.

View Info.: visualizzare le informazioni della tessera dell'utente aggiunta.



Nota

- Il numero della tessera è obbligatorio.
 - È possibile inserire fino a 20 cifre nel numero della tessera.
 - Il numero della tessera può essere 0.
 - Il numero della tessera può iniziare con 0 quando contiene più di un numero, ad es. 012345.
 - Il numero della tessera deve essere univoco.
 - Se il dispositivo non supporta il passaggio delle tessere, è necessario immettere manualmente il numero della tessera. Se è necessario immetterlo manualmente, attivare **Press Key to Input Card No.** Per i dettagli, consultare *Configurazione dei parametri per il dispositivo di controllo accessi.*
-

FP (impronta digitale)

Nella pagina Fingerprint, selezionare un dito e registrarlo in base alle istruzioni vocali.



Nota

- Uno stesso dito non può essere aggiunto più di una volta.
 - È possibile aggiungere fino a 10 impronte digitali per un utente.
 - È inoltre possibile eseguire la scansione delle impronte digitali tramite il registratore di impronte digitali esterno e applicarle al dispositivo tramite il software client.
 - Per informazioni dettagliate sulla scansione dell'impronta digitale, consultare la sezione *Suggerimenti per la scansione delle impronte digitali.*
-

PWD (password)

Creare una password per l'utente e confermarla.



Sono consentiti fino a 8 caratteri.

Dept. (reparto)

Selezionare un reparto dall'elenco e modificarlo.



Per informazioni dettagliate sulla modifica del reparto,

Auth

Selezionare una modalità di autenticazione durante la verifica dell'autorizzazione dell'utente.



- Se si seleziona la modalità di autenticazione **Controller**, è necessario impostare la modalità di autenticazione in **Set System Parameters**. Il sistema autenticherà l'identità dell'utente in base alla modalità di autenticazione configurata. Per impostazione predefinita, la modalità di autenticazione è **Controller**. Questa modalità può essere applicata per modificare le modalità di autenticazione degli utenti in batch.
 - Se un utente deve utilizzare una modalità di autenticazione speciale, diversa da quella configurata in **Set System Parameters**, può utilizzare la tessera/impronta digitale, la tessera, ecc. Il sistema autenticherà prima l'identità dell'utente in base alla modalità di autenticazione configurata. Questa modalità è applicabile alla modifica della modalità di autenticazione di un singolo utente, che dispone di autorizzazioni speciali.
-

Role

Selezionare il ruolo dell'utente come amministratore o utente normale.

- Admin: solo l'amministratore ha l'autorizzazione per utilizzare il dispositivo.
 - User: l'utente normale può verificare le presenze sulla pagina iniziale.
-



- Tutte le persone possono accedere alla pagina principale immettendo la password del dispositivo per utilizzarlo se non è configurato alcun utente amministratore.
 - Dopo aver configurato l'amministratore, è necessario autenticare l'amministratore per accedere alla pagina principale.
 - È possibile utilizzare l'interfaccia USB per importare le informazioni degli utenti. Per ulteriori informazioni, vedere *Trasferimento dei dati*.
-

3. Premere **ESC** e selezionare **Yes** per salvare le impostazioni e uscire dalla pagina.

7.5.2 Gestione delle persone (Ricerca/Modifica/Eliminazione)

Cercare, modificare ed eliminare gli utenti aggiunti. È inoltre possibile eliminare la password, gestire le impronte digitali aggiunte e gestire le tessere degli utenti.

Search User

Spostare il cursore e selezionare **User** → **User** per accedere all'elenco degli utenti.

Immettere il nome dell'utente o l'ID del dipendente nella casella di ricerca, quindi premere **OK** per avviare la ricerca.

Edit User

Spostare il cursore e selezionare **User** → **User** per accedere all'elenco degli utenti. Selezionare un utente dall'elenco e premere **OK**.

Selezionare **Edit User** e consultare la sezione *Aggiunta di persone* per modificare le informazioni dell'utente.

Premere **ESC** e selezionare **Yes** per salvare le impostazioni.

Delete

È possibile eliminare l'utente, eliminare la password, cancellare l'impronta digitale e cancellare la tessera.

Delete User

Consente di eliminare l'utente selezionato.

Delete PWD

Consente di eliminare la password dell'utente selezionato.

Clear FP

Consente di cancellare tutte le impronte digitali aggiunte per l'utente selezionato.

Clear Card

Consente di eliminare tutte le tessere aggiunte per l'utente selezionato.

7.6 Stato di presenza

Impostare la modalità di presenza e scegliere lo stato di presenza.

È possibile impostare lo stato di presenza come check-in, check-out, inizio pausa, fine pausa, inizio straordinario e fine straordinario in base alla situazione effettiva.

7.6.1 Impostazione della presenza automatica

Impostare la modalità di presenza come automatica per impostare lo stato della presenza e la relativa programmazione disponibile. Il sistema modificherà automaticamente lo stato della presenza in base ai parametri configurati.

Prima di iniziare

Aggiungere almeno una persona e impostarne la modalità di autenticazione. Per ulteriori informazioni, consultare *Gestione delle persone*.

Passaggi

1. Spostare il cursore e selezionare **System** → **Att. Status** per accedere alla pagina Attendance Status.
2. Spostare il cursore, selezionare **Attendance Mode** e impostare la modalità di presenza come **Auto**.

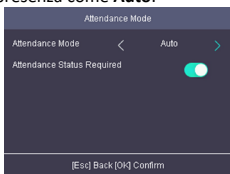


Figura 7-5 Modalità automatica



Nota

Verificare che lo stato di presenza sia abilitato. Per impostazione predefinita è abilitato.

3. Premere **ESC** e salvare la modalità di presenza.
4. Spostare il cursore, selezionare **Shortcut Key** e definire la pianificazione e lo stato di presenza del tasto di scelta rapida.



Nota

Lo stato di presenza sarà valido nell'ambito della pianificazione configurata. Ad esempio, se si imposta il tasto Su come check-in e il tasto Giù come check-out e la pianificazione del check-in come lunedì alle 08:00 e quella del check-out come lunedì alle 17:00, l'autenticazione della persona valida prima delle 17:00 di lunedì verrà contrassegnata come check-in e quella dopo le 17:00 di lunedì sarà contrassegnata come check-out.

5. Premere **ESC** e salvare le impostazioni.

Risultato

Accedere alla pagina iniziale; la modalità di presenza corrente viene visualizzata sulla pagina. Quando si esegue l'autenticazione sulla pagina iniziale, l'autenticazione verrà contrassegnata come lo stato di presenza configurato in base alla pianificazione configurata.

7.6.2 Impostazione della presenza manuale

Impostare la modalità di presenza come manuale e selezionare manualmente uno stato quando si registra la presenza.

Prima di iniziare

Aggiungere almeno una persona e impostarne la modalità di autenticazione. Per ulteriori informazioni, consultare **Gestione delle persone**.

Passaggi

1. Spostare il cursore e selezionare **System** → **Att. Status** per accedere alla pagina Attendance Status.
2. Spostare il cursore, selezionare **Attendance Mode** e impostare la modalità di presenza su **Manual**.

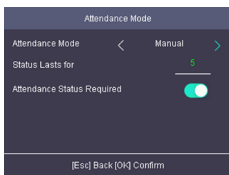


Figura 7-6 Modalità manuale



Nota

Verificare che lo stato di presenza sia abilitato. Per impostazione predefinita è abilitato.

3. Premere **ESC** e salvare la modalità di presenza.
4. Spostare il cursore, selezionare **Shortcut Key** e definire lo stato di presenza del tasto di scelta rapida.
5. Premere **ESC** e salvare le impostazioni.

Risultato

Premere un tasto sulla tastiera per selezionare uno stato di presenza e autenticarsi. L'autenticazione verrà contrassegnata come lo stato di presenza configurato in base al tasto di scelta rapida definito.

Oppure, quando si esegue l'autenticazione sulla pagina iniziale, si accede alla pagina Select Status. Selezionare uno stato per registrare la presenza.



Nota

Se non si seleziona uno stato entro circa 20 secondi, l'autenticazione non verrà eseguita correttamente e non verrà contrassegnata come presenza valida.

7.6.3 Impostazione della presenza manuale e automatica

Impostare la modalità di presenza come manuale e automatica e il sistema modificherà automaticamente lo stato della presenza in base ai parametri configurati. Allo stesso tempo, è possibile modificare manualmente lo stato della presenza prima dell'autenticazione.

Prima di iniziare

Aggiungere almeno una persona e impostarne la modalità di autenticazione. Per ulteriori informazioni, consultare **Gestione delle persone**.

Passaggi

1. Spostare il cursore e selezionare **System → Att. Status** per accedere alla pagina Attendance Status.
2. Spostare il cursore e selezionare **Attendance Mode** e impostare la modalità di presenza su **Manual and Auto**.

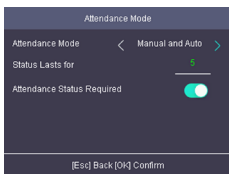


Figura 7-7 Modalità manuale e automatica



Nota

Verificare che lo stato di presenza sia abilitato. Per impostazione predefinita è abilitato.

3. Premere **ESC** e salvare la modalità di presenza.
4. Spostare il cursore, selezionare **Shortcut Key** e definire la pianificazione e lo stato di presenza del tasto di scelta rapida.



Nota

Lo stato di presenza sarà valido nell'ambito della pianificazione configurata. Ad esempio, se si imposta il tasto Su come check-in e il tasto Giù come check-out e la pianificazione del check-in come lunedì alle 08:00 e quella del check-out come lunedì alle 17:00, l'autenticazione della persona valida prima delle 17:00 di lunedì verrà contrassegnata come check-in e quella dopo le 17:00 di lunedì sarà contrassegnata come check-out.

5. Premere **ESC** e salvare le impostazioni.

Risultato

Accedere alla pagina iniziale; la modalità di presenza corrente viene visualizzata sulla pagina. Se non si seleziona uno stato, l'autenticazione verrà contrassegnata come lo stato di presenza configurato in base alla pianificazione. Se si preme il tasto sulla tastiera e si seleziona uno stato per registrare la presenza, l'autenticazione verrà contrassegnata come lo stato di presenza selezionato.

7.6.4 Disattivazione della modalità di presenza

Disattivare la modalità di presenza e il sistema non mostrerà lo stato di presenza nella pagina iniziale.

Spostare il cursore e selezionare **System** → **Att. Status** per accedere alla pagina Attendance Status.

Spostare il cursore e selezionare **Attendance Mode** e impostare la modalità di presenza su **Disable**.

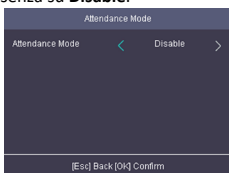


Figura 7-8 Disattivazione della modalità di presenza

La funzione dello stato di presenza è disabilitata e non sarà possibile visualizzare o configurare lo stato di presenza nella pagina iniziale.

7.7 Gestione di orari e presenze

Gestire reparti, turni, ferie, pianificazioni e report.

È possibile aggiungere, modificare, eliminare reparti/turni/ferie/pianificazioni. È inoltre possibile esportare il report delle presenze.

Spostare cursore e selezionare Attendance per accedere alla pagina Attendance.

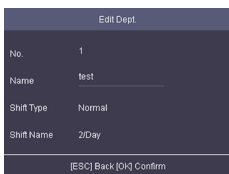
7.7.1 Gestione dei reparti (Modifica/Ricerca/Ripristino)

È possibile modificare il nome del reparto, visualizzare il tipo e il nome del turno. È inoltre possibile eseguire la ricerca del reparto in base al nome del reparto o ripristinare i parametri del reparto.

Modifica dei reparti

Spostare il cursore su **Dept.** e premere **OK** per accedere all'elenco dei reparti.

Selezionare un reparto dall'elenco e selezionare **Edit**, quindi premere **OK** per accedere alla pagina Edit Dept. È possibile modificare il nome del reparto, visualizzare il tipo e il nome del turno.



Edit Dept.	
No.	1
Name	test
Shift Type	Normal
Shift Name	2/Day
[ESC] Back [OK] Confirm	

Figura 7-9 Pagina Edit Department



Nota

- Il nome del reparto supporta numeri, lettere maiuscole, lettere minuscole e simboli.
- Nel nome del reparto sono supportati fino a 32 caratteri.
- È possibile configurare il turno in Shift Management. Per informazioni dettagliate, vedere **Gestione dei turni**.
- Per impostazione predefinita, il sistema contiene 32 reparti.
- Premere il tasto su o giù sulla tastiera per modificare il metodo di immissione.

Ricerca di reparti

Cercare il reparto di destinazione inserendone il nome.

Spostare il cursore su **Dept.** e premere **OK** per accedere all'elenco dei reparti.

Immettere il nome del reparto nella casella di ricerca, quindi premere **OK** per avviare la ricerca.

Ripristino dei reparti

Ripristinare tutti i parametri del reparto di destinazione ai valori predefiniti.

Spostare il cursore su **Dept.** e premere **OK** per accedere all'elenco dei reparti.

Selezionare un reparto dall'elenco e selezionare **Reset**, quindi premere **OK**. Tutti i parametri verranno ripristinati ai valori predefiniti.

7.7.2 Gestione dei turni

È possibile configurare il turno normale e il turno ore-uomo. È possibile impostare la regola di presenza e gli orari di entrata e uscita nel turno normale. È inoltre possibile impostare le ore di lavoro al giorno in un turno ore-uomo.

Normal Shift: è applicabile alla normale situazione di presenza.

Man-Hour Shift: è applicabile a una situazione con orari di lavoro flessibili.

Impostazione della regola di presenza per un turno normale

Spostare il cursore e selezionare **Shift → Normal → Rule**, quindi premere **OK** per accedere alla pagina Rule.

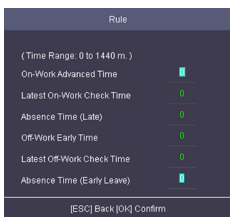


Figura 7-10 Pagina Attendance Rule

Impostare la regola di presenza.

On-work Advanced Time

Il primo orario consentito di arrivo al lavoro.

Latest On-Work Check Time

L'ultimo orario consentito di arrivo al lavoro.

Absence Time (Late)

La durata di tempo limite per arrivare in ritardo.

Off-Work Early Time

Il primo orario consentito per andare via dal lavoro.

Latest Off-Work Check Time

L'ultimo orario consentito per andare via dal lavoro.

Absence Time (Early Leave)

La durata di tempo limite per uscire in anticipo.



Nota

La durata disponibile va da 0 a 1440 minuti.

Impostazione di turni normali

Impostare le informazioni sulla presenza nei turni normali, come il nome del turno e la durata. È possibile anche ripristinare il turno normale dopo la modifica.

Prima di iniziare

Impostare la regola di presenza. Per i dettagli, vedere la sezione *Impostazione della regola di presenza per un turno normale*.

Passaggi

1. Spostare il cursore e selezionare **Shift → Normal** per accedere alla pagina Normal.

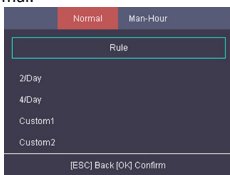


Figura 7-11 Pagina Normal Shift

2. Selezionare un turno e premere **OK**.



Nota

Per impostazione predefinita, il tipo di turno normale comprende le opzioni 2/Day (2 volte al giorno), 4/Day (4 volte al giorno) e 30 tipi personalizzati.

3. Selezionare **Edit** e premere **OK** per accedere alla pagina Edit Shift.
4. Impostare il nome e il periodo del turno.



Nota

- Il nome del turno supporta numeri, lettere maiuscole, lettere minuscole, caratteri cinesi e simboli.
 - Il nome del turno può contenere un massimo di 32 caratteri.
 - È possibile modificare fino a 4 periodi di tempo.
-

5. Premere **ESC** e selezionare **Yes** per salvare le impostazioni.
6. **Opzionale:** selezionare un turno normale e poi **Reset** per ripristinare il valore predefinito del turno.

Impostazione di turni ore-uomo

Impostare i parametri per i turni ore-uomo, come il nome del turno, la durata del lavoro, l'ultima volta "on-work" e il tempo di pausa.

Passaggi

È possibile configurare fino a 32 turni ore-uomo.

1. Spostare il cursore e selezionare **Shift → Man-Hour** per accedere alla pagina Man-Hour.

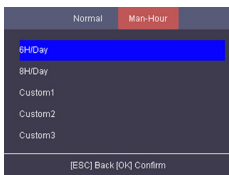


Figura 7-12 Pagina Man-Hour

2. Selezionare un turno dall'elenco e premere **OK**.
3. Selezionare **Edit** per accedere alla pagina Edit Shift.



Nota

Per impostazione predefinita, il tipo di turno ore-uomo comprende le opzioni 6H/Day (6 ore al giorno), 8H/Day (8 ore al giorno) e 30 tipi personalizzati.

4. Modificare il nome e la durata del turno (durata di lavoro), l'ultima volta "on-work" e il tempo di pausa.



Nota

- Il tempo di pausa non verrà conteggiato nelle ore di lavoro.
- Se l'opzione Latest Time (On-Work) è impostata su 0, la funzione Latest Time non sarà abilitata.

5. Premere **ESC** e selezionare **Yes** per salvare le impostazioni.
6. **Opzionale:** selezionare un turno, premere **OK** e selezionare **Reset** per ripristinare il valore predefinito del turno.

7.7.3 Gestione delle ferie (Aggiunta/Ricerca/Modifica/Eliminazione)

Impostare la pianificazione per le ferie. La presenza non verrà registrata durante le ferie. **Aggiunta di ferie**

Spostare il cursore e selezionare **Holiday** → **New** per accedere alla pagina New. Immettere il numero, il nome, la data di inizio e di fine. Premere **OK** per salvare le impostazioni.

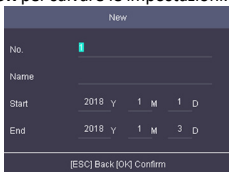


Figura 7-14 Pagina Add Holiday

Ricerca delle ferie

Spostare il cursore e selezionare **Holiday** → **Holiday** per accedere all'elenco delle ferie. Inserire un nome per le ferie e premere **OK** per avviare la ricerca.

Modifica delle ferie

Spostare il cursore e selezionare **Holiday** → **Holiday** per accedere all'elenco delle ferie. Selezionare delle ferie e selezionare **Edit** per modificare le ferie.

Eliminazione delle ferie

Spostare il cursore e selezionare **Holiday** → **Holiday** per accedere all'elenco delle ferie. Selezionare delle ferie e selezionare **Delete** per eliminare le ferie.

7.7.4 Pianificazione dei turni

Combinare i turni e le ferie in base alle proprie esigenze. È possibile pianificare i turni per un reparto e per ogni singola persona.

Pianificazione dei turni per reparto: tutte le persone del reparto utilizzano lo stesso programma di turni per il check-in/check-out.

Schedule Shift by Individual: check in/check-out in base alle condizioni della singola persona.

Pianificazione dei turni per reparto

Tutte le persone del reparto utilizzano lo stesso programma di turni per il check-in/check-out.

Prima di iniziare

- Modificare il reparto. Per i dettagli, consultare la sezione **Gestione dei reparti (Modifica/Ricerca/Ripristino)**.
- Impostare un turno normale o un turno ore-uomo. Per i dettagli, consultare le sezioni **Impostazione di turni normali** e **Impostazione di turni ore-uomo**.

Passaggi

1. Spostare il cursore e selezionare **Schedule** → **Dept. Shift** per accedere alla pagina Dept. Shift.
2. Selezionare un reparto dall'elenco e premere **OK** per accedere alla pagina Edit Shift Schedule by Dept.

Dept. Name	Company
Set Shift	Set Shift
Start	1970 Y 1 M 1 D
End	2037 Y 12 M 31 D
Add Holiday	Select Holiday

[ESC] Back [OK] Confirm

Figura 7-15 Pagina Edit Shift Schedule by Dept.

3. Modificare i parametri.

Dept. Name

Il nome del reparto deve essere modificato nella pagina Edit Dept. Per i dettagli, consultare la sezione *Gestione dei reparti (Modifica/Ricerca/Ripristino)*.

Set Shift

Selezionare un tipo di turno e le durate del turno stesso.

Start

Impostare la data di inizio della pianificazione.

End

Impostare la data di fine della pianificazione.

Add Holiday

Selezionare delle ferie dal relativo elenco. Per ulteriori informazioni sull'aggiunta di ferie, consultare la sezione

Gestione delle ferie

(Aggiunta/Ricerca/Modifica/Eliminazione).

4. Premere **ESC** e selezionare **Yes** per salvare le impostazioni.

Pianificazione dei turni per persona

Check in/check-out in base alle condizioni della singola persona.

Prima di iniziare

- Aggiungere l'utente prima di impostare la pianificazione dei turni per singola persona. Per ulteriori informazioni, consultare la sezione ***Aggiunta di persone***.
- Impostare il turno normale o il turno ore-uomo. Per i dettagli, consultare le sezioni ***Impostazione di turni normali*** e ***Impostazione di turni ore-uomo***.

Passaggi



Nota

La pianificazione dei turni per singola persona ha una priorità maggiore rispetto a quella per reparto. Se un utente ha configurato sia la pianificazione dei turni per reparto che per singola persona, il sistema registrerà le presenze prima di tutto in base alla pianificazione dei turni per singola persona.

1. Spostare il cursore e selezionare **Schedule** → **Individual Shift** per accedere alla pagina Individual Shift.
2. Selezionare **Add Individual Shift** e premere **OK** per accedere alla pagina Add Shift Schedule.

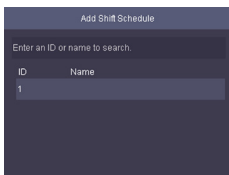


Figura 7-16 Pagina Add Shift Schedule

3. Selezionare una persona dall'elenco e premere **OK** per accedere alla pagina Edit Shift Schedule by Department.
4. Modificare i parametri.

Set Shift

Selezionare un tipo di turno e le durate del turno stesso.

Start

Impostare la data di inizio della pianificazione.

End

Impostare la data di fine della pianificazione.

Add Holiday

Selezionare delle ferie dal relativo elenco. Per ulteriori informazioni sull'aggiunta di ferie, consultare la sezione **Gestione delle ferie (Aggiunta/Ricerca/Modifica/Eliminazione)**.

5. Premere **ESC** e selezionare **Yes** per salvare le impostazioni.

7.7.5 Esportazione del report delle presenze

Esportare il record delle presenze, il report delle presenze, il record delle presenze anomale e il programma di gestione delle presenze.

