



GUIDA RAPIDA QUICK START

V1.0.2

Prefazione

Generale

Questo manuale illustra l'installazione e le operazioni di base del dispositivo Access Standalone (di seguito denominato Dispositivo). Leggere attentamente prima di utilizzare il dispositivo e conservare il manuale per future consultazioni.

Istruzioni di sicurezza

Nel manuale potrebbero comparire le seguenti parole chiave.

Parole chiave	Senso
 DANGER	Indica un elevato potenziale pericolo che, se non evitato, può provocare morte o lesioni gravi.
 WARNING	Indica un rischio potenziale medio o basso che, se non evitato, potrebbe provocare lesioni lievi o moderate.
 CAUTION	Indica un potenziale rischio che, se non evitato, potrebbe causare danni materiali, perdita di dati, cali di prestazioni o risultati imprevedibili.
 NOTE	Fornisce informazioni aggiuntive a complemento del testo.

Cronologia delle revisioni

Versione	Contenuto della revisione	Orario di rilascio
V1.0.2	Ho aggiornato lo schema elettrico.	Aprile 2025
V1.0.1	Inizializzazione aggiunta descrizione.	Dicembre 2024
V1.0.0	Prima edizione.	Agosto 2024

Informativa sulla protezione della privacy

In qualità di utente del dispositivo o titolare del trattamento dei dati, potresti raccogliere dati personali di terzi, come il volto, l'audio, le impronte digitali e il numero di targa. È necessario rispettare le leggi e i regolamenti locali in materia di protezione della privacy per tutelare i diritti e gli interessi legittimi di altre persone, implementando misure che includono, a titolo esemplificativo ma non esaustivo: fornire un'identificazione chiara e visibile per informare le persone dell'esistenza dell'area videosorvegliata e fornire le informazioni di contatto necessarie.

Informazioni sul manuale

- Il manuale è da intendersi solo a scopo di riferimento. Potrebbero esserci lievi differenze tra il manuale e il prodotto.
- Non ci assumiamo alcuna responsabilità per le perdite subite a causa di un utilizzo del prodotto non conforme al manuale.

- Il manuale verrà aggiornato in base alle leggi e ai regolamenti più recenti delle giurisdizioni competenti. Per informazioni dettagliate, consultare il manuale d'uso cartaceo, utilizzare il nostro CD-ROM, scansionare il codice QR o visitare il nostro sito web ufficiale. Il manuale è da intendersi solo come riferimento. Potrebbero esserci lievi differenze tra la versione elettronica e quella cartacea.
- Tutti i progetti e i software sono soggetti a modifiche senza preavviso scritto. Gli aggiornamenti del prodotto potrebbero comportare alcune differenze tra il prodotto reale e il manuale. Si prega di contattare il servizio clienti per ottenere il programma più recente e la documentazione supplementare.
- Potrebbero esserci errori di stampa o discrepanze nella descrizione delle funzioni, del funzionamento e dei dati tecnici. In caso di dubbi o controversie, ci riserviamo il diritto di fornire la spiegazione finale.
- Se il manuale (in formato PDF) non si apre, aggiorna il software del lettore o prova un altro programma di lettura diffuso.
- Tutti i marchi commerciali, i marchi registrati e i nomi delle aziende presenti nel manuale sono di proprietà dei rispettivi proprietari.
- In caso di problemi durante l'utilizzo del dispositivo, si prega di visitare il nostro sito web, contattare il fornitore o il servizio clienti.
- In caso di dubbi o controversie, ci riserviamo il diritto di fornire la spiegazione finale.

Misure di sicurezza e avvertenze importanti

Questa sezione introduce contenuti relativi al corretto utilizzo del Dispositivo, alla prevenzione dei rischi e alla prevenzione dei danni materiali. Leggere attentamente prima di utilizzare il Dispositivo e attenersi alle linee guida durante il suo utilizzo.

Requisiti di trasporto



Trasportare, utilizzare e conservare il Dispositivo entro i limiti consentiti in termini di umidità e temperatura.

Requisiti di stoccaggio



Conservare il dispositivo in condizioni di umidità e temperatura consentite.

Requisiti di installazione



WARNING

- Non collegare l'alimentatore al dispositivo mentre quest'ultimo è acceso.
- Attenersi scrupolosamente alle normative e agli standard locali in materia di sicurezza elettrica. Assicurarsi che la tensione ambiente sia stabile e soddisfi i requisiti di alimentazione del dispositivo.
- Non collegare il dispositivo a due o più tipi di alimentazione, per evitare di danneggiarlo.
- Un uso improprio della batteria potrebbe provocare incendi o esplosioni.
- Si prega di rispettare i requisiti elettrici per alimentare il dispositivo.
 - ◇ Di seguito sono riportati i requisiti per la scelta di un alimentatore.
 - L'alimentatore deve essere conforme ai requisiti delle norme IEC 60950-1 e IEC 62368-1.
 - La tensione deve soddisfare i requisiti SELV (Safety Extra Low Voltage) e non superare gli standard ES-1.
 - Quando la potenza del dispositivo non supera i 100 W, l'alimentatore deve soddisfare i requisiti LPS e non essere superiore a PS2.
 - ◇ Si consiglia di utilizzare l'alimentatore fornito con il dispositivo.
 - ◇ Quando si seleziona l'alimentatore, i requisiti di alimentazione (come la tensione nominale) sono soggetti alle informazioni riportate sull'etichetta del dispositivo.



- Il personale che lavora in quota deve adottare tutte le misure necessarie per garantire la propria sicurezza personale, compreso l'uso del casco e delle cinture di sicurezza.
- Non posizionare il dispositivo in un luogo esposto alla luce solare o vicino a fonti di calore.
- Tenere il dispositivo lontano da umidità, polvere e fuliggine.
- Installare il dispositivo su una superficie stabile per evitare che cada.
- Installare il dispositivo in un luogo ben ventilato e non ostruire le prese d'aria.

- Utilizzare un adattatore o un alimentatore per armadio fornito dal produttore.
- Utilizzare cavi di alimentazione consigliati per la regione e conformi alle specifiche di potenza nominale.
- Il dispositivo è un apparecchio elettrico di classe I. Assicurarsi che l'alimentazione del dispositivo sia collegata a una presa di corrente con messa a terra di protezione.
- Il dispositivo deve essere installato ad un'altezza pari o inferiore a 2 metri.
- Se il prodotto ha un involucro metallico, si consiglia di installarlo in un ambiente con una temperatura inferiore a 40°C (104°F) per evitare il surriscaldamento e compromettere la tua esperienza.

Requisiti operativi



- Prima dell'uso, verificare che l'alimentazione elettrica sia corretta.
- Collegare il dispositivo a una messa a terra di protezione prima di accenderlo.
- Non scollegare il cavo di alimentazione laterale del dispositivo mentre l'adattatore è acceso.
- Utilizzare il dispositivo entro i limiti nominali di potenza in ingresso e in uscita.
- Utilizzare il dispositivo entro i limiti di umidità e temperatura consentiti.
- Non far cadere né spruzzare liquidi sul dispositivo e assicurarsi che non vi siano oggetti contenenti liquidi sul dispositivo che possano impedire al liquido di penetrarvi.
- Non smontare il dispositivo senza le istruzioni di un professionista.
- Questo prodotto è un'attrezzatura professionale.
- Il dispositivo non è adatto all'uso in luoghi in cui è probabile la presenza di bambini.
- Se il prodotto supporta l'alimentazione PoE e può alimentare serrature elettromagnetiche che rimangono normalmente aperte quando sono spente, la serratura collegata si aprirà automaticamente in caso di problemi con il cavo di rete o di sua disconnessione. Si consiglia di controllare regolarmente il cablaggio per ridurre al minimo il rischio di malfunzionamenti. In luoghi con elevati requisiti di sicurezza, si consiglia di utilizzare una serratura elettromagnetica che rimanga normalmente chiusa quando è spenta o di installare un gruppo di continuità (UPS) per prevenire potenziali incidenti.