Passaggi

1. Inserire un'unità flash USB nell'interfaccia USB.



Nota

- Il formato dell'unità flash USB supportato è FAT32.
 - La memoria dell'unità flash USB dev'essere compresa tra 1 e 32 GB. Assicurarsi che lo spazio libero dell'unità flash USB sia superiore a 512 MB.
-

2. Spostare il cursore e selezionare **Report**. Premere **OK** per accedere alla pagina Report.



Figura 7-17 Pagina Report

3. Selezionare un report da esportare.

- Quando si esportano i record delle presenze, i report delle presenze e i record delle presenze anomale, è necessario inserire le date di inizio e di fine del periodo delle presenze relative al numero di dispositivo.



Nota

Il numero di dispositivo serve a differenziare i report dei vari dispositivi.

- Quando si seleziona **Attendance Management Schedule**, la tabella delle impostazioni dei turni, quella della pianificazione dei turni normali e quella della pianificazione dei turni ore-uomo verranno esportate.
-



Nota

Per ulteriori informazioni sulle descrizioni delle tabelle esportate, vedere la sezione **Tabella dei report delle presenze**.

La tabella esportata verrà salvata in un'unità flash USB in formato Excel.

7.7.6 Trasferimento dei dati

È possibile esportare i parametri di controllo degli accessi (impronte digitali e informazioni sull'utente) e i dati sulle presenze (ad esempio, i dati relativi alle presenze e al passaggio delle tessere). È inoltre possibile importare i parametri di controllo degli accessi da un'unità flash USB.

Esportazione dei dati

Spostare il cursore e selezionare **Transfer** → **Export** per accedere alla pagina Export.



Figura 7-18 Pagina Export Data

Collegare un'unità flash USB nell'interfaccia USB del dispositivo e selezionare **Export ACS Para.** o **Export Attendance Data.** Premere **OK** e i dati verranno esportati nell'unità flash USB.



Nota

- Il formato dell'unità flash USB supportato è FAT32.
- La memoria dell'unità flash USB dev'essere compresa tra 1 e 32 GB. Assicurarsi che lo spazio libero dell'unità flash USB sia superiore a 512 MB.

Importazione dei dati

Spostare il cursore e selezionare **Transfer** → **Import** per accedere alla pagina Import. Selezionare **Import ACS Para** e premere **OK**. Il sistema ricaverà i parametri di controllo degli accessi dall'unità flash USB.



Nota

- Il formato dell'unità flash USB supportato è FAT32.
- Il file per l'importazione deve trovarsi nella directory radice.

7.8 Impostazioni di sistema

7.8.1 Impostazione dell'ora

Impostare l'ora del dispositivo e l'ora legale.

Passaggi

1. Spostare il cursore e selezionare **Time** nella pagina principale e premere **OK** per accedere alla pagina Time.

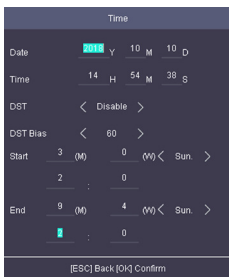


Figura 7-19 Pagina Time

2. Modificare i parametri.

Date

La data visualizzata sul dispositivo.



Nota

L'intervallo disponibile è compreso tra 01.01.1970 e 31.12.2037.

Time

L'ora visualizzata sul dispositivo.

DST

Selezionare l'opzione per attivare o disattivare l'ora legale. Quando la funzione DST è abilitata, è possibile impostare l'ora di inizio e l'ora di fine preferite per l'ora legale.

- DST Bias: è possibile selezionare 30 minuti, 60 minuti, 90 minuti e 120 minuti.
- Start: impostare l'ora di inizio dell'ora legale.
- End: impostare l'ora di fine dell'ora legale.

3. Premere ESC e selezionare Yes per salvare le impostazioni e uscire dalla pagina.

7.8.2 Gestione dei dati di sistema

Eliminare l'evento salvato, i dati delle presenze e dell'utente o l'autorizzazione.

Passaggi

1. Spostare il cursore e selezionare **System → Data**.
2. Premere **OK** per accedere alla pagina Data.

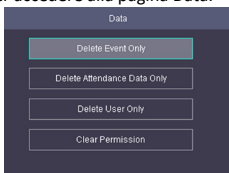


Figura 7-20 Pagina Data

3. Selezionare una voce e premere OK per eliminarla.

Delete Event Only

Consente di eliminare tutti gli eventi registrati nel dispositivo.

Delete Attendance Data Only

Consente di eliminare tutti i dati sulle presenze nel dispositivo.

Delete User Only

Consente di eliminare tutti i dati dell'utente nel dispositivo, inclusi i record di presenze.

Clear Permission

Consente di eliminare l'autorizzazione per la gestione degli amministratori. L'amministratore diventerà un utente normale. L'utente non verrà eliminato.

7.8.3 Impostazione dei parametri di sistema

Impostare i parametri di sistema, come il formato dell'ora del dispositivo, i suoni della tastiera, le istruzioni vocali, il volume, la modalità di sospensione, i comandi per i record delle presenze, la modalità di autenticazione, la funzione di eliminazione dei record e la lingua.

Passaggi

1. Spostare il cursore e selezionare **System** → **System**.
2. Premere **OK** per accedere alla pagina System.

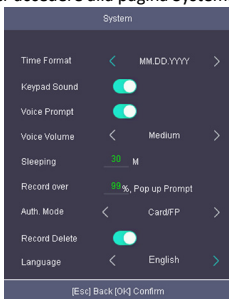


Figura 7-21 Pagina System

3. Modificare i parametri.

Time Format

Selezionare un formato appropriato per l'ora in base alle proprie preferenze.

Keypad Sound

Attivare o disattivare i suoni della tastiera in base alle proprie preferenze.

Voice Prompt

Attivare o disattivare le istruzioni vocali in base alle proprie preferenze.

Voice Volume

Impostare il volume delle istruzioni vocali del dispositivo.

Sleeping

Impostare il tempo di attesa per la sospensione del dispositivo (minuti). Dalla pagina iniziale, se si imposta il tempo di sospensione su 30 minuti, il dispositivo andrà in sospensione dopo 30 minuti senza alcuna operazione.



Nota

Se si imposta il tempo di sospensione su 0, il dispositivo non entrerà in modalità di sospensione.

Notifica dei record oltre la soglia

Se la memoria dei record delle presenze raggiunge il valore configurato, il sistema apre una finestra di notifica. Il valore disponibile va da 1 a 99.



Nota

È possibile salvare fino a 50.000 record di presenze.

Auth Mode (modalità di autenticazione)

La modalità di autenticazione può essere impostata su "Card/FP (impronta digitale)", "Card", "FP (impronta digitale)", "Card & Password", "Card & FP (impronta digitale)", "FP (impronta digitale) & Password", "Card & FP (impronta digitale)", "Password" e "ID (ID dipendente) and password".

Record Delete

Quando la funzione è attivata, il sistema ricorderà all'utente di eliminare i record. Quando la memoria raggiungere la soglia configurata, il sistema eliminerà i primi 3.000 record delle presenze, affinché sia possibile salvare i nuovi record. La funzione è abilitata per impostazione predefinita. Per ulteriori informazioni, consultare **Regola di eliminazione dei record delle presenze**.

Language

Consente di modificare la lingua del sistema. Dopo aver modificato la lingua del sistema, il dispositivo sarà riavviato automaticamente.

4. Premere **ESC** e selezionare **Yes** per salvare le impostazioni e uscire dalla pagina.

7.8.4 Aggiornamento del sistema

Il sistema legge il file di aggiornamento nell'unità flash USB collegata, per aggiornare il dispositivo.

Passaggi

1. Inserire l'unità flash USB nell'interfaccia USB.
-



Nota

- Il file di aggiornamento deve trovarsi nella directory radice.
 - Il nome del file di aggiornamento nell'unità flash USB deve essere digicap.dav.
-

2. Spostare il cursore e selezionare **System → Upgrade**.
3. Premere **OK**.



Nota

Non spegnere il dispositivo durante l'aggiornamento.

Il sistema leggerà il file digicap.dav e si aggiornerà automaticamente. Al termine dell'aggiornamento, il dispositivo si riavvierà automaticamente.



Nota

Al termine dell'aggiornamento, rimuovere l'unità flash USB.

7.8.5 Ripristino delle impostazioni

Ripristinare i parametri di sistema alle impostazioni di fabbrica o a quelle predefinite.

Passaggi

1. Spostare il cursore e selezionare **System** → **Reset**.
2. Premere **OK** per accedere alla pagina Reset.



Figura 7-22 Pagina Reset

3. Selezionare **Factory Settings** o **Default Settings**.

Factory Settings

Tutti i parametri del dispositivo ritorneranno alle impostazioni di fabbrica.

Default Settings

Tutti i parametri, esclusi i parametri di comunicazione, la gestione remota degli utenti e gli eventi, verranno ripristinati alle impostazioni di fabbrica.

4. Confermare le impostazioni nella pagina della richiesta e il dispositivo avvierà il ripristino.

7.8.6 Visualizzazione delle informazioni di sistema

Visualizzare le informazioni del sistema, tra cui la capacità del sistema e le informazioni sul dispositivo.

Visualizzazione della capacità del sistema

Spostare il cursore e selezionare **Info.** → **Capacity** per accedere alla pagina Capacity.

È possibile visualizzare il numero utente del dispositivo aggiunto e il numero dell'impronta digitale.

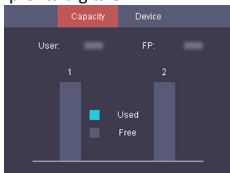


Figura 7-23 Pagina Capacity

Visualizzazione delle informazioni del dispositivo

Spostare il cursore e selezionare **Info**. → **Device** per accedere alla pagina Device.

È possibile visualizzare il nome del dispositivo, il numero di serie, l'indirizzo MAC, il firmware, la versione dell'algoritmo e la data di produzione.

Capacity	Device
Device Name:	10000000000000000000
Serial No.:	10000000000000000000
MAC Address:	10000000000000000000
Firmware:	10000000000000000000
Algorithm:	10000000000000000000
Production Date:	10000000000000000000

Figura 7-24 Pagina Device

8 Configurazione del software client

È possibile utilizzare il dispositivo e gestire i dati tramite il software client.



Nota

L'introduzione del software client in questo documento dipende dalla versione 3.1.

8.1 Aggiunta di un dispositivo

Dopo aver eseguito il client, i dispositivi, come quelli di controllo accessi, i pannelli di controllo di sicurezza, ecc., devono essere aggiunti al client per la configurazione e la gestione da remoto, ad esempio il controllo dello stato delle porte, la gestione delle presenze, le impostazioni degli eventi, ecc.

8.1.1 Aggiunta di dispositivi online

I dispositivi online attivi sulla stessa subnet locale del software client saranno visualizzati nell'area **Online Device**.




Nota

- È possibile fare clic su **Refresh per 60s**, per aggiornare le informazioni dei dispositivi online.
- La funzione di registro SADP può essere attivata o disattivata facendo clic con il pulsante destro del mouse su **Online Device**.

Aggiunta di un singolo dispositivo online

È possibile aggiungere un singolo dispositivo online al software client.

Passaggi

1. Accedere al modulo Device Management.
2. **Opzionale:** fare clic su  sulla destra di **Device Management** e selezionare **Device**.

3. Fare clic su **Online Device** per visualizzare l'area del dispositivo online.

I dispositivi online cercati vengono visualizzati nell'elenco.

4. Selezionare un dispositivo online dall'area **Online Device**.
-



Nota

Per il dispositivo inattivo, è necessario crearne la password prima di poterlo aggiungere correttamente. Per i passaggi dettagliati, consultare la sezione **Attivazione**.

5. Fare clic su **Add** per aprire la finestra di aggiunta dei dispositivi.

6. Immettere le informazioni richieste.

Name

Immettere un nome che descriva il dispositivo.

Address

L'indirizzo IP del dispositivo si ottiene automaticamente in questa modalità di aggiunta.

Port

Il numero di porta viene ottenuto automaticamente.

User Name

Per impostazione predefinita, il nome utente è admin.

Password

Inserire la password del dispositivo.



Attenzione

Il sistema è in grado di valutare automaticamente la complessità della password del dispositivo. Si consiglia vivamente di modificare la password scelta (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto. Rientra nella responsabilità dell'installatore e/o dell'utente finale configurare correttamente tutte le password e altri parametri di sicurezza.

7. **Opzionale:** selezionare **Synchronize Time** per sincronizzare l'ora del dispositivo con il PC su cui è in esecuzione il client dopo aver aggiunto il dispositivo al client.

8. **Opzionale:** selezionare **Import to Group** per creare un gruppo in base al nome del dispositivo.
-



Nota


Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.

9. Fare clic su **OK** per aggiungere

Aggiunta di più dispositivi online

È possibile aggiungere più dispositivi online al software client.

Passaggi

1. Accedere al modulo Device Management.
2. fare clic su  sulla destra di **Device Management** e selezionare **Device**.
3. Fare clic su **Online Device** per visualizzare l'area del dispositivo online.
I dispositivi online cercati vengono visualizzati nell'elenco.
4. Selezionare più dispositivi.



Nota

Per il dispositivo inattivo, è necessario crearne la password prima di poterlo aggiungere correttamente. Per i passaggi dettagliati, consultare la sezione **Attivazione**.

5. Fare clic su **Add** per aprire la finestra di aggiunta dei dispositivi.
6. Immettere le informazioni richieste.

User Name

Per impostazione predefinita, il nome utente è admin.

Password

Inserire la password del dispositivo.



Attenzione

Il sistema è in grado di valutare automaticamente la complessità della password del dispositivo. Si consiglia vivamente di modificare la password scelta (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto. Rientra nella responsabilità dell'installatore e/o dell'utente finale configurare correttamente tutte le password e altri parametri di sicurezza.

7. **Opzionale:** selezionare **Synchronize Time** per sincronizzare l'ora del dispositivo con il PC su cui è in esecuzione il client dopo aver aggiunto il dispositivo al client.
 8. **Opzionale:** selezionare **Import to Group** per creare un gruppo in base al nome del dispositivo.
-



Nota


Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.

9. Fare clic su **OK** per aggiungere i dispositivi.

8.1.2 Aggiunta di un dispositivo tramite l'indirizzo IP o il nome dominio

Quando si conosce l'indirizzo IP o il nome di dominio del dispositivo da aggiungere, è possibile aggiungere dispositivi al client specificando l'indirizzo IP (o il nome di dominio), il nome utente, la password e altri parametri correlati.

Passaggi

1. Accedere al modulo Device Management.
2. **Opzionale:** fare clic su  sulla destra di **Device Management** e selezionare **Device**.
I dispositivi aggiunti vengono visualizzati nell'elenco.
3. Fare clic su **Add** per aprire la finestra Add.
4. Selezionare **IP/Domain** come modalità di aggiunta.
5. Immettere le informazioni richieste, come il nome, l'indirizzo, il numero di porta, il nome utente e la password.

Name

Creare un nome che descriva il dispositivo. Ad esempio, è possibile utilizzare un nome che indichi la posizione o le caratteristiche del dispositivo.

Address

L'indirizzo IP o il nome di dominio del dispositivo.

Port

I dispositivi da aggiungere hanno lo stesso numero di porta. Il valore predefinito è 8000.

User Name

Inserire il nome utente del dispositivo. Per impostazione predefinita, il nome utente è admin.

Password

Inserire la password del dispositivo.



Attenzione

Il sistema è in grado di valutare automaticamente la complessità della password del dispositivo. Si consiglia vivamente di modificare la password scelta (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto. Rientra nella responsabilità dell'installatore e/o dell'utente finale configurare correttamente tutte le password e altri parametri di sicurezza.

6. **Opzionale:** selezionare **Synchronize Time** per sincronizzare l'ora del dispositivo con il PC su cui è in esecuzione il client dopo aver aggiunto il dispositivo al client.
7. **Opzionale:** selezionare **Import to Group** per creare un gruppo in base al nome del dispositivo.




Nota

Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.

8. Completare l'aggiunta del dispositivo.


- Fare clic su **Add** per aggiungere il dispositivo e tornare alla pagina dell'elenco dei dispositivi.
- Fare clic su **Add and New** per salvare le impostazioni e continuare ad aggiungere un altro dispositivo.

9. Eseguire le seguenti operazioni dopo aver aggiunto i dispositivi.


Remote Configuration Fare clic su  nella colonna Operation per impostare la configurazione remota del dispositivo corrispondente.



Nota

- Per alcuni modelli di dispositivi, è possibile aprire la relativa finestra Web. Per aprire la finestra di configurazione remota originale, premere **Ctrl** e fare clic su .
- Per i passaggi sulle operazioni dettagliate per la configurazione remota, consultare il manuale dell'utente del dispositivo.


Device Status

Fare clic su  nella colonna Operation per visualizzare lo stato del dispositivo.

8.1.3 Aggiunta di dispositivi tramite segmento IP

Se si desidera aggiungere dispositivi i cui indirizzi IP si trovano all'interno di uno stesso segmento IP, per aggiungerli è possibile specificare l'indirizzo IP iniziale e quello finale, il nome utente, la password e altri parametri.

Passaggi

1. Accedere al modulo Device Management.
2. **Opzionale:** fare clic su  sulla destra di **Device Management** e selezionare **Device**.
I dispositivi aggiunti vengono visualizzati nell'elenco.
3. Fare clic su **Add** per aprire la finestra Add.
4. Selezionare **IP Segment** come modalità di aggiunta.
5. Immettere le informazioni richieste.

Start IP

Inserire un indirizzo IP iniziale.

End IP

Inserire un indirizzo IP finale nello stesso segmento di rete dell'IP iniziale.

Port

Inserire il numero di porta del dispositivo. Il valore predefinito è 8000.

User Name

Per impostazione predefinita, il nome utente è admin.

Password

Inserire la password del dispositivo.



Attenzione

Il sistema è in grado di valutare automaticamente la complessità della password del dispositivo. Si consiglia vivamente di modificare la password scelta (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto. Rientra nella responsabilità dell'installatore e/o dell'utente finale configurare correttamente tutte le password e altri parametri di sicurezza.

6. Opzionale: selezionare **Synchronize Time** per sincronizzare l'ora del dispositivo con il PC su cui è in esecuzione il client dopo aver aggiunto il dispositivo al client.

7. Opzionale: selezionare **Import to Group** per creare un gruppo in base al nome del dispositivo.




Nota

Per impostazione predefinita è possibile importare tutti i canali del dispositivo nel gruppo corrispondente.

8. Completare l'aggiunta del dispositivo.

- Fare clic su **Add** per aggiungere il dispositivo e tornare alla pagina dell'elenco dei dispositivi.
- Fare clic su **Add and New** per salvare le impostazioni e continuare ad aggiungere un altro dispositivo.

9. Opzionale: fare clic su  nella colonna Operation per visualizzare lo stato del dispositivo.

8.1.4 Aggiunta di dispositivi tramite account

EHome

Per le aree in cui i dispositivi utilizzano indirizzi IP dinamici anziché statici, è possibile aggiungere il dispositivo di controllo accessi connesso tramite il protocollo EHome specificando l'account EHome.

Prima di iniziare

Dapprima impostare i parametri del centro di rete. Per ulteriori dettagli, consultare la sezione **Impostazione dei parametri di rete**.


Passaggi



Nota

I dispositivi aggiunti tramite EHome non supportano il caricamento di eventi con immagini acquisite sul client.

1. Accedere al modulo Device Management.

2. Opzionale: fare clic su  sulla destra di **Device Management** e selezionare **Device**.

I dispositivi aggiunti vengono visualizzati nell'elenco.

3. Fare clic su **Add** per aprire la finestra Add.

4. Selezionare **EHome** come modalità di aggiunta.

5. Immettere le informazioni richieste.

Device Account

Inserire il nome dell'account registrato sul protocollo EHome.

EHome Key

Immettere la chiave EHome se è stata impostata durante la configurazione dei parametri del centro di rete per il dispositivo.



Nota


Questa funzione deve essere supportata dal dispositivo.

6. Opzionale: selezionare **Synchronize Time** per sincronizzare l'ora del dispositivo con il PC su cui è in esecuzione il client dopo aver aggiunto il dispositivo al client.

7. Opzionale: selezionare **Import to Group** per creare un gruppo in base al nome del dispositivo.

8. Completare l'aggiunta del dispositivo.

- Fare clic su **Add** per aggiungere il dispositivo e tornare alla pagina dell'elenco dei dispositivi.
- Fare clic su **Add and New** per salvare le impostazioni e continuare ad aggiungere un altro dispositivo.

9. Opzionale: fare clic su  nella colonna Operation per visualizzare lo stato del dispositivo.

8.1.5 Importazione di dispositivi in batch

I dispositivi possono essere aggiunti in batch al software, inserendo le informazioni dei dispositivi nel file CSV predefinito.

Passaggi

1. Accedere alla pagina Device Management.

2. Fare clic su **Add** per aprire la finestra di aggiunta dei dispositivi.

3. Selezionare **Batch Import** come modalità di aggiunta.

4. Fare clic su **Export Template** e salvare il modello predefinito (file CSV) sul PC.

5. Aprire il file del modello esportato e inserire le informazioni necessarie sui dispositivi da aggiungere nella colonna corrispondente.

Modalità di aggiunta

È possibile inserire i valori **0** o **1** che indicano le diverse modalità di aggiunta. **0** indica che il dispositivo è aggiunto tramite indirizzo IP o nome dominio; **1** indica che il dispositivo è aggiunto tramite EHome.

Address

Modificare l'indirizzo del dispositivo. Se la modalità di aggiunta impostata è **0**, occorre immettere l'indirizzo IP o il nome dominio del dispositivo; se la modalità di aggiunta impostata è **1**, questo campo non è obbligatorio.

Port

Inserire il numero di porta del dispositivo. Il valore predefinito è 8000.

Device Information

Se si imposta **0** come modalità di aggiunta, questo campo non è obbligatorio. Se la modalità di aggiunta è impostata su **1**, inserire l'account EHome.

User Name

Inserire il nome utente del dispositivo. Per impostazione predefinita, il nome utente è admin.

Password

Se la modalità di aggiunta è impostata su **0**, inserire la password. Se la modalità di aggiunta è impostata su **1**, inserire la chiave EHome.




Attenzione

Il sistema è in grado di valutare automaticamente la complessità della password del dispositivo. Si consiglia vivamente di modificare la password scelta (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto. Rientra nella responsabilità dell'installatore e/o dell'utente finale configurare correttamente tutte le password e altri parametri di sicurezza.

Importazione in gruppo

È possibile inserire **1** per creare un gruppo in base al nome del dispositivo. Per impostazione predefinita, tutti i canali del dispositivo verranno importati nel gruppo corrispondente. **0** indica la disattivazione di questa funzione.

6. Fare clic su  e selezionare il file del modello.

7. Fare clic su **Add** per importare i dispositivi.

8.2 Gestione delle persone

È possibile aggiungere al sistema informazioni sulle persone per ulteriori operazioni, quali controllo degli accessi, videocitofono, orari e presenze, ecc. È possibile gestire le persone aggiunte, ad esempio l'emissione di tessere per loro in batch, l'importazione e l'esportazione di informazioni sulle persone in batch, ecc.

8.2.1 Aggiunta di organizzazioni

È possibile aggiungere un'organizzazione e importare le informazioni sulle persone nell'organizzazione per una gestione efficace delle persone. È possibile anche aggiungere un'organizzazione secondaria a quella aggiunta.

Passaggi


1. Accedere al modulo **Person**.
2. Selezionare un'organizzazione padre nella colonna di sinistra e fare clic su **Add** nell'angolo in alto a sinistra per aggiungere un'organizzazione.
3. Creare un nome per l'organizzazione aggiunta.




Nota

È possibile aggiungere un massimo di 10 livelli di organizzazioni.

4. **Opzionale:** è possibile effettuare le operazioni seguenti.

Modifica dell'organizzazi	Passare il mouse su un'organizzazione aggiunta e fare clic su  per modificarne il nome.
----------------------------------	--

Eliminazione di un'organizzazione	Passare il mouse su un'organizzazione aggiunta e fare clic su  per eliminarla.
--	---



Nota

- Eliminando un'organizzazione, anche quelle definite ai suoi livelli inferiori saranno cancellate.
 - Per poter eliminare un'organizzazione, è necessario che non vi siano state aggiunte persone.
-

Visualizzazione di persone nell'organizzazione secondaria	Selezionare Show Persons in Sub Organization e selezionare un'organizzazione per visualizzare le persone nelle organizzazioni secondarie.
--	--

8.2.2 Configurazione delle informazioni di base

È possibile aggiungere persone al software client una alla volta e configurare le informazioni di base della persona, come nome, sesso, numero di telefono, ecc.

Passaggi

1. Accedere al modulo **Person**.
2. Selezionare un'organizzazione dall'elenco delle organizzazioni per aggiungere la persona.
3. Fare clic su **Add** per aprire la finestra di aggiunta di persone. L'ID della persona verrà generato automaticamente.
4. Immettere le informazioni di base, tra cui nome della persona, sesso, numero di telefono, indirizzo e-mail, ecc.

5. Opzionale: impostare il periodo di validità della persona. Una volta scadute, le credenziali e le impostazioni di controllo degli accessi della persona non saranno valide e la persona non avrà l'autorizzazione ad accedere alle porte\ai piani.

Esempio

Ad esempio, se la persona è un visitatore, il suo periodo effettivo può essere breve e temporaneo.

6. Confermare l'aggiunta della persona.

- Fare clic su **Add** per aggiungere la persona e chiudere la finestra Add Person.
- Fare clic su **Add and New** per aggiungere la persona e continuare ad aggiungere altre persone.

8.2.3 Emissione di una tessera per una persona

Quando si aggiunge una persona, è possibile emettere una tessera con un numero di tessera univoco come credenziali per quella persona. Dopo l'emissione, la persona può aprire le porte a cui è autorizzata ad accedere passando la tessera sul lettore di tessere.

Passaggi



Nota

Possono essere emesse fino a cinque tessere a persona.

1. Accedere al modulo **Person**.
 2. Selezionare un'organizzazione dall'elenco delle organizzazioni per aggiungere la persona e fare clic su **Add**.
-



Nota

Immettere prima di tutto le informazioni di base della persona. Per informazioni dettagliate sulla configurazione delle informazioni di base della persona, consultare la sezione **Configurazione delle informazioni di base**.

3. Nel pannello **Credential** → **Card**, fare clic su **+**.
 4. Digitare il numero della tessera.
 - Digitare manualmente il numero della tessera.
 - Per ottenere il numero della tessera, posizionarla sulla postazione di registrazione di tessere o sul lettore di tessere e fare clic su **Read**. Il numero della tessera verrà visualizzato automaticamente nel campo Card No.
-



Nota

È necessario fare clic su **Settings** per impostare prima la modalità di emissione delle tessere e i relativi parametri. Per ulteriori dettagli, consultare la sezione **Impostazione dei parametri di emissione delle tessere**.

5. Selezionare il tipo di tessera in base alle esigenze.

Normal Card

La tessera viene utilizzata per aprire le porte, per un utilizzo normale.

Duress Card

Quando la persona è sotto coercizione, può passare la tessera di coercizione per aprire la porta. La porta sarà sbloccata e il client riceverà un evento di coercizione per avvisare il personale addetto alla sicurezza.

Patrol Card

Questa tessera viene utilizzata per controllare le presenze del personale addetto alle ispezioni. Passando la tessera sul lettore di tessere specifico, la persona viene contrassegnata come di turno di ispezione.

Dismiss Card

Passando la tessera sul lettore di tessera, è possibile interrompere l'avvisatore acustico di tale dispositivo.

6. Fare clic su **Add**.

La tessera sarà assegnata alla persona.

7. Confermare l'aggiunta della persona.

- Fare clic su **Add** per aggiungere la persona e chiudere la finestra Add Person.
- Fare clic su **Add and New** per aggiungere la persona e continuare ad aggiungere altre persone.

8.2.4 Raccolta delle impronte digitali tramite il client

La raccolta di impronte digitali a livello locale consente di acquisirle tramite il registratore di impronte digitali collegato direttamente al PC sul quale è in esecuzione il client. Le impronte digitali registrate possono essere utilizzate come credenziali per le persone che desiderano accedere alle porte autorizzate.

Prima di iniziare

Collegare il registratore di impronte digitali al PC ed utilizzare il client.

Passaggi

1. Accedere al modulo **Person**.
2. Selezionare un'organizzazione dall'elenco delle organizzazioni per aggiungere la persona e fare clic su **Add**.



Nota

Immettere prima di tutto le informazioni di base della persona. Per informazioni dettagliate sulla configurazione delle informazioni di base della persona, consultare la sezione **Configurazione delle informazioni di base**.

3. Nel pannello **Credential** → **Fingerprint**, fare clic su +.
4. Nella finestra a comparsa, selezionare la modalità di raccolta **Local**.
5. Selezionare il modello del registratore di impronte digitali collegato.



Nota

Se il registratore di impronte digitali è DS-K1F800-F, è possibile fare clic su **Settings** per selezionare la porta COM alla quale si connette il registratore di impronte digitali.

6. Raccogliere l'impronta digitale.

- 1) Fare clic su **Start**.
- 2) Per acquisire un'impronta, appoggiare e sollevare il dito in questione sul registratore di impronte digitali.
- 3) Fare clic su **Add** per salvare l'impronta digitale registrata.

7. Confermare l'aggiunta della persona.

- Fare clic su **Add** per aggiungere la persona e chiudere la finestra Add Person.
- Fare clic su **Add and New** per aggiungere la persona e continuare ad aggiungere altre persone.

8.2.5 Raccolta di impronte digitali tramite dispositivo di controllo accessi

Quando si aggiunge una persona, è possibile raccoglierne le impronte digitali tramite il modulo per le impronte digitali del dispositivo di controllo accessi. Le impronte digitali registrate possono essere utilizzate come credenziali per le persone che desiderano accedere alle porte autorizzate.

Prima di iniziare

Assicurarsi che il dispositivo di controllo accessi supporti la raccolta di impronte digitali.

Passaggi

1. Accedere al modulo **Person**.
2. Selezionare un'organizzazione dall'elenco delle organizzazioni per aggiungere la persona e fare clic su **Add**.



Nota

Immettere prima di tutto le informazioni di base della persona. Per informazioni dettagliate sulla configurazione delle informazioni di base della persona, consultare la sezione **Configurazione delle informazioni di base**.

3. Nel pannello **Credential** → **Fingerprint**, fare clic su +.
4. Nella finestra a comparsa, selezionare la modalità di raccolta **Remote**.
5. Dall'elenco a discesa selezionare un dispositivo di controllo accessi che supporti la funzione di riconoscimento delle impronte digitali.
6. Raccogliere l'impronta digitale.
 - 1) Fare clic su **Start**.
 - 2) Per acquisire un'impronta, appoggiare e sollevare il dito in questione sullo scanner di impronte digitali del dispositivo di controllo accessi selezionato.
 - 3) Fare clic su **Add** per salvare l'impronta digitale registrata.

7. Confermare l'aggiunta della persona.

- Fare clic su **Add** per aggiungere la persona e chiudere la finestra Add Person.
- Fare clic su **Add and New** per aggiungere la persona e continuare ad aggiungere altre persone.

8.2.6 Configurazione delle informazioni sul controllo degli accessi

Quando si aggiunge una persona, è possibile impostarne le proprietà di controllo degli accessi, ad esempio l'impostazione della persona come visitatore o come persona nella blacklist o come utente con privilegi avanzati, che dispone di un'autorizzazione privilegiata.

Passaggi

1. Accedere al modulo **Person**.
2. Selezionare un'organizzazione dall'elenco delle organizzazioni per aggiungere la persona e fare clic su **Add**.



Nota

Immettere prima di tutto le informazioni di base della persona. Per informazioni dettagliate sulla configurazione delle informazioni di base della persona, consultare la sezione **Configurazione delle informazioni di base**.

3. Nel pannello **Access Control**, impostare le proprietà di controllo degli accessi per la persona.

PIN Code

Durante l'accesso, il codice PIN deve essere utilizzato dopo la tessera le impronte digitali. Non può essere utilizzato separatamente. Deve contenere da 4 a 8 cifre.

Super User

Se la persona è impostata come utente con privilegi avanzati, avrà l'autorizzazione ad accedere a tutte le porte/piani e sarà esonerato dalle restrizioni sulle porte chiuse, da tutte le regole anti-passback e dall'autorizzazione della prima persona.

Extended Door Open Time

Quando una persona a mobilità ridotta accede alla porta, è possibile concederle più tempo per attraversare le porte configurate, mediante un durata di apertura estesa. Utilizzare questa funzione per le persone a mobilità ridotta. Per ulteriori informazioni sull'impostazione della durata di apertura delle porte, fare riferimento a **Configurazione dei parametri delle porte**.

Add to Blacklist

Aggiungendo una persona alla blacklist, quando tale persona tenta di accedere a porte/piani, viene attivato un evento e inviato al client per avvisare il personale di sicurezza.

Mark as Visitor

Se la persona è un visitatore, impostare il numero massimo di autenticazioni, incluso l'accesso tramite tessera impronta digitale, per limitare i tempi di accesso del visitatore.



Nota

Il numero massimo di autenticazioni deve essere compreso tra 1 e 100.

Device Operator

La persona con ruolo di operatore del dispositivo è autorizzata a utilizzare i dispositivi di controllo accessi.



Nota

Le funzioni Super User, Extended Door Open Time, Add to Blacklist e Mark as Visitor non possono essere attivate contemporaneamente. Ad esempio, se una persona è impostata come utente con privilegi avanzati, non è possibile attivare un tempo di apertura porte esteso per la stessa, aggiungerla alla blacklist o impostarla come visitatore.

4. Confermare l'aggiunta della persona.

- Fare clic su **Add** per aggiungere la persona e chiudere la finestra Add Person.
- Fare clic su **Add and New** per aggiungere la persona e continuare ad aggiungere altre persone.

8.2.7 Personalizzazione delle informazioni personali

È possibile personalizzare le proprietà della persona non predefinite nel client in base alle esigenze effettive, ad esempio il luogo di nascita. Dopo la personalizzazione, quando si aggiunge una persona, è possibile immettere le informazioni personalizzate per completare i dati personali.

Passaggi

1. Accedere al modulo **Person**.

2. Impostare i campi delle informazioni personalizzate.

- 1) Fare clic su **Custom Property**.
- 2) Fare clic su **Add** per aggiungere una nuova proprietà.
- 3) Inserire il nome della proprietà.
- 4) Fare clic su **OK**.

3. All'aggiunta di una persona, impostarne le informazioni personalizzate.

- 1) Selezionare un'organizzazione dall'elenco delle organizzazioni per aggiungere la persona e fare clic su **Add**.
-



Nota

Immettere prima di tutto le informazioni di base della persona. Per informazioni dettagliate sulla configurazione delle informazioni di base della persona, consultare la sezione **Configurazione delle informazioni di base**.

- 2) Nel pannello **Custom Information**, immettere le informazioni sulla persona.
- 3) Fare clic su **Add** per aggiungere la persona e chiudere la finestra Add Person oppure fare clic su **Add and New** per aggiungere la persona e continuare ad aggiungere altre persone.

8.2.8 Configurazione di ulteriori informazioni

Quando si aggiunge una persona, è possibile configurarne ulteriori informazioni, ad esempio il tipo di documento di identità, il numero del documento di identità, il paese, ecc., in base alle necessità.

Passaggi

1. Accedere al modulo **Person**.
2. Selezionare un'organizzazione dall'elenco delle organizzazioni per aggiungere la persona e fare clic su **Add**.



Nota

Immettere prima di tutto le informazioni di base della persona. Per informazioni dettagliate sulla configurazione delle informazioni di base della persona, consultare la sezione **Configurazione delle informazioni di base**.

3. Nel pannello **Additional Information**, inserire ulteriori informazioni sulla persona, ad esempio il tipo di iD, il numero ID, il ruolo, ecc., in base alle necessità.
4. Confermare l'aggiunta della persona.
 - Fare clic su **Add** per aggiungere la persona e chiudere la finestra Add Person.
 - Fare clic su **Add and New** per aggiungere la persona e continuare ad aggiungere altre persone.

8.2.9 Importazione ed esportazione di informazioni di identificazione personali

È possibile importare le informazioni di più persone nel software client in batch. Inoltre, è possibile anche esportare le informazioni delle persone e salvarle nel PC.

8.2.10 Importazione delle informazioni delle persone

È possibile immettere le informazioni di più persone in un modello predefinito (un file CSV) per importarle nel client in batch.

Passaggi


1. Accedere al modulo **Person**.
2. Selezionare dall'elenco una delle organizzazioni aggiunte o fare clic su **Add** nell'angolo in alto a sinistra per aggiungere un'organizzazione e poi selezionarla.
3. Fare clic su **Import** per aprire il pannello relativo all'importazione.
4. Selezionare **Person Information** come modalità di importazione.

5. Fare clic su **Download Template for Importing Person** per scaricare il modello.
6. Inserire le informazioni delle persone nel modello scaricato.



Nota

- Se la persona dispone di più tessere, separare il numero di tessera con un punto e virgola.
- Le voci con asterisco sono obbligatorie.
- Per impostazione predefinita, la data di assunzione è la data corrente.

7. Fare clic su  per selezionare il file CSV con le informazioni
8. Fare clic su **Import** per avviare



Nota

- Se il numero di una persona esiste già sul database del client, eliminare le informazioni esistenti prima dell'importazione.
- È possibile importare informazioni per non più di 10.000 persone.

8.2.11 Esportazione di informazioni delle persone

È possibile esportare le informazioni delle persone aggiunte al PC locale come file CSV.

Prima di iniziare

Assicurarsi di aver aggiunto persone a un'organizzazione.

Passaggi

1. Accedere al modulo Person.
2. **Opzionale:** selezionare un'organizzazione dall'elenco.



Nota

Tutte le informazioni delle persone verranno esportate se non si seleziona alcuna organizzazione.

3. Fate clic su **Export** per aprire il pannello dell'esportazione e selezionare **Person Information** come contenuto da esportare.
4. Selezionare gli elementi da esportare.
5. Fare clic su **Export** per salvare sul PC il file CSV esportato.

8.2.12 Recupero delle informazioni delle persone dal dispositivo di controllo accessi

Se il dispositivo di controllo accessi aggiunto è stato configurato con le informazioni delle persone (quali dettagli personali, impronte digitali e informazioni delle tessere emesse), è possibile acquisire tali informazioni dal dispositivo e importarle nel client per ulteriori utilizzi.



Nota

- Se il nome della persona memorizzato nel dispositivo è vuoto, verrà compilato con il numero della tessera emessa dopo l'importazione nel client.
 - Per impostazione predefinita, il sesso delle persone è **Male**.
 - Se il numero della tessera o l'ID della persona (ID dipendente) memorizzato sul dispositivo esiste già nel database del client, la persona con questo numero di tessera o ID di persona non verrà importata nel client.
-

1. Accedere al modulo **Person**.
2. Selezionare un'organizzazione in cui importare le persone.
3. Fare clic su **Get from Device**.
4. Selezionare il dispositivo di controllo accessi dall'elenco a discesa.
5. Fare clic su **Get** per iniziare a importare le informazioni delle persone nel client.

Le informazioni delle persone in questione, quali dettagli personali, impronte digitali (se configurate) e tessere loro associate (se configurate), saranno importate nell'organizzazione selezionata.

8.2.13 Trasferimento di persone a un'altra organizzazione

È possibile spostare in un'altra organizzazione le persone aggiunte, se necessario.

Prima di iniziare

- Assicurarsi di aver aggiunto almeno due organizzazioni.
- Assicurarsi di aver importato le informazioni delle persone.

Passaggi

1. Accedere al modulo **Person**.
2. Selezionare un'organizzazione dal pannello a sinistra.
Le persone che fanno parte dell'organizzazione verranno visualizzate nel riquadro a destra.
3. Selezionare la persona da trasferire.
4. Fare clic su **Change Organization**.
5. Selezionare l'organizzazione in cui spostare le persone.
6. Fare clic su **OK**.

8.2.14 Rilascio di tessere a persone in batch

Il client fornisce un modo comodo per emettere tessere a più persone in batch.

Passaggi


1. Accedere al modulo **Person**.
2. Fare clic su **Batch Issue Cards**.
Verranno visualizzate tutte le persone aggiunte per le quali non è stata emessa una tessera.


3. Impostare i parametri di emissione delle tessere. Per ulteriori dettagli, consultare la sezione **Impostazione dei parametri di emissione delle tessere**.
4. Fare clic su **Initialize** per inizializzare la postazione di registrazione di tessere o il lettore di tessere e prepararli ad emettere tessere.
5. Fare clic sulla colonna del numero della tessera e immettere il numero della tessera.
 - Posizionare la tessera sulla postazione di registrazione di tessere.
 - Passare la tessera sul lettore di tessere.
 - Inserire manualmente il numero della tessera e premere il tasto **Enter** sulla tastiera.Il numero della tessera sarà letto in automatico e la tessera verrà emessa alla prima persona in elenco.
6. Ripetere i passi precedenti per emettere tessere alle persone in elenco in sequenza.

8.2.15 Segnalazione di smarrimento della tessera

Se una persona ha perso la sua tessera, è possibile segnalare la perdita in modo che la relativa autorizzazione di accesso della tessera venga resa inattiva.

Passaggi

1. Accedere al modulo **Person**.
2. Selezionare la persona per la quale si desidera segnalare la perdita della tessera e fare clic su **Edit** per aprire la finestra Edit Person.
3. Nel pannello **Credential** → **Card**, fare clic su  sulla tessera aggiunta, per impostarla come tessera perduta.

Una volta segnalato lo smarrimento della tessera, l'autorizzazione di accesso della tessera non sarà più valida e verrà disattivata. Chiunque utilizzi questa tessera non potrà accedere alle porte facendo passare questa tessera perduta.
4. **Opzionale:** se la tessera perduta viene ritrovata, è possibile annullarne lo smarrimento facendo clic su .

Una volta annullato lo smarrimento della tessera, l'autorizzazione di accesso della persona sarà valida e attiva.
5. Se la tessera perduta viene aggiunta in un gruppo di accesso e questo è già applicato al dispositivo, dopo aver segnalato la perdita della tessera o averne annullato la segnalazione, compare una finestra che informa l'utente di applicare le modifiche al dispositivo. Dopo averle applicate al dispositivo, queste modifiche potranno avere effetto su di esso.

8.2.16 Impostazione dei parametri di emissione delle tessere

Il client consente due modalità per la lettura del numero di una tessera: tramite postazione di registrazione di tessere o tramite lettore di tessere del dispositivo di controllo accessi. Se è disponibile una postazione di registrazione di tessere, collegarla al computer dove è in esecuzione il client tramite interfaccia USB o COM, quindi posizionare la tessera su tale unità per leggerne il numero. In caso contrario, è anche possibile passare la tessera

sul lettore di tessere del dispositivo di controllo accessi aggiunto per ottenere il numero della tessera. Quindi, prima di emettere una tessera a una persona, è necessario impostare i parametri di emissione inclusi la modalità di emissione e relativi parametri.

Quando si aggiunge una tessera a una persona, fare clic su **Settings** per aprire la finestra Card Issuing Settings.

Modalità locale: rilascio di tessere tramite postazione di registrazione di tessere

Collegare una postazione di registrazione di tessere al computer in cui è in esecuzione il client. È possibile posizionare la tessera sulla postazione di registrazione di tessere per ottenerne il numero.

Postazione di registrazione di tessere

Selezionare il modello della postazione di registrazione di tessere collegata.



Nota

Attualmente, il modello di postazione di registrazione di tessere supportato è DS- K1F180-D8E.

Card Type

Selezionare il tipo di tessera come tessera EM o IC in base al tipo di tessera effettivo.

Buzzing

Attiva o disattiva l'avvisatore acustico quando il numero della tessera viene letto correttamente.

Card No. Type

Selezionare il tipo di numero della tessera in base alle esigenze.

M1 Card Encryption

Se si tratta di una tessera M1 e occorre abilitare la funzione di crittografia delle tessere M1, è necessario abilitarla e selezionare il settore della tessera da crittografare.

Modalità remota: rilascio di tessere tramite lettore di tessere

Selezionare un dispositivo di controllo accessi aggiunto nel client e passare la tessera sul relativo lettore per leggerne il numero.

8.3 Configurazione di pianificazioni e modelli

È possibile configurare il modello per includere pianificazioni di ferie e settimanali. Dopo aver impostato il modello, è possibile utilizzarlo per impostare i gruppi di accesso, in modo che siano validi nei periodi indicati dal modello.



Nota

Per le impostazioni del gruppo di accesso, consultare la sezione ***Impostazione di un gruppo di accesso per l'assegnazione di autorizzazioni di accesso alle persone***

8.3.1 Aggiunta di ferie

È possibile creare ferie e impostarne i giorni, inserendo la data di inizio, la data di fine e la durata delle ferie stesse.

Passaggi



Nota

È possibile aggiungere fino a 64 ferie nel sistema software.