Sommario

Prefazione.....	I
Importanti precauzioni e avvertenze.....	III 1
Struttura.....	1
2 Cablaggio e installazione.....	2
2.1 Requisiti di installazione.....	2
2.2 Cablaggio.....	3
2.3 Procedura di installazione.....	7
3 Configurazioni locali.....	9
3.1 Inizializzazione.....	9
3.2 Menù principale.....	10
3.3 Aggiunta di utenti.....	11
4 Operazioni SmartPSS Lite.....	12
4.1 Installazione.....	12
4.2 Inizializzazione.....	12
4.3 Accesso.....	15
Appendice 1 Raccomandazione di sicurezza.....	17

1 Struttura

Lo schema è puramente indicativo. La struttura e le dimensioni potrebbero differire a seconda dei modelli reali.

Figura 1-1 Dimensioni (unità: mm [pollici])

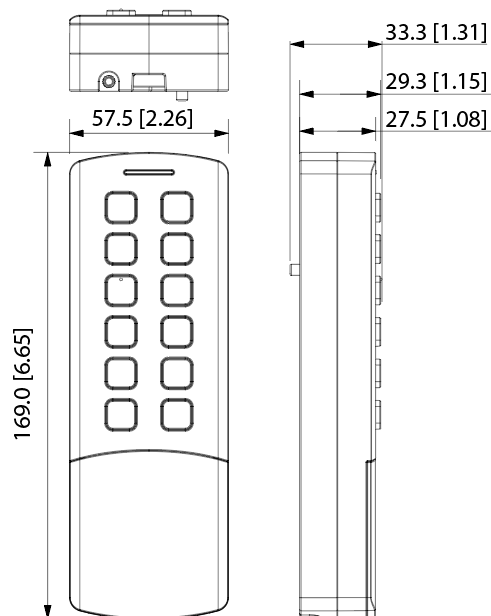
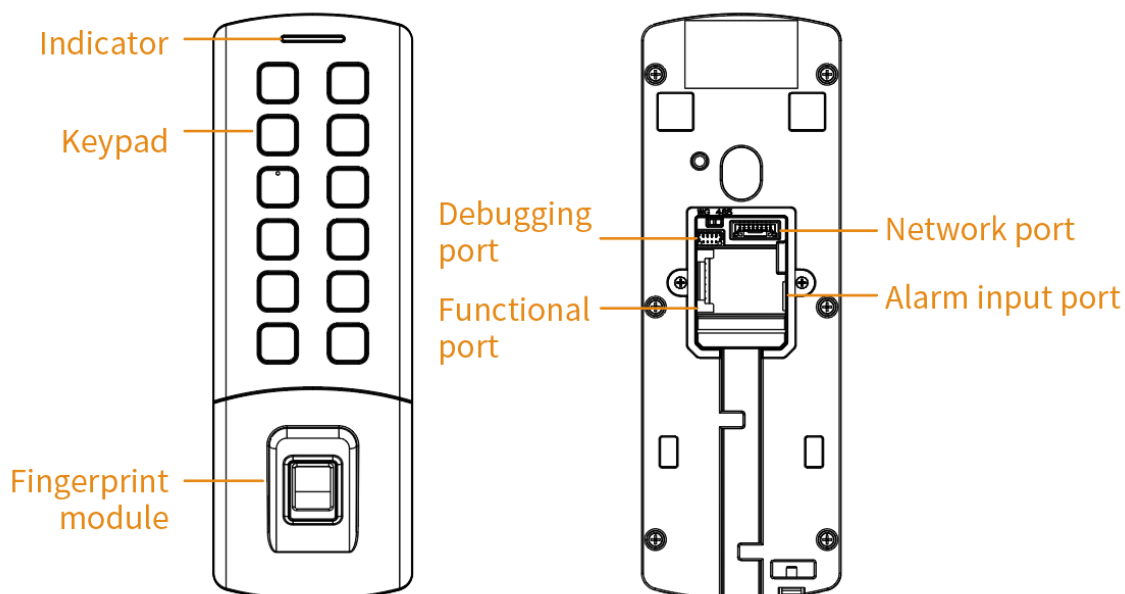


Figura 1-2 Struttura



La funzione di riconoscimento delle impronte digitali è disponibile su alcuni modelli.

2 Cablaggio e installazione

2.1 Requisiti di installazione



- L'altezza di installazione consigliata (dall'indicatore al suolo) è di 1,4 m.
- L'intensità luminosa a 0,5 metri di distanza dal dispositivo non deve essere inferiore a 100 Lux.
- Si consiglia di installare il dispositivo all'interno, ad almeno 3 metri di distanza da finestre e porte e a 2 metri di distanza dalla fonte luminosa.
- Evitate la retroilluminazione, la luce solare diretta, la luce ravvicinata e la luce obliqua.

Requisiti di illuminazione ambientale

Figura 2-1 Requisiti di illuminazione ambientale



Candle: 10 lux



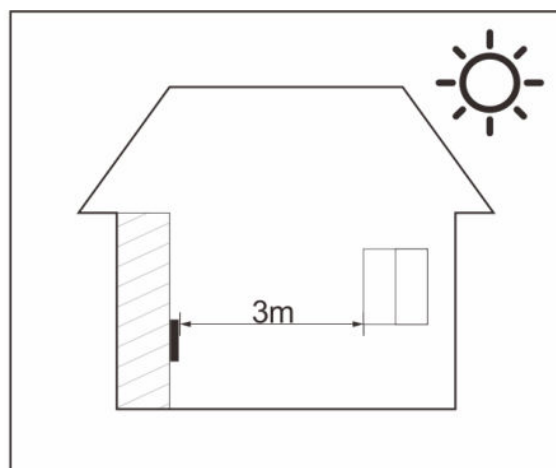
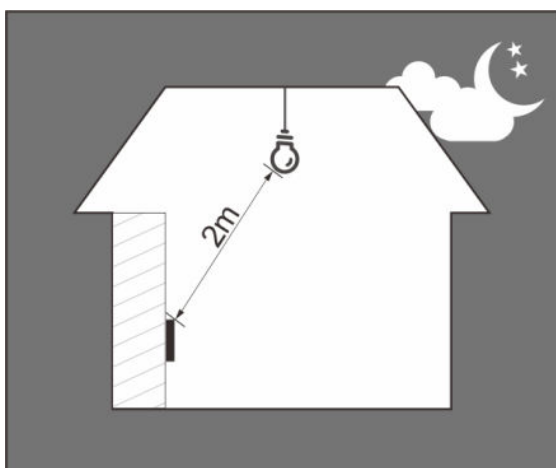
Light bulb: 100 lux-850 lux



Sunlight: ≥ 1200 lux

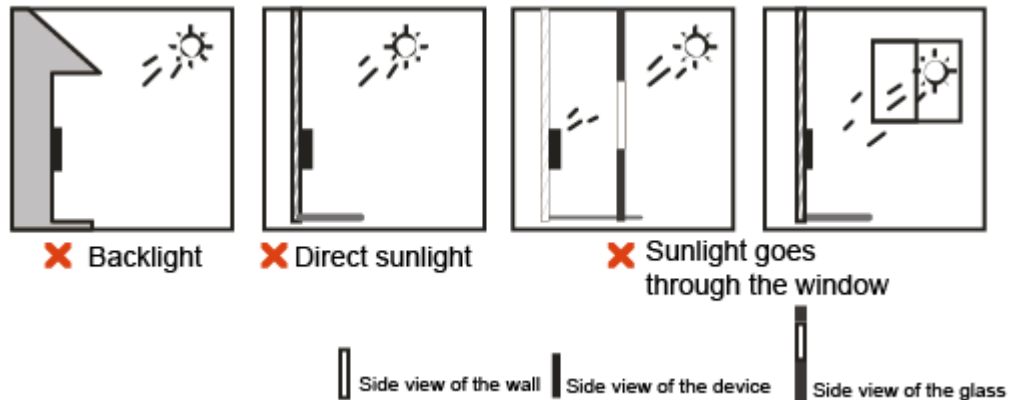
Posizione di installazione consigliata

Figura 2-2 Posizione di installazione consigliata



Luogo di installazione non consigliato

Figura 2-3 Posizione di installazione non consigliata



2.2 Cablaggio

Le porte potrebbero variare a seconda del modello del prodotto.