1. Fare clic su **Access Control** → **Schedule** → **Holiday** per accedere alla pagina Holiday.
 2. Fare clic su **Add** nel pannello a sinistra.
 3. Creare un nome per il giorno di ferie.
 4. **Opzionale:** inserire le descrizioni o alcune notifiche per questa vacanza nella casella dei commenti.
 5. Aggiungere un periodo di ferie all'elenco delle ferie e configurarne la durata.
-



Nota






È possibile aggiungere fino a 16 periodi a un giorno di ferie.

- 1) Fare clic su **Add** nel campo Holiday List.
 - 2) Trascinare il cursore per evidenziare un periodo di tempo, ossia individuare la durata di attivazione del gruppo di accesso.
-



Nota

È possibile definire fino a 8 durate per ciascun periodo di ferie.

- 3) **Opzionale:** effettuare le seguenti operazioni per modificare le durate.
 - Spostare il cursore sulla durata di tempo e trascinarla sulla barra della sequenza temporale nella posizione desiderata quando il cursore assume diventa .
 - Fare clic sulla durata di tempo e modificarne direttamente l'ora di inizio/fine nella finestra di dialogo visualizzata.
 - Spostare il cursore all'inizio o alla fine della durata di tempo e trascinarlo per allungarla o ridurla quando il cursore diventa .
 - 4) **Opzionale:** selezionare la durata di tempo da eliminare, quindi fare clic su  nella colonna Operation, per eliminare la durata di tempo selezionata.
 - 5) **Opzionale:** fare clic su  nella colonna Operation per cancellare tutte le durate nella barra temporale.
 - 6) **Opzionale:** fare clic su  nella colonna Operation per eliminare questo periodo di ferie aggiunto dall'elenco delle ferie.
6. Fare clic su **Save**.

8.3.2 Aggiunta di modelli

Il modello include la pianificazione settimanale e delle ferie. È possibile impostare la pianificazione settimanale e assegnare la durata dell'autorizzazione di accesso a una persona o gruppo diverso. È possibile anche selezionare le ferie aggiunte per il modello.



Nota

È possibile aggiungere fino a 255 modelli nel sistema software.

1. Fare clic su **Access Control** → **Schedule** → **Template** per accedere alla pagina Template.
-



Nota

Sono disponibili due modelli predefiniti: All-Day Authorized e All-Day Denied, che non possono essere modificati né eliminati.

All-Day Authorized

L'autorizzazione di accesso è valida in ogni giorno della settimana e non ci sono ferie.

All-Day Denied



L'autorizzazione di accesso non è valida in alcun giorno della settimana e non ci sono ferie.

2. Facendo clic sul pulsante **Add** nel pannello di sinistra, è possibile creare un nuovo modello.
 3. Creare un nome per il modello.
 4. Inserire le descrizioni o alcune notifiche per questo modello nella casella dei commenti.
 5. Modificare la pianificazione settimanale per applicarla al modello.
 - 1) Fare clic sulla schermata **Week Schedule** nel pannello in basso.
 - 2) Selezionare un giorno della settimana ed evidenziare il periodo di tempo sulla barra della sequenza temporale.
-



Nota

È possibile definire fino a 8 periodi di tempo per ciascun giorno nella pianificazione settimanale.

- 3) **Opzionale:** effettuare le seguenti operazioni per modificare le durate.
 - Spostare il cursore sulla durata di tempo e trascinarla sulla barra della sequenza temporale nella posizione desiderata quando il cursore assume diventa .
 - Fare clic sulla durata di tempo e modificarne direttamente l'ora di inizio/fine nella finestra di dialogo visualizzata.
 - Spostare il cursore all'inizio o alla fine della durata di tempo e trascinarlo per allungarla o ridurla quando il cursore diventa .
 - 4) Ripetere i due passaggi precedenti per evidenziare altri periodi di tempo negli altri giorni della settimana.
6. Aggiungere delle ferie da applicare al modello.
-



Nota


È possibile aggiungere fino a 4 ferie a un modello.

- 1) Fare clic sulla schermata **Holiday**.
- 2) Selezionare delle ferie nell'elenco a sinistra e verranno aggiunte all'elenco selezionato nel pannello a destra.
- 3) **Opzionale:** fare clic su **Add** per aggiungere un nuovo giorno di ferie.



Nota

Per ulteriori informazioni sull'aggiunta di un giorno di ferie, fare riferimento a **Aggiunta di ferie**.

- 4) **Opzionale:** selezionare un determinato giorno di ferie nell'elenco a destra e fare clic su  per rimuoverlo oppure su **Clear** per cancellare tutte le ferie selezionate nell'elenco a destra.
7. Fare clic su **Save** per salvare le impostazioni e completare l'aggiunta del modello.

8.4 Impostazione di un gruppo di accesso per l'assegnazione di autorizzazioni di accesso alle persone

Dopo aver aggiunto la persona e averne configurato le credenziali, è possibile creare i gruppi di accesso per definire quali persone possono accedere a quali porte e quindi applicare il gruppo di accesso al dispositivo di controllo accessi per rendere effettive le autorizzazioni.

Passaggi

- Per una persona, è possibile aggiungere fino a 4 gruppi di accesso al punto di controllo accessi di un dispositivo.
 - È possibile aggiungere fino a 128 gruppi di accesso in totale.
 - Quando le impostazioni dei gruppi di accesso vengono modificate, è necessario applicare nuovamente i gruppi di accesso ai dispositivi per renderle effettive. Le modifiche al gruppo di accesso comprendono modifiche al modello, alle impostazioni del gruppo di accesso, alle impostazioni del gruppo di accesso della persona e ai dettagli relativi alla persona (tra cui numero di tessera, impronta digitale, collegamento tra numero di tessera e impronta digitale, password della tessera, periodo di validità della tessera, ecc.).
1. Fare clic su **Access Control** → **Access Group** per accedere all'interfaccia Access Group.
 2. Fare clic su **Add** per aprire la finestra Add.
 3. Nel campo di testo **Name**, creare un nome per il gruppo di accesso.
 4. Selezionare un modello per il gruppo di accesso.



Nota

Occorre configurare il modello prima di definire le impostazioni del gruppo di accesso. Per ulteriori informazioni, consultare la sezione **Configurazione di pianificazioni e modelli**.

5. Nell'elenco a sinistra del campo Select Person, selezionare le persone che verranno aggiunte all'elenco selezionato.

6. Nell'elenco a sinistra del campo Select Door, selezionare le porte o le postazioni esterne per consentire alle persone selezionate di accedere e le porte o le postazioni esterne selezionate verranno aggiunte all'elenco selezionato.
 7. Fare clic su **OK**.
 8. Dopo l'aggiunta dei gruppi di accesso, è necessario applicarli ai dispositivi di controllo accessi per renderli effettivi.
 - 1) Selezionare uno o più gruppi di accesso da applicare al dispositivo di controllo accessi.
Per selezionare più gruppi di accesso, è possibile tenere premuti i tasti **Ctrl** o **Shift** e selezionare i gruppi di accesso.
 - 2) Fare clic su **Apply All to Devices** per iniziare ad applicare tutti i gruppi di accesso selezionati al dispositivo di controllo accessi o alla postazione esterna.
-




Attenzione

- Fare attenzione quando si fa clic su **Apply All to Devices**, poiché questa operazione cancella tutti i gruppi di accesso dei dispositivi selezionati e applica il nuovo gruppo di accesso, il che potrebbe comportare rischi per i dispositivi.
 - È possibile fare clic su **Apply Changes to Devices** per applicare soltanto la parte modificata dei gruppi di accesso selezionati ai dispositivi.
-

- 3) Visualizzare lo stato di applicazione nella colonna Status o fare clic su **Applying Status** per visualizzare tutti i gruppi di accesso applicati.

Le persone selezionate nei gruppi di accesso applicati avranno l'autorizzazione di ingresso/uscita dalle porte/postazioni esterne selezionate tramite le loro tessere collegate o il riconoscimento con impronte digitali.


9. **Opzionale:** fare clic su  per modificare il gruppo di accesso, se necessario.

8.5 Configurazione delle funzioni avanzate

È possibile configurare le funzioni avanzate di controllo degli accessi per soddisfare alcuni requisiti speciali in diverse scene.



Nota

- Per le funzioni correlate alla tessera (il tipo di tessera di controllo accessi), solo le tessere con il gruppo di accesso applicato saranno elencate durante l'aggiunta di tessere.
 - Le funzioni avanzate devono essere supportate dal dispositivo.
 - Passare il cursore sulla funzione avanzata, quindi fare clic su  per personalizzare le funzioni avanzate da visualizzare.
-

8.5.1 Configurazione dei parametri del dispositivo

Dopo aver aggiunto il dispositivo di controllo accessi, è possibile configurare i parametri dello stesso e dei relativi punti di controllo accessi.

Configurazione dei parametri per il dispositivo di controllo accessi


Dopo aver aggiunto il dispositivo di controllo accessi, è possibile configurarne i parametri.

Passaggi

1. Fare clic su **Access Control** → **Advanced Function** → **Device Parameter**.



Nota

Se è presente Device Parameter nell'elenco Advanced Function, posizionare il cursore su Advanced Function, quindi fare clic su  per selezionare il Device Parameter da visualizzare.

2. Selezionare un dispositivo di accesso per visualizzarne i parametri sulla pagina a destra.
3. Spostare l'interruttore su ON per attivare le funzioni corrispondenti.



Nota

- I parametri visualizzati possono variare in base ai diversi dispositivi di controllo accessi.
 - Alcuni dei seguenti parametri non sono elencati nella pagina Basic Information; fare clic su **More** per modificare i parametri.
-

Voice Prompt

Se si attiva questa funzione, nel dispositivo vengono attivate le istruzioni vocali. È possibile ascoltare le istruzioni vocali quando si utilizza il dispositivo.

Press Key to Enter Card Number


Se si attiva questa funzione, è possibile immettere il numero della tessera premendo il tasto.

4. Fare clic su **OK**.
5. **Opzionale:** fare clic su **Copy to**, quindi selezionare il dispositivo di controllo accessi per copiare i parametri nella pagina sui dispositivi selezionati.

Configurazione dei parametri delle porte

Dopo aver aggiunto il dispositivo di controllo accessi, è possibile configurare i parametri del punto di accesso.

Passaggi

1. Fare clic su **Access Control** → **Advanced Function** → **Device Parameter**.
2. Selezionare un dispositivo di controllo accessi sul pannello di sinistra, quindi fare clic su  per visualizzare le porte del dispositivo selezionato.
3. Selezionare una porta per visualizzarne i parametri sulla pagina a destra.

4. Modificare i parametri della porta o del piano.



Nota

- I parametri visualizzati possono variare in base ai diversi dispositivi di controllo accessi.
 - Alcuni dei seguenti parametri non sono elencati nella pagina Basic Information; fare clic su **More** per modificare i parametri.
-

Name

Inserire il nome preferito per il lettore di tessere.

Door Contact

È possibile impostare il sensore della porta in modo che rimanga chiuso o aperto. In genere, lo stato standard è chiuso.

Exit Button Type

È possibile impostare il pulsante di uscita in modo che rimanga chiuso o aperto. In genere, lo stato standard è aperto.

Door Locked Time

Dopo il passaggio di una tessera normale e l'attivazione del relè, si avvia il timer di chiusura della porta.

Door Left Open Timeout Alarm

L'allarme può essere attivato se la porta non è stata chiusa entro un periodo di tempo configurato. Se è impostato su 0, non viene attivato alcun allarme.

Super Password

Le persone autorizzate possono aprire la porta immettendo la password di livello superiore.

Duress Code

La porta può essere aperta immettendo la password anti-coercizione in caso di minacce. Allo stesso tempo, il client è in grado di segnalare l'evento di coercizione.

Dismiss Code

Creare un codice di interruzione che può essere utilizzato per arrestare l'avvisatore acustico del lettore di tessere (inserendo il codice di interruzione con la tastiera).



Nota

- La password anti-coercizione, il codice di livello superiore e quello di interruzione devono essere differenti.
 - La password anti-coercizione, la password di livello superiore e il codice di interruzione devono essere diversi dalla password di autenticazione.
 - La lunghezza della password anti-coercizione e della password di livello superiore dipende dal dispositivo e in genere contiene da 4 a 8 numeri.
-

5. Fare clic su **OK**.

6. **Opzionale:** fare clic su **Copy to**, quindi selezionare la porta per copiare i parametri nella pagina sulle porte selezionate.




Nota

La durata dello stato della porta sarà copiata anche nelle altre porte selezionate.

Configurazione dei parametri del lettore di tessere

Dopo aver aggiunto il dispositivo di controllo accessi, è possibile configurare i parametri del suo lettore di tessere.

Passaggi

1. Fare clic su **Access Control** → **Advanced Function** → **Device Parameter**.
2. Espandere la porta nell'elenco dei dispositivi sulla sinistra, facendo clic su , quindi selezionare un lettore di tessere per modificarne i parametri, visualizzati sulla destra.
3. Modificare i parametri di base del lettore di tessere nella pagina Basic Information.



Nota

- I parametri visualizzati possono variare in base ai diversi dispositivi di controllo accessi. Qui di seguito sono elencati alcuni dei parametri. Per ulteriori dettagli, consultare il manuale dell'utente del dispositivo.
 - Alcuni dei seguenti parametri non sono elencati nella pagina Basic Information; fare clic su **More** per modificare i parametri.
-

Name

Inserire il nome preferito per il lettore di tessere.

Minimum Card Swiping Interval

Consente di definire l'intervallo di tempo minimo tra due passaggi della stessa tessera: al di sotto di tale valore il passaggio non è valido. È possibile impostare un valore da 0 a 255.

Alarm of Max. Failed Attempts

Consente di abilitare l'allarme di segnalazione dei casi in cui il numero di tentativi falliti di lettura di una tessera raggiunge il valore impostato.

Max. Times of Card Failure

Consente di impostare il numero massimo di tentativi errati ammessi per la lettura di tessere.

Card Reader Type/Card Reader Description

Ottenere il tipo e la descrizione del lettore di tessere. Si tratta di informazioni di sola lettura.

Default Authentication Mode

Visualizzare la modalità di autenticazione predefinita del lettore di tessere.

Fingerprint Capacity

Visualizzare il numero massimo di impronte digitali disponibili.

Existing Fingerprint Number

Visualizzare il numero di impronte digitali presenti nel dispositivo.

4. Fare clic su **Advanced** per configurare altri parametri.

Enable Card Reader

Abilitare la funzione per utilizzare le seguenti funzioni sul lettore di tessere.

Buzzer Polarity

Impostare Buzzer Polarity per la tessera principale in base ai parametri del lettore di tessere. In genere, adotta le impostazioni predefinite.

Max. Interval When Entering PWD

Consente di definire l'intervallo di tempo massimo tra l'inserimento di due cifre durante l'immissione della password del lettore di tessere: al di sopra di tale valore le cifre inserite in precedenza vengono automaticamente cancellate.

Fingerprint Recognition Level

Selezionare il livello di riconoscimento dell'impronta digitale dall'elenco a discesa.

Fingerprint Recognition Interval

Selezionare l'intervallo di riconoscimento delle impronte digitali dall'elenco a discesa.

5. Fare clic su **OK**.

6. **Opzionale:** fare clic su **Copy to**, quindi selezionare il lettore di tessere per copiare i parametri nella pagina sul lettore di tessere selezionato.

8.5.2 Configurazione per mantenere aperta/chiusa una porta

È possibile impostare lo stato della porta come aperta o chiusa. Ad esempio, è possibile impostare la porta per mantenerla chiusa durante le ferie e aperta in un determinato momento della giornata lavorativa.

Prima di iniziare

Aggiungere i dispositivi di controllo accessi al sistema.

Passaggi



1. Fare clic su **Access Control** → **Advanced Function** → **Remain Open/ Closed** per accedere alla pagina Remain Open/Closed.
2. Selezionare la porta da configurare sul pannello a sinistra.
3. Per impostare lo stato della porta durante la giornata di lavoro, fare clic su **Week Schedule** ed effettuare le seguenti operazioni.
 - 1) Fare clic su **Remain Open** o **Remain Closed**.
 - 2) Trascinare il cursore per evidenziare un periodo di tempo, ossia individuare la durata di attivazione del gruppo di accesso.



Nota

È possibile definire fino a 8 periodi di tempo per ciascun giorno nella pianificazione settimanale.

3) **Opzionale:** effettuare le seguenti operazioni per modificare le durate.

- Spostare il cursore sulla durata di tempo e trascinarla sulla barra della sequenza temporale nella posizione desiderata quando il cursore assume diventa .
- Fare clic sulla durata di tempo e modificarne direttamente l'ora di inizio/fine nella finestra di dialogo visualizzata.
- Spostare il cursore all'inizio o alla fine della durata di tempo e trascinarlo per allungarla o ridurla quando il cursore diventa .

4) Fare clic su **Save. Operazioni collegate**

Copy to Whole Week	Selezionare una durata nella barra temporale, fare clic su Copy to Whole Week per copiare tutte le impostazioni di durata in questa barra temporale per altri giorni della settimana.
Delete Selected	Selezionare una durata sulla barra temporale, quindi fare clic su Delete Selected per eliminare questa durata.
Clear	Fare clic su Clear per cancellare tutte le impostazioni di durata nella pianificazione settimanale.

4. Per impostare lo stato della porta durante il giorno di ferie, fare clic su **Holiday** ed effettuare le seguenti operazioni.



- 1) Fare clic su **Remain Open** o **Remain Closed**.
- 2) Fare clic su **Add**.
- 3) Immettere la data di inizio e quella di fine.
- 4) Trascinare il cursore per evidenziare un periodo di tempo, ossia individuare la durata di attivazione del gruppo di accesso.






Nota

È possibile definire fino a 8 durate per ciascun periodo di ferie.

5) effettuare le seguenti operazioni per modificare le durate.

- Spostare il cursore sulla durata di tempo e trascinarla sulla barra della sequenza temporale nella posizione desiderata quando il cursore assume diventa .
- Fare clic sulla durata di tempo e modificarne direttamente l'ora di inizio/fine nella finestra di dialogo visualizzata.
- Spostare il cursore all'inizio o alla fine della durata di tempo e trascinarlo per allungarla o ridurla quando il cursore diventa .

6) **Opzionale:** selezionare la durata di tempo da eliminare, quindi fare clic su  nella colonna Operation, per eliminare la durata di tempo selezionata.

- 7) **Opzionale:** fare clic su  nella colonna Operation per cancellare tutte le durate nella barra temporale.
 - 8) **Opzionale:** fare clic su  nella colonna Operation per eliminare questo periodo di ferie aggiunto dall'elenco delle ferie.
 - 9) Fare clic su **Save**.
5. **Opzionale:** fare clic su **Copy to** per copiare le impostazioni sullo stato della porta su altre porte.

8.5.3 Configurazione della regola Wiegand personalizzata

Basandosi sulla conoscenza della regola di caricamento per l'interfaccia Wiegand di terze parti, è possibile impostare più regole Wiegand personalizzate in modo che comunichino tra il dispositivo e i lettori di tessere di terze parti.

Prima di iniziare

Collegare i cavi tra i lettori di tessere di terzi e il dispositivo.

Passaggi



Nota

- Per impostazione predefinita, il dispositivo disabilita la funzione Wiegand personalizzata. Se il dispositivo abilita la funzione Wiegand personalizzata, tutte le interfacce Wiegand nel dispositivo utilizzeranno il protocollo Wiegand personalizzato.
 - È possibile impostare fino a 5 interfacce Wiegand personalizzate.
 - Per ulteriori informazioni sulla regola Wiegand personalizzata, consultare Descrizione delle regole Wiegand personalizzate.
-

1. Fare clic su **Access Control** → **Advanced Function** → **Custom Wiegand** per accedere alla pagina Custom Wiegand.
 2. Selezionare una regola Wiegand personalizzata a sinistra.
 3. Creare un nome per la regola Wiegand.
-



Nota

Il nome della regola Wiegand personalizzata può contenere un massimo di 32 caratteri.

4. Fare clic su **Select Device** per selezionare il dispositivo di controllo accessi per l'impostazione della regola Wiegand personalizzata.
 5. Impostare la modalità di parità in base alla proprietà del lettore di tessere di terze parti.
-



Nota

- Nella lunghezza totale è consentito un massimo di 80 bit.
 - Il bit di inizio della parità dispari, la lunghezza della parità dispari, il bit di inizio della parità pari e la lunghezza della parità pari vanno da 1 a 80 bit.
 - Il bit di avvio dell'ID della tessera, il codice del produttore, il codice del sito e l'OEM vanno da 1 a 80 bit.
-

6. Impostare la regola di trasformazione dell'uscita.

- 1) Fare clic su **Set Rule** per aprire la finestra Set Output Transformation Rules.

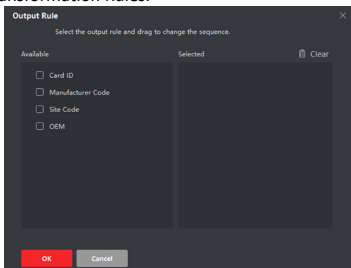


Figura 8-1 Impostazione delle regole di trasformazione dell'uscita

- 2) Selezionare la regole sull'elenco a sinistra.

Le regole selezionate verranno aggiunte all'elenco a destra.

- 3) **Opzionale:** trascinare le regole per modificarne l'ordine.

- 4) Fare clic su **OK**.

- 5) Nella schermata Custom Wiegand, impostare il bit di inizio, la lunghezza e la cifra decimale della regola.

7. Fare clic su **Save**.

8.5.4 Configurazione della modalità di autenticazione e di pianificazione del lettore di tessere

È possibile impostare le regole di passaggio per il lettore di tessere del dispositivo di controllo accessi in base alle proprie esigenze.

Passaggi

1. Fare clic su **Access Control → Advanced Function → Authentication** per accedere alla pagina di configurazione della modalità di autenticazione.
2. Selezionare un lettore di tessere a sinistra per configurarlo.
3. Impostare la modalità di autenticazione del lettore di tessere.
 - 1) Fare clic su **Configuration**.

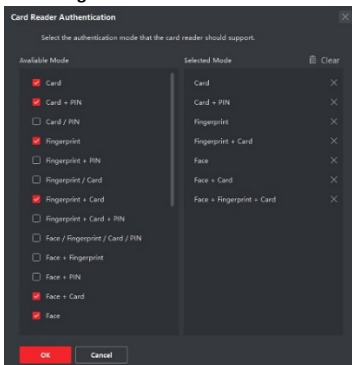


Figura 8-2 Selezione della modalità di autenticazione del lettore di tessere



Nota

Configurazione delle informazioni sul controllo degli accessi.