- RS485A e WG_D0 condividono lo stesso cavo. RS485B e WG_D1 condividono lo stesso cavo.
- Quando il DIP switch è impostato su WG, il cavo condiviso può essere collegato a un dispositivo Wiegand. Quando il DIP switch è impostato su 485, il cavo condiviso può essere collegato a un dispositivo RS-485.
- Se si seleziona **Modulo di controllo porta** Attraverso **Impostazioni di comunicazione > Configurazione RS-485** Il modulo di sicurezza per il controllo della porta deve essere acquistato separatamente. Il modulo di sicurezza necessita di un alimentatore separato.
- Quando la funzione del modulo di sicurezza è attivata, il pulsante di uscita, il controllo della serratura e il collegamento all'allarme diventano inefficaci.

Figura 2-4 Cablaggio

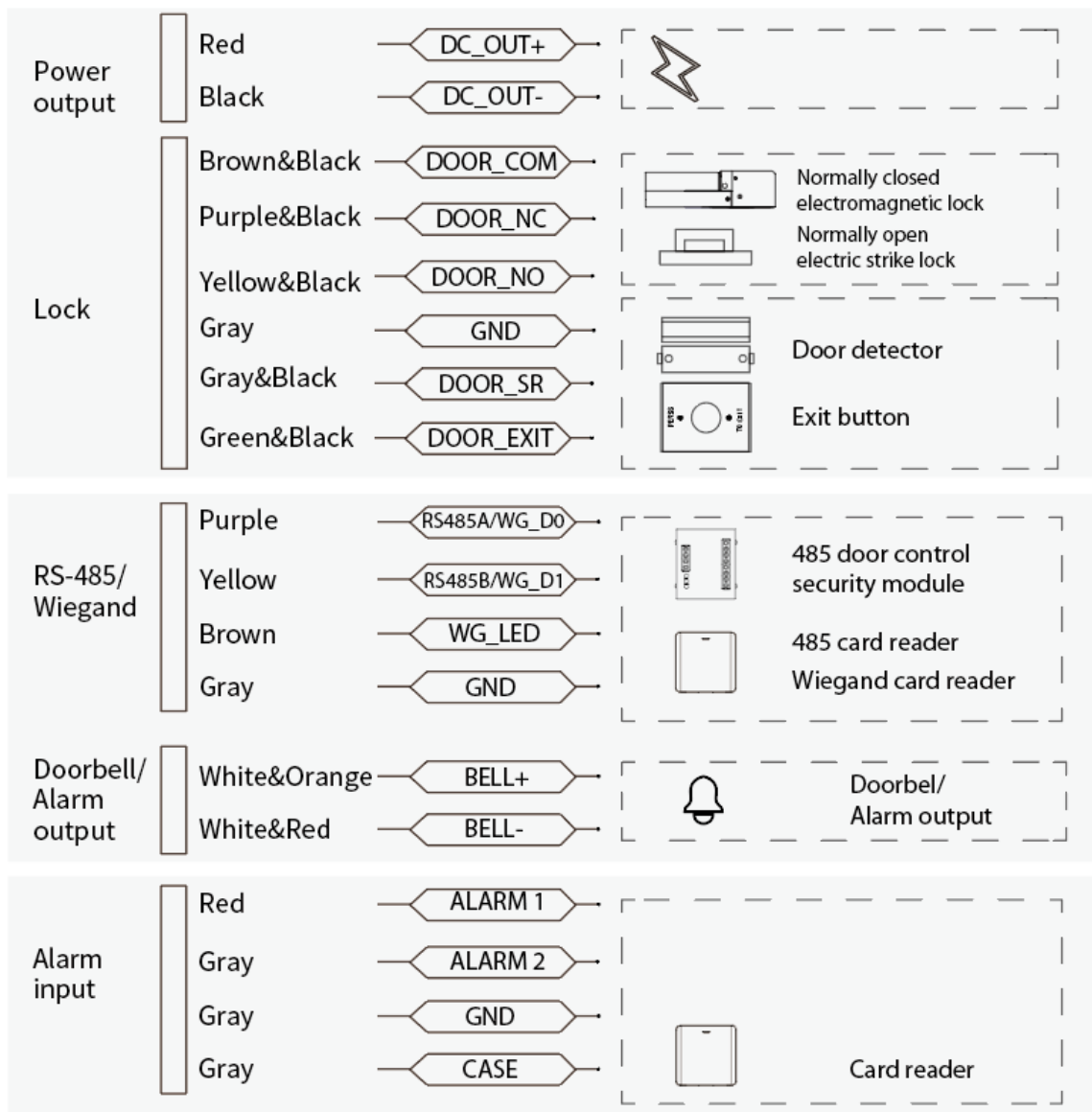


Figura 2-5 Cablaggio per il dispositivo standard

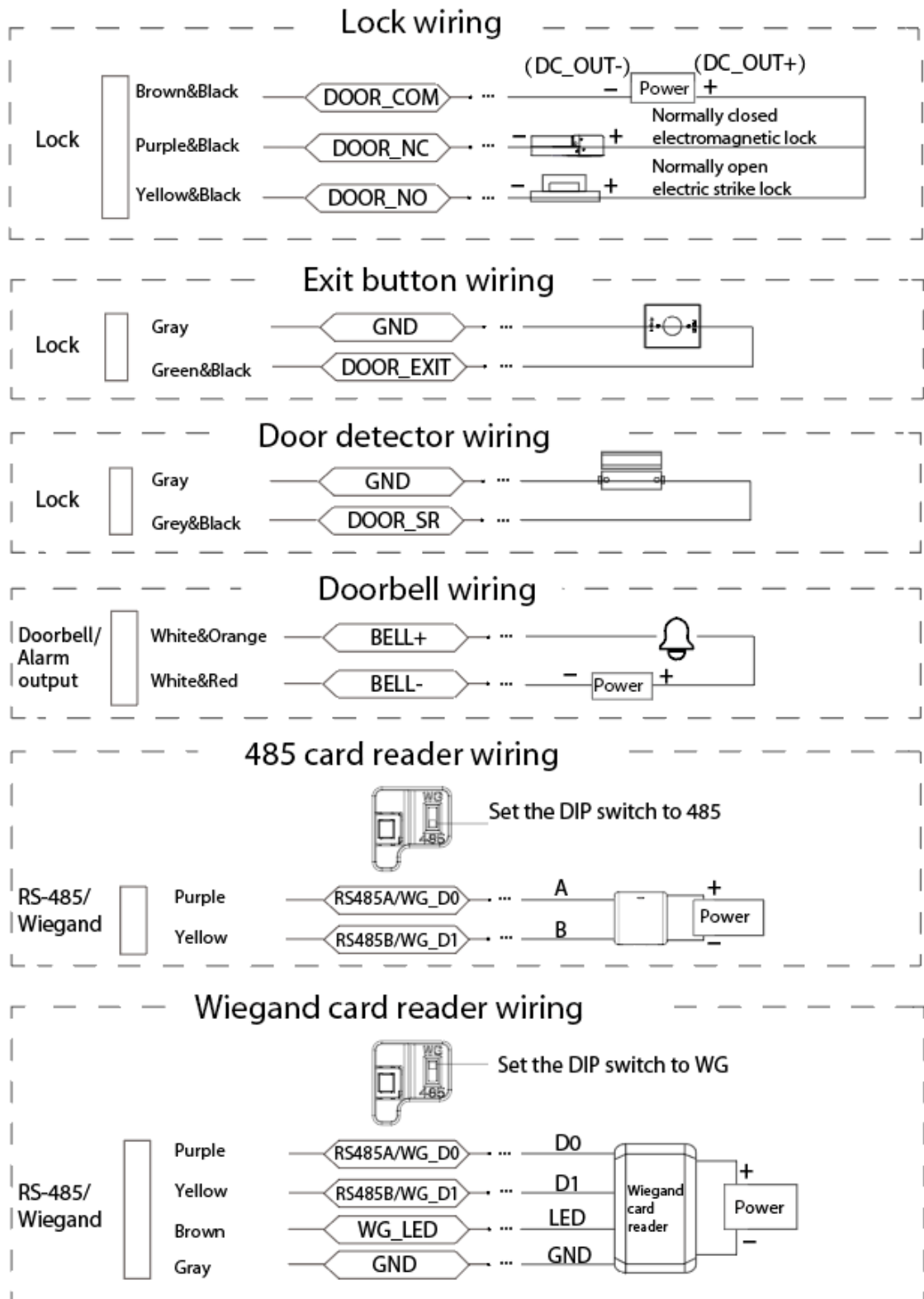


Figura 2-6 Cablaggio per il modulo di sicurezza per il controllo della porta

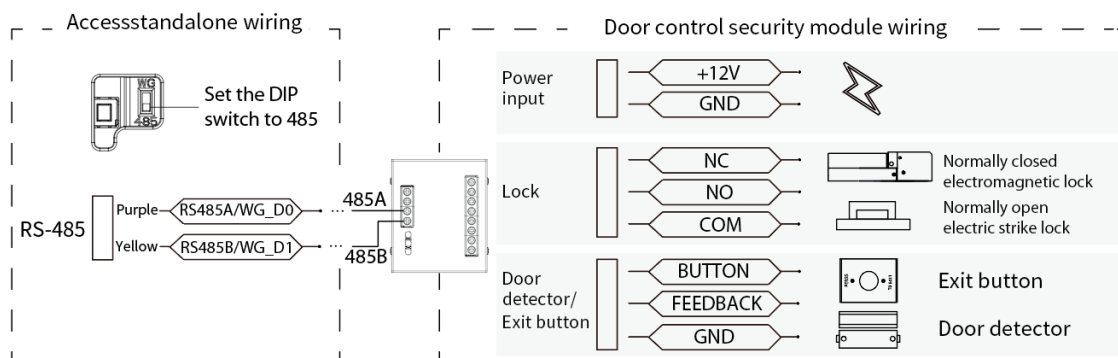


Figura 2-7 Cablaggio di alimentazione

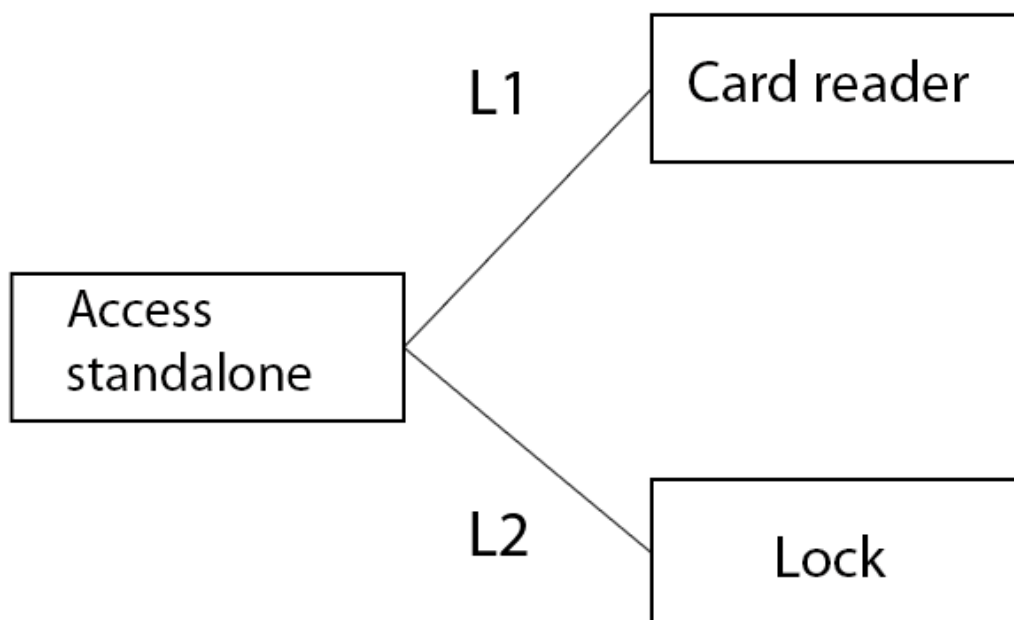


Tabella 2-1 Descrizione delle specifiche del cavo

NO.	Nome	Modello consigliato e Specifiche	Distanza massima consigliata per l'alimentazione e la comunicazione.
L1	Lettore di schede Cavo	- RVV0.5 (resistenza in corrente continua di un singolo conduttore $\leq 39,0 \Omega/\text{km}$) - RVV1.0 (resistenza in corrente continua di un singolo conduttore $\leq 19,5 \Omega/\text{km}$) - RVV1.5 (resistenza in corrente continua di un singolo conduttore $\leq 13,3 \Omega/\text{km}$) - CAT5E (impedenza entro 100 m $\leq 9 \Omega$)	- RVV0.5 - Letto di schede RS_485: $\leq 200 \text{ m}$ - Letto di schede Wiegand: $\leq 120 \text{ m}$ - CAT5E (monoconduttore) - Letto di schede RS_485: $\leq 120 \text{ m}$ - Letto di schede Wiegand: $\leq 50 \text{ m}$

NO.	Nome	Modello consigliato e Specifiche	Distanza massima consigliata per l'alimentazione e la comunicazione.
L2	Cavo di bloccaggio		● RVV0.5 Serratura elettromagnetica a una porta da 280 kg: ≤ 60 m ● RVV1.0 Serratura elettromagnetica a una porta da 280 kg: ≤ 100 m ● RVV1.5 Serratura elettromagnetica a una porta da 280 kg: ≤ 140 m



- Se il lettore di schede è alimentato dal controller di accesso autonomo, si consiglia di selezionare un lettore di schede con una corrente massima non superiore a 200 mA. Il lettore di schede selezionato deve supportare un ampio intervallo di tensione di funzionamento, con una tensione minima non superiore a 9 V.
- Se la serratura è alimentata dal sistema di controllo accessi autonomo, si consiglia di selezionare una serratura con una corrente massima non superiore a 500 mA. La serratura selezionata deve supportare un ampio intervallo di tensione di funzionamento, con una tensione minima non superiore a 10 V.
- La distanza di cablaggio tra L1 e L2 è influenzata dalla tensione di alimentazione e dalle specifiche del cavo di alimentazione. Durante l'installazione, è necessario assicurarsi che la tensione di alimentazione non sia inferiore alla tensione operativa minima dell'unità di controllo accessi, del lettore di schede e della serratura. Inoltre, L1 e L2 non devono condividere lo stesso cavo.
- Quando si utilizza il cavo CAT5E (impedenza entro $100\text{ m} \leq 9\ \Omega$) per l'alimentazione di serrature o lettori di schede, si consiglia di distribuire uniformemente i cavi aggiuntivi, oltre a quelli necessari per il segnale, per l'alimentazione delle serrature o dei lettori di schede, al fine di ridurre al minimo le perdite di alimentazione.
- I dati potrebbero variare a seconda della situazione reale.

2.3 Procedura di installazione

Il dispositivo supporta il montaggio a parete e offre due metodi di cablaggio: cablaggio a vista e cablaggio a incasso.

Procedura

Passo 1 In base alla posizione dei fori della staffa di installazione, praticare 6 fori e 1 fessura per il passaggio dei cavi nella parete.



Per i cablaggi a vista non è necessario prevedere una fessura nel muro.

Passo 2 Inserire le viti di espansione nei fori, quindi avvitare la staffa alla parete. Collegare i cavi al dispositivo. Per