Il PIN si riferisce al codice PIN impostato per aprire la porta.
Consultare

2) Selezionare le modalità nell'elenco Available Mode e verranno aggiunte all'elenco delle modalità selezionate.

3) Fare clic su **OK**.

Una volta selezionate le modalità, queste saranno visualizzate come icone con colori diversi.

4. Fare clic sull'icona per selezionare una modalità di autenticazione del lettore di tessere e trascinare il cursore per tracciare una barra colorata sulla pianificazione, che indica il periodo di validità dell'autenticazione del lettore di tessere.

5. Ripetere la precedente operazione per definire altri periodi.

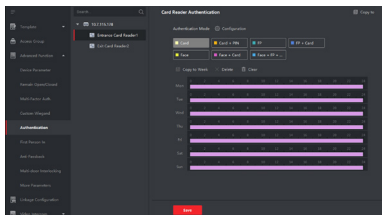


Figura 8-3 Impostazione delle modalità di autenticazione per i lettori di tessere

6. **Opzionale:** selezionare un giorno configurato e fare clic su **Copy to Week** per applicare le stesse impostazioni all'intera settimana.

7. **Opzionale:** fare clic su **Copy to** per copiare le impostazioni su altri lettori di tessere.

8. Fare clic su **Save**.

8.5.5 Configurazione dei parametri del dispositivo

Dopo aver aggiunto il dispositivo di controllo accessi, è possibile impostarne i parametri, come i parametri di rete.

Impostazione dei parametri di rete

Dopo aver aggiunto il dispositivo di controllo accessi, è possibile impostare la modalità di caricamento del registro del dispositivo e creare un account EHome tramite una rete cablata.

Impostazione della modalità di caricamento dei registri

È possibile impostare la modalità di caricamento dei registri per il dispositivo tramite il protocollo EHome.

Passaggi



Nota

Assicurarsi che il dispositivo non sia aggiunto da EHome.

1. Accedere al modulo Access Control.
 2. Sulla barra di navigazione a sinistra, accedere a **Advanced Function** → **More Parameters**.
 3. Selezionare un dispositivo di controllo accessi nell'elenco dei dispositivi e accedere a **Network** → **Uploading Mode**.
 4. Selezionare il gruppo centrale dall'elenco a discesa.
 5. Selezionare **Enable** per permettere l'impostazione della modalità di caricamento.
 6. Selezionare la modalità di caricamento dal menu a discesa.
 - Abilitare **N1** o **G1** per il canale principale e quello di backup.
 - Selezionare **Close** per disattivare il canale principale o quello di backup.
-



Nota

Il canale principale e quello di backup non possono attivare contemporaneamente N1 o G1.

7. Fare clic su **Save**

Creazione di account EHome in modalità di comunicazione cablata

È possibile impostare l'account per il protocollo Ehome nella modalità di comunicazione cablata. Sarà poi possibile aggiungere dispositivi tramite il protocollo EHome.

Passaggi



Nota

- Assicurarsi che il dispositivo non sia aggiunto da EHome.
 - Questa funzione deve essere supportata dal dispositivo.
-

1. Accedere al modulo Access Control.
 2. Sulla barra di navigazione a sinistra, accedere a **Advanced Function** → **More Parameters**.
 3. Selezionare un dispositivo di controllo accessi nell'elenco dei dispositivi e accedere a **Network** → **Network Center**.
 4. Selezionare il gruppo centrale dall'elenco a discesa.
 5. Impostare **Address Type** su **IP Address** o **Domain Name**.
 6. Immettere l'indirizzo IP o il nome di dominio in base al tipo di indirizzo.
 7. Immettere il numero di porta per il protocollo.
-



Nota

Il numero di porta della rete wireless e della rete cablata deve essere coerente con il numero di porta di EHome.

8. Impostare **Protocol Type** su **EHome**.
9. Impostare un nome account per il centro di rete.
10. Fare clic su **Save**.

Impostazione dello stato di presenza

È possibile impostare la modalità di presenza sul dispositivo tramite il client. È possibile anche impostare i parametri di presenza come check in, check out, inizio pausa, fine pausa, inizio straordinario e fine straordinario sul dispositivo, in base alle esigenze effettive.



Nota

Questa funzione deve essere supportata dal dispositivo.

Disattivazione della modalità di presenza

Disattivare la modalità di presenza e il sistema non mostrerà lo stato di presenza nella pagina iniziale del dispositivo.

Prima di iniziare

Aggiungere almeno una persona e impostarne la modalità di autenticazione. Per ulteriori informazioni, consultare **Gestione delle persone**.

Passaggi

1. Fare clic su **Access Control** → **Advanced Function** → **More Parameters** per accedere alla pagina More Parameters.
2. Selezionare un dispositivo dal pannello a sinistra.
3. Fare clic su **Attendance Status**.
4. Impostare la modalità di presenza su **Disable**.
5. Fare clic su **Save**.

Risultato

La funzione dello stato di presenza è disabilitata e non sarà possibile visualizzare o configurare lo stato di presenza nella pagina iniziale del dispositivo.

Impostazione della presenza manuale

Impostare la modalità di presenza come manuale e selezionare manualmente uno stato quando si registra la presenza sul dispositivo.

Prima di iniziare

Aggiungere almeno una persona e impostarne la modalità di autenticazione. Per ulteriori informazioni, consultare **Gestione delle persone**.

Passaggi

1. Fare clic su **Access Control** → **Advanced Function** → **More Parameters** per accedere alla pagina More Parameters.
2. Selezionare un dispositivo dal pannello a sinistra.
3. Fare clic su **Attendance Status**.
4. Impostare la modalità di presenza su **Manual**.
5. Assicurarsi che **Attendance Status Required** sia attivato.



Nota

Per impostazione predefinita, **Attendance Status Required** è attivato.

6. Impostare il tasto di scelta rapida dall'elenco a discesa per lo stato di presenza.

7. Fare clic su **Save**.

Risultato

Premere un tasto sulla tastiera del dispositivo per selezionare uno stato di presenza e autenticarsi. L'autenticazione verrà contrassegnata come lo stato di presenza configurato in base al tasto di scelta rapida definito.

Oppure, quando si esegue l'autenticazione sulla pagina iniziale del dispositivo, si accede alla pagina Select Status. Selezionare uno stato per registrare la presenza.



Nota

Se non si seleziona uno stato entro circa 20 secondi, l'autenticazione non verrà eseguita correttamente e non verrà contrassegnata come presenza valida.

Impostazione della presenza automatica

Impostare la modalità di presenza su automatica per impostare lo stato della presenza e il periodo di tempo disponibile. Il sistema modificherà automaticamente lo stato della presenza in base ai parametri configurati.

Prima di iniziare

Aggiungere almeno una persona e impostarne la modalità di autenticazione. Per ulteriori informazioni, consultare **Gestione delle persone**.

Passaggi

1. Fare clic su **Access Control** → **Advanced Function** → **More Parameters** per accedere alla pagina More Parameters.
 2. Selezionare un dispositivo dal pannello a sinistra.
 3. Fare clic su **Attendance Status**.
 4. Impostare la modalità di presenza su **Auto**.
 5. Assicurarsi che **Attendance Status Required** sia attivato.
-



Nota

Per impostazione predefinita, **Attendance Status Required** è attivato.

6. Impostare la durata disponibile per lo stato di presenza di destinazione.
 - 1) Spostare il cursore sull'ora di destinazione per visualizzare la casella di controllo per l'attivazione.
 - 2) Selezionare la casella di controllo e impostare la durata disponibile.
 - 3) Fare clic in un punto qualsiasi della pagina per confermare le impostazioni. L'ora configurata verrà visualizzata in bianco.
7. Impostare il tasto di scelta rapida dall'elenco a discesa per lo stato di presenza.
8. Fare clic su **Save**.

Lo stato di presenza sarà valido nell'ambito del periodo di tempo configurato.

Risultato

Accedere alla pagina iniziale del dispositivo; la modalità di presenza corrente sarà visualizzata sulla pagina. Quando si esegue l'autenticazione sulla pagina iniziale, l'autenticazione verrà contrassegnata come stato di presenza configurato in base all'ora configurata.

Esempio

Se si imposta il tasto Su come check-in e quello Giù come check-out e si imposta la pianificazione del check-in come lunedì alle 08:00 e quella del check-out come lunedì alle 17:00, l'autenticazione della persona valida prima delle 17:00 di lunedì verrà contrassegnata come check-in e quella dopo le 17:00 di lunedì sarà contrassegnata come check-out.

Impostazione della presenza manuale e automatica

Impostare la modalità di presenza come manuale e automatica e il sistema del dispositivo modificherà automaticamente lo stato della presenza in base ai parametri configurati. Allo stesso tempo, è possibile modificare manualmente lo stato della presenza prima dell'autenticazione.

Prima di iniziare

Aggiungere almeno una persona e impostarne la modalità di autenticazione. Per ulteriori informazioni, consultare **Gestione delle persone**.

Passaggi

1. Fare clic su **Access Control** → **Advanced Function** → **More Parameters** per accedere alla pagina More Parameters.
2. Selezionare un dispositivo dal pannello a sinistra.
3. Fare clic su **Attendance Status**.
4. Impostare la modalità di presenza su **Manual and Auto**.
5. Assicurarsi che **Attendance Status Required** sia attivato.



Nota

Per impostazione predefinita, **Attendance Status Required** è attivato.

6. Impostare la durata dell'ultimo stato.
7. Impostare la durata disponibile per lo stato di presenza di destinazione.
 - 1) Spostare il cursore sull'ora di destinazione per visualizzare la casella di controllo per l'attivazione.
 - 2) Selezionare la casella di controllo e impostare la durata disponibile.
 - 3) Fare clic in un punto qualsiasi della pagina per confermare le impostazioni. L'ora configurata verrà visualizzata in bianco.
8. Impostare il tasto di scelta rapida dall'elenco a discesa per lo stato di presenza.
9. Fare clic su **Save**.

Lo stato di presenza sarà valido nell'ambito del periodo di tempo configurato.

Risultato

Accedere alla pagina iniziale del dispositivo; la modalità di presenza corrente sarà visualizzata sulla pagina. Se non si seleziona uno stato, l'autenticazione verrà contrassegnata come stato di presenza configurato in base all'ora configurata. Se si preme il tasto sulla tastiera e si seleziona uno stato per registrare la presenza, l'autenticazione verrà contrassegnata come lo stato di presenza selezionato.

Esempio

Se si imposta il tasto Su come check-in e il tasto Giù come check-out e si imposta l'ora del check-in come lunedì alle 08:00 e l'ora del check-out come lunedì alle 17:00, l'autenticazione della persona valida prima delle 17:00 di lunedì verrà contrassegnata come check-in e quella dopo le 17:00 di lunedì sarà contrassegnata come check-out.

8.6 Configurazione delle azioni di collegamento per il controllo accessi

È possibile configurare diverse azioni di collegamento per l'evento rilevato dal dispositivo di controllo accessi.

Successivamente, le azioni di collegamento vengono attivate al verificarsi dell'evento. Questo meccanismo viene utilizzato per informare il personale di sicurezza dell'evento o per attivare il controllo automatico degli accessi in tempo reale.

Sono supportati due tipi di azioni di collegamento:

- **Azioni del client:** al rilevamento dell'evento, si attiveranno le azioni sul client, ad esempio il client che emette un avviso acustico.
- **Azioni del dispositivo:** a rilevamento dell'evento, si attiveranno le azioni di un dispositivo specifico, ad esempio l'avvisatore acustico di un lettore di tessere e l'apertura/chiusura di una porta.

8.6.1 Configurazione delle azioni del client per gli eventi di accesso

È possibile assegnare azioni di collegamento del client a un evento definendo una regola. Ad esempio, quando viene rilevato un evento, viene emesso un avviso acustico diretto al personale addetto alla sicurezza.

Passaggi



Nota

Le azioni di collegamento qui riportate si riferiscono al collegamento delle azioni del software client, quali avvisi acustici, collegamenti e-mail, ecc.

1. Fare clic su **Event Management** → **Access Control Event**.

I dispositivi di controllo accessi aggiunti verranno visualizzati nell'elenco dei dispositivi.

2. Selezionare una risorsa dall'elenco dei dispositivi.

Verranno visualizzati i tipi di evento supportati dalla risorsa selezionata.

3. Selezionare uno o più eventi e fare clic su **Edit Priority** per definire la priorità per tali eventi, utilizzabile per filtrare gli eventi nel modulo Event Center.
4. Impostare le azioni di collegamento dell'evento.
 - 1) Selezionare gli eventi e fare clic su **Edit Linkage** per impostare le azioni del client in caso di attivazione degli eventi.

Audible Warning

Il software client emette un avviso acustico all'attivazione dell'allarme. È possibile selezionare la suoneria di allarme per l'avviso acustico.



Nota

Per impostare la suoneria di allarme, consultare la sezione *Impostazione della suoneria di allarme* nel manuale dell'utente del software client.

Email Linkage

Consente di inviare un'e-mail di notifica contenente informazioni sull'allarme a uno o più destinatari.

- 2) Fare clic su **OK**.
5. Abilitare l'evento in modo che quando viene rilevato venga inviato al client e si attivino le azioni di collegamento.
6. **Opzionale:** fare clic su **Copy to...** per copiare le impostazioni dell'evento su un altro dispositivo di controllo accessi, ingresso di allarme, porta o lettore di tessere.

8.6.2 Configurazione delle azioni del dispositivo per gli eventi di accesso

È possibile impostare le azioni di collegamento del dispositivo di controllo accessi per gli eventi attivati dal dispositivo di controllo accessi. Successivamente, all'attivarsi di un evento, possono attivarsi l'uscita di allarme, l'avvisatore acustico sul controller di accesso e altre azioni.

Passaggi



Nota

Le azioni di collegamento devono essere supportate dal dispositivo.

1. Fare clic su **Access Control → Linkage Configuration**.
2. Selezionare il dispositivo di controllo accessi dall'elenco a sinistra.
3. Fare clic su **Add** per aggiungere un nuovo collegamento.
4. Selezionare **Event Linkage** come sorgente dell'evento.
5. Selezionare il tipo di evento e l'evento dettagliato per impostare il collegamento.
6. Nell'area Linkage Target, impostare la proprietà di destinazione per abilitare questa azione.

Buzzer on Controller

L'avviso acustico del dispositivo di controllo accessi verrà attivato.

Capture

Quando si verifica l'evento selezionato, viene acquisita un'immagine relativa all'evento.

Recording

Quando si verifica l'evento selezionato, viene acquisita un'immagine relativa all'evento.



Nota

Il dispositivo deve supportare la registrazione.

Buzzer on Reader

L'avviso acustico del lettore di tessere verrà attivato.

Alarm Output

L'uscita di allarme verrà attivata per la notifica al verificarsi dell'evento selezionato.

Alarm Input

Attivare o disattivare l'ingresso di allarme.



Nota

Il dispositivo deve supportare la funzione di ingresso allarme.

Access Point

Verranno attivati i possibili stati della porta (aperta, chiusa, resta aperta, resta chiusa).



Nota

La porta di destinazione e quella di origine non possono coincidere.

Audio Play

Verrà attivato il messaggio audio. Il contenuto audio relativo all'indice audio selezionato verrà riprodotto in base alla modalità di riproduzione configurata.

7. Fare clic su **Save**.

8. **Opzionale:** una volta aggiunto il collegamento del dispositivo, è possibile eseguire una delle seguenti operazioni:

Modifica delle impostazioni di collegamento Selezionare le impostazioni di collegamento configurate nell'elenco dei dispositivi e modificare i parametri di origine degli eventi, tra cui la sorgente dell'evento e la destinazione di collegamento.

Eliminazione delle impostazioni di collegamento Selezionare le impostazioni di collegamento configurate nell'elenco dei dispositivi e fare clic su **Delete** per eliminarle.

8.6.3 Configurazione delle azioni del dispositivo per il passaggio della tessera

È possibile abilitare le azioni di collegamento del dispositivo di controllo accessi (ad esempio disattivando una zona e attivando un messaggio audio) per il passaggio di una tessera specifica. In questo modo, è possibile monitorare i comportamenti e la posizione del titolare della tessera.

Passaggi

Questa funzione deve essere supportata dal dispositivo.



Nota

1. Fare clic su **Access Control** → **Linkage Configuration**.
2. Selezionare il dispositivo di controllo accessi dall'elenco a sinistra.
3. Fare clic su **Add** per aggiungere un nuovo collegamento.
4. Selezionare **Card Linkage** come sorgente dell'evento.
5. Immettere il numero della tessera o selezionare la tessera dall'elenco a discesa.
6. Selezionare il lettore di tessere in cui passare la tessera.
7. Nell'area Linkage Target, impostare la proprietà di destinazione per abilitare questa azione.

Buzzer on Controller

L'avviso acustico del dispositivo di controllo accessi verrà attivato.

Buzzer on Reader

L'avviso acustico del lettore di tessere verrà attivato.

Capture

Quando si verifica l'evento selezionato, viene acquisita un'immagine relativa all'evento.

Recording

Quando si verifica l'evento selezionato, viene acquisita un'immagine relativa all'evento.



Nota

Il dispositivo deve supportare la registrazione.

Alarm Output

L'uscita di allarme verrà attivata per le notifiche.

Alarm Input

Attivare o disattivare la funzione di ingresso allarme.



Nota

Il dispositivo deve supportare l'ingresso di allarme.

Access Point

Verranno attivati i possibili stati della porta (aperta, chiusa, resta aperta, resta chiusa).

Audio Play

Verrà attivato il messaggio audio. Il contenuto audio relativo all'indice audio selezionato verrà riprodotto in base alla modalità di riproduzione configurata.

8. Fare clic su **Save**.

Quando la tessera (configurata nel passaggio 5) viene passata sul lettore di tessere (configurato nel passaggio 6), può attivare le azioni collegate (configurate nel passaggio 7).

9. **Opzionale**: una volta aggiunto il collegamento del dispositivo, è possibile eseguire una delle seguenti operazioni:

Eliminazione delle impostazioni di collegamento Selezionare le impostazioni di collegamento configurate nell'elenco dei dispositivi e fare clic su **Delete** per eliminarle.

Modifica delle impostazioni di collegamento Selezionare le impostazioni di collegamento configurate nell'elenco dei dispositivi e modificare i parametri di origine degli eventi, tra cui la sorgente dell'evento e la destinazione di collegamento.

8.6.4 Configurazione delle azioni del dispositivo per ID della persona

È possibile impostare le azioni di collegamento del dispositivo di controllo accessi per l'ID della persona specificata. Quando il dispositivo di controllo accessi rileva l'ID della persona specificata, può attivare l'uscita di allarme, l'avvisatore acustico sul lettore di tessere e altre azioni, in modo da implementare un monitoraggio speciale della persona specificata.

Passaggi

Questa funzione deve essere supportata dal dispositivo.



Nota

1. Fare clic su **Access Control** → **Linkage Configuration**.
2. Selezionare il dispositivo di controllo accessi dall'elenco a sinistra.
3. Fare clic su **Add** per aggiungere un nuovo collegamento.
4. Selezionare **Person Linkage** come sorgente dell'evento.
5. Immettere il numero del dipendente o selezionare la persona dall'elenco a discesa.
6. Selezionare il lettore di tessere in cui passare la tessera.
7. Nell'area Linkage Target, impostare la proprietà di destinazione per abilitare questa azione.

Buzzer on Controller

L'avviso acustico del dispositivo di controllo accessi verrà attivato.

Buzzer on Reader

L'avviso acustico del lettore di tessere verrà attivato.

Capture

Quando si verifica l'evento selezionato, viene acquisita un'immagine relativa all'evento.

Recording

Quando si verifica l'evento selezionato, viene acquisita un'immagine relativa all'evento.



Nota

Il dispositivo deve supportare la registrazione.

Alarm Output

L'uscita di allarme verrà attivata per le notifiche.

Alarm Input

Attivare o disattivare l'ingresso di allarme.



Nota

Il dispositivo deve supportare la funzione di ingresso allarme.

Access Point

Verranno attivati i possibili stati della porta (aperta, chiusa, resta aperta, resta chiusa).

Audio Play

Verrà attivato il messaggio audio. Il contenuto audio relativo all'indice audio selezionato verrà riprodotto in base alla modalità di riproduzione configurata.

8. Fare clic su **Save**.

9. **Opzionale:** una volta aggiunto il collegamento del dispositivo, è possibile eseguire una delle seguenti operazioni:

Eliminazione delle impostazioni di collegamento Selezionare le impostazioni di collegamento configurate nell'elenco dei dispositivi e fare clic su **Delete** per eliminarle.

Modifica delle impostazioni di collegamento Selezionare le impostazioni di collegamento configurate nell'elenco dei dispositivi e modificare i parametri di origine degli eventi, tra cui la sorgente dell'evento e la destinazione di collegamento.

8.7 Controllo delle porte

Nel modulo Monitoring, è possibile visualizzare in tempo reale lo stato delle porte gestite dal dispositivo di controllo accessi aggiunto. È inoltre possibile controllare le porte tramite il client da remoto per aprirle/chiuderle o farle restare aperte/chiuso. Gli eventi di accesso in tempo reale vengono visualizzati in questo modulo. È possibile visualizzare i dettagli di accesso e quelli della persona.



Nota

L'utente con l'autorizzazione per il controllo delle porte potrà accedere al modulo Monitoring e controllare le porte. Oppure le icone utilizzate per il controllo non saranno visualizzate. Per impostare l'autorizzazione dell'utente, consultare la sezione **Gestione delle persone**.

8.7.1 Controllo dello stato della porta

È possibile controllare lo stato di una singola porta (aperta, chiusa, resta aperta, resta chiusa).

Passaggi

1. Fare clic su **Monitoring** per accedere alla pagina del modulo di monitoraggio.
2. Selezionare un gruppo di punti di accesso nell'angolo in alto a destra.



Nota

Per la gestione del gruppo di punti di accesso, consultare la sezione *Gestione di gruppi* nel manuale dell'utente del software client.

Saranno visualizzate le porte nel gruppo di controllo accessi selezionato.

3. Fare clic sull'icona di una porta per selezionarla oppure premere **Ctrl** per selezionare più porte.
4. Fare clic sui seguenti pulsanti per controllare la porta.

Open Door

Se la porta è bloccata, verrà sbloccata e si aprirà una sola volta. Al termine della durata di apertura, la porta si chiuderà e si bloccherà di nuovo automaticamente.

Close Door

Se la porta è sbloccata, verrà bloccata e sarà chiusa. La persona con autorizzazione di accesso può attraversare la porta con le proprie credenziali.

Remain Open

La porta è sempre sbloccata (indipendentemente dallo stato di apertura o chiusura). Tutte le persone possono attraversare la porta, senza bisogno di credenziali.

Remain Closed

La porta sarà sempre chiusa e bloccata. Nessuno può attraversare la porta, anche se in possesso di credenziali autorizzate, ad eccezione degli utenti con privilegi avanzati.

Capture

Consente di acquisire una foto manualmente.



Nota

Il pulsante **Capture** è disponibile quando il dispositivo supporta la funzione di acquisizione. L'immagine viene salvata nel PC su cui è in esecuzione il client. Per impostare il percorso di salvataggio, fare riferimento a *Impostazione del percorso di salvataggio dei file* nel manuale dell'utente del software client.

Risultato

Se l'operazione viene eseguita correttamente, l'icona delle porte cambia in tempo reale in base all'operazione.

8.7.2 Controllo dei record di accesso in tempo reale

I record di accesso verranno visualizzati in tempo reale, inclusi i record di passaggio delle tessere, i record di confronto delle impronte digitali, ecc. È possibile visualizzare le informazioni sulla persona e l'immagine acquisita durante l'accesso.

Passaggi

1. Fare clic su **Monitoring** e selezionare un gruppo dall'elenco a discesa nell'angolo in alto a destra.

I record di accesso attivati presso le porte del gruppo selezionato verranno visualizzati in tempo reale. È possibile visualizzare i dettagli dei record, quali numero di tessera, nome del titolare, organizzazione, orario dell'evento, ecc.

2. **Opzionale:** selezionare il tipo e lo stato degli eventi in modo che questi eventi vengano visualizzati nell'elenco se rilevati. I tipi e gli stati degli eventi non selezionati non verranno visualizzati nell'elenco.

3. **Opzionale:** selezionare **Show Latest Event** e il record di accesso più recente verrà selezionato e visualizzato nella parte superiore dell'elenco dei record.

4. **Opzionale:** fare clic sull'evento per visualizzare i dettagli della persona che ha effettuato l'accesso, tra cui le foto della persona (foto acquisita e profilo), il numero e il nome della persona, l'organizzazione, il telefono, l'indirizzo di contatto, ecc.



Nota

È possibile fare doppio clic sull'immagine acquisita per ingrandirla e visualizzarne i dettagli.

5. **Opzionale:** fare clic con il pulsante destro del mouse sul nome della tabella degli eventi di accesso per mostrare o nascondere la colonna in base alle esigenze.

8.8 Modulo Event Center

Nel modulo Event Center è possibile visualizzare gli eventi in tempo reale, cercare nella cronologia degli eventi e consultare le informazioni sugli allarmi.


Prima che il client possa ricevere le informazioni sugli eventi dal dispositivo, è necessario innanzitutto attivare il dispositivo stesso. Per i dettagli, consultare la sezione **Attivazione della ricezione di notifiche degli eventi dai dispositivi**.

Prima di poter visualizzare le informazioni sugli allarmi, è necessario attivare l'immagine a comparsa di allarme attivato in Event Center. Per i dettagli, consultare la sezione .

8.8.1 Attivazione della ricezione di notifiche degli eventi dai dispositivi

Prima che il software client possa ricevere notifiche degli eventi dal dispositivo, è necessario innanzitutto attivare il dispositivo stesso.

Passaggi

1. Fare clic su  → **Tool** → **Device Arming Control** per aprire la pagina Device Arming Control.

Tutti i dispositivi aggiunti saranno visualizzati in questa pagina.

2. Nella colonna Auto-Arming, attivare l'interruttore per abilitare l'attivazione automatica.

Dopodiché i dispositivi saranno attivi. E le notifiche sugli eventi attivati dai dispositivi attivi verranno inviate automaticamente al software client in tempo reale.

8.8.2 Visualizzazione degli eventi in tempo reale

Nel modulo Real-time Event della pagina Event Center, è possibile visualizzare le informazioni in tempo reale sugli eventi, tra cui la sorgente, l'ora dell'evento, la priorità, le parole chiave dell'evento, ecc.

Prima di iniziare

Abilitare la ricezione di eventi dai dispositivi prima che il client possa ricevere informazioni sugli eventi dal dispositivo; per i dettagli, vedere **Attivazione della ricezione di notifiche degli eventi dai dispositivi**.

Passaggi

1. Fare clic su **Event Center** → **Real-time Event** per accedere alla pagina degli eventi in tempo reale e visualizzare gli eventi in tempo reale ricevuti dal client.

Event Time

Per il dispositivo video, l'ora dell'evento è l'ora del client quando riceve l'evento. Per i dispositivi senza video, l'ora dell'evento è l'ora in cui l'evento viene attivato.

Priority

Il grado di urgenza dell'evento.

2. Filtrare gli eventi.

Filtrare per tipo di dispositivo e (o) priorità Selezionare i tipi di dispositivi e (o) le priorità per filtrare gli eventi.

Filtrare per parole chiave Immettere le parole chiave per filtrare gli eventi.

3. **Opzionale:** fare clic con il pulsante destro del mouse sull'intestazione della tabella dell'elenco degli eventi per personalizzare gli elementi correlati agli eventi da visualizzare nell'elenco.

4. Visualizzare i dettagli dell'evento.

1) Selezionare un evento dal relativo elenco.

2) Fare clic su **Expand** nell'angolo in basso a destra della pagina.

3) Visualizzare l'immagine correlata, la descrizione dettagliata e i record di gestione dell'evento.

4) **Opzionale:** spostare il cursore sulla relativa immagine, quindi fare clic sull'icona di download nell'angolo in alto a destra dell'immagine per scaricarla sul PC locale. È possibile impostare manualmente il percorso di salvataggio.

5. Opzionale: se necessario, effettuare le seguenti operazioni.

Gestione di un singolo evento

Fare clic su **Handle** per immettere il suggerimento sull'elaborazione, quindi fare clic su **Commit**.



Nota

Dopo la gestione di un evento, il pulsante **Handle** diventa **Add Remark**. Fare clic su **Add Remark** per aggiungere altri commenti a questo evento gestito.

Gestione degli eventi in batch

Selezionare gli eventi da elaborare, quindi fare clic su **Handle in Batch**. Immettere il suggerimento sull'elaborazione, quindi fare clic su **Commit**.

Attivazione/Disattivazione dell'audio degli allarmi

Fare clic su **Enable Audio/Disable Audio** per attivare/disattivare l'audio dell'evento.

Selezione automatica dell'evento più recente

Selezionare **Auto-Select Latest Event** per selezionare automaticamente l'evento più recente e visualizzarne le informazioni dettagliate.

Cancellazione di eventi

Fare clic su **Clear** per cancellare tutti gli eventi nell'elenco degli eventi.

Invio di e-mail

Selezionare un evento, quindi fare clic su **Send Email** e i dettagli dell'evento verranno inviati tramite e-mail.



Nota

È necessario configurare prima i parametri delle e-mail, vedere per ulteriori informazioni.

8.8.3 Ricerca di eventi nella cronologia

Nel modulo Event Search della pagina Event Center, è possibile cercare gli eventi nella cronologia in base all'ora, al tipo di dispositivo e ad altre condizioni in base al tipo di dispositivo specificato, quindi elaborarli.

Prima di iniziare

Abilitare la ricezione di eventi dai dispositivi prima che il client possa ricevere informazioni sugli eventi dal dispositivo; per i dettagli, vedere **Attivazione della ricezione di notifiche degli eventi dai dispositivi**.

Passaggi

1. Fare clic su **Event Center** → **Event Search** per accedere alla pagina di ricerca degli eventi.

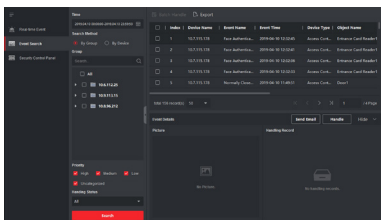


Figura 8-4 Ricerca di eventi nella cronologia

2. Impostare le condizioni di filtro per visualizzare solo determinati eventi.

Time

L'ora del client quando inizia l'evento.

È possibile fare ricerche in base ai seguenti parametri:

Group: cercare gli eventi che si sono verificati sulle risorse del gruppo selezionato.

Device: cercare gli eventi che si sono verificati sul dispositivo selezionato.

Device Type

Il tipo di dispositivo sul quale si è verificato l'evento.

All

Consente di selezionare tutti i tipi di dispositivi. Inoltre, è possibile impostare le seguenti condizioni di filtro: gruppo, priorità e stato.

Video Intercom

Per gli eventi del videocitofono, è necessario selezionare l'ambito di ricerca: All Records e Only Unlocking.

All Records: è possibile applicare il filtro su tutti gli eventi di videocitofono ed è necessario impostare le seguenti condizioni di filtro: dispositivo, priorità, stato.

Only Unlocking: è possibile applicare il filtro su tutti gli eventi di sblocco di videocitofono ed è necessario impostare le seguenti condizioni di filtro: dispositivo, tipo di sblocco.

Controllo degli accessi

Per gli eventi di controllo degli accessi, è possibile impostare le seguenti condizioni di filtro: dispositivo, priorità, stato, tipo di evento, tipo di lettore di tessere, nome della persona, numero di tessera, organizzazione.



Nota

Fare clic su **Show More** per impostare il tipo di evento, il tipo di lettore di tessere, il nome della persona, il numero di tessera, l'organizzazione.

Group

Il gruppo del dispositivo sul quale si è verificato l'evento. È necessario impostare il gruppo come condizione solo quando si seleziona Device Type su **All**.

Device

Il dispositivo sul quale si è verificato l'evento.

Priority

La priorità, che può essere bassa, media, alta e non categorizzata, indica il livello di urgenza dell'evento.

Status

Lo stato di gestione dell'evento.

3. Fare clic su **Search** per cercare gli eventi in base alle condizioni impostate.
4. **Opzionale:** fare clic con il pulsante destro del mouse sull'intestazione della tabella dell'elenco degli eventi per personalizzare gli elementi correlati agli eventi da visualizzare nell'elenco.

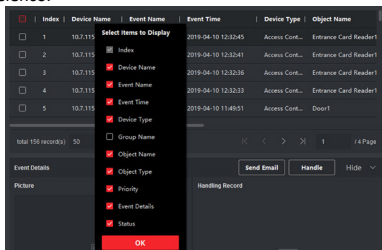


Figura 8-5 Personalizzazione delle voci relative agli eventi da visualizzare

5. **Opzionale:** eseguire una delle seguenti operazioni.

Gestione di un singolo evento Gestire un singolo evento: selezionare un evento da elaborare, quindi fare clic su **Handle** nella pagina dei dettagli dell'evento e immettere il suggerimento sull'elaborazione.



Nota

Dopo la gestione di un evento, il pulsante **Handle** diventa **Add Remark**. Fare clic su **Add Remark** per aggiungere altri commenti a questo evento gestito.

Gestione di eventi in batch Gestire gli eventi in batch: selezionare gli eventi da elaborare, quindi fare clic su **Handle in Batch** e immettere il suggerimento sull'elaborazione.

Dopo la gestione di un evento, il pulsante **Handle** diventa **Add Remark**. Fare clic su **Add Remark** per aggiungere altri commenti a questo evento gestito.

Invio di e-mail Selezionare un evento, quindi fare clic su **Send Email** e i dettagli dell'evento verranno inviati tramite e-mail.



Nota

È necessario configurare prima i parametri delle e-mail, vedere per ulteriori informazioni.

Esportazione delle informazioni sull'evento Download dell'immagine relativa all'evento Fare clic su **Export** per esportare il registro o le immagini degli eventi sul PC locale in formato CSV. È possibile impostare manualmente il percorso di salvataggio. Spostare il cursore sulla relativa immagine, quindi fare clic sull'icona di download nell'angolo in alto a destra dell'immagine per scaricarla sul PC locale. È possibile impostare manualmente il percorso di salvataggio.

8.9 Orari e presenze

Il modulo Time and Attendance offre più funzionalità per tracciare e monitorare gli orari in cui i dipendenti iniziano e finiscono di lavorare, nonché il controllo completo degli orari di lavoro dei dipendenti, come gli arrivi in ritardo, le uscite anticipate, la durata delle pause e le assenze.



Nota

In questa sezione, sono presenti le configurazioni necessarie per ottenere i report delle presenze. I record di accesso registrati dopo queste configurazioni verranno calcolati nelle statistiche.

8.9.1 Configurazione dei parametri di presenza

È possibile configurare i parametri di presenza, come la regola generale, i parametri per gli straordinari, i checkpoint delle presenze, le ferie, il tipo di permesso o congedo, ecc.

Configurazione della regola generale

È possibile configurare la regola generale per il calcolo delle presenze, ad esempio l'inizio della settimana, l'inizio del mese, la fine settimana, le assenze, ecc.

Passaggi



Nota

I parametri configurati qui saranno impostati come predefiniti per ogni nuovo periodo di tempo aggiunto. Non influiranno su quelli già esistenti.

1. Accedere al modulo Time & Attendance.
2. Fare clic su **Attendance Settings → General Rule**.
3. Impostare il giorno come inizio della settimana e la data come inizio del mese.
4. Selezionare i giorni come fine settimana.
5. Impostare i parametri per le assenze.
6. Fare clic su **Save**.

Configurazione dei parametri per gli straordinari

È possibile configurare i parametri per gli straordinari nei giorni lavorativi e non, tra cui il livello degli straordinari, il tasso salariale, lo stato di presenza per gli straordinari, ecc.

Passaggi

1. Accedere al modulo Time & Attendance.
2. Fare clic su **Attendance Settings → Overtime**.

3. Impostare le informazioni necessarie.

Livelli di straordinario per i giorni lavorativi

Quando si lavora per un determinato periodo di tempo dopo l'orario lavorativo in un giorno feriale, si raggiunge un livello diverso di straordinari: livello di straordinario 1, livello di straordinario 2 e livello di straordinario 3. È possibile impostare un tasso salariale diverso per i tre livelli di straordinario.

Tasso salariale

Impostare i tassi salariali corrispondenti per i tre livelli di straordinario, generalmente utilizzati per calcolare le ore di lavoro totali.

Regola degli straordinari per i giorni non lavorativi

È possibile abilitare la regola degli straordinari per i giorni non lavorativi e impostare la modalità di calcolo.

4. Fare clic su **Save**.

Configurazione di checkpoint delle presenze

È possibile definire i lettori di tessere di un punto di accessi come checkpoint delle presenze, in modo che l'autenticazione sui lettori di tessere sarà registrata per le presenze.

Prima di iniziare

È necessario aggiungere un dispositivo di controllo accessi prima di configurare il checkpoint delle presenze. Per i dettagli, consultare la sezione **Aggiunta di un dispositivo**.

Passaggi



Nota

Per impostazione predefinita, tutti i lettori di tessere dei dispositivi di controllo accessi aggiunti sono impostati come checkpoint delle presenze. **1.** Accedere al modulo Time & Attendance.

2. Fare clic su **Attendance Settings** → **Attendance Check Point** per accedere alla pagina Attendance Check Point Settings.

3. Opzionale: disattivare l'interruttore di **Set All Card Readers as Check Points**.

Solo i lettori di tessere inseriti in elenco saranno utilizzati come checkpoint delle presenze.

4. Selezionare i lettori di tessere desiderati nell'elenco dei dispositivi come checkpoint delle presenze.

5. Impostare la funzione checkpoint su **Start/End-Work**, **Start-Work** o **End-Work**.

6. Fare clic su **Set as Check Point**.

Il checkpoint delle presenze configurato viene visualizzato nell'elenco a destra.

Configurazione delle festività

È possibile aggiungere le festività, ossia i periodi durante i quali il check-in o il check-out non vengono registrati.

Aggiunta di festività fisse

È possibile configurare le festività che si verificano ogni anno in giorni fissi durante il periodo di validità, come Capodanno, Festa della Repubblica, Natale, ecc.

Passaggi


1. Accedere al modulo Time & Attendance.
2. Fare clic su **Attendance Settings** → **Holiday** per accedere alla pagina Holiday Settings.
3. Selezionare **Regular Holiday** come tipo di festività.
4. Scegliere un nome personalizzato per la festività.
5. Impostare il primo giorno festivo.
6. Immettere il numero di giorni festivi.
7. Impostare lo stato di presenza se il dipendente lavora in un giorno festivo.
8. **Opzionale:** selezionare **Repeat Annually** per rendere questa impostazione per le festività valida ogni anno.
9. Fare clic su **OK**.

Le festività aggiunte saranno visualizzate nell'elenco delle festività e nel calendario.

Se una stessa data viene scelta per festività diverse, verrà registrata con la prima festività aggiunta.

10. **Opzionale:** dopo aver aggiunto le festività, eseguire una delle seguenti operazioni.

Modifica delle festività

Fare clic su  per modificare le informazioni relative alle festività.

Eliminazione delle festività

Selezionare una o più delle festività aggiunte e fare clic su **Delete** per eliminare le festività dall'elenco delle festività.

Aggiunta di festività non fisse

È possibile configurare una festività valida ogni anno in giorni non fissi durante il periodo di validità, come il giorno di Pasqua.

Passaggi

1. Accedere al modulo Time & Attendance.
2. Fare clic su **Attendance Settings** → **Holiday** per accedere alla pagina Holiday Settings.
3. Fare clic su **Add** per aprire la pagina Add Holiday.
4. Selezionare **Irregular Holiday** come tipo di festività.
5. Scegliere un nome personalizzato per la festività.
6. Impostare la data di inizio delle festività.

Esempio

Se si desidera impostare il quarto giovedì di novembre 2019 come giorno del Ringraziamento, è necessario selezionare 4, novembre, 2019 e giovedì dai quattro elenchi a discesa.

7. Immettere il numero di giorni festivi.


8. Impostare lo stato di presenza se il dipendente lavora in un giorno festivo.
9. **Opzionale:** selezionare **Repeat Annually** per rendere questa impostazione per le festività valida ogni anno.
10. Fare clic su **OK**.

Le festività aggiunte saranno visualizzate nell'elenco delle festività e nel calendario.

Se una stessa data viene scelta per festività diverse, verrà registrata con la prima festività aggiunta.

11. **Opzionale:** dopo aver aggiunto le festività, eseguire una delle seguenti operazioni.

Modifica delle festività

Fare clic su  per modificare le informazioni relative alle festività.

Eliminazione delle festività


Selezionare una o più delle festività aggiunte e fare clic su **Delete** per eliminare le festività dall'elenco delle festività.

Configurazione del tipo di permesso o congedo

È possibile personalizzare il tipo di permesso o congedo (tipo di permesso o congedo maggiore o minore) in base alle esigenze. È anche possibile modificare o eliminare i tipi di permessi o congedi.

Passaggi


1. Accedere al modulo Time & Attendance.
2. Fare clic su **Attendance Settings** → **Leave Type** per accedere alla pagina Leave Type Settings.
3. Fare clic su **Add** a sinistra per aggiungere un tipo di permesso o congedo maggiore.
4. **Opzionale:** effettuare una delle seguenti attività per il tipo di permesso o congedo maggiore.

Edit Spostare il cursore sul tipo di permesso o congedo maggiore e fare clic su  per modificarlo.

Delete Selezionare un tipo di permesso o congedo maggiore e fare clic su **Delete** a sinistra per eliminarlo.

5. Fare clic su **Add** a destra per aggiungere un tipo di permesso o congedo minore.

6. **Opzionale:** effettuare una delle seguenti attività per il tipo di permesso o congedo minore.

Edit Spostare il cursore sul tipo di permesso o congedo minore e fare clic su  per modificarlo.

Delete Selezionare uno o più tipi di permessi o congedi maggiori e fare clic su **Delete** a destra per eliminare i tipi selezionati.

Sincronizzazione del record di autenticazione su database di terze parti

I dati relativi alle presenze registrati nel software client possono essere utilizzati da altri sistemi per il calcolo o altre operazioni. È possibile abilitare la funzione di sincronizzazione per applicare automaticamente il record di autenticazione dal software client al database di terze parti.

Passaggi

1. Accedere al modulo Time & Attendance.
2. Fare clic su **Attendance Settings → Third-Party Database**.
3. Attivare l'interruttore di **Apply to Database** per abilitare la funzione di sincronizzazione.
4. Impostare i parametri richiesti per il database di terze parti, come il tipo di database, l'indirizzo IP del server, il nome del database, il nome utente e la password.
5. Impostare i parametri della tabella del database in base alle configurazioni effettive.
 - 1) Immettere il nome della tabella del database di terze parti.
 - 2) Impostare i campi della tabella mappata tra il software client e il database di terze parti.
6. Fare clic su **Connection Test** per verificare se il database può essere collegato.
7. Fare clic su **Save** per salvare le impostazioni.

I dati relativi alle presenze verranno scritti sul database di terze parti.

Configurazione dei tempi di pausa

È possibile aggiungere il tempo di pausa e impostare l'ora di inizio, l'ora di fine, la durata, la modalità di calcolo e altri parametri per la pausa. Il tempo di pausa aggiunto può essere modificato o eliminato.

Passaggi

1. Fare clic su **Time & Attendance → Timetable**.

Le tabelle degli orari aggiunti saranno visualizzate nell'elenco.
2. Selezionare una delle tabelle di orari aggiunte o fare clic su **Add** per accedere alla pagina di impostazione di tali tabelle.
3. Fare clic su **Settings** nell'area dei tempi di pausa per accedere alla pagina di gestione dei tempi di pausa.
4. Aggiungere un tempo di pausa.
 - 1) Fare clic su **Add**.
 - 2) Immettere un nome che descriva il tempo di pausa.
 - 3) Impostare i parametri correlati al tempo di pausa.

Start Time / End Time

Impostare l'ora di inizio e fine della pausa.

No Earlier Than / No Later Than

Impostare la prima ora del passaggio della tessera per iniziare la pausa e l'ultima ora possibile del passaggio per interrompere la pausa.

Break Duration

La durata della pausa dall'ora di inizio all'ora di fine.

Calcolo

Auto Deduct

La durata fissa della pausa sarà esclusa dalle ore di lavoro.

Must Check

La durata della pausa verrà calcolata ed esclusa dall'orario di lavoro in base all'orario effettivo di check-in e check-out.



Nota

Se si seleziona **Must Check** come metodo di calcolo, è necessario impostare lo stato di presenza per un rientro tardivo o anticipato dalla pausa.

5. Fare clic su **Save** per salvare le impostazioni.
6. **Opzionale:** fare clic su **Add** per continuare ad aggiungere tempi di pausa.