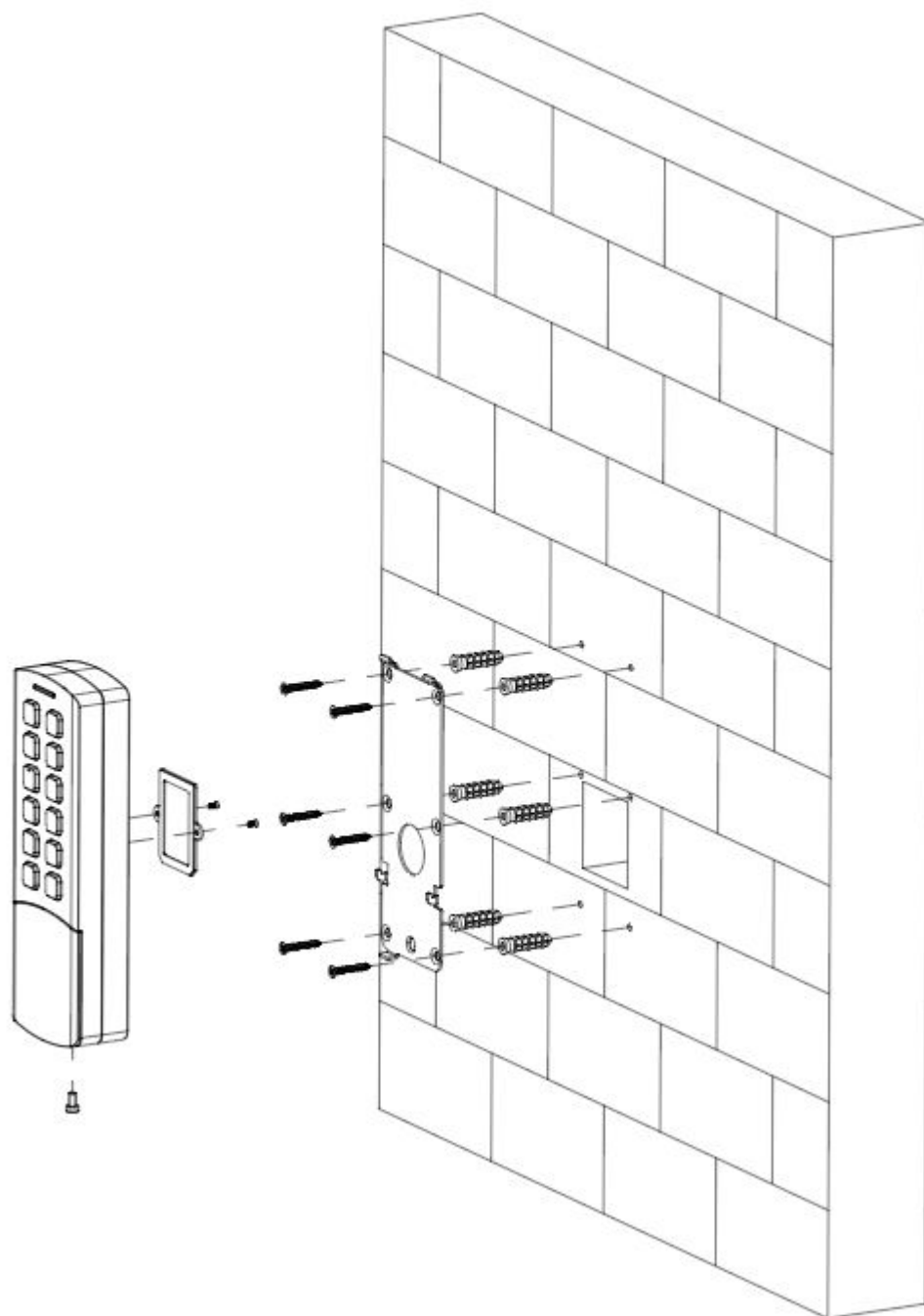
Passo 3 maggiori dettagli, consultare la sezione "2.2 Cablaggio".

- Far passare il cavo attraverso il pannello posteriore di installazione e la fessura per il cablaggio a parete.
- Per i cablaggi a vista, il cavo non deve necessariamente passare attraverso il pannello posteriore di installazione.

Passo 4 Fissare il dispositivo alla staffa del pannello posteriore.

Passo 5 Avvitare una vite nella parte inferiore del dispositivo.

Figura 2-8 Installazione



3 configurazioni locali

Le operazioni locali potrebbero variare a seconda dei diversi modelli di controller di accesso.

3.1 Inizializzazione

Dopo aver acceso il dispositivo per la prima volta, è necessario impostare la password di amministratore. La password di amministratore viene utilizzata per accedere al menu principale del dispositivo.

Procedura

Passo 1 Accendi il dispositivo e la spia luminosa lampeggerà lentamente in rosso.

Passo 2 Premi#, inserisci la password dell'amministratore e poi premi#.

La password deve essere lunga da 1 a 8 caratteri.

Se la spia luminosa è blu fissa, significa che il dispositivo è stato inizializzato.



Dopo l'inizializzazione, è possibile utilizzare solo le funzioni presenti sul Dispositivo. Se si desidera accedere alla pagina web del Dispositivo, è necessario inizializzare il Dispositivo tramite la relativa pagina web o attraverso il ConfigTool.

Operazioni correlate

- È possibile impostare numeri come password dell'account amministratore solo durante l'inizializzazione tramite il dispositivo.
- È possibile impostare numeri, lettere e altri caratteri come password dell'account amministratore durante la fase di inizializzazione tramite la piattaforma ConfigTool.

Dopo aver completato l'inizializzazione del dispositivo, è possibile eseguire operazioni solo sul dispositivo stesso. Se è necessario connettere il dispositivo alla rete, utilizzare ConfigTool o la piattaforma per inizializzarlo.

Quando si utilizza ConfigTool o la piattaforma per inizializzare il dispositivo, dopo aver configurato l'account di rete e la password, il dispositivo completerà automaticamente l'inizializzazione ed entrerà in modalità standby. La password di amministratore locale viene convertita dalla password di rete. Se la password supera gli 8 caratteri, vengono mantenuti solo i primi 8. Le lettere vengono convertite in cifre secondo lo standard E.161. La conversione della password non fa distinzione tra maiuscole e minuscole e tutti gli altri simboli vengono convertiti in 0.



- Dopo l'inizializzazione, se si modifica la password di rete, la password dell'amministratore locale non verrà modificata.
- Se si inizializza prima tramite il dispositivo e poi tramite ConfigTool o la piattaforma, la password dell'amministratore locale non verrà modificata.

Figura 3-1 E.161 (tastiera T9)

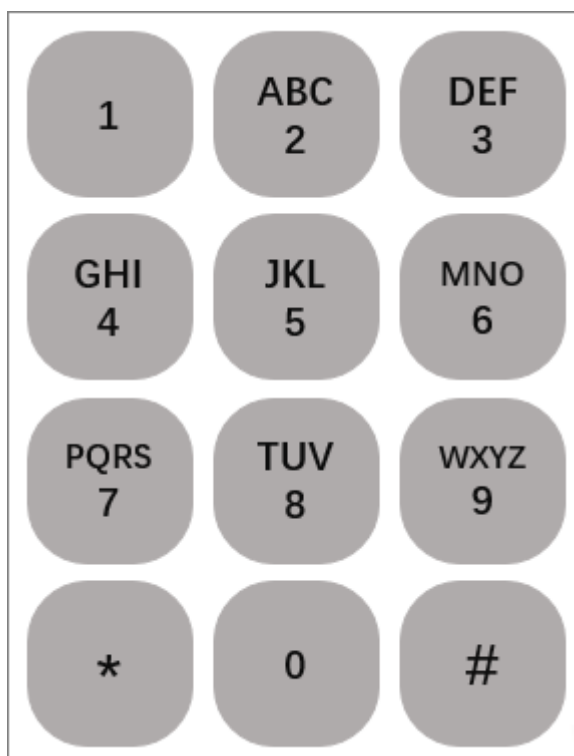


Tabella 3-1 Esempio di conversione

Password di rete	Password dell'amministratore locale
ABC12345	22212345
admin123	23646123
admin12!	23646120
admin123456	23646123

3.2 Menu principale

Accesso al menu principale

Premere#, inserisci la password dell'amministratore e poi premi#.

- L'indicatore lampeggia in blu e significa che sei entrato nel menu principale.
- L'indicatore lampeggia una volta in rosso, il cicalino emette 3 bip e poi l'indicatore diventa blu fisso, il che significa che la password è errata.

Suggerimenti correlati

- L'indicatore lampeggia una volta in verde e il cicalino emette un segnale acustico, a indicare che l'operazione o la verifica del controllo accessi è andata a buon fine.
- L'indicatore lampeggia una volta in rosso e il cicalino emette tre segnali acustici, il che significa che l'operazione o la verifica del controllo accessi non è andata a buon fine.
- Se l'indicatore lampeggia lentamente in rosso, significa che il dispositivo non è stato de-inizializzato.

- Se l'indicatore è blu fisso, significa che il dispositivo è in modalità standby.
- L'indicatore lampeggia in blu, a indicare che il dispositivo è entrato nel menu principale.
- La tastiera è bianca quando si utilizza il dispositivo. Se non viene rilevata alcuna operazione entro 10 secondi, la luce si spegne e il dispositivo esce dalla schermata corrente.