Configurazione della visualizzazione dei report

È possibile configurare i contenuti visualizzati nel report delle presenze, ad esempio il nome dell'azienda, il logo, il formato della data, il formato dell'ora e il contrassegno.

Passaggi

1. Accedere al modulo Time & Attendance.
2. Fare clic su **Attendance Statistics** → **Report Display**.
3. Configurare le impostazioni di visualizzazione per il report delle presenze.

Company Name

Immettere il nome dell'azienda per visualizzarlo nel report.

Date Format / Time Format

Impostare il formato della data e dell'ora in base alle esigenze.

Attendance Status Mark in Report

Immettere il contrassegno e selezionare il colore. I campi relativi allo stato di presenza nel report vengono visualizzati con il contrassegno e il colore.

Weekend Mark in Report

Immettere il contrassegno e selezionare il colore. I campi del fine settimana nel report vengono visualizzati con il contrassegno e il colore.

4. Fare clic su **Save**.

8.9.2 Aggiunta di tabelle di orari

È possibile aggiungere la tabella di orari alla pianificazione dei turni.

Passaggi

1. Fare clic su **Time & Attendance** → **Timetable** per accedere alla finestra delle impostazioni delle tabelle di orari.

2. Fare clic su **Add** per accedere alla pagina Add Timetable.
3. Creare un nome per la tabella di orari.
4. Selezionare il metodo di calcolo.

First In & Last Out

L'orario del primo check-in viene registrato come ora di inizio del lavoro e l'orario dell'ultimo check-out viene registrato come ora di fine del lavoro.

Each Check-In/Out

Ogni orario di check-in e check-out è valido e la somma di tutti i periodi compresi tra ciascun check-in e il relativo check-out verrà registrata come durata di lavoro valida.

È necessario impostare **Valid Auth. Interval** per questo metodo di calcolo. Ad esempio, se l'intervallo di tempo tra due passaggi della stessa tessera è al di sotto del valore impostato, il passaggio non è valido.

5. **Opzionale:** attivare l'interruttore di **Enable T&A Status** per calcolare in base allo stato di presenza del dispositivo.
6. Impostare l'ora per la presenza.

Start/End-Work Time

Impostare gli orari di inizio e fine del lavoro.

Valid Check-in/out Time

Impostare il periodo di validità entro il quale il check-in o il check-out sono validi.

Calculated as

Impostare la durata calcolata come durata effettiva del lavoro.

Late/Early Leave Allowable

Impostare il periodo di tempo per un'uscita tardiva o anticipata.

7. **Opzionale:** selezionare il tempo di pausa da escludere dal totale delle ore di lavoro.



Nota

È possibile fare clic su **Settings** per gestire i tempi di pausa. Per ulteriori dettagli sulla configurazione dei tempi di pausa, consultare la sezione **Configurazione dei tempi di pausa**.

8. Fare clic su **Save** per aggiungere la tabella di orari.
9. **Opzionale:** eseguire una o più delle seguenti operazioni dopo aver aggiunto la tabella di orari.

Edit Timetable Selezionare una tabella di orari per modificarne le informazioni.

Delete Timetable Selezionare una tabella di orari dall'elenco e fare clic su **Delete** per eliminarla.

8.9.3 Aggiunta di turni

È possibile aggiungere il turno per la pianificazione dei turni.

Prima di iniziare

Aggiungere prima di tutto una tabella di orari. Per i dettagli, consultare la sezione **Aggiunta di tabelle di orari**.

Passaggi

1. Fare clic su **Time & Attendance** → **Shift** per accedere alla pagina delle impostazioni dei turni.
2. Fare clic su **Add** per accedere alla pagina Add Shift.
3. Inserire il nome del turno.
4. Selezionare la durata del turno dall'elenco a discesa.
5. Selezionare la tabella di orari aggiunta e fare clic sulla barra temporale per applicarla.

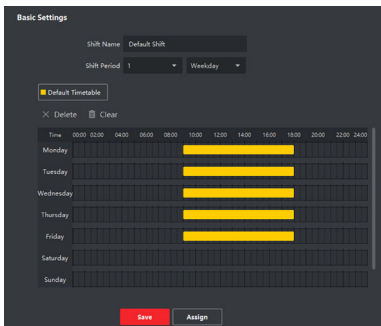


Figura 8-6 Aggiunta di turni

6. Fare clic su **Save**.

Il turno aggiunto sarà visualizzato sul pannello sinistro della pagina. Si possono aggiungere fino a 64 turni.

7. **Opzionale:** assegnare il turno all'organizzazione o alla persona per una pianificazione rapida dei turni.

- 1) Fare clic su **Assign**.

- 2) Selezionare la schermata **Organization** o **Person** e selezionare la casella relativa all'organizzazione o alla persona desiderata.

Le organizzazioni o le persone selezionate verranno elencate nella pagina a destra.

- 3) Impostare il periodo di validità della pianificazione dei turni.

- 4) Impostare altri parametri per la pianificazione dei turni, tra cui Checkin Not Required, Check-out Not Required, Effective for Holiday e Effective for Overtime.

- 5) Fare clic su **Save** per salvare la pianificazione rapida dei turni.

8.9.4 Gestione della pianificazione dei turni

Il lavoro a turni è una pratica di lavoro progettata per utilizzare tutte le 24 ore dei giorni della settimana. In genere, la pratica considera il giorno come suddiviso in turni, ossia periodi di tempo prestabiliti, durante i quali i diversi turnisti svolgono le proprie mansioni.

È possibile impostare la pianificazione di un reparto, di una persona e temporanea.

Impostazione della pianificazione di un reparto

È possibile impostare la pianificazione dei turni per un reparto e a tutte le persone del reparto verrà assegnata la pianificazione dei turni.

Prima di iniziare

Nel modulo Time & Attendance, l'elenco dei reparti è lo stesso di quello dell'organizzazione. È necessario prima di tutto aggiungere organizzazioni e persone nel modulo Person. Per i dettagli, vedere **Gestione delle persone**.

Passaggi

1. Fare clic su **Time & Attendance** → **Shift Schedule** per accedere alla pagina Shift Schedule Management.
2. Fare clic su **Department Schedule** per accedere alla pagina Department Schedule.
3. Selezionare il reparto dall'elenco di organizzazioni sulla sinistra.



Nota

Se è selezionata l'opzione **Include Sub Organization**, durante la selezione dell'organizzazione verranno selezionate contemporaneamente le relative organizzazioni secondarie.

4. Selezionare il turno dall'elenco a discesa.
5. Selezionare la casella di controllo per abilitare **Multiple Shift Schedules**.



Nota

Dopo aver selezionato **Multiple Shift Schedules**, è possibile selezionare i periodi di tempo validi tra quelli aggiunti per le persone del reparto.

Multiple Shift Schedules

Contiene più di un periodo di tempo. La persona può effettuare il check-in/check-out in qualsiasi periodo di tempo e la presenza sarà valida.

Se la pianificazione di più turni comprende tre periodi di tempo: dalle ore 00:00 alle 07:00, dalle 08:00 alle 15:00 e dalle 16:00 alle 23:00. La presenza della persona che adotta questa pianificazione di più turni sarà valida in uno qualsiasi dei tre periodi di tempo. Se la persona effettua il check-in alle 07:50, verrà applicato il periodo di tempo più vicino alla presenza della persona, tra le 08:00 e le 15:00.

6. Impostare le date di inizio e di fine.
7. Impostare altri parametri per la pianificazione, tra cui Check-in Not Required, Check-out Not Required, Effective for Holiday ed Effective for Overtime.
8. Fare clic su **Save**.

Impostazione della pianificazione di una singola persona

È possibile assegnare la pianificazione dei turni a una o più persone. È inoltre possibile visualizzare e modificare i dettagli della pianificazione della singola persona.

Prima di iniziare

Aggiungere un reparto e una persona nel modulo Person. Per i dettagli, vedere **Gestione delle persone**.

Passaggi



Nota

La pianificazione per singola persona ha una priorità più alta rispetto a quella per reparto.

1. Fare clic su **Time & Attendance** → **Shift Schedule** per accedere alla pagina Shift Schedule Management.
 2. Fare clic su **Person Schedule** per accedere alla pagina Person Schedule.
 3. Selezionare l'organizzazione e le persone.
 4. Selezionare il turno dall'elenco a discesa.
 5. Selezionare la casella di controllo per abilitare **Multiple Shift Schedules**.
-



Nota

Dopo aver selezionato **Multiple Shift Schedules**, è possibile selezionare le tabelle di orari valide tra quelle aggiunte per le persone.

Multiple Shift Schedules

Contiene più di una tabella di orari. La persona può effettuare il check-in/check-out in una qualsiasi delle tabelle di orari e la presenza sarà valida.

Se la pianificazione di più turni comprende tre tabelle di orari: dalle ore 00:00 alle 07:00, dalle 08:00 alle 15:00 e dalle 16:00 alle 23:00. La presenza della persona che adotta questa pianificazione di più turni sarà valida in una qualsiasi delle tre tabelle di orari. Se la persona effettua il check-in alle 07:50, verrà applicata la tabella di orari più vicina alla presenza della persona, tra le 08:00 e le 15:00.

6. Impostare le date di inizio e di fine.
7. Impostare altri parametri per la pianificazione, tra cui Check-in Not Required, Check-out Not Required, Effective for Holiday ed Effective for Overtime.
8. Fare clic su **Save**.

Impostazione di una pianificazione temporanea

È possibile aggiungere una pianificazione temporanea per la persona e quest'ultima verrà assegnata con la pianificazione temporanea dei turni. È inoltre possibile visualizzare e modificare i dettagli della pianificazione temporanea.

Prima di iniziare

Aggiungere un reparto e una persona nel modulo Person. Per i dettagli, vedere **Gestione delle persone**.

Passaggi



Nota

Le pianificazioni temporanee hanno una priorità maggiore di quelle per reparti o singole persone.

1. Fare clic su **Time & → Shift Schedule** per accedere alla pagina Shift Schedule Management.
2. Fare clic su **Temporary Schedule** per accedere alla pagina Temporary Schedule.
3. Selezionare l'organizzazione e le persone.
4. Fare clic su una data o fare clic e trascinare per selezionare più date per la pianificazione temporanea.
5. Selezionare **Workday** o **Non-Workday** dall'elenco a discesa. Se si seleziona **Non-Workday**, è necessario impostare i seguenti parametri.

Calculated as

Selezionare il livello normale o straordinario per contrassegnare lo stato di presenza per la pianificazione temporanea.

Timetable

Selezionare una tabella di orari dall'elenco a discesa.

Multiple Shift Schedule

Contiene più di una tabella di orari. La persona può effettuare il check-in/check-out in una qualsiasi delle tabelle di orari e la presenza sarà valida.

Se la pianificazione di più turni comprende tre tabelle di orari: dalle ore 00:00 alle 07:00, dalle 08:00 alle 15:00 e dalle 16:00 alle 23:00. La presenza della persona che adotta questa pianificazione di più turni sarà valida in una qualsiasi delle tre tabelle di orari. Se la persona effettua il check-in alle 07:50, verrà applicata la tabella di orari più vicina alla presenza della persona, tra le 08:00 e le 15:00.

Rule



Impostare un'altra regola per la pianificazione, ad esempio **Check-in Not Required** e **Check-out Not Required**.

6. Fare clic su **Save**.

Verifica della pianificazione dei turni

È possibile verificare la pianificazione dei turni in modalità Calendar o List. È inoltre possibile modificare o eliminare la pianificazione dei turni.

Passaggi

1. Fare clic su **Time & Attendance → Shift Schedule** per accedere alla pagina Shift Schedule Management.
2. Selezionare l'organizzazione e le persone corrispondenti.
3. Fare clic su  o  per visualizzare la pianificazione dei turni in modalità Calendar o List.

Calendar

In modalità Calendar, è possibile visualizzare la pianificazione dei turni per ogni giorno del mese. È possibile fare clic sulla pianificazione temporanea per un giorno per modificarla o eliminarla.

List

In modalità List, è possibile visualizzare i dettagli sulla pianificazione dei turni di una persona o organizzazione, ad esempio il nome del turno, il tipo, il periodo di validità e così via. Selezionare una o più pianificazioni dei turni, quindi fare clic su **Delete** per eliminare le voci selezionate.

8.9.5 Correzione manuale del record di check-in/check-out

Se lo stato di presenza non è corretto, è possibile correggere manualmente il record di check-in o check-out. È inoltre possibile modificare, eliminare, cercare o esportare il record di check-in o check-out.

Prima di iniziare


- È necessario aggiungere organizzazioni e persone nel modulo Person. Per i dettagli, consultare la sezione **Gestione delle persone**.
- Lo stato di presenza della persona non è corretto.

Passaggi



1. Fare clic su **Time & Attendance** → **Attendance Handling** per accedere alla pagina di gestione delle presenze.
2. Fare clic su **Correct Check-In/Out** per accedere alla pagina di aggiunta di correzioni di check-in/check-out.
3. Selezionare una persona dall'elenco a sinistra per correggerla.
4. Selezionare la data di correzione.
5. Impostare i parametri delle correzioni di check-in/check-out.
 - Selezionare **Check-in** e impostare l'effettivo orario di inizio del lavoro.
 - Selezionare **Check-out** e impostare l'effettivo orario di fine del lavoro.



Nota

È possibile fare clic su  per aggiungere più voci di check in/check-out. Sono supportate al massimo 8 voci di check-in/check-out.

6. **Opzionale:** inserire i commenti in base alle necessità.
7. Fare clic su **Save**.
8. **Opzionale:** dopo aver aggiunto la correzione del check-in/check-out, effettuare una delle seguenti operazioni.

View Fare clic su  o su  per visualizzare le informazioni relative alla gestione delle presenze aggiunte in modalità Calendar o List.



Nota

In modalità Calendar, è necessario fare clic su **Calculate** per ottenere lo stato di presenza della persona in un mese.

- Edit**
- In modalità Calendar, fare clic sull'etichetta relativa alla data per modificarne i dettagli.
 - In modalità List, fare doppio clic sui relativi campi nelle colonne Date, Handling Type, Time o Remark per modificarne le informazioni.
- Delete** Eliminare le voci selezionate.
- Export** Esportare i dettagli relativi alla gestione delle presenze sul computer locale.
-



I dettagli esportati vengono salvati in formato CSV.

8.9.6 Aggiunta di congedi, permessi e viaggi di lavoro

È possibile aggiungere un congedo, un permesso o un viaggio di lavoro quando il dipendente li richiede o deve viaggiare per lavoro.

Prima di iniziare

È necessario aggiungere organizzazioni e persone nel modulo Person. Per i dettagli, consultare la sezione **Gestione delle persone**.



Passaggi

1. Fare clic su **Time & Attendance** → **Attendance Handling** per accedere alla pagina di gestione delle presenze.
 2. Fare clic su **Apply for Leave/Business Trip** per accedere alla pagina di aggiunta di un permesso/congedo o viaggio di lavoro.
 3. Selezionare una persona dall'elenco a sinistra.
 4. Impostare una o più date per il permesso, il congedo o il viaggio di lavoro.
 5. Selezionare il tipo permesso/congedo maggiore e minore dall'elenco a discesa.
-



È possibile impostare il tipo di permesso o congedo in Attendance Settings. Per i dettagli, consultare la sezione

6. Impostare l'ora del permesso o congedo.
7. **Opzionale:** inserire i commenti in base alle necessità.
8. Fare clic su **Save**.
9. **Opzionale:** dopo aver aggiunto il permesso, il congedo o il viaggio di lavoro, effettuare una delle seguenti operazioni.

View Fare clic su  o su  per visualizzare le informazioni aggiunte in merito alla gestione delle presenze in modalità Calendar o List.



In modalità Calendar, è necessario fare clic su **Calculate** per ottenere lo stato di presenza della persona in un mese.

- Edit**
- In modalità Calendar, fare clic sull'etichetta relativa alla data per modificarne i dettagli.
 - In modalità List, fare doppio clic sui campi nelle colonne Date, Handling Type, Time o Remark per modificarne le relative informazioni.

Delete Eliminare le voci selezionate.

Export Esportare i dettagli relativi alla gestione delle presenze sul computer locale.



Nota

I dettagli esportati vengono salvati in formato CSV.

8.9.7 Calcolo dei dati sulle presenze

È necessario calcolare i dati relativi alle presenze prima di cercare e visualizzare la panoramica dei dati sulle presenze, dei dati dettagliati sulle presenze dei dipendenti, sulle presenze anomale e sugli straordinari dei dipendenti, nonché il registro di passaggio delle tessere.

Calcolo automatico dei dati sulle presenze

È possibile configurare una pianificazione in modo che il client possa calcolare automaticamente i dati relativi alle presenze all'ora stabilita ogni giorno.

Passaggi



Nota

Il sistema calcolerà i dati relativi alle presenze fino al giorno precedente.

1. Accedere al modulo Time & Attendance.
2. Fare clic su **Attendance Settings** → **General Rule**.
3. Nell'area relativa Auto-Calculate Attendance, impostare l'orario in cui si desidera che il client calcoli i dati ogni giorno.
4. Fare clic su **Save**.

Calcolo manuale dei dati sulle presenze

È possibile calcolare manualmente i dati relativi alle presenze impostando l'intervallo di date.

Passaggi

1. Accedere al modulo Time & Attendance.
2. Fare clic su **Attendance Statistics** → **Calculate Attendance**.
3. Impostare l'ora di inizio e l'ora di fine per definire l'intervallo di date delle presenze.
4. Impostare altre condizioni, tra cui reparto, nome della persona, numero del dipendente e stato di presenza.
5. Fare clic su **Calculate**.



Nota

Il calcolo delle presenze viene effettuato solo entro i tre mesi precedenti.

6. Eseguire una delle seguenti operazioni.

Correct Check-in/out	Fare clic su Correct Check-in/out per aggiungere correzioni di check-in/check-out.
Report	Fare clic su Report per generare il report delle presenze.
Export	Fare clic su Export per esportare i dati sulle presenze sul computer locale.



Nota

I dettagli esportati vengono salvati in formato CSV.

8.9.8 Statistiche delle presenze

È possibile controllare il record delle presenze originale, generare ed esportare il report delle presenze in base ai dati sulle presenze calcolati.

Record delle presenze originale

Per ottenere un record originale dei dipendenti, è possibile effettuare una ricerca per tempo di presenza del dipendente, stato di presenza, checkpoint, ecc. definendo un determinato periodo di tempo.

Prima di iniziare

- È necessario aggiungere organizzazioni e persone nel modulo Person e le persone che hanno passato le tessere. Per i dettagli, consultare la sezione **Gestione delle persone**.
- Calcolare i dati relativi alle presenze.



Nota

- Il client calcolerà automaticamente i dati relativi alle presenze del giorno precedente, alle ore 01:00 del giorno successivo.
 - Mantenere in funzione il client alle ore 01:00 altrimenti non sarà in grado di calcolare automaticamente i dati relativi alle presenze del giorno precedente. Se non vengono calcolati automaticamente, è possibile calcolare manualmente i dati delle presenze. Per i dettagli, consultare la sezione **Calcolo manuale dei dati sulle presenze**.
-

Passaggi

1. Accedere al modulo Time & Attendance.
2. Fare clic su **Attendance Statistics → Original Records**.
3. Impostare l'orario di inizio e di fine per il quale si desidera effettuare la ricerca delle presenze.
4. Impostare altre condizioni di ricerca, quali reparto, nome della persona e numero del dipendente.
5. **Opzionale:** fare clic su **Get from Device** per ottenere i dati sulle presenze dal dispositivo.
6. **Opzionale:** fare clic su **Reset** per reimpostare tutte le condizioni di ricerca e modificarle nuovamente.

7. Fare clic su **Search**.

Il risultato viene visualizzato sulla pagina. È possibile visualizzare lo stato di presenza e il checkpoint richiesti dal dipendente.

8. **Opzionale**: dopo aver cercato il risultato, eseguire una delle seguenti operazioni.

Generate Report	Fare clic su Report per generare il report delle presenze.
Export Report	Fare report clic su Export per esportare i risultati sul computer locale.

Generazione di report istantanei

È supportata la generazione manuale di una serie di report delle presenze per visualizzare i risultati sulle presenze dei dipendenti.

Prima di iniziare

Calcolare i dati relativi alle presenze.



Nota

È possibile calcolare manualmente i dati relativi alle presenze o impostare la pianificazione in modo che il client possa calcolare automaticamente i dati ogni giorno. Per i dettagli, consultare la sezione **Calcolo dei dati sulle presenze**.

Passaggi

1. Accedere al modulo Time & Attendance.
2. Fare clic su **Attendance Statistics → Report**.
3. Selezionare un tipo di report.
4. Selezionare il reparto o la persona per visualizzarne il report delle presenze.
5. Impostare l'ora di inizio e di fine del periodo di tempo dei dati sulle presenze da visualizzare nel report
6. Fare clic su **Report** per generare il report sulle statistiche e aprirlo.

Personalizzazione dei report delle presenze

Il client supporta più tipi di report ed è possibile predefinire il contenuto del report che verrà inviato automaticamente all'indirizzo e-mail configurato.

Passaggi



Nota

Impostare i parametri delle e-mail prima di attivare le funzioni di invio automatico delle e-mail. Per i dettagli, consultare la sezione **Impostazione dei parametri delle e-mail** nel manuale dell'utente del software client.

1. Accedere al modulo Time & Attendance.
2. Fare clic su **Attendance Statistics → Custom Report**.
3. Fare clic su **Add** per predefinire un report.

4. Impostare il contenuto del report.

Report Name

Immettere un nome per il report.

Report Type

Selezionare un tipo di rapporto per generarlo.

Report Time

L'ora selezionabile può variare in base al tipo di report.

Person

Selezionare le persone aggiunte, i cui record di presenza verranno generati per il report.

5. **Opzionale:** impostare la pianificazione affinché invii automaticamente il report agli indirizzi e-mail.

- 1) Selezionare **Auto-Sending Email** per abilitare tale funzione.
- 2) Impostare il periodo di validità durante il quale il client invierà il report nelle date di invio selezionate.
- 3) Selezionare le date in cui il client invierà il report.
- 4) Impostare l'ora in cui il client invierà il report.

Esempio

Se si imposta il periodo di validità **2018/3/10 to 2018/4/10**, selezionare **Friday** come data di invio e impostare l'ora di invio su **20:00**; il client invierà il report ogni venerdì alle 20:00 nel periodo dal 10/3/2018 al 10/4/2018.



Nota

Assicurarsi che i record delle presenze siano calcolati prima dell'ora di invio. È possibile calcolare manualmente i dati relativi alle presenze o impostare la pianificazione in modo che il client possa calcolare automaticamente i dati ogni giorno. Per i dettagli, consultare la sezione **Calcolo dei dati sulle presenze**.