3.3 Aggiunta di utenti



- È possibile aggiungere una sola carta, una sola password o una sola impronta digitale per utente. È necessario aggiungere almeno un metodo di autenticazione tra carta, password e impronta digitale.
- La funzione di riconoscimento delle impronte digitali è disponibile su alcuni modelli.

Procedura

Passo 1 Premere#, inserisci la password dell'amministratore e poi premi#.

Accedi al menu principale e l'indicatore lampeggia in blu.

Passo 2 Premi1E#per aggiungere utenti. Inserisci l'ID utente e poi

Passo 3 premi#.

- Se l'indicatore non si accende e il dispositivo emette un segnale acustico, l'ID utente è stato aggiunto correttamente.
- Se l'indicatore lampeggia in rosso e il dispositivo emette un segnale acustico, l'aggiunta dell'ID utente non è andata a buon fine. Il motivo potrebbe essere che l'ID esiste già. Prova con un altro ID.



Sul dispositivo è possibile inserire solo numeri come ID.

Passo 4 Dopo aver strisciato la carta, premere#per aggiungere la scheda.

Se non è necessario aggiungere la carta, premere#per

Passo 5 saltarlo. Inserisci la password utente e poi premi#.

Se non è necessario impostare la password utente, premere#per saltarlo.



La password può essere lunga da 1 a 8 caratteri.

Passo 6 Aggiungi l'impronta digitale e poi premi#.

Se non è necessario impostare l'impronta digitale, premere#per saltarlo.



Questa funzione è disponibile su alcuni modelli.

Passo 7 RipeterePasso 2 APasso 6 per aggiungere altri utenti.

Dopo aver aggiunto l'utente, premere*per tornare al menu principale, quindi premere*per tornare allo stato di standby.

4 Operazioni SmartPSS Lite

4.1 Installazione

Contatta l'assistenza tecnica o visita il sito web ufficiale per ottenere SmartPSS Lite. Se ottieni il pacchetto software di SmartPSS Lite, installalo ed eseguilo seguendo le istruzioni presenti sulla pagina.

4.2 Inizializzazione

Inizializza SmartPSS Lite al primo accesso, impostando una password per l'accesso e domande di sicurezza per il ripristino della password.

Procedura

Passo 1 Fare doppio clic su SmartPSSLite.exe.

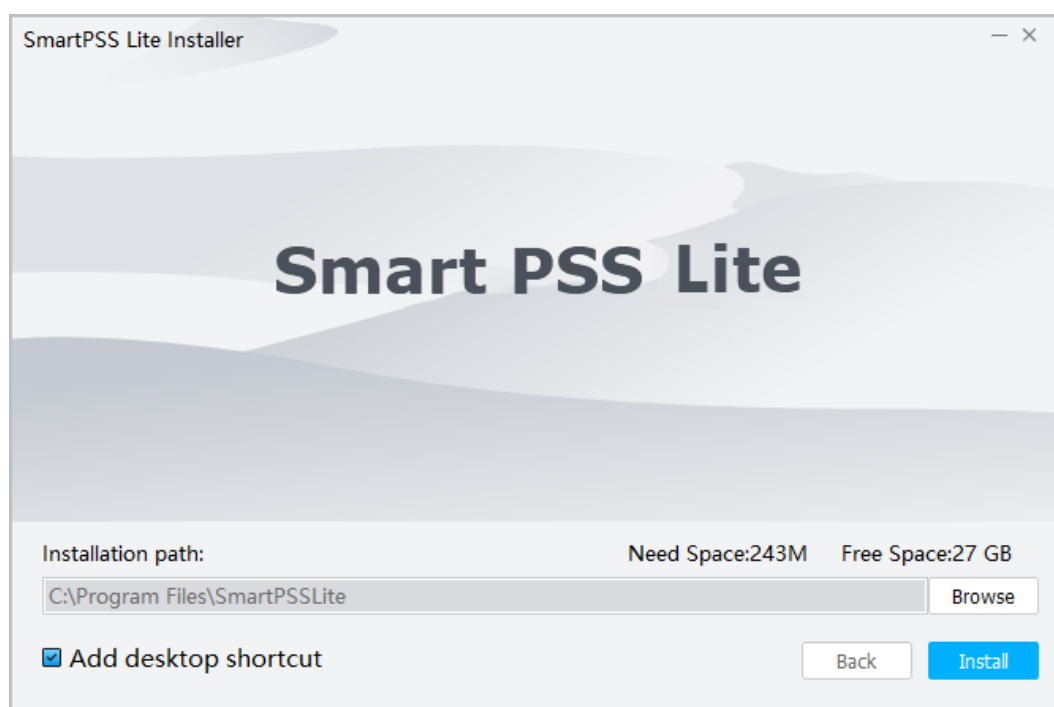
Passo 2 Seleziona la lingua dall'elenco a discesa, seleziona **Ho letto e accetto il contratto di licenza del software.**, e poi fai clic **Prossimo**.

Figura 4-1 Seleziona la lingua



Passo 3 Clic **Sfoglia** per selezionare il percorso di installazione, quindi fare clic **Installare**.

Figura 4-2 Selezionare il percorso di installazione

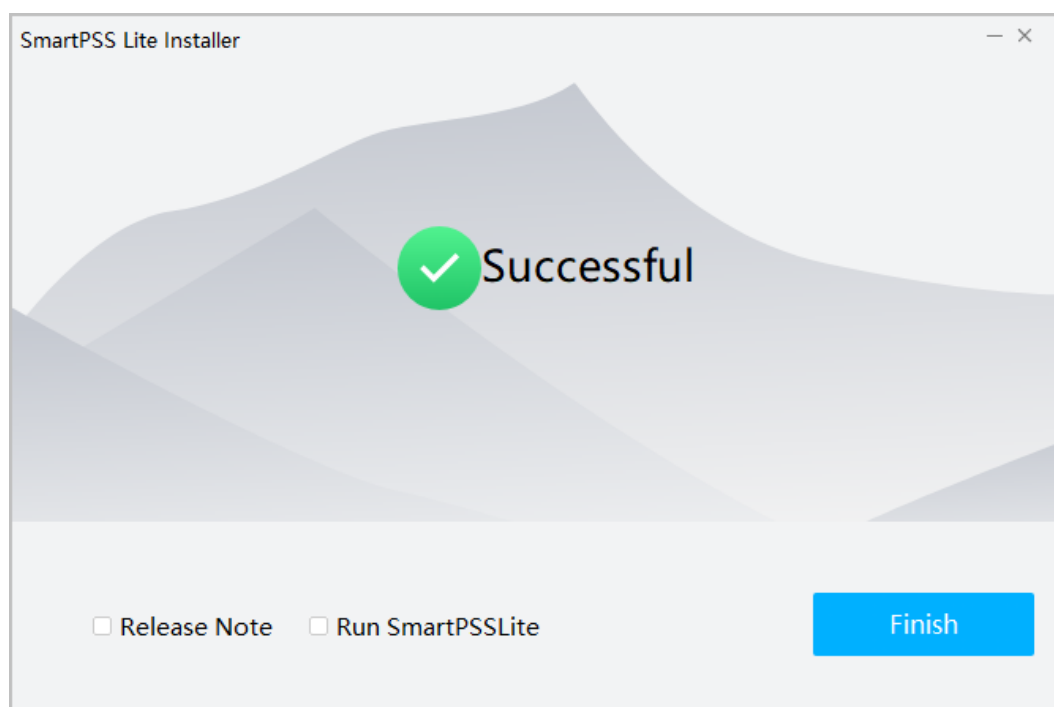


Passo 4 Clic**Fine**per completare l'installazione.



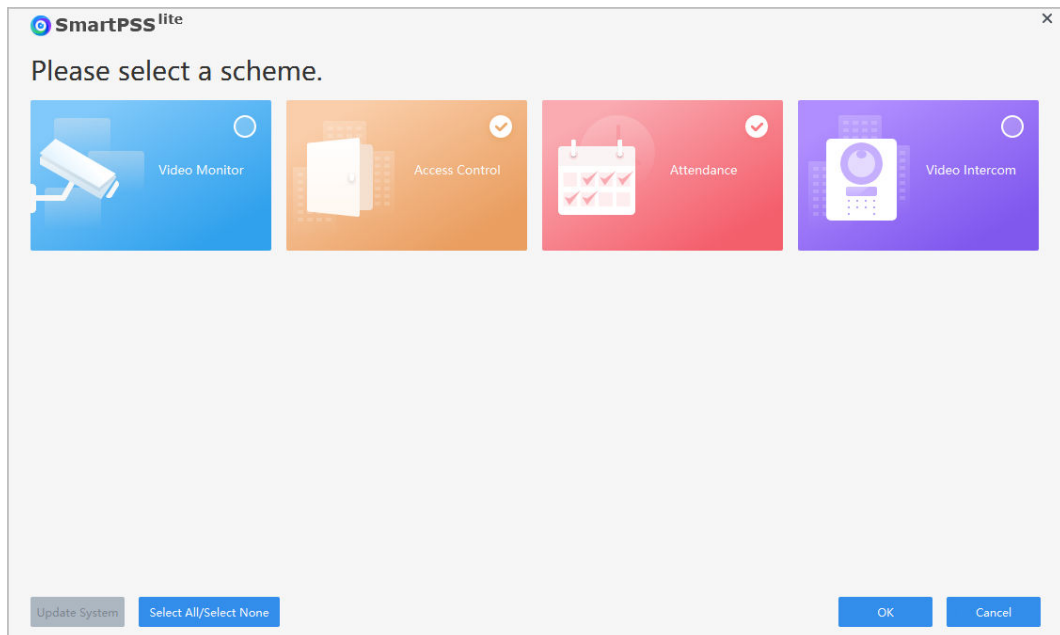
Selezionare**Esegui SmartPSSlite**per avviare SmartPSS Lite.

Figura 4-3 Installazione completata



Passo 5 Seleziona le scene dell'applicazione che desideri aggiungere, quindi fai clic**OK**.

Figura 4-4 Selezione di scenari applicativi



Passo 6 Clic**Accetto e continuo** per concordare **Contratto di licenza software** **Informativa sulla privacy del prodotto**.

Passo 7 Imposta la password su **Inizializzazione** pagina e quindi fai clic **Prossimo**.

Figura 4-5 Imposta password

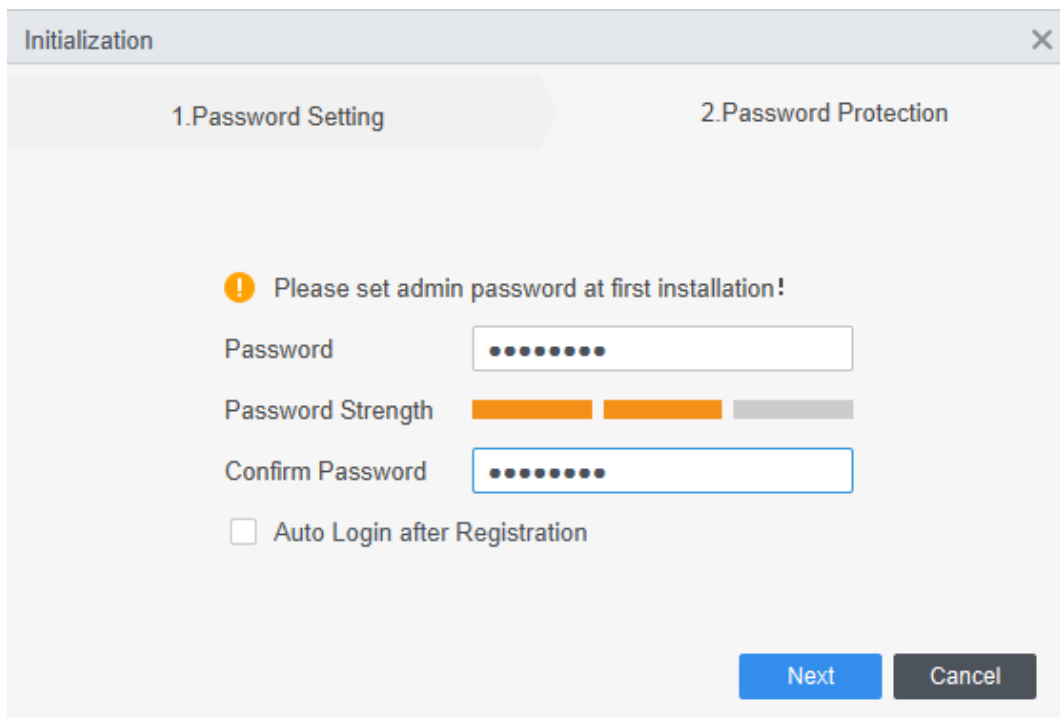


Tabella 4-1 Parametri di inizializzazione

Parametro	Descrizione
Password	La password deve essere composta da 8 a 32 caratteri non vuoti e contenere almeno due tipi di caratteri tra maiuscole, minuscole, numeri e caratteri speciali (esclusi ' " ; : &).
Forza della password	Mostra l'efficacia di una password contro tentativi di indovinare o attacchi di forza bruta. Il verde indica che la password è sufficientemente sicura, mentre il rosso indica che è meno sicura. Imposta una password con un livello di sicurezza elevato in base alle indicazioni sulla robustezza della password.
Conferma password	Inserisci nuovamente la password per confermarla.
Accesso automatico dopo la registrazione	Abilitare Accesso automatico dopo la registrazione in modo che SmartPSS Lite effettui l'accesso automaticamente dopo l'inizializzazione; altrimenti viene visualizzata la pagina di accesso.

Passo 8 Imposta le domande di sicurezza, quindi fai clic **Fine**.

Figura 4-6 Imposta le domande di sicurezza

The screenshot shows a window titled 'Initialization' with a close button (X) in the top right corner. Inside, there are two tabs: '1.Password Setting' (active) and '2.Password Protection'. Below the tabs, there is a warning icon and the text 'Please set security questions!'. Three sets of questions are provided, each with a dropdown menu for the question and a text input field for the answer. The questions are: 'What is your favorite children's book?', 'What was the first name of your first boss?', and 'What is the name of your favorite fruit?'. At the bottom right, there is a blue button labeled 'Finish'.

4.3 Accesso

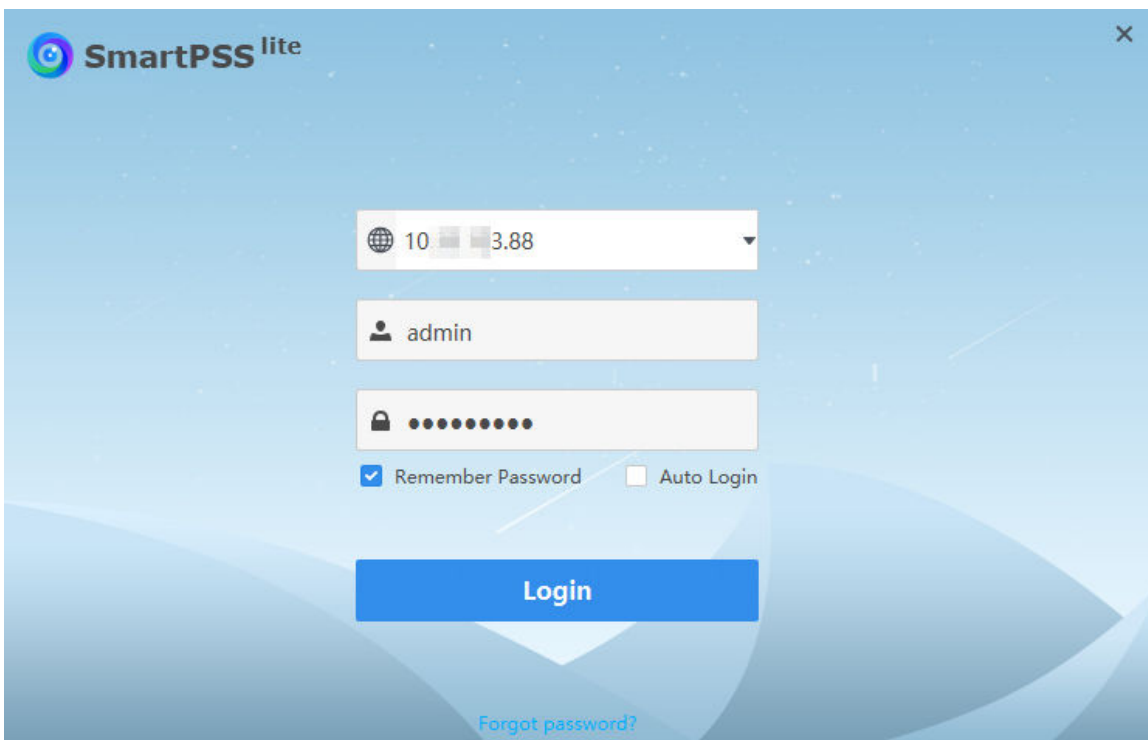
Procedura

Passo 1 Fare doppio clic su SmartPSSLite.exe.