- 5) Immettere gli indirizzi e-mail dei destinatari.



Nota

Fare clic su **+** per aggiungere un nuovo indirizzo e-mail. Sono consentiti fino a 5 indirizzi e-mail.

- 6) **Opzionale:** fare clic su **Preview** per visualizzare i dettagli dell'e-mail.

6. Fare clic su **OK**.

7. **Opzionale:** dopo aver aggiunto il report personalizzato, è possibile eseguire una o più delle seguenti operazioni:

- | | |
|------------------------|---|
| Edit Report | Selezionare un report aggiunto e fare clic su Edit per modificarne le impostazioni. |
| Delete Report | Selezionare un report aggiunto e fare clic su Delete per eliminarlo. |
| Generate Report | Selezionare un report aggiunto e fare clic su Report per generare in modo istantaneo il report visualizzandone i dettagli. |


9 Configurazione remota (Web)

Configurare i parametri del dispositivo da remoto.

9.1 Gestione dell'ora

Gestire il fuso orario del dispositivo, la sincronizzazione dell'ora e i parametri DST.

Fuso orario e sincronizzazione dell'ora

Nella pagina Device for Management, selezionare un dispositivo e fare clic su  → **System** → **Time** per accedere alla schermata Time.

È possibile selezionare un fuso orario, impostare i parametri NTP o sincronizzare manualmente l'ora.

Time Zone

Selezionare un fuso orario dall'elenco a discesa.


NTP

Il dispositivo sincronizzerà automaticamente l'ora con NTP.

Dopo aver abilitato **NTP**, è necessario impostare l'indirizzo del server NTP, la porta NTP e l'intervallo di sincronizzazione.

Manual Time Synchronization

Dopo aver attivato **Manual Time Synchronization**, è possibile impostare manualmente l'ora del dispositivo.

Se si seleziona **Synchronize with Computer Time**, **Set Time** mostrerà l'ora corrente del computer. A questo punto, deselezionare **Synchronize with Computer Time** e fare clic su , per modificare manualmente l'ora del dispositivo.

Fare clic su **Save** per salvare le impostazioni.

DST

Nella pagina Device for Management, fare clic su **Remote Configuration** → **System** → **Time** → **DST** per accedere alla schermata DST.


Abilitare DST per modificare l'ora DST preferita, l'ora DST di inizio e l'ora di fine.

Fare clic su **Save**.

9.2 Impostazione delle informazioni di rete

9.2.1 Impostazioni dei parametri di rete

Impostare i parametri di rete del dispositivo, inclusi il tipo di NIC, DHCP e HTTP.

Nella pagina Device for Management, fare clic su  → **Network** → **Network Parameters** per accedere alla schermata Network Parameters Settings.

NIC Type

Selezionare un tipo di NIC dall'elenco a discesa. È possibile selezionare Self-adaptive, 10M o 100M.

DHCP

Se si disattiva la funzione, è necessario impostare manualmente l'indirizzo IPv4 del dispositivo, la subnet mask IPv4, il gateway IPv4 predefinito, l'MTU e la porta.


Se si attiva la funzione, il sistema assegnerà automaticamente l'indirizzo IPv4, la subnet mask IPv4 e il gateway IPv4 predefinito per il dispositivo.

HTTP

Impostare la porta HTTP, l'indirizzo del server DNS1 e l'indirizzo del server DNS2.

9.2.2 Impostazioni dei parametri del centro di rete

È possibile impostare il centro di sorveglianza delle notifiche, l'indirizzo IP del centro, il numero di porta, il protocollo (EHome), il nome utente dell'account EHome, ecc. affinché trasmettano i dati tramite il protocollo EHome.

Nella pagina Device for Management, fare clic su  → **Network** → **Network Center Parameters** per accedere alla pagina Network Center Parameters Settings.

Selezionare un centro dall'elenco a discesa.

Dopo aver attivato la funzione, è possibile impostare il tipo di indirizzo del centro, l'indirizzo IP/nome di dominio, il numero di porta, un nome utente EHome, ecc.

Fare clic su **Save**.


9.3 Modifica della password del dispositivo

È possibile modificare la password del dispositivo.

Prima di iniziare

Accertarsi che il dispositivo sia acceso. Per ulteriori dettagli, consultare la sezione *Attivazione*.

Passaggi

1. Nella pagina Device for Management, fare clic su  → **System** → **User** per accedere alla schermata User.
2. Selezionare un utente e fare clic su **Edit** per accedere alla pagina Edit.
3. Immettere la vecchia password, crearne una nuova e confermarla.



Attenzione

Il sistema è in grado di valutare automaticamente la complessità della password del dispositivo. Si consiglia vivamente di modificare la password scelta (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Si consiglia di modificare con regolarità la password, soprattutto nei sistemi ad alta sicurezza: la modifica mensile o settimanale è in grado di proteggere meglio il prodotto.

Rientra nella responsabilità dell'installatore e/o dell'utente finale configurare correttamente tutte le password e altri parametri di sicurezza.


4. Fare clic su **OK**.

Risultato

La password del dispositivo è stata modificata. Immettere la nuova password nella pagina Device for Management per ricollegare il dispositivo.

9.4 Impostazioni della modalità di sicurezza

Impostare la modalità di sicurezza per accedere al software client.

Nella pagina Device for Management, fare clic su  → **System** → **Security** per accedere alla schermata Security Mode.

Selezionare una modalità di sicurezza dall'elenco a discesa e fare clic su **Save**.

Security Mode

Elevato livello di sicurezza per la verifica delle informazioni dell'utente durante l'accesso al software client.


Compatible Mode

La verifica delle informazioni dell'utente è compatibile con la vecchia versione del software client utilizzata per l'accesso.

9.5 Manutenzione del sistema

È possibile riavviare il dispositivo, ripristinarlo alle impostazioni predefinite e aggiornarlo.

Reboot

Nella pagina Device for Management, fare clic su  → **System** → **System Maintenance** per accedere alla schermata System Maintenance.

Fare clic su **Reboot** per riavviare il dispositivo.

Ripristino delle impostazioni predefinite

Nella pagina Device for Management, fare clic su **Remote Configuration** → **System** → **System Maintenance** per accedere alla schermata System Maintenance.

Restore Default

Verranno ripristinati i parametri predefiniti ad esclusione dell'indirizzo IP.

Restore All

Tutti i parametri del dispositivo verranno ripristinati ai valori predefiniti. Il dispositivo deve essere attivato dopo il ripristino.

Upgrade

Nella pagina Device for Management, fare clic su **Remote Configuration** → **System** → **System Maintenance** per accedere alla schermata System Maintenance.

Selezionare un tipo di dispositivo dall'elenco a discesa, fare clic su **Browse** e selezionare un file di aggiornamento dal computer locale, quindi fare clic su **Upgrade**.




Nota

- Se si seleziona Card reader come tipo di dispositivo, è necessario selezionare anche un numero di lettore di tessere dall'elenco a discesa.
- L'aggiornamento dura circa 2 minuti. Non spegnere durante l'aggiornamento. Dopo l'aggiornamento, il dispositivo si riavvierà automaticamente.

9.6 Visualizzazione delle informazioni del dispositivo

Visualizzare e impostare il nome del dispositivo, visualizzare il tipo di dispositivo, il numero di serie, la versione, il numero del relè e il numero di blocco.

Selezionare un dispositivo dalla schermata Device for Management e fare clic su  → **System** → **Device Information** per accedere alla pagina Device Information.

Device Name	<input type="text"/>
Device Type:	<input type="text"/>
Serial No.	<input type="text"/>
Firmware Version:	<input type="text"/>
Web Version	<input type="text"/>
Hardware Version:	<input type="text"/>
Local Zone Number:	4
Local Relay Number:	4
Lock Number	4
Local RS-485 Number:	8

Figura 9-1 Visualizzazione delle informazioni del dispositivo

È possibile impostare il nome del dispositivo, visualizzare il tipo di dispositivo, il numero di serie, la versione, il numero del relè e il numero di blocco. Fare clic su **Save** per salvare le impostazioni.

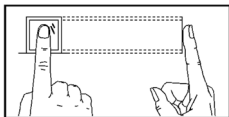
A. Suggerimenti per la scansione delle impronte digitali

Dita consigliate

Indice, medio o anulare.

Scansione corretta

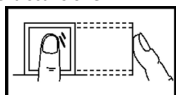
L'immagine riportata di seguito mostra il modo corretto per scansionare il dito:



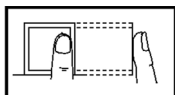
Premere il dito orizzontalmente sullo scanner. Il centro del dito scansionato deve essere allineato con il centro dello scanner.

Scansione errata

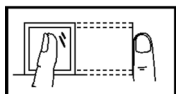
Le immagini qui sotto mostrano le posizioni errate del dito durante la scansione:



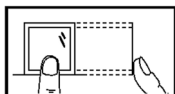
Vertical



Edge I



Side



Edge II

Ambiente

Non collocare lo scanner alla luce diretta del sole, non sottoporlo a temperature elevate, umidità e pioggia.

In caso di clima secco, lo scanner potrebbe non riconoscere correttamente l'impronta digitale. È possibile soffiare sul dito e ripetere la scansione.

Altro

Se i solchi dell'impronta sono poco profondi o si incontrano difficoltà durante la scansione, consigliamo di utilizzare altri metodi di autenticazione.

In caso di ferite al dito scansionato, lo scanner potrebbe non riconoscere l'impronta. È possibile cambiare dito e riprovare.

B. Capacità di controllo accessi

Visualizzare la capacità dei dati di controllo degli accessi, come l'autorizzazione per la tessera, lo stato della porta, la modalità di autenticazione del lettore di tessere e i dati sulle presenze.

Tabella B-1 Autorizzazione tessere

Contenuto	Parametri massimi configurabili
Week Schedule	32 Sono supportati fino a 8 periodi di tempo per una pianificazione settimanale
Holiday Schedule	128 Sono supportate fino a 8 durate per una pianificazione delle ferie. Una pianificazione delle ferie può appartenere a più gruppi di ferie.
Holiday Group	64 Sono supportate fino a 16 pianificazioni di ferie per un gruppo di ferie.
Schedule Template	64 Sono supportate fino a 1 pianificazione settimanale e 4 gruppi di ferie per un modello di pianificazione.

Tabella B-2 Stato della porta

Contenuto	Parametri massimi configurabili
Week Schedule	1
Holiday Schedule	32
Holiday Group	4
Schedule Template	1

Tabella B-3 Modalità di autenticazione del lettore di tessere

Contenuto	Parametri massimi configurabili
Week Schedule	2
Holiday Schedule	64
Holiday Group	8
Schedule Template	2

Tabella B-4 Presenze

Contenuto	Parametri massimi configurabili
Department	32
Normal Shift	32
Man-Hour Shift	32
Holiday	32
Holiday Group	64
Schedule by Department	32
Schedule by Individual	32

C. Regola di eliminazione dei record delle presenze

Attivazione dell'eliminazione dei record

Impostare la percentuale per la comparsa della finestra di notifica dei record di presenze oltre la soglia.

1. Quando il record raggiunge la soglia, sarà visualizzato un allarme di superamento del limite del record delle presenze sullo schermo del dispositivo. L'informazione dell'allarme sarà: Log will be full, export the report. Card authentication is available. L'interfaccia tornerà all'interfaccia degli allarmi dopo l'autenticazione
2. Quando il record è pieno, sarà visualizzato un allarme di superamento del limite del record delle presenze sullo schermo del dispositivo. L'informazione dell'allarme sarà: Log is full, export the report. Card authentication is available. E i primi 3000 record di presenze verranno eliminati automaticamente. L'interfaccia tornerà all'interfaccia degli allarmi dopo l'autenticazione.
3. Deleting by time e Deleting all sono disponibili durante l'eliminazione dei record delle presenze.

Disattivazione dell'eliminazione dei record

Impostare la percentuale per la comparsa della finestra di notifica dei record di presenze oltre la soglia.

1. Quando il record raggiunge la soglia, sarà visualizzato un allarme di superamento del limite del record delle presenze sullo schermo del dispositivo. L'informazione dell'allarme sarà: Log will be full, export the report. Card authentication is available. L'interfaccia tornerà all'interfaccia degli allarmi dopo l'autenticazione.
2. Quando il record è pieno, sarà visualizzato un allarme di superamento del limite del record delle presenze sullo schermo del dispositivo. L'informazione dell'allarme sarà: Log is full, export the report. Card authentication is available. E non verranno aggiunti altri nuovi record di presenze. L'interfaccia tornerà all'interfaccia degli allarmi dopo l'autenticazione.
3. Deleting by time e Deleting all sono disponibili durante l'eliminazione dei record delle presenze.

D. Tabella dei report delle presenze

Inserire qui una breve descrizione del concetto (opzionale).
Questo è l'inizio del concetto.

Descrizione del nome del file del report delle presenze

File Name Rule: N. dispositivo + Tipo di report.xls

Device No.: un numero di serie da 0 a 8.

Report Type:

- Abnormal Attendance: tabella Attendance Abnormal

- **AbnormalAttendance2:** quando la riga della tabella Attendance Abnormal è superiore a 60000, il record verrà esportato in due tabelle. Qui AbnormalAttendance2 fa riferimento alla seconda tabella Attendance Abnormal.
- **Attendance Summary:** la tabella Attendance Summary
- **Attendance Record:** la tabella Attendance Record
- **Attendance Schedule:** la tabella Attendance Schedule
- **Normal Shift:** la tabella Normal Shift
- **Man Hour Shift:** la tabella Man-Hour Shift

Tabella Attendance Schedule

Attendance Schedule											
Create Time: 2017-04-26 10:12:20											
Employee ID	Card No.	Name	Department	2017/01/01 (Sun.)		2017/01/02 (Mon.)		2017/01/03 (Tue.)		2017/01/04 (Wed.)	
				Shift No.	Shift Type	Shift No.	Shift Type	Shift No.	Shift Type	Shift No.	Shift Type

Tabella Attendance Schedule: in questa tabella vengono visualizzate tutte le informazioni sulla pianificazione dei turni degli utenti per un determinato periodo. È possibile impostare le informazioni sui turni e sulle ferie (nessuna presenza registrata durante le ferie) nella configurazione della pianificazione dei turni.

- **Employee ID:** il numero ID dell'utente.
- **Card No.:** il numero della tessera dell'utente.
- **Name:** il nome dell'utente.
- **Department:** il reparto dell'utente.

Tabella Normal Shift

Normal Shift									
Create Time: 2017-04-26 10:12:20									
Shift No.	Shift Name	Period 1		Period 2		Period 3		Period 4	
		Start	Stop	Start	Stop	Start	Stop	Start	Stop

Tabella Normal Shift: è possibile configurare fino a 4 periodi nella configurazione dei turni normali. È possibile registrare la presenza in base al periodo configurato.

Ad esempio: se si imposta il periodo 1 dalle 9:00 (Start) alle 17:00 (End), l'utente potrà registrare la presenza tra le 9:00 e le 17:00.

In combinazione con la regola di partecipazione, è possibile impostare più tipi di presenze.

Tabella Man-Hour Shift

Tabella Man-Hour Shift					
Create Time: 2017-04-26 10:12:20					
Shift No.	Shift Name	Work Duration (min)	Latest Start-Work Time	Period 1	
				Start	End

Tabella Man-Hour Shift: impostare la durata del turno di lavoro ore-uomo. Se si imposta Latest Start-Work Time su 0, tutti gli utenti risulteranno presenti. Se si imposta Latest Start-Work Time su un valore superiore a 0, l'utente risulterà assente se presente dopo l'orario configurato.

Ad esempio: se si imposta una durata di lavoro di 6 ore, l'orario di inizio del lavoro sarà alle 09:00, l'orario di fine del lavoro alle 17:00 e il periodo di pausa dalle 12:00 alle 13:00, mentre le ore di lavoro effettive dell'utente andranno dalle 17:00 alle 09:00 (dalle 13:00 alle 12:00).

Tabella Abnormal Attendance

Abnormal Attendance Table							
Create Time: 2017-04-26 10:12:20							
Employee ID	Card No.	Name	Department	SW-EW	Late Duration (min)	Early Leave Duration (min)	Total (min)

Tabella Abnormal Attendance Record: calcolare le presenze anomale in base ai record di presenze e alla configurazione del programma dei turni.

- Employee ID: il numero ID dell'utente.
- Card No.: il numero della tessera dell'utente.
- Name: il nome dell'utente.
- Department: il reparto dell'utente.
- Date: la data in cui vengono generati i dati.
- SW-EW: si possono configurare fino a 4 periodi. Viene registrato ogni giorno l'orario di presenza di ciascun utente.

- Late Duration (min): l'orario di presenza di inizio del lavoro è successivo al normale orario di inizio del lavoro.
- Early Leave Duration (min): l'orario di presenza di fine del lavoro è precedente al normale orario di fine del lavoro.
- Total: la durata totale di assenza in un giorno.

Tabella Attendance Record

Attendance Record Table									
Create Time: 2017-04-26 10:12:20									
Employee ID	Card No.	Name	Department	2017/01/01	2017/01/02	2017/01/03	2017/01/04	2017/01/05	2017/01/06
				SW-EW	SW-EW	SW-EW	SW-EW	SW-EW	SW-EW

Tabella Attendance Record: immettere l'ora di inizio e di fine del lavoro per esportare i dati sulle presenze valide per la durata configurata.

- Employee ID: il numero ID dell'utente.
- Card No.: il numero della tessera dell'utente.
- Name: il nome dell'utente.
- Department: il reparto dell'utente.

Tabella Attendance Summary

Attendance Summary Table									
Create Time: 2017-04-26 10:12:20									
Employee ID	Card No.	Name	Department	Late Times	Late Duration (min)	Early Leave Duration (min)	Absence Times	Absence Time Duration (min)	Attendance/ Total Work Days

Tabella Attendance Summary: immettere l'ora di inizio e di fine per calcolare le informazioni sulle presenze dell'utente tramite le informazioni sui turni e quelle sulle ferie, in base alla configurazione del programma dei turni.

- Employee ID: il numero ID dell'utente.
- Card No.: il numero della tessera dell'utente.
- il nome dell'utente.
- Department: il reparto dell'utente.
- Late Times: l'orario di presenza di inizio del lavoro è successivo al normale orario di inizio del lavoro. Arrivo in ritardo non più di una volta al giorno.

- Late Duration (min): durata totale del ritardo.
- Early Leave Times: l'orario di presenza di fine del lavoro è precedente al normale orario di fine del lavoro. Uscita anticipata non più di una volta al giorno.
- Early Leave Duration (min): durata totale delle uscite anticipate.
- Absence Times: tempo di assenza totale.
- Absence Time Duration (min): durata totale dell'assenza.
- Attendance/Total Work Days: giorni di presenza totali.

E. Descrizioni delle regole Wiegand personalizzate

Prendiamo Wiegand 44 come esempio, dove i valori dell'impostazione nella schermata Custom Wiegand sono i seguenti:

Custom Wiegand Name	Wiegand 44				
Total Length	44				
Transformation Rule (Decimal Digit)	byFormatRule[4]=[1][4][0][0]				
Parity Mode	XOR Parity				
Odd Parity Start Bit		Length			
Even Parity Start Bit		Length			
XOR Parity Start Bit	0	Length per Group	4	Total Length	40
Card ID Start Bit	0	Length	32	Decimal Digit	10
Site Code Start Bit		Length		Decimal Digit	
OEM Start Bit		Length		Decimal Digit	
Manufacturer Code Start Bit	32	Length	8	Decimal Digit	3

Dati Wiegand

Dati Wiegand = Dati validi + Dati di parità

Total Length

Lunghezza dei dati Wiegand.

Transportation Rule

4 byte. Visualizzare i tipi di combinazione dei dati validi.

L'esempio mostra la combinazione di ID della tessera e codice produttore. I dati validi possono essere una regola singola o una combinazione di più regole.

Parity Mode

Parità valida per i dati Wiegand. È possibile selezionare parità dispari o parità pari.

Odd Parity Start Bit e Length

Se si seleziona Odd Parity, sono disponibili le seguenti voci. Se il bit di avvio di parità dispari è 1 e la lunghezza 12, allora il sistema avvierà il calcolo della parità dispari dal bit 1. Calcolerà 12 bit. Il risultato sarà in bit 0. Il bit 0 è il primo bit.

Even Parity Start Bit e Length

Se si seleziona Even Parity, sono disponibili le seguenti voci. Se il bit di avvio di parità pari è 12 e la lunghezza 12, allora il sistema avvierà il calcolo della parità pari dal bit 12. Calcolerà 12 bit. Il risultato sarà nell'ultimo bit.

XOR Parity Start Bit, Length per Group e Total Length

Se si seleziona XOR Parity, sono disponibili le seguenti voci. A seconda della tabella visualizzata sopra, il bit di avvio è 0, la lunghezza per gruppo è 4 e la lunghezza totale è 40. Significa che il sistema calcolerà dal bit 0, calcolerà ogni 4 bit e calcolerà 40 bit in totale (10 gruppi in totale). Il risultato sarà negli ultimi 4 bit. La lunghezza del risultato è uguale alla lunghezza per gruppo.

Card ID Start Bit, Length, e Decimal Digit

Se si utilizza la regola di trasformazione, sono disponibili le seguenti voci. A seconda della tabella visualizzata sopra, il bit di avvio ID tessera è 0, la lunghezza è 32 e la cifra decimale è 10. Rappresenta ciò dal bit 0, ci sono 32 bit che rappresentano l'ID della tessera. La lunghezza qui viene calcolata per bit. La lunghezza della cifra decimale è 10 bit.

Site Code Start Bit, Length e Decimal Digit

Se si utilizza la regola di trasformazione, sono disponibili le seguenti voci. Per le informazioni dettagliate, consultare la spiegazione dell'ID della tessera.

OEM Start Bit, Length, e Decimal Digit

Se si utilizza la regola di trasformazione, sono disponibili le seguenti voci. Per le informazioni dettagliate, consultare la spiegazione dell'ID della tessera.

Manufacturer Code Start Bit, Length e Decimal Digit

Se si utilizza la regola di trasformazione, sono disponibili le seguenti voci. A seconda della tabella visualizzata sopra, il bit di avvio del codice produttore è 32, la lunghezza è 8 e la cifra decimale è 3. Rappresenta ciò dal bit 32, ci sono 8 bit che rappresentano il codice del produttore. La lunghezza qui viene calcolata per bit. La lunghezza decimale è 3 bit.