Passo 2 Inserisci nome utente e password, quindi fai clic **Login**.

Se sul computer sono disponibili più reti, è possibile selezionarne una.

Figura 4-7 Accesso



The image shows the login screen for SmartPSS lite. At the top left is the logo 'SmartPSS lite' and a close button 'X' at the top right. The background is a light blue gradient with abstract shapes. The login form is centered and includes:

- A dropdown menu showing a globe icon, the number '10', and '3.88'.
- A text input field containing 'admin' with a user icon on the left.
- A password input field with a lock icon on the left and ten dots representing the password.
- Two checkboxes: 'Remember Password' (checked) and 'Auto Login' (unchecked).
- A large blue 'Login' button.
- A link 'Forgot password?' at the bottom.

Tabella 4-2 Parametri di accesso

Parametro	Descrizione
Ricordare Password	Abilitare Ricorda la password in modo da non dover inserire nuovamente la password al prossimo accesso.
Accesso automatico	Abilitare Accesso automatico in modo che SmartPSS Lite effettui l'accesso automaticamente la prossima volta che utilizzerai lo stesso account utente.
Ha dimenticato la password?	Clicca Ha dimenticato la password? per reimpostare la password tramite domande di sicurezza quando la si dimentica.

Appendice 1 Raccomandazione di sicurezza

Gestione account

1. Utilizzare password complesse

Si prega di fare riferimento ai seguenti suggerimenti per impostare le password:

- La lunghezza non deve essere inferiore a 8 caratteri;
- Includi almeno due tipi di caratteri: lettere maiuscole e minuscole, numeri e simboli;
- Non inserire il nome dell'account né il nome dell'account in ordine inverso;
- Non utilizzare caratteri consecutivi, come 123, abc, ecc.;
- Non utilizzare caratteri ripetuti, come 111, aaa, ecc.

2. Cambiare le password periodicamente

Si raccomanda di cambiare periodicamente la password del dispositivo per ridurre il rischio che venga indovinata o violata.

3. Assegnare account e autorizzazioni in modo appropriato

Aggiungere gli utenti in modo appropriato in base ai requisiti di servizio e di gestione e assegnare a ciascun utente i set minimi di autorizzazioni.

4. Attiva la funzione di blocco dell'account

La funzione di blocco dell'account è abilitata per impostazione predefinita. Si consiglia di mantenerla attiva per proteggere la sicurezza dell'account. Dopo diversi tentativi di accesso errati, l'account e l'indirizzo IP di origine corrispondenti verranno bloccati.

5. Impostare e aggiornare tempestivamente le informazioni per il ripristino della password.

Il dispositivo supporta la funzione di reimpostazione della password. Per ridurre il rischio che questa funzione venga utilizzata da malintenzionati, in caso di modifiche alle informazioni, si prega di aggiornarle tempestivamente. Quando si impostano le domande di sicurezza, si consiglia di non utilizzare risposte facili da indovinare.

Configurazione del servizio

1. Abilita HTTPS

Si raccomanda di abilitare HTTPS per accedere ai servizi web tramite canali sicuri.

2. Trasmissione crittografata di audio e video

Se i contenuti audio e video sono molto importanti o sensibili, si consiglia di utilizzare la funzione di trasmissione crittografata per ridurre il rischio che vengano intercettati durante la trasmissione.

3. Disattiva i servizi non essenziali e utilizza la modalità sicura.

Se non necessari, si consiglia di disattivare alcuni servizi come SSH, SNMP, SMTP, UPnP, hotspot AP ecc., per ridurre le superfici di attacco.

Se necessario, si raccomanda vivamente di scegliere modalità sicure, tra cui, a titolo esemplificativo ma non esaustivo, i seguenti servizi:

- SNMP: scegli SNMP v3 e imposta password di crittografia e autenticazione robuste.
- SMTP: scegli TLS per accedere al server di posta.
- FTP: scegli SFTP e imposta password complesse.
- Hotspot AP: scegli la modalità di crittografia WPA2-PSK e imposta password complesse.

4. Modifica le porte HTTP e altre porte di servizio predefinite

Si consiglia di modificare la porta predefinita di HTTP e di altri servizi, impostandola su una porta compresa tra 1024 e 65535, per ridurre il rischio di essere individuati da malintenzionati.

Configurazione di rete

1. Abilita lista consentita

Si consiglia di attivare la funzione di lista di indirizzi consentiti e di autorizzare l'accesso al dispositivo solo agli indirizzi IP presenti nella lista. Pertanto, assicurarsi di aggiungere alla lista di indirizzi consentiti sia l'indirizzo IP del computer che quello del dispositivo di supporto.

2. associazione indirizzo MAC

Si raccomanda di associare l'indirizzo IP del gateway all'indirizzo MAC del dispositivo per ridurre il rischio di ARP spoofing.

3. Creare un ambiente di rete sicuro

Al fine di garantire al meglio la sicurezza dei dispositivi e ridurre i potenziali rischi informatici, si raccomanda quanto segue:

- Disabilitare la funzione di port mapping del router per evitare l'accesso diretto ai dispositivi della rete intranet dalla rete esterna;
- In base alle effettive esigenze di rete, partizionare la rete: se non vi è alcuna richiesta di comunicazione tra le due sottoreti, si consiglia di utilizzare VLAN, gateway e altri metodi per partizionare la rete e ottenere l'isolamento della rete;
- Implementare un sistema di autenticazione degli accessi 802.1x per ridurre il rischio di accessi non autorizzati alla rete privata da parte dei terminali.

Audit di sicurezza

1. Controlla gli utenti online

Si raccomanda di controllare regolarmente gli utenti online per identificare quelli che utilizzano metodi illegali.

2. Controlla il registro del dispositivo

Consultando i log, è possibile ottenere informazioni sugli indirizzi IP che tentano di accedere al dispositivo e sulle operazioni principali eseguite dagli utenti connessi.

3. Configurare il registro di rete

A causa della capacità di archiviazione limitata dei dispositivi, la quantità di log memorizzati è limitata. Se è necessario conservare i log per un lungo periodo, si consiglia di abilitare la funzione di registrazione di rete per garantire la sincronizzazione dei log critici con il server di log di rete ai fini della tracciabilità.

Sicurezza del software

1. Aggiornare il firmware in tempo

Secondo le specifiche operative standard del settore, il firmware dei dispositivi deve essere aggiornato tempestivamente all'ultima versione per garantire che il dispositivo disponga delle funzionalità e della sicurezza più recenti. Se il dispositivo è connesso a una rete pubblica, si consiglia di abilitare la funzione di rilevamento automatico degli aggiornamenti online, in modo da ricevere tempestivamente le informazioni sugli aggiornamenti del firmware rilasciate dal produttore.

2. Aggiornare tempestivamente il software client

Si raccomanda di scaricare e utilizzare il software client più recente.

Protezione fisica

Si raccomanda di adottare misure di protezione fisica per i dispositivi (in particolare per i dispositivi di archiviazione), come ad esempio collocarli in una sala macchine e in un armadio dedicati e di disporre di un sistema di controllo degli accessi.

e un sistema di gestione delle chiavi per impedire al personale non autorizzato di danneggiare l'hardware e altre apparecchiature periferiche (ad esempio, unità flash USB, porta seriale).

Hiltron Land S.r.l.

Strada Provinciale di Caserta, 218 - 80144 - Napoli

t: +39 081 185 39 000

www.hiltronsecurity.net
